REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE SAAD DAHLAB DE BLIDA

Faculté des sciences
Département d'Informatique

Mémoire présenté par :

M^elle HAMZAOUI Nesrine

En vue d'obtenir le diplôme de Master

Domaine : Mathématiques et Informatique (MI)
Filière : Informatique
Spécialité : Informatique
Option : Ingénierie du Logiciel

Sujet :

DEVELOPPEMENT ET DEPLOIEMENT D'UNE PKI :

APPLICATION « E-BANKING »

Proposé par :

M^elle BOUSTIA Narhimène

Encadré par :

M^me AOUCHETA K.Sabrina

Soutenue devant le jury composé de :

W. HADJ YAHIA	Président
M. FERFERA	Examinateur
I. AZZOUZ	Examinatrice

Année Universitaire 2010/2011

ملخص

الابتكار التكنولوجي في يومنا هذا، يغير عاداتنا. الإنترنت تعدت حدود المكانية-الزمنية، لم نعد بحاجة للتنقل لمعرفة رصيد حسابنا المصرفي أو لإجراء التحويلات المصرفية المختلفة أو حتى دفع الفواتير. الخدمات المصرفية الالكترونية تسعى لاستبدال هذه العمليات التقليدية وتوفير الكثير من الوقت للأشخاص الذين يستخدمون هذه الخدمات.

غير أن، الاتصالات عبر الانترنت ليست آمنة من الهجمات التي تهدف لاعتراض المعلومات السرية، لانتحال صفة زبون أو إدخال معلومات خاطئة.

الهدف من مشروعنا هو مواجهة هذه الهجمات و تقديم بيئة آمنة للزبائن من خلال المصادقة على هويتهم، و ضمان سرية و سلامة المعلومات المتبادلة. البروتوكول «SSL/TLS» و البنية التحتية بالمفتاح العام « PKI » سوف يكونان حلولنا ضد هذه الهجمات .

كلمات المفاتيح : الخدمات المصرفية الالكترونية، *امن شبكة الانترنت*، *التشفير بالمفتاح العام*، البنية التحتية بالمفتاح العام PKI , SSL/TLS .

Résumé

L'innovation technologique aujourd'hui, change nos habitudes. L'Internet a franchit les limites spatio-temporelles. Nous n'avons plus besoin de se déplacer pour consulter notre compte bancaire ou de faire les différentes transactions bancaires, ou même le paiement des factures. L'e-banking vient remplacer ces traditions et économiser beaucoup de temps aux gens qui utilisent ces services.

Cependant, les communications via le réseau Internet ne sont pas à l'abri d'attaques visant à intercepter les informations confidentielles, d'usurper l'identité d'un client ou d'injecter de fausses informations.

L'objectif de notre projet est de faire face à ces attaques et offrir un environnement sûr aux clients en assurant leurs authentifications, la confidentialité et l'intégrité des données échangées. Le protocole « SSL/TLS » et l'infrastructure à clé publique « PKI » seront nos solutions contre ces attaques.

Mots clés : *e-banking, sécurité web, cryptographie à clé publique « asymétrique », l'infrastructure à clé publique « PKI », SSL/TLS*

Abstract

The technological innovation today, changes our habits. The Internet has cleared the spacio-temporal limits. We no longer need to move to consult our bank account or to do the various bank transactions, or even paying bills. The e-banking is replacing these traditions and save a lot of time for people who use these services.

However, the communications over the Internet are not safe from attacks aiming to intercept confidential information, to usurp client identification or to inject misinformation.

The aim of our project is to face these attacks and offer a safe environment to clients by being sure of their authentication, confidentiality and the integrity of the data exchanged. The « SSL/TLS » protocol and the public key infrastructure « PKI » will be our solutions against these attacks.

Key words: *e-banking, web security, public key cryptography « asymmetric », public key infrastructure « PKI », SSL/TLS.*

Dédicaces

Je dédie ce travail à ceux qui m'ont poussé toujours en avant pour être la meilleure, à mon père et ma mère.

A mes chers frères.

A ma chère amie Batel Sarra.

A mes chères cousines.

A toute ma famille.

A tous mes amies et amis.

A l'équipe de département informatique de la CNEP-Banque réseau Alger centre surtout Mme Aoucheta Sabrina.

Nesrine

Remerciements

Nos remerciements et notre gratitude se portent tout d'abord vers M^elle^ Boustia Narhimène, notre promotrice enseignante chercheuse à l'Université Saad Dahlab de Blida pour l'intérêt qu'elle a porté à notre travail, pour sa disponibilité, pour ses compétences et son ouverture d'esprit.

Nous remerciements également à M^me^ Aoucheta Kheira Sabrina, chargée de l'intérieur du département informatique de la CNEP-Banque réseau Alger centre, qui nous a encadré toute au long de notre travail pour son entière disponibilité, ses conseils, ses encouragements et surtout sa modestie ainsi M^elle^ Kassiwi Hayate.

Nous remercions très sincèrement chacun des membres du jury d'avoir bien voulu d'accepter d'examiner notre travail.

Nous remercions nos amis(e) surtouts Batel Sarra, Boumaza Abed El-karime, Guesmia Khalida et Bouchenafa Aness pour leurs conseils et leurs aides.

Nous adressons également nos remerciements, à tous nos enseignants qui nous ont donnée les bases de la science toute au long de nos cursus universitaire.

Un grand merci à tous ceux qui n'ont épargné le moindre effort, de près ou de loin, pour nous permettre d'accomplir notre projet.

TABLE DES MATIERE

TABLES DES FIGURES

LISTE DES ABREVIATIONS

PKI	Public Key Infrastructure
API	Application Programming Interface
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IT	Information Technology
JSP	JavaServer Pages
J2EE	Java 2 Enterprise Edition
SGBD	Système de Gestion de Bases de Données
UML	Unified Modeling Language
XML	Extensible Markup Language

INTRODUCTION GENERALE

1.1 introduction

L'innovation technologique a touché le domaine de la banque. Des plateformes bancaires à distance, sont en pleine expansion. Clients personnels, entreprises, et autres, tous procurent cette solution leur permettant de rationaliser le temps consacré à des suivis bureaucratiques, et d'engager des économies de frais généraux (déplacement,...etc.). La consultation des comptes bancaires ou le paiement des factures via l'internet connu sous le nom de « e-banking » est basé sur l'accès à des comptes bancaires en ligne, pour consulter ou effectuer des transactions, diffusé par l'intermédiaire du réseau Internet.

Cette innovation technologique rend les ordinateurs personnels et les réseaux informatiques de plus en plus vulnérables face à des attaques destructrices, s'ils ne sont pas correctement sécurisés. Les pirates informatiques, les virus, les employés vindicatifs et même les erreurs humaines sont autant de menaces pesant constamment sur les réseaux. Tous les utilisateurs d'ordinateurs, du simple particulier surfant sur Internet aux grandes entreprises, sont susceptibles d'être affectés par des failles dans la sécurité de leur système.

Il est donc de plus en plus important pour les organisations de bénéficier d'un accès constant et fiable à des plateformes bancaires à distance puissants et efficaces.

1.2 Présentation du sujet

1.2.1 L'organisme d'accueil

L'entreprise concernée par la mise en œuvre est ***CNEP*** « *Caisse National d'Epargne et d'Encaissement* ». Ses clients sont soit des particuliers « clients ordinaires », des personnels « ses propres employeurs », soit des entreprises commerciales.

La Caisse Nationale d'Epargne et de Prévoyance-Banque est spécialisée, depuis sa création le 10 août 1964, dans la collecte de l'épargne, les crédits immobiliers aux particuliers et le financement des promoteurs publics et privés.

Par ailleurs, la CNEP-Banque intervient dans le financement des projets d'investissement dans les secteurs de l'énergie, de l'eau, de la pétrochimie ou de l'aluminerie.

1.2.2 Problématique

Dans ce contexte née notre problématique qui consiste à mettre en œuvre une plate forme de travail bancaire en ligne « e-banking » et comment mettre les transactions bancaires a l'abri des attaques, c'est-à-dire comment assurer que :

- ✓ Le client communique avec la bonne plateforme.
- ✓ Le client qui accède à la plateforme possède les droits d'accès.
- ✓ Les transactions au sein de la plateforme ne sont pas interceptées ou altérées.

1.2.3 Objectifs

Un tas de questions auxquelles nous allons répondre pour atteindre les objectifs tracés à savoir garantir l'authentification des clients, la confidentialité et l'intégrité des échanges.

Pour la réalisation de notre application, une étude bibliographique portera sur les plateformes e-banking et la sécurité des échanges sur Internet ainsi qu'une étude des infrastructures à clé publique PKI. Nous passerons ensuite à la conception puis la réalisation de notre système. Nous développerons une plate forme e-banking. Nous développerons ensuite une PKI ; une application web qui gère des certificats numériques. Notre PKI sera utilisée pour gérer les certificats numériques de l'ensemble des acteurs de la plateforme e-banking CNEP-Banque sécurisant ainsi l'accès à cette dernière.

1.3 Organisation du mémoire

Ce mémoire est composé d'une introduction générale suivie de deux parties, une partie théorique et une autre pratique.

La première partie sera consacrée à l'étude théorique des grands concepts rencontrés lors de la réalisation de notre projet, structurée en trois chapitres.

- Le premier chapitre va traiter les attaques informatiques et la sécurité web,
- le second s'intéressera à l'infrastructure à clé publique PKI « Public Key Infrastructure » une infrastructure de gestion des certificats numériques.
- Enfin, le troisième chapitre dans lequel nous présenterons le travail bancaire en ligne tout en mettant l'accent sur les plateformes e-banking étant le domaine d'application de notre étude, et une identification des besoins en sécurité de telles plateformes. Nous finirons par une petite représentation de l'organisme d'accueil CNEP-Banque.

Après avoir donné une idée sur les concepts utiles pour la réalisation de notre projet, nous aborderons dans la deuxième partie, le développement de notre solution suivant la méthode en Cascade.

- Dans la première partie, on décrit et délimite les parties à développer. Nous verrons en premier temps une modélisation UML détaillée décrit notre plate forme e-banking, ensuite la modélisation de notre PKI.
- Dans la deuxième partie nous présenterons l'architecture technique de notre PKI avec justification de nos choix en matière d'environnement de développement (serveurs, langage, …etc.). Une présentation détaillée du fonctionnement de la plate forme e-banking ainsi notre PKI.

Nous terminerons par une conclusion générale, quelques perspectives et des annexes.

Nous présentons dans la première annexe quelques algorithmes à clé publique, et dans la deuxième annexe le langage de modélisation UML.

CHAPITRE 1

Attaques et Sécurité informatiques

1.1 Introduction

Depuis quelques années, la révolution des moyens de communication, particulièrement l'Internet a mené à une large liberté en circulation d'informations confidentielles et une haute disponibilité de nombreuses ressources. Ceci a fait naître de nouveaux problèmes en sécurité informatique donc de nouveaux besoins.

Pour parer à ces problèmes il est nécessaire de connaître les différentes menaces existantes, ainsi que les vulnérabilités présentent sur un tel système, pour établir une stratégie de sécurité fiable contre ces attaques.

Donc dans ce premier chapitre. On étudiera les différentes faiblesses du système, et les attaques exploitant ces failles. On introduira après les principaux mécanismes et outils de la sécurité web. Cette investigation va nous permettra par la suite d'étudier les étapes nécessaires pour mener une stratégie de sécurité fiable.

1.2 Les attaques informatiques

1.2.1 Définition d'une attaque

Une « attaque » est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables [1].

1.2.2 Définition d'un Pirate (hacker)

Un hacker est une personne qui quelle que soit sa motivation, pénètre sans autorisation et de manière illégale, dans un système appartenant à tiers [3].

1.2.3 Etapes de réalisation d'une attaque

La première phase est de **collecte d'information** et de **recherche de vulnérabilité** d'un système a pour objet de récolter le maximum d'informations sur le système ciblé. Cela consiste essentiellement à prendre connaissance des mécanismes et des niveaux de sécurité en vigueur concernant, l'identification, le contrôle d'accès, la cryptographie, la surveillance et identifier **les failles techniques, organisationnelle et humaine de l'environnement**.

De plus, le fraudeur s'emploiera à détecter et à **exploiter les failles de la sécurité** connus mais non encore réparées et à utiliser les outils d'attaque accessibles en ligne (bibliothèques d'attaque contenant des logiciels, par exemple).

La phase d'**exfiltration** a pour objectifs principaux de faire en sorte que l'attaque ne soit pas détecter et que l'attaquant ne laisse pas de trace pouvant servir à son identification. Pour

contribuer à cela, le malveillant s'emploiera à rester anonyme, à utiliser des alias (pseudonymes), à usurper l'identité numérique d'utilisateurs ou encore à brouiller les pistes en passant par plusieurs systèmes intermédiaires [2].

1.2.4 Les malwares

Un malware est un logiciel développé dans le but de nuire à un système informatique. Il existe plusieurs familles des malwares [5]. On va définir les plus intéressants :

a. Virus

C'est un programme malveillant introduit à l'insu des utilisateurs dans un système, il possède la capacité de se dupliquer (s'auto-reproduire) [2].

b. Cheval de Troie

Un programme ou un code malveillant est intégré à une application par ajout ou par modification de son code. Ainsi lors de l'exécution de ce programme inoffensif, le bout de code malveillant pourra exécuter des commandes spécifiques (récupération de fichiers de mot de passe, altération du système, etc.) à l'insu de l'utilisateur [4].

c. Ver

Un ver informatique est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier, etc.) pour se propager [4].

d. Spyware

Les Spywares ou Espiogiciels permettent de connaître l'activité exécutée sur l'ordinateur infecté. On y retrouve: Les Keyloggers et les Tempests [3].

- **Key logger:** Un keylogger (littéralement enregistreur de touches) est un dispositif chargé d'enregistrer les frappes de touches du clavier, à l'insu de l'utilisateur.
- **Tempest :** Tempest est un dispositif électronique permettant de capter les émissions électromagnétiques générées par un appareil électrique.

1.2.5 Quelques attaques connues

a. Attaques de mot de passe

- **Attaque par force brute :** On appelle « **attaque par force brute** » le cassage d'un mot de passe en testant tous les cas possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération [1].

* **Attaque par dictionnaire :** Les outils d'attaque par force brute peuvent demander des heures, voire des jours, de calcul même avec des machines équipées de processeurs puissants. Ainsi, une alternative consiste à effectuer une « **attaque par dictionnaire** ».

Le programme utilise une liste de mots prédéfinis dans un fichier externe. Cette liste est appelée un dictionnaire ; ces mots sont la plupart du temps ceux provenant d'un dictionnaire contenant les mots du langage courant. Le programme les encrypte avec l'algorithme d'encryptage adéquat un par un et les compare au mot de passe encrypté [4].

* **Attaque hybride :** Le dernier type d'attaques de ce type, appelées « **attaques hybrides** », vise particulièrement les mots de passe constitué d'un mot traditionnel et suivi d'une lettre ou d'un chiffre (tel que « nesrine5 »). Il s'agit d'une combinaison des attaques précédentes [1].

b. Attaque « Man In The Middle »

L'attaque « **man in the middle** » notée *MITM*, est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie les échanges afin de se faire passer pour l'une des parties [1].

* **ARP Poising :** C'est l'attaque la plus célèbre des attaques « Man In The Middle », consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet ARP falsifié indiquant que l'adresse MAC de l'autre machine a changé, l'adresse MAC fournie étant celle de l'attaquant.

Les deux machines cibles vont ainsi mettre à jour leur table dynamique appelée Cache ARP. De cette manière, à chaque fois qu'une des deux machines souhaitera communiquer avec la machine distante, les paquets seront envoyés à l'attaquant, qui les transmettra de manière transparente à la machine destinatrice [1].

* **Vol de session TCP (TCP session hijacking) :** L'ARP-Poisining permet de rediriger tout le trafic IP mais, si l'attaquant n'a besoin que du trafic TCP, il peut interférer entre une connexion client-serveur pour rediriger le flux du client vers lui. La synchronisation TCP est assurée par les numéros de séquences TCP. Si, pendant un échange, l'attaquant envoie des paquets malformés au client avec une adresse IP correspondant à celle du serveur en y plaçant des mauvais numéros de séquences, le client va croire qu'il a perdu la connexion et stoppera ses échanges avec le serveur. Mais si l'attaquant envoie les bons numéros de séquences au serveur, il récupèrera la connexion pour lui [4].

1.2.6 Les Sniffers

Un Sniffer « analyseur réseau » est un dispositif permettant *d'écouter* le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent [1].

1.3 Sécurité web

1.3.1 Définition de la sécurité informatique

La sécurité informatique c'est l'ensemble des moyens et méthodes mis en œuvre pour assurer la protection des ressources [1].

Le **risque** en termes de sécurité est généralement caractérisé par l'équation suivante :

$$Risque = \frac{Vulnérabilité \times Menace}{ContreMesure}$$

- **La menace** « threat » **:** représente le type d'action susceptible de nuire dans l'absolu ;
- **La vulnérabilité:** représente le niveau d'exposition face à la menace dans un contexte particulier ;
- **La contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace.

1.3.2 Cryptographie

La cryptographie est à la base de la sécurité informatique, sa connaissance est nécessaire pour comprendre les technologies de sécurité utilisées pour sécuriser les réseaux.

Le mot **cryptographie** vient du grec *kryptos* « caché » et *graphein* « écrire » [10].

La **cryptographie** est la science d'écriture et de lecture des messages codés [10]. Elle permet de transmettre des données de manière confidentielle. [13]

Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible, c'est ce qu'on appelle **chiffrement** ou **cryptage**, qui à partir d'un texte en claire donne un texte chiffré ou **cryptogramme**. Inversement, le **déchiffrement** ou **décryptage** est l'action qui permet de reconstituer le texte en claire à partir du texte chiffré.

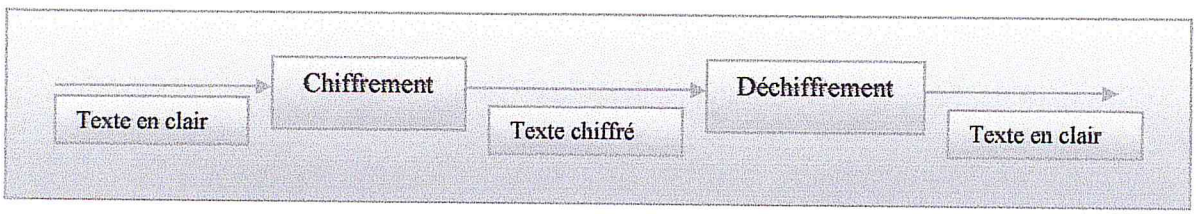


Figure I.1 : Principe générale de la cryptographie.

Dans la cryptographie moderne, les transformations en questions sont des fonctions mathématiques, appelées algorithmes cryptographiques qui dépendent d'un paramètre appelé **clé**.

D'autres termes se réfèrent à ce domaine tel que la **cryptanalyse** qui est l'étude des procédés cryptographiques dans le but de pouvoir décrypter des textes chiffrés et la **cryptologie** qui englobe les deux domaines : cryptographie et cryptanalyse. [13]

1.3.3 Les besoins cryptographiques

Transmettre des données de manière confidentielle, tel était le but de la cryptographie traditionnelle. Aujourd'hui la confidentialité ne suffit plus. Des services de sécurité plus élaborés sont offerts. En plus de la confidentialité, l'authentification, l'intégrité et la non répudiation sont les garanties de la cryptographie moderne

a. L'intégrité

L'**intégrité** permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.

b. La confidentialité

La confidentialité est le maintien du secret des informations… (Le petit Robert[1]).

La confidentialité peut être vue comme la protection des données contre une divulgation non autorisée.

c. L'identification et l'authentification

Un nom associé à des caractéristiques identifie une entité : individu, ordinateur, programme, document, etc. L'**identification** est la reconnaissance de cette entité.

L'**authentification** permet de vérifier l'identité annoncée et de s'assurer de la non-usurpation de l'identité d'une entité. Pour cela, l'entité devra produire une information spécifique telle que par exemple un mot de passe (un code, un mot de passe, une empreinte biométrique, etc.).

d. La non-répudiation

Est le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu.

1.3.4 Les méthodes de cryptographie

a. La cryptographie à clé secrète

[1] ***Le Petit Robert*** est un dictionnaire de langue française, publié par les dictionnaires Le Robert.

a.1 Principe

Les systèmes à clé secrète « *ou symétrique* » utilisent une **même clé** et un **même algorithme** de chiffrement pour chiffrer et déchiffrer un message. Donc les communicants doivent s'entendre par avance sur l'algorithme de chiffrement à employer et également sur la clé secrète à utiliser avec l'algorithme [10].

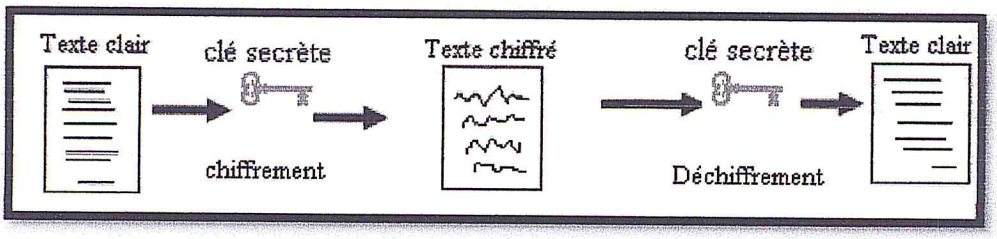


Figure I.2 : Chiffrement à clé secrète [11]

a.2 Quelques algorithmes de chiffrement symétrique

- **Substitution :** Le code de César est le plus vieil algorithme de chiffrement symétrique par substitution connu. Il consiste à remplacer chaque lettre du message d'origine par une lettre de l 'alphabet situé n positions plus loin (par une simple translation). N constitue la clé secrète. [10]

Exemple : La clé est 3

Texte claire	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
Texte chiffré	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

- **Transposition:** Le principe de codage par transposition est de modifier selon une loi prédéfinie l'ordre des caractères. [11]

La méthode de pliage constitue un exemple simple de chiffrement par transposition. Elle consiste à écrire le message d'origine dans une matrice « écriture en ligne » comportant autant de colonnes que la clé secrète. La clé secrète est constituée de numéros de colonnes. Le cryptogramme est obtenu en lisant cette matrice en colonnes selon l'ordre défini par la clé

Exemple :

Le message d'origine: UNE PLANCHE A VOILE

La clé de codage : 4312

Le message crypté : PCVE ENAL ULHO NAEL

1	2	3	4
U	N	E	P
L	A	N	C
H	E	A	V
O	I	L	E

* **Le codage DES, combinaison de substitution et transposition :** L'algorithme DES, « *Data Encryption Standard* », a été créé dans les laboratoires de la firme IBM. C'est un chiffrement qui transforme des blocs de **64 bits** avec une clé secrète de **56 bits** au moyen de permutations et de substitutions.

La clé est en fait constituée de 64 bits, dont 56 bits sont générés aléatoirement et utilisés dans l'algorithme. Les huit autres bits peuvent être utilisés pour la détection d'erreurs (bits de parité) [11].

a.3 Problème de la cryptographie à clé secrète

La cryptographie à clé secrète présente l'inconvénient de la complexité de gestion des clés secrètes vu les causes suivantes : [10]

* Pour n personnes communicantes, il faut gérer **n*(n-1)/2** clés (car chaque deux communicants possèdent leur propre clé de chiffrement). Pour une centaine de personne par exemple, il faut 4950 clés, ce qui n'est pas pratique pour sécuriser les communications au sein d'une organisation avec des milliers de communicants ;
* Les clés secrètes doivent être changé fréquemment pour éviter quelles ne soient découvertes ;
* L'échange de clés secrètes doit être sécurisé.

Ces problèmes ont incité à la réflexion à une autre méthode cryptographique plus sûre et moins complexe en matière de gestion. La cryptographie à clé publique est apparue.

b. La cryptographie à clé publique

b.1 Principe

Dans la cryptographie à clé publique « *ou cryptographie asymétrique* » chaque communicant utilisent deux clés, l'une est connue par tous « *clé publique* », l'autre n'est connue que par lui-même « *clé privée* ». Le message crypté avec l'une ne peut être décrypté qu'avec l'autre [11]

Les deux clés sont reliées mathématiquement entre elles de telle sorte qu'il est impossible de retrouver la clé privée en connaissant la clé publique. Les astuces mathématiques utilisées dans les algorithmes à clé publique sont présentées dans l'annexe 1.

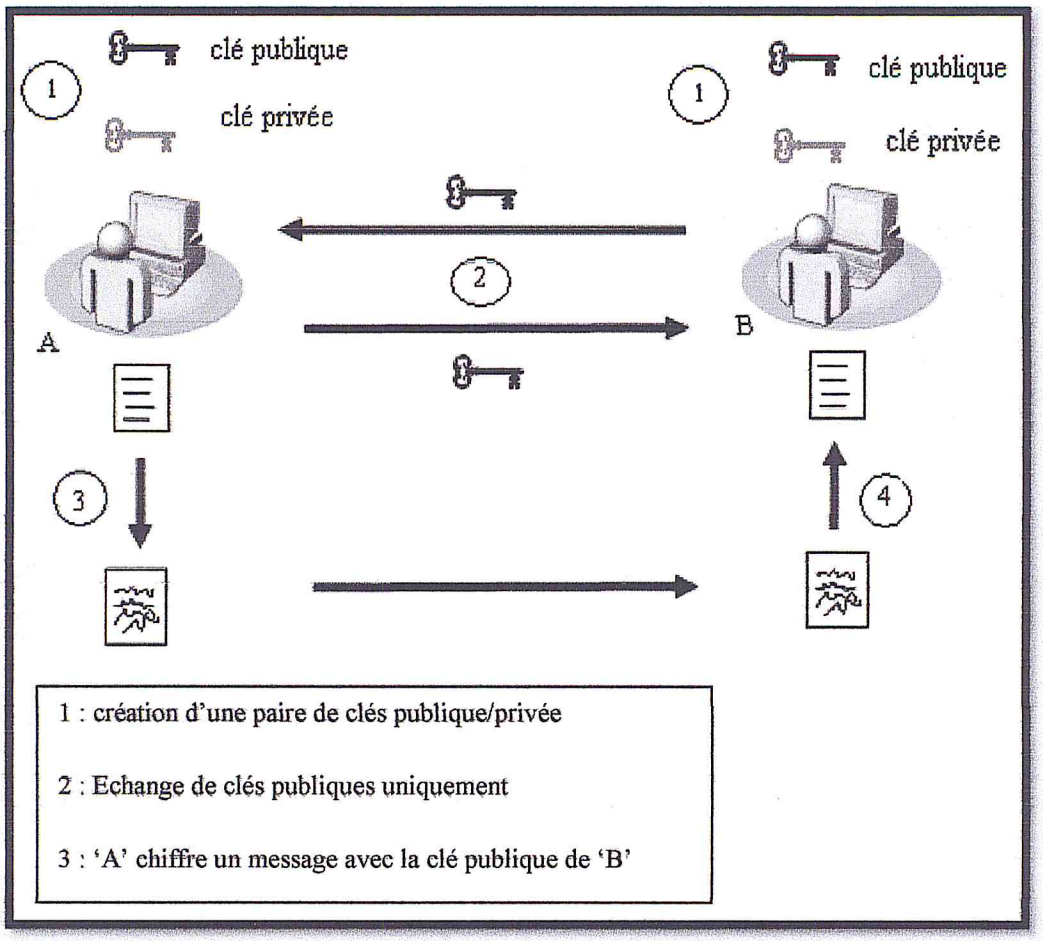


Figure I.3 : Chiffrement à clé publique

b.2 Quelques algorithmes à clé publique

- **Le codage RSA :** Inventé à la fin des années 1970, il utilise des clés très longues (jusqu'à 1024 bits) et offre toutes les garanties cryptographiques (confidentialité, intégrité, authentification et non répudiation). La sécurité apportée par le système RSA se fonde sur la difficulté à factoriser le produit de deux grands nombres premiers. Le RSA reste sécurisé face aux attaques, mais on doit employer des nombres premiers de plus en plus grands, car la puissance des microprocesseurs croît sans cesse (plus de détaille dans l'annexe 1).
- **Le codage DSA :** Le DSA « *Digital Signature Algorithm* » a été adopté en tant que standard **FIPS** (Federal Information Processing standard) au début des années 1990, il a été révisé en 1998.

Comme pour le RSA, le DSA assure l'authentification, l'intégrité, et la non-répudiation. Mais contrairement au RSA, le DSA ne peut servir à la confidentialité (plus de détailles dans l'annexe 1).

b.3 Certificat numérique et autorité de certification

Le principal avantage de la cryptographie à clé publique est qu'elle permet à des utilisateurs n'ayant pas d'accord de sécurité préalable d'échanger des messages de manière sûre. En effet, ces utilisateurs n'auront plus besoin d'échanger la clé secrète qui serait utilisée pour chiffrer les données échangées entre eux ; toutes les communications impliquent uniquement des clés publiques, et aucune clé privée n'est jamais transmise ou partagée.

Le problème posé par les systèmes cryptographiques à clé publique, est le fait que les utilisateurs doivent s'assurer qu'ils chiffrent leurs messages en utilisant la véritable clé publique de leur destinataire. Afin de confirmer l'appartenance d'une clé à son propriétaire supposé, on utilise le principe de certificats numériques qui font appel à une partie tiers appelé autorité de certification.

* **Certificat numérique :** Un certificat numérique fonctionne comme une pièce d'identité. C'est une information attachée à une clé publique, signé numériquement par une partie tierce de confiance (autorité de certification). L'objet de la signature est de garantir que les informations de certification ont été contrôlées et validées.

  Les certificats numériques sont utilisés donc pour empêcher les tentatives de falsification de clé publique [12].

* **Le standard X509 :** Les certificats requièrent un format commun et ils s'appuient actuellement en grande partie sur le standard X.509.

  X.509 est un standard de cryptographie de l'UIT « *Union Internationale des Télécommunications* ». Il a été crée en 1988 [14].

