UNIVERSITE SIDI MOHAMED BEN ABDELLAH
FACULTE DES SCIENCES ET TECHNIQUES FES
DEPARTEMENT D'INFORMATIQUE

Projet de Fin d'Etudes

Licence Sciences et Techniques Génie Informatique

Modules de signature Des Documents Electroniques

Lieu de stage : Centre National de Recherche et de Développement - BCP

Réalisé par :

Ouajjani Ali

Kharbane Yahya

Encadré par :

Pr. Karbout Abderrahim

Pr. R. Benabbou

Pr. L. Lamrini

Soutenu le 16/06/2012 devant le jury composé de :

Pr. A. Benabbou

Pr. A. Zarghili

Pr. R. Benabbou

Remerciement

Avant toute chose, je tiens à remercier Allah pour cette grâce d'être en vie et en bonne santé, et pour avoir terminé ce travail dans les meilleures conditions et ce malgré toutes les contraintes et les obstacles que j'ai pus rencontrer.

Je remercie mes parents qui m'ont toujours soutenu dans le meilleur comme dans le pire, et qui n'ont jamais hésité à sacrifier le tout pour mon propre confort, et je prie Dieu pour qu'il les récompense pour toutes ces années qu'ils m'ont consacré.

Mes remerciements s'adressent particulièrement à mon encadrant Mr. Karbout Abderrahim pour son aide et sa disponibilité tout au long du stage.

Je tiens également à exprimer toute ma reconnaissance à Mr Yassine Ellahet et Mr Othman Maimouni et tous les membres du personnel du CNRD pour m'avoir considéré comme l'un des leurs, et aussi pour avoir partagé leur précieuse connaissance et expérience avec moi. Leur confiance, encouragement, et soutien technique ont fait de cette période de stage une expérience qui a été certes très enrichissante.

Enfin, je remercie toute personne qui m'a encouragé, et aidé de près ou de loin dans ce projet.

Sommaire

Listes des Figures

Liste des Abréviations

Abréviation	Désignation
GBP	Groupe Banque Populaire
BCP	Banque Centrale Populaire
POSI	Pole Organisation & Système d'Informations
PME	Petites et Moyennes Entreprises
CPM	Crédit Populaire du Maroc
BPR	Banque Populaire Régionale
Green IT	Green Information Technology
AC	Autorité de Certification
PC	Politique de Certificats
JEE	Java Entreprise Edition
JSE	Java Standard Edition
JSP	Java Server Page
XML	Extensible Markup Language
HTTP	HyperText Transfer Protocol
HTML	HyperText Markup Language
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
MD5	Message Digest 5
RIPEMD	Race Integrity Primitives Evaluation Message Digest
RSA	Rivest Shamir Adleman
PKI	Public Key Infrastructure
PGP	Pretty Good Privacy
API	Application Programming Interface

Introduction

The Green IT : une manière globale et cohérente de réduire les nuisances rencontrées dans le domaine des équipements informatiques et ce, « du berceau jusqu'à la tombe » de chaque équipement : soit aux différents stades de fabrication, d'utilisation (consommation d'énergie) et de fin de vie (gestion/récupération des déchets, pollution, épuisement des ressources non renouvelables), et l'un de ses aspects Majeurs du Green Computing est : *La Dématérialisation*.

La dématérialisation des données existe depuis un certain temps déjà, beaucoup d'entreprises ou d'organismes, beaucoup de particuliers aussi travaillent sur des documents électroniques, les échangent, les stockent. Mais lorsqu'il s'agit de documents contractuels (contrats, factures, avenants..) ou sensibles, ces données sont imprimées pour être envoyées par courrier papier signé.

L'objet de la dématérialisation est de transformer ou conserver sous format électronique les données échangées dans le cadre d'activités professionnelles ou privées, dans les conditions légales qui permettent de conserver les mêmes garanties qu'un échange ou stockage papier. Son développement est résolument engagé : la dématérialisation apporte des avantages indéniables en terme de réduction de déchets, de coûts administratifs, de gains de temps, ainsi que dans l'amélioration des processus métier.

De grands projets de dématérialisation des échanges sont en chantier. Ceux-ci concernent notamment l'administration électronique (gestion des documents et démarches administratives par le moyen des échanges électroniques signés) le commerce et la banque en ligne, et c'est dans ce cadre que le groupe Banque Populaire a opté pour s'investir dans ce grand chantier.

Ce qui nous ramène a la nécessité d'implémentation d'une solution pour signer ces documents électroniques et garantir l'authenticité et la valeur juridiques de ces derniers.

Ce rapport va présenter dans un premier temps la société d'accueil, Ensuite, la deuxième partie sera consacrée pour l'étude théorique du concept de la signature numérique ainsi que du domaine de la cryptographie. Finalement, nous allons réaliser un module de signature de documents électroniques et un autre pour vérifier les documents signés.

CHAPITRE I : PRESENTATION DE L'ORGANISME D'ACCEUIL ET DE SA DEMARCHE DE GESTION DES PROJETS INFORMATIQUES

I. INTRODUCTION

Dans ce chapitre nous allons présenter l'organisme d'accueil et sa méthode de gestion des projets informatiques. Nous commençons tout d'abord par une présentation générale de l'organisme d'accueil, le Groupe Banque Populaire (GBP), puis de son organisme central, la Banque Centrale Populaire (BCP), le Pôle Organisation & Système d'Information (POSI) pour finir par une synthèse de la démarche de gestion des projets informatiques au sein de la BCP en vue de l'analyser dans la deuxième partie.

II. SECTION I : PRESENTATION DE L'ORGANISME D'ACCUEIL

BANQUE POPULAIRE

Figure 1 : LOGO de la Banque Populaire

Cette section est consacrée à la présentation du lieu de la recherche, il s'agit dans un premier lieu de décrire le Groupe Banque Populaire et la Banque Centrale Populaire en tant qu'entité centrale du groupe, et en deuxième lieu le pôle Organisation et Système d'Information.

II.1. Groupe Banque Populaire

II.1.1. Vision

Le Crédit Populaire du Maroc est un groupement de banques constitué par la Banque Centrale Populaire et les Banques Populaires Régionales.

Fidèle à son esprit d'entreprise, le Crédit Populaire du Maroc s'est fixé comme objectif d'accompagner toutes les entreprises, moyennes ou petites, artisanales, industrielles ou de services par la distribution de crédit à court, moyen et long terme.

Il propose une gamme élargie et complète de services et produits financiers répondant à l'ensemble des besoins de sa clientèle. Il développe également ses activités à travers quatre orientations stratégiques majeures :

II.1.1.1. La consolidation des positions acquises

Cet axe concerne le développement des activités d'intermédiation et de marché du groupe. Le GBP accélère le développement de ses activités de banque de détail par une stratégie volontariste d'extension de ses points de vente, de la collecte de ressources et de la distribution des crédits.

Disposant du plus large réseau de secteur bancaire, le groupe ouvre une centaine d'agences chaque année.

Grâce à ce dispositif, la collecte des ressources progresse. Les crédits enregistrent également un développement soutenu en matière des crédits aux entreprises, avec les offres Banque Populaire Entreprises, consistant en une nouvelle approche Banque Populaire dans ses relations avec les entreprises.

Les crédits immobiliers et les crédits à la consommation enregistrent également un trend haussier, et le groupe a l'ambition d'augmenter sensiblement ses parts de marché dans ces catégories de crédits.

II.1.1.2. La Banque citoyenne

Banque de proximité, le Groupe Banque Populaire joue un rôle de premier plan dans le développement des régions à travers l'action des Banques Populaires Régionales. Il est l'accompagnateur financier de la région à travers la mobilisation de l'épargne, son utilisation au niveau local, au bénéfice des acteurs économiques et sociaux.

Dans le plan de développement du Groupe, l'implication reste effective et très prononcée en matière de bancarisation de la population, qui reste encore à un niveau très faible au Maroc. Ceci est possible grâce à la politique de proximité du groupe et la souplesse dans les ouvertures de compte ainsi qu'à son large réseau de distribution. La cadence observée actuellement dans les ouvertures de comptes auprès de la clientèle de masse en atteste largement.

Le Groupe Banque Populaire est le 1er réseau bancaire du pays. Son réseau est constitué à fin décembre 2010 de 948 agences et plus de 1068 guichets automatiques.

Le soutien aux activités à fortes retombées sociales est également encouragé par le biais de développement des microcrédits dont l'encours ne cesse d'augmenter et qui enregistre une évolution annuelle moyenne de plus de 50%, grâce à l'ouverture de nouvelles branches au niveau de toutes les régions du pays.

L'appui de la Fondation Création d'Entreprises tend à encourager les porteurs de projets en les assistants dans toutes les phases pour l'aboutissement de la création de leurs entreprises.

Le GBP encourage également l'habitat social en prévoyant d'augmenter annuellement de 25% ses encours en la matière.

Enfin, les PME-PMI sont accompagnées dans l'action de leur mise à niveau.

II.1.1.3. L'amélioration des performances

L'important développement du Groupe Banque Populaire contribue à l'amélioration de ses indicateurs de performances : rentabilité, productivité, commissions et maîtrise des risques.

Ainsi, la rentabilité financière est fortement appréciée, fruit des résultats nets de l'ensemble des entités du groupe, ainsi que la nette progression du produit net bancaire, et la maîtrise des charges d'exploitation. La productivité quant à elle, connaît une amélioration surtout grâce à l'automatisation plus poussée des opérations effectuées au niveau des agences.

La part des commissions dans le produit net bancaire enregistre une évolution moyenne annuelle de l'ordre de 10%.

Concernant la maîtrise des risques, le groupe tend à maintenir sa tendance d'afficher les meilleurs ratios prudentiels du secteur que ce soit celui de la solvabilité, de la liquidité, de la division des risques ou des créances en souffrance.

II.1.1.4. La conquête de nouveaux territoires et la croissance externe

Un nouvel élan est pris par le GBP dans son intervention dans les opérations de la corporate Banking, pour conforter son positionnement stratégique dans ce créneau, et plus spécifiquement dans les métiers de conseil aux entreprises et de l'ingénierie financière, d'émissions obligataires, du capital-risque, de la gestion collective de l'épargne, de l'intermédiation boursière et de financement du commerce international.

Les activités du groupe s'étendent également à la bancassurance.

Du reste, les filiales spécialisées du groupe ne restent pas à l'écart de cette nouvelle dynamique commerciale, et un plan de développement ambitieux est prévu pour chacune d'entre elles en vue de participer fortement à l'amélioration des performances du groupe, ce qui deviendra possible par l'amélioration de leurs parts de marché dans leurs domaines d'activité respectifs.

II.1.2. Valeurs

Les valeurs identitaires du Crédit Populaire du Maroc découlent des principes de la coopération et de la mutualité.

Cet esprit coopératif et mutualiste qui anime les Banques Populaires Régionales puise ses origines dans les valeurs et **les traditions culturelles** du Maroc, basées **sur la solidarité, l'entraide et l'intérêt commun.**

Les valeurs identitaires de l'institution constituent les fondements de l'action du groupe et confirment **sa mission nationale** au service du développement économique et social du pays.

Il tire également sa force de **sa spécificité coopérative**, qui confère au sociétaire l'originalité d'être à la fois un client et un copropriétaire de la banque.

Cette communauté de sociétaires constitue l'essence du groupe et participe activement à la vie de la banque, à travers notamment les Conseils de Surveillance des Banques Populaires Régionales, dont les membres sont élus par l'Assemblée Générale des sociétaires.

Destiné à promouvoir l'économie sociale, par le biais de la **coopérative financière** et l'encouragement à **la solidarité interprofessionnelle**, le Crédit Populaire du Maroc a été tout naturellement amené à jouer **un rôle moteur** dans **l'amélioration du taux de bancarisation du pays** et dans la **collecte de l'épargne**. Il constitue un groupement de banques de proximité, accessibles à tous et fortement enracinées dans toutes les régions du Royaume.

II.1.3. Histoire

Introduit au Maroc par le Dahir du 25 mai 1926, le modèle organisationnel et commercial du groupe est fondé, dès l'origine, sur les concepts de mutualité et de coopération.

Ainsi, les premières Banques Populaires de type coopératif et à vocation régionale, furent créées, dès la fin des années 20 du siècle dernier, dans les principales villes du Royaume.

Au lendemain de l'indépendance, les pouvoirs publics ont procédé, dans le cadre de la mise en place des premiers jalons du système bancaire et financier Marocain, à la refonte du Crédit Populaire du Maroc (CPM), à travers le Dahir du 28 février 1961, en le dédiant au développement de l'artisanat et de la PME/ PMI.

Pour améliorer les traitements et sécuriser les opérations, la banque s'est dotée depuis 1972 de son premier système informatique.

A partir de 2000, le CPM a connu une réforme qui a renforcé le modèle organisationnel du CPM, basé désormais sur l'existence de Banques Populaires

Régionales (BPR), d'une entité centrale : la Banque Centrale Populaire, et d'une instance fédératrice : le Comité Directeur du CPM.

Cette réforme a ainsi valorisé la dimension régionale des BPR et élargi les prérogatives du Comité Directeur.

L'année 2004 a été marquée par l'introduction en Bourse de la Banque Centrale Populaire.

II.1.4. Organismes du GBP

L'organisation institutionnelle du GBP fait apparaître une structure pyramidale à trois niveaux :

- La Banque Centrale Populaire (BCP) ;
- Les Banques Populaires Régionales (BPR) ;
- Les filiales et les fondations.

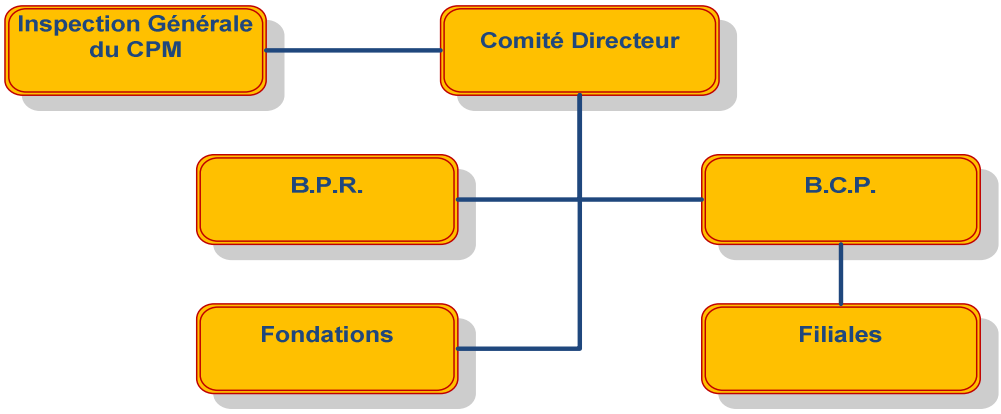


Figure 2 : Organismes du CPM

II.1.4.1. Comité Directeur

Le Comité Directeur est l'instance suprême du Crédit Populaire du Maroc exerçant exclusivement la tutelle sur les différents organismes du CPM.

Le Comité Directeur comprend :

- Cinq Présidents des Conseils de Surveillance des Banques Populaires Régionales élus par leurs pairs ;

- Cinq représentants du Conseil d'Administration de la Banque Centrale Populaire, nommés par ledit Conseil.

