Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2013/09

TrueCrypt
Version 7.1a

Paris, le 24 octobre 2013

Le directeur général de l'agence nationale de la sécurité des systèmes d'information

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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 doit 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 présupposées 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 l'agence nationale de la sécurité des systèmes d'information (ANSSI), 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 et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2013/09**
Nom du produit **TrueCrypt**
Référence/version du produit **7.1a**
Catégorie de produit **Stockage sécurisé**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU *(CSPN)***
Développeur **TrueCrypt Foundation** **http://www.truecrypt.org**
Commanditaire **Agence nationale de la sécurité des systèmes d'information** **51, boulevard de la Tour Maubourg** **75700 – Paris – 07 SP**
Centre d'évaluation **Amossys** **4 bis, allée du Batiment** **35000 Rennes**

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 modifié. Ce décret indique que :

- L'agence nationale 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

1.1. Présentation du produit

Le produit évalué est « TrueCrypt**,** 7.1a **»** développé par la fondation *TrueCrypt Foundation*.

TrueCrypt est une application logicielle conçue pour le chiffrement de masse des données de l'utilisateur.

Le chiffrement de disque est une méthode de protection de données pour les supports de stockage. Il est possible de chiffrer :

- soit l'ensemble du disque dur (FDE, *Full Disk Encryption*), pour empêcher qu'un attaquant accède à l'ensemble des données du système (y compris le système d'exploitation) ;
- soit des partitions ou des volumes, pour empêcher qu'un attaquant d'accède à certaines données.

En particulier, TrueCrypt permet de créer 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.

TrueCrypt réalise un chiffrement 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'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 les données ne sont protégées par TrueCrypt que 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.

1.2. Description du produit évalué

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

1.2.1. Catégorie du produit

☐ 1 - détection d'intrusions
☐ 2 - anti-virus, protection contre les codes malicieux
☐ 3 – firewall
☐ 4 - effacement de données
☐ 5 - administration et supervision de la sécurité
☐ 6 - identification, authentification et contrôle d'accès
☐ 7 - communication sécurisée
☐ 8 - messagerie sécurisée
☒ **9 – stockage sécurisé**
☐ 10 - matériel et logiciel embarqué
☐ 99- Autres

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.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- l'authentification de l'utilisateur préalable à tout montage de volume et toute modification des paramètres d'authentification ;
- la création et la gestion (montage/démontage) de volumes Truecrypt ;
- la création et la gestion (montage/démontage) de volumes Truecrypt cachés ;
- le démontage automatique des volumes ;
- l'effacement des données sensibles en mémoire ;
- le chiffrement et le déchiffrement, de manière transparente, des données écrites sur et lues depuis le volume TrueCrypt une fois monté ;
- la génération des clés de chiffrement associées au volume TrueCrypt ;
- la génération de nombres aléatoires.

1.2.4. Configuration évaluée

La configuration évaluée est celle par défaut.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation a été conforme à la charge de travail prévue lors de la demande de certification, elle-même conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] 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 [CDS] (chapitre 3 « Description du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 5 « Description des biens sensibles que le produit doit protéger »).

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

Conforme à la cible de sécurité [CDS] (chapitre 6 « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 7 « Description des fonctions de sécurité du produit »).

2.3.1.5. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre 3.2 « Description de la manière d'utiliser le produit »).

2.3.2. Installation du produit

2.3.2.1. Plate-forme de test

TrueCrypt a été évalué en version 7.1a sur le système d'exploitation Windows 7 SP1 64 bits, supportant une architecture de type Intel Core 2.

L'installation du produit est réalisée en exécutant l'installeur `TrueCrypt Setup.exe`.

2.3.2.2. Particularités de paramétrage de l'environnement

Sans objet.

2.3.2.3. Options d'installation retenues pour le produit

Sans objet.

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

Lors de la vérification de l'intégrité et de l'authenticité de l'installeur, le certificat de la *TrueCrypt Foundation* est apparu comme n'étant pas valide. Ceci empêche de vérifier la période de validité des certificats et leur état de révocation.

2.3.2.5. Durée de l'installation

L'installation s'effectue en quelques minutes.

2.3.2.6. Notes et remarques diverses

L'installation est simple et ne requiert aucune configuration de la part de l'utilisateur.

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES]. La documentation est claire et aucune non-conformité n'a été relevée. Il est à noter que la documentation en ligne (composée d'un ensemble documentaire étoffée, d'une FAQ et d'un forum) est particulièrement riche et de nombreux tutoriels y sont présents.

