*Ce document s'inscrit dans les prérequis à la certification CSPN délivrée par l'ANSSI*

# Cible de sécurité

V1.6

LockSelf

| Version | Date | Description | Auteur |
|---|---|---|---|
| 1.0 | 30.08.2017 | Version initiale pour LockSelf 2.0 | J.Tessier |
| 1.1 | 11.09.2017 | Prise en compte des commentaires d'Amossys | J.Tessier |
| 1.2 | 13.09.2017 | Ajout des mécanismes cryptographiques RSA et TLS | J.Tessier |
| 1.3 | 16.09.2017 | Prise en compte de la reformulation des mécanismes cryptographique. | J.Tessier |
| 1.4 | 13.04.2018 | Modifications en vue de la réévaluation. | J.Tessier |
| 1.5 | 24.04.2018 | Prise en compte des remarques d'Amossys | J.Tessier |
| 1.6 | 01.08.2018 | Modifications en vue de la réévaluation. | L.Tadajewski |

| | |
|---|---|
| **Organisation éditrice** | LockSelf SAS |
| **Lien vers l'organisation** | https://www.lockself.com/ |
| **Nom commercial du produit** | LockSelf |
| **Numéro de la version évaluée** | LockSelf v2.2 sur un noyau Gnu/Linux v4.15.0-32 |
| **Catégorie de produit** | Stockage sécurisé |

# Table des matières

# 1. ARGUMENTAIRE DU PRODUIT

## a. Description générale du produit

**LockSelf** répond aux problématiques de contrôle du stockage, de l'accès et du partage des données sensibles d'une entreprise telles que ses mots de passe ou ses fichiers confidentiels.

- Les mots de passe sont stockés dans le produit LockPass et peuvent être partagés à plusieurs utilisateurs à l'aide des catégories de partage.

- Les fichiers peuvent être stockés dans le produit LockFiles et être partagés et accessibles par d'autres utilisateurs LockSelf à l'aide des répertoires de partage.

- Les fichiers peuvent être stockés et partagés auprès de non-utilisateurs de LockSelf à l'aide du produit LockTransfer. Un mot de passe doit être appliqué sur les fichiers LockTransfer pour ajouter une sécurité à l'accès au fichier en plus du lien unique de téléchargement. Ce mot de passe devra être composé au minimum de 12 caractères et devra comprendre au minimum une majuscule, une minuscule, un chiffre et un caractère spécial. L'entreprise peut prendre la responsabilité de demander lors de l'installation que le mot de passe soit facultatif, ce qui est contraire aux recommandations de sécurité de l'ANSSI.
Ne pas mettre de mot de passe a pour conséquence d'avoir la même clé de chiffrement pour tous les fichiers.

- Les fichiers stockés sur LockFiles n'utilisent pas de mot de passe possiblement défini par l'utilisateur mais se basent sur deux salts stockés dans un fichier de configuration.

LockSelf permet de gérer au travers de sa gestion utilisateur, les accès et l'historique d'utilisation de chaque utilisateur.
Les prestataires pourront bénéficier d'un accès particulier leur donnant accès aux données de l'entreprise sous le contrôle en temps réel de leur responsable.
La gestion utilisateur de LockSelf permet de déléguer la gestion de certains utilisateurs à un ou plusieurs responsables en les assignant à une organisation. La gestion des utilisateurs étant segmentable, celle des partages de mots de passe et fichiers se fait tout aussi simplement en utilisant les catégories de partage, administrable par le ou les responsables d'une organisation.

LockSelf est un gestionnaire de données pour entreprise ayant la particularité d'être disponible en mode Cloud Privé et On-Premises en plus de la classique offre Saas.

Ces deux modes d'installation permettent à l'entreprise utilisatrice de centraliser le stockage des données protégées via la solution LockSelf.
Plus particulièrement :

- Avec l'offre Cloud Privé, les données sont stockées chez un hébergeur certifié, Outscale ;
- L'offre On-Premises permet à une entreprise de stocker les données sur son propre serveur. Pour cette offre, la solution LockSelf sera installée dans un mode "blackbox", l'installation du serveur sera faite par les équipes de LockSelf.

A noter que la certification CSPN est relative à l'installation de LockSelf en On-Premises.