Le Président du Comité Directeur est élu parmi les membres dudit Comité et sa nomination est ratifiée par le Ministre chargé des Finances.

Le Comité Directeur :

- Définit les orientations stratégiques du groupe ;
- Exerce un contrôle administratif, technique et financier sur l'organisation et la gestion des organismes du CPM ;
- Définit et contrôle les règles de fonctionnement communes au groupe ;
- Prend toutes les mesures nécessaires au bon fonctionnement des organismes du CPM et à la sauvegarde de leur équilibre financier.

II.1.4.2. La Banque Centrale Populaire

La Banque Centrale Populaire est un établissement de CPM. Elle joue un rôle central au sein du groupe, et elle a pour missions principales de :

- Gérer les excédents de trésorerie des BPR;
- Compenser les créances et les dettes réciproques des organismes du CPM;
- Centraliser les déclarations vis à vis de Bank Al Maghreb, des administrations et des organismes professionnels ;
- Centraliser les souscriptions des valeurs mobilières pour le compte du CPM;
- Gérer les services d'intérêt communs au profit des BPR (informatique, ressources humaines …etc.).

Aujourd'hui, au regard de la loi 12/96 portant la réforme du Crédit Populaire du Maroc, la BCP reste l'organe central du GBP, tout en ayant la possibilité de développer son propre fonds de commerce, en tant que banque universelle.

II.1.4.3. Les Banques Populaires Régionales

Les Banques Populaires Régionales (BPR), Banques de proximité, actuellement au nombre de 10 constituent le socle du Crédit Populaire du Maroc.

Ce sont des établissements de crédit habilités à effectuer toutes les opérations de banque dans leurs circonscriptions territoriales respectives, les BPR ont pour

mission de contribuer au développement de leur région par la diversité des produits qu'elles offrent, le financement de l'investissement et la bancarisation de l'économie.

Elles constituent le levier du Crédit Populaire du Maroc dans la collecte de l'épargne au niveau régional, sa mobilisation et son utilisation dans la région où elle est collectée.

Les Banques Populaires sont organisées sous la forme des coopératives à capital variable, à Directoire et à Conseil de Surveillance.

Leur mode d'organisation unique au sein du système bancaire leur permet d'approcher différemment leurs clients, puisque ces derniers se trouvent également être les détenteurs du capital, formant ainsi ce que l'on appelle « le sociétariat ».

Outre le fait qu'ils bénéficient des différents services bancaires, les clients sociétaires participent également à la vie sociale de leur banque (Participation aux Assemblées Générales, possibilité de siéger au Conseil de Surveillance).

II.1.4.4. Les Filiales et Fondations

Il s'agit principalement des entités suivantes:

- MEDIAFINANCE : filiale bancaire ;
- CIB OFFSHORE : filiale bancaire ;
- BANQUE MAROCO-GUINEENNE : filiale bancaire ;
- BANQUE MAROCO-CENTREAFRICAINE : filiale bancaire ;
- BANQUE CHAABI DU MAROC : filiale bancaire ;
- CHAABI LEASING : société de financement ;
- ASSALAF CHAABI : société de financement ;
- UPLINE : Gestion d'actif et bourse ;
- ALISTITMAR CHAABI : Gestion d'actif et bourse ;
- AL WASSIT : Gestion d'actif et bourse ;
- CHAABI MOUSAHAMA : capital risque ;
- MAROC ASSISTANCE INTERNATIONALE : assurance ;
- CHAABI COURTAGE : assurance ;
- CHAABI DOC NET : société de service ;
- CHAABI LLD : société de service ;
- ESSOUKNA : société de service ;

- FONDATION MICRO-CREDIT ;
- FONDATION CREATION D'ENTREPRISES ;
- FONDATION EDUCATION ET CULTURE.

II.2. Banque Centrale Populaire

Cotée en bourse depuis le 8 juillet 2004, la Banque Centrale Populaire (BCP) est un établissement de crédit, sous forme de société anonyme à Conseil d'Administration.

II.2.1. Mission

La BCP, qui assure un rôle central au sein du groupe, est investie de deux missions principales :

- Etablissement de crédit habilité à réaliser toutes les opérations bancaires, sans toutefois disposer d'un réseau propre .
- Organisme central bancaire des BPR.

A ce titre, elle coordonne la politique financière du Groupe, assure le refinancement des BPR et la gestion des services d'intérêt commun pour le compte de ses organismes comme par exemple les services informatiques.

II.2.2. Organigramme

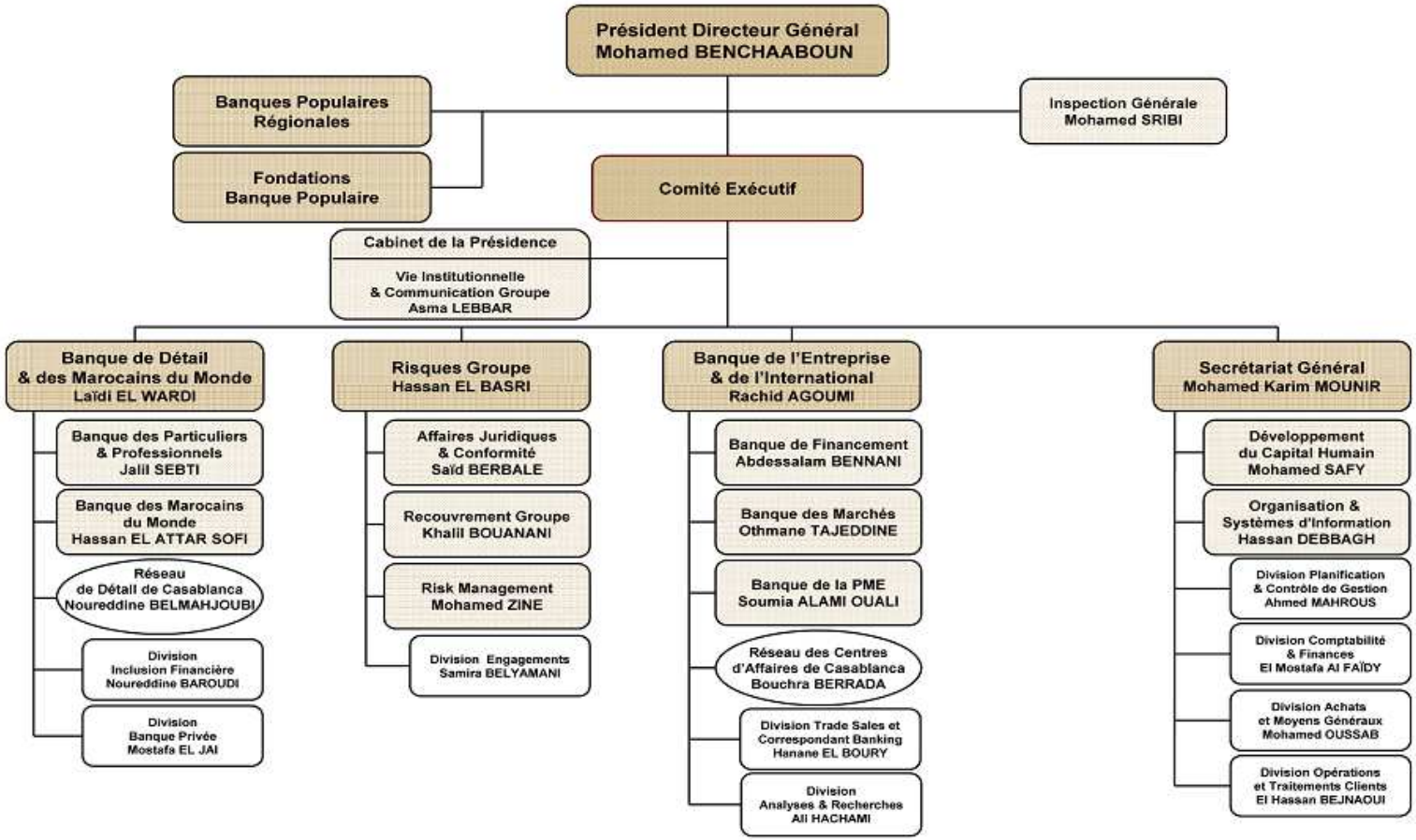


Figure 3 : Organigramme de la BCP

II.3. Pôle Organisation et Système d'Information

II.3.1. Mission générale

Le Pôle Organisation et Systèmes d'Information est rattaché à Direction Générale Secrétariat Générale.

Sa mission principale est :

- Elaboration et mise en œuvre du système d'information de l'institution et des systèmes informatiques, de télécommunications dont ils se composent, tels qu'ils sont approuvés par le Comité de Pilotage informatique ;
- La sauvegarde et la gestion du patrimoine tangible (matériel, logiciel et outils informatiques) et intangible (données, bases d'information et de connaissance, méthodes et documentation) de l'institution.

II.3.2. Domaines de responsabilité

Les responsabilités du Pôle d'Organisation et Systèmes d'Information s'étendent sur plusieurs domaines à savoir :

- La proposition de la stratégie de l'institution en matière d'informatique et de télécommunications et de la planification qui en découle ;
- La mise en œuvre des équipements et de l'infrastructure ;
- L'acquisition et/ou le développement des solutions informatiques répondant aux besoins de l'institution ainsi que leur mise en œuvre ;
- Assistance des fonctions métiers dans toutes les phases des projets ;
- L'exploitation et le support des applications informatiques ;
- La participation à la définition de la stratégie monétique, et sa mise en œuvre, avec la prise en charge également de toute la partie " back-office " monétique ;
- L'approvisionnement du Groupe des Banques Populaires en produits et consommables informatiques et para-informatiques.

II.3.3. Attributions par domaine

DOMAINE 1: STRATEGIE INFORMATIQUE

- Etablir la vision informatique à moyen terme pour l'institution en assurant la veille technologique et en analysant le comportement du système d'information.
- Définir l'approche et les moyens nécessaires à l'acquisition et à la mise en œuvre du système d'information répondant de manière optimale aux besoins fonctionnels de l'institution ;
- Définir les normes et les standards en matière d'équipement et d'infrastructure, d'assurance qualité, de sécurité et d'exploitation et en assurer l'application systématique ;
- Garantir l'application rigoureuse de la structure logique des données, des règles de gestion et des composants logiciels de l'institution pour en préserver la valeur informationnelle ;
- Administrer et optimiser le patrimoine de l'Institution et pourvoir à son évolution et son remplacement.

DOMAINE 2: Programmation et planification

- Planifier et ordonnancer les projets de réalisation et de mise en œuvre des solutions ;
- Optimiser l'utilisation et l'affectation des ressources par projet en accord avec les priorités retenues ;
- Maîtriser la qualité, les coûts et les délais des projets de réalisation et de mise en œuvre des solutions ;
- Promouvoir une approche qualité totale ;
- Gérer les budgets et les investissements de manière optimale ;
- Gérer les emplois et les compétences et assurer leur développement par un encadrement de proximité et une formation continue.

DOMAINE 3 : Mise en œuvre des équipements et de l'infrastructure

- Gérer le patrimoine tangible et les moyens d'exploitation informatique et de télécommunications ;

- Déployer les nouvelles solutions informatiques et optimiser les solutions existantes.

DOMAINE 4 : Acquisitions et développement des solutions

- Etudier et documenter les meilleures solutions aux besoins exprimés par les utilisateurs en prenant en compte les spécificités du SI du groupe ;
- Réaliser ou acquérir, intégrer, puis livrer, après recette de l'utilisateur, les solutions informatiques ou les modifications au système d'information ;
- Réaliser les modifications nécessaires aux applications existantes en termes d'adaptations réglementaires ou fonctionnelles, performance, qualité, sécurité et facilité d'utilisation.

DOMAINE 5 : Monétique

- Participer à la définition d'une stratégie monétique, en accord avec les orientations stratégiques de la banque ;
- Mettre en œuvre cette stratégie ;
- Prendre en charge toute la partie " back-office " monétique.

DOMAINE 6 : Exploitation Informatique

- Assurer les services applicatifs de la banque, en termes de moyens matériels et de ressources humaines, en garantissant une qualité de service en accord avec les utilisateurs, conformément aux contrats de service.

DOMAINE 7 : Approvisionnement du GBP

- Approvisionner le Groupe des Banques Populaires en matériel et consommables informatiques et para-informatiques ;
- Administrer et optimiser le patrimoine de l'institution et pourvoir à son évolution et son remplacement ;
- Gérer les budgets et les investissements de manière optimale.

II.3.1. l'organigramme du pôle Organisation & Systèmes d'Informations

POSI selon la dernière version du Mars 2011 :

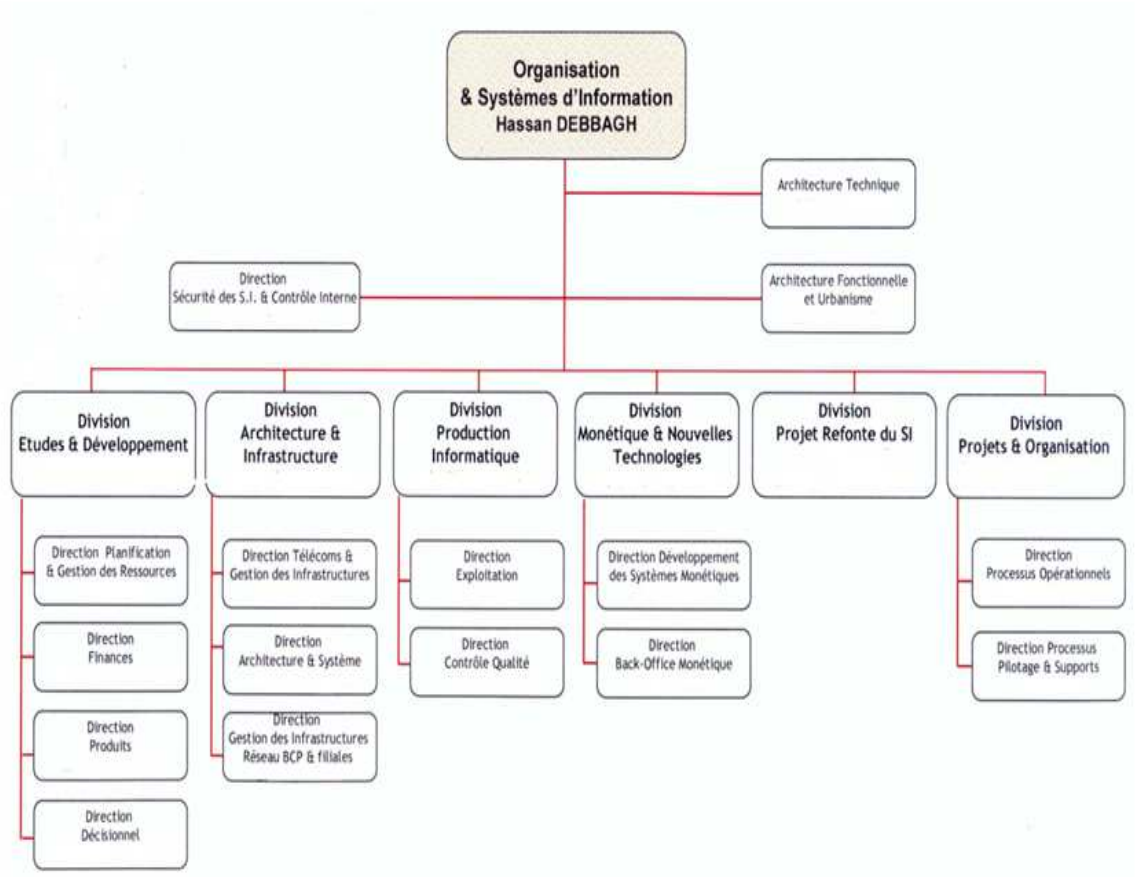


Figure 4 : Organigramme du pôle POSI

Le Pôle Organisation et Systèmes D'Information comporte les entités suivantes:

- Division Etude et Développement ;
- Division Architecture et Infrastructure ;
- Division Production Informatique ;
- Division Monétique & Nouvelles Technologies;
- Division Projet Refonte du SI ;
- Division Projets & Organisation ;
- Direction Sécurité des SI et Contrôle Interne ;
- Architecture Technique ;

Cahier de Charge

- **Contexte du travail :**

Tout entreprise désirant développer un projet de dématérialisation afin de conserver sous formes électroniques les données échangées dans le cadre d'activités privées ou bien professionnels doit pouvoir assurer les mêmes garanties qu'un échange ou stockage papier et pour ce l'entreprise devra pouvoir signer et prouver l'identité du propriétaire ainsi que la date de création ou de modification.

