



RAPPORT DU PROJET DE FIN D'ÉTUDES

Pour l'obtention du diplôme de

Poste Graduation Spécialisée en Sécurité Informatique

**Conception et développement d'une architecture
sécurisé de communication médecin-patient**

Réalisé par:

- BOUKOFFA Nabil
- BOUDEFFA Salah

Encadrer par:

- Mr DERKI Mohamed Saddek

Devant le jury composé de:

- | | |
|------------------------|------------|
| - Mme. ZEGHACHE Linda | Présidente |
| - M. KRINAH Abdelghani | Examineur |
| - M. BOUCENNA Fateh | Examineur |

Table des matières

Table des Matières	02
Liste des Figures.....	06
Introduction Générale.....	08
Chapitre I: La sécurité et le domaine de la santé	
1. Introduction	11
1.1 Définitions de l'e-Santé.....	11
1.2 L'e-santé dans la sphère de l'Internet des Objets et du Cloud Computing.....	12
1.3 Impacts attendus de l'e-Santé.....	13
1.4 Autres champs de l'e-Santé	14
2. Le dossier médical personnel.....	14
2.1 Intérêt du Dossier Médical Personnel.....	14
2.2 Dossier Médical Personnel Informatisé.....	15
2.3 Caractéristique du Dossier Médical Personnel Informatisé	15
2.4 Intérêt du Dossier Médical Personnel Informatisé.....	15
2.5 Dossier médical partagé.....	16
2.6 Intérêts du dossier médical partagé.....	16
3. La sécurité dans les systèmes e-santé	17
3.1 Sécurité des données personnelles de santé et préservation de la vie privée.....	17
3.1.1 Données à caractère personnel.....	17
3.1.2 Données à caractère sensibles.....	18
3.1.3 Traitement de données à caractère personnel.....	18
3.1.4 Les règles relatives au traitement automatisé des données à caractère personnel.....	18
4. Le contrôle d'accès.....	21
4.1 Définition.....	21
4.2 Définition d'une politique de contrôle d'accès.....	22
4.3 Modèles de contrôle d'accès.....	22
4.3.1 Contrôle d'accès discrétionnaires (DAC).....	22

4.3.1.1	Modèle de Lampson.....	23
4.3.2	Le contrôle d'accès obligatoire (MAC).....	24
4.3.3	Contrôle d'accès basé sur les rôles (RBAC).....	25
4.3.4	Contrôle d'accès basé sur les attributs (ABAC).....	27
4.3.5	Le contrôle d'accès par la cryptographie (ABE).....	29
5.	Conclusion.....	30
Chapitre II: Le Chiffrement par attributs (ABE)		
1.	Introduction.....	31
2.	Le Chiffrement par attributs (ABE).....	31
2.1	Les variantes principales du chiffrement basé sur les attributs (ABE).....	32
2.1.1	Chiffrement basé sur les attributs de stratégie de clé (KP-ABE).....	32
2.1.2	Chiffrement basé sur les attributs de stratégie de texte chiffré (CP-ABE).....	33
2.2	L'algorithme pour schéma ABE.....	34
2.3	Les critères d'un idéal schéma de cryptage basé sur les attributs.....	35
3.	Chiffrement basé sur les attributs de stratégie de texte chiffré (CP-ABE).....	36
3.1	Bref aperçu du CP-ABE.....	36
3.2	Structure d'accès.....	37
3.3	BilinearMaps.....	37
3.4	CP-ABE: Algorithmes fondamentaux.....	37
3.5	Avantages et inconvénients de CP-ABE.....	39
3.5.1	Avantages.....	39
3.5.2	Inconvénients.....	39
3.6	Domaines d'application du CP-ABE.....	40
3.6.1	Domaines d'e-santé (systèmes DSE).....	40
3.6.2	Internet des objets.....	41
3.6.3	Services Cloud.....	42
4.	Conclusion.....	43
Chapitre III: Conception		
1.	Introduction.....	44

2. Présentation de langage UML.....	44
2.1 Définition d'UML.....	44
2.2 Les différents types de diagrammes.....	44
2.2.1 Diagrammes statiques (structurels).....	44
2.2.2. Diagrammes dynamique (comportementaux).....	44
3. Le choix de la méthode.....	45
3.1 Définition du processus unifié (UP).....	45
3.2 Les caractéristiques du processus unifié.....	45
3.3 Cycle de vie du processus unifié.....	46
4. Architecture générale du projet	46
5. Diagramme de cas d'utilisation.....	47
5.1 Identification des acteurs.....	47
5.2 Identification des cas d'utilisations.....	47
5.3 Les cas d'utilisations de notre application.....	48
5.3.1 Patient.....	48
5.3.2 Médecin.....	48
6. Diagramme de séquence.....	49
7. Diagramme de classes.....	55
7.1 Identification des classes.....	55
7.2 L'association.....	55
7.3 Description des classes.....	55
7.4 Dictionnaire de données.....	56
7.5 Description des associations.....	57
8. Conclusion.....	58
Chapitre IV: Réalisation	
1. Introduction.....	59
2. Outils et langage utilisé.....	59
2.1 Environnement de réalisation.....	59
2.1.1 L'environnement matériel.....	59

2.1.2 L'environnement logiciel.....	59
2.1.2.1 Langage de programmation.....	59
2.1.2.2 Interfaces graphiques.....	61
2.1.2.3 Système de gestion de base de données.....	61
3. Réalisation du projet.....	62
3.1 L'Arborressance de l'application.....	62
3.2 Présentation des interfaces.....	63
3.2.1 Page d'accueil.....	63
3.2.2 Fenêtre login.....	64
3.2.3 Fenêtre principale.....	64
3.2.4 Admin.....	74
4 Conclusion.....	74
Conclusion Générale et perspectives.....	75
Référence Bibliographique.....	76