Cible de Sécurité CSPN

Produit TrueCrypt version 7.1a

Catégorie *Stockage Sécurisé*

Référence : ST-TrueCrypt_v7.1a-1.00

Date : le 15/01/2013

Siège : 4 bis Allée du Bâtiment • 35000 Rennes • France • **www.amossys.fr**
SIRET : 493 348 890 000 36 • **NAF** : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

FICHE D'ÉVOLUTIONS

RÉVISION	DATE	DESCRIPTION	RÉDACTEUR
1.00	15/01/2013	Création	JLR

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document constitue la cible de sécurité du produit TrueCrypt de la catégorie des produits de type « Stockage Sécurisé ».

1.2. DOCUMENTS DE RÉFÉRENCE

Référence	Titre
[CER-I-01.1]	*Méthodologie pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau*. N°1416/ANSSI/SR du 30 mai 2011.
[CER-I-02.1]	*Critères pour l'évaluation en vue d'une Certification de Sécurité de Premier Niveau*. N°1417/ANSSI/SR du 30 mai 2011.

1.3. GLOSSAIRE

Acronyme	Définition
AES	Advanced Encryption Standard (algorithme de chiffrement symétrique)
CRC	Cyclic Redundancy Check (somme de contrôle)
FAT	File Allocation Table (système de fichiers)
HMAC	Hash-based Message Authentication Code (code d'authentification de message reposant sur une fonction de hachage et une clé symétrique)
NTFS	New Technology File System (système de fichiers)
RIPEMD	RACE Integrity Primitives Evaluation Message Digest (famille de fonctions de hachage cryptographique)
SHA	Secure Hash Algorithm (famille de fonctions de hachage cryptographiques)
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing (mode opératoire de chiffrement par bloc utilisant deux clés)

2. IDENTIFICATION DU PRODUIT

Identification du produit évalué	
Nom de l'éditeur	TrueCrypt Foundation
Lien vers l'éditeur	www.truecrypt.org
Nom du produit	TrueCrypt
N° de version évaluée	7.1a (du 07/02/2012)
Catégorie du Produit	Stockage Sécurisé

3. DESCRIPTION DU PRODUIT

3.1. DESCRIPTION GÉNÉRALE DU PRODUIT

TrueCrypt est une application logicielle de protection de données de l'utilisateur, utilisée pour réaliser du chiffrement de masse. Le chiffrement est réalisé à la volée au niveau des partitions logiques des disques durs. Il peut être mis en œuvre pour chiffrer des supports amovibles et permettre ainsi l'échange sécurisé d'informations.

L'application est gratuite et open-source (distribution sous licence « TrueCrypt License Version 3.02 »), développée par TrueCrypt Fondation. Elle est basée initialement sur le logiciel E4M et sa première version date de février 2004. L'objectif principal est de protéger la confidentialité de l'information stockée en mémoire persistante en cas de vol ou de perte de la machine ou du support amovible.

TrueCrypt permet de gérer trois types de conteneurs chiffrés (volumes TrueCrypt) :

- les *conteneurs fichiers* qui sont des fichiers de taille variable définie par l'utilisateur, et d'extension quelconque. Un tel fichier peut être stocké sur n'importe quel support de données ;
- les *conteneurs partitions* qui sont des partitions physiques complètes qui font office de conteneur. Peuvent également être chiffrés suivant cette méthode, les disques durs entiers, les disques dur USB, les disquettes, les clés USB ou tout autre type de matériel de stockage de données ;
- la *partition système* ou tout le disque système. Il y a alors chiffrement de toute la partition contenant le système d'exploitation ; il faut déverrouiller le disque au boot pour pouvoir utiliser le système d'exploitation.

Globalement, TrueCrypt permet de :

- créer un disque virtuel chiffré (volume TrueCrypt ou conteneur) contenu dans un fichier ou sur une partition du disque dur et de le monter comme un disque physique réel ;
- chiffrer/déchiffrer de façon automatique, à la volée (i.e. en temps réel) et transparente ;
- chiffrer une partition entière (y compris le système d'exploitation, les fichiers temporaires, swap, etc.) ou un périphérique de stockage (clé USB ou disque dur) ;
- protéger les données selon deux niveaux :
    - via la création d'un volume normal chiffré ;
    - via la création d'un volume caché (difficile à détecter) permettant le déni plausible. En effet, le volume chiffré caché est créé à la fin d'un volume normal chiffré. Etant donné, qu'un volume chiffré TrueCrypt s'apparente à l'aléa, il n'est pas possible de détecter la présence d'un volume caché. Le mot de passe du le volume chiffré caché doit être différent de celui utilisé pour le volume normal.