- **Objectif :**

Développer un module d'une application Web qui permet d'implémenter la signature numérique sur des documents électroniques issus du processus de la dématérialisation.

- **Fonctions des modules développés :**

  - ***Module de signature de documents électroniques :***

L'application doit permettre de générer des pairs de clés et de signer les divers documents de la banque stockés sous formes électroniques.

  - ***Module de vérification de l'authenticité de documents électroniques signés :***

L'application doit pouvoir vérifier l'identité su signataire ainsi que l'intégrité du document.

CHAPITRE II : La Signature Electronique et La Sécurité des Documents

I. Introduction :

I.1. Définition :

La signature électronique (aussi appelée signature numérique) est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier. Un mécanisme de signature électronique doit présenter les propriétés suivantes :

- Il doit permettre au lecteur d'un document d'identifier la personne ou l'organisme qui a apposé sa signature.
- Il doit garantir que le document n'a pas été altéré entre l'instant où l'auteur l'a signé et le moment où le lecteur le consulte.

Pour cela, les conditions suivantes doivent être réunies :

- Authentique : L'identité du signataire doit pouvoir être retrouvée de manière certaine.
- Infalsifiable : La signature ne peut pas être falsifiée. Quelqu'un ne peut se faire passer pour un autre.
- Non réutilisable: La signature n'est pas réutilisable. Elle fait partie du document signé et ne peut être déplacée sur un autre document.
- Inaltérable : Un document signé est inaltérable. Une fois qu'il est signé, on ne peut plus le modifier.
- Irrévocable : La personne qui a signé ne peut le nier.

La signature électronique n'est devenue possible qu'avec la cryptographie asymétrique.

Elle se différencie de la signature écrite par le fait qu'elle n'est pas visuelle, mais correspond à une suite de nombres.

I.2. Pourquoi la signature électronique :

L'acte d'apposer sa signature sur un document ou une œuvre est un geste que l'humanité fait depuis des siècles à l'aide de différentes méthodes. Au 21e siècle, la conduite des affaires se fait de plus en plus sur support électronique. En conséquence, l'apposition de votre signature ne se fait plus avec un stylo ou un traditionnel sceau encreur, mais plutôt à l'aide de technologies liant de manière irréfutable votre identité à vos documents électroniques en plus d'en protéger leur intégrité. La signature électronique aide à conférer le même degré d'authenticité à vos documents électroniques que conférait jadis votre signature manuscrite à vos documents papier.

Aujourd'hui, il est pratiquement impensable d'exercer sa profession sans avoir recours aux technologies de l'information (p. ex. : traitement de texte, chiffrier, dessins assistés par ordinateur, etc.). Le défi devient donc de conférer aux documents électroniques une valeur légale équivalente aux documents papier tout en étant conformes aux exigences qui assurent qualité, intégrité et sécurité.

La signature en lot de plans, de devis et de documents d'usage courant est une solution extrêmement intéressante pour tous ceux qui ont à signer et à expédier par courrier un volume important de documents, ca permet en outre de :

- certifier les documents et les e-mails.
- garantir la confidentialité des écrits.
- garantir la provenance et l'intégrité des écrits.
- garantir l'auteur des écrits.
- garantir la non-répudiation : le signataire ne peut pas nier être l'auteur de la signature.

II. Valeur Légale :

II.1. l'Union Européenne:

Au niveau européen, la Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 portant sur un cadre communautaire pour les signatures électroniques, a établit le cadre juridique pour les signatures électroniques et certains services de certification. L'objectif est de faciliter l'utilisation des signatures électroniques et de contribuer à leur reconnaissance juridique au sein des États membres.

La directive définit de nouvelles notions:

- **la signature électronique**, une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification.
- **la signature électronique avancée**, signature électronique qui satisfait aux exigences suivantes:
    1. être liée uniquement au signataire;
    2. permettre d'identifier le signataire;
    3. être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;
    4. être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.
- **le certificat qualifié,** certificat qui doit notamment comporter:
    1. une mention indiquant que le certificat est délivré à titre de certificat qualifié;
    2. l'identification du prestataire de service de certification;
    3. le nom du signataire;
    4. la possibilité d'inclure une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné;
    5. des données afférentes à la vérification de la signature qui correspondent aux données pour la création de signature sous le contrôle du signataire;
    6. l'indication du début et de la fin de la période de validité du certificat;
    7. le code d'identité du certificat;
    8. la signature électronique avancée du prestataire de service de certification qui délivre le certificat.

II.2. En France:

Depuis 2000, la signature électronique d'un document a en France la même valeur légale qu'une signature manuscrite, conformément aux textes suivants :

- La loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique;
- Son décret d'application n° 2001-272 du 30 mars 2001.

Selon ce décret, un dispositif sécurisé de création de signature électronique doit être certifié conforme aux exigences définies plus haut :

1. Soit par le Premier ministre, dans les conditions prévues par le décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. La délivrance du certificat de conformité est rendue publique.
2. Soit par un organisme désigné à cet effet par un État membre de l'Union européenne.

La transposition complète de la Directive européenne 1999/93/CE a toutefois nécessité un processus plus long[1].

Depuis 2010, d'autre part, le concept de signature numérique, définie comme la conservation sous forme numérique d'une signature manuscrite produite via un écran tactile, a été introduite dans le droit français par l'article R 249-11 du code de procédure pénale.

II.3. Au Maroc:

L'internet est aujourd'hui un outil indispensable au quotidien. Des mails jusqu'au e-commerce (le payement par internet est possible au Maroc depuis le 2 octobre 2007), en passant par les e-déclarations, plus rien n'échappe à l'emprise du net.

Plusieurs pays se sont déjà dotés de moyens juridiques permettant de faire face aux difficultés pouvant être soulevées par l'utilisation des TIC.

C'est pour ça que la loi sur l'échange électronique des données juridiques, n° 53-05, a été promulgué par Dahir du 30 novembre 2007, Bulletin Officiel n° 5584.

En voilà les principaux articles :

- L'article premier de la loi confirme son caractère restrictif, puisqu'il affirme que celle-ci s'applique " aux données juridiques échangées par voie électronique et à l'équivalence des documents établis sur support papier et sur support électronique et à la signature électronique, Cet article dit aussi déterminer le cadre juridique applicable aux opérations effectuées par les prestataires de services de certification électronique, ainsi que les règles à respecter par ces derniers et les titulaires des certificats électroniques délivrés.
- L'article 417-1 confère la même force probante à l'écrit électronique que l'écrit sous forme papier, à condition qu'il permette à la personne dont il émane d'être dûment identifiée et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

- L’article 417-2 donné également à la signature électronique la même valeur que celle conférée à la signature sur papier, lorsqu’un procédé fiable d’identification garantit le lien entre la signature et l’acte concerné. La signature électronique peut être apposée devant un officier public habilité à certifier afin de conférer l’authenticité à l’acte.
- L’article 417-3 pose une présomption de fiabilité du procédé de signature électronique lorsque celui-ci est sécurisé. Il s’agit d’une présomption simple. lorsque cet acte est horodaté, il a la même force qu’un acte légalisé ayant date certaine.
- Le dispositif de création de la signature électronique est prévu à l’article 8 de la loi et consiste en ” un matériel et/ou logiciel destiné à mettre en application les données de création de signature électronique, comportant les éléments distinctifs caractérisant le signataire, tels que la clé cryptographique privée “.
- Les conditions qui doivent être satisfaites pour sa validité sont prévues à l’article 6 de la loi et sont les suivantes :

    - être propre au signataire.
    - être créé par des moyens que le signataire puisse garder sous son contrôle exclusif.
    - garantir avec l’acte auquel elle s’attache un lien tel que toute modification ultérieure dudit acte soit détectable.
    - être produite par un dispositif de création de signature électronique, attesté par un certificat de conformité.
    - le certificat électronique sécurisé doit mentionner les données de vérification de la signature électronique sécurisée.

III. Principe de Fonctionnement :

III.1. Définitions des notions :

III.1.1. Cryptographie asymétrique :

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder. Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu. Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message.

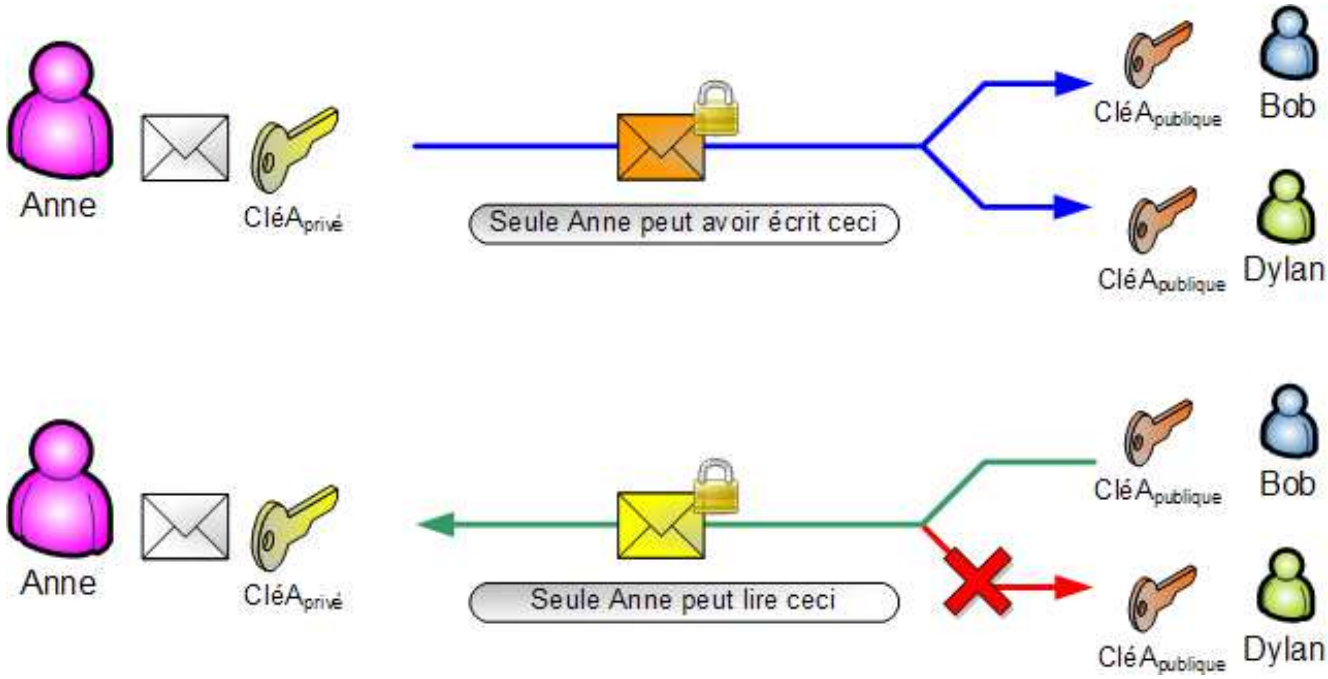


Figure 5 : Principe de la cryptographie asymétrique.

III.1.2. Fonction de hachage :

On nomme fonction de hachage une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une *empreinte* servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Les fonctions de hachage sont utilisées en informatique et en cryptographie.
Le résultat d'une fonction de hachage peut être appelé selon le contexte *somme de contrôle*, *empreinte*, *hash*, *résumé de message*, *condensé*, *condensat* ou

encore *empreinte cryptographique* lorsque l'on utilise une fonction de hachage cryptographique. Il ne faut toutefois pas confondre une fonction de hachage avec une signature numérique qui fournit, en plus du code de hachage, une information sur l'identité de l'émetteur du message.

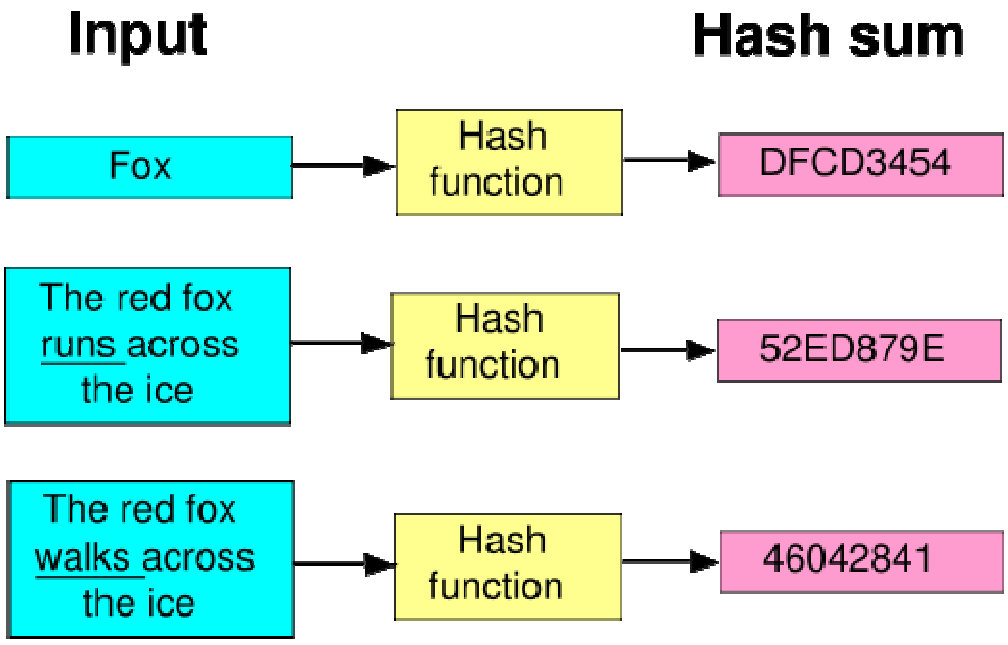


Figure 6 : Principe de la Fonction de Hachage.

