



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-CSPN-2008/03

TrueCrypt version 6.0a

Paris, le 01 décembre 2008

*Le Directeur central de la sécurité des
systèmes d'information*

Patrick Pailloux
[ORIGINAL SIGNE]



Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié. C'est pourquoi ce rapport de certification devrait être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présumées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par la Direction centrale de la sécurité des systèmes d'information (DCSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

La reproduction de ce document sans altération ni coupure est autorisée.

<i>Référence du rapport de certification</i>	DCSSI-CSPN-2008/03
<i>Nom du produit</i>	TrueCrypt version 6.0a
<i>Référence/version du produit</i>	Version 6.0a
<i>Critères d'évaluation et version</i>	CERTIFICATION SECURITE DE PREMIER NIVEAU (CSPN, Version expérimentale)
<i>Développeur(s)</i>	TrueCrypt Foundation http://www.truecrypt.org/
<i>Commanditaire</i>	Secrétariat Général de la Défense Nationale 51, boulevard de la Tour Maubourg 75700 – Paris – 07 SP France
<i>Centre d'évaluation</i>	SOGETI Infrastructure Services 6 - 8, Rue Duret, 75016 Paris, France Tél : +33 (0)1 58 44 55 66, mél : edouard.jeanson@sogeti.com

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1	LE PRODUIT	7
1.1	PRESENTATION DU PRODUIT	7
1.2	DESCRIPTION DU PRODUIT EVALUE	8
1.2.1	<i>Catégorie du produit</i>	8
1.2.2	<i>Identification du produit.....</i>	8
1.2.3	<i>Services de sécurité</i>	9
1.2.4	<i>Configuration évaluée</i>	10
2	L'ÉVALUATION	11
2.1	REFERENTIELS D'ÉVALUATION	11
2.2	CHARGE DE TRAVAIL PREVUE ET DUREE DE L'ÉVALUATION.....	11
2.3	TRAVAUX D'ÉVALUATION	11
2.3.1	<i>Fonctionnalités, environnement d'utilisation et de sécurité.....</i>	11
2.3.1.1	Spécification de besoin du produit	11
2.3.1.2	Biens sensibles manipulés par le produit	11
2.3.1.3	Description des menaces contre lesquelles le produit apporte une protection	11
2.3.1.4	Fonctions de sécurité.....	11
2.3.1.5	Utilisateurs typiques.....	11
2.3.2	<i>Installation du produit</i>	11
2.3.2.1	Plate-forme de test.....	11
2.3.2.2	Particularités de paramétrage de l'environnement	12
2.3.2.3	Options d'installation retenues pour le produit	12
2.3.2.4	Description de l'installation et des non-conformités éventuelles.....	12
2.3.2.5	Durée de l'installation	12
2.3.2.6	Notes et remarques diverses.....	12
2.3.3	<i>Analyse de la conformité</i>	13
2.3.3.1	Analyse de la documentation	13
2.3.3.2	Revue du code source.....	13
2.3.3.3	Fonctionnalités testées.....	13
2.3.3.4	Fonctionnalités non testées.....	14
2.3.3.5	Conformité des mécanismes cryptographiques.....	14
2.3.3.6	Synthèse des fonctionnalités testées / non testées et des non-conformités.....	14
2.3.3.7	Avis d'expert sur le produit.....	14
2.3.4	<i>Analyse de la résistance des mécanismes et des fonctions</i>	14
2.3.4.1	Liste des fonctions testées et résistance	14
2.3.4.2	Avis d'expert sur la résistance des mécanismes.....	15
2.3.5	<i>Analyse des vulnérabilités (conception, construction...).....</i>	15
2.3.5.1	Liste des vulnérabilités connues.....	15
2.3.5.2	Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert	15
2.3.6	<i>Analyse de la facilité d'emploi et préconisations</i>	16
2.3.6.1	Cas où la sécurité est ambiguë	16
2.3.6.2	Recommandations pour une utilisation sûre du produit.....	17
2.3.6.3	Avis d'expert sur la facilité d'emploi.....	19
2.3.6.4	Notes et remarques diverses	19
2.3.6.5	Accès aux développeurs	19
2.4	ANALYSE DE LA RESISTANCE DES MECANISMES CRYPTOGRAPHIQUES	19
2.5	ANALYSE DU GENERATEUR D'ALEAS.....	20
3	LA CERTIFICATION.....	21
3.1	CONCLUSION.....	21

3.2	RESTRICTIONS D'USAGE.....	21
ANNEXE 1.	RÉFÉRENCES DOCUMENTAIRES DU PRODUIT ÉVALUÉ	22
ANNEXE 2.	RÉFÉRENCES LIÉES À LA CERTIFICATION	23

1 Le produit

1.1 Présentation du produit

L'ordinateur d'une entreprise ou d'un service administratif peut être l'objet d'un vol au même titre que tout autre objet de valeur. Ce risque est aujourd'hui accentué par le nomadisme croissant des équipements, plus susceptibles de quitter le lieu de travail qu'auparavant. TrueCrypt est une application logicielle de chiffrement des données à la volée sur toute mémoire de masse persistante fixe ou amovible (disque dur, clé USB...) permettant de protéger la confidentialité de ces données et de réduire l'impact de leur pertes en termes de divulgation non autorisée en cas de vol de matériel.

