SOGETI
Infrastructure Services

6 - 8, Rue Duret
75016 Paris

Tél. : +33(0)1.58.44.55.66
Fax : +33(0)1.58.44.55.40

SGDN

TrueCrypt 6.0a

Cible de sécurité CSPN

Référence SOGETI : **K08-LC-PRE-651-2008**
Version v**0.3**

VALIDITE DU DOCUMENT

Identification		
Client	**Projet**	**Fournisseur**
SGDN	TrueCrypt 6.0a	SOGETI IS / ESEC

Validité du document				
Action	**Date**	**Nom**	**Fonction**	**Visa**
Rédaction	28/07/2008	L. CORNET	Consultant Sécurité IT	
Vérification	8/08/2008	Th. BOUSSON	Directeur de projet	

Historique des modifications			
Date création	**Date application**	**V.R.**	**Evolution**
28/07/2008		0.1	Proposition initiale
6/08/2008		0.2	Intégration des commentaires de la DCSSI
8/08/2008		0.3	Corrections mineures suite à réunion avec la DCSSI

Diffusion (suivie en mise à jour)			
	SGDN		

TABLE DES MATIERES

1 IDENTIFICATION

1.1 Identification de la cible de sécurité

La cible de sécurité de TrueCrypt version 6.0a a été rédigée par SOGETI ESEC dans le cadre d'un marché public.

Cette cible de sécurité a été élaborée en vue d'une évaluation CSPN.
Les statuts des versions de cette cible de sécurité sont présentés en page 2 du document.

1.2 Identification du produit

Catégorie	Identification
Organisation éditrice	TrueCrypt Foundation
Lien vers l'organisation	www.truecrypt.org
Nom commercial du produit	TrueCrypt
Numéro de la version évaluée	6.0a
Catégorie de produit	Application de chiffrement de mémoire de masse

2 ARGUMENTAIRE (DESCRIPTION) DU PRODUIT

2.1 Description générale du produit

Une application de chiffrement de données à la volée sur toute mémoire persistante de stockage permet de protéger en confidentialité les données enregistrées sur tout ou partie de la mémoire persistante de stockage d'une machine (ou, plus généralement, sur un support de stockage éventuellement amovible), dans les deux cas suivants :

1. l'application est hors fonctionnement,
2. l'application est en fonctionnement mais sans qu'un utilisateur légitime ne se soit authentifié à l'application.

TrueCrypt est une application logicielle de chiffrement de données à la volée sur mémoire de masse. Elle permet de créer un disque virtuel chiffré (volume TrueCrypt) contenu dans un fichier et de le monter comme un disque physique réel. TrueCrypt peut aussi chiffrer une partition entière ou un périphérique, comme une disquette ou une clé USB.

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 le disque chiffré.

L'activation du disque requiert l'authentification de l'utilisateur. Une fois activé, rien ne distingue le disque chiffré des autres mémoires de masse auxquelles l'utilisateur a accès.

En cours de fonctionnement, TrueCrypt chiffre (respectivement, déchiffre) de façon transparente pour l'utilisateur, les données écrites (respectivement, lues) sur le disque.

TrueCrypt protège les données sensibles de l'utilisateur à l'intérieur de conteneurs chiffrés. Ces conteneurs constituent les « disques chiffrés » dans la suite de ce document.

TrueCrypt permet de gérer trois types de « disques chiffrés » :

- ***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 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.

Les fonctionnalités de sécurité principales sont :

- L'authentification de l'utilisateur : Le montage du disque et toute modification des paramètres d'authentification sont conditionnés à l'authentification préalable de l'utilisateur.
- Le chiffrement et déchiffrement de manière transparente des données écrites sur et lues depuis le « disque chiffré » 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 « disque chiffré ».

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.

2.2 Description de la manière d'utiliser le produit

L'utilisateur n'a d'interaction explicite avec TrueCrypt que de plusieurs façons :

- lors de la création d'un disque chiffré ;
- au moment où il monte un disque chiffré ;
- au moment où il démonte explicitement un disque chiffré ;
- lors du paramétrage du disque chiffré.