Le chiffrement appliqué par LockSelf sur les données qu'il gère permet de garantir un stockage sécurisé des informations sensibles de l'entreprise.

## b. Description de la manière d'utiliser le produit

L'accès à LockSelf se fait pour chaque utilisateur au travers des plugins Chrome, Firefox et de l'application web.
Une fois l'utilisateur authentifié sur le plugin, il pourra accéder aux différents produits ainsi qu'à la gestion utilisateur si celui-ci a été nommé responsable ou modérateur d'une organisation.
Tout utilisateur pourra donc, en ayant renseigné son code PIN à l'authentification, déchiffrer les données auxquelles il peut accéder, mais également en ajouter pour son usage personnel ou en ajouter dans les différentes catégories de partage et dossier de partage.

## c. Description de l'environnement prévu pour son utilisation

LockSelf peut être utilisé sur Windows, Mac OS ou Linux au travers de leur navigateur web.
La solution LockSelf permettant le choix du lieu de l'hébergement de la solution et du stockage des données, il est possible de l'utiliser en mode cloud public, cloud privé ou on-premises.

## d. Description des hypothèses sur l'environnement

*Postes utilisateurs :*
Les différents plugins LockSelf ou sa webapp doivent être installés et utilisés sur un environnement sain (système d'exploitation et navigateur web) à jour des correctifs en vigueur au moment de l'installation.

*Administration:*
Les administrateurs sont considérés de confiance. Ils sont formés à l'utilisation et l'administration de la TOE ainsi que de l'environnement hébergeant la TOE (systèmes d'exploitation, services, etc.).

*Exploitation:*
Une connexion réseau doit être maintenue entre le client et le serveur hébergeant la solution LockSelf.

*Environnement sécurisé* :
Le serveur LockSelf ainsi que les serveurs participant à la mise en œuvre de la solution sont installés sur des systèmes d'exploitation sains et correctement mis à jour. Les services et partages inutiles sont désactivés.
Les serveurs de la solution LockSelf sont installés au sein d'une DMZ (protégée selon les règles de l'état de l'art et réputée de confiance). En particulier, des moyens techniques sont mis en place en entrée de la DMZ (pare-feu, anti-DDOS, etc.).
Les serveurs de la solution LockSelf sont déployés dans un local dont les accès sont nominativement contrôlés.
Les serveurs de la solution LockSelf sont eux-mêmes sécurisés par l'utilisation de pare-feu, les accès distants se font uniquement par SSH avec une authentification par clé uniquement.
Chaque serveur LockSelf on-premises est accessible par une paire de clef RSA différente.
L'accès SSH des équipes LockSelf est supprimé une fois le déploiement effectué si l'entreprise cliente souhaite gérer elle-même l'infogérance de son serveur LockSelf.

## e. Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit.

L'application web et le plugin navigateur sont compatibles avec les dernières versions des navigateurs Chrome et Firefox.

Le serveur Linux fourni par l'entreprise aux équipes LockSelf pour le déploiement de la solution doit être au minimum sous Ubuntu 16.04, et contenir au minimum 5Go d'espace libre pour l'installation de la solution. Pour l'installation on-premises, les fichiers peuvent être stockés sur le filesystem. Si cette option est retenue par l'entreprise, il faudra prévoir un espace de stockage plus conséquent afin d'y accueillir les fichiers chiffrés.

## f. Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts…) et de leur rôle particulier dans l'utilisation du produit.

Il existe deux types d'utilisateurs pour LockSelf :

**Utilisateur "simple" (sans droit d'administration)**

Il peut accéder aux mots de passe et fichiers qui lui ont été partagés et en ajouter des nouveaux dans LockSelf.

**Administrateur/Modérateur d'organisation**

Il peut faire les mêmes choses que les utilisateurs "simple" mais peut en plus définir les politiques de partage des mots de passe et des fichiers.
Il peut contrôler l'historique de connexion et d'accès aux données des utilisateurs "simple" dont il a la gestion.
Il peut désactiver/activer l'accès à LockSelf de ses utilisateurs et également les supprimer.

## g. Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concerné par l'évaluation.

Seule l'offre « On Premises » de la solution LockSelf sera considérée dans le cadre de l'évaluation.
Seule l'application web hébergée sur le serveur d'évaluation sera utilisée dans le cadre de l'évaluation.