Les données sont protégées à l'intérieur d'un ou plusieurs *Volumes TrueCrypt* chiffrés qui peuvent être de trois types :

- **les conteneurs fichiers** qui sont des fichiers avec n'importe quelle extension et d'une taille variable définie par l'utilisateur. Un fichier conteneur est un fichier standard pouvant être stocké sur n'importe quel support de données ;
- **les partitions « non-systèmes »** qui correspondent complètement ou partiellement à un disque physique et qui ne contiennent pas le système d'exploitation destiné à être lancé au démarrage de la machine. Ces partitions sont typiquement destinées à recueillir des données. Peuvent également être chiffrés suivant cette méthode, les disques durs fixes entiers, les disques durs amovibles, les disquettes, les clés USB ou tout autre type de matériel de stockage de données ;
- **les partitions systèmes et disques complets**. Il y a alors chiffrement de toutes les partitions contenant, entre autres, le système d'exploitation. L'ordinateur ne peut démarrer sur ce système d'exploitation qu'après authentification de l'utilisateur au lancement (*boot*) du système.

L'application TrueCrypt est un intermédiaire transparent entre les applications que l'utilisateur emploie pour manipuler ses données (lecture, modification, sauvegarde) et le support de stockage contenant un ou plusieurs volumes TrueCrypt.

L'utilisation d'un volume TrueCrypt requiert l'authentification préalable de l'utilisateur. Si cette authentification réussit, le volume TrueCrypt est dit « monté » et rien ne le distingue des autres mémoires de masse auxquelles l'utilisateur a accès à part le fait que tout ce qui y est stocké est chiffré.

Il est important de comprendre que, paradoxalement, les données ne sont protégées par TrueCrypt que lorsque celui-ci n'est pas en fonction (ou pour être plus précis, lorsque le volume chiffré contenant les données n'est pas monté). En effet, lorsqu'un volume TrueCrypt est monté, tout utilisateur ou processus de la machine ayant les droits d'accès peut lire ou écrire sur ce volume. Par contre, si le volume n'est pas monté, un utilisateur ou un processus n'aura accès qu'à de l'information chiffrée. La confidentialité de ces informations dépendra alors de la robustesse de la cryptographie utilisée et de la bonne conception du produit (par exemple, le fait que le produit assure la confidentialité des clés de chiffrement qu'il utilise).

Les principales fonctionnalités de sécurité de TrueCrypt sont :

- l'authentification de l'utilisateur : le montage du volume TrueCrypt et toute modification des paramètres d'authentification sont conditionnés à l'authentification préalable de l'utilisateur ;
- le chiffrement et le déchiffrement, de manière transparente, des données écrites sur et lues depuis le volume TrueCrypt lorsque celui-ci a été monté. Cette activation nécessite une authentification de l'utilisateur à travers la fourniture de données d'authentification de type mot ou phrase de passe ;
- la génération des clés de chiffrement associées au volume TrueCrypt.

Bien que les données d'authentification et les clés de chiffrement ne soient pas associées à des données utilisateur devant être protégées par le produit, leur confidentialité doit être assurée :

- l'efficacité du mécanisme d'authentification dépend de la confidentialité des données d'authentification ;
- l'efficacité des mécanismes de chiffrement dépend de la confidentialité des clés de chiffrement.

En cas de divulgation de ces données, la protection en confidentialité des données de l'utilisateur ne peut plus être assurée.

1.2 Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 Catégorie du produit

<input type="checkbox"/> 1 - détection d'intrusions
<input type="checkbox"/> 2 - anti-virus, protection contre les codes malicieux
<input type="checkbox"/> 3 - firewall
<input type="checkbox"/> 4 - effacement de données
<input type="checkbox"/> 5 - administration et supervision de la sécurité
<input type="checkbox"/> 6 - identification, authentification et contrôle d'accès
<input type="checkbox"/> 7 - communication sécurisée
<input type="checkbox"/> 8 - messagerie sécurisée
<input checked="" type="checkbox"/> 9 - stockage sécurisé
<input type="checkbox"/> 10 - matériel et logiciel embarqué
<input type="checkbox"/> 11 - messagerie sécurisée

1.2.2 Identification du produit

Une fois installée, la version est identifiable en cliquant sur la rubrique « A propos... » du menu « Aide » de TrueCrypt. Une boîte de dialogue affichant en caractères gras la version du produit apparaît alors.