  Un certificat au format **X509** version3 contient les données énumérées dans la figure suivante : [6]

Version du certificat (certificate format version)
Numéro de série du certificat (certificate serial number)
Description de l'algorithme de signature de l'autorité de certification AC (signature algorithm identifier for certificate authority CA)
Nom de l'AC qui a généré le certificat (issuer x.500 name)
Période de validité (validity period)
Nom de l'utilisateur auquel appartient le certificat (Subject X.500 name)

Clé publique (subject public key)
Description de l'algorithme à utiliser avec la clé publique (subject public key information)
Identification possible de l'AC (optionnel) (issuer unique identifier)
Identification possible de l'utilisateur (optionnel) (subject unique identifier)
Extensions (optionnel)
Signature de l'AC (CA signature)

Figure I.4 : Format d'un certificat X.509 V3

* **Autorité de certification AC :** L'autorité de certification est une partie tierce de confiance qui se porte garante de la validité de certificats numériques.

  L'autorité de certification délivre, distribue les certificats numériques et elle les révoque en cas où les informations qu'ils contiennent ne sont plus valables [12].

b.4 Problème de la cryptographie à clé publique

Les méthodes de chiffrement à clé publique (RSA/DSA) sont jusqu'à 1000 fois plus lentes que les méthodes de chiffrements à la clé secrète (DES) [10].

c. Hachage

c.1 Principe

Le hachage « appelé aussi résumé de message ou empreinte numérique » est une représentation plus bref d'un message. [10]

La fonction de hachage reçoit en entrée un message de longueur aléatoire et produit un message de longueur fixe.

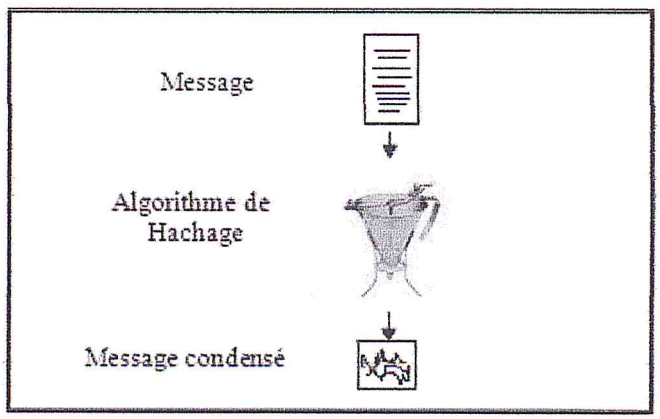


Figure I.5 : Principe du hachage.

Un algorithme de hachage doit être [12] :

- Cohérent : le même message en entrée doit toujours produire le même résultat.
- Aléatoire : ou en donne l'impression pour empêcher la découverte de message d'origine.
- Unique : deux messages différents ne doivent jamais produire le même condensé.
- Non réversible : il doit être extrêmement difficile, voir impossible d'obtenir le message d'origine à partir de son condensé.

Le hachage est généralement utilisé pour fournir une empreinte d'un message ou fichier pour assurer l'intégrité et l'authentification du message.

c.2 Type de hachage

Selon que l'algorithme de hachage utilise une clé ou non, on distingue trois types de hachage :

* **Hachage sans clé : MIC** « *Message Integrity Code* »

Dans ce type, le message est soumis à un algorithme de hachage sans clé (sans paramètre en entrée). Les algorithmes les plus utilisés sont MD5 et SHA1.

La plupart des signatures numériques à clé publique emploient des résumés de message sans clé.

* **Hachage avec clé : MAC** « *Message Authentification Code* »

Dans ce type, le message est soumis à une fonction de hachage qui reçoit comme paramètre d'entrée une clé.

* **HMAC :** « *keyed-hash message authentication code* »

Le HMAC combine les deux méthodes précédentes. Le message est concaténé à une clé secrète. Le tout est soumis à une fonction de hachage sans clé.

d. Signature numérique

d.1 Définition

Une signature numérique est un **condensé de message crypté** qui joint un document. Elle combine l'utilisation du cryptage à clé publique et d'une fonction de hachage.

d.2 Processus de création d'une signature

1. Créer une paire de clés publique/ privée
2. Soumettre le message à une fonction de hachage
3. Crypter le résultat de hachage avec la clé privée

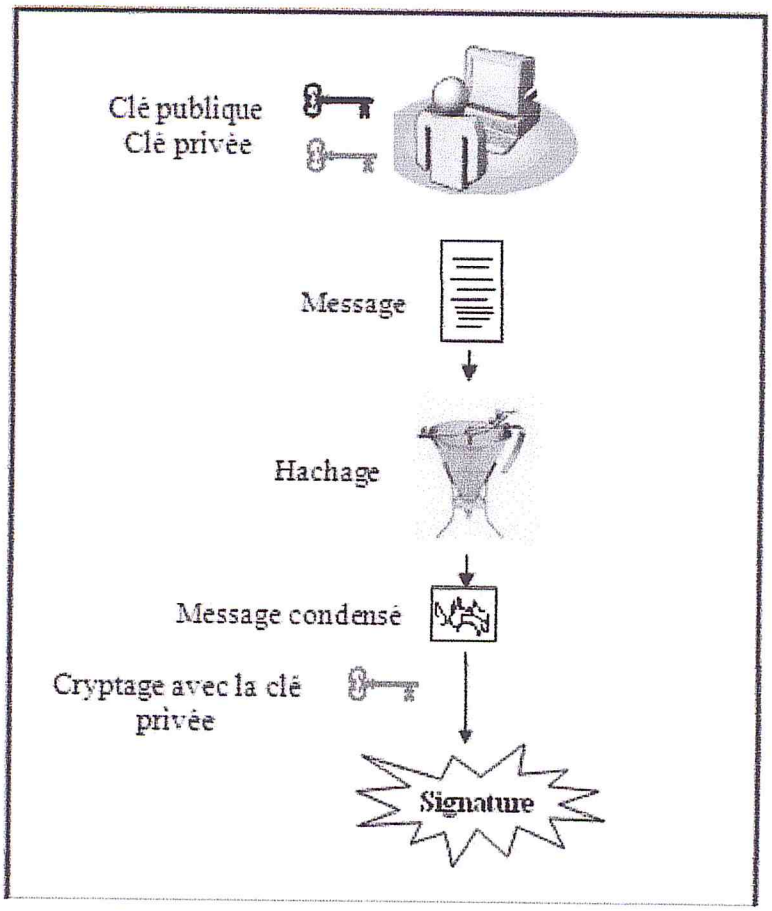


Figure I.6: processus de création d'une signature

Remarque :

L'émetteur envoie au destinataire son message en lui concaténant la signature obtenue et la clé publique (ou un certificat numérique contenant la clé publique). La clé publique servira pour la vérification de la signature.

d.3 Processus de vérification d'une signature

Le destinataire reçoit un message signé par une clé privée. La clé publique correspondante à cette dernière est à sa disposition. Pour vérifier cette signature et donc vérifier que le message provient du bon émetteur, il procède ainsi :

1. Séparer la signature du message
2. Décrypter la signature avec la clé publique de l'émetteur (on obtient ainsi le résumé du message originale).
3. Soumettre le message à la même fonction de hachage (les communiquant s'entendent sur l'algorithme de hachage avant de commencer l'échange de message)
4. Comparer le résumé obtenu dans 3 avec celui obtenu dans 2.

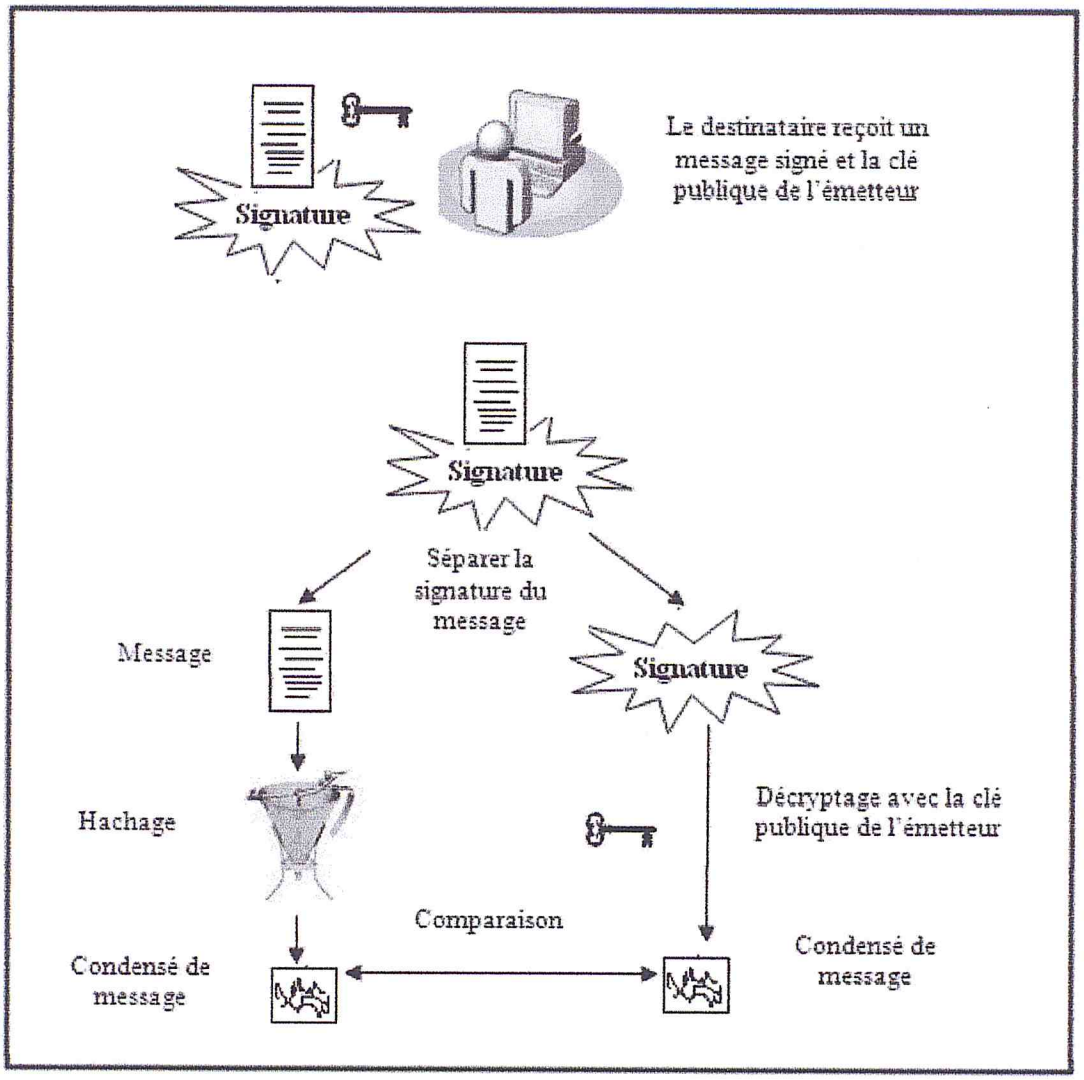


Figure I.7: Vérification d'une signature

1.3.5 SSL « Secure Socket Layer »

SSL est un protocole qui permet la sécurisation d'un canal de communication de type socket (couche TCP). Il assure trois garanties cryptographiques: l'authentification, la confidentialité, et l'intégrité des messages. Il chiffre aussi les données transmises entre un navigateur et un serveur Internet [6].

a. Historique

SSL a été développé par Netscape en 1994. La version 2 a été lancée en 1995.Un produit concurrent de Microsoft « ***PCT*** *Private community Technology* » apparu en 1995 a poussé Netscape à lancer la version3 de SSL dans la même année.

En 1996, l'IETF « *Internet Engineering Task Force* » constitua un comité pour développer et publier un **standard** SSL.

En Janvier 1999, on a publié TLS « *Transport Layer Security* » fondé sur SSL version 3. Il est géré par Microsoft et Netscape [6].

b. Position de la couche SSL dans la pile TCP/IP

TCP/IP « *Transmission Contrôle Protocole/ Internet Protocole* » est un ensemble de standards et de procédures qui permet à une machine de communiquer avec le monde extérieur. Il est reconnu comme le protocole de communication prédominant pour interconnecter différents systèmes informatiques. [11]

Les fonctionnalités de TCP/IP sont regroupées dans quatre couches :

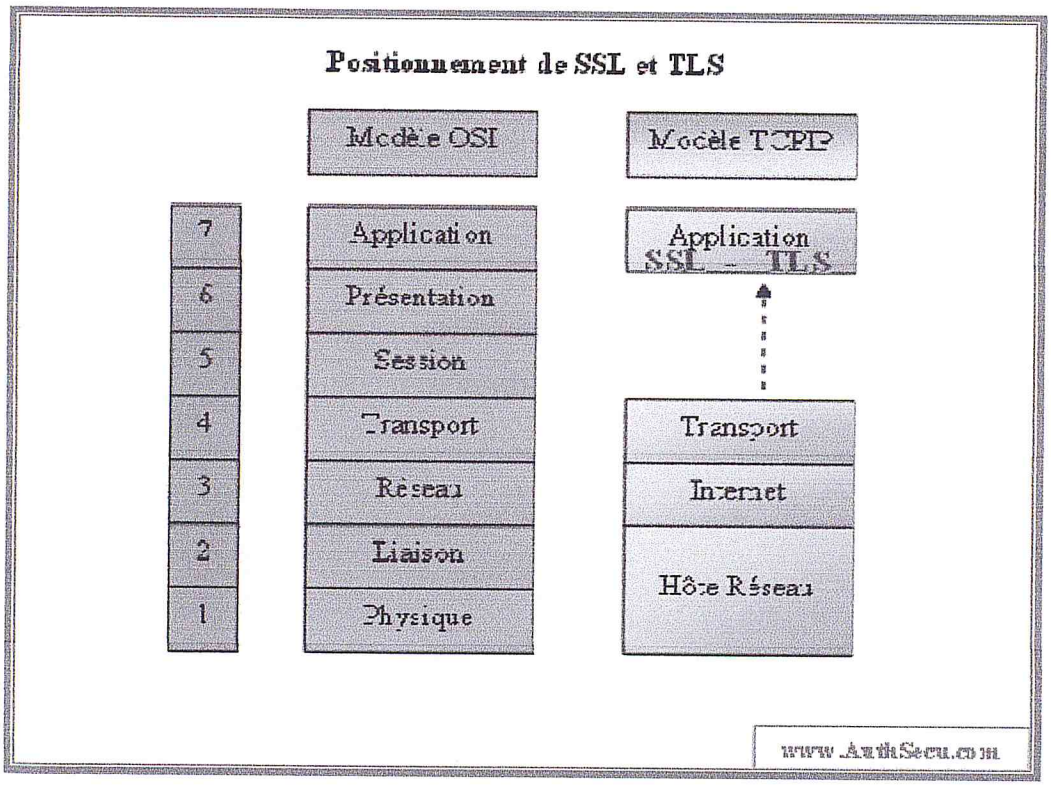


Figure I.8: Couches TCP/IP

- **Couche application:** supporte les applications réseaux telles que HTTP, FTP, etc.
- **Couche transport:** elle assure le contrôle d'erreur, les accusés de réception et sert d'interface aux applications réseaux.
- **Couche Internet:** elle est responsable de la gestion du routage des données.
- **Couche réseau:** elle englobe les routines d'accès aux réseaux physiques tel que conversion des trames en signaux analogique. [11]

Une nouvelle couche est implémentée dans ce modèle, appelé **SSL** « *Secure Socket Layer* ». Elle fonctionne entre la couche application et la couche transport. Elle fournit un mécanisme pour garantir la sécurité des données entre un client et un serveur dans un réseau.

c. Session SSL

SSL combine simultanément l'utilisation de clé asymétriques et de clés symétriques. Il utilise un protocole de négociation qui permet, à l'aide des clés asymétriques des clients et du serveur, d'établir une session qui sera chiffrée à l'aide d'une clé symétrique générée et qui n'est pas valable que pour cette session [6]. Les étapes d'une session SSL sont :

* **La première étape :** dans une session SSL est la négociation des paramètres cryptographiques entre deux ordinateurs. Il faut s'entendre sur la version SSL/TLS, sur la méthode de chiffrement de clé secrète (ex : DES), sur l'algorithme de hachage (ex : SHA-1), et sur l'algorithme d'échange de clé publique (ex : RSA)
* **La deuxième étape :** consiste à échanger les certificats numériques pour s'authentifier.
* **La troisième étape :** dans cette étape on s'accorde sur les clés secrètes échangées: l'émetteur envoie une valeur aléatoire, sur 48 octets, chiffrée avec la clé publique du destinataire. Le destinataire la déchiffre avec sa clé privée.
* **La dernière étape :** d'une session SSL est le chiffrement de données:

d. Problèmes de SSL/TLS

* SSL/TLS ne protège pas contre l'analyse du trafic, c'est à dire contre les cryptanalystes qui s'intéressent aux adresses sources et destinations.
* En effet SSL/TLS est situé au dessus de la couche transport dans la pile des protocoles. Il n'a donc aucun moyen de masquer l'adresse et le port des adresses sources et de destinations.
* La négociation des paramètres cryptographiques se fait en claire sans chiffrement.

e. Applications de SSL

Le protocole SSL permet la sécurisation de tout protocole applicatif qui s'appuie sur la pile TCP/IP, tels que http, LDAP, SMTP, FTP, ...etc. Nous explicitons dans la suite quelques exemples :

e.1 HTTPS

Le HTTP « *HyperText Transfert Protocol* » est le protocole le plus utilisé sur Internet. C'est un protocole client/serveur utilisé pour transférer les documents entre le serveur HTTP et le navigateur web lors de la consultation d'un site web.

HTTP protège peu la confidentialité des données. En effet les documents sont transmis sans être chiffrés.

Pour améliorer la confidentialité, on utilise le protocole HTTPS « HTTP over SSL ».

La sécurité offerte par HTTPS réside dans le fait qu'il authentifie le client et le serveur grâce au certificat numérique. Il chiffre également la communication (garanties apportées par SSL).

Il est généralement utilisé pour les transactions financières en ligne : e-commerce, e-banque. Il est même utilisé lors d'une simple inscription à un site web pour des raisons de confidentialité.

e.2 LDAPS

LDAP « *Lightweight Directory Access Protocol* » est un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. Un annuaire LDAP respecte généralement le modèle X.500 « X.500 désigne l'ensemble des normes informatiques sur les services d'annuaire ».

Pour sécuriser les communications LDAP, l'implémentation de SSL constitue la meilleure solution. A ce moment, on parle de LDAPS (LDAP over SSL).

e.3 SMTPS

Le protocole SMTP « *Simple Mail Transfer Protocol, traduisez Protocole Simple de Transfert de Courrier* » est le protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point. Le courrier est remis directement au serveur de courrier du destinataire. SMTPS est le protocole SMTP au dessus de la couche SSL.

e.4 IMAPS

Le protocole IMAP « *Internet Message Access Protocol* » permet comme son nom l'indique d'aller récupérer son courrier sur un serveur distant « le serveur IMAP ». Il est nécessaire pour les personnes n'étant pas connectées en permanence à Internet afin de pouvoir consulter les mails reçus hors connexion. IMAPS est le protocole IMAP au dessus de la couche SSL.

1.4 Conclusion

Nous avons vu dans ce chapitre la stratégie de sécurité utilisée pour protéger les ressources et assurer les services de la sécurité (l'intégrité, disponibilité, confidentialité). Mais malgré toutes ces planifications, le système reste exposer aux attaques, et le taux de risque existe toujours, donc il n'est possible de mener une stratégie de sécurité où la vulnérabilité et le risque sont nuls.

HTTPS permet au client de vérifier l'identité du site auquel il accède grâce à un certificat d'authentification. La génération de certificat et leur gestion nécessitent une infrastructure à clé publique **PKI** l'objet du chapitre suivant.

CHAPITRE 2

PKI
Infrastructure à clé publique

« Public Key Infrastructure »

« Le seule système infaillible est celui qui est éteint et débranché,

enfermé dans un coffre en titane, enterré dans un block en béton,

entouré d'un nuage de gaz neuroplégique et de garde armé très bien payés.

Même ainsi je ne parierais pas ma vie dessus »

Jim Conallen.

2.1 Introduction

Le principal avantage de la cryptographie à clé publique est qu'elle permet à des utilisateurs n'ayant pas d'accord de sécurité préalable d'échanger des messages de manière sûre. En effet, ces utilisateurs n'auront plus besoin d'échanger la clé secrète qui serait utilisée pour chiffrer les données échangées entre eux ; toutes les communications impliquent uniquement des clés publiques, et aucune clé privée n'est jamais transmise ou partagée.

Le problème posé par les systèmes cryptographiques à clé publique, est le fait que les utilisateurs doivent s'assurer qu'ils chiffrent leurs messages en utilisant la véritable clé publique de leur destinataire. A fin de confirmer l'appartenance d'une clé à son propriétaire supposé, on utilise le principe de certificats numériques qui font appel à une partie tiers appelé autorité de certification

2.2 Définition

Une **PKI** « *Public Key Infrastructure* » ou **ICP** « *Infrastructure à Clé Publique* » est définit comme étant: l'ensemble des équipements, des logiciels, des personnes, des stratégies et des procédures nécessaires à la création, la gestion, le stockage, la distribution et la révocation des certificats basés sur un chiffrement à clé publique. [12]. Aussi appelée **IGC** *« Infrastructure de Gestion de Clés ».*

Remarque :

Nous utiliserons l'appellation PKI tout au long des chapitres ; elle est connue plus par ce nom.

2.3 Certificat numérique

Un certificat numérique fonctionne comme une pièce d'identité. C'est une information attachée à une clé publique, signé numériquement par une partie tierce de confiance (autorité de certification). L'objet de la signature est de garantir que les informations de certification ont été contrôlées et validées.

Les certificats numériques sont utilisés donc pour empêcher les tentatives de falsification de clé publique.

2.4 Normalisation des PKI

PKIX « *Internet X.509 Public Key Infrastructure* » est un groupe travaillant pour le développement des normes nécessaires au support des PKI pour Internet. Il a été formé en 1995. Ce groupe travaille à la définition des éléments suivants : [13]

1. Format de certificat X.509 et des listes de révocation X.509 pour une infrastructure adapté à l'Internet. Un grand nombre de standards Internet, des **RFC**[2] ont été publiées.
2. Des protocoles de distribution des certificats et des listes de révocation aux systèmes qui les utilisent. Divers systèmes sont développés, en particulier des procédures basées sur **LDAP** « *Lightweight Directory Access Protocol* », **OCSP** « *Online Certificate Status Protocol* ».
3. Des protocoles de gestion, qui permettent aux différentes entités composant la PKI de dialoguer et d'échanger les informations.
4. Des règles d'usage et des considérations pratiques : exigences en matière d'identification des sujets, règles pour la révocation des certificats, …etc.

2.5 Les acteurs d'une PKI

Les acteurs qui interviennent dans une PKI sont illustrés dans la figure suivante : [6]

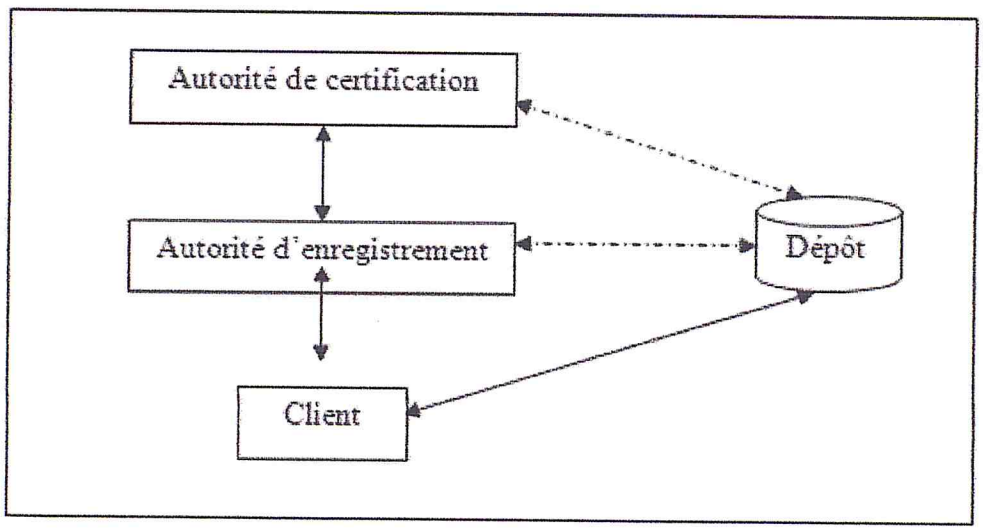


Figure II.1: Les acteurs d'une PKI.

2.5.1 L'autorité de certification AC

C'est l'entité qui détient l'entière responsabilité de la gestion des certificats et des clés (création, attribution, mise à jour, révocation et le recouvrement). Elle certifie des clients mais aussi des autorités de certification subordonnées et des autorités d'enregistrements AE.

C'est l'AC qui édite la règlementation à respecter dans une PKI, on parle de Politique de Certification PC.

[2] ***Les Requests For Comments*** sont une série de document et de normes concernant l'Internet. Peu de RFC sont des standards, mais tous les standards de l'Internet sont enregistrés en tant que RFC. Les RFC sont rédigés sur l'initiative d'un expert technique puis sont revue par la communauté Internet dans son ensemble. [14]

2.5.2 L'autorité d'enregistrement AE

C'est l'entité responsable des interactions entre le client et l'AC. Elle diminue la charge de l'AC en s'occupant de la tâche de vérification et validation des demandes de certificats et la distribution des certificats aux clients.

L'AE se porte garante du lien entre un certificat, l'identité du porteur et autre attributs « informations personnelles du client ».

2.5.3 L'entité d'enrôlement EE

C'est l'entité de la PKI à partir de laquelle un client communique avec la PKI. Elle offre les fonctionnalités nécessaires à l'obtention d'un certificat, sa révocation et le recouvrement de clés.

Un client communicant avec la PKI n'est pas toujours une personne. Il peut être un composant intermédiaire (AE, AC fille) ou des machines de service (serveur, routeur) qui disposent eux aussi de bi-clé de signature donc de certificat.

2.5.4 Le dépôt

C'est une base de données en ligne qui rend disponible les certificats émis par l'AC ainsi qu'une liste de certificats révoqués connu par LCR à l'ensemble des utilisateurs.

La quasi-totalité des dépôts sont implémentés sous forme d'annuaires type LDAP (Lightweight Directory Access Protocol) dont l'accès peut être protégé.

2.5.5 Autre composante complémentaire : l'Horodatage

C'est une composante qui associe une date/heure à un évènement (transaction électronique) ayant lieu dans la PKI comme une demande de création de certificat, génération de certificat, demandes de révocation, etc.

L'horodatage est souvent utilisé pour prouver l'antériorité d'un message ou une transaction par rapport à un évènement.

2.6 Les processus dans une PKI

En fonction de la répartition des rôles et des responsabilités dans une organisation, ainsi que les objectifs que l'on se fixe en terme de niveau de sécurité et de coût, les processus peuvent sensiblement varier d'une PKI à une autre.

Nous citons dans la suite les principales fonctionnalités devant être offerte par une PKI :

2.6.1 Enregistrement d'un client

Lorsqu'une entité se présente pour l'obtention d'un certificat, elle est enregistrée auprès de l'AE. L'enregistrement consiste à recueillir les informations caractéristiques du demandeur : son nom, son adresse électronique, etc.

Pour l'enregistrement, deux contrôles sont réalisés : l'authentification et la vérification des attributs.

* **L'authentification :** Peut être envisagée soit par déplacement physique du demandeur avec présentation de pièces d'identités justificatives, soit par simple envoi de copie de pièce d'identité. Le choix du mode d'authentification dépend du niveau de confiance accordé
* **La vérification :** Consiste à vérifier la validité des attributs du client demandeur de certificat (appartenance à une société, fonction dans l'organisation, ...etc.)

2.6.2 Génération d'une paire de clé

La génération d'une paire de clé publique/privée peut être centralisée ou décentralisée.

- Dans la **génération centralisée,** la paire de clé est générée par l'autorité de certification. Elle est envoyée au client via un canal sécurisé ***SSL***.
- Dans la **génération décentralisé,** c'est le client qui génère la paire de clés et envoie une requête de signature de certificat « **CSR** : *Certificate Signing Request* » à l'AC pour lui générer un certificat

2.6.3 Création d'un certificat

Les étapes de création d'un certificat sont présentées dans la figure suivante : [6]

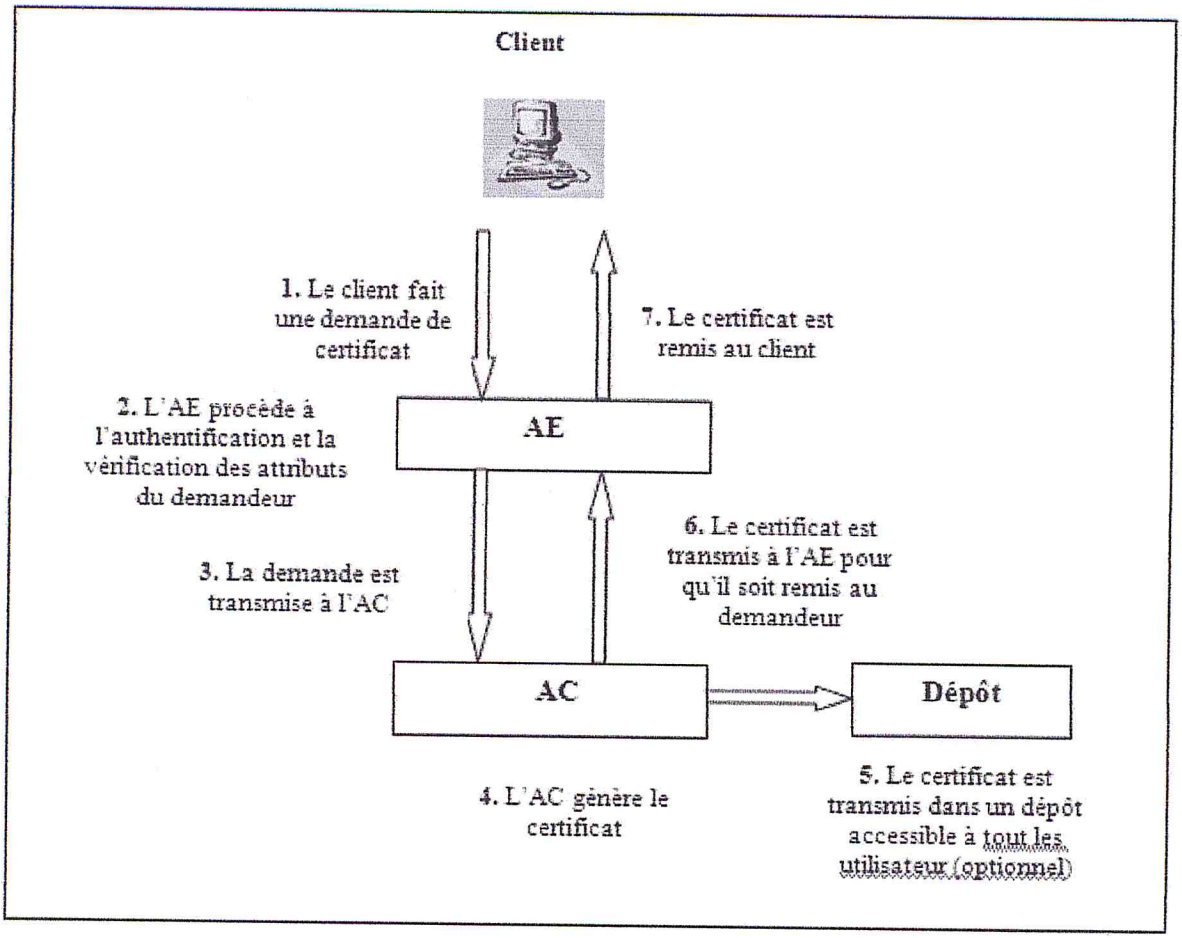


Figure II.2: Processus de création d'un certificat.