2.3.4. Revue du code source (facultative)

Le code source complet est disponible depuis le site de TrueCrypt. L'évaluateur a constaté que les développeurs avaient pensé le code de sorte à faciliter sa maintenance et que l'emploi de fonctions dites « sensibles » était limité.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification de l'utilisateur	**Réussite**
Création et formatage des volumes	**Réussite**
Montage et démontage des volumes	**Réussite**
Effacement des données sensibles en mémoire	**Réussite**
Chiffrement et déchiffrement des données	**Réussite**
Génération et dérivation des clés	**Réussite**
Génération d'aléas	**Réussite**
Protection des clés de chiffrement de données et des clés maitresse	**Réussite**

2.3.6. Fonctionnalités non testées

La fonction de création et de gestion de volumes cachés n'a pas été testée par l'évaluateur.

2.3.7. Synthèse des fonctionnalités testées / non testées et des non-conformités

La totalité des tests de conformité du produit n'ont pas été rejoués par l'évaluateur depuis leur validation lors de la version 6.0a du produit [CSPN-2008/03]. En effet, pour mener son analyse, l'évaluateur a pu s'appuyer sur le rapport technique d'évaluation de la dernière version certifiée de TrueCrypt [RTE-6.0a] en réalisant une étude des modifications apportées au produit entre la version 6.0a et la version 7.1a.

2.3.8. Avis d'expert sur le produit

Les tests n'ont pas permis de mettre en évidence de non-conformité sur les fonctions proposées par l'application TrueCrypt.

2.3.9. Analyse de la résistance des mécanismes et des fonctions

2.3.9.1. Liste des fonctions et des mécanismes testés

Fonction et mécanisme
Résistance du mot de passe
Résistance des *keyfiles*
Effacement des données sensibles
Protection de la mémoire

Traitement des IOCTL
Robustesse du générateur d'aléas
Robustesse des mécanismes cryptographiques

2.3.9.2. Avis d'expert sur la résistance des mécanismes

Lorsque la politique de mot de passe de l'utilisateur est conforme aux recommandations de TrueCrypt (chaîne de plus de 20 caractères), l'évaluateur n'a pas pu mettre en défaut le mécanisme d'authentification par mot de passe. Il est à noter que l'utilisation de *keyfiles* seuls n'offre pas une meilleure sécurité compte tenu que seul le premier Mo de données est utilisé pour la dérivation en clé d'entête.

Concernant l'effacement des données sensibles en RAM lors du montage d'un volume, l'évaluation a montré que TrueCrypt verrouille en mémoire ses variables sensibles (mot de passe, clés maîtresses, ...) avant de les utiliser. On notera néanmoins qu'aucun contrôle n'est réalisé pour vérifier le succès du verrouillage.

2.3.10. Analyse des vulnérabilités (conception, construction…)

2.3.10.1. Liste des vulnérabilités connues

Parmi les vulnérabilités connues sur le produit et celles découvertes dans l'évaluation de la version 6.0a [RTE-6.0a], toutes n'ont pas été corrigées. Les vulnérabilités suivantes sont encore applicables à la version 7.1a du produit :

- l'effacement du mot de passe dans le tampon clavier du BIOS permet de faire fuir des informations sur la taille du mot de passe ;
- l'effacement du mot de passe du dernier volume créé n'est pas correctement réalisé ;
- le fichier d'hibernation permet théoriquement de récupérer données sensibles ;
- le fichier de *crash dump* permet de récupérer des données sensibles en cas de défaillance du système ;
- le chemin d'accès aux *keyfiles* peut être récupéré en mémoire après le démontage d'un volume.

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

Aucune nouvelle vulnérabilité n'a été découverte durant l'évaluation.

2.3.11. Accès aux développeurs

Sans objet.

2.3.12. Analyse de la facilité d'emploi et préconisations

2.3.12.1. Cas où la sécurité est remise en cause

Néant.

2.3.12.2. Recommandations pour une utilisation sûre du produit

Recommandations générales

Recommandations concernant le poste de travail sur lequel s'exécute TrueCrypt

L'utilisation du produit doit être faite sur un PC hébergeant un système d'exploitation à jour concernant les correctifs de sécurité et être correctement administré. Le poste doit être durci afin d'être protégé contre des codes malveillants (voir le guide d'hygiène informatique [GUIDE-ANSSI], notamment ses règles 14 et 15).

Recommandations concernant les données d'authentification

Il est recommandé de suivre les recommandations de la TrueCrypt Foundation concernant le choix des mots de passes et *keyfiles*.

Les *keyfiles* ne doivent pas être utilisés comme facteur unique d'authentification. Lorsqu'ils sont combinés à un mot de passe, il est recommandé de les stocker sur un support externe. Par ailleurs, il est recommandé de ne pas utiliser de *keyfiles* d'une taille supérieure à 1Mo.