2.3 Description de l'environnement d'utilisation prévu

Le produit TrueCrypt fonctionne dans les environnements Windows, Linux et MacOS.

Le matériel informatique 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 accentué par le nomadisme des équipements..

TrueCrypt est une application de chiffrement des données à la volée sur un support informatique permettant de protéger la confidentialité de ces dernières et de réduire l'impact de la perte en cas de vol de matériel.

TrueCrypt permet de chiffrer et d'assurer la confidentialité de la totalité des données stockées sur des disques durs internes ou externes (disques dur USB, etc.), des disquettes, des clés USB, ou de tout autre type de matériel de stockage de données.

Les « disques chiffrés » peuvent être sauvegardés sur CD ou DVD.

Les « disques chiffrés » sont indépendants du système d'exploitation. Ils peuvent être montés dans tout environnement dans lequel TrueCrypt peut être exécuté.

2.4 Description des hypothèses sur l'environnement

Environnement opérationnel

L'environnement opérationnel ne permet pas à un attaquant d'accéder au disque lorsque des données sensibles sont accessibles à un utilisateur légitime sur l'équipement.

Rémanence

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

2.5 Description des dépendances

TrueCrypt est évalué, en tant que produit, sur une plate-forme PC sous les systèmes d'exploitation identifiés au §3.2.

La procédure d'authentification des utilisateurs et le fonctionnement de TrueCrypt (chiffrement et déchiffrement) peuvent faire appel à des matériels spécifiques (clés USB, cartes à puce, etc.) en fonction de la mise en œuvre mais cette cible de sécurité ne pose aucune exigence particulière concernant ce type de matériel qui n'est pas considéré dans l'évaluation.

2.6 Description des utilisateurs typiques

L'utilisateur typique est l'utilisateur du compte géré par le système d'exploitation. TrueCrypt permet à l'utilisateur de protéger ses données en confidentialité sur le disque de la machine.

2.7 Définition du périmètre de l'évaluation

L'évaluation porte sur l'intégralité des fonctionnalités du produit.

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 Matériel compatible ou dédié

Aucune contrainte particulière.

3.2 Système d'exploitation compatible

Les systèmes d'exploitation utilisables avec TrueCrypt version 6.0a sont :

- *Windows Vista/XP/2000*
- *Mac OS X (10.5 Leopard, 10.4 Tiger)*
- *Linux (OpenSusE – x86, OpenSuSE – X64, Ubuntu x86, Unbuntu – x64)*

4 DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

L'objectif premier de l'application est de protéger les données enregistrées sur le disque par les utilisateurs en cas de vol du support ou de la machine le contenant. Ces données sont protégées en confidentialité via le chiffrement par une clé secrète (la clé maître) qui est elle-même chiffrée par une autre clé secrète (clé d'entête dérivée à partir des données d'authentification).

Données utilisateurs

Les données de l'utilisateur déposées sur le disque chiffré sont à protéger en confidentialité par l'application TrueCrypt.

Données de sécurisation

Les données utilisées par TrueCrypt pour assurer la confidentialité des données utilisateur doivent également être protégées en confidentialité :

- Les données d'authentification utilisées pour contrôler l'identité annoncée par l'utilisateur (mot ou phrase de passe et éventuellement fichier « keyfiles »[1]) ;
- La clé d'entête utilisée pour chiffrer les données d'entête qui contiennent en particulier la clé maître. Cette clé est obtenue par dérivation à partir des données d'authentification ;
- La clé maître utilisée pour chiffrer les données de l'utilisateur.

[1] Ces fichiers, décrits plus loin, contiennent une part des données d'authentification de l'utilisateur.

5 DESCRIPTION DES MENACES

Les menaces existantes lorsque le produit est en fonctionnement avec un utilisateur légitime authentifié ne sont pas considérées.