2.6.4 Renouvellement d'un certificat

Un certificat possède une période de validité. Une fois le certificat expiré (date limite dépassé), son utilisation n'est plus valable. La PKI assure alors le renouvellement d'un certificat dés son expiration.

2.6.5 Révocation d'un certificat

Un certificat peut être révoqué (annulé) pour des raisons telles que : perdre la clé privée, changer des informations personnelles, quitter l'organisation,... etc.

Le processus de révocation est illustré dans la figure suivante : [6]

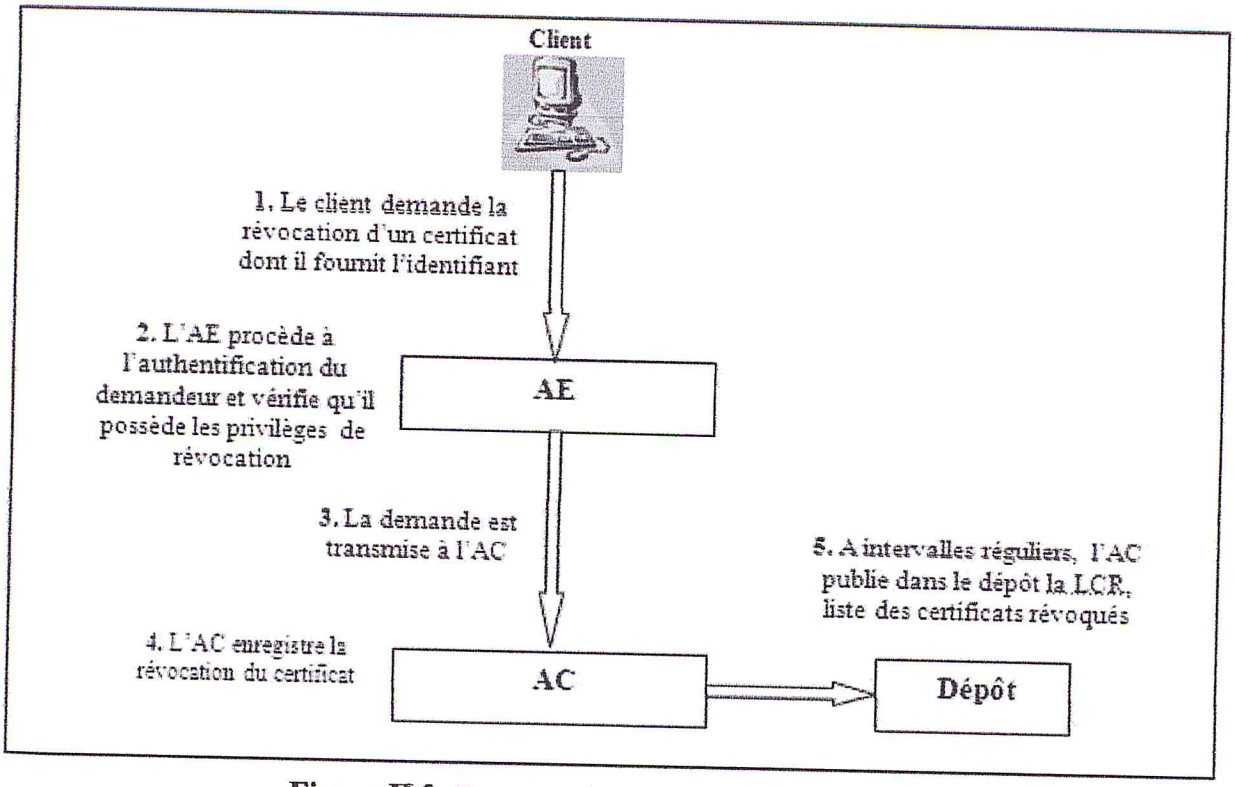


Figure II.2: Processus de révocation d'un certificat.

- **LCR, Liste de certificats Révoqués**

Lorsqu'un certificat est révoqué, son numéro est inséré dans une Liste de Certificats Révoqués (LCR). Le format d'une LCR est standardisé. La figure suivante illustre le format X.509 v2 : [6]

Version (CRL format version)
Description de l'algorithme de signature (signature)
Nom de l'émetteur qui a généré la LCR (issuer)
Date d'émission (thisUpdate)
Date d'émission de la prochaine LCR (nextUpdate)
Clé publique (subject public key)
Liste des certificats révoqués (revokedCertificate)
Identification possible de l'AC (optionnel) **(Issuer unique identifier)**
Identification possible de l'utilisateur (optionnel) **(Subject unique identifier)**
Extension de la LCR (CRLExtension)
Description de l'algorithme de signature (SignatureAlgorithme)
Signature de l'émetteur (signatureValue)

Figure II.4: Format d'une LCR X.509 v2.

La mise à jour d'une **LCR** se fait périodiquement. La période doit être petite pour diminuer le risque qu'un client récupère une LCR entre la révocation d'un certificat et la mise à jour de la LCR et probablement utilise ce certificat révoqué ce qui présente un risque de sécurité pour lui.

Le protocole **OCSP** « *Online Certificate Status Protocol* » a été développé pour traiter des besoins de contrôle en ligne de l'état d'un certificat donnée ce qui permet d'obtenir une information plus à jour qu'en passant par la consultation d'une LCR. [6]

2.6.6 Recouvrement d'une clé privée

Grâce à cette fonctionnalité, les clés privées perdues peuvent être reconstituées. Cependant, pour des raisons de sécurité, on n'autorise que le recouvrement de clés correspondantes aux certificats de chiffrement. (Rappel: il existe principalement trois types de certificats : Certificat d'authentification, signature et de chiffrement).

Nous illustrons le processus de recouvrement d'une clé privée dans la figure qui suit : [6]

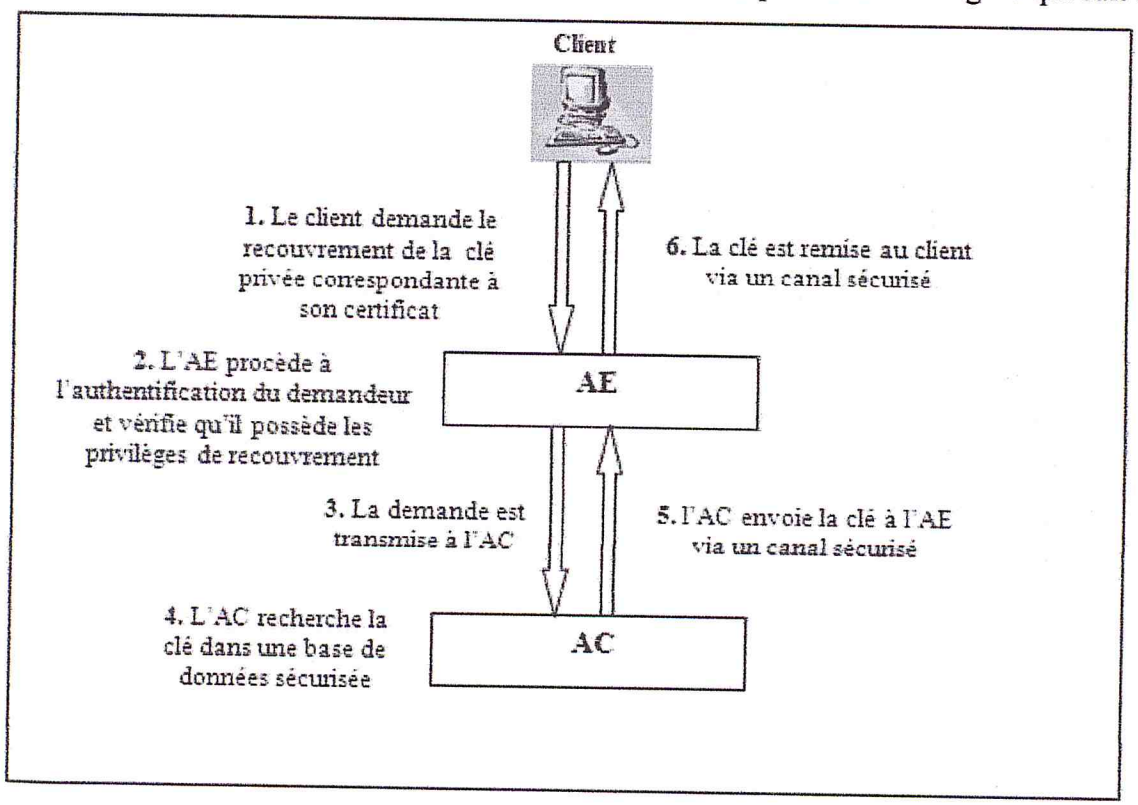


Figure II.5: Processus de recouvrement d'une clé privée.

Pourquoi seulement les clés de chiffrement ?

- un client possédant un certificat d'authentification s'authentifie pour accéder aux applications sécurisées faisant confiance à l'AC signant son certificat. S'il la perd et si elle tombe dans des mains d'un malfaiteur, ce dernier pourra usurper son identité.
- Un client possédant un certificat de signature, signe des messages avec sa clé privée. S'il la perd et si elle tombe dans des mains d'un malfaiteur, ce dernier pourra signer des messages en son nom. Recouvrir cette clé présente donc un danger. Il est nécessaire de révoquer le certificat et demander un autre correspondant à une nouvelle clé privée.
- On doit recouvrir la clé privée correspondante à un certificat de chiffrement pour permettre le déchiffrement des messages déjà chiffrés avec la clé publique correspondante. Le risque qu'un malfaiteur trouvant la clé privée déchiffre ces messages est minime puisqu'il ne devrait pas avoir accès à ces messages.

2.6.7 Cocertification

C'est la génération d'un certificat à une entité pour qu'elle puisse elle-même générer des certificats.

2.7 Architectures d'une PKI

Il existe principalement trois types d'architecture : architecture simple (à une seule AC), architecture hiérarchique et l'architecture hybride. [6] [7]

Pour choisir une architecture qui correspond aux besoins des utilisateurs, les concepteurs des architectures PKI doivent répondre aux questions comme :

- Quelles sont les PKI auxquelles un utilisateur fait confiance ?
- Existe-t-il un accord de reconnaissance mutuelle entre la PKI d'un abonné et d'autres
- Quelle est la capacité d'évolution de la PKI ?
- Quelle est la capacité de l'organisation (humain et technique) à distribuer des certificats intermédiaire de confiance à tous ces abonnés ?

2.7.1 Architecture simple

C'est l'architecture de base d'une PKI. Elle est composée d'une seule autorité de certification. L'AC peut gérer une ou plusieurs AE selon l'architecture de l'organisation pour laquelle on conçoit la PKI.

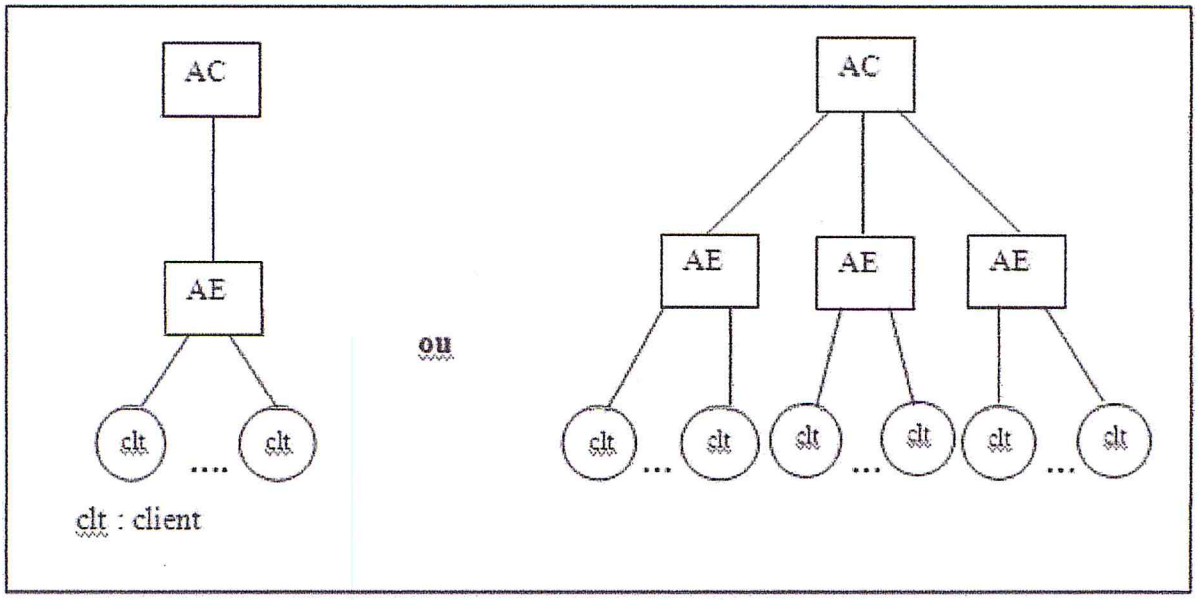


Figure II.6: Architecture simple d'une PKI

Le déploiement d'une telle architecture est simple. Cependant elle présente des points faibles tels que :

- il existe une seule AC qui gère les clés de toutes les entités. Si la clé privée de l'AC est compromise, tous les certificats délivrés par cette AC seront révoqués ainsi que le certificat de cette dernière. Pour rétablir l'AC, elle doit délivrer de nouveaux certificats pour toutes les entités de la PKI.
- Cette architecture convient à de petite organisation avec un nombre limité d'utilisateurs.

2.7.2 Architecture hiérarchique

Pour résoudre le problème de l'architecture simple concernant la gestion centralisée des certificats, une PKI peut avoir une architecture hiérarchique. Comme pour l'architecture simple, les AC filles peuvent communiquer avec une ou plusieurs AE.

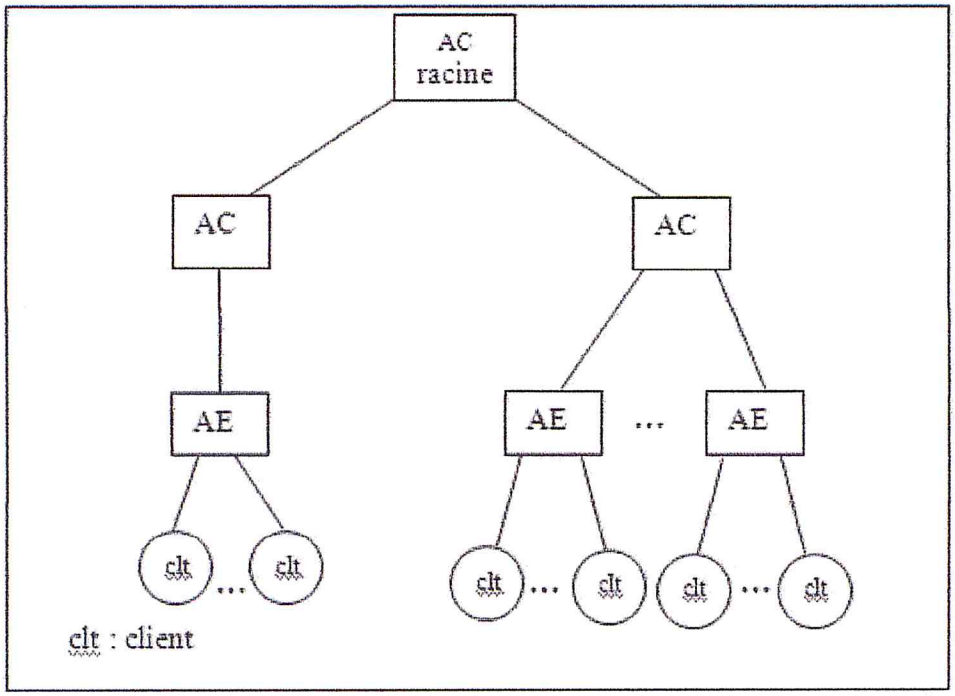


Figure II.7 : Architecture hiérarchique d'une PKI

Points faibles :

- En cas de compromission de la clé privée d'une AC fille, seuls les utilisateurs de cette AC voient leur service interrompu. L'AC de niveau supérieur régénère un certificat pour l'AC fille qui va ensuite réémettre les clés et les certificats à ces clients. Mais la corruption de l'AC racine aurait des conséquences semblables à celles de l'architecture simple, toute la hiérarchie est mise en cause.
- Un autre problème concerne les modifications dans l'architecture suite à la modification de l'architecture de l'organisation pour laquelle on conçoit la PKI (car l'architecture PKI doit être une image de l'architecture de l'organisation). La modification entraîne la régénération des certificats pour les niveaux qui ont été touché par la modification.

Chemin de certification :

Dans une architecture hiérarchique, la vérification de la signature d'un certificat nécessite l'analyse de tout un chemin de certification.

Un chemin de certification est une séquence ordonnée de certificats qui est analysée pour obtenir la validation de la clé publique de l'entité finale du chemin, à partir de la clé publique de l'entité de confiance, la plus haute du chemin. [6]

L'analyse se déroule en deux étapes :

1. La reconstitution du chemin en s'assurant qu'on possède l'ensemble des certificats jusqu'à l'AC racine.
2. La validation du chemin qui consiste à la vérification de la signature de chaque certificat commençant par celui de l'AC racine (voir processus de vérification d'une signature au chapitre3).

2.7.3 Architecture hybride

L'architecture hybride est nécessaire pour concrétiser des relations de confiance entre différentes AC. Par exemple si deux sociétés doivent fréquemment valider des transactions mutuelles dans le cadre d'un accord préalable, il est possible de concrétiser cet accord en établissant une certification croisée entre leur AC. Le schéma suivant illustre l'architecture hybride.

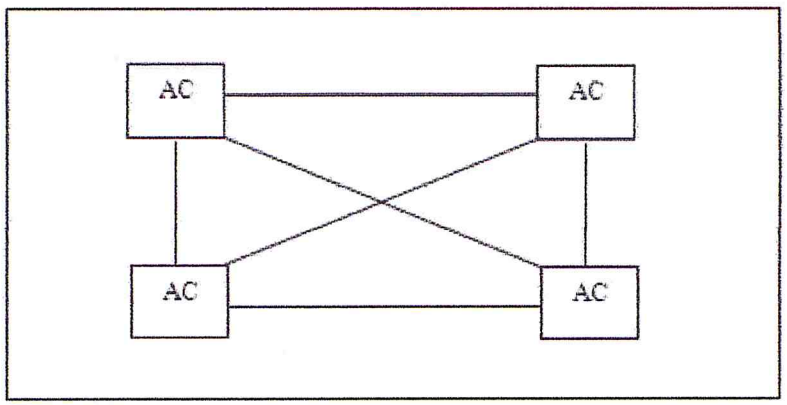


Figure II.8 : Architecture hybride

Lorsque la clé privée d'une AC est compromise, elle régénère son certificat au AC avec lesquelles existe une certification croisée (et bien sûr régénère des certificats à ces clients)

2.8 Conclusion

L'adoption du protocole HTTPS pour sécuriser les applications web nécessite l'utilisation de certificats pour l'authentification des clients et des serveurs ainsi que crypter les données échangées entre eux. Cependant la gestion des certificats requiert une infrastructure à clé publique ou PKI « *Public Key Infrastructure* ».

Nous avons présenté dans ce chapitre l'architecture d'une telle infrastructure et les différents processus s'exécutant au sein d'elle.

Le déploiement d'une PKI est l'objectif de notre projet. Sa conception puis son implémentation seront l'objet des chapitres suivants.

CHAPITRE 3

Cas pratique

TRAVAIL BANCAIRE EN LIGNE
« E-Banking »

3.1 Introduction

Les plateformes e-banking révolutionnent aujourd'hui le monde du commerce visant tout autant les entreprises et même les particuliers.

Dans ce chapitre, nous commençons par présenter le travail bancaire à distance, et une analyse des risques menaçants la plate-forme e-banking pour arriver à l'identification des besoins en sécurité.

Nous finirons dans ce chapitre par une vue globale de l'organisme d'accueil, Caisse National d'Epargne et de Prévoyance CNEP-Banque.

3.2 E-banking

3.2.1 Définition

Le terme banque en ligne désigne un établissement financier qui propose un ensemble de services bancaires destiné aux clients déroulant par voie électronique « Internet » : ouverture et clôture des comptes, virements, achats et ventes de produits financiers, consultation de comptes, commande de chéquiers, …etc. [20]

Les banques en ligne vous permettent ainsi d'avoir accès depuis n'importe quel ordinateur à tous les services bancaires 24 heures sur 24 et 7 jours sur 7.

3.2.2 Objectifs d'e-banking

Autonomie, confort, interactivité, informations telles sont les promesses de la banque en ligne. Dans ce secteur très concurrentiel, chaque banque cherche à fidéliser ses clients en leur proposant continuellement de nouveaux produits qui répondent à un réel besoin et d'autres qui cherchent à créer ou devancer un besoin.

Tous les grands établissements financiers du monde se sont désormais placés sur le secteur de la banque en ligne. La plupart dispose même d'un site "portail" qui permet à leurs clients de se diriger vers le site de banque à distance qui leur est destiné. On retrouve en général les mêmes services sur tous les sites.

Les principaux objectifs de la banque en ligne sont les suivants : [19]

a. La consultation des comptes « soldes et historique »

Ce service permet aux clients de consulter leurs comptes professionnels et / ou privés. Ce type de service est adapté aux moyens de communication utilisés par le client, ou être alerté par e-mail ou SMS si le solde de votre compte franchit à la baisse le seuil que vous avez

préalablement défini. Certains sites offrent même la possibilité de charger ses propres relevés sur un programme adéquat, tel qu'Excel.

b. La gestion au quotidien

Ce produit permet la réalisation des opérations courantes telle que les virements internes, externes, les commandes diverses, la gestion de crédit permanent, possibilité d'effectuer un virement, de commander un chéquier, d'imprimer un RIB[3], d'envoyer un mail à son chargé de clientèle...etc.

c. Accéder aux services de bourse

Les services bourses ne sont pas une exclusivité des sites des grands établissements financiers. On retrouve ainsi sur le Web une multitude de courtiers en ligne qui se proposent de passer vos ordres de bourse, à partir de votre ordinateur personnel. Certains sites sont tous de même sous tutelle d'établissements bancaires, ce qui assure l'utilisateur d'un service minimum et d'une garantie de sérieux.

d. L'information sur les produits

C'est un descriptif des différents produits qui ne sont pas forcément à distance et donne aussi les tarifs des différentes prestations.

e. La sécurisation des moyens de paiements

C'est un service qui permet d'éviter toute action frauduleuse et ainsi effectuer ses achats en toute sécurité.

3.2.3 L'évolution de la banque électronique

a. E-banking dans le monde

La banque sur Internet gagne du terrain. De plus en plus, les banques ont des sites web où les clients peuvent non seulement s'informer sur le solde de leurs comptes et les taux d'intérêt et de change, mais aussi effectuer diverses opérations.

Malheureusement, il n'existe guère de données, et la diversité des définitions complique les comparaisons internationales. On sait quand même que la banque en ligne est particulièrement utilisée en Autriche, en Corée, en Espagne, dans les pays scandinaves, à Singapour et en Suisse, où plus de **75%** des banques offrent de tels services (voir figure III.1)

[3] ***Le RIB Relevé d'Identité Bancaire :*** est un document papier qui contient l'identité du titulaire d'un compte-chèques

C'est en Scandinavie que les utilisateurs d'Internet à des fins bancaires sont les plus nombreux, jusqu'à un tiers du total des clients en Finlande et en Suède.

Aux États-Unis, la banque en ligne reste concentrée dans les grandes banques. En 2001, **44%** des banques américaines, soit près de deux fois plus qu'au troisième trimestre de 1999, offraient un site web permettant d'effectuer des opérations. Ces banques représentent plus de **90%** des actifs du système bancaire national. Les grandes banques offrent généralement une plus large gamme de services électroniques, notamment des demandes de prêt et des services de courtage. Si la plupart des clients américains ont des comptes auprès de banques qui offrent des services sur Internet, **6%** seulement utilisent ces services.

À l'heure actuelle, la plupart des banques combinent les nouveaux circuits de distribution électroniques et les agences traditionnelles, mais quelques-unes offrent leurs produits et services principalement, ou exclusivement, par voie électronique.

Ces banques « virtuelles » (présentes uniquement sur Internet) ne possèdent pas de réseau d'agences, mais elles ont parfois une présence physique, par exemple un bureau administratif, des kiosques interactifs ou des guichets automatiques. On compte une trentaine de banques virtuelles aux États-Unis, deux en Asie, établies en 2000 et 2001, et plusieurs dans l'Union Européenne, soit des entités disposant d'un agrément distinct, soit des filiales ou succursales de banques traditionnelles. [18]

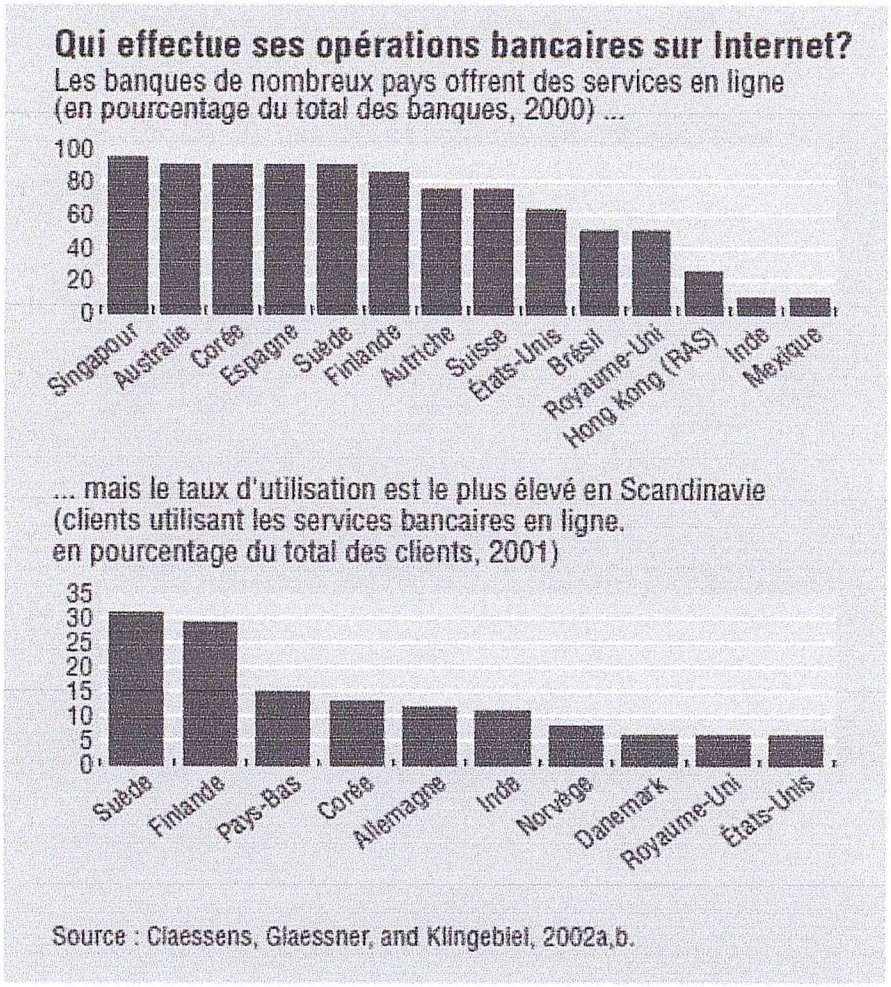


Figure III.1 : E-banking dans le monde [18]

b. E-banking dans notre pays

L'e-banking est quasiment inexistant en Algérie. Quelques banques publiques possèdent des sites web mais aucune allusion aux transactions en lignes. Quelques banques étrangères proposent ce genre de solution, mais très peu d'Algériens possèdent des comptes. Il existe en Algérie une particularité qui est que la majorité des habitants possèdent des comptes ccp (comptes postaux) alors que la poste n'est pas considérer comme une banque. La poste algérienne propose différents services comme le transfert d'argents mais aucun ne peut se faire en ligne. Le seul service proposé en ligne est la vérification du solde « ***home-banking*** est un exemple de la vérification du solde appliqué au CNEP-banque ». Cependant, le serveur hébergeant ce service est souvent hors service. Le système bancaire algérien est en retard il n'est pas favorable au développement du e-commerce. [21]

A cause de la quasi-inexistence de l'e-payement, les seules applications possibles en Algérie sont la consultation d'annonces via Internet. Ensuite, le paiement se fait par cash et la livraison se fait de main en main.[21]

3.2.4 Les limites

Si la banque en ligne a beaucoup d'avantages aussi bien pour le client que pour la banque, il existe cependant certaines limites. [19]

- En effet, l'ouverture du marché national favorise l'entrée de nouveaux concurrents. Créer un réseau d'agences demande un investissement exceptionnel. En revanche, créer et vendre des produits sur Internet « e-commerce » est à la portée d'un challenger. Le réseau des banques classiques est ainsi attaqué par une multitude de concurrents qui choisissent des niches de produits ou de clientèles.
- De plus, il faut veiller à ce que la banque en ligne ne se substitue pas à la banque traditionnelle. Car, même si elle plait à une clientèle « active » dont les jeunes, il ressort que les clients « adultes » des banques ont besoin de contact humain pour développer une relation de confiance.
- Enfin, il est important de préciser que « l'agence » est économiquement efficace. En effet c'est l'agence qui est le principal générateur de bénéfice **PNB** parmi tous les canaux disponibles. Le conseiller de clientèle est le principal acteur de la relation commerciale, la majorité des ventes passent par lui. La banque en ligne n'offre pas un service suffisamment complet pour vendre des nouveaux produits. La banque en ligne peut intervenir au moment de la recherche d'informations et des différentes opérations après-vente. Ainsi la banque en ligne n'a pas de raison d'être sans le soutien d'un réseau en dur.