Lors de la création d'un conteneur chiffré, plusieurs algorithmes cryptographiques sont à spécifier par l'utilisateur. L'étape de « Formatage du volume » correspond à la génération des clés indispensables au chiffrement du volume, sur un modèle le plus aléatoire possible, sans utiliser la fonction pseudo aléatoire du système d'exploitation hôte. Les formatages FAT et NTFS sont supportés.

Le chiffrement du volume opère par bloc suivant le mode XTS dit « tweakable », nécessitant deux clés symétriques de même longueur :

- une clé de chiffrement ;

- une clé permettant le calcul du tweak.

La Figure 1 illustre le fonctionnement global de TrueCrypt.

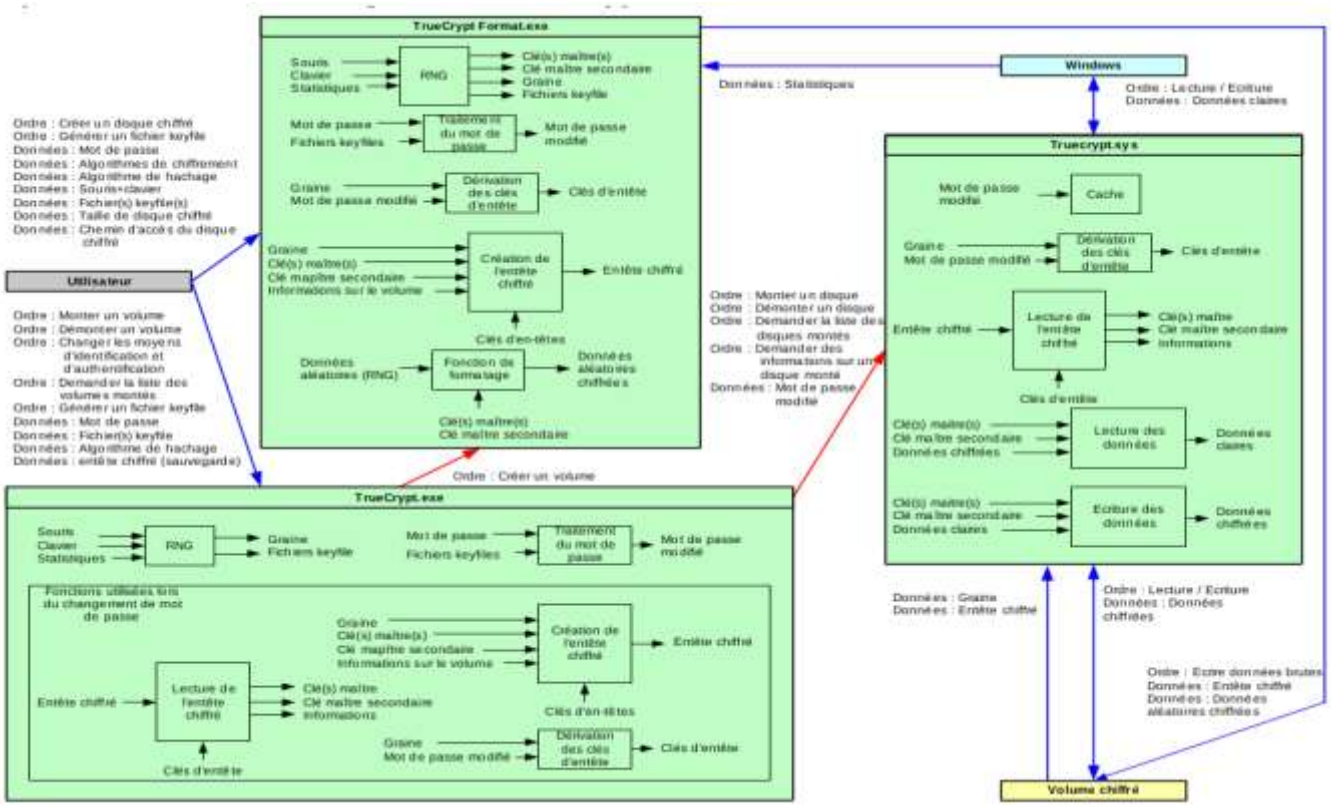

Figure 1 - Fonctionnement de la TOE

Pour assurer ses services, TrueCrypt requiert quatre clés symétriques de 256 bits :

