

## Rapport de la maquette de Chiffrement des cartes SD des tablettes

### Table des matières

1. INTRODUCTION.....	1
1.1. Le but du chiffrement des cartes SD sur les tablettes .....	1
1.2. Les contraintes techniques et l'approche retenue.....	2
1.3. Les fonctionnalités d'un conteneur chiffré.....	2
2. L'UTILISATION D'EDS LITE.....	3
2.1. Présentation d'EDS LITE .....	3
2.2. Fonctionnalités clés d'EDS LITE (version gratuite) .....	3
2.3. Configuration et utilisation .....	3
2.4. Les limites d'EDS LITE gratuit sur Android 7 .....	4
3. L'AUTOMATISATION DES TÂCHES AVEC MACRODROID .....	4
3.1. Présentation de MacroDroid .....	4
3.2. La macro utilisée .....	4
3.3. Le but stratégique de cette macro.....	5
4. CONCLUSION .....	5

## 1. INTRODUCTION

### 1.1. Le but du chiffrement des cartes SD sur les tablettes

Dans un environnement où la mobilité des équipements et la sensibilité des données sont croissantes, la protection des informations stockées sur les supports amovibles tels que les cartes SD est primordiale. Le chiffrement des cartes SD vise à :

- **Assurer la confidentialité des données :** Protéger les informations sensibles contre tout accès non autorisé en cas de perte, de vol ou de compromission de la tablette.
- **Garantir l'intégrité des données :** S'assurer que les informations n'ont pas été altérées ou modifiées de manière malveillante.

- **Répondre aux exigences réglementaires** : Se conformer aux diverses réglementations en matière de protection des données personnelles et professionnelles.
- **Réduire les risques** : Minimiser l'impact potentiel d'une fuite de données pour l'organisation.

## 1.2. Les contraintes techniques et l'approche retenue

Le développement de cette solution a pris en compte plusieurs contraintes techniques majeures :

- **Robustesse du chiffrement** : Nécessité d'utiliser des algorithmes cryptographiques reconnus et validés par les autorités compétentes (ex: ANSSI).
- **Facilité d'utilisation** : L'intégration doit être transparente et intuitive pour les utilisateurs finaux afin de minimiser la charge de formation et les erreurs humaines.
- **Performance** : Le chiffrement ne doit pas impacter significativement les performances d'utilisation de la tablette.
- **Évolutivité** : La solution doit permettre une adaptation future, notamment en termes de taille de stockage.

Pour répondre à ces contraintes, l'approche retenue combine la création de conteneurs chiffrés basés sur la cryptographie symétrique et l'automatisation des tâches de gestion de fichiers via une macro.

## 1.3. Les fonctionnalités d'un conteneur chiffré

Un conteneur chiffré est un fichier qui simule un disque dur virtuel. Ses principales fonctionnalités sont :

- **Isolation des données** : Toutes les données stockées à l'intérieur du conteneur sont chiffrées collectivement.
- **Accès contrôlé** : L'accès au contenu du conteneur est conditionné par la saisie d'un mot de passe ou d'une clé de chiffrement.
- **Montage/Démontage** : Le conteneur peut être "monté" (rendu accessible comme un lecteur standard) et "démonté" (rendu inaccessible et chiffré) à la demande.
- **Portabilité** : Le fichier conteneur peut être déplacé ou sauvegardé comme n'importe quel autre fichier, tout en conservant sa protection.

## 2. L'UTILISATION D'EDS LITE

### 2.1. Présentation d'EDS LITE

EDS LITE est une application mobile gratuite et open source conçue pour Android, permettant de créer et de gérer des conteneurs chiffrés. Elle est compatible avec le format "VeraCrypt", une référence en matière de chiffrement de disques et de conteneurs, reconnu pour sa sécurité et sa flexibilité. EDS LITE offre une interface utilisateur simplifiée pour interagir avec ces conteneurs directement sur l'appareil mobile.

### 2.2. Fonctionnalités clés d'EDS LITE (version gratuite)

La version gratuite d'EDS LITE offre les fonctionnalités essentielles pour notre besoin :

- **Création de conteneurs VeraCrypt** : Possibilité de générer des fichiers conteneurs de différentes tailles, sur la carte SD ou la mémoire interne.
- **Algorithmes de chiffrement robustes** : Supporte des algorithmes tels que AES-256, Twofish, Serpent, et des fonctions de hachage comme SHA-512, ce qui permet de se conformer aux recommandations de l'ANSSI.
- **Montage et démontage de conteneurs** : Permet d'ouvrir et de fermer les conteneurs chiffrés, les rendant accessibles ou sécurisés.
- **Accès aux fichiers** : Une fois monté, le conteneur apparaît comme un dossier accessible via un gestionnaire de fichiers, permettant de lire, écrire et modifier les données.