- *Utilité :*

Les fonctions de hachage servent à rendre plus rapide l'identification des données : calculer l'empreinte d'une donnée ne doit coûter qu'un temps négligeable. Une fonction de hachage doit par ailleurs éviter autant que possible les *collisions* (états dans lesquels des données différentes ont une empreinte identique) : dans le cas des tables de hachage, ou de traitements automatisés, les collisions empêchent la différenciation des données ou, au mieux, ralentissent le processus. En cryptographie les contraintes sont plus exigeantes et la taille des empreintes est généralement bien plus longue que celle des données initiales ; un mot de passe dépasse rarement une longueur de 8 caractères, mais son empreinte peut atteindre une longueur de plus de 100 caractères. La priorité principale est de protéger l'empreinte contre une attaque par force brute, le temps de calcul de l'empreinte passant au second plan.

- *Choix d'une bonne fonction de hachage :*

Une bonne fonction de hachage est cruciale pour les performances. Les collisions étant en général résolues par des méthodes de recherche linéaire, une mauvaise fonction de hachage, i.e. produisant beaucoup de collisions, va fortement dégrader la rapidité de la recherche. D'autre part, il est préférable que la fonction de hachage ne soit pas de complexité élevée.
Le calcul du hachage se fait parfois en 2 temps :

1. Une fonction de hachage particulière à l'application est utilisée pour produire un nombre entier à partir de la donnée d'origine.
2. Ce nombre entier est converti en une position possible, en général en calculant le reste modulo la taille de la table de hachage.

III.1.3. Certificat Electronique :

Le certificat est la pièce d'identité électronique garantit par une autorité de certification qui permet de :

- vérifier l'identité de l'émetteur
- contrôler l'intégrité du contenu
- rendre non répudiable un échange ou la signature d'un document

En outre, il permet d'effectuer des échanges confidentiels, et il contient :

- au moins une clé publique ;
- des informations d'identification, par exemple : noms, localisation, emails ;
- au moins une signature ; de fait quand il n'y en a qu'une, l'entité signataire est une autorité dont elle-seule permet de prêter confiance (ou non) à l'exactitude des informations du certificat.

- *L'Autorité de Certification :*

La validité des éléments d'authentification contenus dans le certificat numérique est assurée par une autorité de certification (AC). Cette autorité de certification est chargée de délivrer les certificats numériques, de leur assigner une date de validité et de garantir l'identité de son propriétaire. Elle doit également mettre à disposition de l'organisme/ entité/ personne la possibilité de révoquer les certificats en cas de compromission ou de perte de la clé privée, ou en cas de modifications des données contenues dans le certificat.

Barid eSign

Tiers de confiance

En tant qu'Autorité de Certification (AC), Barid eSign délivre des certificats électroniques qui garantissent le lien entre l'identité d'une personne (ou d'un serveur) et une bi-clé de signature qui lui est associée.

Pour cela, tous les certificats numériques sont produits conformément à une politique de certification (PC) spécifique selon la classe du certificat, c'est à dire de son mode d'enregistrement et de sa délivrance. Plus la classe est haute et plus le mode de délivrance et la vérification des identités et des droits sont stricts :

Classe 1 : certificat logiciel P12.
Classe 2 : certificat sur support cryptographique.
Classe 3 : certificat sur support cryptographique évalué.

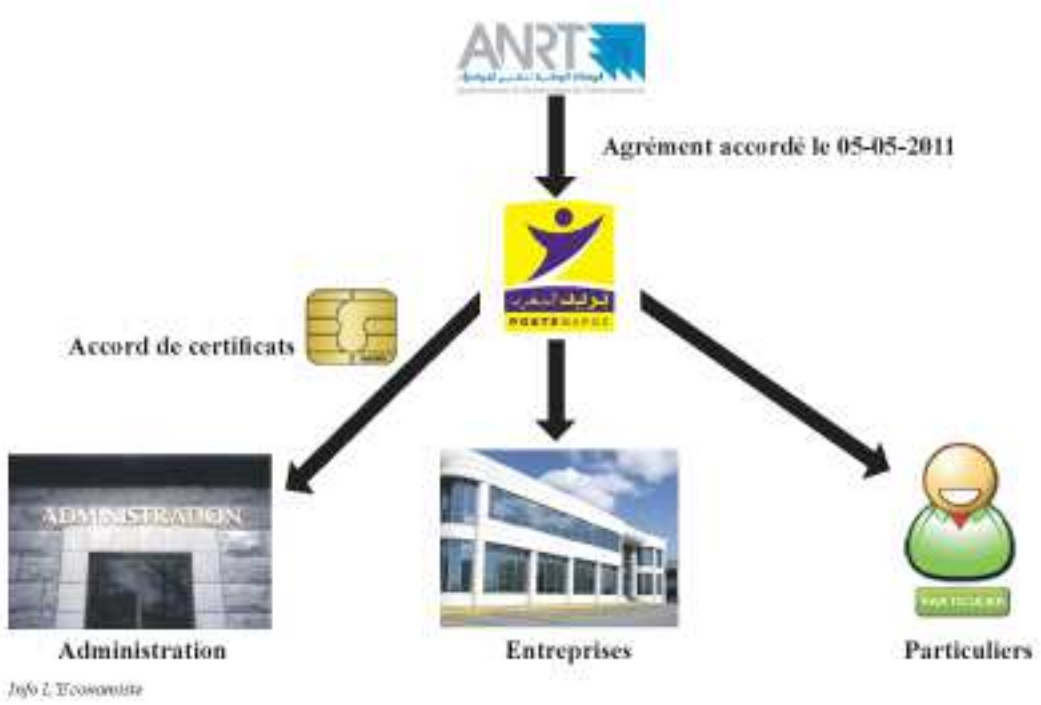


Figure 7 : Hiérarchie Tiers de confiance Barid eSign.

III.2. Pratique :

Supposons que l'on dispose d'un algorithme de chiffrement asymétrique . Notons $\mathbf{C_A}$, la fonction de chiffrement et $\mathbf{D_A}$ celle de déchiffrement. La fonction $\mathbf{C_A}$ est capable de chiffrer une information "claire". La fonction $\mathbf{D_A}$ ne peut que déchiffrer une information préalablement chiffrée par $\mathbf{C_A}$. $\mathbf{C_A}$ est "fournie" par la clé privée, et n'est donc connue que du propriétaire légitime. Quant à $\mathbf{D_A}$, elle est "fournie" par la clé publique, et ainsi possiblement connue par tous.

Lorsque la personne **« A »** souhaite signer un message M, il utilise la procédure suivante.

1. il utilise une fonction **H** de hachage (ou de condensat), Le résultat $\mathbf{H_A(M)}$ de cette opération, hash ou condensé, permet de s'assurer de l'intégrité du document, qu'il est bien entier et sans erreur.
2. Le condensé $\mathbf{H_A(M)}$ peut être généré par n'importe qui. Afin d'assurer que c'est bien **« A »** qui a rédigé le message **M**, ce condensé est chiffré par $\mathbf{C_A}$.
3. C'est ce condensé chiffré $\mathbf{C_A(H_A(M))}$ qui constitue la signature **S(M)** du message, aux côtés duquel elle est transmise.

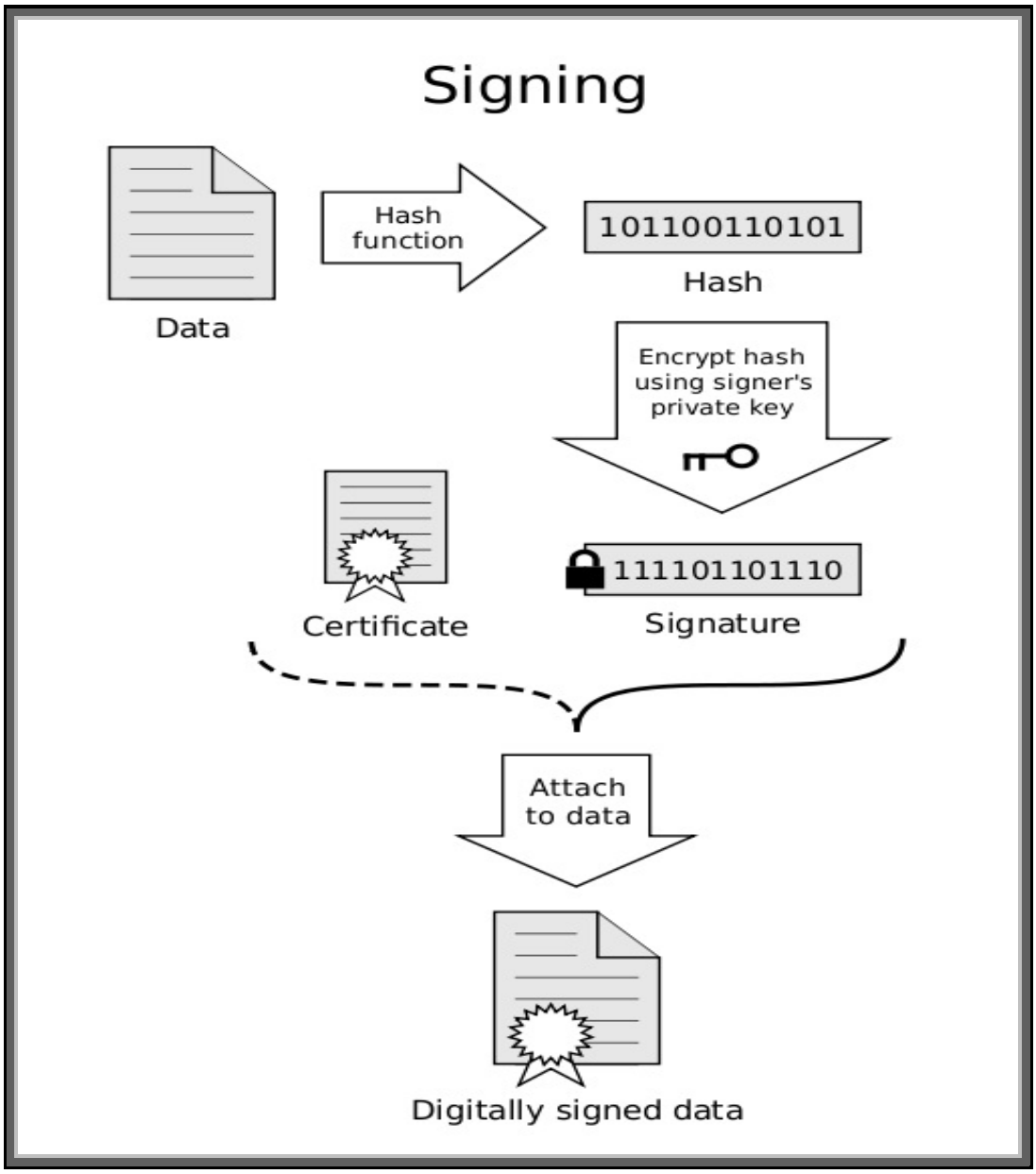


Figure 8 : Etape de signature d'un document électronique.

La personne **« B »**, qui connait la clé publique de **A**, reçoit le message **M** ainsi que la signature **S(M)** associée. Afin de vérifier son authenticité, la procédure suivante est employée :

1. Le condensé $\mathbf{H_B(M)}$ du message est généré au moyen de la même fonction **H** (nécessité de mise en place d'un protocole de communication).

2. Parallèlement, la signature **S(M)** est déchiffrée au moyen de la clé publique. Le condensé censé avoir été généré par A est ainsi retrouvé côté récepteur par $\mathbf{D_A(S(M))}$.

3. Le condensé $\mathbf{H_B(M)}$ est comparé avec celui déchiffré depuis la signature :

    - En cas d'égalité, le message **M** est authentifié car seul **A** avec sa clé privée est capable de générer un condensé "compatible" avec sa clé publique et l'intégrité du message.

    - Si les deux sont différents, soit le message a été altéré, soit il n'a pas été rédigé par **A**.

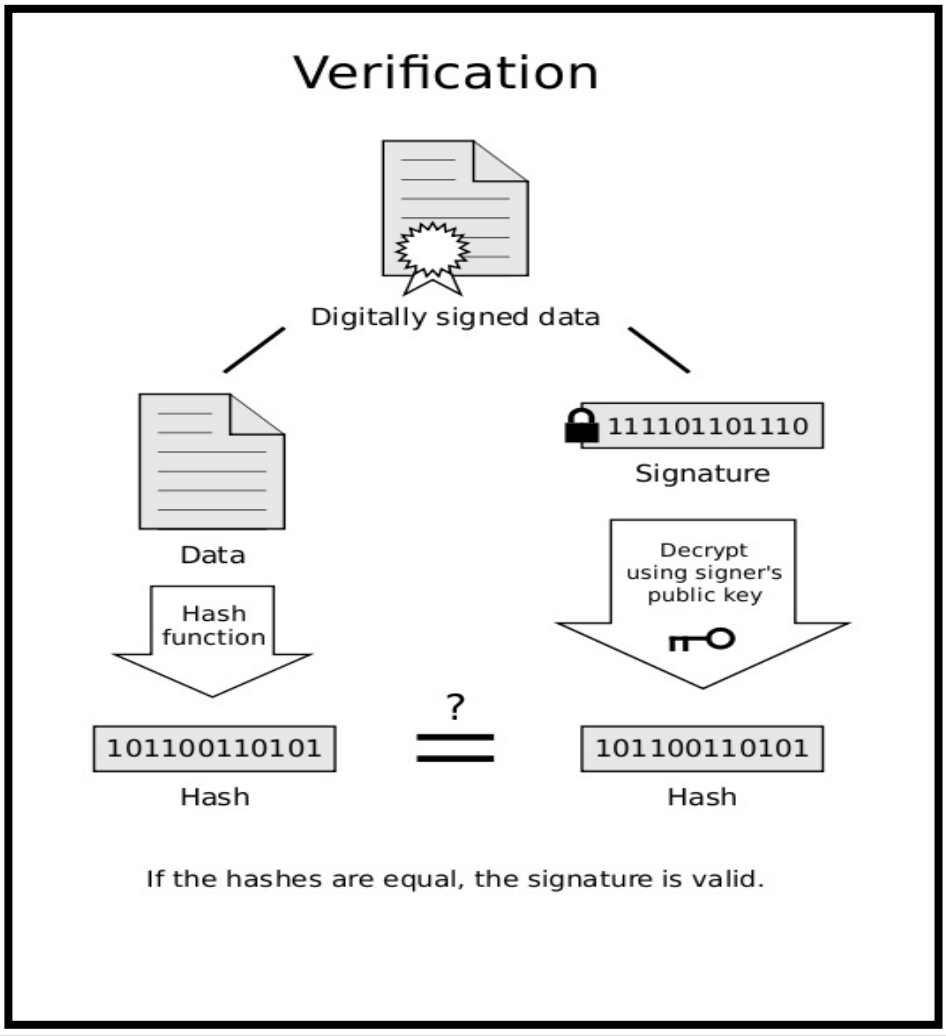


Figure 9 : vérification d'un document électronique signé.

