

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



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

Thème

**Conception et Déploiement d'une PKI pour
sécuriser la messagerie électronique**

Réalisé par:

- HADDADJI Samir
- MEHADA Issam

Encadré par :

- Dr. NOUALI Omar

Soutenu devant le juré composé de :

- | | | |
|--------------------------|------------------------------|------------|
| - Dr. BESSAI Fatma Zohra | Maitre de Recherche, CERIST | Présidente |
| - Mr. KHOUATMI Fouad | Attaché de Recherche, CERIST | Examineur |
| - Mr. SAIDI Ahmed | Chargé d' Etudes, CERIST | Examineur |

-Promotion 2012/2013-

Remerciements

Nous remercions, en premier lieu, Dieu le tout puissant de nous avoir donné le courage et la puissance pour terminer ce travail.

Nous exprimons nos profonds remerciements et reconnaissances à **Monsieur NOUALI Omar** pour les nombreux conseils et orientations qui nous ont été très précieux au cours de la réalisation de ce travail.

Un merci tout particulier aux **membres de jury** d'avoir accepté de juger notre travail et nous avoir honoré par leur présence et pour nos enseignants de la PGS pour nous avoir enseigné, aidé et dirigé tout au long de cette formation.

Nous tenons à remercier nos responsables en l'occurrence **Mr. MALEK Lounes** et **Mr.MAAKOUF Zineddine** pour nous avoir donné l'occasion de suivre cette formation.

En fin, que tous ceux qui ont, de près ou de loin, contribué à l'élaboration de ce travail, particulièrement Messieurs : **GUERGUER Samir, MOKHTARI Hamid, SELMANI Haider, BOUCHAREB Farid, BOUKRICHE Mohamed-Amine, SADOUNE Ahmed, BOUKHOBZA Brahim, NIAR Hocine, DAHRIB Hakim, HADDAD Sofiane** et **TAFAT Adel**, trouvent ici l'expression de notre profonde reconnaissance.

Dédicaces

A mes chers parents qui ont sacrifié pour m'instruire, pour leur amour et leur soutien, c'est grâce à eux que Je suis devenu ce que je suis, à ceux que j'aime, particulièrement mes sœurs et frères, mon épouse et mes deux enfants Razane et Abderrahmane, je dédie ce modeste travail.

Samir

Dédicaces

A mes chers parents qui ont souffert pour m'éduquer et qui ont sacrifié pour m'instruire, c'est grâce à eux que je suis devenu ce que je suis. A ceux que j'aime, mon frère Sami et ma femme, je dédie ce modeste travail.

Issam

Résumé

La messagerie électronique est un moyen moderne d'échange d'informations offrant la possibilité d'augmenter la rapidité des communications, de diffuser massivement des informations, d'éliminer des opérations de paperasserie, par ailleurs la mise en œuvre d'une politique de protection de ce système est primordiale pour faire face aux multiples risques de sécurité des messages échangés.

L'exploitation des outils de cryptographie garantit les deux aspects de la sécurité des messages électroniques, à savoir, la confidentialité et l'intégrité, les deux autres aspects, à savoir, l'authenticité et la non-répudiation, nécessitent l'instauration d'une confiance au sein du système de messagerie à travers l'implication d'une tierce partie garantissant la correspondance et la concordance entre une identité électronique et l'identité réelle.

Une infrastructure PKI (Public Key Infrastructure) est la méthode la plus adaptée pour instaurer cette confiance et assure la sécurité des communications lors de l'échange de messages électroniques.

Microsoft Windows server permet l'intégration d'une PKI supportant les algorithmes et les outils cryptographiques les plus solides à l'aide de son service AD CS (Active Directory Certificate Services) et liant l'identité d'un utilisateur, d'un périphérique ou d'un service à une clé correspondante.

Sommaire

Introduction	01
I. Cryptographie, Notions de Base	
1. Introduction	03
2. Définitions	03
3. Principe générale de la Cryptographie	04
4. Les algorithmes Cryptographiques	05
4.1.La Cryptographie classique	05
4.1.1. Le code César	05
4.1.2. Le code Vigenère	05
4.1.3. La machine Enigma	06
4.2.La Cryptographie moderne	07
4.2.1. Les modes de chiffrement	07
4.2.2. La Cryptographie conventionnelle (Symétrique)	09
4.2.3. La Cryptographie Asymétrique (à clé publique)	12
4.2.4. Le système de Cryptage Hybride	15
4.2.5. Les algorithmes de calcul d'empreinte	16
4.2.6. Signature Numérique	17
5. Protocole	20
5.1.SSL (Secure Socket Layer)	20
5.1.1. Fonctionnement de SSL	20
5.1.2. Application SSL	20
5.2.S/MIME	21
6. Objectif de la Cryptographie	21
6.1.Authentification	21
6.2.Confidentialité	22
6.3.Intégrité	22
6.4.Non Répudiation	22
II. L'infrastructure à clés publiques	
1. Introduction	23
2. Notion de Certificat Numérique	23
2.1.Classification des Certificats Numériques	24
2.2.Normalisation des Certificats Numériques	24
3. Infrastructure à clés publiques	25
3.1.Les entités d'une PKI	25

3.2. Architecture d'une PKI	27
3.2.1. Architecture simple	27
3.2.2. Architecture hiérarchique	27
3.2.3. Architecture hybride	28
3.3. Cycle de vie d'un certificat émis par une PKI	28
3.4. Services d'une PKI	29
3.4.1. Enregistrement d'un Client	29
3.4.2. Génération d'une paire de clé	29
3.4.3. Création d'un Certificat	30
3.4.4. Renouvellement d'un Certificat	30
3.4.5. Révocation d'un Certificat	30
3.4.6. Recouvrement d'une clé privée	31
3.4.7. Publication de certificat	32

III. Conception de la PKI

1. Etude de l'existant	33
1.1. Présentation de l'entreprise	33
1.2. Topologie du réseau informatique existant	33
1.3. La messagerie électronique de l'entreprise	34
1.4. Schéma de la plateforme active directory et exchange	34
1.5. L'évolution de la messagerie électronique de l'entreprise	35
2. Conception de la PKI de l'entreprise	36
2.1. La configuration logique	37
2.1.1. Architecture de l'Autorité de Certification	37
2.1.2. Type de l'Autorité de Certification	38
2.1.3. Algorithmes cryptographiques	39
2.1.4. Longueurs des clés	39
2.1.5. Durées de validités des certificats	39
2.1.6. Déploiement du certificat de la CA racine	40
2.1.7. Accès aux informations de l'Autorité de Certification	41
2.1.8. Demande et déploiement des certificats	42
2.1.9. Révocation de certificats	42
2.1.10. Gestion de la PKI	44
2.1.11. Sécurité de l'Autorité de Certification	44
2.2. Configuration physique	47
2.2.1. Matériel	47
2.2.2. Disponibilités	50

IV. Mise en œuvre de la PKI

1. introduction	51
2. Mise en œuvre de la PKI	52
2.1.Installation et configuration de l'Autorité de Certification racine (CA ROOT)	52
2.2.Installation et configuration de l'Autorité de Certification Emettrice (CA Entreprise)	61
2.3.Soumission de la demande de certification de la CA émettrice à la CA ROOT	62
2.4.Copiage de deux certificats CA ROOT et CA Emettrice dans la CA Emettrice	67
2.5.Etablissement et déploiement des certificats	67
2.6.Configuration des clients Outlook	70
3. Tests de fonctionnement	72
Conclusion et perspectives	78
Bibliographie	
Liste de figures	