3.2.5 Besoins en sécurité

Une plateforme e-banking est une application web dont les flux de données menacés sont présentés dans la figure suivante :

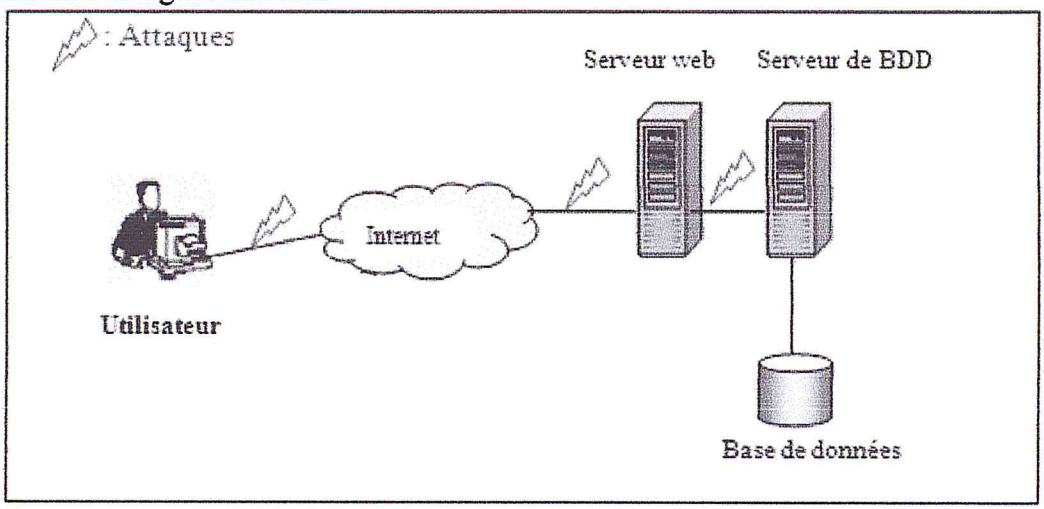


Figure III.2 : Architecture d'une application web et flux menacés

Dans l'interaction entre le client et le serveur web, un navigateur web transmet des données au serveur web. Elles sont transférées à l'application qui entre en interaction avec la base de données. En suivant ces routes, nous pouvons repérer les points faibles dans la communication entre le client et le serveur web, et la communication entre le serveur web et le serveur de base de données. [15]

a. Communication entre utilisateur et serveur web

La communication d'un client avec le serveur via Internet se fait avec le protocole **HTTP**. Cependant, le trafic **HTTP** n'est pas sécurisé. Un pirate peut facilement intercepter les données transférées entre le client et le serveur, injecter de fausses informations, usurper l'identité d'un client ou un serveur, ...etc. bref, on n'est pas sûr d'être avec le bon serveur ou le bon client. Dans les plateformes e-banking, ceci présente un risque dans des cas tels que :

- Interception d'informations personnelles et mots de passe lors de l'inscription d'un nouvel utilisateur ;
- Interception d'une transaction bancaire confidentielle;
- Injection de fausses informations dans les réponses des consultations lors d'une vérification de solde ;
- Usurpation de l'identité d'un client, d'un d'administrateur. Une anarchie totale en données, etc.

b. Communication entre serveur web et serveur de base de données

Le serveur web et le serveur de base de données s'exécutent probablement sur des machines différentes et la base de données d'une plateforme e-banking peut contenir des données confidentielles (mot de passe, informations confidentielles, ...etc.), il faut donc trouver un moyen pour sécuriser les communications entre les deux serveurs. [15]

En résumé, pour obtenir une plateforme e-banking sécurisée, on doit garantir :

- La sécurisation de la communication entre le client et le serveur (authentification du client, authentification du serveur, chiffrement du trafic entre eux) ;
- La sécurisation entre le serveur web et serveur de base de données s'ils s'exécutent sur des machines différentes ;
- La sécurisation des objets de la base de données (chiffrement des données confidentielles) ;
- La sécurisation des outils de transactions offerts par la plateforme.

3.3 Cas pratique

3.3.1 Caisse Nationale d'Epargne et de Prévoyance – Banque

La CNEP-Banque a été crée le 10 août 1964 sur la base du réseau de la caisse de solidarité des départements et des communes d'Algérie **CSDCA** avec pour mission la mobilisation et la collecte de l'épargne, la première agence de la CNEP a officiellement ouvert ses portes le premier Mars 1967 à Tlemcen, cependant le livret d'épargne CNEP était commercialisé depuis une année à travers le réseau poste et timbre.

Figure III.3 : Le logo de la CNEP-Banque.

3.3.2 Historique

La CNEP a connu diverse changements tant sur le plan statutaire que sur le plan de ses activités :

a. 1ére période (1964- 1974)

Durant cette période la CNEP s'est assignée comme mission :

- La collecte de l'épargne sur livret pour les ménages « taux d'intérêt de 2.8% jusqu'à 1970 »
- L'octroi de crédits pour achat de logement « prêts sociaux » le réseau de collecte de l'épargne était constitué de deux agence « Alger, Tizi ouzou » qui furent ouvertes au public 1967

La collecte était surtout assurée par le réseau des PTT « 575 points de collecte »

b. 2éme période (1971- 1979)

Durant cette période, était surtout consacrée a l'encouragement du financement d'habitat, activités principale durant cette période se résument comme suit :

- Mise en place du système d'épargne logement « arrêté ministériel du 19/02/1971 »
- Le financement de l'habitat « instruction CNEP du 08/04/1971 »

- Mise en œuvre d'un nouveau produit d'épargne qui est le compte d'épargne devise « instruction CNEP N° 08 du moins de mai 1971 »

Ces activités ont données un essor considérable en matière d'épargne, le développement de la CNEP par l'amélioration de son réseau qui a joué un rôle important essor en 1979 le nombre d'agences et bureaux de collecte est passé à 46.

c. 3éme période (1980-1996) :

La CNEP s'est assignée de nouvelles activités qui concernent :

- Le suivi des crédits construction octroyés aux particuliers ;
- Le financement de l'habitat promotionnel « décret N°80-123 » du 13 /09/1980 sur fonds d'épargne avec vente aux engament seulement ;
- Le financement des secteurs hors habitat « profession libérales transports, coopérative ...etc.).ceci à énormément encouragé grâce a la diversification des produit offerts à la clientèle.

La CNEP a également des produits durant cette période, augmentée le nombre d'agence « 120 agence 1988 et 172 en 1996 ».

Suit à la promulgation de la loi sur la monnaie et le crédit « loi 90-10 avril 1990 » de nombreux bouleversement ont marqué le système bancaire Algérien qui est désormais livré la concurrence et donc à la diversification de ses produits

Ainsi la CNEP a connu depuis 1997 une modification des statuts qui a marqué son passage d'une caisse chargée de la collecte à une banque exerçant l'ensemble des activités qui lui sont accordée et présente actuellement le statut juridique de société par action « **SPA** » au capitale de 14000000 DA divisé en 14000 action entièrement libérés par l'unique actionnaire qui est trésor public.

d. 4éme période (1997 à nos jours)

L'assemble générale ordinaire de la 17/07/2008 relative au repositionnement stratégique de la banque décide que son activité autorise au titre crédits aux particuliers :

- Les crédits hypothécaires prévus par les textes particuliers en vigueur au sein de la banque à l'exclusion des prêts pour l'achat locaux, la construction, l'extension et l'aménagement des locaux à l'usage commercial ou professionnel.

Il y a aussi le financement de la promotion immobilière, sont autorisés à savoir :

- Le financement des programmes immobiliers destinés à la vente ou à la location, y compris au intégrant des locaux à usage commercial ou professionnel ;
- Le financement de l'acquisition ou l'aménagement de terrains destinés à la réalisation de logements ;
- Financement des entreprises les segments qui sont autorisés :
  - Le financement des opérations d'acquisitions, d'extension et ou de renforcement des moyens de réalisation « équipements » initiés par des entreprises de production de matériaux de construction ou des entreprises de réalisation intervenant dans le secteur de bâtiment ;
  - Le financement de projets d'investissement dans les secteurs de l'énergie, de l'eau, de la pétrochimie ou de l'aluminerie.

3.3.3 Les structures de la CNEP-Banque

a. Les structures au niveau central :

La CNEP/Banque est dirigée par un Président Directeur Général **PDG**, assisté de six Directeurs Généraux Adjoints **DGA** :

- Le DGA chargé du développement ;
- Le DGA chargé de l'administration ;
- Le DGA chargé du crédit ;
- Le DGA chargé de l'assainissement ;
- Le DGA chargé de l'épargne et des réseaux d'exploitation ;
- Le DGA chargé du recouvrement.

Ces DGA sont sous l'autorité directe du PDG. Ils ont pour missions d'assurer l'animation, la coordination, l'assistance et le suivi des activités des vingt et une Directions centrales placées sous leurs autorités. En sus de ces Directions Générales Adjointes, la direction de l'inspection générale et une cellule chargée de l'audit interne.

b. Les directions régionales :

Structure hiérarchique et de soutien, la direction de réseau constitue le maillon intermédiaire entre les agences et les directions du siège central. Elle exerce à l'échelon régional certaines fonctions financières et toute fonction déléguée par la direction générale en disposant d'une action notamment, sur les agences implantées dans sa circonscription territorial définie par voie réglementaire.

En outre, la direction de réseau est l'interlocuteur nature des autorités ou entités locales dont elle peut financer, selon le seuil de compétence qui est dévolue, les projets relatifs aux opérations immobilières.

La direction de réseau exerce à ce titre les fonctions de direction, d'assistance, et de contrôle. La fonction de direction relève des prérogatives du directeur de réseau qui doit veiller avec la collaboration de ses chefs de département à faire exécuter le travail dans les meilleures conditions d'efficacité.

Le réseau regroupe actuellement sept départements :

- Le département du personnel et des moyens ;
- Le département du financement ;
- Le département de la comptabilité ;
- Le département de l'informatique ;
- Le département de l'épargne ;
- Le département de recouvrement ;
- La cellule de contrôle ;
- Le comité de sécurité.

Remarque :

Notre application sera réalisée au niveau du département informatique du réseau d'Alger Centre.

La CNEP/Banque compte, actuellement, 17 réseaux d'exploitation .nous avons repris par un organigramme l'ensemble d'exploitation de la CNEP/Banque.

c. Organigramme de la direction régionale

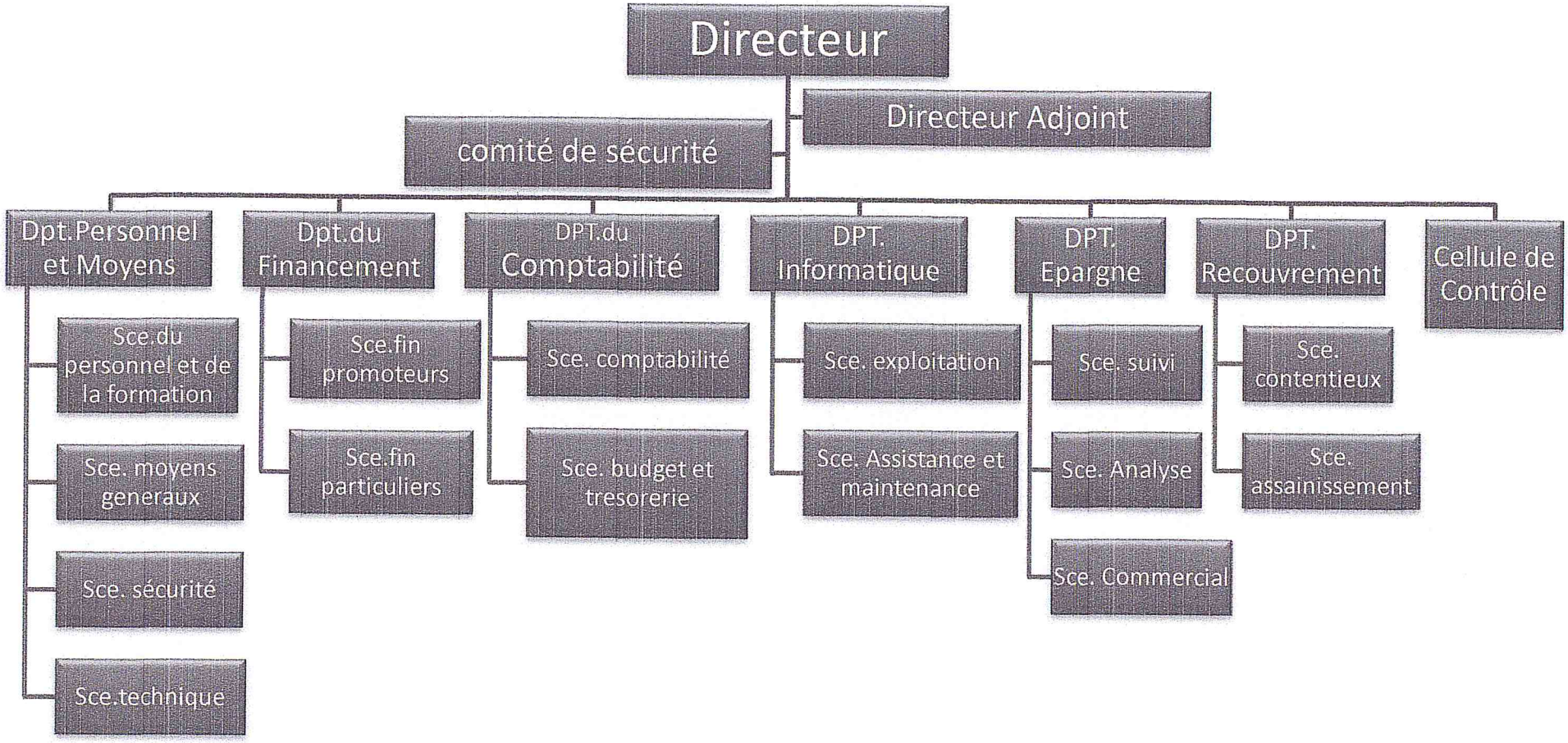


Figure III.4 : Organigramme de la direction régionale

3.3.4 Les produits de la CNEP-Banque

Grâce à son propre réseau d'agences constitué de 189 agences, toutes informatisées, et les 3.500 bureaux de poste, la CNEP-Banque offre à sa clientèle une large gamme de produits. Son objectif étant, d'un côté, la satisfaction de leurs besoins, et de l'autre côté, de rivaliser ces concurrents sur le marché bancaire algérien. Le large éventail de produits proposés par la CNEP-Banque est constitué de :

a. Les produits de l'épargne

Les produits de placement offerts à la clientèle englobent:

- ✓ **LEL:** Livret Épargne Logement conférant à leur titulaire le droit d'accès à un crédit avec des conditions privilégiées;
- ✓ **LEP:** Livret Épargne Populaire ne donnant aucun droit à son titulaire ;
- ✓ **DAT :** logement: Dépôts À Terme ;
- ✓ **DAT banque:** Dépôts À Terme;
- ✓ **Bon de caisse**.

b. Les crédits à la clientèle

Afin de financer ses clients, la CNEP6Banque a mis en place un certain nombre de produits à savoir :

b.1 Les produits de l'habitat :

- **Les entreprises :** la CNEP-Banque finance les programme de construction de logements réalisés par les promoteurs publics ou privés y compris des programmes de vente sur plan et des ensemble promotionnels immobiliers intégrés par acquisition de terrains et des études de réalisation ;
- **Les particuliers :** elle finance tous types d'habitat y compris :
  - La construction de logements individuels ou coopératifs,
  - L'achat auprès d'un promoteur public ou privé d'un logement neuf,
  - L'achat auprès d'un particulier de logements neufs ou anciens,
  - L'achat de terrain pour la construction
  - Et enfin, l'aménagement ou extension de logements.

b.2 Les crédits hors habitat:

- **Les entreprises :** le financement des crédits d'investissement et d'exploitation est une nouvelle activité de la CNEP-Banque.

- **Les particuliers :** offre des crédits d'équipement domestique « crédit confort »

3.4 Conclusion

Si la banque électronique présente des avantages pour les clients et de nouvelles possibilités commerciales pour les banques, elle aggrave les risques bancaires traditionnels.

Dans ce chapitre, nous avons définit le concept de e-banking, les différents flux d'information circulant dans de telles plateformes. Une analyse de l'architecture des plateformes e-banking nous a aidés à déduire leurs besoins en sécurité. La réponse à ces besoins est l'objet de notre projet.

Nous finirons dans ce chapitre par une vue globale de l'organisme d'accueil, Caisse National d'Epargne et de Prévoyance CNEP-Banque.

CHAPITRE 4

Conception et mise en œuvre

Le schéma suivant résume l'enchaînement des besoins qui délimitent le travail à réaliser :

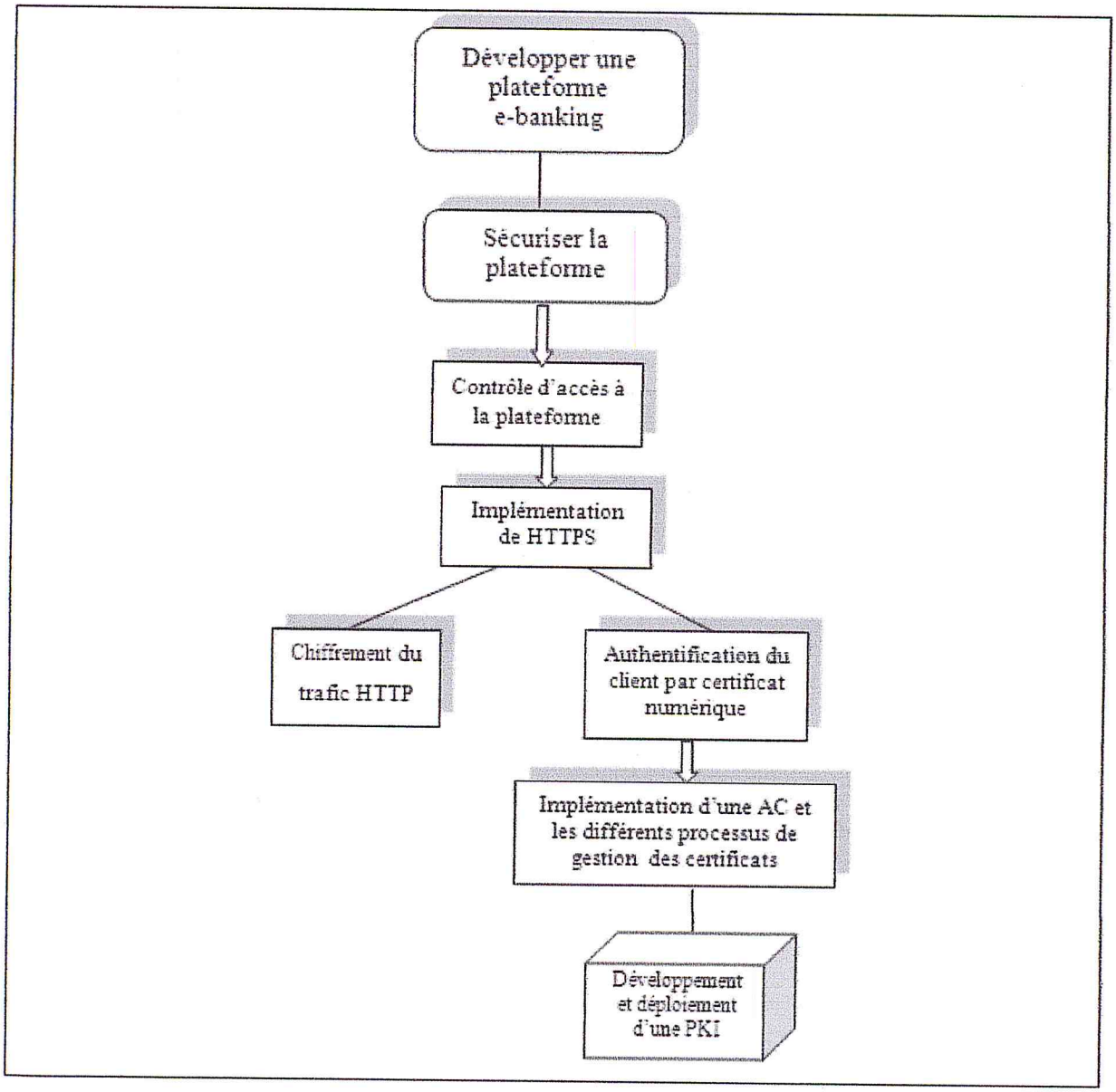


Figure IV.3: Organigramme délimitant le contexte de notre travail.

4.2 Déploiement de la plateforme e-banking ainsi la PKI

Pour bien assimiler l'approche de notre conception, il est nécessaire d'avoir des connaissances sur la plateforme e-banking et sur les PKI. Les notions de base sur ces derniers sont abordées dans les chapitres 2 et 3.

4.2.1 Architecture générale de la PKI

Les principales composantes de notre PKI et les acteurs agissant sur elle sont présenté dans la figure suivante :

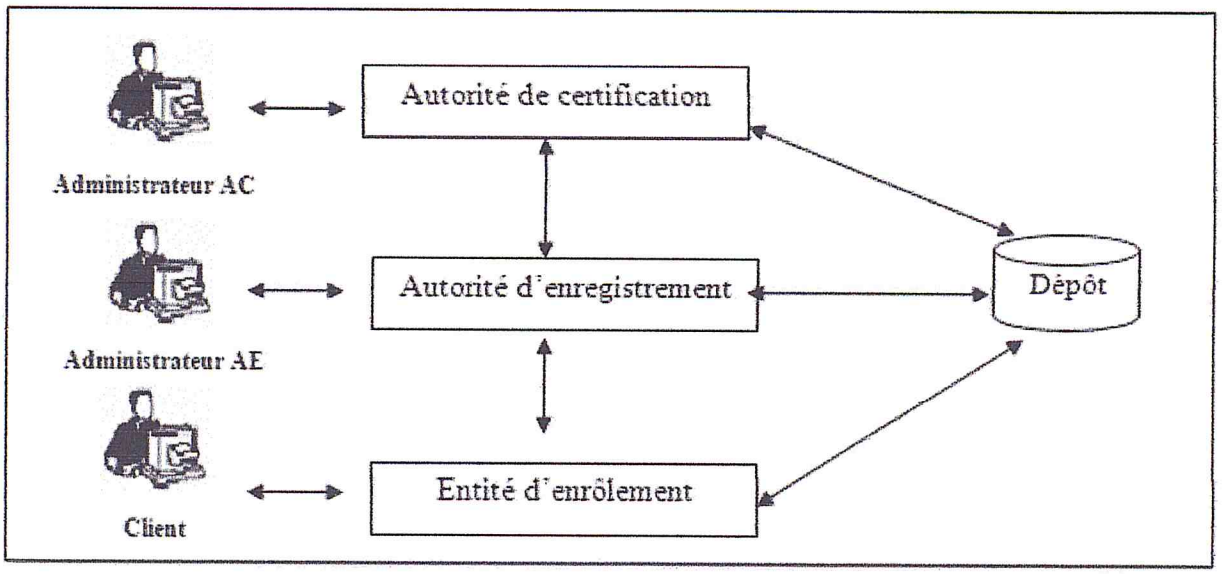


Figure IV.5: Composantes et acteurs de notre PKI.

a. Choix de l'architecture de la PKI

Nous avons présenté dans le chapitre 3 les différentes architectures possibles d'une PKI. Elles sont de trois types : architecture simple, architecture hiérarchique et architecture hybride. Comme nous l'avons déjà mentionné, le choix de l'architecture dépend de l'organisation pour laquelle on développe la PKI.

Même chose pour les plateformes e-banking. On ne peut pas choisir une architecture commune pour toutes les plateformes e- banking. Le choix dépend de la complexité de l'architecture de cette dernière. Dans notre conception, nous nous intéressons à l'architecture simple, qui est la base de toute autre architecture.

b. Architecture fonctionnelle de la PKI

Les principaux modules nécessaires au bon fonctionnement de notre PKI sont présentés dans la figure suivante :

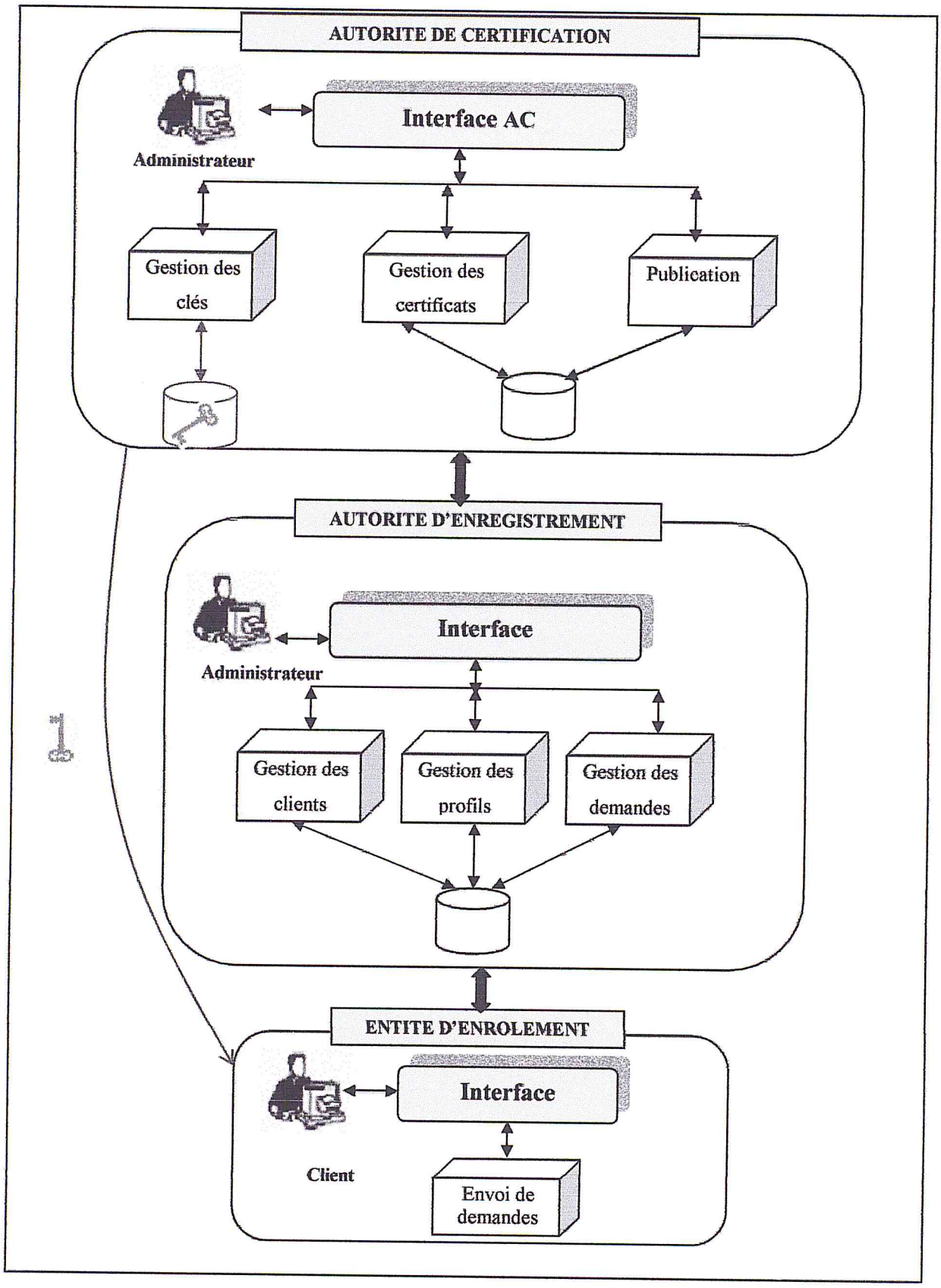


Figure IV.6: Architecture fonctionnelle de notre PKI

- L'entité d'enrôlement est l'interface client qui lui permet de communiquer ses demandes à l'autorité d'enregistrement.
- L'autorité d'enregistrement AE s'occupe de 3 tâches principales :

c. La gestion des clients :

Elle comprend l'enregistrement, la modification d'informations, la suppression et la recherche d'un client.

d. La gestion des profils :

Nous avons intégrer ce module pour permettre d'adapter notre PKI à n'importe quelle organisation. On peut ajouter, modifier, supprimer des profils. Une période de validité du certificat est associée à chaque profil. Dans notre cas, les profils avec les périodes de validités associées par défaut sont présentés dans le tableau suivant :

Profil	Période de validité
Particulier	**1 an**
Promoteur	**2 ans**
Société	**5 ans**

Figure IV.7: profils et périodes de validité associées

e. La gestion des demandes :

Elle concerne les demandes de certificats, de révocation et de recouvrement. Elle consiste en la vérification et la validation de ces dernières ainsi que leurs enregistrements.

La vérification consiste à vérifier si le client est enregistré, vérifier ses informations personnelles, vérifier s'il ne possède pas déjà un certificat valide, etc.

