

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:

**Étude pratique et déploiement d'une
infrastructure à clé publique Windows au
niveau d'une entreprise nationale**

Présenté par : Mr Sayah Tarek

Encadré par : Dr. Nouali Omar

Devant le jury :

Dr. Tandjaoui Djamel

Président

Mme. Benmeziane Souad

Examinatrice

Mme. Bessai Fatma Zohra

Examinatrice

Promotion 2005/2006

TH. 5721

Remerciements

Je tiens à remercier dieu pour tous ce qu'il m'a offert.

Je remercie tout particulièrement et chaleureusement Dr. Nouafi Omar, pour son encadrement, sa collaboration totale, sa patience, sa présence, ses conseils très précieux, son dévouement et sa disponibilité à l'élaboration et à la rédaction de ce travail ;

Je voudrais remercier aussi :

- Le Pr. Khelladi Abdelkader, directeur du Cerist, de nous avoir accepter dans son établissement;*
- Le Dr. Tandjaoui Djamel, d'avoir eu la gentillesse de présider la soutenance ;*
- Mme Benméziane Souad et Mme Bessai Fatma Zohra de m'avoir enseigné et d'avoir accepté d'être examinatrices ;*
- Tous mes collègues de la promotion 2005/2006 pour la bonne ambiance de travail qui régnait dans la classe ;*
- Tout le personnel du Cerist, spécialement celui du service Formation et Relations extérieures ;*
- Tout le personnel de la DRGE ;*
- Tous ceux qui ont participé de près ou de loin à la réalisation de ce travail. Merci à tous mes amis, mes proches et surtout tous les membres de ma famille, mes parents en premier, et ma femme qui m'a beaucoup encouragé, ainsi que mes deux filles qui ont participé à leur manière à l'élaboration de ce travail.*

Sommaire

Introduction	1
I Concepts de base de la cryptographie	3
1 La cryptographie.....	3
2 La cryptographie à clé symétrique.....	4
3 La cryptographie à clé asymétrique / publique	5
4 Signatures numériques.....	6
5 Cryptage hybride de données	8
6 Protocoles.....	8
6.1 S/MIME	9
6.2 SSL.....	9
6.3 SET	10
6.4 IPSec	11
6.5 LDAP.....	12
II Sécurité des messages par la cryptographie à clé publique	14
1 Signatures numériques des messages.....	14
2 Chiffrement des messages	16
3 Signature numérique et chiffrement des messages.....	19
III Infrastructure à clé publique de Microsoft Windows	24
1 Infrastructure à clé publique.....	24
1.1 Organisation d'une PKI	24
1.2 Les certificats.....	25
1.3 Les autorités de certification.....	26
1.4 Autorité d'Enregistrement.....	27
1.5 Annuaire de publication.....	27
1.6 Normes et standards.....	27
2 Infrastructure à clé publique Windows.....	32
2.1 Composants de l'infrastructure à clé publique Windows.....	32
2.2 Services de certificats Microsoft.....	36
2.3 Types d'autorités de certification	37
2.4 Hiérarchie d'autorités de certification	38
2.5 Demandes de certificats	43
2.6 Les Magasins de certificats.....	45
2.7 Révocation de certificats.....	47
2.8 Archivage et récupération des clés	49

IV Étude et déploiement d'une PKI	53
1 Présentation générale du réseau de l'entreprise	53
2 Définition du besoin	54
3 Approche proposée	54
4 Implémentation des différentes ACs	55
4.1 Implémentation de l'AC Racine	55
4.2 Configuration des propriétés.....	58
4.3 Implémentation de l'AC Emettrice.....	58
4.4 Configuration des propriétés de l'autorité de certification émettrice	60
5 Choix du modèle de certificat	61
6 Configuration de l'archivage de clés pour l'AC émettrice	63
6.1 Certificats de récupération de clés	63
6.2 Agent de récupération de clés	64
6.3 Archivage de clés.....	66
7 Configuration des postes utilisateurs	69
7.1 Demande de certificats clients	69
7.2 Configuration de Outlook Express	73
Conclusion	76
Bibliographie.....	77