1.2.3 Services de sécurité

L'objectif principal du produit TrueCrypt est d'assurer la confidentialité des données des utilisateurs contenues dans un ou plusieurs volumes TrueCrypt non montés. Pour ce faire, lorsque le ou les volumes TrueCrypt sont montés, le produit doit être en mesure de préserver la confidentialité des informations confidentielles qu'il manipule. Cet objectif dépend en partie du produit lui-même (par exemple, le produit doit effacer les clés de chiffrement qu'il utilise lorsque le volume TrueCrypt est démonté) et en partie de la façon dont l'ordinateur est configuré et utilisé.

Fonctions de sécurité sur les opérations cryptographiques :

- génération de nombres aléatoires pour générer la clé maître de chiffrement, la clé secondaire (LRW mode), la graine et les fichiers « keyfiles » ;
- génération de la clé maître associée à un disque ;
- écriture de données chiffrées sur un volume TrueCrypt préalablement monté en utilisant les clés et algorithmes de chiffrement associés à ce volume TrueCrypt ;
- lecture de données chiffrées sur un volume TrueCrypt préalablement monté en utilisant les clés et algorithmes de chiffrement associés à ce volume TrueCrypt.

Fonctions de sécurité sur le contrôle d'accès

- Mise en place d'un système de répudiation crédible basé sur l'utilisation d'un volume TrueCrypt caché et sur le fait qu'un volume TrueCrypt ne contient aucune forme de signature permettant de l'identifier.

Le principe des « disques chiffrés » cachés est la création d'un volume TrueCrypt au sein d'un autre volume TrueCrypt (dans l'espace libre sur le disque). Même lorsque le volume TrueCrypt externe est monté, il est impossible de prouver s'il y a un volume TrueCrypt caché à l'intérieur ou pas. Le mot de passe pour le volume TrueCrypt caché doit être différent du mot de passe pour le volume TrueCrypt externe.

- Génération, par les utilisateurs autorisés, de leurs mots ou phrase de passe, ainsi que les fichiers «keyfiles» auxquels le mot de passe peut être associé.
 - création du mot de passe lors de la création d'un volume TrueCrypt ;
 - modification du mot de passe ;
 - contrôle de la qualité des mots de passe ;
 - gestion des fichiers « keyfiles » : Les fichiers « keyfiles » sont des fichiers dont le contenu est combiné avec le mot de passe. L'utilisation des fichiers «keyfiles» est optionnelle. Dans le cas où l'utilisateur choisit de les utiliser, le ou les volumes TrueCrypt ne pourront être montés tant que le mot de passe et les bons fichiers « *keyfiles* » ne sont pas fournis à l'application. Cette fonction de sécurité permet à l'utilisateur de déterminer les fichiers « *keyfiles* » à utiliser, et éventuellement les générer.
- Dérivation des clés d'en-têtes suivant le standard PKCS#5 à partir des données d'authentification de l'utilisateur. Cette clé d'en-tête permet ensuite d'accéder aux données contenues dans l'en-tête, dont la clé maître.

Fonctions de sécurité sur la gestion d'un volume TrueCrypt

- Création d'un volume TrueCrypt :
 - formatage de la zone mémoire allouée ;

- lors de l'initialisation, si l'option « *Quick Format* » n'est pas sélectionnée, le volume TrueCrypt est formaté et rempli d'aléa ;
 - création de l'en-tête contenant la clé maître.
- Création et exécution d'un système d'exploitation caché et chiffré.
 - Démontage d'un volume TrueCrypt à la demande de l'utilisateur.
 - Démontage automatique d'un volume TrueCrypt montés lors des événements suivants :
 - fermeture de l'OS ;
 - mise en veille.

Cette fonctionnalité offre en outre la possibilité, lorsque les options associées sont sélectionnées, de démonter automatiquement un volume TrueCrypt lors des événements suivants :

- fermeture de session ;
- déclenchement de l'économiseur d'écran ;
- mise en mode économie d'énergie ;
- atteinte d'un délai fixé par l'utilisateur (ce délai n'est pas associé à un «disque chiffré», mais à l'application).

Enfin, il est possible de forcer le démontage d'un volume TrueCrypt, même lorsque ce volume contient des fichiers ou des répertoires ouverts par des applications.

- Génération de la liste des volumes TrueCrypt montés.

Cette gestion consiste à ajouter les disques montés à la liste et à les supprimer lors du démontage.

Fonctions de sécurité pour la protection des données de TrueCrypt

- Effacement des données sensibles (les mots de passe des disques chiffrés) présentes dans la mémoire du driver.

Une option permet d'appeler cette fonction de manière automatique, pour effacer le mot de passe dans la zone de cache lors du démontage d'un volume TrueCrypt, ou lors de la fermeture du logiciel.

- Verrouillage en mémoire des variables susceptibles de contenir des informations sensibles (ex: le contenu de la RAM associé ne doit pas pouvoir être copié dans le fichier de SWAP du système d'exploitation). Ce verrouillage n'est toutefois pas toujours possible ; c'est la raison pour laquelle la documentation du logiciel préconise la désactivation du fichier d'échange.