La validation consiste à générer une requête de signature de certificat **CSR** et l'envoyer à l'autorité de certification.

L'autorité de certification **AC** s'occupe également de 3 tâches principales :

- **La gestion des certificats et des clés** : le rôle principal de l'AC. Elle englobe : génération, renouvellement, révocation de certificats, recouvrement de clés privées.
- **La publication** consiste à mettre en ligne les certificats et les listes de certificats révoqués.

Remarque :

Toutes les communications entre le client et l'AC se font par l'intermédiaire de l'AE sauf la récupération de la clé privée qui se fait directement.

4.2.2 Modélisation de la PKI

a. Spécification des besoins

La phase d'expression des besoins est très importante, car dans cette étape on va déterminer les objectifs et les fonctionnalités attendues de notre système « PKI » c'est à dire sécuriser l'accès à la plate forme e-banking. Pour exprimer les besoins, on a utilisé les diagrammes **USE CASE** du langage UML.

La plate forme e-banking et PKI à réaliser sont des applications web qui permet :

- **A l'administrateur de l'AE :**
  - La gestion des clients (demandeur de certificat) qui englobe : enregistrement, suppression, modification, recherche.
  - la gestion des demandes des clients qui sont de trois types : demande de certificat, demande de révocation et demande de recouvrement de clés.
  - La gestion des profils qui comprend l'ajout, la modification et la suppression d'un profil.
  - l'accès aux services annuaire.
- **A l'administrateur de l'AC :**
  - La gestion des certificats qui rassemble : génération, révocation des certificats et recouvrement de clés privées.
  - La publication dans un annuaire
- **Au client :**
  - Se connecter à la plateforme et accéder à son propre compte.
  - L'envoi de demande de certificat, demande de révocation et de recouvrement de clé.
  - L'accès à l'annuaire pour consulter les listes de révocation.

b. Diagrammes de cas d'utilisation

A partir de la spécification des besoins, nous pouvons identifier les acteurs et les cas d'utilisations suivants :

b.1 Identification des acteurs

Les acteurs sont les utilisateurs extérieurs au système qui interagissent avec ce dernier [17].

Nous identifions trois acteurs dans notre PKI :

- Un client.
- Un administrateur de l'autorité d'enregistrement.
- Un administrateur de l'autorité de certification.

b.2 Identification des cas d'utilisation

Nous envisageons une multitude de cas d'utilisation que nous regroupons comme suit :

- Gestion des clients :
  - Inscription d'un client
  - Enregistrement d'un client ;
  - Suppression d'un client ;
  - Modification d'un client ;
  - Recherche d'un client.
- Gestions des demandes :
  - Demandes de certificat ;
  - Demandes de révocation ;
  - Demandes de recouvrement.
- Gestion des certificats et des clés :
  - Génération d'un certificat ;
  - Révocation d'un certificat ;
  - Recouvrement d'une clé privée.
- Accès au service annuaire :
  - Rechercher une LCR.
- Accès au compte :
  - Connecter à la plateforme e-banking
  - Consulter le compte

b.3 Diagrammes de cas d'utilisation

↳ Diagramme de cas d'utilisation pour l'accès au compte

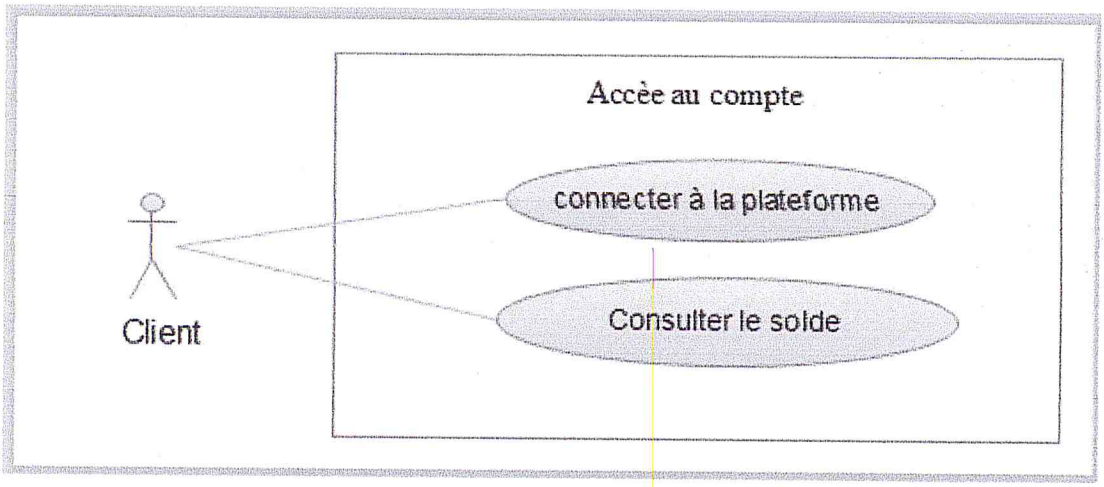


Figure IV.8: Diagramme de cas d'utilisation pour l'accès au compte.

- L'accès au compte bancaire dans notre plateforme nécessite une connexion à la plateforme qui est demande le certificat généré par notre PKI.
- Sinon ; si le client ne possède pas d'un certificat généré par notre PKI, donc il doit s'inscrive à notre PKI pour lui générer un certificat.

Remarque :

L'inscription dans notre PKI implique une inscription automatique dans notre plateforme e-banking.

↳ Diagramme de cas d'utilisation pour la gestion des clients

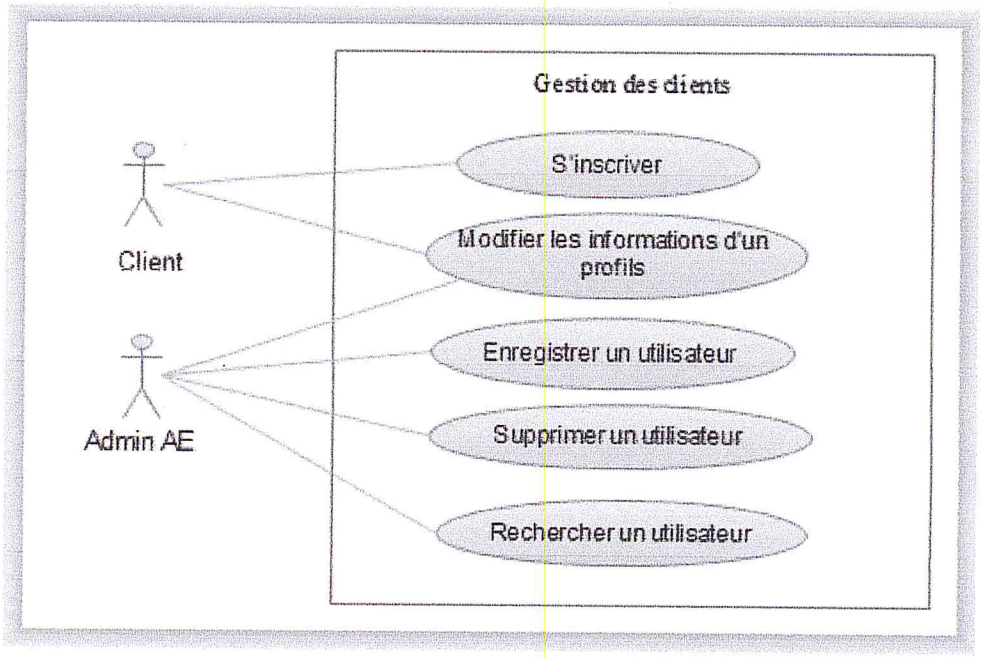


Figure IV.9: Diagramme de cas d'utilisation pour la gestion des clients

- L'inscription et l'enregistrement d'un utilisateur ou la modification de ces informations personnelles pour ceux qui sont déjà enregistrés nécessite la présence du client muni de pièces d'identités justificatives.
- La suppression d'un utilisateur n'est possible que si ce dernier ne possède aucun certificat valide délivré par notre PKI.
- La suppression d'un utilisateur est une suppression logique.

Diagramme de cas d'utilisation pour la gestion des demandes

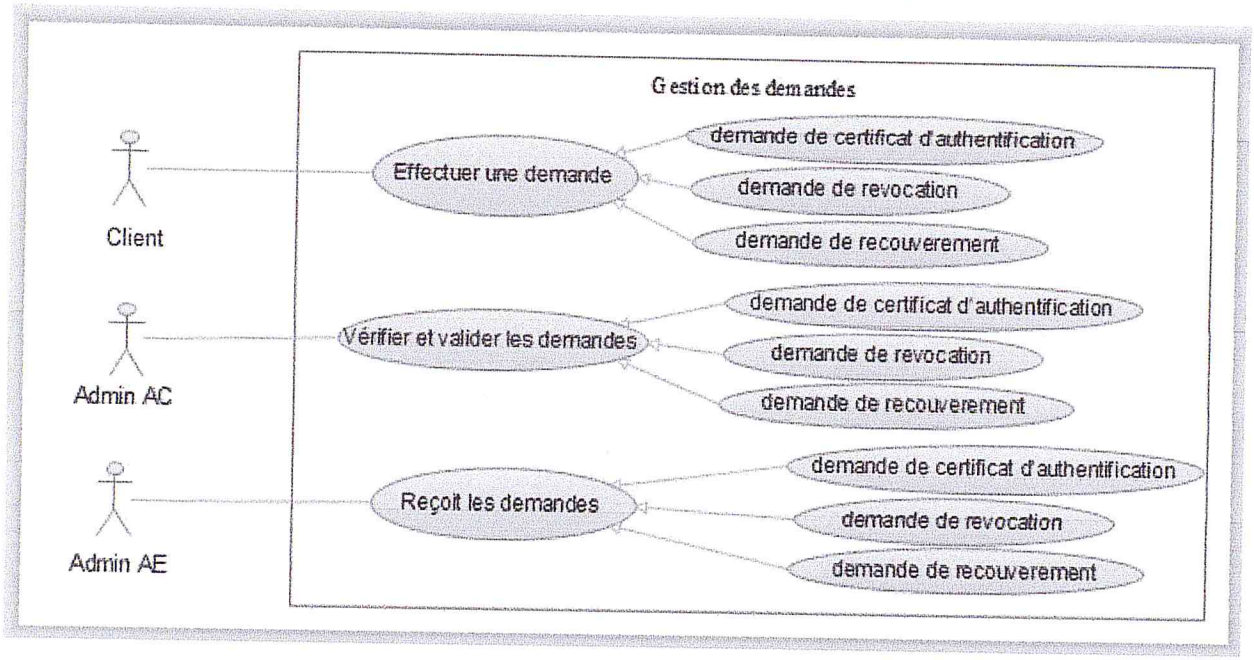


Figure IV.10: Diagramme de cas d'utilisation pour la gestion des demandes

- Un client effectue une demande de certificat d'authentification. Ceci nécessite sa présence auprès de l'AE, car il doit être enregistré. Avec ce certificat il peut accéder à la PKI pour effectuer des demandes des demandes de révocation, de certificats ou de recouvrement de clés privées.
- L'administrateur de l'AE vérifie et valide les demandes provenant du client et les renvoie à l'AC.

↳ Diagramme de cas d'utilisation pour la gestion des certificats

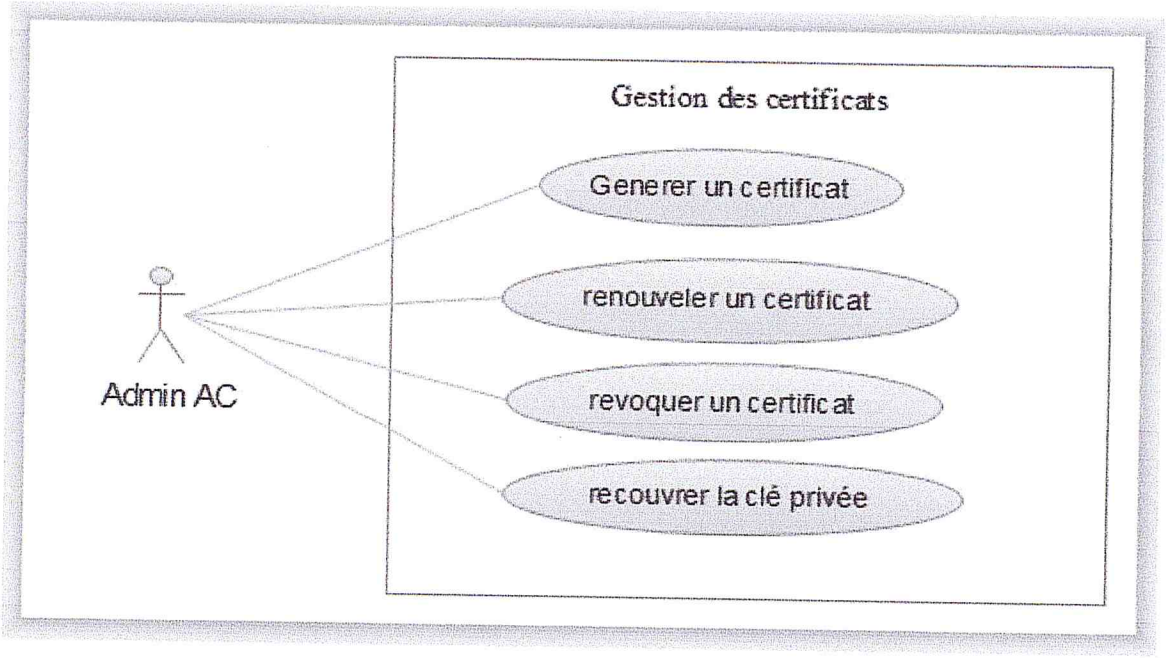


Figure IV.11: Diagramme de cas d'utilisation pour la gestion des certificats

- L'administrateur de l'AC génère un certificat, l'envoie à l'administrateur de l'AE qui enregistre les références du certificat et le renvoie au client.
- L'administrateur de l'AC révoque un certificat et envoie un avertissement à l'administrateur de l'AE qui enregistre cette révocation et renvoie l'avertissement au client.
- L'administrateur de l'AC renouvelle un certificat, l'envoie à l'AE pour enregistrer les références du certificat. L'AE l'envoie ensuite au client.
- L'administrateur de l'AC recouvre une clé privée et l'envoie directement au client.

Diagramme de cas d'utilisation pour l'accès à l'annuaire

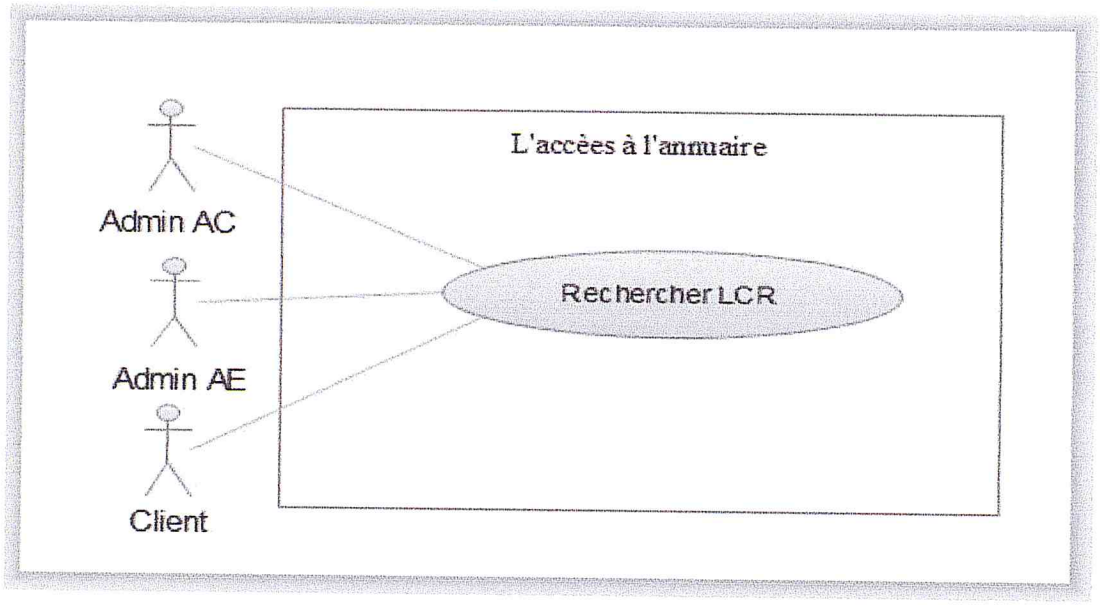


Figure IV.12: Diagramme de cas d'utilisation pour l'accès à l'annuaire

- Tous et seulement les membres de la PKI peuvent accéder au service annuaire.
- Les listes de révocation « LCR » sont mises à jours et publiées à chaque révocation d'un certificat. Il est nécessaire d'acquérir la dernière liste publiée.

c. Diagrammes de séquence

Un diagramme de séquence est une série d'évènements ordonnés dans le temps, simulant une exécution particulière du système. Le temps y est représenté explicitement par une dimension verticale et s'écoule de haut en bas [18].

Diagramme de séquence : Accès au compte

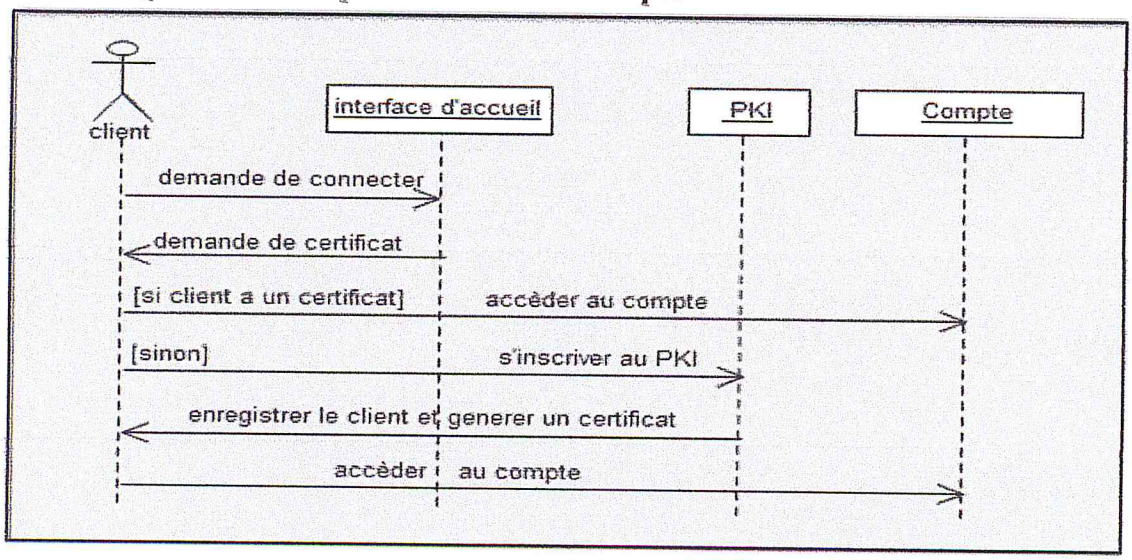


Figure IV.13: Diagramme de séquence Accès au compte

Pour que le client puisse connecter à notre plateforme, doit tout avant avoir un certificat généré par notre PKI, ce qu'il fait le client doit s'inscrive dans notre PKI qui implique une inscription automatique dans la plateforme.

↳ Diagramme de séquence : Enregistrement d'un client

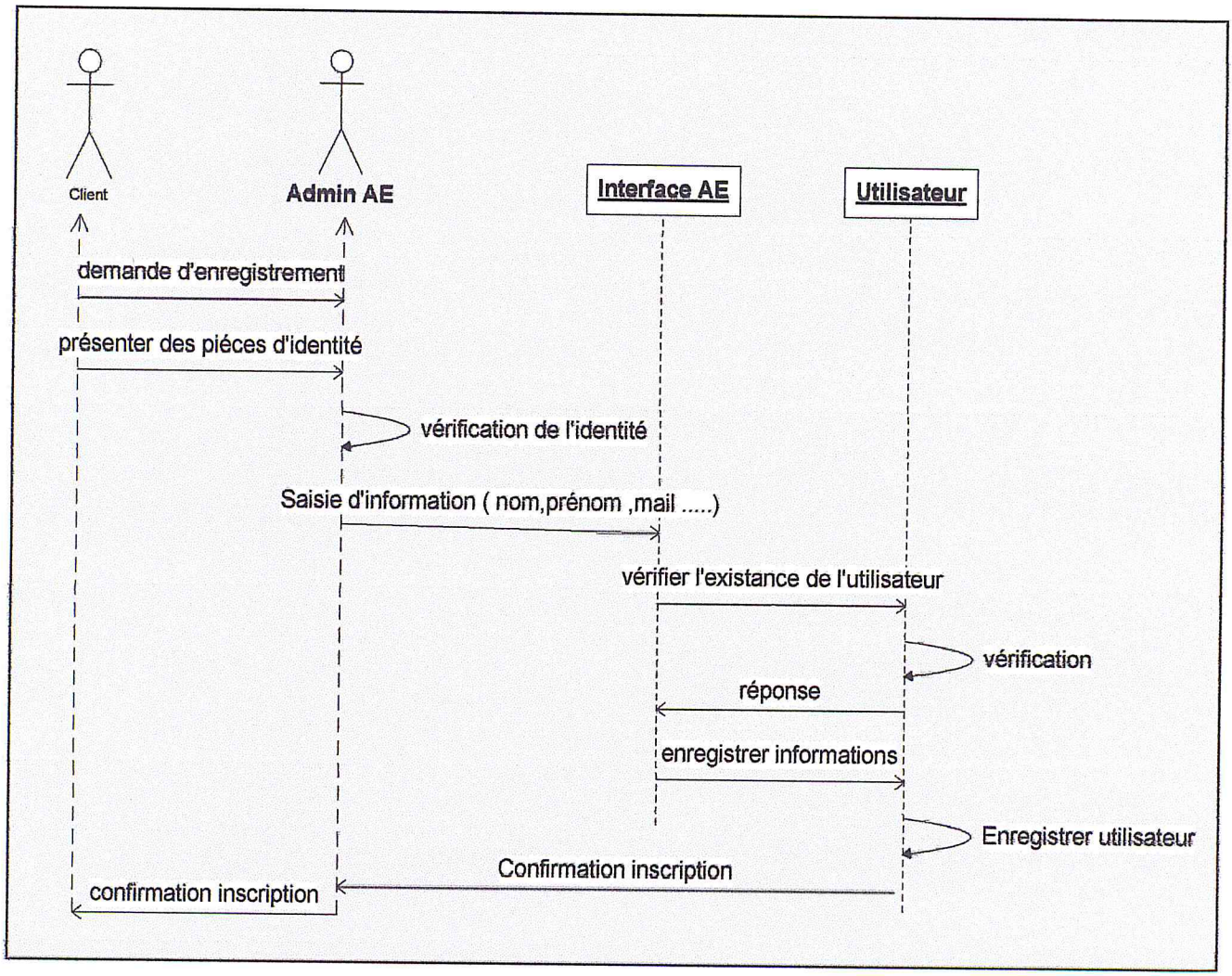


Figure IV.14: Diagramme de séquence Enregistrement d'un client

Avant tout utilisation de notre PKI, un client doit être enregistré auprès de l'AE.

Le client justifie son identité et son appartenance à l'organisation pour laquelle la PKI délivre les certificats.

L'administrateur de l'AE vérifie que le client n'est pas déjà enregistré. Si non, il l'enregistre.

Diagramme de séquence : Suppression d'un client

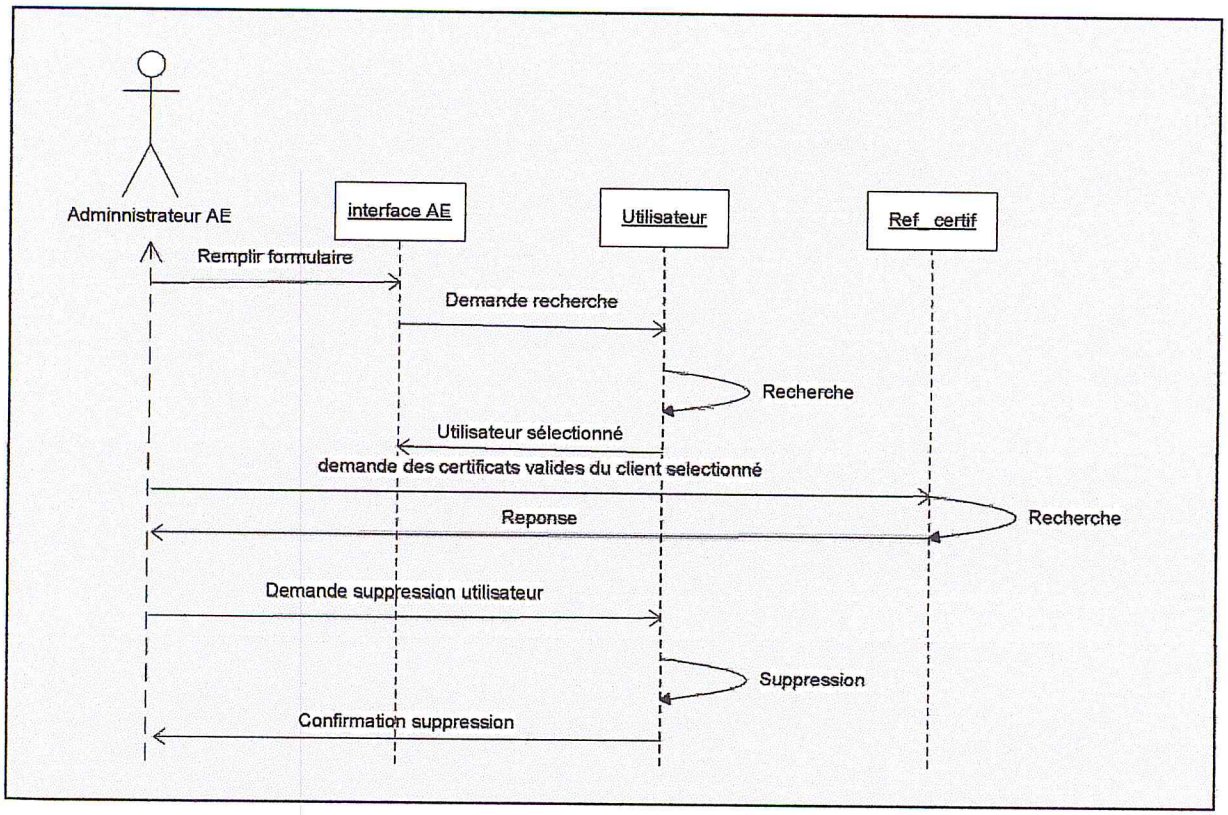


Figure IV.15: Diagramme de séquence : Suppression d'un client

L'administrateur de l'AE donne les informations sur l'utilisateur à supprimer.

Une recherche dans la base de données vérifie l'existence de l'utilisateur et le sélectionne. L'utilisateur ne peut être supprimé que s'il ne possède aucun certificat valide délivré par notre PKI. La vérification se fait dans la table des références des certificats.

S'il possède des certificats valides, ces dernières devront être révoquées avant la suppression de l'utilisateur (le scénario de révocation sera décrit dans la suite). Sinon, l'utilisateur est supprimé.

