

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

Une architecture d'infrastructure de certification de clefs
pour les entreprises dans un environnement Cloud basée sur
des solutions open sources

Réalisé par :

CHEKKOUF Mohamed El Ouard

Encadré par :

Dr. NOUALI Omar

Soutenu devant le juré composé de :

- Mr. BOUCENNA Fateh

- Mr. KHEMISSA Hamza

Président

Examineur

Promotion 2018-2019

Résumé

Le Cloud computing est un modèle qui permet un accès omniprésent, pratique et à la demande à un réseau partagé et à un ensemble de ressources informatiques configurable (NIST).

Il est composé de cinq (5) caractéristiques essentielles, de trois (3) modèles de services et de quatre (4) modèles de déploiement.

Une Infrastructure à Clés Publiques (ICP) est un ensemble de moyens matériels, logiciels et organisationnels nécessaires pour déployer à grande échelle un système cryptographique basé sur les certificats X509.

Un des principaux rôles de l'Infrastructure à Clés Publiques (ICP) est de s'acquitter de la gestion complète du cycle de vie des clés et des certificats.

Les certificats ont de nombreuses applications, ils peuvent être utilisés pour sécuriser les échanges avec un serveur web (HTTPS), signer et chiffrer des courriers électroniques.

L'objectif de ce travail est de mettre en proposition une architecture d'infrastructure de certification de clés pour les entreprises dans un environnement Cloud basée sur des solutions open sources.

Entreprise Java Bean Certification Authority EJBCA (produit d'ICP sous licence LGPL) a été choisi comme outil pour la réalisation de notre ICP.

Mots clés : *Cloud computing, ICP, X509, EJBCA, AC, AE, Certificat numérique...*

Tables des matières

Table des matières	4
Liste des figures	7
Liste des tableaux	9
Abréviations	10
Introduction	12
Chapitre I : Cloud Computing	14
I.1 Introduction.....	14
I.2 Description du Cloud Computing.....	14
I.3 Caractéristiques.....	15
I.4 Les différents services du Cloud Computing.....	15
I.4.1 Logiciel en tant que service (SaaS).....	16
I.4.2 Plateforme en tant que service (PaaS).....	16
I.4.3 Infrastructure en tant que service (IaaS).....	16
I.4.4 Avantages et Inconvénients des services.....	17
I.5 Types de Cloud Computing.....	18
I.5.1 Cloud privé.....	18
I.5.2 Cloud public.....	18
I.5.3 Cloud hybride.....	18
I.5.4 Cloud communautaire.....	18
I.6 Architecture du Cloud Computing.....	19
I.7 Avantages du Cloud Computing.....	20
I.8 Inconvénients du Cloud Computing.....	21
I.9 Les grands défis relatifs à l'adoption du Cloud Computing.....	21
I.9.1 Sécurité.....	21
I.9.2 Tolérance aux fautes et disponibilité.....	21
I.9.3 L'équilibrage de charge.....	22
I.10 Conclusion.....	22
Chapitre II : Gestion des clés publiques	23
II.1 Rappels sur la cryptographie	23
II.1.1 Chiffrement/déchiffrement.....	24
II.1.2 Les clés.....	24
II.1.3 Les familles cryptographiques.....	24
II.1.3.1 Cryptographie symétrique.....	25
II.1.3.2 Cryptographie asymétrique.....	25
II.1.4 Fonction de hachage.....	27
II.1.5 Signature numérique.....	27
II.1.6 Certificats numériques.....	29
II.1.6.1 Contenu d'un certificat.....	29
II.1.6.2 Types de certificat.....	30
II.1.6.3 Classification des Certificats.....	30