Les données étant stockées sur un unique serveur, il s'agit de valider la sécurité de ce serveur en vérifiant l'absence de faille dans l'API utilisée par les différents plugins ainsi que sur les éventuels services en écoute.

Le déchiffrement des données étant fait sur l'application LockSelf, le chiffrement HTTPS et la surcouche HSTS doivent être validés pour assurer la confidentialité de la transmission des données entre le serveur LockSelf et les plugins des utilisateurs.

# 2. ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT DU PRODUIT

## a. Côté client

L'utilisation de LockSelf nécessite pour chacun des utilisateurs la présence d'un navigateur web, Chrome ou Firefox, recommandés grâce à leur extension permettant une utilisation optimale.
Les autres navigateurs web tel qu'Internet Explorer, Safari ou encore Opera restent compatibles avec LockSelf malgré l'absence d'un plugin qui ne permet donc pas d'accéder aux fonctionnalités de remplissage automatique d'un formulaire et d'ajout automatique d'un nouveau mot de passe pour l'outil LockPass.
Les systèmes d'exploitations grand public tel que Windows, Mac OS et Linux sont tous compatibles via l'utilisation d'un navigateur web.
Pour l'évaluation, seule l'application web hébergée sur le serveur d'évaluation sera utilisée dans le cadre de l'évaluation.

## b. Côté serveur

L'installation de la partie serveur de LockSelf hébergeant et chiffrant les données est à la charge des ingénieurs de LockSelf.
L'installation peut être réalisée sur un serveur directement fourni par l'entreprise utilisatrice et celui-ci doit uniquement présenter un système d'exploitation Linux Ubuntu 16.04 LTS à jour.
Les équipes LockSelf procèdent à l'installation en totale autonomie.

Sont installés :
- Pour PHP, les paquets php-7.0 (Dépendances : common, cli, curl, fpm, readline, mysql, mbstring, mcrypt, pdo, xml)
- Pour Apache, les paquets apache2 et libapache2-mod-php7.0. Apache est installé dans sa dernière version disponible.
- Pour MySQL, mysql-server-5.7. MySQL est installé dans sa dernière version disponible.

Le paquet précompilé OpenSSL (1.0.2g-1ubuntu4.8 1 Mar 2016) provenant des dépôts Ubuntu est nécessaire pour le bon fonctionnement de la TOE.

# 3. BIENS SENSIBLES DEVANT ETRE PROTEGES

**B. Données à protéger**

LockSelf est destiné à protéger en premier lieu les mots de passe et les documents de l'entreprise.

**B. Données Authentification**

Pour accéder aux données chiffrées, un utilisateur doit au préalable déchiffrer sa clé privée en renseignant son code PIN puis se connecter en renseignant ses identifiants.
À noter que le code PIN de l'utilisateur n'est à aucun moment stocké sur le serveur ou en base de données.

**B. Clés**

La paire de clé RSA de chaque utilisateur est stockée en base de données et la clé privée est symétriquement chiffrée en AES 256 CBC avant son stockage.

**B. Flux**

Les flux de la TOE entre les postes clients et le serveur doivent être protégés en intégrité et en confidentialité.

**B. Journaux**

Les évènements générés lors des processus d'authentification et de déchiffrement sont journalisés en base de données (sans chiffrement). Ces données ne sont accessibles que par les utilisateurs responsables ou modérateurs après s'être authentifiés via leur plugin.

# 4. MESURES D'ENVIRONNEMENT

Le produit peut être utilisé dans un environnement Windows, Mac ou Linux et seul un navigateur web et une connexion internet ou intranet vers le serveur de LockSelf est nécessaire pour accéder à l'interface du produit.

Les filesystems de la TOE doivent être en ext4 ou ext3 (data mode=ordered).

L'envoie des SMS comprenant le mot de passe d'un transfert est effectué par l'appel externe à l'API Nexmo (https://developer.nexmo.com/).

Le serveur hébergeant la solution LockSelf doit répondre aux critères cités dans le chapitre 5.