CHAPITRE III :

Réalisation des modules de l'application

I. Choix d'Outils :

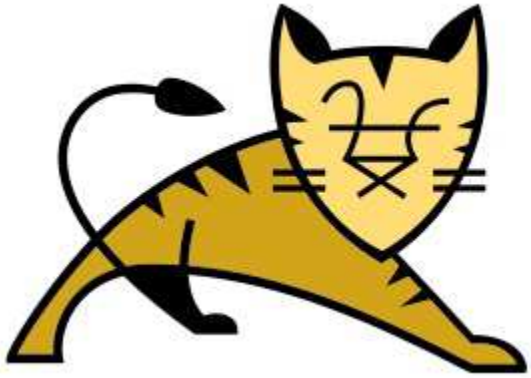
I.1. JAVA EE :

Java Enterprise Edition, ou Java EE (anciennement J2EE), est une spécification pour la technique Java de Sun plus particulièrement destinée aux applications d'entreprise. Ces applications sont considérées dans une approche multi-niveaux. Dans ce but, toute implémentation de cette spécification contient un ensemble d'extensions au *framework* Java standard (JSE, *Java Standard Edition*) afin de faciliter la création d'applications réparties.

Pour ce faire, Java EE définit les éléments suivants :

- Une plate-forme (*Java EE Platform*), pour héberger et exécuter les applications.
- Une suite de tests (*Java EE Compatibility Test Suite*) pour vérifier la compatibilité.
- Une réalisation de référence (*Java EE Reference Implementation*), qui est GlassFish.
- Un catalogue de bonnes pratiques (*Java EE BluePrints*).

I.2. Apache Tomcat :



Apache Tomcat est un conteneur libre de servlets et JSP Java EE. Issu du projet Jakarta, c'est un projet principal de l'*Apache Software Foundation*. Il implémente les spécifications des servlets et des JSP du Java Community Process, est paramétrable par des fichiers XML et de propriétés, et inclut des outils pour la configuration et la gestion. Il comporte également un serveur HTTP.

I.3. HTML :

L'*Hypertext Markup Language*, généralement abrégé HTML, est le format de données conçu pour représenter les pages web. C'est un langage de balisage qui permet d'écrire de l'hypertexte, d'où son nom. HTML permet également de structurer sémantiquement et de mettre en forme le contenu des pages, d'inclure des ressources multimédias dont des images, des formulaires de saisie, et des éléments programmables tels que des *applets*. Il permet de créer des documents interopérables avec des équipements très variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilisé conjointement avec des langages de programmation (JavaScript) et des formats de présentation (feuilles de style en cascade). HTML est initialement dérivé du *Standard Generalized Markup Language* (SGML).

I.4. CSS :

Cascading Style Sheets , Les feuilles de styles en cascade sont un langage qui permet de gérer la présentation d'une page web, c'est un ensemble de règles stylistiques appliquées à un ou plusieurs documents HTML.

Le but de CSS est de séparer la structure d'un document HTML et sa présentation

I.5. Barid eSign

La solution Barid eSign a pour rôle de fournir un certificat dit sécurisé délivré par l'autorité de certification au Maroc Barid eSign pour un usage de signature numérique.

- Les captures d'écrans suivantes détailleront les étapes d'installations de cet outil :

➢ ***INSTALLATION DE LA CHAINE DE CONFIANCE :***

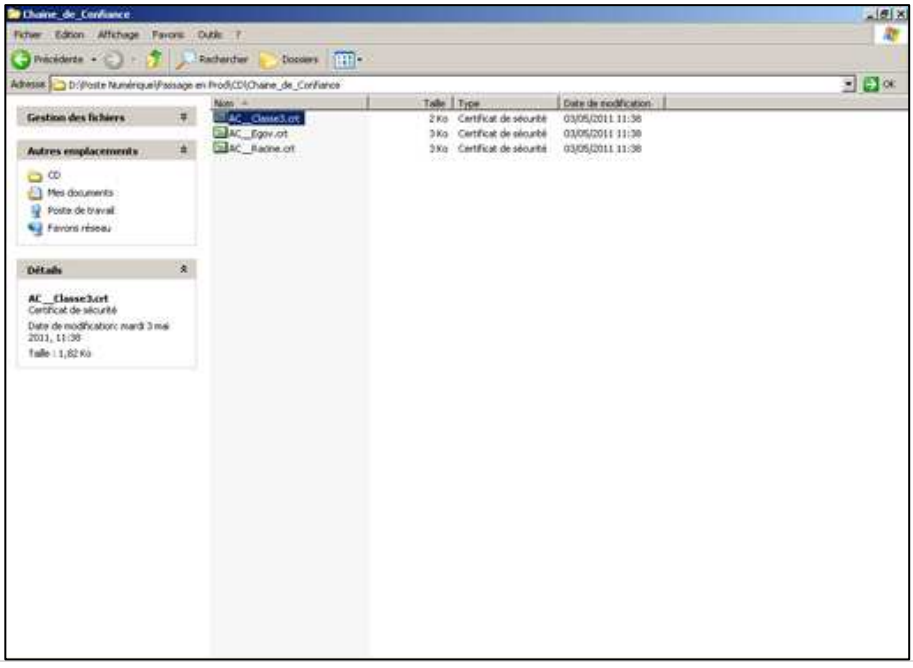


*Figure 10 :Dans le CD fourni on trouve : un répertoire intitulé « **Chaîne de confiance** »*

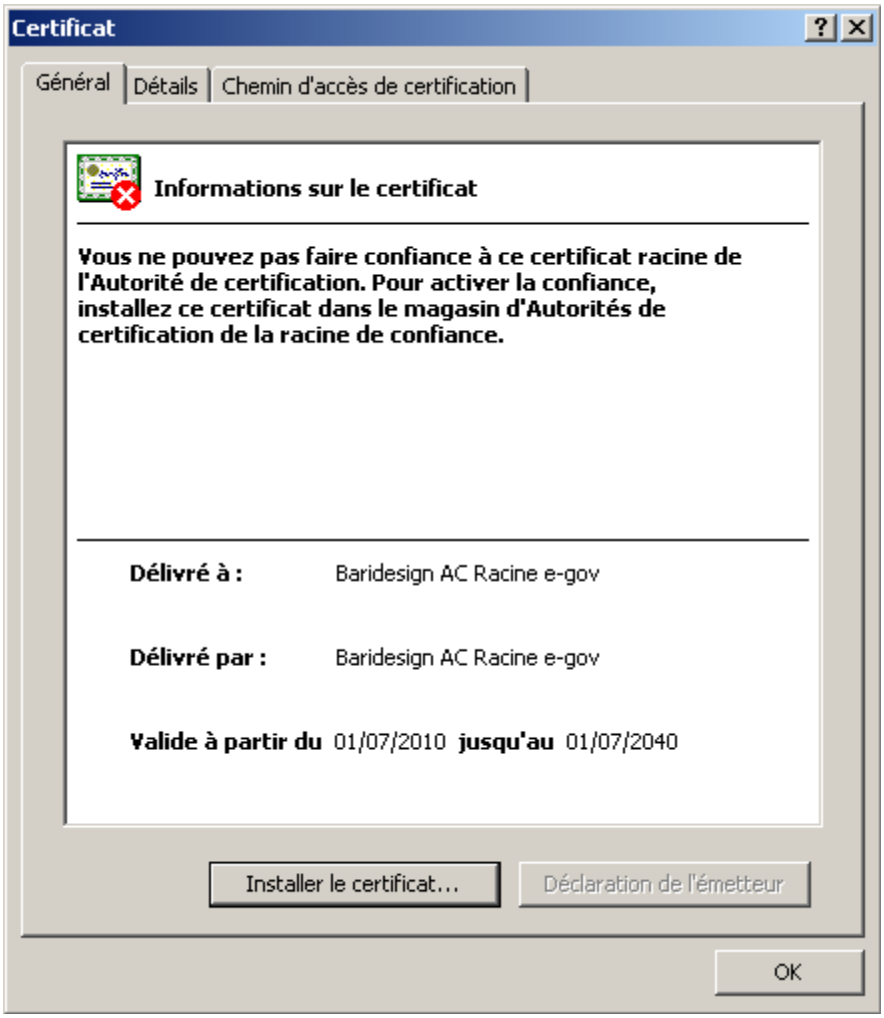


*Figure 11 : Installation du Certificat Racine depuis le fichier « **AC__Racine.crt** » de la figure 10.*

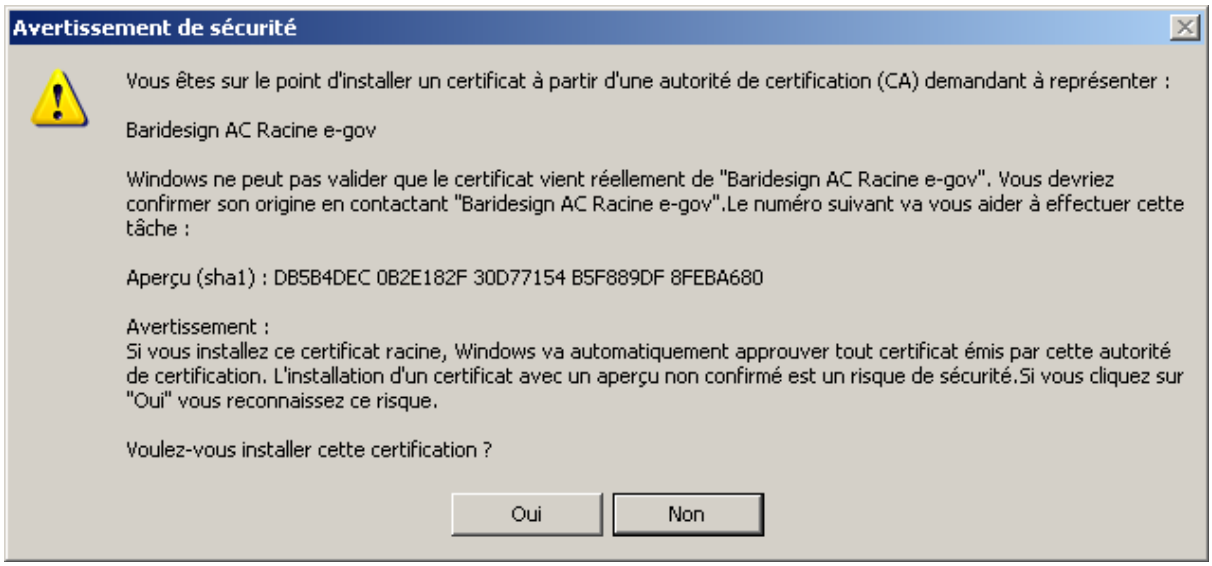


Figure 12 : Message de confirmation de l'installation du certificat racine

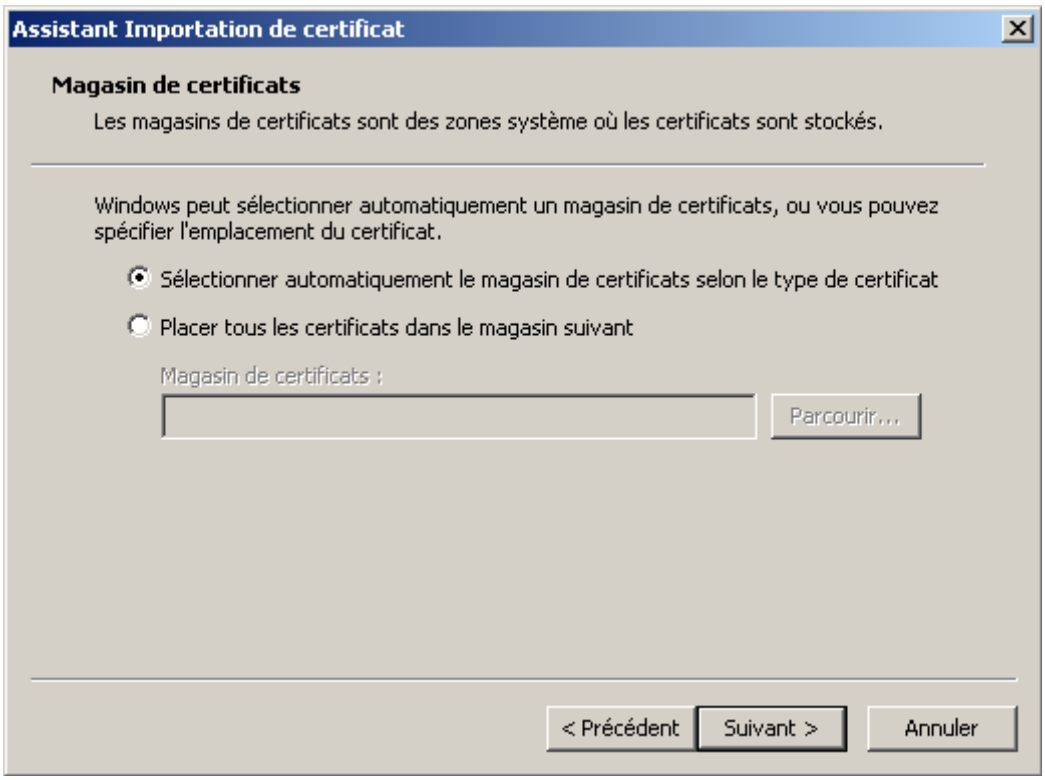


*Figure 13 : Installation du certificat intermédiaire « Egov » depuis « **AC__Egov.crt** » de la figure 10.*

