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 : Examinateur.

Promotion 2011/ 2012

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

DEDICACE

A NOS CHERS PARENTS, A NOS FEMMES ET ENFANTS.

QUE DIEU LES GARDE.

BIBLIOTHEQUE DU CERIST

Remerciements

Nous adressons nos vifs remerciements à **Mr NOUALI Omar** et **Mme CHALLAL Zakia**, nos encadreurs et enseignants au CERIST pour leur entière disponibilité, leurs conseils, leurs encouragements et surtout leur modestie.

Nous tenons à remercier **Mme Taboudjemet-Nouali Nadia** d'avoir accepté de présider cet honorable jury.

Nous remercions aussi **Mme Bessai F-Zohra** et **Mr Seba Abderazek** pour nous avoir fait l'honneur d'examiner notre travail.

Nous remercions notamment tous nos enseignants au CERIST pour nous avoir enchéri nos connaissances dans le domaine de la sécurité informatique.

Nous remercions toutes les personnes qui nous ont aidées afin que nous puissions réaliser ce travail.

Enfin, nous remercions aussi toute l'équipe de l'administration de la formation pour leur entière disponibilité.

BIBLIOTHEQUE DU CERIST

RESUME

Depuis quelques années, l'accès à Internet à 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.

BIBLIOTHEQUE DU CERIST

Sommaire

Introduction générale.....**1-2**

Chapitre 1 : Notions fondamentales sur la cryptographie

1 Introduction ……..……..**3**

2 Cryptographie……...……...…….……...**3**

2.1 Définition…….…….……..**3**

2.2 Historique…….……**4**

2.3 Besoins cryptographiques…….……**4**

2.3.1 Authentification…….…….……..**4**

2.3.2 Confidentialité…….……..**4**

2.3.3 Intégrité…….**4**

2.3.4 Non répudiation…….……...**4**

2.4 Les méthodes de cryptographie…….**5**

2.4.1 Cryptographie à clé secrète……...**5**

2.4.2 Cryptographie à clé publique…….....**7**

2.4.3 Hachage…….……...**9**

2.4.4 Signature numérique…….…….……...**10**

3 Secure Socket Layer « SSL»…….……**12**

3.1 Fonctionnement du SSL…….……**12**

3.2 Applications du SSL…….……..**12**

4 Conclusion……..……..**13**

Chapitre 2 : Infrastructure à clé publique

1 Introduction……...……**14**

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**

BIBLIOTHEQUE DU CERIST

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

Conclusion générale et perspectives 48

Références.....49

Annexe.....51

BIBLIOTHEQUE DU CERIST