THALES	ORIGINE	
	Etablissement	**Emetteur**
	Division Solutions de Sécurité & Services Security Systems	T3S/CESTI THALES - CNES

KEEPASS

Cible de Sécurité CSPN
KEEPASS v2.10 portable

THALES

TABLE DES MATIERES

I. INTRODUCTION

I.1 IDENTIFICATION DE LA CIBLE DE SECURITE

La cible de sécurité de Keepass version portable 2.10 a été rédigée par THALES dans le cadre d'un marché public de SGDSN/ANSSI correspondant au CCTP PA-10-13. Cette cible de sécurité a été rédigée selon le référentiel CSPN en vue d'une évaluation.

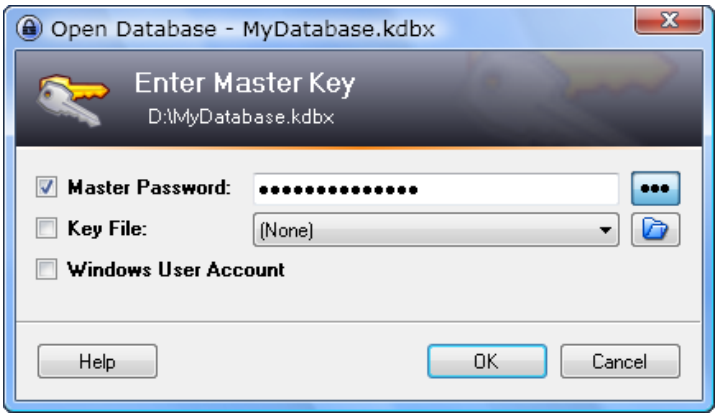
I.2 IDENTIFICATION DU PRODUIT

Nom de l'éditeur	Dominik Reich
Nom du produit	**Keepass**
Lien	http://keepass.info/
N° de version évaluée	**Keepass version portable 2.10**
Hash du package	md5 1a7a1cc9367869a5ce86aac60d22e40f
Catégorie de produit	Stockage sécurisé

II. DESCRIPTION DU PRODUIT

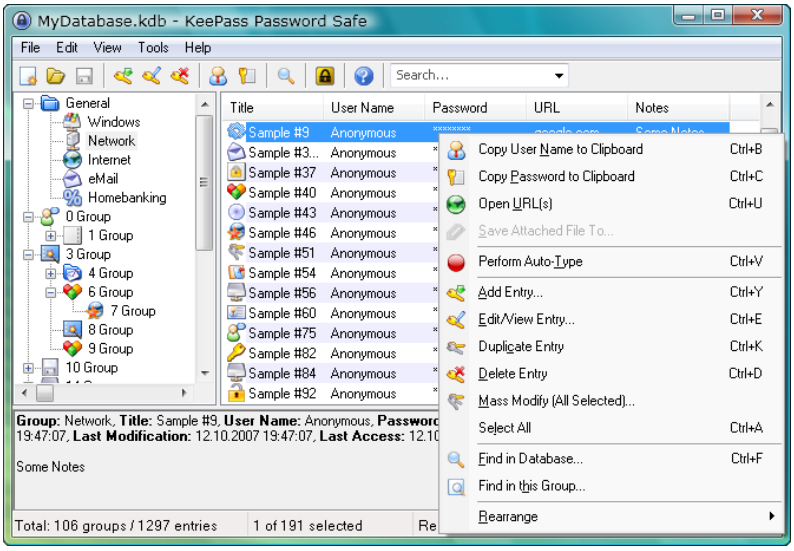
II.1 DESCRIPTION GENERALE DU PRODUIT

Le logiciel KeePass est un coffre-fort de mots de passe. KeePass est un logiciel open source (certifié OSI) qui permet de gérer différents mots de passe de manière sécurisée et chiffrée. Tous les mots de passe sont stockés dans une base de données, verrouillée avec une clé maître ou un fichier clé. Il suffit de se rappeler du mot de passe maître ou de sélectionner le fichier clé pour accéder à la base de données.



Cette base de données est chiffrée en utilisant l'AES avec une clé de 256 bits et peut-être facilement transférable d'un ordinateur à un autre.

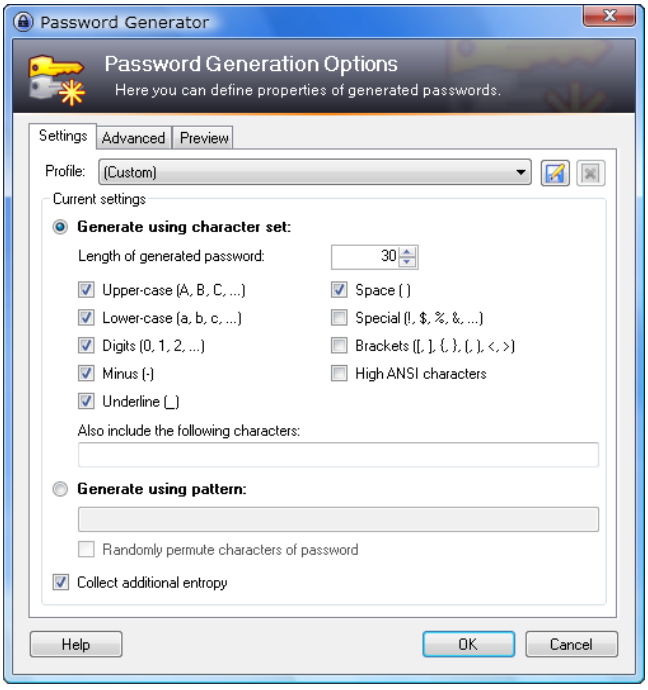
Keepass supporte des groupes de mot de passes et ils peuvent être triés par exemple entre Windows, Réseau, Internet, Mèl… Ils peuvent aussi être copiés/collés dans d'autres fenêtres. La saisie automatique des mots de passe permet à l'utilisateur la saisie automatique des identifiants et des mots de passe associés dans une autre fenêtre de connexion. Keepass permet aussi d'exporter la base données dans divers formats, il permet aussi d'importer différents formats de bases de mots passes (plus de 20 différent formats sont supportés comme les fichiers génériques CSV).