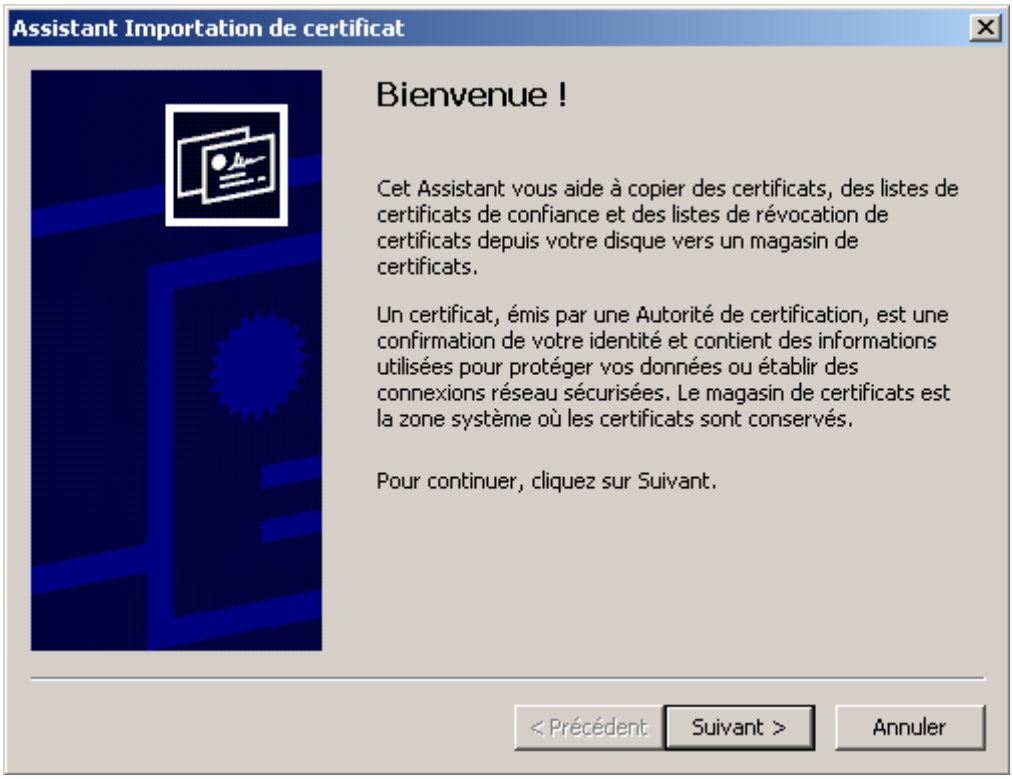


Figure 14 : Assistant d'importations des certificats

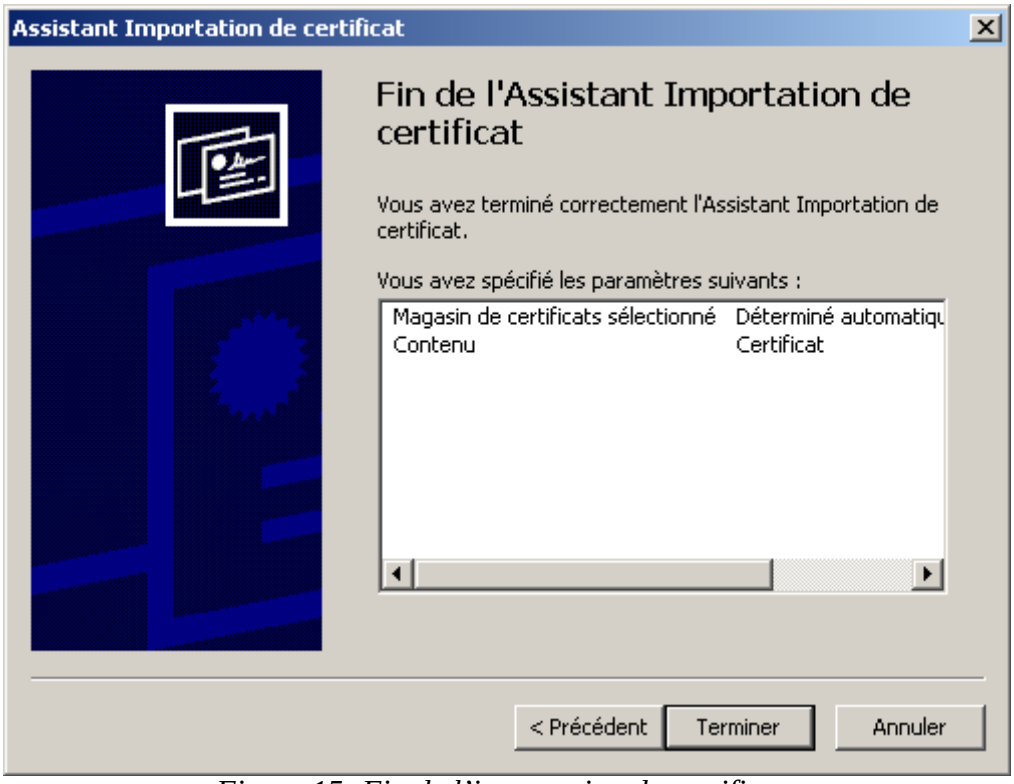


Figure 15 :Fin de l'importation de certificat .

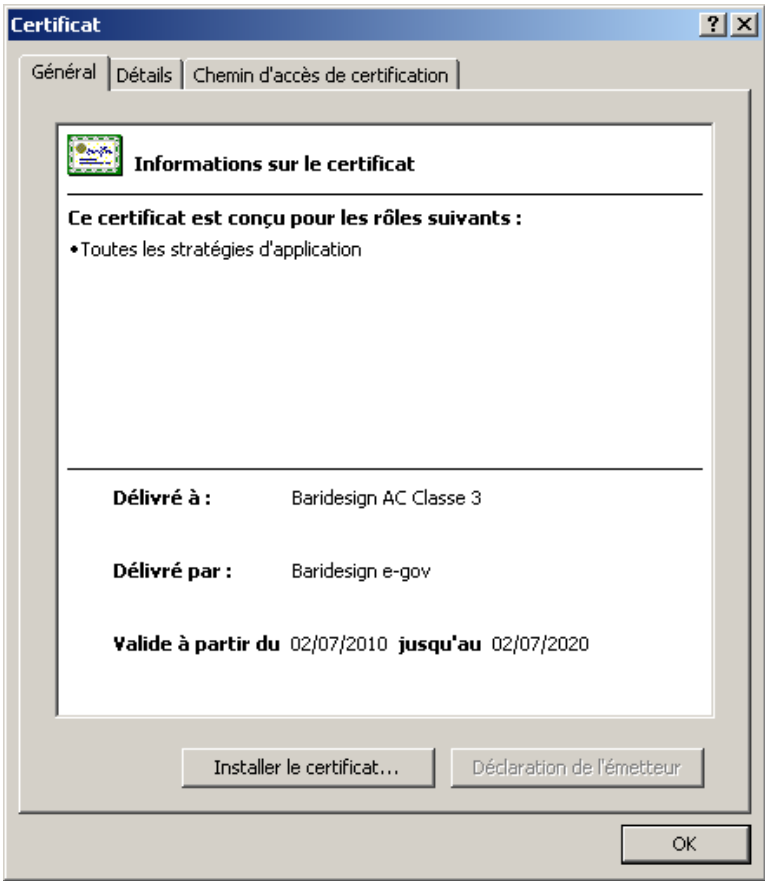


*Figure 16 :Installation du certificat intermédiaire « Classe 3 » depuis le fichier « **AC__Classe3.crt** » de la figure 10.*

➢ *INSTALLATION DE CLIENT MIDDLEWARE*

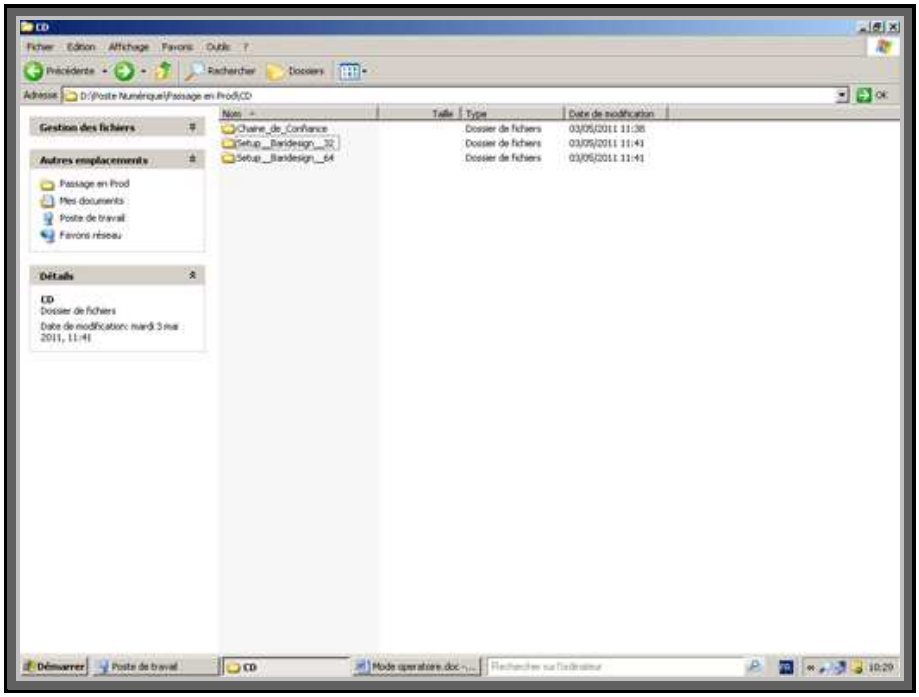


*Figure 17 : Installation du client depuis le répertoire intitulé« **Setup__Baridesign__32**»*

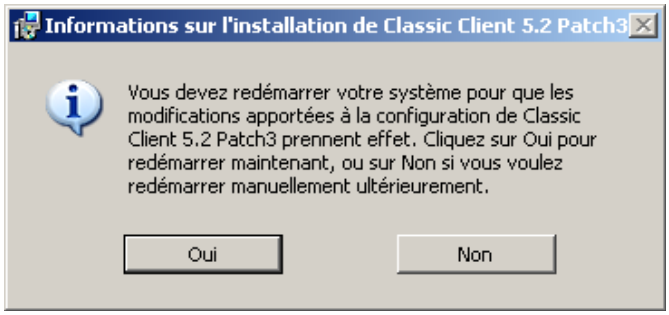


Figure 18 : Redémarrage du système après installation.

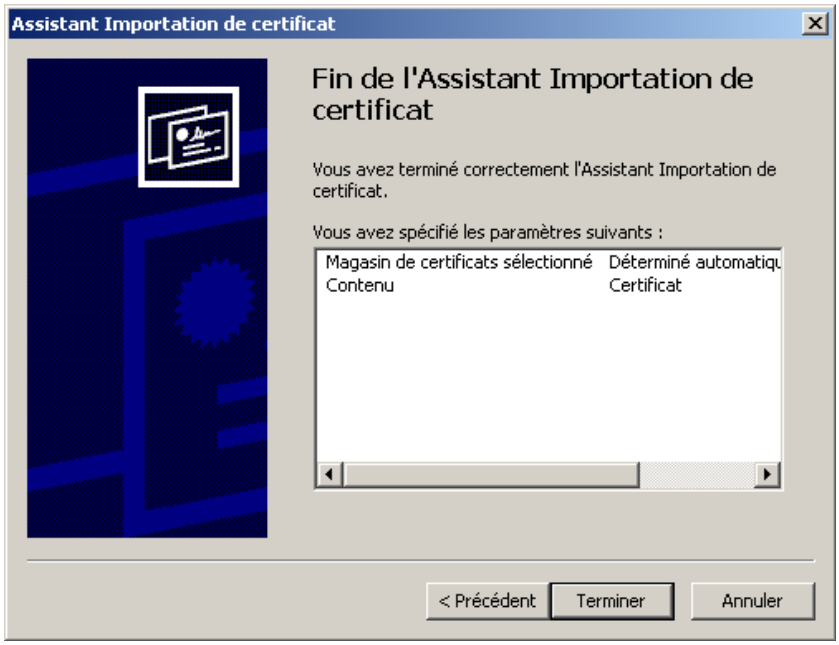


Figure 19 : Fin de l'installation.

II. Choix d'algorithmes :

II.1. Fonction de Hachage : SHA1

SHA-1 est une fonction de hachage cryptographique conçue par la National Security Agency des États-Unis (NSA), et publiée par le gouvernement des États-Unis comme un standard fédéral de traitement de l'information (Federal Information Processing Standard du National Institute of Standards and Technology (NIST)). Elle produit un résultat appelé « hash » ou condensat.

Le SHA-1 est un excellent générateur de nombres pseudo-aléatoires (comme beaucoup de fonctions de hachage) et il passe avec succès tous les tests statistiques. Un test conduit par Eric Filiol a confirmé la qualité mathématique des sorties qui sont « plus aléatoires » que celles de MD5, RIPEMD-160 ou SHA-0.

II.2. Algorithme de génération de clés : RSA

Le RSA a été invente par Rivest, Shamir et Adleman en 1978. C'est l'exemple le plus courant de cryptographie asymétrique, toujours considère comme sur, avec la technologie actuelle, pour des clés suffisamment grosses (1024, 2048 voire 4096 bits). D'ailleurs le RSA128 (algorithme avec des clés de 128 bits), propose en 1978 par Rivest, Shamir et Adleman, n'a été "cassé" qu'en 1996, en faisant travailler en parallèle de nombreux ordinateurs sur internet. Mais le concept de chiffrement asymétrique avec une clef publique était légèrement antérieur (1976). L'idée générale était de trouver deux fonctions f et g sur les entiers, telles que f _g = Id, et telle que l'on ne puisse pas trouver f, la fonction de décryptage, à partir de g, la fonction de cryptage. L'on peut alors rendre publique la fonction g (ou clef), qui permettra aux autres de crypter le message à envoyer, tout en étant les seuls à connaıtre f, donc à pouvoir décrypter.

Malgré une apparente simplicité, le système RSA reste l'un des plus sûrs. Jusqu'à très récemment, la plupart des gens s'accordaient sur l'idée que décoder un message sans connaıtre la clef était équivalent a factoriser l'entier n (i.e. trouver p et q).

II.3. Certificat Electronique : X509

X.509 est une norme de cryptographie de l'Union internationale des télécommunications pour les infrastructures à clés publiques (PKI). X.509 établit entre autres les formats standards de certificats électroniques et un algorithme pour la validation de chemin de certification.

X.509 a été créé en 1988 dans le cadre de la norme X.500. Il repose sur un système hiérarchique d'autorités de certification, à l'inverse des réseaux de confiance (comme PGP), où n'importe qui peut signer (et donc valider) les certificats des autres.

II.4. API utilisés :

Durant le Développement des deux modules on a eu recours à un ensemble de définitions de Classes contenant des méthodes exposées publiquement, ces définitions de Classes sont incluses dans des API qu'on doit importer afin de pouvoir gérer les objets dérivés et utiliser des méthodes à partir de ces classes :

- java.io.File.* :

Permet d'effectuer divers traitement sur des fichiers.

- org.apache.commons.fileupload.* :

Un composant pour le traitement des uploads de fichiers HTML tel que spécifié par la RFC 1867.

- javax.servlet.* :

Contient un certain nombre de classes et d'interfaces qui décrivent et définissent les contrats conclus entre une classe servlet et l'environnement d'exécution prévu à une instance d'une telle classe par un conteneur de servlet conforme.

- Java.util.* :

Contient les classes utilitaires divers par exemple une chaine tokenizer, un générateur de nombres aléatoires, un tableau de bits…

- Java.security.* :

Fournit des classes et des interfaces pour le cadre de la sécurité, notamment des méthodes pour la certification de clé publique par un tiers de confiance prédéfinie, et pour instancier des objets de type signature/ clé.

Démonstration

Le but de notre projet était de développer deux modules l'un pour signer les documents électroniques et l'autre pour vérifier l'authenticité des documents signés, afin de les intégrer à la solution de dématérialisation de l'entreprise.

Ici on va présenter les interfaces des modules :

- ***Signature Du Fichier :***

- L'utilisateur choisi sur sa machine le fichier à signer :

Figure 20 : Interface du module de signature des documents électroniques.