Menace sur la mémoire de masse

Un attaquant prend connaissance des données sensibles de l'utilisateur stockées sur le disque, par exemple, après avoir récupéré une ou plusieurs image(s) partielle(s) ou totale(s) du disque (éventuellement à des moments différents) ou bien après avoir volé l'équipement ou le disque.

Menace sur les mémoires temporaires

Après l'arrêt de l'application de chiffrement par l'utilisateur, un attaquant avec accès aux mémoires de travail de l'application (par exemple, RAM) prend connaissance des données sensibles de l'utilisateur ou des clés cryptographiques.

6 DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

L'objectif principal est de couvrir le vol de la machine ou du support. Néanmoins, les risques de la phase opérationnelle vis-à-vis du service de protection des données en confidentialité rendu par le produit sont couverts (comme, par exemple, l'écriture d'informations confidentielles sur des zones non chiffrées ou l'écriture de la clé en clair sur une mémoire persistante). La confidentialité des données inscrites sur la mémoire de masse est garantie quels que soient les états successifs de la machine lors de la phase opérationnelle. En cas d'arrêt logique du système d'exploitation, s'il est configuré pour ne pas créer une image mémoire de la RAM, par hypothèse (non rémanence), il n'y a pas d'atteinte possible à la confidentialité des données sensibles inscrites temporairement en RAM.

Fonctions de sécurité sur les opérations cryptographiques :

- Génération de nombres aléatoires pour générer la clé maître de chiffrement, la clé secondaire (XTS mode), la graine et les fichiers « keyfiles »
- Génération de la clé maître associée à un disque
- Écriture de données chiffrées sur un "disque chiffré" préalablement monté en utilisant les clés et algorithmes de chiffrement associés à ce "disque chiffré"
- Lecture de données chiffrées sur un "disque chiffré" préalablement monté en utilisant les clés et algorithmes de chiffrement associés à ce "disque chiffré"
- Calcul du haché d'une donnée associé à un "disque chiffré", suivant l'algorithme de calcul de haché associé à ce "disque chiffré".

Fonctions de sécurité sur le contrôle d'accès

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

  Le principe des "disque chiffré" cachés est la création d'un "disque chiffré" TrueCrypt au sein d'un autre "disque chiffré" TrueCrypt (dans l'espace libre sur le disque). Même lorsque le "disque chiffré" externe est monté, il est impossible de prouver s'il y a un "disque chiffré" caché à l'intérieur ou pas. Le mot de passe pour le "disque chiffré" caché doit être différent du mot de passe pour le "disque chiffré" 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 "disque chiffré";
  - Modification du mot de passe;
  - Contrôle de la qualité des mots de passe;
  - Gestion des fichiers keyfiles:

    Les fichiers keyfile 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 choisi de les utiliser, les "disques chiffrés" 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'entêtes suivant le standard PKCS#5 à partir des données d'authentification de l'utilisateur. Cette clé d'entête permet ensuite d'accéder aux données contenues dans l'entête, dont la clé maître.

Fonctions de sécurité sur la gestion des disques chiffrés

- Création d'un "disque chiffré":
  - Formatage de la zone mémoire allouée;
  - Lors de l'initialisation, si l'option "Quick Format" n'est pas sélectionnée, le "disque chiffré" est formaté et remplis d'aléa;
  - Création de l'entête contenant la clé maître;
- Création et exécution d'un système d'exploitation caché et chiffré.
- Démontage des "disques chiffrés" à la demande de l'utilisateur.
- Démontage automatique des "disques chiffrés" 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 les "disques chiffrés" lors des événements suivants:
  - Fermeture de session.
  - Déclanchement 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 de "disques chiffrés", même lorsque ces "disques chiffrés" contiennent des fichiers ou des répertoires ouverts par des applications.
- Génération de la liste des "disques chiffrés" qui sont 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 pilote.

  Une option permet d'appeler cette fonction de manière automatique, pour effacer le mot de passe dans la mémoire lors du démontage des "disques chiffrés", 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.

FIN DU DOCUMENT