

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique  
Centre de Recherche sur l'Information Scientifique et Technique



Mémoire pour l'obtention du diplôme  
de Post Graduation Spécialisée en Sécurité Informatique

## Thème

# Gestion des certificats numériques

Réalisé par :

BOUSSAHA Halim

LABIOD Adel

Encadré par : Dr. NOUALI Omar

Co-Encadreur : Mme CHALLAL Zakia

Soutenu devant le jury :

- Mme Taboudjemet-Nouali Nadia, DR : Présidente.
- Mme Bessai F-Zohra, MRB : Examinatrice.
- Mr Seba Abderazek , AR : Examineur.

Promotion 2011/ 2012

## RESUME

Depuis quelques années, l'accès à Internet a pris une grande ampleur. Les échanges « professionnels ou privés » par courrier électronique, les achats sur des sites de vente en ligne, les espaces intranet et extranet collaboratifs se sont multipliés. Or, il manquait aux débuts de ce phénomène un élément essentiel qui est le moyen d'identifier de manière certaine son interlocuteur. En effet, il est possible à n'importe qui de se créer une adresse de courrier électronique sans fournir de justificatif quelconque sur son identité.

Afin d'être sûr qu'on a affaire au bon interlocuteur, il faut qu'on soit capable de prouver son identité sur Internet, on doit savoir si quelqu'un a modifié le message reçu, on doit aussi, savoir que le message qu'on a envoyé est bien arrivé inchangé.

Le certificat numérique permet d'apporter des garanties sur l'identité de nos interlocuteurs sur internet, sur l'intégrité des messages, et de sécuriser les envois.

## Sommaire

<b>Introduction générale.....</b>	<b>1-2</b>
-----------------------------------	------------

### **Chapitre 1 : Notions fondamentales sur la cryptographie**

<b>1 Introduction .....</b>	<b>3</b>
<b>2 Cryptographie.....</b>	<b>3</b>
<b>2.1 Définition.....</b>	<b>3</b>
<b>2.2 Historique.....</b>	<b>4</b>
<b>2.3 Besoins cryptographiques.....</b>	<b>4</b>
<b>2.3.1 Authentification.....</b>	<b>4</b>
<b>2.3.2 Confidentialité.....</b>	<b>4</b>
<b>2.3.3 Intégrité.....</b>	<b>4</b>
<b>2.3.4 Non répudiation.....</b>	<b>4</b>
<b>2.4 Les méthodes de cryptographie.....</b>	<b>5</b>
<b>2.4.1 Cryptographie à clé secrète.....</b>	<b>5</b>
<b>2.4.2 Cryptographie à clé publique.....</b>	<b>7</b>
<b>2.4.3 Hachage.....</b>	<b>9</b>
<b>2.4.4 Signature numérique.....</b>	<b>10</b>
<b>3 Secure Socket Layer « SSL».....</b>	<b>12</b>
<b>3.1 Fonctionnement du SSL.....</b>	<b>12</b>
<b>3.2 Applications du SSL.....</b>	<b>12</b>
<b>4 Conclusion.....</b>	<b>13</b>

### **Chapitre 2 : Infrastructure à clé publique**

<b>1 Introduction.....</b>	<b>14</b>
----------------------------	-----------

2 Définition.....	14
3 Normalisation des PKI.....	15
4 Acteurs d'une PKI.....	15
4.1 Autorité de certification AC.....	16
4.2 Autorité d'enregistrement AE.....	16
4.3 Entité d'enroulement EE.....	16
4.4 Dépôt.....	16
4.5 L'horodatage.....	16
5 Processus d'une PKI.....	16
5.1 Enregistrement d'un client.....	17
5.2 Génération d'une paire de clé .....	17
5.3 Création d'un certificat.....	17
5.4 Renouvellement d'un certificat.....	18
5.5 Révocation d'un certificat .....	18
5.6 Recouvrement d'une clé privée.....	18
6 Architecture d'une PKI.....	19
6.1 Architecture simple.....	19
6.2 Architecture hiérarchique.....	20
6.3 Architecture hybride.....	20
7 Conclusion.....	20

### Chapitre 3 : Conception

1 Introduction.....	21
2 Architecture de la PKI.....	21
3 Cas d'utilisation et diagrammes de séquences.....	22
4 Architecture globale.....	28

4.1	Module "gestion des clients".....	28
4.2	Module "gestions des demandes".....	29
4.3	Module "gestion des certificats et des clés".....	29
5	Structure de données.....	30
5.1	Base de données AE.....	30
5.2	Base de données AC.....	31
6	Conclusion.....	32

### Chapitre 4 : Réalisation

1	Introduction.....	33
2	Environnement de développement.....	33
2.1	Langage de programmation.....	33
2.2	SGBD.....	33
2.3	Outil cryptographique.....	34
3	Architecture technique de notre PKI.....	34
4	Interfaces de notre PKI.....	35
4.1	Interface de l'application Autorité d'Enregistrement.....	35
4.2	Interface de l'application Autorité de Certification.....	40
4.3	Exemple illustratif .....	43
5	Conclusion.....	47
	<b>Conclusion générale et perspectives .....</b>	<b>48</b>
	<b>Références.....</b>	<b>49</b>
	<b>Annexe.....</b>	<b>51</b>