Diagramme de séquence : Modification des informations d'un client

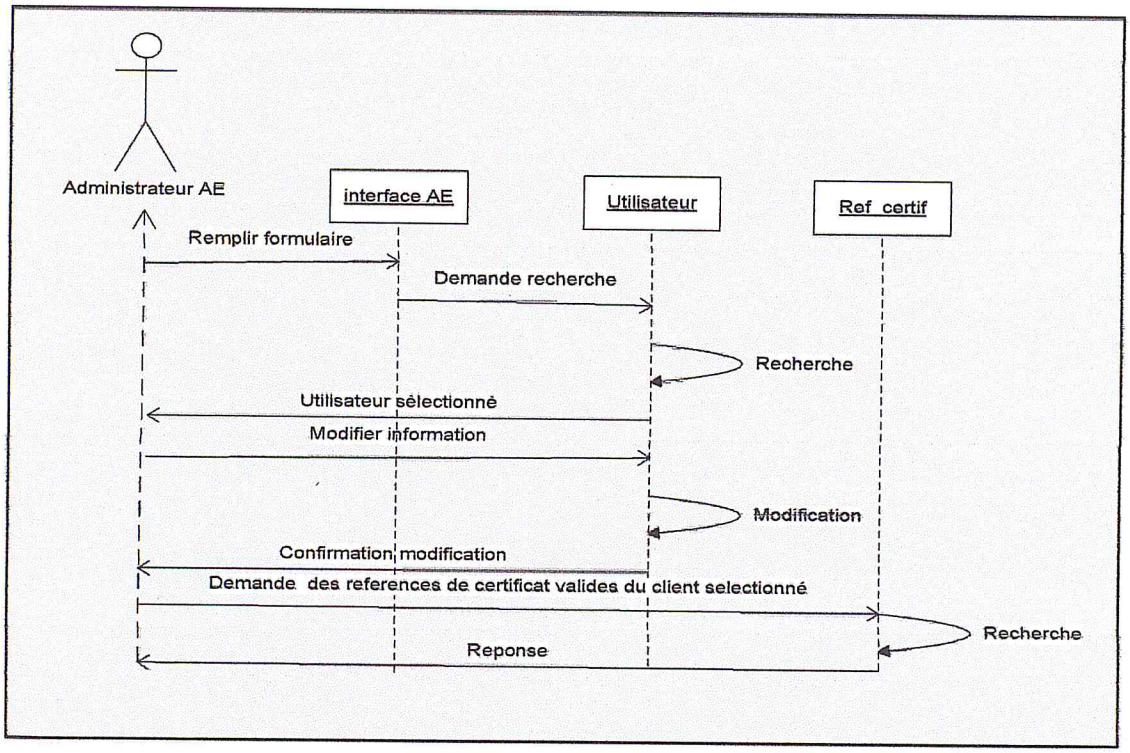
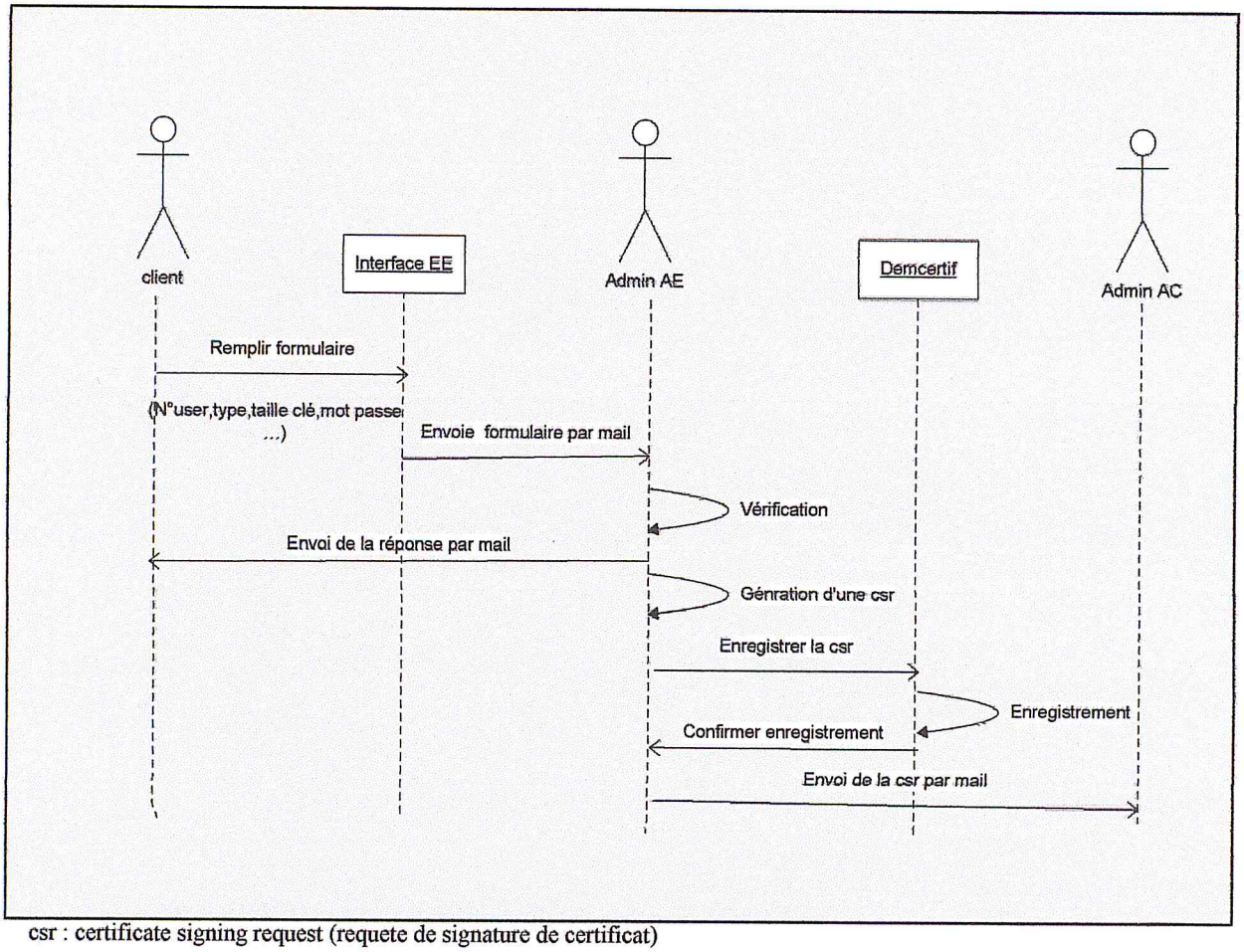


Figure IV.16: Diagramme de séquence modification des informations d'un client

Après modification des informations d'un client et si ce dernier possède des certificats valides, l'administrateur AE doit effectuer une demande de révocation (décrite dans la suite) avec comme raison : modification d'information personnel. Après la révocation un nouveau certificat correspondant aux nouvelles informations lui sera généré.

Diagramme de séquence : Demande d'un certificat



csr : certificate signing request (requete de signature de certificat)

Figure IV.17: Diagramme de séquence Demande d'un certificat

Le client remplit un formulaire par des informations personnelles et d'autres informations nécessaires à la génération d'un certificat.

Les informations à remplir pour une personne sont : nom, prénom, profil, agence, pays, ville, adresse mail, type de certificat, taille de la clé, mot de passe.

- Le mot de passe qui sera utilisé pour protéger sa clé privée.
- Les certificats d'authentification sont demandés par présence physique auprès de l'AE)
- La taille de la clé est 1024 bits par defaut.

Le formulaire est envoyé par mail à l'administrateur de l'AE.

L'administrateur de l'AE procède à la vérification des informations envoyées par le client et lui répond par mail (demande acceptée ou refusée).

Si la demande est acceptée, une requête de signature de certificat CRS est générée, enregistrée puis envoyée à l'administrateur de l'AC.

Diagramme de séquence : Demande de révocation ou recouvrement

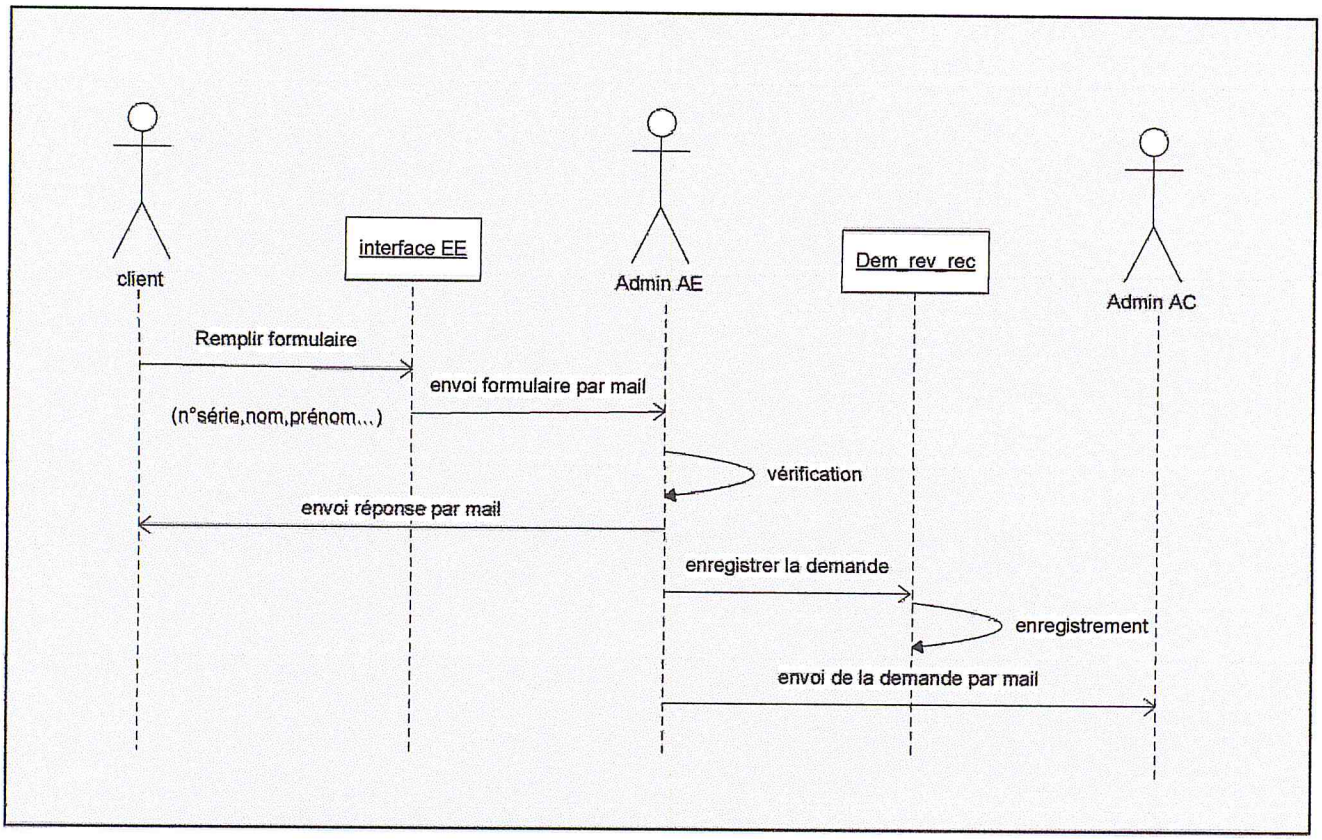


Figure IV.18: Diagramme de séquence : Demande de révocation ou recouvrement

Le client envoie une demande de révocation ou de recouvrement.

L'administrateur de l'AE vérifie les informations envoyées, vérifie également que le certificat à révoquer ou recouvrir sa clé privée existe et est valide.

L'AE répond au client par mail (demande acceptée ou refusée).

La demande est enregistrée puis envoyée à l'administrateur de l'AC.

Diagramme de séquence : Génération d'un certificat

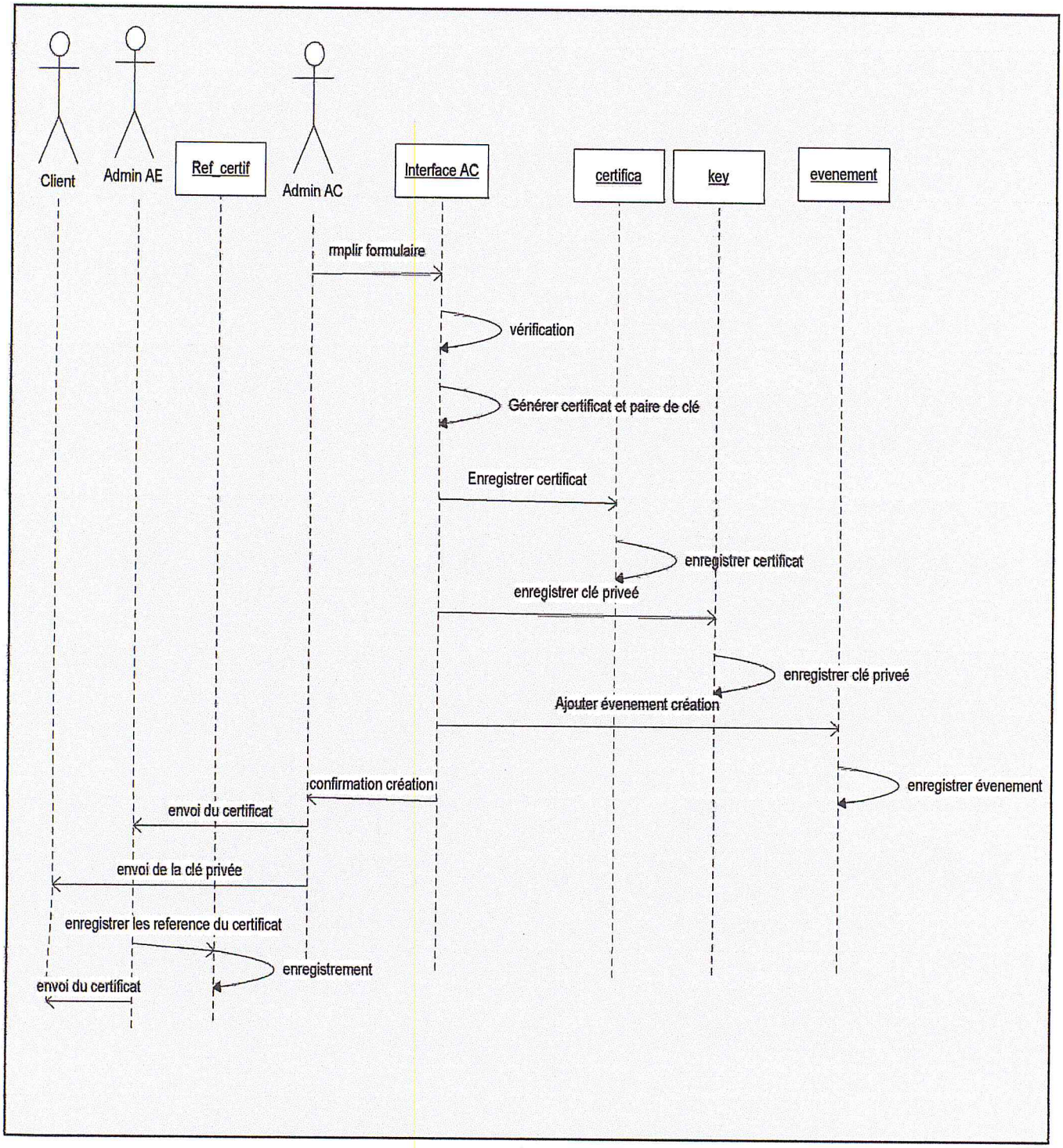


Figure IV.19: Diagramme de séquence : Génération d'un certificat

C'est l'administrateur de l'AC qui génère les certificats.

- ✓ La vérification se fait seulement quand l'AC génère un certificat sans demande provenant de l'AE (dans des cas particuliers tel que la cocertification d'une sous AC).

Après génération du certificat :

- ✓ Le certificat est enregistré et envoyé à l'AE qui le renvoi au client après avoir enregistré ses références.
- ✓ La clé privée est enregistrée et envoyée directement au client.
- ✓ L'évènement 'création ' du certificat est enregistré associé d'une date de création et du numéro de l'administrateur créateur du certificat.

↳ Diagramme de séquence : Renouvellement d'un certificat

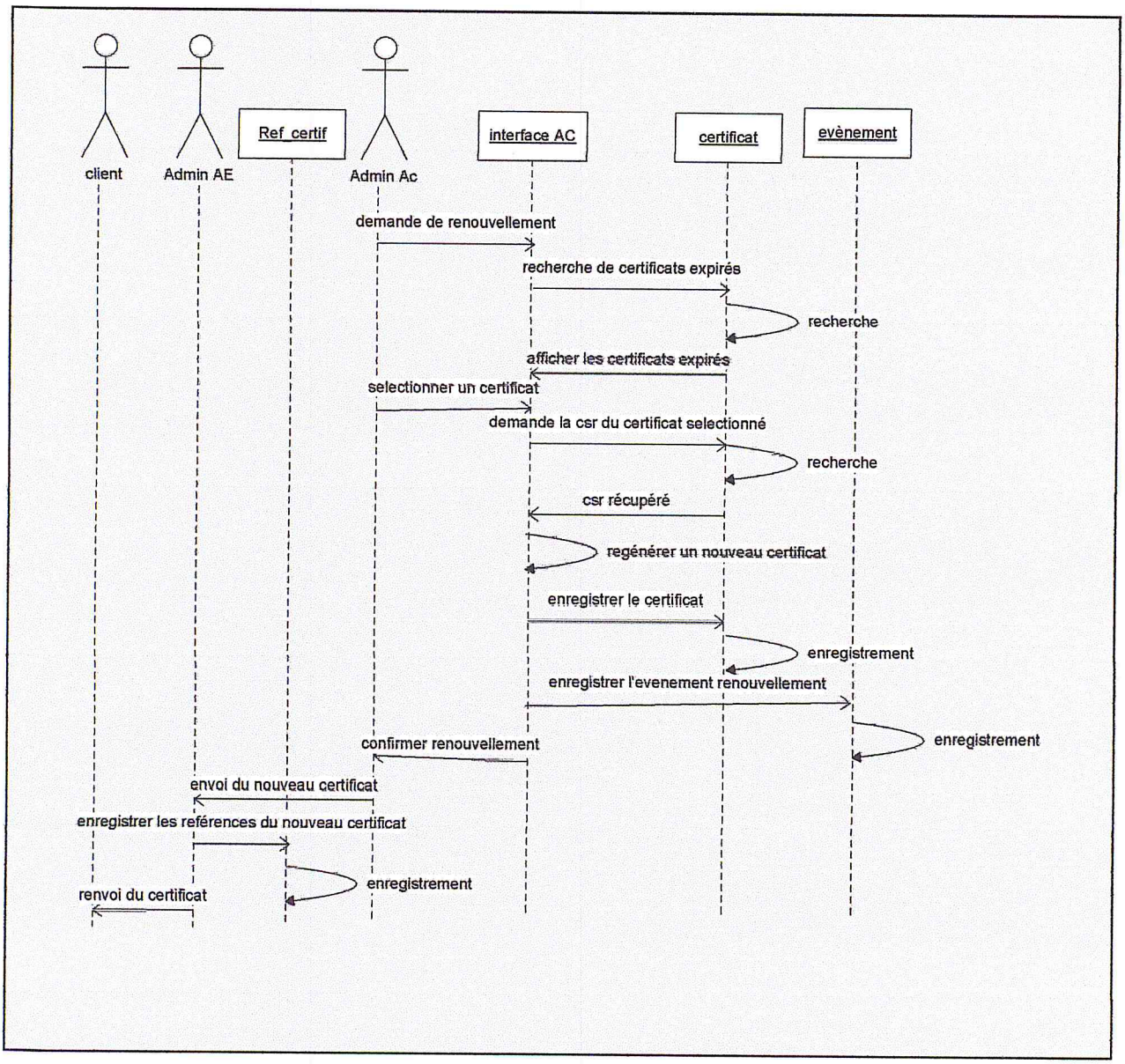


Figure IV.20: Diagramme de séquence : Renouvellement d'un certificat

Le renouvellement de certificat consiste à signer à nouveau l'ancienne requête de signature de certificat CSR (puisque les informations incluses dans la requête ne sont pas changées). Le résultat est un nouveau certificat avec une nouvelle période de validité.

Comme pour la génération d'un certificat, le nouveau certificat est enregistré ainsi que l'évènement ' renouvellement'.

Le nouveau certificat est envoyé à l'administrateur de l'AE pour enregistrer ses références puis le renvoi au bon client.

Diagramme de séquence : Révocation d'un certificat

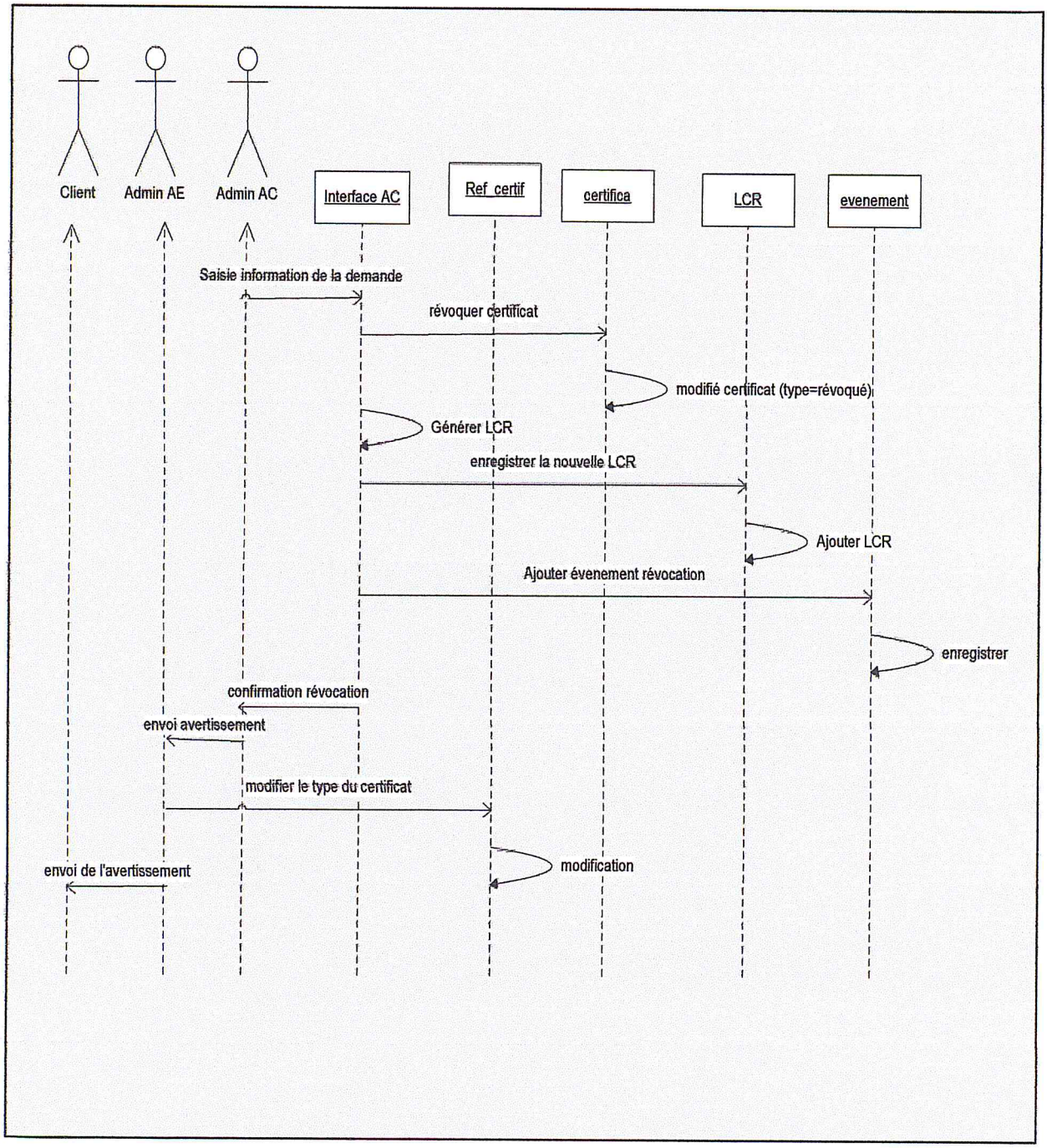


Figure IV.21: Diagramme de séquence : Révocation d'un certificat

La révocation d'un certificat est suivi d'une génération d'une nouvelle liste de certificats révoqués LCR et sa publication.

L'évènement 'révocation' est enregistré associé à la date de révocation et numéro de l'administrateur qui a révoqué le certificat. L'évènement est lui aussi publié.

Un avertissement est envoyé à l'administrateur de l'AE pour mettre à jour la table des références des certificats.

L'AE renvoie l'avertissement au client.

Remarque :

La révocation se fait pour une des causes suivantes :

- Quitter l'organisation,
- Changer des informations personnelles
- La clé privée est perdue ou compromise.

Dans les deux derniers cas, une régénération automatique du certificat est effectuée.

Diagramme de séquence : Recouvrement d'une clé

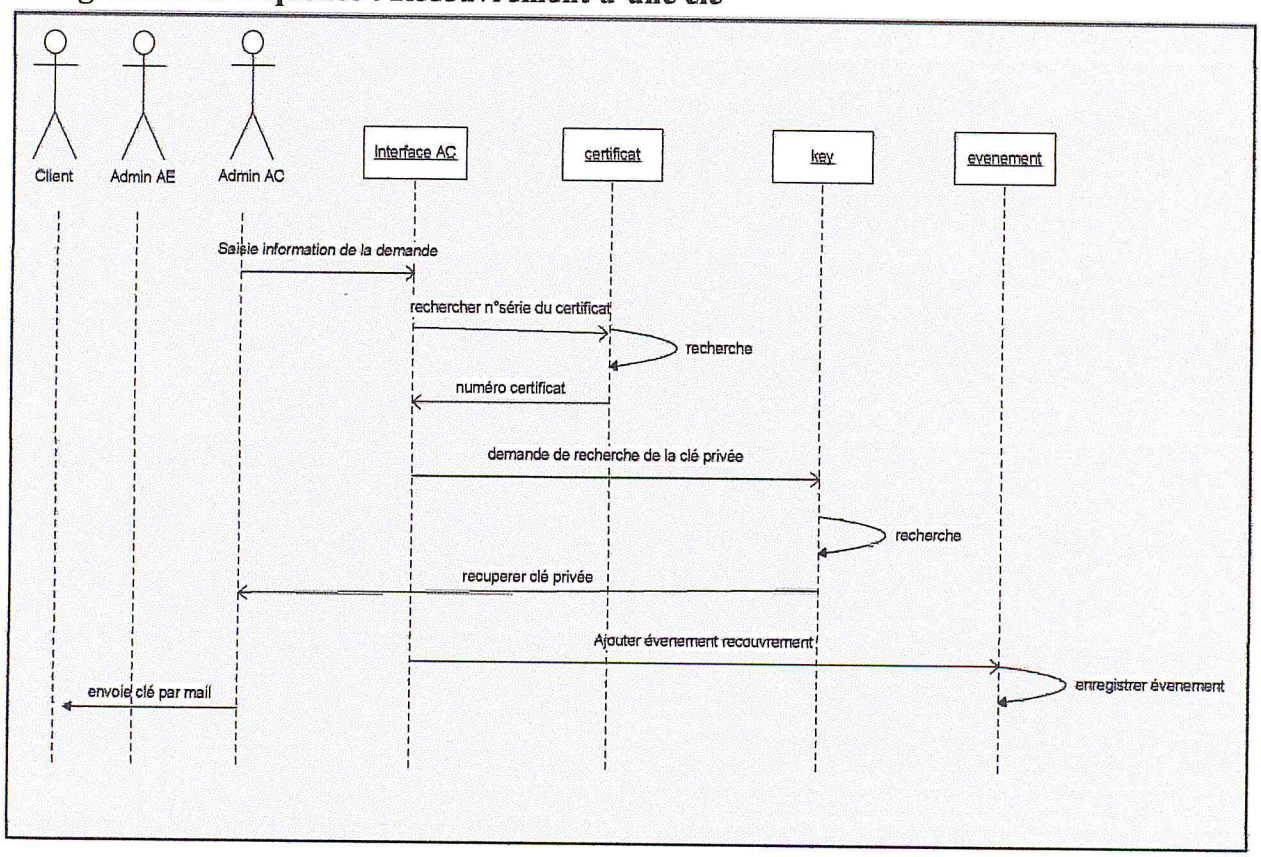


Figure IV.22: Diagramme de séquence : Recouvrement d'une clé privée

Le recouvrement d'une clé consiste à récupérer la clé de la base de données des clés privées et l'envoyer au client concerné.

Dans la base de donnée des clés privées, on ne peut rechercher une clé qu'en connaissant le numéro du certificat correspondant. C'est pour cela que l'administrateur de l'AC commence par effectuer une recherche du numéro du certificat en fournissant les informations nécessaires (nom, prénom, adresse mail, etc.).

Possédant le numéro du certificat, il peut rechercher la clé privée.

L'évènement 'recouvrement' est enregistré.

Enfin la clé privée est envoyée au client par mail via un canal sécurisé.

↳Diagramme de séquence : Rechercher la dernière LCR

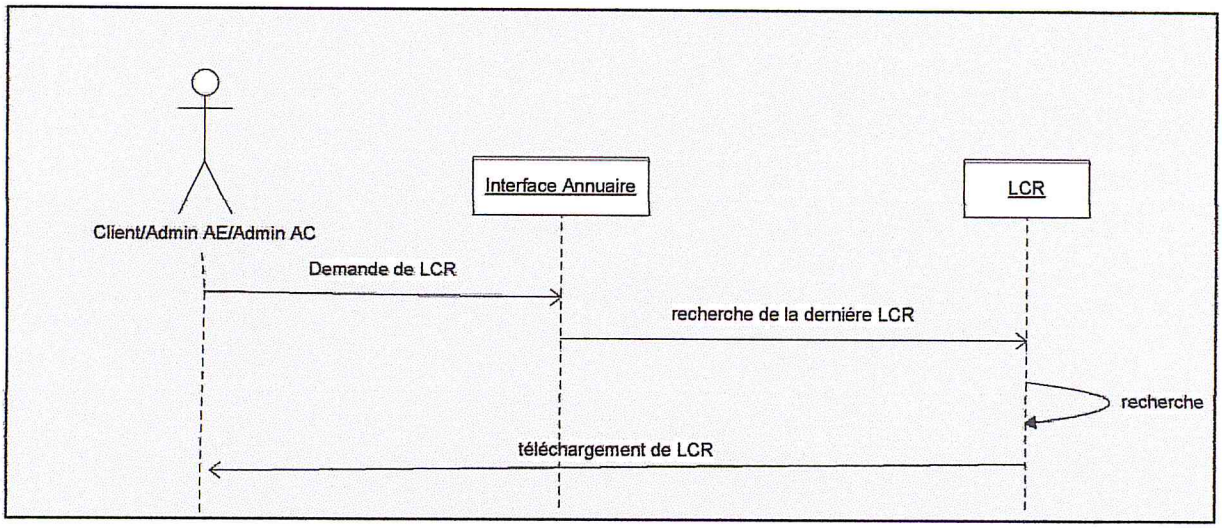


Figure IV.23: Diagramme de séquence : Rechercher la LCR

d. Diagramme de classe

Le diagramme de classe représente les objets qui interviennent dans la résolution du problème ainsi que leurs associations.

Une classe est la description d'un ensemble d'objets qui partagent les mêmes attributs, les mêmes opérations, les mêmes relations et la même sémantique.

Dans notre système, il existe deux bases de données :

- ✓ une base de données pour l'autorité d'enregistrement qui contient principalement les données sur les utilisateurs ; et l'autorité de certification qui contient principalement les données relatives aux certificats.
- ✓ une base de données pour la clé privée

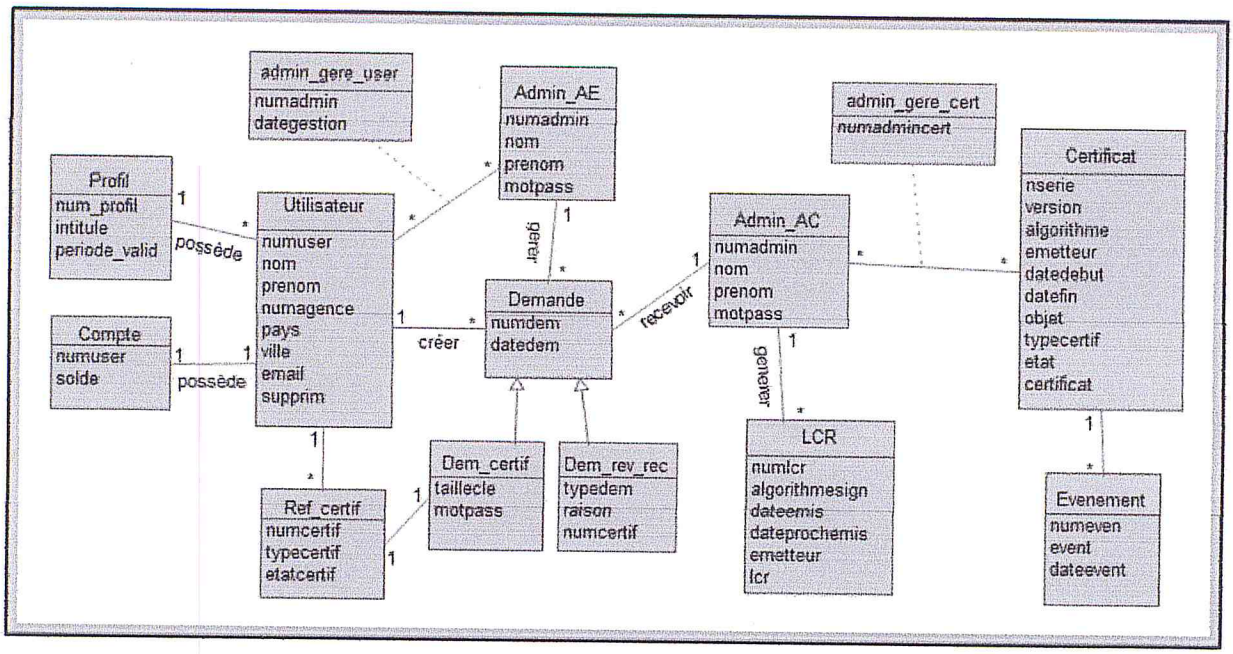


Figure IV.24: Diagramme de classe

Description du diagramme

La classe client contient les informations personnelles d'un client enregistré au sein de notre PKI. L'attribut 'supprim' sert à une suppression logique du client.