# 5. DESCRIPTION DES MENACES

Les menaces sont diverses et peuvent venir aussi bien d'un acteur interne à l'entreprise, utilisant déjà LockSelf qu'un acteur externe tentant de pénétrer dans LockSelf pour y voler des données.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

**M1. Déchiffrement Illégitime**

Un attaquant (externe ou interne) prend connaissance du contenu des documents chiffrés d'un (autre) utilisateur.

**M2. Élévation Privilèges**

Un acteur interne tentera de profiter de ses privilèges existants pour étendre son contrôle sur des données ne lui étant pas destinées (via une faille applicative ou système).

**M3. Usurpation Identité Utilisateur**

Un acteur externe tentera d'usurper les identifiants d'un acteur interne pour accéder à ses données.

**M4. Écoute Passive**

Un acteur externe écoute les flux générés entre un poste utilisateur et le serveur LockSelf afin de récupérer les données sensibles en confidentialité échangées.

**M5. Man In The Middle**

Un acteur externe pourra tenter une interception des données en attaquant le réseau. Il les modifie dans le but d'altérer les données sensibles en intégrité.

**M6. Alteration des journaux**

Un acteur interne/externe pourra tenter d'altérer les journaux afin de dissimuler ses actions effectuées sur LockSelf.

# 6. SPECIFICATION DES FONCTIONS DEDIEES A LA SECURITE

Le produit implémente différentes sécurités sur le stockage, le transfert des données et les authentifications.

**F1. Chiffrement**

Lors de l'inscription de l'utilisateur, une paire de clés RSA 2048 bits est créée permettant le chiffrement et le déchiffrement des mots de passe. La clé privée est chiffrée en AES-256-CBC à l'aide d'une passphrase, dérivée notamment du code PIN de l'utilisateur. Code PIN qui n'est à aucun moment stocké sur le serveur applicatif ou en base de données. Un chiffrement asymétrique est donc appliqué sur chaque mot de passe créé et partagé dans LockSelf avec la clé publique de l'utilisateur qui doit recevoir une copie du mot de passe.

Les fichiers stockés sur LockSelf sont chiffrés symétriquement en AES 256 CBC à l'aide d'une passphrase.

**F2. Authentification Contrôle Accès**

L'accès à LockSelf se fait par une double authentification, un login/mot de passe est d'abord demandé, si correct, le code PIN est demandé.
L'authentification est conditionnée par la connaissance du PIN pour déverrouiller la clé privée RSA de l'utilisateur.
Une vérification applicative des droits de l'utilisateur est enclenchée à chaque action effectuée sur l'interface.

**F3. Communications Sécurisées**

Le chiffrement du transfert de données entre chaque utilisateur et le serveur LockSelf grâce à l'utilisation du protocole HTTPS sur-couchée avec du HSTS permettant d'éviter les attaques de type Man In The Middle.
Le serveur LockSelf utilise TLS 1.2 uniquement pour le HTTPS ainsi que des ciphers fort.

**F4. Journalisation**

La journalisation des actions d'authentification, d'accès et d'utilisation.

# 7. COUVERTURES

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "D", "I" et "C" représentent respectivement les besoins de Disponibilité, Intégrité et Confidentialité) :

| | B. Données À Protéger | B. Données Authentification | B. Clés | B. Flux | B. Journaux |
|---|---|---|---|---|---|
| M1. Déchiffrement Illégitime | C | | | | |
| M2. Élévation Privilèges | C | C | | | |
| M3. Usurpation Identité Utilisateur | | C | C | | |
| M4. Écoute Passive | | | | C | |
| M5. Man In The Middle | | | | I | |
| M6. Altération Journaux | | | | | I |

*Tableau 1 - Couverture des biens sensibles par les menaces*

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

| | F1. Chiffrement | F2. Authentification Contrôle Accès | F3. Communications Sécurisées | F4.Journalisation |
|---|---|---|---|---|
| M1.Déchiffrement Illégitime | √ | | | |
| M2.Élévation Privilèges | | √ | | |
| M3.Usurpation Identité Utilisateur | | √ | | √ |
| M4.Écoute Passive | | | √ | |
| M5.Man In The Middle | | | √ | |
| M6.AltérationJournaux | | √ | | |

*Tableau 2 - Couverture des menaces par les fonctions de sécurité*