1.2.4 Configuration évaluée

Le périmètre de l'évaluation couvre l'intégralité des fonctionnalités du produit.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

2.2 Charge de travail prévue et durée de l'évaluation

La charge de travail prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 30 homme/jour. L'évaluation s'est déroulée de début août 2008 à mi-septembre 2008.

2.3 Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [ST] fournie en entrée de l'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1 *Fonctionnalités, environnement d'utilisation et de sécurité*

2.3.1.1 *Spécification de besoin du produit*

Conforme à la cible de sécurité.

2.3.1.2 *Biens sensibles manipulés par le produit*

Conforme à la cible de sécurité.

2.3.1.3 *Description des menaces contre lesquelles le produit apporte une protection*

Conforme à la cible de sécurité.

2.3.1.4 *Fonctions de sécurité*

Conforme à la cible de sécurité.

2.3.1.5 *Utilisateurs typiques*

Conforme à la cible de sécurité.

2.3.2 *Installation du produit*

2.3.2.1 *Plate-forme de test*

Pour l'évaluation, l'architecture nécessaire à la réalisation de l'évaluation a été déployée à l'aide de machines virtuelles, dans un souci de reproductibilité des tests et de stockage des

archives. Le logiciel **VMware Workstation** a été utilisé dans sa version **6.0.4 build-93057**. La machine virtuelle utilisée est un poste standard :

- sur lequel est installé **Windows XP Professionnel, version 5.1 (2600), Service Pack 2** ;
- possédant l'ensemble des mises à jour disponibles depuis le site Windows Update au début de l'évaluation.

L'installation a également été testée sur une machine virtuelle standard, sous **Linux Ubuntu 7.04**, comprenant l'ensemble des mises à jour disponibles depuis les serveurs Canonical.

Enfin, l'installation a été effectuée sur un ordinateur portable Apple équipé de **Mac OS X Leopard 10.5.4** à jour.

2.3.2.2 Particularités de paramétrage de l'environnement

Aucun paramétrage supplémentaire n'a été effectué.

2.3.2.3 Options d'installation retenues pour le produit

L'installation sous Windows a été effectuée en conservant les options de TrueCrypt activées par défaut, c'est-à-dire :

- l'association des fichiers .tc avec TrueCrypt ;
- la création d'un point de restauration ;
- la suppression du fichier de pagination.

Le *pack* « français » permettant de disposer de l'interface utilisateur en français a ensuite été ajouté.

Sous Ubuntu et OS X l'installation se fait avec un installeur ne présentant pas d'options de configuration.

2.3.2.4 Description de l'installation et des non-conformités éventuelles

L'installation ne pose aucun problème.

La seule « non-conformité » rencontrée par rapport à la documentation est que celle-ci ne détaille pas qu'un message est affiché lors du premier lancement du programme invitant l'utilisateur à lire une partie du guide de l'utilisateur, avant d'utiliser le produit.

La traduction de l'interface utilisateur ne fonctionne que sur les versions Windows, comme spécifié dans la documentation.

2.3.2.5 Durée de l'installation

L'installation prend moins de 10 minutes.

2.3.2.6 Notes et remarques diverses

Néant.

2.3.3 Analyse de la conformité

2.3.3.1 Analyse de la documentation

La documentation du produit TrueCrypt est complète, didactique et détaillée.

La lecture des « Guides utilisateurs » et des « Précautions de sécurité » est recommandée pour une utilisation sûre du produit.

L'évaluateur n'a pas identifié de non-conformité dans la documentation du produit.

2.3.3.2 Revue du code source

Le code source complet est disponible depuis le site de TrueCrypt. L'évaluateur a considéré qu'il était en général bien structuré, « bien pensé » et que l'exigence de portabilité avait été bien prise en compte ce qui indique une bonne rigueur de la part des développeurs (avis d'expert). Les parties du code source qui sont le moins lisibles semblent être les plus anciennes et celles qui concernent l'interface utilisateur.

Pour les besoins de l'évaluation, l'évaluateur a recompilé et parfois modifié le produit. La compilation n'a pas posé de problème particulier.

2.3.3.3 Fonctionnalités testées

Les fonctionnalités portant les intitulés suivants ont été testées avec succès :

- génération des mots de passe :
 - modification des mots de passes d'un volume chiffré ;
 - changement des mots de passe d'un volume caché ;
 - vérification de la robustesse des mots ou phrases de passe lors de la création d'un volume TrueCrypt ;
 - gestion des fichiers keyfiles.
- administration des fonctions de sécurité :
 - création d'un volume chiffré dans un conteneur ;
 - création d'un volume caché ;
 - création d'une partition système chiffrée ;
 - création d'une partition système primaire chiffrée et d'une partition système secondaire chiffrée contenant une copie cachée du système d'exploitation ;
 - montage du volume externe et caché de la partition système secondaire contenant une copie cachée du système d'exploitation ;
 - démontage automatique d'un volume TrueCrypt à la fermeture de l'OS ;
 - démontage automatique d'un volume TrueCrypt à la mise en veille ;
 - démontage automatique d'un volume TrueCrypt à la fermeture de session ;
 - démontage automatique d'un volume TrueCrypt lors de déclenchement de l'économiseur d'écran ;
 - démontage automatique d'un volume TrueCrypt lors de l'atteinte du délai fixé par l'utilisateur ;
 - démontage automatique d'un volume TrueCrypt lors de la mise en mode économie d'énergie ;
 - forçage du démontage d'un volume contenant des fichiers ou programmes en cours d'utilisation.