- une **clé maîtresse** utilisée pour le chiffrement/déchiffrement des données écrites/lues dans un volume TrueCrypt ;
- une **clé d'entête**, de même taille, utilisée pour chiffrer/déchiffrer la zone chiffrée de l'entête d'un volume chiffré (contenant notamment la clé maitresse et sa clé secondaire associée) ;
- **deux clés secondaires** (associées aux clés maitresse et d'entête), utilisées par le mode XTS.

Les clés maitresses (principale et secondaire) sont générées par appel à la fonction `RandGetBytes` du générateur d'aléa et stockées dans l'entête[1] du volume chiffré.

Les clés d'entête (principale et secondaire) sont dérivées suivant la fonction `PBKDF2` décrite dans PKCS#5 v2.0 à partir des données d'authentification (mot de passe et éventuellement *keyfiles*) et d'une graine de 64 octets.

Les volumes chiffrés sont indépendants du système d'exploitation. Ils peuvent être montés dans tout environnement dans lequel la TOE peut être exécutée. Leur activation requiert l'authentification de l'utilisateur par mot de passe seul ou combiné avec une liste de fichiers *keyfiles*[2]. Une fois activé, rien ne distingue le disque chiffré des autres mémoires de masse

[1] L'entête d'un volume chiffré correspond aux 512 premiers octets. Un disque chiffré possédant un disque caché, a un deuxième entête se situant au 1536 octet en partant de la fin du disque hôte.

[2] Les *keyfiles* sont des fichiers dont le contenu est combiné avec le mot de passe.

auxquelles l'utilisateur a accès. TrueCrypt chiffre, de façon transparente pour l'utilisateur, les données écrites sur le volume. Pour le déchiffrement, les données chiffrées sont d'abord copiées en mémoire puis déchiffrées. Les données sont donc protégées en confidentialité, même en cas d'arrêt brutal de la machine hôte, si le système d'exploitation est configuré pour ne pas créer une image mémoire de la RAM.

3.2. DESCRIPTION DE LA MANIÈRE D'UTILISER LE PRODUIT

Le produit est une application qui s'installe sur le poste utilisateur dont les données sont à protéger en confidentialité. Le code source est accessible sur son site officiel, à l'adresse suivante : http://www.truecrypt.org/downloads

TrueCrypt met en œuvre une authentification préboot de l'utilisateur lorsque la partition système est chiffrée. Une fois que l'utilisateur est authentifié auprès du logiciel, le chiffrement/déchiffrement est réalisé de manière transparente entre les applications que l'utilisateur emploie pour manipuler ses données (lecture, modification, sauvegarde), et le support de stockage contenant le conteneur chiffré.

Globalement, l'utilisateur n'a d'interactions explicites avec la TOE seulement sur trois étapes.

1) lors de la création d'un conteneur chiffré :

L'utilisateur fournit les informations nécessaires à la création du volume TrueCrypt :

- le type de conteneurs chiffrés ;
- le type de protection (volume standard ou caché) ;
- l'emplacement du volume ;
- l'algorithme ou la séquence d'algorithmes de chiffrement ;
- la fonction hachage ;
- la taille du volume chiffré à créer ;
- le mot de passe utilisateur ;
- la liste de fichiers *keyfiles* (optionnels) ;
- les options de formatage du volume.

En particulier, l'utilisateur spécifie les algorithmes cryptographiques qui seront utilisés. TrueCrypt supporte les algorithmes symétriques de chiffrement par bloc AES[3], Serpent et Twofish. L'utilisateur peut choisir soit d'en spécifier un, soit d'en utiliser deux ou trois en cascade (i.e. de façon combinée comme par exemple AES-Twofish-Serpent[4]). Chacun des algorithmes, utilisé seul ou en cascade, utilise sa propre clé de chiffrement, de 256 bits. Le mode de chiffrement utilisé est XTS.

[3] A partir de la version 7, TrueCrypt est capable d'utiliser les nouvelles instructions AES des processeurs récents afin d'accélérer les opérations de chiffrement.