Recommandations concernant l'utilisation de TrueCrypt

Afin d'effacer correctement les secrets contenus en mémoire, il est recommandé de redémarrer l'ordinateur après la création d'un volume TrueCrypt.

Certaines vulnérabilités identifiées par l'évaluateur sont couvertes par le chiffrement de la partition système ou de l'intégralité du disque système. Ainsi, si les conditions d'emploi le permettent, il est recommandé de privilégier l'utilisation d'une partition système chiffrée en lieu et place d'un simple conteneur. Lorsque les conditions d'emploi ne le permettent pas, les recommandations suivantes doivent être appliquées.

Recommandations relatives à l'utilisation de conteneurs chiffrés

Recommandations concernant le poste de travail sur lequel s'exécute TrueCrypt

Afin d'éviter que des informations sensibles puissent être récupérées en mémoire, il est recommandé, lors de l'utilisation de TrueCrypt, de désactiver la mise en veille prolongée du système, de désactiver les fichiers de pagination et de désactiver la production de *dumps* à la suite d'une défaillance système.

Recommandations concernant l'utilisation de TrueCrypt

Il est recommandé d'activer le démontage automatique dans les divers cas de figures autorisés par le produit.

Les données protégées dans les conteneurs TrueCrypt n'étant plus protégées lorsque ces derniers sont montés, il est recommandé de démonter les volumes dès que les données stockées ne sont plus utilisées.

2.3.12.3. 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.

Moyennant le respect des recommandations évoquées dans le §2.3.12.2, l'évaluateur n'a pas identifié de cas où le produit serait configuré ou utilisé de façon non sûre mais qu'un utilisateur pourrait raisonnablement croire sûre.

2.3.12.4. Notes et remarques diverses

Néant.

2.4. Analyse de la résistance des mécanismes cryptographiques

Parmi les algorithmes cryptographiques mis en œuvre par TrueCrypt, seul RIPEMD-160 ne respecte pas une des règles du référentiel de sécurité de l'ANSSI [REF-CRY] relatif aux fonctions de hachage.

Cependant, au vu des améliorations apportées par le développeur pour couvrir ces faiblesses, l'évaluateur estime que la fonction de hachage RIPEMD-160 peut être considérée robuste pour une utilisation en tant que fonction pseudo-aléatoire dans PBKDF2.

2.5. Analyse du générateur d'aléas

Le générateur d'aléas de TrueCrypt a subit une seule une modification depuis la version 6.0a certifiée [CSPN-2008/03] concernant la taille de son état interne. Cette dernière a été réduite à 320 octets.

Les moyens mis en œuvre pour la génération et le retraitement des nombres aléatoires utilisés par TrueCrypt permettent donc toujours d'atteindre le niveau de résistances aux attaques visé par la CSPN.

3. La certification

3.1. Conclusion

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

Ce certificat atteste que le produit « TrueCrypt**,** 7.1a **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

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 [CDS] et suivre les recommandations énoncées dans le présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN du produit TrueCrypt ;* Référence : *CEL002-CDS-C2.13.P13-TrueCrypt-1.00* ; Date : *07/02/2013.*
[RTE]	*Rapport Technique d'Evaluation CSPN du produit TrueCrypt ;* Référence : *CEL002-RTE_CSPN-C2.13.P13-TrueCrypt-1.00* ; Rédacteur : *Amossys* ; Date : *30/04/2013.*
[RTE-6.0a]	*Evaluation CSPN - Truecrypt v6.0a ;* Référence : *K08-JBB-CR-671-2008* ; Rédacteur : *Sogeti* ; Date : *20/10/2008.*
[CSPN-2008/03]	*Rapport de certification DCSSI-CSPN-2008/03 – Truecrypt version 6.0a* Référence : *DCSSI-CSPN-2008/03* Date : 01/12/2008
[GUIDES]	Guide d'utilisation : *TrueCrypt Free open-source on-the-fly encryption User's Guide ;* Version : *7.1a*. Documentation en ligne : *http://www.truecrypt.org/docs/* *http://www.truecrypt.org/faq/* *http://forums.truecrypt.org*

Annexe 2. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau (CSPN) des technologies de l'information, version 1, n° 1414/ANSSI/SR du 30 mai 2011. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1417/ANSSI/SR du 30 mai 2011. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1, n° 1416/ANSSI/SR du 30 mai 2011. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr
[GUIDE-ANSSI]	Guide d'hygiène informatique de l'agence nationale de la sécurité des systèmes d'information (ANSSI), version finalisée du 28 janvier 2013. Document disponible sur www.ssi.gouv.fr/hygiene-informatique.