- protection des données de l'utilisateur :
 - protection du volume caché chiffré contre les dommages ;
 - tests d'intégrité du volume et restauration des en-têtes défectueux.

2.3.3.4 Fonctionnalités non testées

La fonction de suppression des données temporaires en mémoire (comme les clés de chiffrement) a été vérifiée par analyse du code source et non pas par des tests (voir §2.3.5.2).

2.3.3.5 Conformité des mécanismes cryptographiques

L'implémentation des algorithmes de chiffrement symétrique AES, Twofish et Serpent ainsi que le mode XTS ont été vérifiés et sont conformes.

L'implémentation des algorithmes de hachage SHA512, Whirpool et RIPEMD-160 a été vérifiée et est conforme.

L'implémentation de la fonction PBKDF2 a été vérifiée et est conforme.

L'implémentation de la fonction de calcul d'intégrité a été vérifiée et est conforme.

2.3.3.6 Synthèse des fonctionnalités testées / non testées et des non-conformités

L'ensemble des fonctionnalités testées est conforme à la cible de sécurité.

2.3.3.7 Avis d'expert sur le produit

La documentation est complète et très lisible. Le produit est conforme à sa cible de sécurité. Toutes les fonctionnalités testées sont implémentées. Le produit inspire confiance.

2.3.4 Analyse de la résistance des mécanismes et des fonctions

2.3.4.1 Liste des fonctions testées et résistance

Résistance du mot de passe d'un volume chiffré

La fonction de dérivation de clé PKBDF2 utilisée, combinée à un mot de passe fort, rendra l'attaque a priori impraticable.

Résistance du mécanisme de vérification d'intégrité sur le volume

La probabilité de générer un en-tête de volume vérifiant le mécanisme d'intégrité est de l'ordre de $\frac{1}{2^{96}}$

Résistance du mot de passe d'un volume caché et du déni plausible

La résistance de ce mécanisme est la même que celle du mécanisme de résistance du mot de passe d'un volume normal.

Résistance des clés maîtres de chiffrement

L'attaque sur les clés maîtres de chiffrement revient à une recherche exhaustive sur ces clés.

Résistance du déni plausible du système d'exploitation caché

Il n'est pas possible de révéler la présence d'un système caché.

2.3.4.2 Avis d'expert sur la résistance des mécanismes

Les mécanismes de sécurité, aussi bien pris séparément que dans leur ensemble, sont robustes et bien pensés. Ils s'appuient soit sur des standards reconnus (notamment AES et PBKDF2), soit sur l'état de l'art (comme XTS et Whirlpool).

L'analyse du code source montre que les développeurs se sont souciés des problèmes de sécurité liés à l'utilisation de TrueCrypt, en particulier en ce qui concerne la gestion des clés et le déni plausible.

L'enchaînement des mécanismes est bien construit.

2.3.5 Analyse des vulnérabilités (conception, construction...)

2.3.5.1 Liste des vulnérabilités connues

Aucune vulnérabilité publique n'est connue a priori sur la version 6.0a de TrueCrypt. Les vulnérabilités découvertes sur la version précédente (mauvaise gestion de l'hibernation et mémoire clavier du BIOS non effacée) ont été corrigées.

2.3.5.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Cinq vulnérabilités ont été découvertes lors de l'évaluation. Il s'agit d'erreurs de programmation, et non d'erreurs de conception. La plupart d'entre elles induisent des fuites d'informations, notamment sur le mot de passe ou les clés de chiffrement. Elles ne sont exploitables que dans des cas particuliers d'utilisation. Aucune possibilité d'attaque à partir d'un volume chiffré uniquement n'a été trouvée.

Vulnérabilité n°1 : la taille du mot de passe d'une partition système est présente dans la mémoire du BIOS.

Conséquences

Un attaquant est en mesure de prévoir la longueur du mot de passe du système chiffré une fois que celui-ci est monté. Ceci est possible en mode utilisateur et permet de réduire l'espace de recherche du mot de passe de démarrage en vue d'une attaque par recherche exhaustive, par exemple à partir d'une copie de disque. Cette vulnérabilité n'affecte qu'un volume TrueCrypt dont la partition système est entièrement chiffrée.

