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-2018/23

LockSelf on-premises
Version 2.2

Paris, le 24 décembre 2018

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

Guillaume POUPARD
[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@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2018/23**
Nom du produit **LockSelf on-premises**
Référence/version du produit **Version 2.2**
Catégorie de produit **Stockage sécurisé**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **LockSelf** **10 rue du colonel de Rochebrune** **92500 Rueil Malmaison**
Développeur **LockSelf** **10 rue du colonel de Rochebrune** **92500 Rueil Malmaison**
Centre d'évaluation **Amossys** **4 bis allée du bâtiment, 35000 Rennes, France**
Fonctions de sécurité évaluées **Chiffrement de données stockées** **Authentification et contrôle d'accès des utilisateurs** **Communications sécurisées** **Journalisation**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage **Non**

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 CSPN 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 le « LockSelf on-premises, version 2.2 » développé par *LOCKSELF*. Installé sur un serveur, *LockSelf* a pour but de stocker et de partager de façon sécurisée les données que les utilisateurs y déposent. Pour cela, le produit *LockSelf* se décompose en trois sous-produits :

- *LockFiles* : qui permet de stocker les documents de façon chiffrée ;
- *LockTransfer* : qui permet de transférer les documents stockés par *LockFiles* ;
- *LockPass* : qui permet de stocker et partager les identifiants et mots de passe de façon sécurisée.

Le serveur *LockSelf* peut être déployé suivant deux modes :

- cloud privé : hébergé dans un *Cloud* certifié ;
- *on premises* : hébergé par l'entreprise utilisant la solution *LockSelf*.

L'utilisateur interagit avec le produit au travers de son navigateur web suite à l'installation d'un plugin, pour *LockPass*, qui permet notamment de stocker les mots de passe de l'utilisateur.

La figure ci-dessous explicite l'architecture du produit.

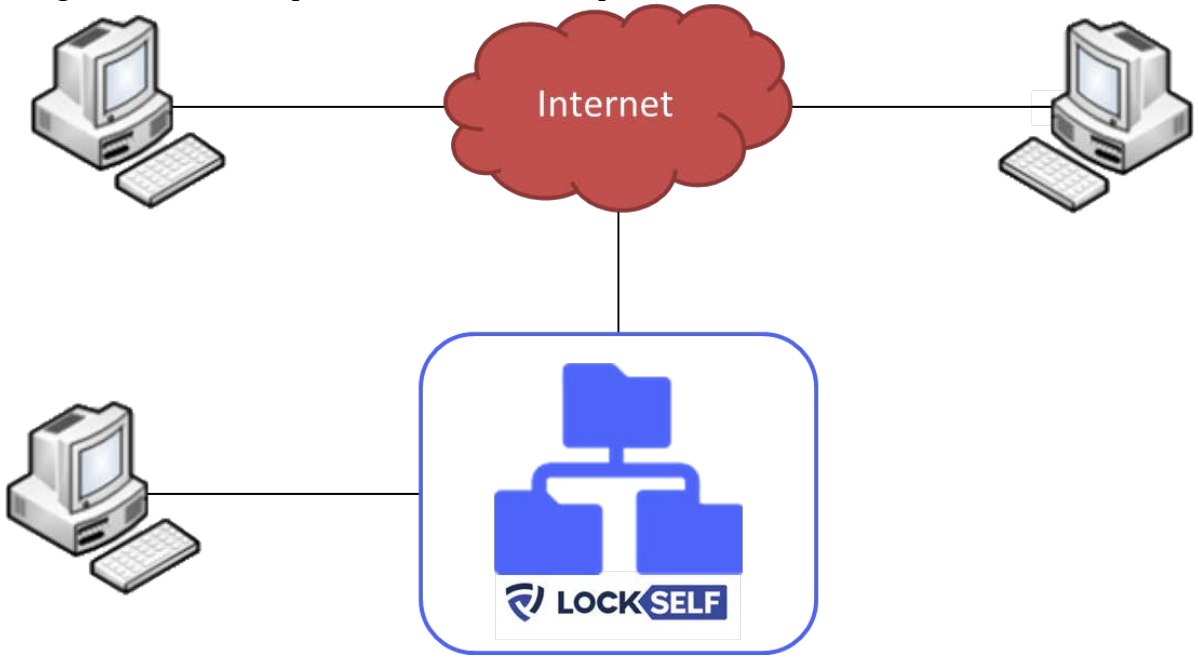

Figure 1 - Architecture Produit.

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 – pare-feu
☐ 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 – environnement d'exécution sécurisé
☐ 11 – terminal de réception numérique (*Set top box*, STB)
☐ 12 – matériel et logiciel embarqué
☐ 13 – automate programmable industriel
☐ 99 – autre

1.2.2. Identification du produit

Nom du produit	LockSelf on-premises
Numéro de la version évaluée	2.2
Numéro de version du plugin	20.2.28

La version certifiée du produit peut être identifiée sur la page de connexion à l'interface web (https://« nom du serveur »/application/). La version 2.2 est alors affichée.