[4] Mécanisme de trois chiffrements en cascade fonctionnant en mode XTS. Chaque bloc de 128 bits est d'abord chiffré avec l'algorithme Serpent et une clé de 256 bits en mode XTS, puis avec l'algorithme Twofish et une seconde clé de 256 bits en mode XTS, et enfin avec l'AES et une troisième clé de 256 bits en mode XTS.

L'utilisateur spécifie également une fonction de hachage parmi RIPEMD-160, SHA-512 et Whirlpool. La première fournit une sortie de 160 bits tandis que les deux autres fournissent une sortie de 512 bits. La fonction de hachage spécifiée sera utilisée :

- par la fonction `RandMix` du générateur d'aléa de TrueCrypt : ce dernier génère pour chaque nouveau volume :
  - un couple de clés symétriques (clé maître et clé secondaire) utilisé avec le mode XTS pour chiffrer les données du volume TrueCrypt ;
  - une graine de 512 bits utilisée pour construire les clés d'entête principale et secondaire utilisées pour chiffrer l'entête du volume suivant le mode XTS.
- couplée avec la fonction HMAC, par la fonction pseudo-aléatoire PBKDF2 lors de la dérivation des données d'authentification et d'une graine en clés d'entête de volume.

2) <u>au moment du montage/démontage du conteneur chiffré</u> :

TrueCrypt demande une authentification avant de monter le disque virtuel chiffré. Elle repose sur un mot de passe choisi par l'utilisateur et, si elle a été définie, la liste de fichiers *keyfiles*.

Il s'agit de fichiers dont le contenu est combiné avec le mot de passe. Seul le premier Mo du fichier *keyfile* est utilisé pour l'authentification. Ces fichiers offrent une protection supplémentaire en ne permettant de monter un volume que si le fichier est présent. Un *keyfile* peut résider sur un support amovible comme une clé USB (ce qui permet une authentification à deux éléments) ou un support cryptographique respectant le standard PKCS#11 (clé USB ou carte à puce).

Une fois monté, le volume TrueCrypt est vu comme un disque ordinaire et l'accès au système de fichiers inclus est totalement transparent.

3) <u>lors du paramétrage du conteneur chiffré,</u>

La TOE permet à l'utilisateur de :

- modifier son mot de passe ;
- générer aléatoirement des fichiers *keyfiles* de 64 octets ;
- créer un volume caché ;
- créer une liste de disques chiffrés favoris permettant d'automatiser l'opération de montage ;
- tester les performances et/ou la conformité des algorithmes de chiffrement implémentés ;
- paramétrer l'application.

En particulier, l'utilisateur peut configurer le démontage automatique de tous les volumes TrueCrypt :

- lors de la fermeture de la session de l'utilisateur ;
- lors de la mise en veille simple du poste ;
- lors de la mise en veille prolongée (hibernation, option activée par défaut) ;
- si aucune donnée n'a été lue/écrite durant un temps fixé ;
- même si certains fichiers ou répertoires sont ouverts.

Il peut également configurer TrueCrypt pour :

- monter un volume en lecture seule ;

- que le mot de passe soit gardé en mémoire temporaire, permettant le montage/démontage des volumes sans avoir à saisir le mot de passe au cours d'une session ;
- effacer les mots de passe mis en cache à la fermeture de TrueCrypt, ainsi que d'éventuelles données associées de *keyfiles* ;
- effacer les mots de passe mis en cache lors du démontage automatique de volumes (option activée par défaut) ;
- ouvrir l'explorateur de fichiers pointant vers la racine du volume, chaque fois qu'il est monté avec succès ;
- fermer automatiquement les fenêtres d'explorateur de fichiers au démontage du volume (option activée par défaut) ;
- ne pas mettre à jour la date de dernière modification du volume chiffré au fil des accès (option activée par défaut).

3.3. DESCRIPTION DE L'ENVIRONNEMENT PRÉVU POUR SON UTILISATION

La TOE fonctionne dans les environnements suivants :

- Windows : Windows 7, Windows Vista, Windows XP et Windows 2000 SP4 ;
- Windows Server : 2008 R2, 2008 et 2003 ;
- Linux 32/64 bits ;
- Mac OS X (10.4 à 10.7).

TrueCrypt permet également de créer une partition chiffrée sur tout type de support amovible.

Remarque : le chiffrement de la partition système n'est supporté que pour les systèmes d'exploitation Windows.

