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 de fin d'études pour l'obtention du diplôme de

Post-Graduation Spécialisée en Sécurité Informatique

Thème

DEPLOIEMENT D'UNE INFRASTRUCTURE DE CERTIFICATION AVEC L'OUTIL OPEN SOURCE EJBCA

Présenté par : *Mr Aissa Toufik* Encadreur : *DrOmar Nouali* *Mr ToumiSidali*

Organisme d'accueil : CERIST

Soutenue le : , devant le jury composé de :

Mme DR NOUALI-TABOUDJEMAT NADIA	Présidente
Mme ZEGHILET HOUDA	Examinatrice
Mr KRINAH ABDELGHANI	Examinateur

2012/2013

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

DEPLOIEMENT D'UNE INFRASTRUCTURE DE CERTIFICATION AVEC L'OUTIL OPEN SOURCE EJBCA

BIBLIOTHEQUE DU CERIST

Résumé

Une **PKI P**ublic **K**ey **I**nfrastructure ou **ICP** (en français) est un système permettant la gestion de certificats numériques, un tel certificat permet d'identifier aussi bien des machines que des personnes. Les certificats ont de nombreuses applications, ils peuvent être utilisés pour sécuriser les échanges avec un serveur web (**HTTPS**) mais aussi de signer et chiffrer ses courriers électroniques.

Le rôle d'une infrastructure de gestion de clés et donc permettre la création de tels certificats mais aussi leur destruction appelée révocation, les certificats sont normalisés et peuvent prendre plusieurs formes la plus courante est la norme **X509**.

L'objectif de ce travail est de mettre en proposition une infrastructure de gestion de clés à partir d'un outil en open source (**EJBCA**) au profit d'un organisme national.

Mots clés: **PKI**, **ICP**, **EJBCA**, **X509**, **AC**, **Certificat numérique**.

BIBLIOTHEQUE DU CERIST

REMERCIEMENTS

NOUS COMMENCONS PAR REMERCIER

DR NOUALI OMAR QUI NOUS A PROPOSE, SOUTENU ET ENCOURAGE A REALISER CE TRAVAIL

NOUS REMERCIONS AUSSI TOUTE L'EQUIPE PEDAGOGIQUE QUI A CONTRIBUE A NOTRE FORMATION.

NOUS REMERCIONS ENSUITE TOUS LES MEMBRES DE JURY QUI ONT ACCEPTE DE JUGER NOTRE TRAVAIL.

NOUS REMERCIONS EGALEMENT

L'EQUIPE DE LA DIRECTION DE LA FORMATION POUR LEURS DISPONIBILITE ET LEURS DEVOUILLEMENT

NOS DERNIERS REMERCIEMENTS REVIENNENT A LA PROMOTION PGS EN SECURITE INFORMATIQUE 2012/2013

Sommaire

Introduction générale **1**

Partie I : Etat de l'art

Chapitre I : Gestion des clés publiques **4**

1. Cryptographie 4

2. Mécanismes cryptographiques 4

2.1 Chiffrement 4

2.2 Fonction de hachage 5

2.3 Signature numérique 5

3.Familles d'algorithmes cryptographiques 6

3.1 Algorithmes symétriques (à clé secrète) 6

3.2 Algorithmes asymétriques (à clé publique) 7

4 Normes et standards 8

4.1 IETF PKIX 9

4.2 RSA PKCS 10

4.3 ITU-T 11

Chapitre II :L'infrastructure à clé publique (ICP) **12**

1.Introduction 12

2.Composantes de l'ICP 13

3.Services de gestion offerts par l'ICP 15

4. Services de sécurité offerts par l'ICP 16

5. Protocoles de l'ICP 17

5.1 OCSP (OnlinecertificateStatus Protocol) 17

5.2 PKIX-CMP (Certificate Management Protocol) 18

5.3 SCEP (SimpleCertificateEnrollment Protocol) 18

5.4 XKMS (XML Key Management Specification) 18

5.5 TSP (TimeStampprotocol) 19

BIBLIOTHEQUE DU CERIST

6.Certificat à clé publique 19

6.1 Classes de certificats 21

6.2.Nommage 22

6.3 Extensions 24

6.4 Gestion de cycle de vie des clés et des certificats 24

6.4.1Phase « Initialisation » 25

6.4.1.1 Enregistrement 25

6.4.1.2 Génération de la paire de clés 26

6.4.1.3 Création du certificat 26

6.4.1.4 Dissémination du certificat 26

6.4.1.5 Sauvegarde de la clé 26

6.4.2Phase « Emission » 26

6.4.2.1 Récupération du certificat 26

6.4.2.2 Validation du certificat 27

6.4.2.3 Recouvrement des clés 27

6.4.2.4 Mise à jour des clés 27

6.4.3Phase «Annulation » 27

6.4.3.1 Expiration du certificat 27

6.4.3.2 Révocation du certificat 27

6.4.3.3 Historique des clés 27

6.4.3.4 Archive des clés 28

7.Notion de confiance 28

8.Politiques 28

8.1Politique de certification (CP) 28

8.2Enoncé des pratiques de certification (CPS) 28

9.Composantes Physiques 29

9.1Equipement Informatique 29

BIBLIOTHEQUE DU CERIST

9.2 Module de sécurité *29*

Chapitre III :La solution PKI avec EJBCA **30**

1.Introduction 30

2. RSA Digital certificate Solution 30

3.EntrustAuthority 32

4.EJBCA 35

4.1 Architecture applicative d'EJBCA 35

4.2 Architecture fonctionnelle d'EJBCA 37

5.Observation 39

6. Conclusion *40*

Partie II : Proposition d'une conception et réalisation d'une ICP

Chapitre IV : Infrastructure de certification proposée **41**

1.Introduction 41

2.Logiciels libres requis 42

2.1 Linux (distribution au choix) 43

2.2 EJBCA *43*

2.3Jboss 43

2.4 Java SE Development Kit 43

2.5MySql 43

2.6 Apache DS 44

2.7SignServer 44

2.8 Apache http Server 44

2.9 Mod-Security 44

3. Configuration logicielle des serveurs 45

4. Proposition d'un modèle réseau sécurisé 45

5. Modèle de confiance 47

6. Gestion des clés cryptographiques 48

BIBLIOTHEQUE DU CERIST

7. Fonctions de hachage 49

8. Génération des clés 49

9.Utilisations des clés 50

10.Période de validité des certificats 51

Chapitre V : Réalisation de l'ICP **56**

1.Description de l'environnement *56*

2. Configurations logicielles *57*

3.Architecture de la PKI 58

4.Création des entités dans la PKI 60

5.Génération et installation des certificats SSL 61

6. Certificat SSL du serveur Web 61

7.Certification du client dans le fureteur web FireFox 65

7.1 Activation de l'authentification client par certificat *70*

8. Conclusion 72

Conclusion Générale *73*

Bibliographie

BIBLIOTHEQUE DU CERIST