Cahier des Charges

1. Description Générale

1.1 Intention et Portée du Projet

1.1.1 Objectif Principal

Le projet vise à mettre en place un système de transfert sécurisé d'images en utilisant l'algorithme AES, permettant ainsi la protection des données sensibles lors de la transmission sur des réseaux.

1.1.2 Objectifs Spécifiques

- **Chiffrer les images avant leur transmission :** Utiliser l'algorithme AES pour garantir la confidentialité des données pendant la transmission.
- **Assurer la confidentialité des images pendant le transfert :** Éviter toute interception ou accès non autorisé aux images pendant leur transfert.
- **Permettre la récupération des images d'origine à la réception :** Assurer que le destinataire peut déchiffrer les images et les restaurer dans leur état d'origine.

1.2 Contexte d'Entreprise

1.2.1 Situation Actuelle

Avec la prolifération des dispositifs électroniques en Tunisie, la sécurisation des données devient cruciale. Ce projet émerge dans le contexte de renforcer la confidentialité des images échangées, répondant ainsi aux préoccupations actuelles en matière de sécurité.

1.3 Parties Prenantes

1.3.1 Internes

- **Équipe de développement :** Responsable de la conception, du développement et de la mise en œuvre du système.
- **Responsables informatiques :** Garants de la sécurité et de l'intégration du système dans l'infrastructure existante.

1.3.2 Externes

- **Utilisateurs finaux :** Personnes utilisant le système pour le transfert sécurisé d'images.
- **Autorités réglementaires :** Entités responsables de l'approbation et de la conformité aux régulations en vigueur.

1.4 Idée de la Solution

1.4.1 Méthode de Sécurité

L'algorithme AES (Advanced Encryption Standard) sera utilisé pour chiffrer les images, assurant ainsi un niveau élevé de sécurité.

1.4.2 Bénéfices

- **Transfert sécurisé d'images confidentielles :** Réduction des risques de divulgation non autorisée.
- **Application potentielle dans les domaines médical et militaire :** Possibilité d'utiliser le système dans des secteurs sensibles nécessitant une sécurité renforcée.

1.5 Plan du Document

2. Services du Système

2.1 Portée du Système

2.1.1 Utilisateurs Cibles

Les utilisateurs visés comprennent les professionnels médicaux, les militaires et toute personne nécessitant un transfert sécurisé d'images.

2.1.2 Fonctionnalités Complémentaires

- **Gestion des clés de chiffrement :** Le système devra fournir des mécanismes permettant de générer, stocker et gérer les clés de chiffrement utilisées pour sécuriser les images. Cela inclut la possibilité de partager les clés de manière sécurisée avec les destinataires autorisés.
- **Audit et journalisation :** Le système devra être capable de suivre et d'enregistrer les activités liées au transfert d'images, y compris les opérations de chiffrement, de déchiffrement et de transmission. Cela permettra de garantir la traçabilité des actions effectuées sur les images.

2.2 Besoins Fonctionnels

2.2.1 Fonctionnalités Principales

- **Chiffrement des images :** Application de l'algorithme AES pour rendre les images illisibles pendant la transmission.
- **Déchiffrement des images :** Utilisation d'une clé de déchiffrement pour restaurer les images à leur état d'origine.
- **Transmission sécurisée sur le réseau :** Garantir la sécurité des images pendant le transfert.

2.2.2 Fonctionnalités Complémentaires

- **Compression des images :** Le système peut inclure une fonctionnalité de compression des images avant le chiffrement pour réduire la taille des fichiers et accélérer le transfert.
- **Notification de transfert :** Le système peut envoyer des notifications aux utilisateurs pour informer de la réussite ou de l'échec du transfert d'une image.
- **Gestion des erreurs :** Le système devra être capable de gérer les erreurs qui peuvent survenir pendant le transfert, en les signalant aux utilisateurs et en prenant les mesures appropriées pour résoudre les problèmes.

3. Contraintes du Système

3.1 Contraintes d'Interface

3.1.1 Interface Utilisateur

Une interface conviviale basée sur Python et Tkinter sera mise en place pour faciliter l'interaction des utilisateurs avec le système.

3.2 Contraintes de Performance

3.2.1 Taille des Images

Pour assurer une performance optimale, la taille des images ne doit pas dépasser 5 Mo, évitant ainsi des délais excessifs lors du chiffrement et du déchiffrement.

3.3 Contraintes de Sécurité

3.3.1 Clé de Chiffrement

La sécurité du système repose sur l'utilisation de clés de chiffrement. Le chiffrement et le déchiffrement ne peuvent avoir lieu qu'avec la même clé.

3.4 Contrainte Opérationnelle

3.4.1 Connexion Réseau

Le système suppose que l'émetteur et le récepteur sont connectés à un réseau pour permettre la transmission des images chiffrées.

3.5 Contraintes Politiques et Légales

3.5.1 Conformité aux Lois Tunisiennes

Le système doit être développé et utilisé en conformité avec les lois et régulations tunisiennes en matière de protection des données.

4. Éléments du Projet

4.1 Planning Préliminaire

4.1.1 Phases du Projet

1. **Analyse des besoins (1 mois) :** Identification approfondie des exigences fonctionnelles et non fonctionnelles.
2. **Conception et développement (2 mois) :** Création de l'interface utilisateur, intégration de l'algorithme AES.
3. **Tests et validation (2 semaines) :** Vérification de la conformité aux spécifications.
4. **Déploiement (2 semaine) :** Mise en production du système.

4.2 Budget Préliminaire

4.2.1 Estimation des Coûts

Une estimation initiale des coûts pour le développement, les tests et le déploiement du système sera établie, tenant compte des ressources humaines, matérielles et logicielles nécessaires.

5. Appendices

5.1 Glossaire

- **AES (Advanced Encryption Standard) :** Algorithme de chiffrement symétrique.
- **Tkinter() :** Module Python pour la création d'interfaces graphiques.

5.2 Documents et Formulaires d'Entreprise

- **Politiques de sécurité de l'entreprise :** Directives internes concernant la sécurité des données.
- **Règlements internes :** Procédures internes à suivre pendant le développement et la mise en œuvre du système.

5.3 Références Bibliographiques

- D. Boneh, "Twenty Years of Attacks on the AES Cryptosystem." Journal of Cryptology, 2020.
- J. Daemen , V. Rijmen, “The Design of Rijndael, AES - The Advanced Encryption Standard”, Springer Berlin Heidelberg, 2020.
- W. Stallings, "Cryptography and Network Security: Principles and Practice", Pearson, 2020.
- NIST Special Publication 800-38A, "Recommendation for Block Cipher Modes of Operation: Methods and Techniques", National Institute of Standards and Technology, 2020