### 2.3. Configuration et utilisation

La configuration initiale implique la création d'un conteneur sur la carte SD. Lors de la maquette, une taille de 2 Go a été définie à des fins de test. Les algorithmes choisis sont AES-256 pour le chiffrement des données et SHA-512 pour la fonction de hachage, en ligne avec les directives de l'ANSSI.

L'utilisation quotidienne par l'agent est simplifiée :

1. L'agent ouvre l'application EDS LITE.
2. Il sélectionne le fichier conteneur situé sur la carte SD.
3. Il saisit le mot de passe défini pour déverrouiller le conteneur.
4. Le conteneur est monté et les données sont accessibles.

## 2.4. Les limites d'EDS LITE gratuit sur Android 7

Il est important de noter que l'utilisation de logiciels tiers sur des versions spécifiques d'Android peut présenter des limites. Des investigations complémentaires seraient nécessaires pour identifier précisément les éventuelles restrictions ou comportements inattendus d'EDS LITE sur Android 7, notamment en termes de gestion des permissions de stockage ou d'intégration avec le système de fichiers. À ce stade, aucune limitation majeure n'a été identifiée lors des tests initiaux, mais une analyse approfondie est recommandée avant un déploiement à grande échelle.

---

# 3. L'AUTOMATISATION DES TÂCHES AVEC MACROIDROID

## 3.1. Présentation de MacroDroid

MacroDroid est une application d'automatisation puissante pour les appareils Android. Elle permet aux utilisateurs de créer des "macros" qui sont des règles définies par un déclencheur (événement), une action (tâche à exécuter) et des contraintes (conditions spécifiques). Son objectif est de simplifier les tâches répétitives, d'améliorer la productivité et de personnaliser le comportement de l'appareil.

## 3.2. La macro utilisée

Une macro spécifique a été développée pour automatiser le processus de sécurisation des fichiers. Son fonctionnement est le suivant :

- **Surveillance active :** La macro est configurée pour surveiller en permanence les répertoires par défaut où sont stockés les téléchargements, les photos (par exemple, le dossier "DCIM") et les documents.
- **Déclencheur :** Chaque nouvelle modification ou création de fichier dans ces répertoires déclenche une action de la macro.
- **Actions conditionnelles :**
  - **Si le disque virtuel est déverrouillé (monté) :** La macro détecte les nouveaux fichiers (téléchargements, photos, documents) et les déplace automatiquement vers le répertoire du disque virtuel chiffré.
  - **Si le disque virtuel n'est pas déverrouillé (non monté) :** La macro est conçue pour supprimer automatiquement les nouveaux fichiers détectés dans les répertoires surveillés, empêchant ainsi leur stockage non chiffré.

- **Tests de validation :** Des tests rigoureux ont été effectués, notamment avec la capture de photos, confirmant que celles-ci sont bien redirigées et stockées *uniquement* sur le disque virtuel chiffré, sans laisser de traces sur le stockage non chiffré de la tablette.
- **Statut de la fonctionnalité de suppression :** Il est important de noter que la partie de la macro dédiée à la suppression automatique des fichiers lorsque le conteneur n'est pas déverrouillé n'est pas encore pleinement fonctionnelle et nécessitera un développement et des tests supplémentaires pour être opérationnelle et fiable.

### 3.3. Le but stratégique de cette macro

L'intégration de cette macro poursuit plusieurs objectifs stratégiques :

- **Simplification de l'expérience utilisateur :** Les agents n'ont pas à se soucier de déplacer manuellement les fichiers, réduisant ainsi la charge cognitive et le risque d'erreurs.
  - **Garantie de la sécurité par défaut :** En automatisant le transfert vers le conteneur chiffré, la solution assure que les données sensibles sont protégées dès leur création ou acquisition. La logique de suppression vise à empêcher toute donnée sensible de résider sur un espace non chiffré.
  - **Conformité automatique :** La macro aide à maintenir une conformité constante avec les politiques de sécurité des données, sans intervention active de l'utilisateur.
  - **Réduction des risques de fuite :** En s'assurant que les données sensibles ne résident jamais durablement sur un espace non chiffré (grâce au déplacement ou à la suppression), le risque de fuite est considérablement diminué.
- 

## 4. CONCLUSION

La solution de chiffrement des cartes SD proposée, s'appuyant sur EDS LITE et MacroDroid, offre une approche robuste et conviviale pour la protection des données sensibles sur les tablettes. Elle intègre des algorithmes cryptographiques reconnus et une automatisation intelligente pour minimiser les contraintes utilisateur tout en maximisant la sécurité.