3.4. DESCRIPTION DES HYPOTHÈSES D'ENVIRONNEMENT

H1. SystemeExploitation

Le système d'exploitation, support de la TOE, met en œuvre des mécanismes de protection adéquats (confinement, contrôle d'accès, etc.) paramétrés et configurés selon les règles de l'état de l'art. De plus, il est à jour des correctifs en vigueur au moment de l'installation, sain et exempt de virus, chevaux de Troie, etc.

H2.InstallationIntegre

L'exécutable nécessaire à l'installation et l'utilisation de la TOE est intègre.

H3.Remanence

La mémoire vive (RAM) utilisée par la machine qui exécute le produit n'est pas rémanente par construction.

H4.Protect

Une fois démarré, le système d'exploitation empêche les programmes malveillants d'exfiltrer les données en clair issues des volumes protégés par la TOE.

3.5. DESCRIPTION DES DÉPENDANCES PAR RAPPORT À DES MATÉRIELS, DES LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTÈME QUI NE SONT PAS FOURNIS AVEC LE PRODUIT

Il n'existe aucune dépendance à l'installation ou l'exécution de TrueCrypt.

3.6. DESCRIPTION DES UTILISATEURS TYPIQUES CONCERNÉS (UTILISATEURS FINAUX, ADMINISTRATEURS, EXPERTS…) ET DE LEUR RÔLE PARTICULIER DANS L'UTILISATION DU PRODUIT

Les utilisateurs qui ont un accès à la TOE sont les utilisateurs souhaitant accéder légitimement aux données protégées par la TOE.

3.7. DÉFINITION DU PÉRIMÈTRE DE L'ÉVALUATION, À SAVOIR LES CARACTÉRISTIQUES DE SÉCURITÉ DU PRODUIT CONCERNÉES PAR L'ÉVALUATION.

L'évaluation porte sur les fonctionnalités du logiciel TrueCrypt. Le périmètre de l'évaluation du produit comprend notamment :

- l'authentification de l'utilisateur ;
- le chiffrement/déchiffrement des données de l'utilisateur ;
- la génération de clés cryptographiques associées à un volume TrueCrypt.

Le système d'exploitation hôte est considéré hors TOE.

4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DANS LEQUEL LE PRODUIT DOIT FONCTIONNER

4.1. MATÉRIEL COMPATIBLE OU DÉDIÉ

L'installation de TrueCrypt ne nécessite pas de matériel dédié particulier. La TOE peut être installée sur Windows, Linux ou Mac OS et chiffrer un disque complet ou un support amovible.

4.2. SYSTÈME D'EXPLOITATION RETENU

Le système d'exploitation retenu pour la réalisation de l'étude est Windows 7 SP1 (64 bits).

5. DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTÉGER

Les biens sensibles que la TOE doit protéger sont les suivants.

Les données stockées

Les données de l'utilisateur stockées dans un volume chiffré et protégées en confidentialité par l'application TrueCrypt.

Les données d'authentification

Les données d'authentification utilisées pour contrôler l'identité de l'utilisateur et accéder à un volume chiffré (i.e. le mot de passe de l'utilisateur et, si elle est spécifiée, la liste de fichiers *keyfiles*).

Les clés cryptographiques

L'ensemble des clés symétriques utilisées pour protéger les données dans un volume TrueCrypt. Il s'agit :

- des clés maitresses (principale et secondaire) utilisées pour le chiffrement/déchiffrement des données de l'utilisateur. Elles sont générées par appel au générateur d'aléa et stockées chiffrées dans l'entête du volume TrueCrypt ;
- des clés d'entête (principale et secondaire) utilisées pour protéger les clés maitresses. Elles sont dérivées des données d'authentification et d'une graine aléatoire.

6. DESCRIPTION DES MENACES

Les agents de menace sont les suivants :

- **Entités non autorisées** : un attaquant humain ou entité qui interagit avec la TOE mais ne dispose pas d'accès légitime à la TOE.

Les menaces pesant sur la TOE sont les suivantes.

M1.Divulgation du mot de passe

Un attaquant parvient à connaitre le mot de passe d'accès aux données sensibles contenues dans un volume TrueCrypt en menaçant l'utilisateur légitime.

M2. Accès illégitime aux données

Un attaquant parvient à accéder, à l'insu du l'utilisateur légitime, aux données sensibles de l'utilisateur stockées sur la partition TrueCrypt alors que celle-ci est montée.