Le client possède un profil qui détermine la période de validité du certificat à lui générer.

L'administrateur de l'AE gère les clients et leurs demandes. Un client peut être géré par plusieurs administrateur (un l'enregistre, l'autre modifie ces information, etc.).Une demande est traitée par un seul administrateur. La trace de cette gestion est gardée dans la classe d'association 'Admin_gere_user'.

Les demandes sont de trois types : une demande de certificat, une demande de révocation et une demande de recouvrement. Les deux dernières sont regroupées dans la même classe puisqu'elles possèdent les mêmes attributs.

La classe Ref_certif contient les références de touts les certificats d'un client relatif à une demande.

La classe certificat contient les informations comprises dans un certificat x.509. De plus elle contient le texte du certificat, son type et son état.

L'état du certificat peut être : valide, révoqué ou expiré.

Un certificat est géré par un ou plusieurs administrateur (un le génère, l'autre le révoque, ...etc.). Évidemment un administrateur gère plusieurs certificats.

La classe évènement contient touts les évènements portés sur un certificat par un administrateur.

Un évènement peut être : une création, révocation, ou recouvrement d'une clé privée.

La classe LCR contient les listes de certificats révoqués. Les attributs standards figurant d'une LCR X.509 sont compris. L'attribut 'lcr' de la classe représente le texte de la LCR au format PEM.

- **Diagramme de classe pour la base de données des clés privées**

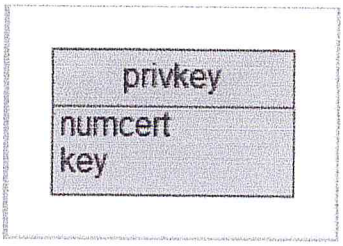


Figure IV.25: Diagramme de classe de la base de données des clés privées.

Pour des raisons de sécurité, nous avons choisit de sauvegarder les clés privées dans une base de données à part au lieu de les sauvegarder dans la base de données principale de l'AC (présentée ci-dessus). En effet cette dernière est mise en ligne via l'annuaire.

Nous avons pensé tout d'abord à utiliser un fichier pour la sauvegarde des clés privées au lieu de toute une base de données. Mais cette solution complique la gestion des clés et offre des moyens de sécurité moins élaborés que les solutions possibles avec les SGBD.

Dans la classe 'privkey', nous avons choisit comme identifiant de la clé privée, le numéro du certificat lui correspondant puisqu'il est unique.

e. Diagramme d'état

Un diagramme d'état est propre à une classe donnée, il décrit les états des objets de cette classe, les évènements auxquels ils réagissent et les transitions qu'ils effectuent.

Les classes de notre système ayant un comportement dynamique et donc nécessitant un digramme d'état sont : la classe utilisateur, la classe certificat et la classe LCR.

Diagramme d'état : utilisateur

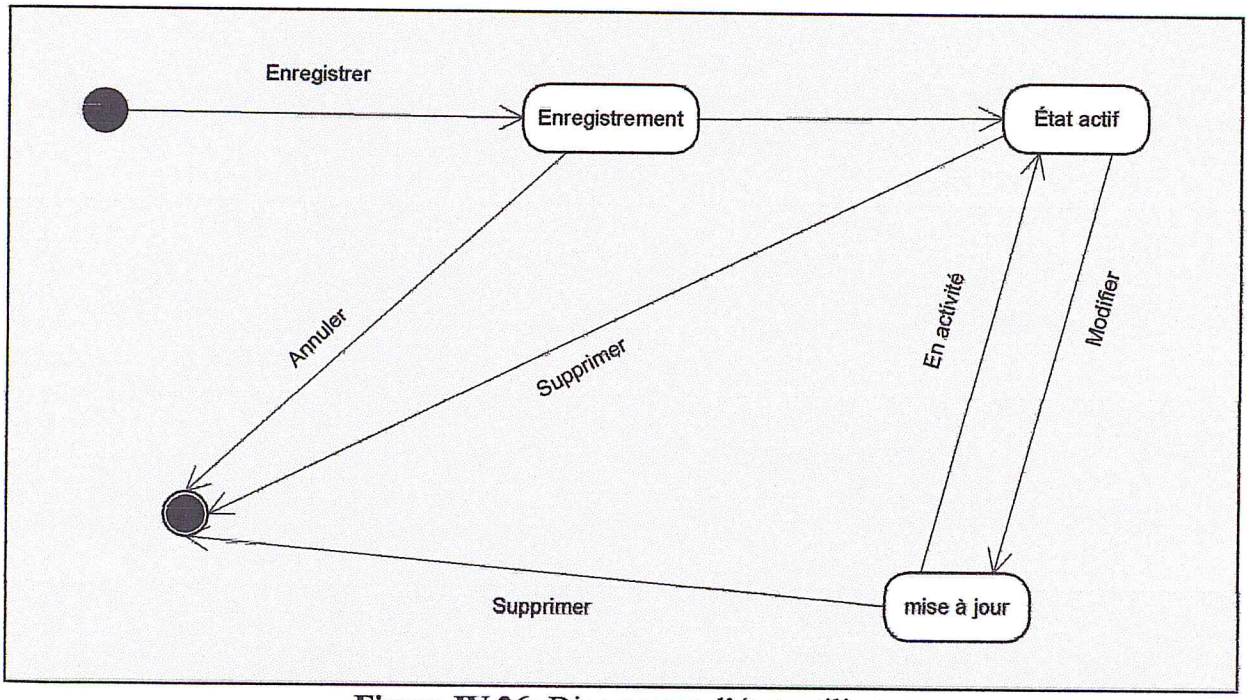


Figure IV.26: Diagramme d'état utilisateur

Tout client PKI est enregistré.

On peut lui modifier ces informations personnelles, son profil.

Il peut être supprimé pour des raisons telle que : quitter l'organisation.

Diagramme d'état : certificat

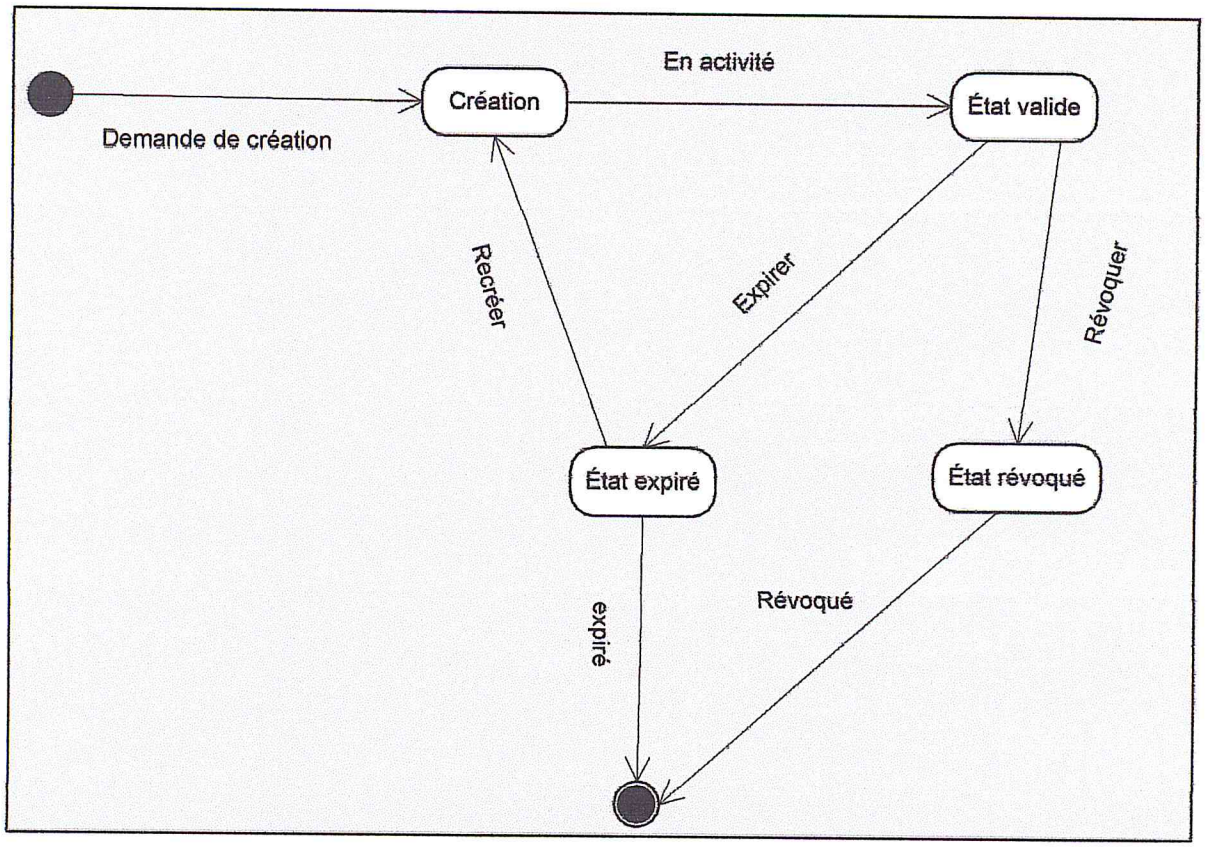


Figure IV.27: Diagramme d'état : certificat

Un certificat généré est valide jusqu'à :

Soit sa révocation pour des raisons telles que : compromission de clé privée, modification des informations d'un client ou quitter l'organisation.

Soit son expiration : la période de validité est écoulé.

Un certificat expiré peut être renouvelé.

Diagramme d'état : LCR

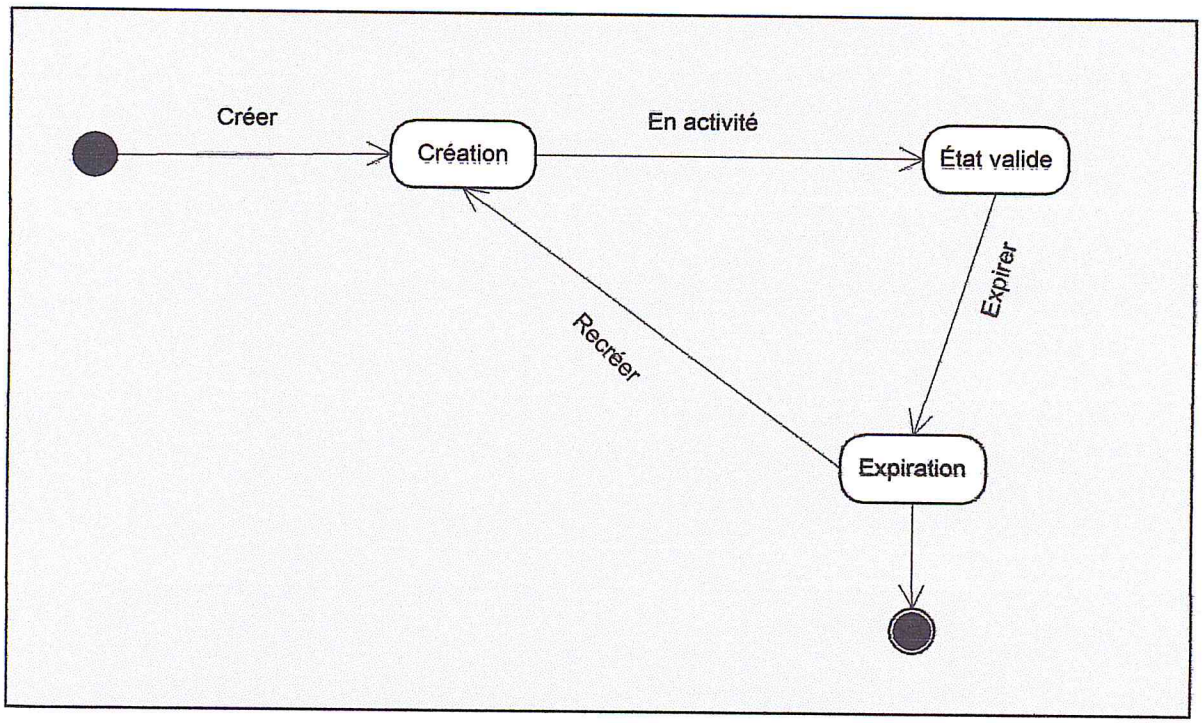


Figure IV.28: Diagramme d'état : LCR

Une liste de certificats révoqués a aussi une période de validité limite (30 jours par défaut). Lors de son expiration une nouvelle LCR est automatiquement générée.

4.3 Conclusion

Dans ce chapitre nous avons étudié et analysé d'abord les besoins et les objectifs du notre système, ce qui nous a mené par la suite à tracer les grands lignes à suivre pour concevoir et implémenter notre application, en utilisant l'approche **UML**.

Le chapitre suivant intéressera aussi aux détailles des phases tests globaux.

CHAPITRE 5

REALISATION

5.1 Introduction

On a vu dans le chapitre précédant la conception et la modélisation de notre plate forme e-banking et notre PKI, et comme tout autre logiciel de sécurité, on doit valider ses fonctionnalités en établissant une série de tests.

5.2 Environnement de développement

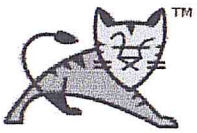
Nous présentons dans cette section les outils que nous avons utilisés pour réaliser notre travail (serveur web, SGBD, langages de programmation, …etc.) tout en justifiant nos choix.

Les logiciels que nous avons utilisés sont :

- Apache Tomcat version 6.0
- MySQL version 5.1

Pour le développement de nos pages web, nous avons utilisé le leader des environnements de développement web : Java EE

5.2.1 Le serveur web Apache



Les serveurs web les plus populaires aujourd'hui sont : Apache, Microsoft IIS, Zeus et Sun One, etc. Nous avons choisit Apache pour les avantages suivants : [16]

- ✓ Apache est gratuit.
- ✓ Le code source d'Apache est libre ce qui permet sa personnalisation pour une application particulière. Cette disponibilité du code source est la raison principale de sa popularité.
- ✓ La configuration d'Apache s'effectue en modifiant ses fichiers de configuration au sein desquels des directives permettent de définir son comportement. Cette méthode de configuration lui procure une souplesse permettant à l'administrateur du serveur un contrôle sur les fonctionnalités et la sécurité offerte par Apache.
- ✓ Apache a une structure modulaire. L'administrateur du serveur est libre de déterminer les modules nécessaires seulement.
- ✓ Apache implémente SSL grâce au module mod-ssl et la bibliothèque Openssl «une boite à outils cryptographiques implémentant le protocole SSL).

5.2.2 Le SGBD MYSQL

Les SGBD libres et gratuits sont nombreux. MYSQL, mSQL, Postgres en sont des exemples. Si nous avons choisit MYSQL, c'est plus pour des raisons de performances et fonctionnalités offertes. Nous citerons dans la suite ses principaux avantages : [17]

- ✓ MYSQL est beaucoup moins complexes à installer et à administrer que d'autres systèmes.
- ✓ MYSQL supporte le langage de requête SQL comme on peut lui accéder via ODBC.
- ✓ MYSQL permet des connexions multiples en même temps et utiliser différentes bases de données simultanément.
- ✓ MYSQL dispose d'un système de contrôle intégré qui interdit la consultation de données à ceux qui n'en ont pas l'autorisation.

5.2.3 Environnement de développement

Notre choix s'est porté vers l'EDI, qui permet de créer des applications Java EE et Web, incluant des outils pour JavaEE, JPA, JSP et d'autres.

5.3 Architecture technique de la plateforme e-banking

La plate-forme e-banking permet aux clients de suivre les actualités de leur banque en ligne, de consulter ses comptes et d'effectuer des transitions bancaires.

Le schéma suivant illustre l'architecture technique de la plateforme e-banking :

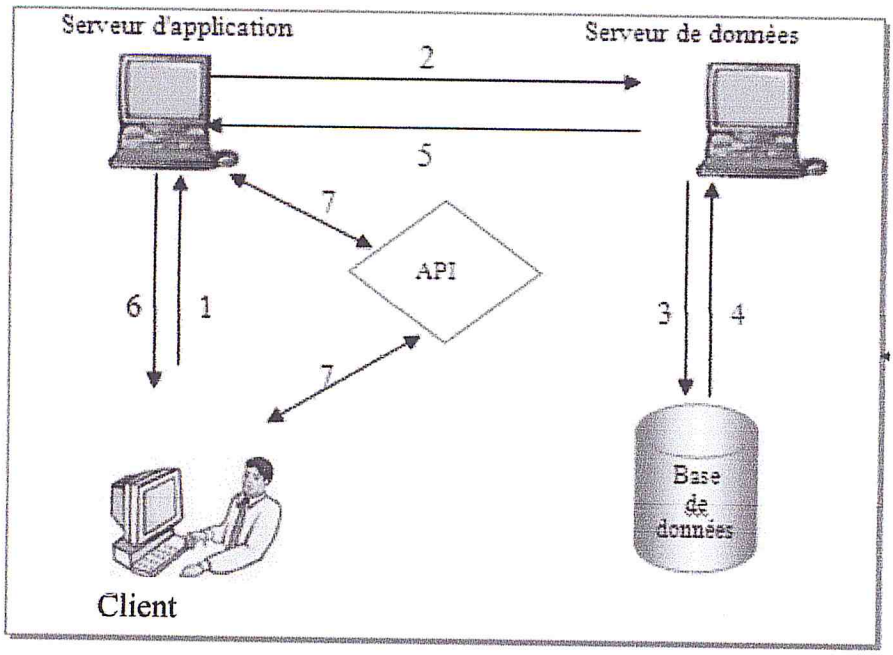


Figure V.1: Architecture technique de la plateforme e-banking.

Le schéma de la figure IV.1 montre l'interaction entre les différentes entités constituant la plate-forme e-banking:

1: Le client demande une ressource au système (serveur d'application).

2: Le serveur d'application fait appel au serveur de données afin d'identifier le client et de lui fournir ses ressources propres.

3, 4 et 5 : Le serveur de données accède à la base de données, (3) pour récupérer les données qui lui sont demandées par le serveur d'application (4) puis les lui envoie (5).

6: Le serveur d'application fournit la ressource demandée au client.

7: Si la ressource demandée par le client est un objet statistique (relevé des transactions bancaires), le système lance l'API qui à son tour interagit avec le client pour récupérer les modèles de données.

5.4 Architecture technique de NS-PKI

NS-PKI est le nom de notre PKI. C'est l'acronyme de Nesrine-Security Public Key Infrastructure.

Notre PKI est constituée principalement de trois applications web différentes :

- Une destiné au client. Dans notre cas : particulier, promoteur, ou société. Cette application lui permet seulement d'envoyer des demandes. Aucun serveur de base de données n'est donc nécessaire.

- Une deuxième application destinée l'administrateur de l'AE lui permettant la gestion des clients, des profils, des demandes. Une base de données est donc nécessaire.
- La troisième application est destinée à l'administrateur de l'AC. Elle lui permet la gestion des certificats et des clés. Une base de données pour les certificats et les LCR est nécessaire. Cependant, cette base sera en ligne ; accessible à partir de l'annuaire pour afficher LCR. C'est pour cela qu'on a choisit de sauvegarder les clés privées dans une base de données à part.

Lors de son premier contact, le client doit se présenter auprès de l'AE pour s'enregistrer et acquérir un certificat d'authentification.

Toutes les communications dans la PKI sont sécurisées. En effet, des informations personnelles, des mots de passe, des clés privées sont échangés entre l'EE, l'AE et l'AC.

Les communications entre EE, AE, AC et le serveur web se font avec le protocole HTTPS.

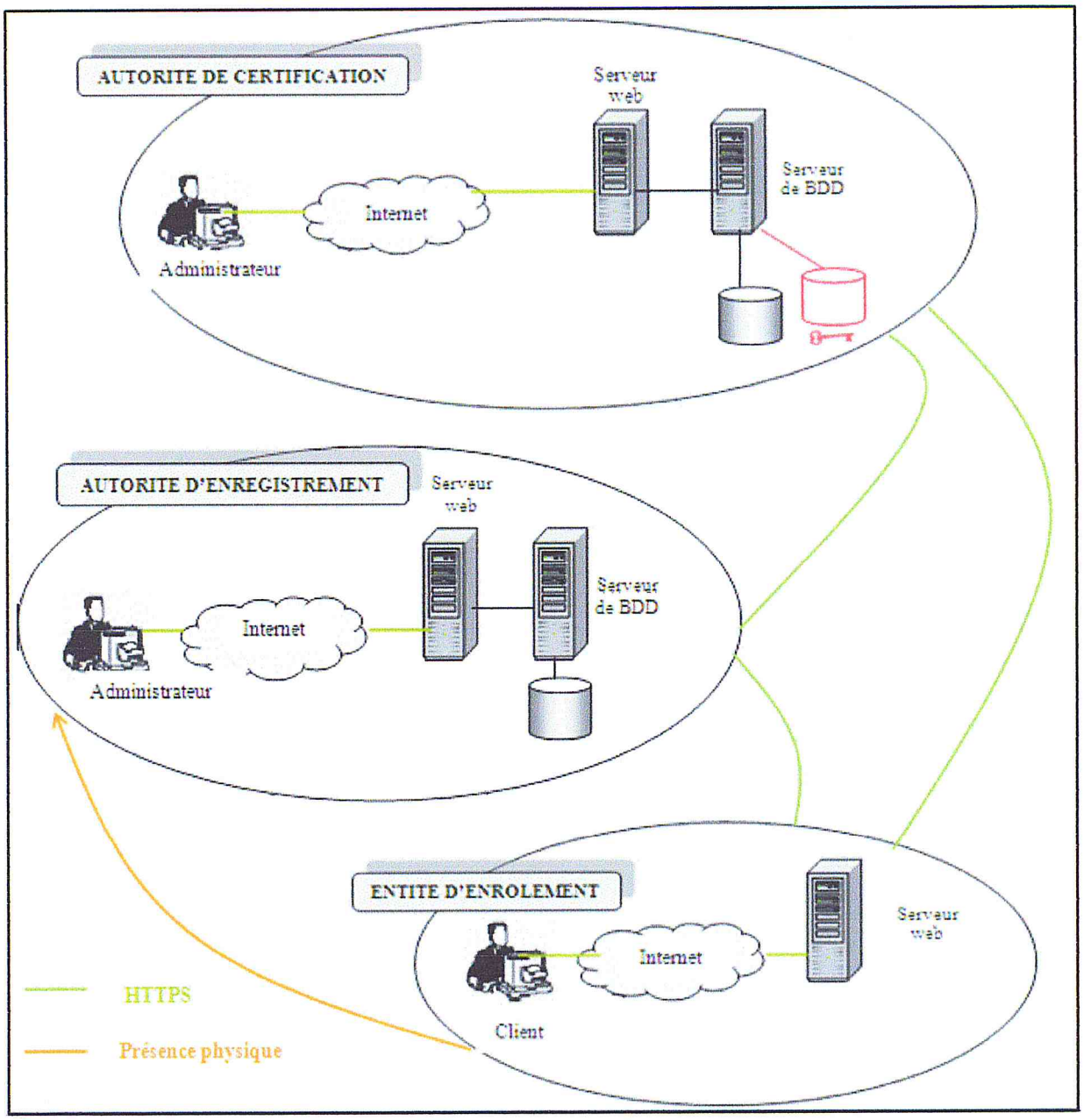


Figure V.2: Architecture technique explicite de PKI.

5.5 Fonctionnement de notre application

Dans ce qui suit, nous allons présenter certains aspects de notre système sous forme d'interfaces.

5.5.1 Page d'accueil de notre site e-banking

Figure V.3: Page d'accueil du site.

5.5.2 Sécuriser la connexion à la plateforme

Afin de sécuriser l'accès aux comptes utilisateurs, on a eu recours à certaines précautions comme :

- Identification d'un acteur par un pseudonyme et un mot de passe.
- Mots de passe cryptés
- Un poste ne supporte qu'un seul compte à la fois
- Un compte ne peut être ouvert sur deux postes simultanément

Pour renforcer la sécurité de la plateforme, nous avons eu recourt à l'authentification par certificat numérique en plus sécuriser la avec un mot de passe.

L'autorité de confiance de notre plateforme e-banking ; personne ne peut accéder s'il ne possède pas un certificat délivré par NS-PKI

Si on essaye de se connecter, le serveur demande le certificat du client pour l'authentifier :

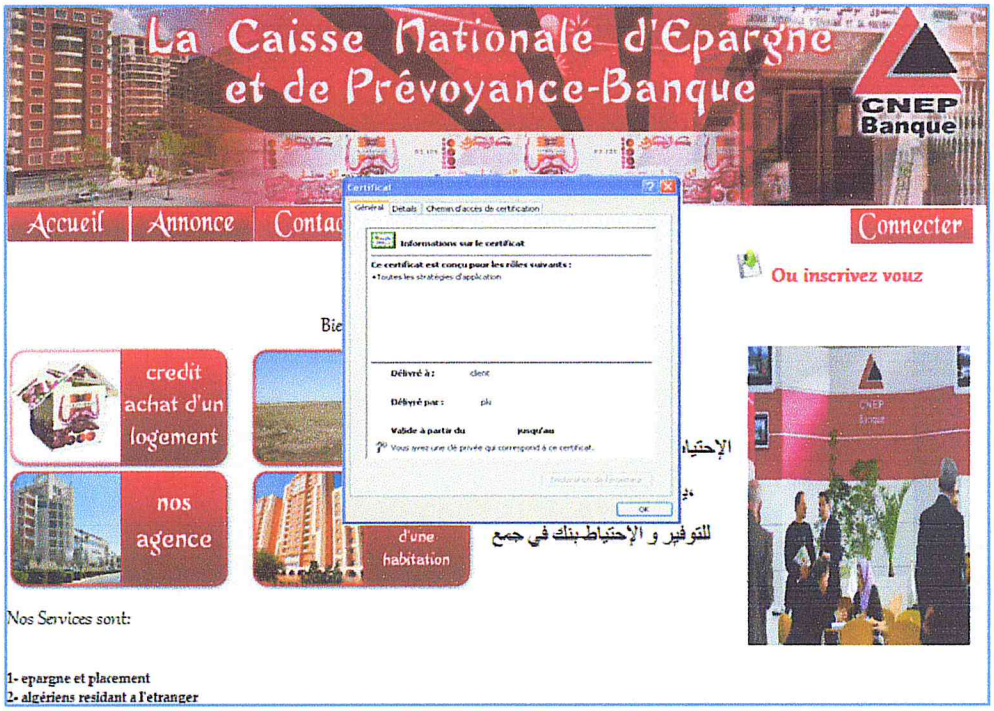


Figure V.4 : Authentification d'un client pour l'accès au compte

Enfin, le client peut accéder à son compte :

Figure V.5: Accès au compte client

5.5.3 Page d'accueil de NS-PKI

Figure V.6: page d'accueil de NS-PKI

5.5.4 Entité d'enrôlement : Application client

Si le client veut accéder à son compte bancaire, doit d'abord inscriver dans notre PKI pour avoir un certificat d'authentification.

L'enregistrement dans notre site e-banking est automatiquement validé après l'enregistrement dans la PKI.

Le client ne peut accéder à l'entité d'enrôlement que s'il possède un certificat d'authentification délivré par NS-PKI et l'installe dans son navigateur (le serveur authentifie le client).