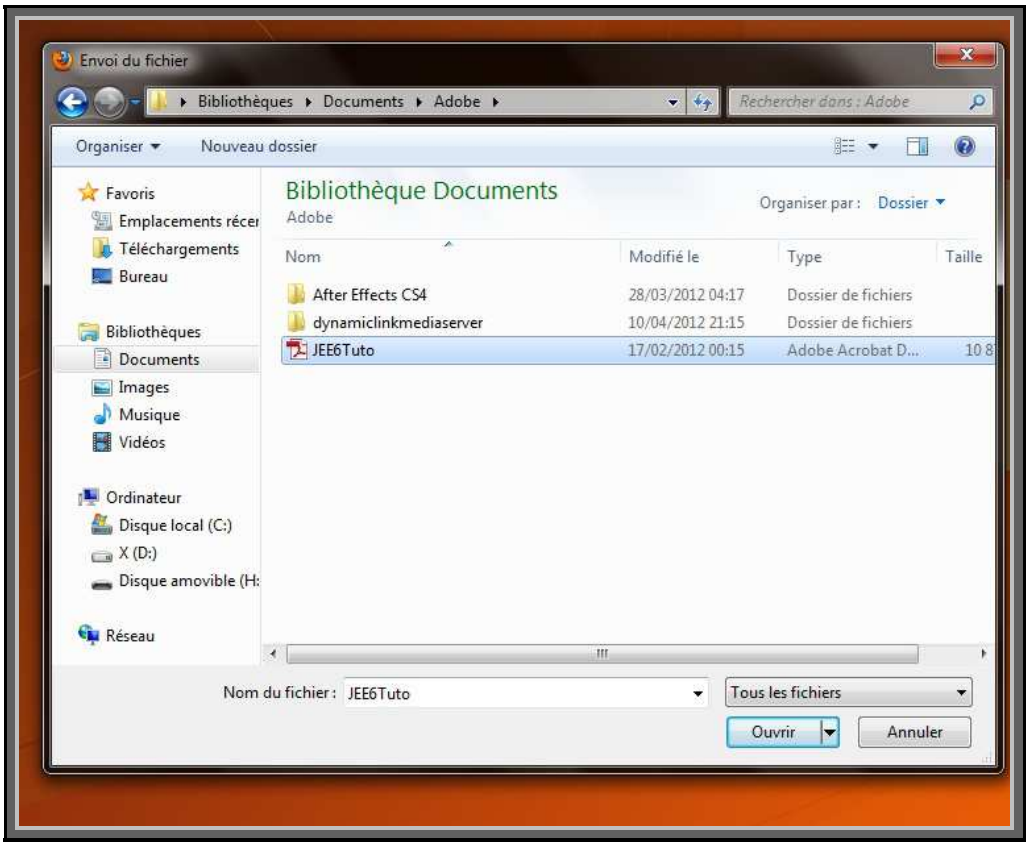


Figure 21 : Sélection du document électronique à signer

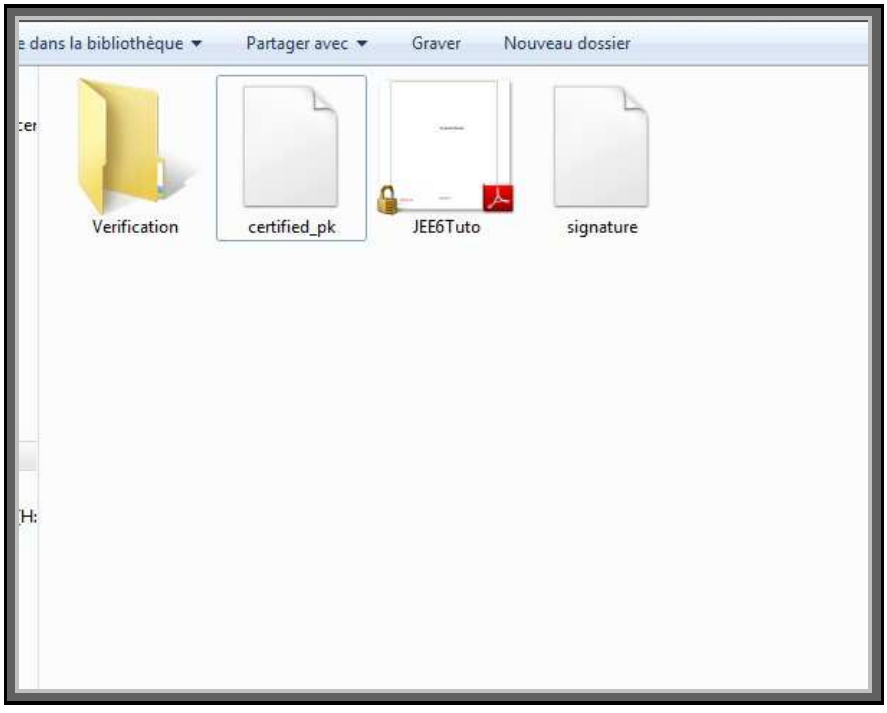


Figure 22 : Signature du document effectué avec succès.

Comme on le remarque sur la Figure 22, après la signature du document sélectionné par l'utilisateur, trois nouveaux fichiers sont générés :

- Document Electronique Signé.
- Signature.
- Clé Publique Certifié.

➢ ***Vérification de la signature :***

L'utilisateur choisi les trois fichiers résultant du premier module depuis sa machine.

Figure 23 : Interface du module de vérification de signatures.

Le module confirme par un message que la Signature est conforme et que le document n'as pas été altéré.

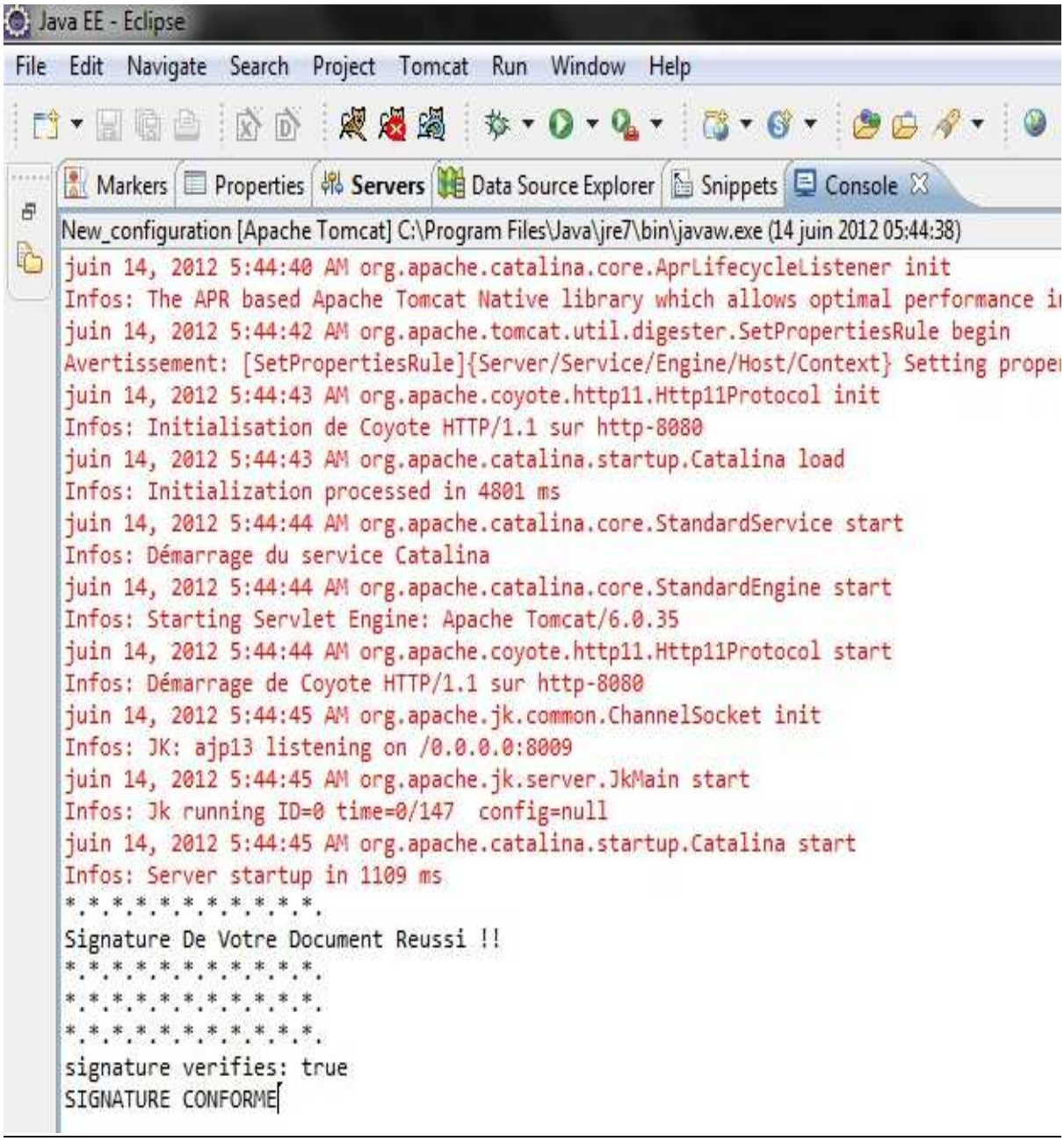


Figure 24 : Résultat du traitement : Document Authentique.

Perspectives

Nous avons proposé comme amélioration de créer deux autorités internes au sein de l'entreprise :

- Une autorité d'enregistrement : Cette autorité sera chargée de contrôler et d'administrer une base de données contenant des pairs de clés générés par cette même autorité.
- Une autorité de dépôt : cette autorité sera chargée d'administrer une base de données contenant les certificats électroniques des utilisateurs

On illustre notre plan par le schéma suivant :

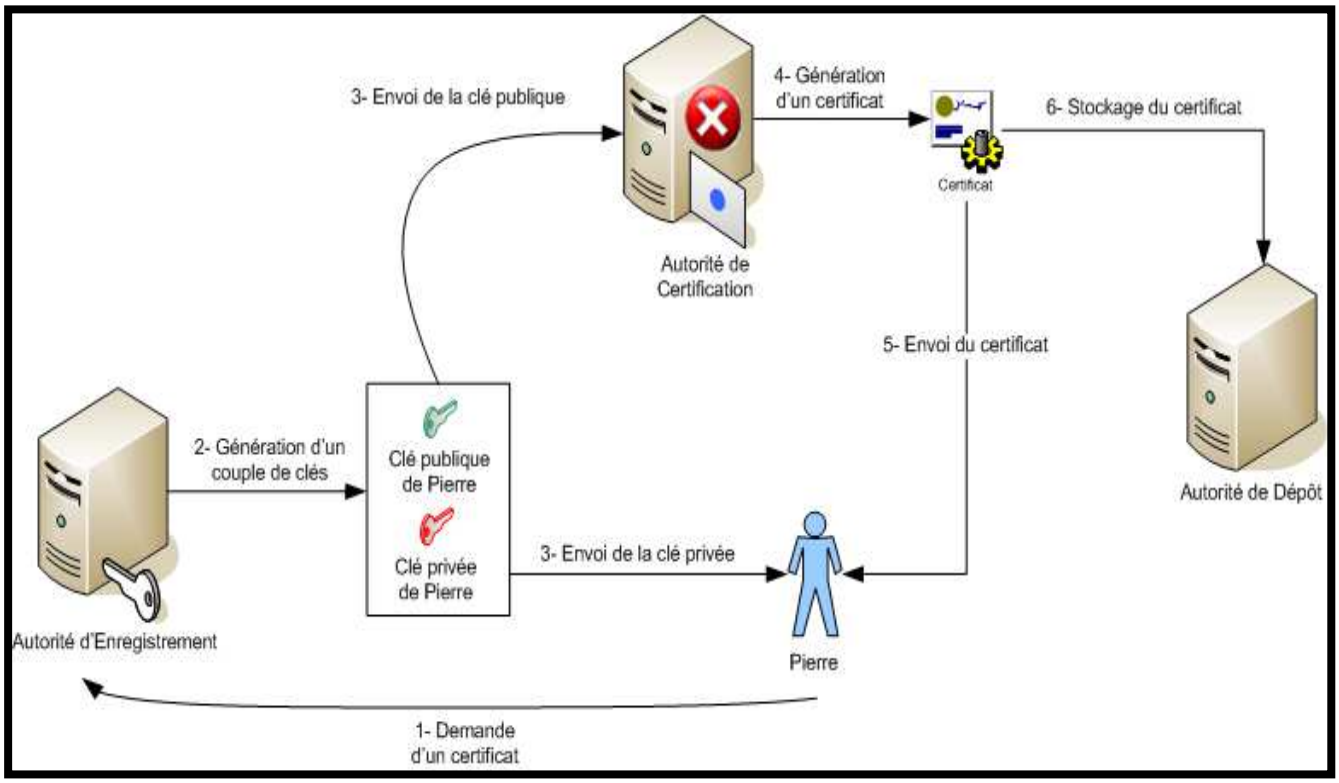


Figure 25 : Illustration de la nouvelle perspective

Conclusion Générale

Ce rapport de synthèse de notre projet de fin d'études présente brièvement le projet que nous avons été amenés à réaliser dans les semaines de stage, tout au long de ce rapport, on a présenté les divers composants ainsi que les différentes phases nécessaires au développement de ces deux modules.

Après des recherches approfondies dans le domaine de la signature électronique qui lit l'informatique et les mathématiques, on a essayé dans ce projet de répondre aux attentes de la société qui a mis en nous sa confiance, et restituer des modules faciles à utiliser et à intégrer dans le processus de dématérialisation

Cette période de stage nous a permis non seulement de découvrir et maitriser de nouveaux langage de programmation orienté objet très courant (JAVA, J2EE) mais aussi d'acquérir une expérience extrêmement valorisante d'un point de vue personnel. Et surtout d'avoir une première vision concrète de la mission d'un informaticien dans le milieu professionnel, et de la façon dont une organisation aussi bien réputée que le groupe Banque Populaire fonctionne.

Ce projet nous a profondément marqué, et a vraiment changé notre vision, car on a eu la chance de laisser notre trace dans le Green Computing, et ainsi réduire l'empreinte écologique de l'informatique sur notre environnement, notamment en participant à un grand projet visant à diminuer de 75% les déchets papiers de l'entreprise ainsi préserver notre mère nature.

On n'oubliera jamais toutes ces personnes qu'on a eu la chance de rencontrer durant notre stage, des gens qui savent relier boulot, compétence et passion, et qui n'hésitent pas à vous faire entrer dans leur monde et partager avec vous tout leur acquis sans demander rien en retour.

Bibliographie/Webographie

- **Bibliographie :**

- Schneier, Cryptographie appliquée : protocoles, algorithmes et codes sources en C, J. Wiley, 1997
- Michael T. Goodrich et Roberto Tamassia, Data Structures and Algorithms in Java, John Wiley & Sons, Inc., 4e éd.
- Colliding X.509 certificates , Arjen Lenstra, Wang Xiaoyun & Benne de Weger
- Cryptographie : principes et mises en œuvre, Pierre Barthélemy, Robert Rolland, Pascal Véron
- W. Diffie and M.E. Hellman, Multiuser cryptographic technics, Proceedings of AFIPS National Computer Conference.
- R.C. Merkle, M.E. Hellman,, Hiding information and signatures in trapdoor functions, IEEE transactions on information theory.
- Ronald Rivest, Adi Shamir, Leonard Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems, Communications of the ACM.

- **Webographie :**

- http://www.worldcat.org/title/collectioninformatique/oclc/637510404?lang=fr
- www.google.com
- http://java.developpez.com/cours/
- http://java.developpez.com/cours/servlets/

➢ *L'algorithme RSA :*

- ***Description du protocole***

Le but du jeu est bien sûr de pouvoir transmettre un message codé, que seul le récepteur "officiel" puisse décrypter, c'est-à-dire qui ne puisse pas être décrypté par un tiers qui intercepterait ledit message. Nous appellerons Alice la destinatrice du message, et Bernard l'émetteur.