M3.Récupération d'informations partielles

Un attaquant parvient à identifier la présence de données sur un conteneur chiffré (si le formatage complet n'a pas été réalisé à la création du volume) en analysant la mémoire de travail de l'application (RAM).

M4. Accès aux données temporaires

Un attaquant parvient à récupérer les données sensibles de l'utilisateur ou des clés cryptographiques après analyse de la mémoire de travail de l'application (RAM).

7. DESCRIPTION DES FONCTIONS DE SÉCURITÉ DU PRODUIT

Les fonctions de sécurité de la TOE sont les suivantes.

F1.Authentification de l'utilisateur

Le montage du disque et toute modification des paramètres d'authentification sont conditionnés à l'authentification préalable de l'utilisateur. Celle-ci requiert un mot de passe et, si elle a été spécifiée à la création du volume, la liste des fichiers *keyfiles*.

F2.Chiffrement/Déchiffrement de données

La TOE assure la protection en confidentialité des données sensibles enregistrées dans le volume chiffré. Pour se faire, elle chiffre (respectivement déchiffre) à la volée et de façon transparente les données écrites sur (respectivement lues depuis) le volume TrueCrypt. La fonction de chiffrement/déchiffrement opère selon le mode XTS avec une paire de clés de 256 bits stockées chiffrées dans l'entête du volume.

F3.Protection des clés de chiffrement de données

La TOE assure la protection en confidentialité des clés maitresses (principale et secondaires) utilisées pour le chiffrement de données, en chiffrant l'entête de volume les contenant (hormis les 64 premiers octets, correspondant à une graine) avec une clé d'entête dérivée des données d'authentification et de la graine.

F4.Intégrité des clés maitresses

La TOE assure des contrôles d'intégrité lors du déchiffrement de l'entête d'un volume chiffré. Elle vérifie que les 4 octets (positionnés après les 512 bits de la graine) sont bien égaux à la chaine « TRUE » en ASCII. La somme de contrôle (CRC-32) des 256 derniers octets de l'entête déchiffré (correspondant aux clés maitresses principale et secondaire) est également calculée et comparée à la valeur stockée dans l'entête.

F5.Génération d'aléa

La TOE utilise, durant son fonctionnement, des clés de chiffrement associées au volume chiffré. Ces clés sont générées par appel à la fonction `RandGetBytes` du générateur d'aléa de TrueCrypt. Il s'agit :

- des clés maîtresses (principale et secondaire) de 256 bits utilisées pour le chiffrement, en mode XTS, des données de l'utilisateur ;
- de la graine de 512 bits (stockée dans l'entête du volume) utilisée pour dériver les clés d'entête (principale et secondaire).

F6.Dérivation de clés

La TOE utilise la fonction `PBKDF2` de PKCS#5 v2 pour dériver les deux clés d'entête (principale et secondaire) de 256 bits à partir de la graine et des données d'authentification de l'utilisateur (mot de passe et éventuellement *keyfiles*). Cette fonction utilise le mécanisme HMAC, couplée avec la fonction de hachage spécifiée par l'utilisateur, comme fonction pseudo-aléatoire. Les clés dérivées sont utilisées pour chiffrer selon le mode XTS l'entête (512 octets) du volume TrueCrypt et, par suite, protéger en confidentialité les clés maitresses.

F7.Formatage

Lors de la création d'une partition chiffrée, la TOE fait appel au générateur d'aléa pour initialiser la mémoire allouée avec de l'aléa (hormis les 512 premiers octets, correspondant à l'entête chiffré). La fonction de formatage garantit que tout volume TrueCrypt ne pourra être formaté par une autre application.

F8.Démontage

La TOE permet le démontage des partitions chiffrées à la demande de l'utilisateur ou de façon automatique. Cette fonction permet de rendre les données inaccessibles en lecture en cas de menace immédiate.

F9.Répudiation

La TOE permet l'utilisation d'un volume chiffré caché au sein d'un autre volume chiffré.

Même lorsque la partition chiffrée hôte est montée, il est impossible de prouver l'existence d'un volume chiffré caché à l'intérieur. Cette fonction permet de protéger les informations sensibles contre un attaquant qui chercherait à obtenir par la force les données d'authentification de l'utilisateur.

F10.Effacement des éléments secrets

La TOE permet d'effacer les données sensibles (telles que les mots de passe) présentes dans la mémoire en cache lors du démontage des volumes chiffrés.

Fin du document