Vulnérabilité n°2 : une fonction du pilote TrueCrypt est sensible à une attaque liée au type d'une donnée.

Conséquences

Un système d'exploitation chiffré peut être sujet à une attaque par déni de service, voire à une exécution de code arbitraire en mode noyau depuis un compte utilisateur. Cette attaque n'est pas réalisable si la partition système n'est pas chiffrée.

Vulnérabilité n°3 : le chemin des fichiers clés n'est jamais effacé dans la mémoire.

Conséquences

Tout attaquant ayant un accès au compte de l'utilisateur est en mesure de retrouver le ou les fichiers clés utilisés pour monter un volume TrueCrypt, même si celui-ci est démonté. Dans le cas où un volume n'est protégé qu'avec des fichiers clés, et donc sans mot de passe, l'accès au volume est immédiat. Les partitions système ne pouvant pas être montées avec des fichiers clés, cette attaque n'est pas réalisable pour ce type de volume TrueCrypt.

Vulnérabilité n°4 : la fonctionnalité de sauvegarde de l'en-tête d'un volume chiffré n'efface pas correctement les clés de chiffrement.

Conséquences

Tout attaquant ayant un accès au compte de l'utilisateur, après que celui-ci a fait une sauvegarde d'un en-tête de volume, est capable de retrouver la clé secondaire de chiffrement du volume. En pratique, il devra toujours retrouver la clé primaire pour déchiffrer les données du volume.

Cette vulnérabilité a en revanche un impact plus important dans les versions antérieures à la version 5, où le mode LRW était utilisé. Le mode LRW a en effet été abandonné suite aux problèmes de sécurité engendrés si la clé secondaire était compromise.

Vulnérabilités n°5 : les mots de passe ne sont pas correctement effacés lors de la création d'un nouveau volume.

Conséquences

Tout attaquant ayant un accès au compte de l'utilisateur est en mesure de retrouver le mot de passe du dernier volume chiffré créé, même si celui-ci a été démonté. Cette attaque n'est possible que si le processus « TrueCrypt Format.exe » est en cours d'exécution. Ce processus est normalement fermé par l'utilisateur à la fin de la création du volume, ce qui réduit en principe fortement les possibilités d'attaque.

Bilan

Ces problèmes mineurs ont été signalés à la fondation TrueCrypt. En attendant, des recommandations d'utilisation permettent de pallier les problèmes découverts (voir 2.3.6.2) sauf pour la vulnérabilité n°2 qui peut entraîner un déni de service. Même si l'exécution de code n'est pas avérée et la vulnérabilité difficilement exploitable en utilisation normale, les conséquences peuvent nécessiter de devoir restaurer le *bootloader* à partir du CD-ROM de restauration.

2.3.6 Analyse de la facilité d'emploi et préconisations

2.3.6.1 Cas où la sécurité est remise en cause

La documentation de TrueCrypt recommande, s'ils sont employés, d'utiliser des fichiers « *keyfiles* » d'une taille supérieure ou égale à 30 octets. Un utilisateur peut créer un volume chiffré sans mot de passe tout en utilisant un « *keyfile* » de taille nulle. Dans un tel cas, l'interface de TrueCrypt ne génère aucun message d'avertissement de sécurité à destination de l'utilisateur. À titre de comparaison, lorsque l'utilisateur crée un volume chiffré en utilisant un mot de passe seul, un avertissement lui est envoyé si la longueur du mot de passe est inférieure à 20 caractères.

Mis à part ce cas, il n'a pas été constaté de cas d'utilisation du produit où la sécurité est remise en cause.

2.3.6.2 *Recommandations pour une utilisation sûre du produit*

Les recommandations sont de deux ordres :

- celles d'ordre général, elles reprennent notamment des recommandations spécifiées dans la documentation ;
- celles liées aux contre-mesures nécessaires à mettre en place pour limiter l'exploitabilité des vulnérabilités recensées au § 2.3.5.

Recommandations générales

- **Robustesse du mot de passe**

Une attaque sur le mot de passe du volume chiffré par recherche exhaustive est envisageable sur un volume avec un mot de passe court. Afin d'éviter ce type d'attaque, TrueCrypt recommande d'utiliser des mots de passe d'au moins 20 caractères. Pour les mêmes raisons, si des fichiers clés sont utilisés, leur taille doit être supérieure ou égale à 30 octets. La génération de fichiers clés de 64 octets par TrueCrypt est une bonne solution pour garantir le caractère aléatoire de ces fichiers.

- **Fichier de pagination**

En utilisation normale de la machine, le système d'exploitation gère un fichier de pagination. Ce fichier sert au système d'exploitation comme une extension de la mémoire vive (RAM). TrueCrypt ne peut garantir que des informations sensibles contenues dans la mémoire du pilote comme les clés maîtres de chiffrement ne seront pas écrites en clair dans ce fichier par le système d'exploitation. TrueCrypt recommande donc de désactiver le fichier de pagination lorsque le produit est installé. Cette remarque n'est pas à prendre en compte dans le cas d'un système intégralement chiffré.