KeePass fournit également bien sûr un générateur de mot de passe qui est paramétrable suivant divers critères comme :

- Longueur du mot de passe
- Type de caractère
- Majuscules
- Minuscules
- Chiffres
- Spécial: !, $, % , &, …
- Parenthèses: [,], {, }, (,)
- …
- …

Diverses options sont disponibles (comme permettre de ne pas répéter les caractères : option à éviter, mais aussi permettre d'utiliser d'autres types de générateurs).



KeePass propose également une architecture de plugin afin d'étendre les fonctionnalités dont le support d'autres formats de données, l'archivage, le support de fonctionnalités réseau. Les plugins ne sont pas forcément développés par l'équipe de développement et peuvent donc contenir du code hostile. Il est donc conseillé d'utiliser de manière précautionneuse ces plugins.

II.2 ENVIRONNEMENT D'UTILISATION PREVU

Le produit Keepass fonctionne dans les environnements Windows 98 / ME / 2000 / XP, Vista et Windows 7.

II.3 HYPOTHESES SUR L'ENVIRONNEMENT

H1 : Environnement opérationnel
L'environnement opérationnel protège le logiciel des attaques ciblées et l'accès aux fichiers de pagination ou d'hibernation.

H2 : Rémanence
La mémoire vive (RAM) utilisée par la machine qui exécute le produit n'est pas rémanente par construction.

H3 : Politique de sécurité
L'utilisateur se doit d'utiliser le générateur de mot de passe et/ou générateur de clef maître fourni par le logiciel ou de mot de passe ayant les propriétés de sécurité requises définie dans une politique de sécurité adaptée

II.4 DESCRIPTION DES DEPENDANCES PAR RAPPORT A DES MATERIELS, DES LOGICIELS ET/OU DES MICROPROGRAMMES DU SYSTEME QUI NE SONT PAS FOURNIS AVEC LE PRODUIT

Keepass nécessite que le framework .NET soit installé pour Windows 98 / ME / 2000 / XP. Il est inclus dans Windows Vista et les versions suivantes.

II.5 UTILISATEURS TYPIQUES

L'utilisateur typique est l'utilisateur du compte géré par le système d'exploitation.
Keepass permet à l'utilisateur de protéger ses mots de passe en confidentialité sur le disque de la machine ou sur un support externe.

II.6 PERIMETRE DE L'EVALUATION

L'évaluation porte sur l'intégralité des fonctionnalités du logiciel Keepass en version portable fonctionnant sur Windows Xp et Windows 7 conformément au CCTP PA 10-13.

III. BIENS A PROTEGER

Il existe trois types de biens sensibles que le logiciel doit protéger en confidentialité et en intégrité :

- **B1 :** Les mots de passe stockés par le produit lui-même,
- **B2 :** Les métadonnées associées : absence/présence de mot de passe pour un compte précis, horodatage des derniers accès
- **B3 :** Le mot de passe et/ou le fichier de clé maître (ou leurs condensats) de la base de données

IV. MENACES

IV.1 LOGICIEL EN FONCTIONNEMENT

M1 : Un attaquant a accès en cours de fonctionnement aux données temporaires du logiciel. Cette menace couvre principalement l'exécution de keylogger sur la machine.

IV.2 LOGICIEL ARRETE

M2 : Un attaquant a accès de manière récurrente ou non au disque dur (ou à la clé USB) sur lequel est stocké la base de données afin de retrouver les mots de passe ou les métadonnées associées.

M3 : Un attaquant a accès après l'arrêt de l'application aux mémoires temporaires (RAM par exemple) afin de retrouver les mots de passe ou les métadonnées associées.

M4 : Un attaquant essaie de casser par recherche exhaustive les mots de passe employés pour avoir accès au coffre-fort des mots de passe.

M5 : Un attaquant essaie de casser par recherche exhaustive la clef maître employée pour avoir accès au coffre-fort des mots de passe.

V. FONCTIONS DE SECURITE DU PRODUIT

Les fonctions de sécurité du logiciel Keepass sont les suivantes :

- Génération de mot de passe robuste
- Génération de clé maître robuste
- Authentification de l'utilisateur (contrôle d'accès par mot de passe et/ou fichier clé)
- Chiffrement/déchiffrement des données de la base données
- Intégrité de la base de données (protection et vérification)
- Effacement des données temporaires (dont le presse-papiers)
- Chiffrement des données temporaires
- Déconnexion automatique de la base de données pour prévenir une perte de données et un accès permanent à la base.
- Mécanisme d' « *obfuscation* » des mots de passe et des identifiants de connexion (par exemple « login » de compte Internet) à travers le presse-papiers et la simulation de frappe clavier