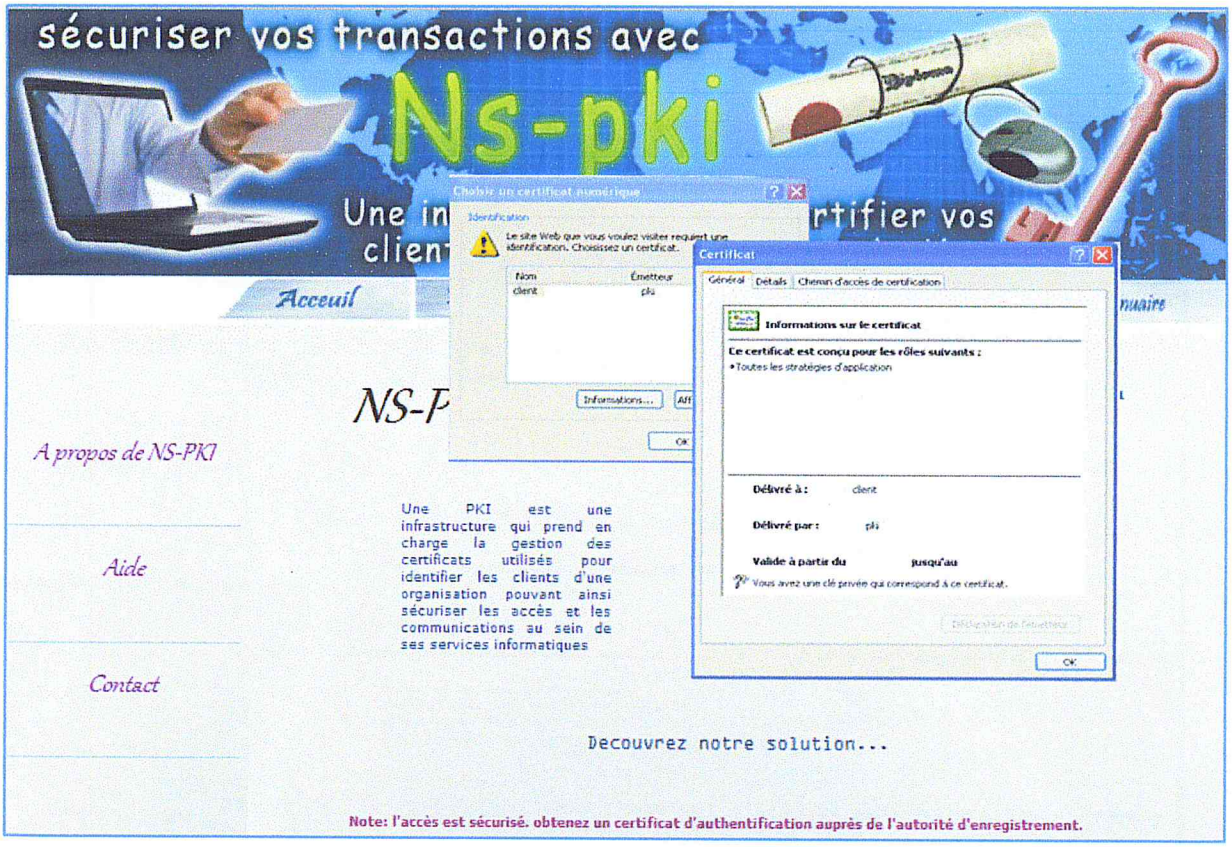


Figure V.7: Authentification du client pour l'accès à l'EE

Le certificat est protégé par un mot de passe ; en cas ou le client oublie son certificat dans le navigateur, personne ne peut l'utiliser.

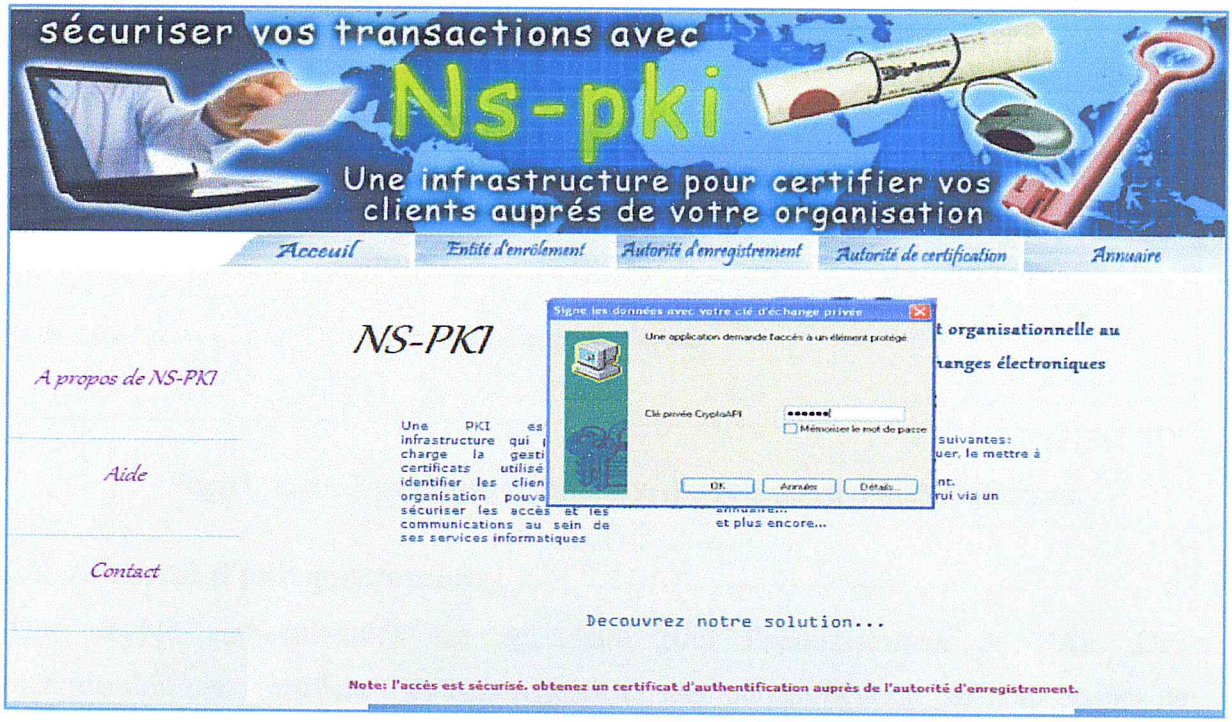


Figure V.8: protection du certificat par mot de passe.

Figure V.11: Authentification de l'administrateur de l'AE

5.5.6 Autorité de certification

Comme pour l'administrateur de l'AE, une double authentification est nécessaire pour l'administrateur de l'AC. Une authentification par certificat d'authentification et une authentification par nom et mot de passe. Il pourra ensuite accéder à sa page d'accueil :

Figure V.12: page d'accueil de l'AC

L'AC met en ligne un annuaire dont l'accès n'est possible que pour les acteurs de NS-PKI

Figure V.13: page d'accueil de l'annuaire

5.6 Conclusion

NS-PKI est une infrastructure à clé publique mettant en œuvre les fonctionnalités nécessaires à la gestion des certificats des clients de notre plateforme e-banking.

Par son architecture générale et ces modules implémentés indépendamment d'une application spécifique, NS-PKI peut être adapté à n'importe quel utilisation que ce soit e-learning, e-commerce, e-gouvernement…etc.

Dans le cadre de notre réalisation, nous avons exploité une plateforme e-banking et la une PKI pour sécuriser l'accès à la plateforme.

CONCLUSION GENERALE

L'arrivée des technologies de l'information et de la communication a ouvert la voie à l'échange d'information à distance. Le travail bancaire en ligne « e-banking » a pris naissance et est aujourd'hui en pleine expansion en monde. Cependant les échanges des informations confidentielles des clients sont menacés par des attaques visant à les intercepter et d'usurper l'identité d'un client, …etc. Pour expliciter ce contexte, nous avons fait une étude bibliographique englobant :

- Un chapitre sur les attaques informatiques et la sécurité des échanges parcourant les notions de base de la cryptographie et le protocole SSL « Secure Socket Layer ».
- Un chapitre sur les PKI, les infrastructures de gestion de certificats numériques.
- Un autre chapitre sur le travail bancaire en ligne « e-banking » sur lesquelles a porté notre application, tout en dégageant leurs besoins en sécurité.

Nous sommes passées ensuite à la conception puis la réalisation de notre système. Nous avons développé une plateforme e-banking de CNEP-banque qui fournit plusieurs services en ligne pour ces clients, et pour sécuriser l'accès à cette plateforme et gérer des certificats numériques à ces clients nous avons développer une PKI ; une application Web qui gère des certificats numériques nécessaires pour s'authentifier lors d'une session HTTPS « protocole de transfert de données sécurisé ».

Les objectifs fixés sont atteints. Cependant, des améliorations sur notre PKI peuvent être rajoutées, nous citerons à titre d'exemples :

☞ Intégration d'un module de publication qui permet la mise à disposition des certificats à des serveurs LDAP « Lightweight Directory Access Protocol ». LDAP est un protocole d'annuaire sur TCP/IP offrant beaucoup plus de fonctionnalités par rapport à un annuaire géré par un SGBD. En plus de la diffusion de données pour les utilisateurs, LDAP met l'information à disposition d'autres applications et systèmes d'exploitation.

☞ Adapter notre PKI pour supporter le protocole WTLS « Wireless Transport Security Layer » correspondant à l'adaptation du protocole TLS au monde du sans fil WAP « Wireless Application Protocol ». Des certificats spécifiques sont définit pour ce protocole. Cette adaptation permet des échanges sécurisés à partir de terminaux mobiles comme les téléphones mobiles et les assistants personnels électroniques.

Le projet nous a de plus permis d'approfondir nos connaissances sur la programmation en JAVA, et le langage SQL, Perfectionner en améliorant nos connaissances en programmation web.

BIBLIOGRAPHIE

[1]. Jean-François Pillou, « Tout sur la sécurité informatique »,
édition DUNOD, 2005.

[2]. Solange Ghernaouti-Hélie, « Sécurité informatique et réseau »,
édition DUNOD, 2006.

[3]. Le grand livre de sécuritéinfo.com, 2004.

[4]. www.linux-france.org

[5]. Eric Maiwald, « Sécurité des réseaux »,
édition CAMPUSPRESS, 2001.

[6]. Thierry Autret, Laurent Belfin « Sécuriser ses échanges électroniques avec une PKI : solutions techniques et aspects juridiques ».
édition Eyrolles, 2002.

[7]. Suranjan Choudhury, Kartik Bhatnagar «Public Key Infrastructure Implementation and Design»
édition Hungry Minds, 2002.

[8]. Paul DUBOIS « MYSQL, le serveur SQL de bases de données multi API »
édition CompusPress, 2000

[9]. Livre de Jim Conallen « Concevoir des applications web avec UML. »
édition Eyrolles, 2000.

[10]. H.X.MEL, Dous BAKER « La cryptographie décryptée. »
édition CompusPress, 2001

[11]. Claude SERVIN « Réseaux et Télécommunications. Cours et exercices corrigés. »
édition Dunod, 2003

[12]. Khelfi Fatima Zohra, Challal Zakia, « Développement et Déploiement d'une PKI pour sécuriser une plateforme de travail collaboratif à distance appliquée au E-learning » thèse d'ingéniorat, INI, 2006/2007

[13]. Présentation de G.Labouret « PKI et certificats. ». 1999
http://www.hsc.fr/ressources/presentations/pki/img14.htm

[14]. www.wikipedia.org, 2007

[15]. Livre Anonyme. « Sécurité optimale : le guide d'un ex-hacker pour protéger vos sites web et votre réseau. »
Edition CompusPress. 2001

[16]. Peter WAINWRIGHT «Apache professionnel. »
Edition Eyrolles, 2000

[17]. Paul DUBOIS « MYSQL, le serveur SQL de bases de données multi API. »
Edition CompusPress, 2000

[18]. Saleh M.Nsouli, Andrea Schaechter « Les enjeux de la banque électronique »
http://www.imf.org/external/pubs/ft/fandd/fre/2002/09/pdf/nsouli.pdf

[19]. AESplus.net

[20]. www.epargnebourse.com

[21]. Sarra Batel, Chanane Aicha « conception et réalisation d'un site web d'enchère en ligne sécurisé » thèse de master 2. Université Saad Dahlab 2010/2011

ANNEXES

ANNEXE 1

QUELQUES ALGORITHMES A CLE PUBLIQUE

Dans la cryptographie à clé publique « ou cryptographie asymétrique » chaque communicant utilisent deux clés, l'une est connue par tous (clé publique), l'autre n'est connue que par lui-même (clé privée). Le message crypté avec l'une ne peut être décrypté qu'avec l'autre [11]. Les deux clés sont reliées mathématiquement entre elles de telle sorte qu'il est impossible de retrouver la clé privée en connaissant la clé publique.

5.7 1.1 L'algorithme RSA « Rivest Shamir Adleman »

Il existe différents algorithmes asymétriques. L'un des plus connus est le **RSA** «de ses concepteurs Rivest, Shamir et Adleman ». Cet algorithme est très largement utilisé, par exemple dans les navigateurs pour les sites sécurisés et pour chiffrer les e-mails. Il est dans le domaine public.

L'algorithme est remarquable par sa simplicité. Il est basé sur les nombres premiers.

Pour encrypter un message, on fait:	$\mathbf{c = m^e \bmod n}$
Pour décrypter:	$\mathbf{m = c^d \bmod n}$

m = message en clair

c = message encrypté

(e,n) constitue la clé publique

(d,n) constitue la clé privée

n est le produit de 2 nombres premiers

mod est l'opération de modulo (reste de la division entière)

1.1.1 Créer une paire de clés

Pour créer une paire de clés, il ne faut pas choisir n'importe comment **e**,**d** et **n**. Voici comment procéder:

1. Prendre deux nombres premiers **p** et **q** (de taille à peu près égale). Calculer **n = p*q**.
2. Prendre un nombre **e** qui n'a aucun facteur en commun avec **(p-1)(q-1)**.
3. Calculer **d** tel que **e*d mod (p-1)(q-1) = 1**

Le couple **(e,n)** constitue la clé publique. **(d,n)** est la clé privée.

1.1.2 Exemple

Commençons par créer notre paire de clés:

- Prenons 2 nombres premiers au hasard: **p = 29**, **q = 37**
- On calcul **n = p*q = 29 * 37 = 1073**
- On doit choisir **e** au hasard tel que **e** n'ai aucun facteur en commun avec **(p-1)(q-1)**:
- **(p-1)(q-1) = (29-1)(37-1) = 1008**
- On prend **e = 71**
- On choisit **d** tel que **71*d mod 1008 = 1**
- On trouve **d = 1079**
- On a maintenant nos clés :

La clé publique est **(e,n) = (71,1073)** (=clé d'encryptage)
La clé privée est **(d,n) = (1079,1073)** (=clé de décryptage)

On va encrypter le message '**HELLO**'. On va prendre le code ASCII de chaque caractère et on les met bout à bout:

m = 7269767679

Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que **n** ; **n** comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres:

726 976 767 900

(on complète avec des zéros)

Ensuite on encrypte chacun de ces blocs:

$726^{71} \bmod 1073 = 436$

$976^{71} \bmod 1073 = 822$

$767^{71} \bmod 1073 = 825$

$900^{71} \bmod 1073 = 552$

Le message encrypté est **436 822 825 552**. On peut le décrypter avec d:

$$436^{1079} \bmod 1073 = 726$$

$$822^{1079} \bmod 1073 = 976$$

$$825^{1079} \bmod 1073 = 767$$

$$552^{1079} \bmod 1073 = 900$$

C'est à dire la suite de chiffre **726976767900**.

On retrouve notre message en clair **72 69 76 76 79** : **'HELLO'**.

1.1.3 Dans la pratique

Dans la pratique, ce n'est pas si simple à programmer:

- Il faut trouver de grands nombres premiers (ça peut être très long à calculer)
- Il faut obtenir des nombres premiers **p** et **q** *réellement* aléatoires (ce qui est loin d'être évident).
- On n'utilise pas de blocs aussi petits que dans l'exemple ci-dessus: il faut être capable de calculer des puissances et des modulos sur de très grands nombres.

En fait, on utilise jamais les algorithmes asymétriques pour chiffrer toutes les données, car ils sont trop longs à calculer : on chiffre les données avec un simple algorithme symétrique dont la clé est tirée au hasard, et c'est cette clé qu'on chiffre avec un algorithme asymétrique comme le RSA.

Référence : http://sebsauvage.net/comprendre/encryptage/crypto_rsa.html

5.8 1.2 L'algorithme DSA « Digital Signature Algorithm »

Le DSA est un algorithme de signature numérique standardisé par le NIST aux États-Unis, du temps où le RSA était encore breveté. Une révision mineure a été publiée en 1996 « FIPS 186-1 » et le standard a été amélioré en 2002.

Le processus de signature se fait en trois étapes :

- génération des clés
- signature du document
- vérification du document signé

1.2.1 Générations des clés

- Choisir un nombre premier p de L-bit, avec $512 \leq L \leq 1024$, et L est divisible par 64
- Choisir un nombre premier q de 160 bits, de telle façon que $p - 1 = qz$, avec z un entier

- Choisir h, avec $1 < h < p - 1$ de manière à ce que $g = h^z \bmod p > 1$
- Générer aléatoirement un x, avec $0 < x < q$
- Calculer $y = g^x \bmod p$
- La clé publique est «p, q, g, y). La clé privée est x

1.2.2 Signature

- Choisir un nombre aléatoire s, tel que $1 < s < q$
- Calculer $s1 = (g^s \bmod p) \bmod q$
- Calculer $s2 = (\mathrm{H}(m) + s1*x)s^{-1} \bmod q$,
  où $\mathrm{H}(m)$ est le résultat d'un hachage cryptographique avec SHA-1 sur le message m
- La signature est ($s1$,$s2$)

1.2.3 Vérification

- Rejeter la signature si 0<s1<q ou 0<s2<q n'est pas vérifié
- Calculer $w = (s2)^{-1} \pmod q$
- Calculer $u1 = \mathrm{H}(m)*w \pmod q$
- Calculer $u2 = s1*w \pmod q$
- Calculer $v = [g^{u1}*y^{u2} \bmod p] \bmod q$
- La signature est valide si $v = s1$

Référence : http://fr.wikipedia.org/wiki/Digital_Signature_Algorithm

ANNEXE 2:

UML « UNIFIED MODELING LANGUAGE »

UML « Unified Modeling language » est un langage de modélisation graphique et textuel destiné à décrire des besoins, spécifier, documenter des systèmes et architectures logicielles et concevoir des solutions.

2.1 Les treize diagrammes UML

UML 2.0 s'articule autour de treize types de diagrammes, chacun d'eux étant dédié à la représentation des concepts particuliers d'un système logiciel. Ces types de diagrammes sont répartis en deux grands groupes :

- Six diagrammes structurels (concerne la structure du système pris " au repos ")
  - **Diagramme de classes :** Il montre les briques de base statiques : classes, associations, interfaces, attributs, opérations, généralisations, … etc.
  - **Diagramme d'objets :** Il montre les instances des éléments structurels et leurs liens à l'exécution.
  - **Diagramme de packages :** Il montre l'organisation logique du modèle et les relations entre packages.
  - **Diagramme de structure composite :** Il montre l'organisation interne d'un élément statique complexe.
  - **Diagramme de composants :** Il montre des structures complexes, avec leurs interfaces fournies et requises.
  - **Diagramme de déploiement :** Il montre le déploiement physique des « artefacts » sur les ressources matérielles.
- Sept diagrammes comportementaux : (concerne la dynamique de fonctionnement du système)
  - **Diagramme de cas d'utilisation :** Il montre les interactions fonctionnelles entre les acteurs et le système à l'étude.
  - **Diagramme de vue d'ensemble des interactions :** Il fusionne les diagrammes d'activité et de séquence pour combiner des fragments d'interaction.

- **Diagramme de séquence :** Il montre la séquence verticale des messages passés entre objets au sein d'une interaction.
- **Diagramme de communication :** Il montre la communication entre objets dans le plan au sein d'une interaction.
- **Diagramme de temps :** Il fusionne les diagrammes d'états et de séquence pour montrer l'évolution de l'état d'un objet au cours du temps.
- **Diagramme d'activité :** Il montre l'enchaînement des actions et décisions au sein d'une activité.
- **Diagramme d'états :** Il montre les différents états et transitions possibles des objets d'une classe.

Nous détaillons dans la suite les quatre diagrammes que nous avons utilisé pour modéliser notre application, à savoir le diagramme de cas d'utilisation, de séquence de classe et d'état transition.

2.2 Diagrammes de cas d'utilisation

La représentation par diagramme de cas d'utilisation permet de voir de façon simple les différents acteurs, comment est délimité le système, les fonctionnalités demandées au système, et les rôles des différents acteurs vis-à-vis du système.

Une phase de spécification des besoins doit précéder la modélisation par diagramme de cas d'utilisation. Elle doit décrire sans ambiguïté le système logiciel à développer .

2.2.1 Identification des acteurs

Les acteurs sont les utilisateurs extérieurs au système qui interagissent avec ce dernier . Un acteur peut consulter et/ou modifier directement l'état du système en mettant et/ou en recevant les messages susceptible d'être porteur de données.

2.2.2 Identification des cas d'utilisation

Un cas d'utilisation est un ensemble de séquences d'actions réalisées par le système produisant un résultat observable intéressant pour un acteur particulier. Il permet de décrire ce que le futur système devra faire sans spécifier comment il le fera.

2.2.3 Représentation graphique

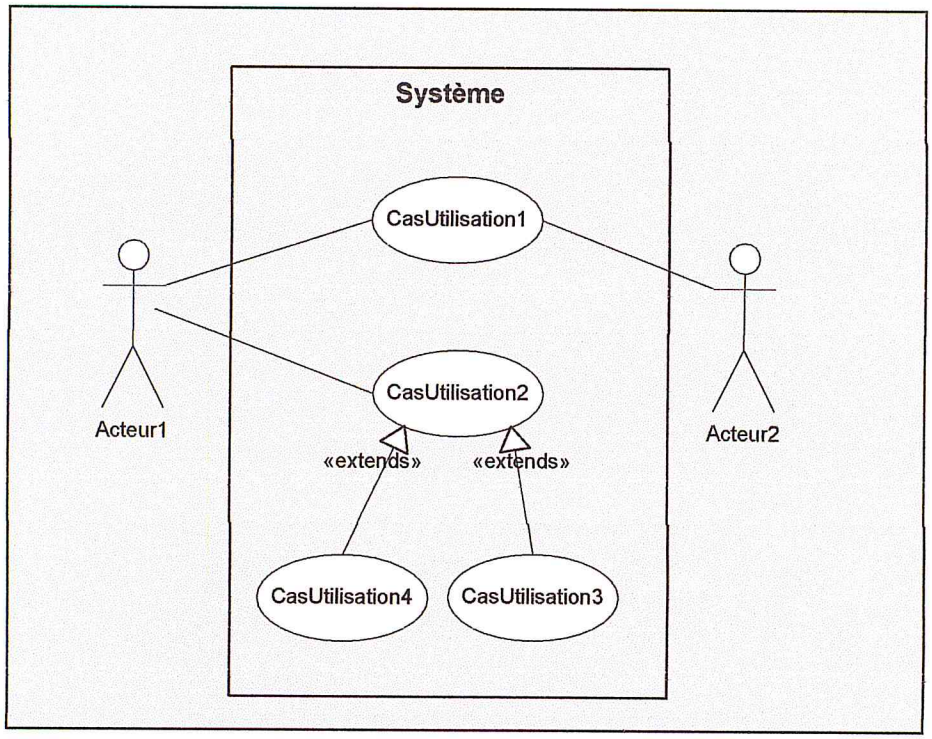


Figure 1: Représentation d'un diagramme de cas d'utilisation

Les associations entre acteurs et cas d'utilisation sont des relations qui signifient simplement « participe à ».

La relation « extends » indique que tout les cas d'utilisation fils sont des cas particuliers du cas utilisation père. Ils héritent de ces caractéristiques, c'est-à-dire qu'ils ont les mêmes liens avec les acteurs.

2.3. Diagrammes de séquence

Un diagramme de séquence est une série d'évènements ordonnés dans le temps, simulant une exécution particulière du système. Le temps y est représenté explicitement par une dimension verticale et s'écoule de haut en bas.

Dans un diagramme de séquence, les objets sont associés à **une ligne de vie**. Une ligne de vie est une représentation de l'existence d'un élément participant dans un diagramme de séquence.

L'élément de communication entre les objets est le **message**. Un message déclenche une activité dans l'objet destinataire. La réception d'un message provoque un événement dans l'objet récepteur. Leur ordre est donné par leurs positions sur la ligne de vie. Le concept de message unifie toutes les formes de communication entre objets (appel de procédure, événement discret, signal entre flots d'exécution ou interruption matérielle).

2.3.1 Représentation graphique

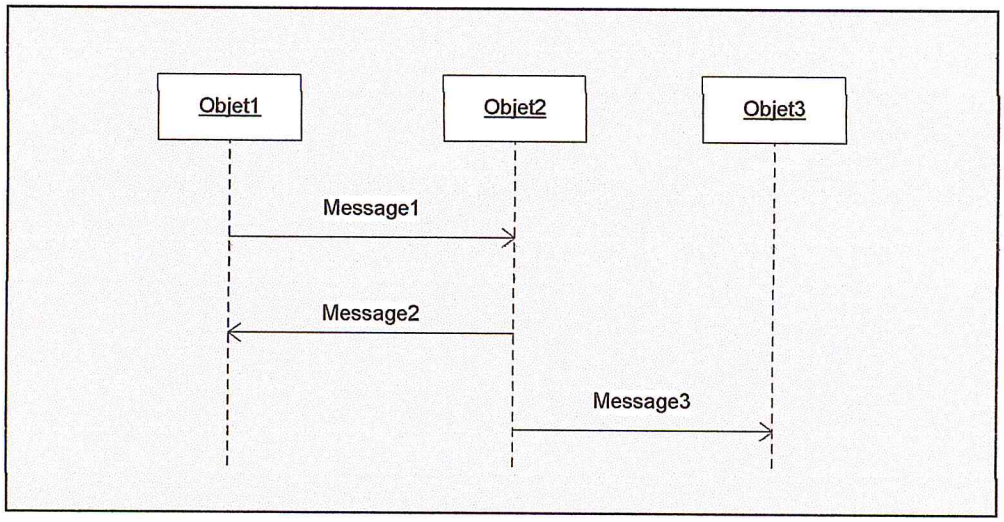


Figure 2: Représentation d'un diagramme de séquence

2.4 Diagrammes de classe

Le diagramme de classe représente les objets qui interviennent dans la résolution du problème ainsi que leurs associations.

Un digramme de classe est composé principalement de classes, d'associations entre classes et des classes d'association.

- **Classe :** c'est une description d'un ensemble d'objets qui partage les mêmes attributs, opérations, méthodes, relations et contraintes. Une instance d'une classe est appelée objet.
- **Association :** c'est une relation structurelle bidirectionnelle qui décrit un ensemble de liens entre différents éléments
- **Classe association :** Une association peut être représentée par une classe appelée classe associative ou classe association. Utile par exemple, lorsque l'association a des attributs ou bien qu'on souhaite lui attacher des opérations. La classe association contient des attributs sans participer à des relations avec d'autres classes.

2.4.1 Représentation graphique

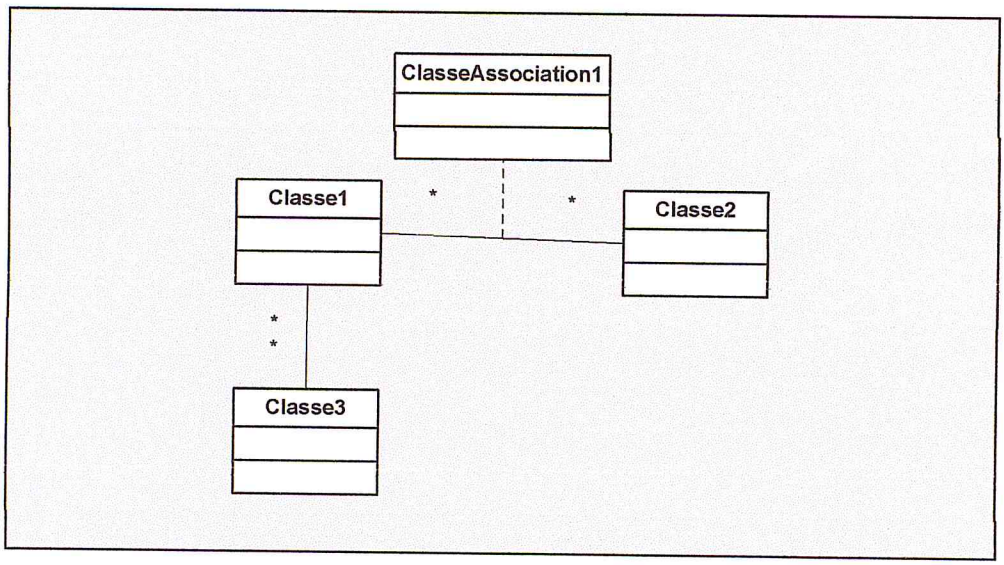


Figure 3: Représentation d'un diagramme de classe

2.5 Diagramme d'état

Un diagramme d'état est propre à une classe donnée, il décrit les états des objets de cette classe, les évènements auxquels ils réagissent et les transitions qu'ils effectuent.

Ces diagrammes sont des automates d'états finis, composés de transitions, d'événement et d'activités. Ils représentent la vue dynamique d'un système. Le comportement est modélisé dans un graphe dont les nœuds sont les états possibles des objets de la classe et les arcs sont les transitions d'état à état. Une transition représente le passage instantané d'un état vers un autre et elle est déclenchée par un événement.

2.5.1 Représentation graphique

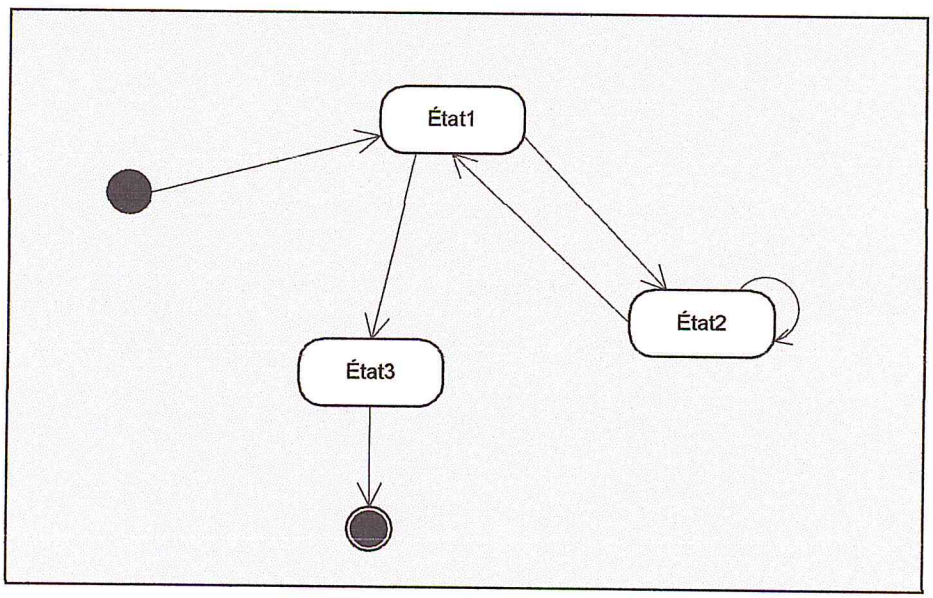


Figure 4: Représentation d'un diagramme d'état transition