- **Mise en veille prolongée**

Lors du déclenchement de la veille prolongée, le système d'exploitation crée un fichier d'hibernation contenant une copie de la mémoire système. La mémoire du pilote TrueCrypt contenant les clés maîtres de chiffrement peut alors être copiée sur le disque dur de la machine lors de la mise en veille prolongée. TrueCrypt recommande donc de désactiver la mise en veille prolongée pendant l'utilisation du produit. Cette remarque n'est pas à prendre en compte dans le cas d'un système intégralement chiffré.

- **Partitions systèmes chiffrées**

Afin de prévenir d'éventuelles fuites de données sensibles concernant un volume TrueCrypt et son contenu, il est préférable d'utiliser une partition système chiffrée en lieu et place d'un simple conteneur. En effet, dans le cas d'un volume simple, le système d'exploitation ou des applications tierces peuvent écrire temporairement dans une zone externe au conteneur, et donc non chiffrée. Dans le cas d'une partition, les données écrites sur le disque seront toujours chiffrées.

- **Informations de débogage**

Lors de certaines erreurs système, Windows propose d'effectuer une copie de tout ou partie de la mémoire noyau (*dump*) pour analyse post-mortem de la machine. Des informations sensibles comme les clés maîtres de chiffrement, contenues dans la mémoire du pilote, peuvent alors être copiées sur le disque dur de la machine. Pour cette raison, il est

recommandé de désactiver l'option « Ecriture des informations de débogage » du système d'exploitation durant l'utilisation de TrueCrypt.

- **Changement de mot de passe**

Lors du changement de mot de passe d'un volume chiffré, seul l'en-tête de ce dernier est modifié, les clés maîtres servant au chiffrement du système de fichier du volume chiffré restent inchangées. Il est donc recommandé, lors d'un changement de mot de passe, de créer un nouveau volume chiffré et de créer ainsi de nouvelles clés maîtres de chiffrement, particulièrement si l'ancien mot de passe est susceptible d'avoir été compromis.

- **Changement de mot de passe d'un volume caché**

Lors du changement du mot de passe d'un volume caché, seul l'en-tête de ce dernier est modifié. Si un attaquant a accès au volume chiffré avant et après le changement de mot de passe, il constatera le changement d'en-tête chiffré. L'en-tête du volume chiffré se trouvant à une adresse fixe et documentée, **l'attaquant en déduira de façon certaine la présence d'un volume chiffré**. Pour cette raison, nous recommandons de ne pas changer le mot de passe d'un volume caché, mais plutôt de créer un nouveau volume chiffré hôte contenant un volume caché.

- **CD-Rom de sauvegarde**

Lors de la création d'une partition chiffrée, TrueCrypt impose de graver une copie de sauvegarde de l'en-tête sur un média qu'il faut stocker de manière sûre. De la même manière, nous recommandons d'effectuer une copie de sauvegarde d'un en-tête d'un volume TrueCrypt (hors partition et partition système où cela est imposé afin de poursuivre la création). Cette sauvegarde doit impérativement être stockée de façon sûre.

- **Formatage d'un volume chiffré**

Lors de la phase de création d'un volume (quel que soit le type de volume : simple ou partition), il est préconisé de ne jamais utiliser l'option « Formatage rapide ».

- **Systèmes de fichiers journalisés**

Dans le cadre de l'emploi de conteneurs chiffrés (hors partitions), il est préconisé l'utilisation de systèmes de fichiers non journalisés tels que FAT32. L'utilisation de systèmes de fichiers journalisés tels que NTFS peut permettre la récupération d'informations par le biais des métadonnées propres aux systèmes des fichiers journalisés.

- **Défragmentation d'un volume**

Il est préconisé de ne pas défragmenter les systèmes de fichiers contenant des conteneurs TrueCrypt. En effet, si le système de fichier est défragmenté, il est possible de retrouver certaines parties ou certains fragments du conteneur. Dans le cas d'un changement de mot de passe par exemple, il serait ainsi possible de monter le volume avec un ancien mot de passe compromis (ou des anciens *KeyFiles*), en reconstruisant un ancien en-tête avec les fragments retrouvés.

Si le système de fichier est toutefois défragmenté, il est préconisé d'effacer de manière sûre tout l'espace libre après l'opération de défragmentation.

Recommandations suite aux vulnérabilités découvertes

- **Copier / Coller**

Lorsqu'un utilisateur effectue un copier / coller de son mot de passe dans une des boîtes de dialogue de « TrueCrypt » ou « TrueCrypt Format », ou qu'il sélectionne l'option « Afficher

le mot de passe », le mot de passe sera présent, en totalité ou en partie, dans le contexte des processus. Ceci est dû aux fonctionnalités du système d'exploitation, qui n'effacent pas les tampons mémoire manipulés. Il est donc recommandé de ne pas copier son mot de passe, et de ne pas sélectionner l'option affichant le mot de passe.