II.2 Infrastructure à clés publiques.....	31
II.2.1 Les composants d'une ICP.....	31
II.2.2 Répartition des AC	33
II.2.2.1 Modèle hiérarchique	33
II.2.2.2 Modèle croisé (Peer-to-Peer).....	33
II.2.2.3 Modèle en graphe	34
II.2.3 La gestion du cycle de vie des clés et des certificats.....	34
II.2.3.1 Phase Initialisation.....	34
II.2.3.1.1 Enregistrement.....	34
II.2.3.1.2 Génération de la paire de clés.....	35
II.2.3.1.3 Création du certificat et distribution de la clé du certificat.....	35
II.2.3.1.4 Dissémination du certificat.....	35
II.2.3.1.5 Sauvegarde de la clé.....	36
II.2.3.2 Phase Emission	36
II.2.3.2.1 Récupération du certificat.....	36
II.2.3.2.2 Validation du certificat.....	36
II.2.3.2.3 Recouvrement de clés.....	36
II.2.3.2.3 Mise à jour des clés.....	36
II.2.3.3 Phase Annulation.....	36
II.2.3.3.1 Expiration du certificat.....	36
II.2.3.3.2 Révocation du certificat.....	36
II.2.3.3.3 Historique des clés.....	37
II.2.3.3.4 Archive de clés.....	37
II.2.4 La politique d'une ICP.....	37
II.2.5 Annuaire.....	37
II.2.5.1 Définition.....	37
II.2.5.2 Annuaire et ICP.....	37
II.2.5.3 Protocole d'accès au répertoire	38
II.2.5.3.1 X.500.....	38
II.2.5.3.2 LDAP (Lightweight Directory Access Protocol)	38
II.3 Conclusion.....	39
Chapitre III : Les outils de développement d'ICP.....	40
III.1 Solutions propriétaires.....	40
III.1.1 RSA Digital Certificate Solution.....	40
III.1.2 Entrust Authority.....	42
III.1.3 TrustyKey.....	44
III.2 Solutions open-source.....	46
III.2.1 IDX-PKI.....	46
III.2.2 EJBCA.....	49
III.3 Conclusion.....	53
Chapitre IV : Proposition d'une solution ICP dans un environnement Cloud.....	54
IV.1 Déploiement des ICP	54
IV.1.1 En interne.....	54
IV.1.2 En Externe (cloud)	56
IV.1.3 Hybride (sur site et cloud)	58

**Une architecture d'infrastructure de certification de clés pour les entreprises
dans un environnement Cloud basée sur des solutions open sources**

IV.2	Logiciels libres requis.....	61
IV.2.1	Linux (distribution au choix)	62
IV.2.2	EJBCA.....	62
IV.2.3	Jboss.....	62
IV.2.4	Java SE Development Kit.....	62
IV.2.5	MySQL.....	62
IV.2.6	ApacheDS.....	62
IV.2.7	SignServer.....	62
IV.2.8	Apache http Server	63
IV.2.9	ModSecurity.....	63
IV.3	Organisation des composantes.....	63
IV.3.1	Configuration logicielle des serveurs.....	63
IV.3.2	Répartition des serveurs sur le réseau.....	64
IV.4	Modèle de confiance.....	66
IV.5	Gestion des clés cryptographiques.....	66
IV.6	Fonction de hachage.....	67
IV.7	Génération des clés.....	67
IV.8	Utilisation des clés.....	67
IV.9	Période de validité des certificats.....	68
IV.10	Conclusion.....	69
Chapitre V Réalisation d'une solution ICP open source pour une entreprise.....		70
V.1	Description de l'environnement	70
V.2	Configurations logicielles.....	71
V.3	Configuration Initiale d'EJBCA.....	72
V.3.1	Connexion au module d'administration.....	72
V.3.2	Configuration du Système.....	73
V.3.3	Création d'interfaces de publication	74
V.3.4	Création d'une CA Subordonnée.....	75
V.3.5	Création de modèle de certificat.....	76
V.4	Architecture de l'ICP.....	77
V.5	Création des entités dans l'ICP.....	79
V.6	Génération et installation des certificats SSL.....	80
V.6.1	Certificat SSL du serveur Web.....	80
V.7	Certificat du client dans le navigateur Web Firefox.....	84
V.8	Activation de l'authentification client par certificat.....	88
V.9	Conclusion.....	89
Conclusion Générale.....		90
Annexes.....		91
Normes et standards.....		91
Protocoles d'ICP.....		93
Bibliographie.....		95