

Explication détaillée du fichier CryptoManager.cs

But du fichier

Le fichier CryptoManager.cs est une classe statique qui permet de chiffrer (encrypt) et de déchiffrer (decrypt) des fichiers. Elle utilise l'algorithme AES (Advanced Encryption Standard) en mode 256 bits pour sécuriser les données.

Dans la version 3.0, cette classe a été améliorée pour fonctionner en mode 'Mono-Instance' grâce à un objet système appelé 'Mutex'. Cela signifie qu'une seule opération de chiffrement ou déchiffrement peut être exécutée à la fois sur la machine.

Fonctionnement global

1. La clé de chiffrement (Key) et le vecteur d'initialisation (IV) sont définis au début.
2. Deux méthodes publiques : EncryptFile et DecryptFile sont disponibles pour sécuriser ou ouvrir un fichier.
3. Un Mutex nommé "Global\EasySave_Crypto_Mutex" est utilisé pour empêcher plusieurs accès concurrents.
4. Toute opération de chiffrement/déchiffrement est protégée dans une méthode TryRunCryptoOperation.
5. Si une erreur survient ou si le mutex est déjà utilisé, le programme affiche un message clair à l'utilisateur.

Composants importants

- byte[] Key / IV : la clé et le vecteur utilisés pour chiffrer les fichiers (AES-256).
- Mutex : objet système qui permet de bloquer l'accès concurrent à une ressource partagée.
- EncryptFile / DecryptFile : méthodes principales pour chiffrer et déchiffrer un fichier.
- TryRunCryptoOperation : méthode privée qui sécurise l'accès et gère les erreurs.
- LogMutexRefused / LogCryptoError : méthodes qui affichent un message si un problème survient.

Pourquoi utiliser un Mutex (Mono-Instance) ?

Quand plusieurs sauvegardes s'exécutent en parallèle, il est dangereux de chiffrer plusieurs fichiers en

Explication détaillée du fichier CryptoManager.cs

même temps (risques de conflits, lenteur, plantages). Le Mutex garantit qu'une seule opération de CryptoSoft tourne à la fois, même si plusieurs threads ou programmes essaient de l'utiliser.

Cela protège l'intégrité des fichiers et améliore la stabilité.

Conclusion

CryptoManager.cs est un composant essentiel d'EasySave. En rendant le chiffrement mono-instance, il sécurise encore mieux le processus de sauvegarde, tout en informant l'utilisateur en cas de problème. Cette approche est propre, efficace et adaptée à un logiciel de production.