- **Création d'un nouveau volume**

Lors de la création d'un volume chiffré avec l'outil « *TrueCrypt Format* », le mot de passe du dernier volume chiffré créé n'est pas effacé de la mémoire de ce processus. Le processus « *TrueCrypt Format* » doit être au moins immédiatement fermé après la création d'un volume chiffré. Il est conseillé de redémarrer directement le système d'exploitation.

- **Sauvegarde des en-têtes de volume**

Une fois l'en-tête d'un volume sauvegardé et conservé en lieu sûr, il est recommandé de fermer puis relancer TrueCrypt, voire de relancer le système d'exploitation, afin d'éviter que la clé de chiffrement secondaire du volume ne reste présente en mémoire.

Fichiers clés

Le chemin des fichiers de clés n'est jamais effacé en mémoire. Il est conseillé de ne pas utiliser de fichiers clés, ou avec une extrême précaution, tant que cette vulnérabilité n'a pas été corrigée.

- **Déni de service et exécution de code potentielle**

La mauvaise gestion des paramètres passés au pilote sur un système d'exploitation chiffré ne peut pas être corrigée par des moyens simples. Il n'y a donc pas de recommandations sur ce point.

2.3.6.3 Avis d'expert sur la facilité d'emploi

Le produit est simple à utiliser et à administrer. Les précautions d'utilisation sont nombreuses et documentées. Les données techniques présentes dans la documentation permettent de comprendre pourquoi ces mesures ont été préconisées.

2.3.6.4 Notes et remarques diverses

Néant.

2.3.6.5 Accès aux développeurs

Le code source complet est disponible depuis le site de TrueCrypt.

L'évaluateur n'a pas eu de contact avec la communauté de développeurs de TrueCrypt durant l'évaluation.

2.4 Analyse de la résistance des mécanismes cryptographiques

Cette analyse vise à vérifier la conformité des mécanismes cryptographique par rapport au référentiel [CRYPTO] de la DCSSI.

Robustesse des algorithmes de chiffrement symétrique

Les algorithmes de chiffrement AES, Serpent ou Twofish utilisés avec le mode XTS sont des mécanismes de chiffrement symétrique de niveau standard.

Manipulation des fichiers clés

Le mécanisme utilisé pour traiter les fichiers clés afin d'obtenir un mot de passe « aléatoire » pour le volume n'atteint pas le niveau standard : il est relativement aisé de trouver des collisions.

Mécanisme de dérivation des clés PBKDF2

Le mécanisme de dérivation des clés PBKDF2, utilisé comme spécifié dans PKCS#5, est un mécanisme cryptographique de niveau standard. Cependant, après une revue du code source, un problème de mise en œuvre a été identifié (problème de conversion d'une chaîne). Bien que ce problème n'ait pas d'impact sur la robustesse cryptographique de la fonction de dérivation de clé PBKDF2, sa mise en œuvre dans TrueCrypt n'est pas de niveau standard.

Fonction de calcul d'intégrité

Le mécanisme de vérification de l'intégrité des données n'est pas de niveau standard. Il faut cependant noter qu'il est principalement utilisé pour authentifier l'utilisateur plus que pour vérifier l'intégrité des données de l'en-tête. La probabilité de générer un en-tête de volume vérifiant le mécanisme d'intégrité est de l'ordre de $\frac{1}{2^{96}}$.

2.5 Analyse du générateur d'aléas

Le générateur est formé d'un état perturbé par des éléments extérieurs ne constituant pas une véritable source physique d'aléa, retraités par une fonction de hachage cryptographique de niveau standard. Cette composition n'est pas reconnue de niveau standard pour la génération d'aléa selon le référentiel de la DCSSI. Cependant, elle ne remet pas en cause la robustesse des clés maîtres.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles en vigueur, avec la compétence et l'impartialité requise pour un centre d'évaluation agréé.

Ce certificat atteste que le produit « [TrueCrypt version 6.0a](#) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST].

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation spécifiés dans la cible de sécurité [ST], suivre les recommandations énoncées dans le présent rapport de certification ainsi que celles se trouvant dans les guides fournis [GUIDE] avec le produit.

Annexe 1. Références documentaires du produit évalué

[ST]	Cible de sécurité CSPN TrueCrypt 6.0a version 0 révision 3, 08 août 2008.
[RTE]	RTE - TrueCrypt v6.0a version 1 révision 2, 20 octobre 2008.
[GUIDE]	Guide d'installation et d'utilisation du produit : Documentation FR TrueCrypt 6.0a.

Annexe 2. Références liées à la certification

Décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CSPN-CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, DCSSI.
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 2.4, phase expérimentale, n°915/SGDN/DCSSI/SDR/CCN, 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1.4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1.3.
[CRYPTO]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques.

Ces documents sont disponibles sur le site www.ssi.gouv.fr.