1. Alice génère deux gros nombres premiers p et q, ainsi qu'un gros nombre d premier avec le produit $w = (p-1)(q-1)$.
2. Alice calcule $n = pq$ et e tel que $de \equiv 1[w]$.
3. Alice diffuse n et e, garde d et oublie w.
4. Bernard crypte un message M par $M \mapsto M^e[n]$ et envoie le résultat à Alice.
5. Alice décode alors le message crypté par $C \mapsto C^d[n]$

EXEMPLE : Voyons ce qui se passe si l'on prend pour les deux nombres p et q les valeurs 11 et 17. On a alors $n = 187$ et $w = (11-1)(17-1) = 160$. Comme $161 = 7 \times 23$, on peut prendre $e = 7$ et $d = 23$.

Alice va rendre public le couple $(187, 7)$.

Bernard veut transmettre à Alice un message codé plus petit que $n = 187$, mettons la date à laquelle ils vont faire une surprise à Cédric (par exemple, le 10), message qui ne doit pas être intercepté par ledit Cédric, bien sûr.

Bernard va donc calculer $10^7 = 187 \times 53475 + 175$, et envoyer le résultat 175 à Alice.

Alice va calculer le reste de la division euclidienne de 175^{23} par 187 :

- Elle calcule d'abord $175^2 = 30625 = 163 \times 187 + 144$, donc $175^2 \equiv 144[187]$.
- Ensuite, $144^2 = 20736 = 110 \times 187 + 166$, donc $175^4 \equiv 166[187]$.
- Puis, $166^2 = 27556 = 147 \times 187 + 67$ donc $175^8 \equiv 67[187]$.
- Et $67^2 = 4489 = 24 \times 187 + 1$ donc $175^{16} \equiv 1[187]$.
- Enfin, $175^{23} = 175^{16} \times 175^4 \times 175^2 \times 175$ donc

$$175^{23} \equiv 1 \times 166 \times 144 \times 175[187]$$

Or $166 \times 144 \times 175 = 4183200 = 22370 \times 187 + 10$.

Alice retrouve donc bien le message envoyé, à savoir 10.

- ***Preuve de l'algorithme :***

Dans la suite, nous allons utiliser constamment la propriété des congruences suivante :

Pour tout quadriplet d'entiers (a, b, c, r), si $a \equiv b[c]$, alors $a^r \equiv b^r[c]$. Cette propriété se démontre aisément si l'on remarque que $a - b$ divise $a^r - b^r$...

Le but du protocole est bien sûr qu'Alice retrouve le message d'origine. Les transformations successives appliquées au message d'origine sont :

$$\mathrm{M} \mapsto \mathrm{M}^e[n] \mapsto (\mathrm{M}^e[n])^d[n]$$

- Si le message M est premier à n :
  On a $(\mathrm{M}^e[n])^d[n] \equiv \mathrm{M}^{de}[n]$, et par hypothèse $de \equiv 1[w]$, c'est-à-dire que $de = 1 + kw$, avec k un entier.
  Mais alors on peut appliquer le théorème 1.3 : M est premier à n donc $\mathrm{M}^{\varphi(n)} \equiv 1[n]$. Et d'après le lemme 1.1, comme on a $n = pq$, on sait que $\varphi(n) = (p-1)(q-1) = w$. On a donc :

  $$\mathrm{M}^w \equiv 1[n], \text{ donc } \mathrm{M}^{de} = \mathrm{M}^{kw+1} \equiv \mathrm{M}.1^k[n] \equiv \mathrm{M}[n]$$

  et donc on revient bien ainsi au message originel.
- Sinon, M non premier à $n = pq$, c'est-à-dire que M est multiple de p ou de q. Considérons le cas où M est de la forme $p^\alpha m$, avec m entier non multiple de p.,
  Comme $\mathrm{M} < n$, on peut affirmer que m est premier à n (sinon, M serait à la fois multiple de p et de q, donc plus grand que n !). Et on a :

  $$\mathrm{M}^{de} = (p^\alpha m)^{de}[n] \equiv p^{\alpha de} * m^{de}[n] \equiv p^{\alpha de} * m[n]$$

  d'après ce qui précède, appliqué à m.
  Or $p^{\alpha de} \equiv p^\alpha[p]$ (c'est évident !) et $p^{\alpha de} \equiv p^\alpha[q]$: par le théorème 1.3, on a $p^{q-1} \equiv 1[q]$ et comme $de = kw + 1$, on obtient $p^{de} \equiv p.1^{k(p-1)}[q] \equiv p[q]$.
  En élevant la relation à la puissance α, il vient bien $p^{\alpha de} \equiv p^\alpha[q]$.
  Mais alors la différence $p^{\alpha de} - p^\alpha$ est à la fois multiple de p et de q, donc multiple de pq en utilisant le lemme de Gauss. On obtient bien $p^{\alpha de} \equiv p^\alpha[n]$ et donc :

  $$\mathrm{M}^{de} \equiv p^\alpha m[n] \equiv \mathrm{M}[n]$$

  et Alice retrouve bien le message originel.
- Les nombres p et q jouant des rôles identiques, le cas où M est multiple de q est identique.

N.B. Au vu de ce qui précède, on serait tenté d'énoncer un corollaire au théorème 1.3 du type : "Pour tout entier a, on a $a^{\varphi(n)+1} \equiv a[n]$". C'est malheureusement faux lorsque n est multiple d'un carré : $\varphi(4) = 2$ et 2^2 n'est pas congru à 2 modulo 4. Une formulation juste, mais un peu lourde, serait :

"Si n est un entier non multiple d'un carré, alors pour tout entier a, on a $a^{\varphi(n)+1} \equiv a[n]$."

- ***Contenu du Fichier Web.xml :***

```
<?xml version="1.0" encoding="UTF-8"?>
<web-app id="WebApp_ID" version="2.4" xmlns="http://java.sun.com/xml/ns/j2ee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
    "http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd">
    <display-name>SIGNATURE</display-name>
    <servlet>
        <description>
        </description>
        <display-name>SignSV</display-name>
        <servlet-name>SignSV</servlet-name>
        <servlet-class>com.bcp.sign.SignSV</servlet-class>
    </servlet>
    <servlet>
        <description>
        </description>
        <display-name>VerifSignSV</display-name>
        <servlet-name>VerifSignSV</servlet-name>
        <servlet-class>com.bcp.sign.VerifSignSV</servlet-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>SignSV</servlet-name>
        <url-pattern>/SignSV</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>VerifSignSV</servlet-name>
        <url-pattern>/VerifSignSV</url-pattern>
    </servlet-mapping>
    <welcome-file-list>
        <welcome-file>index.html</welcome-file>
        <welcome-file>index.htm</welcome-file>
        <welcome-file>index.jsp</welcome-file>
        <welcome-file>default.html</welcome-file>
        <welcome-file>default.htm</welcome-file>
        <welcome-file>default.jsp</welcome-file>
    </welcome-file-list>
</web-app>
```

- ***API utilisés dans la Class de génération de signature (GenSig):***

```
package com.bcp.sign;
import java.io.BufferedInputStream;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.SecureRandom;
import java.security.Signature;

class GenSig {
```

- ***API utilisés dans la Class de vérification de signature (VerSig):***

```
package com.bcp.sign;
import java.io.*;
import java.security.*;
import java.security.spec.*;


public class VerSig {
```

- ***Loi N°53-05 relative à l'échange électronique des données juridiques (Constitution du Maroc):***

CHAPITRE PRELIMINAIRE

ARTICLE PREMIER

La présente loi fixe le régime applicable aux données juridiques échangées par voie électronique, à l'équivalence des documents établis sur papier et sur support électronique et à la signature électronique.

Elle détermine également le cadre juridique applicable aux opérations effectuées par les prestataires de service de certification électronique, ainsi que les règles à respecter par ces derniers et les titulaires des certificats électroniques délivrés.

TITRE PREMIER

DE LA VALIDITE DES ACTES ETABLIS SOUS FORME ELECTRONIQUE OU TRANSMIS PAR VOIE ELECTRONIQUE

Article 2

Le chapitre premier du titre premier du livre premier du dahir formant code des obligations et des contrats est complété par un article 2-1 ainsi conçu :

« *Article 2-1.* – Lorsqu'un écrit est exigé pour la validité « d'un acte juridique, il peut être établi et conservé sous forme « électronique dans les conditions prévues aux articles 417-1 « et 417-2 ci-dessous.

« Lorsqu'une mention écrite est exigée de la main même de « celui qui s'oblige, ce dernier peut l'apposer sous forme « électronique, si les conditions de cette apposition sont de nature « à garantir qu'elle ne peut être effectuée que par lui-même.

« Toutefois, les actes relatifs à l'application des « dispositions du code de la famille et les actes sous seing privé « relatifs à des sûretés personnelles ou réelles, de nature civile ou « commerciale, ne sont pas soumis aux dispositions de la « présente loi, à l'exception des actes établis par une personne « pour les besoins de sa profession. »

Article 3

Le titre premier du livre premier du dahir formant Code des obligations et des contrats est complété par un chapitre premier *bis* conçu ainsi qu'il suit :

***« Chapitre premier* bis**

« Du contrat conclu sous forme électronique
« ou transmis par voie électronique.

« Section I. – **Dispositions générales**

« *Article 65-1.* – Sous réserve des dispositions du présent « chapitre, la validité du contrat conclu sous forme électronique « ou transmis par voie électronique est régie par les dispositions « du chapitre premier du présent titre.

« *Article 65-2.* – Les dispositions des articles 23 à 30 et 32 « ci-dessus ne sont pas applicables au présent chapitre.

« Section II. – **De l'offre**

« *Article 65-3.* – La voie électronique peut être utilisée pour « mettre à disposition du public des offres contractuelles ou des « informations sur des biens ou services en vue de la conclusion « d'un contrat.

« Les informations qui sont demandées en vue de la « conclusion d'un contrat ou celles qui sont adressées au cours de « son exécution peuvent être transmises par courrier électronique « si leur destinataire a accepté expressément l'usage de ce moyen.

« 5 - les langues proposées pour la conclusion du contrat ;

« 6 - les modalités d'archivage du contrat par l'auteur de « l'offre et les conditions d'accès au contrat archivé, si la nature « ou l'objet du contrat le justifie ;

« 7- les moyens de consulter, par voie électronique, les « règles professionnelles et commerciales auxquelles l'auteur de « l'offre entend, le cas échéant, se soumettre.

« Toute proposition qui ne contient pas l'ensemble des « énonciations indiquées au présent article ne peut être « considérée comme une offre et demeure une simple publicité « et n'engage pas son auteur.

« Section III . – **De la conclusion d'un contrat sous forme électronique**

« *Article 65-5.* – Pour que le contrat soit valablement « conclu, le destinataire de l'offre doit avoir eu la possibilité de « vérifier le détail de son ordre et son prix total et de corriger « d'éventuelles erreurs, et ce avant de confirmer ledit ordre pour « exprimer son acceptation.

« L'auteur de l'offre doit accuser réception, sans délai « injustifié et par voie électronique, de l'acceptation de l'offre qui « lui a été adressée.

« Le destinataire est irrévocablement lié à l'offre dès sa « réception.

« L'acceptation de l'offre, sa confirmation et l'accusé de « réception sont réputés reçus lorsque les parties auxquelles ils « sont adressés peuvent y avoir accès.

« Section IV. – **Dispositions diverses**

« Section II. – **De l'offre**

« *Article 65-3.* – La voie électronique peut être utilisée pour « mettre à disposition du public des offres contractuelles ou des « informations sur des biens ou services en vue de la conclusion « d'un contrat.

« Les informations qui sont demandées en vue de la « conclusion d'un contrat ou celles qui sont adressées au cours de « son exécution peuvent être transmises par courrier électronique « si leur destinataire a accepté expressément l'usage de ce moyen.

« Les informations destinées à des professionnels peuvent « leur être transmises par courrier électronique, dès lors qu'ils ont « communiqué leur adresse électronique.

« Lorsque les informations doivent être portées sur un « formulaire, celui-ci est mis, par voie électronique, à la « disposition de la personne qui doit le remplir.

« *Article 65-4.* – Quiconque propose, à titre professionnel, « par voie électronique, la fourniture de biens, la prestation « de services ou la cession de fonds de commerce ou l'un de « leurs éléments met à disposition du public les conditions « contractuelles applicables d'une manière permettant leur « conservation et leur reproduction.

« Sans préjudice des conditions de validité prévues dans « l'offre, son auteur reste engagé par celle-ci, soit pendant la « durée précisée dans ladite offre, soit, à défaut, tant qu'elle est « accessible par voie électronique de son fait.

« L'offre comporte, en outre :

« 1 - les principales caractéristiques du bien, du service « proposé ou du fonds de commerce concerné ou l'un de ses « éléments ;

« 2 - les conditions de vente du bien ou du service ou celles de « cession du fonds de commerce ou l'un de ses éléments ;

« 3 - les différentes étapes à suive pour conclure le contrat « par voie électronique et notamment les modalités selon « lesquelles les parties se libèrent de leurs obligations réciproques ;

« 4 - les moyens techniques permettant au futur utilisateur, « avant la conclusion du contrat, d'identifier les erreurs « commises dans la saisie des données et de les corriger ;

« lui a été adressée.

« Le destinataire est irrévocablement lié à l'offre dès sa « réception.

« L'acceptation de l'offre, sa confirmation et l'accusé de « réception sont réputés reçus lorsque les parties auxquelles ils « sont adressés peuvent y avoir accès.

« Section IV. – **Dispositions diverses**

« Articles 65-6. - L'exigence d'un formulaire détachable est « satisfaite lorsque, par un procédé électronique spécifique, il est « permis d'accéder au formulaire, de le remplir et de le renvoyer « par la même voie.

« Article 65-7. – Lorsqu'une pluralité d'originaux est « exigée, cette exigence est réputée satisfaite, pour les actes « établis sous forme électronique, si l'acte concerné est établi et « conservé conformément aux dispositions des articles 417-1, 417-2 « et 417-3 ci-dessous et que le procédé utilisé permet à chacune des « parties intéressées de disposer d'un exemplaire ou d'y avoir « accès. »

Article 4

La section II du chapitre premier, du titre septième, du livre premier du dahir formant Code des obligations et des contrats est complétée par les articles 417-1, 417-2 et 417-3 ainsi conçus :

« Section II. – **De la preuve littérale**

« *Article 417-1.* – L'écrit sur support électronique a la « même force probante que l'écrit sur support papier.

« L'écrit sous forme électronique est admis en preuve au « même titre que l'écrit sur support papier, sous réserve que « puisse être dûment identifiée la personne dont il émane et qu'il « soit établi et conservé dans des conditions de nature à en « garantir l'intégrité.

« *Article 417-2* – La signature nécessaire à la perfection « d'un acte juridique identifie celui qui l'appose et exprime son « consentement aux obligations qui découlent de cet acte.

« Lorsque la signature est apposée par devant un officier « public habilité à certifier, elle confère l'authenticité à l'acte.