Le plugin est en version 20.2.28 et est identifiable dans le menu des plugins du navigateur. Le résultat du hachage SHA-256 du fichier xpi est le suivant :
a7e9d4db20baa6755485e33c7f5c2498632e3ab4c3c9e0dca342379986396059.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- le chiffrement de données stockées ;
- l'authentification et contrôle d'accès des utilisateurs ;
- les communications sécurisées ;
- la journalisation.

1.2.4. Configuration évaluée

La configuration évaluée correspond à un déploiement de type « *on-premises* », où le serveur est donc hébergé chez l'utilisateur de la solution *LockSelf*. Ce serveur considéré dispose du système d'exploitation *LINUX UBUNTU* 16.04.5 LTS avec noyau 4.15.0-33.

Côté utilisateur final, le navigateur web considéré est *FIREFOX*.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. 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 est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3. Travaux d'évaluation

Les travaux d'évaluation ont été menés sur la base du besoin de sécurité, des biens sensibles, des menaces, des utilisateurs et des fonctions de sécurité définis dans la cible de sécurité [CDS].

2.3.1. Installation du produit

2.3.1.1. Particularités de paramétrage de l'environnement et options d'installation

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

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

L'installation est faite à distance par le développeur. Pour cela une connexion SSH depuis le système d'information du développeur vers le serveur à installer est nécessaire. La copie de la clé publique du développeur dans le fichier `authorized_keys` du serveur, puis l'authentification par certificat sont nécessaires pour procéder à cette installation.

Après installation, il est nécessaire de fermer le flux SSH et de supprimer la clé publique *LockSelf* du serveur, comme indiqué dans le guide d'installation du produit [GUIDES].

2.3.1.3. Durée de l'installation

L'installation dure moins d'une journée.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment détaillée, claire et précise. Elle contient des captures d'écran et des exemples, ce qui en facilite la compréhension et permet d'avoir une prise en mains rapide du produit.

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue du code source et estime que le code est organisé et correctement documenté, chaque interface est bien commentée.

2.3.4. Analyse de la conformité des fonctions de sécurité

Toutes les fonctions de sécurité testées se sont révélées conformes à la cible de sécurité [CDS].

2.3.5. Analyse de la résistance des mécanismes des fonctions de sécurité

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

2.3.6. Analyse des vulnérabilités (conception, construction, etc.)

2.3.6.1. Liste des vulnérabilités connues

Aucune vulnérabilité connue et exploitable affectant la version évaluée du produit n'a été identifiée.

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit.

2.3.8. Analyse de la facilité d'emploi et préconisations

2.3.8.1. Cas où la sécurité est remise en cause

L'évaluateur a constaté que lorsqu'un fichier est partagé via *LockTransfer*, si l'utilisateur omet de mettre un mot de passe, celui par défaut est utilisé. Il est donc important que l'utilisateur choisisse un mot de passe spécifique pour transférer le document.

Il est également important de respecter la section *Configuration SSH* du guide d'installation du produit [GUIDES] afin de fermer le flux SSH et de supprimer la clé publique *LockSelf* du serveur.

2.3.8.2. Recommandations pour une utilisation sûre du produit

Il est important que l'utilisateur choisisse un mot de passe pour transférer le document lors de l'utilisation de *LockTransfer*.
Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté.

2.3.8.4. Notes et remarques diverses

Aucune note, ni remarque n'a été formulée dans le [RTE].

2.4. Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le générateur aléatoire du produit a été analysé au titre de cette évaluation CSPN. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

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 « LockSelf on-premises, version 2.2 » 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 spécifiés dans la cible de sécurité [CDS], et mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Cependant l'évaluation a mis en avant des restrictions d'usage à respecter pour une utilisation sécurisée du produit décrites ci-après :

- après installation il est important de fermer le flux SSH et de supprimer la clé publique *LockSelf* du serveur accueillant le produit ;
- l'utilisateur doit choisir un mot de passe spécifique pour transférer un document lors de l'utilisation de *LockTransfer*.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité* Version : *1.6* ; Date : *1 aout 2018.*
[RTE]	*Rapport Technique d'Évaluation CSPN, Produit LockSelf - version 2.2* Référence : CSPN-RTE-LockSelf3-1.02 ; Version : 1.02 ; Date : *28 novembre 2018.*
[ANA-CRY]	*Expertise des mécanismes cryptographiques, Produit LockSelf - version 2.2* Référence : CSPN-CRY-LockSelf3-1.01 ; Version : 1.01 ; Date : *26 novembre 2018.*
[SPEC-CRY]	*Mécanismes cryptographiques* Version : 1.4 ; Date : *24 aout 2018.*
[GUIDES]	Guide d'utilisation du produit : – *Guide utilisateur Solution LockPass ;* – *Guide utilisateur Solution LockTransfer.* Guide d'installation du produit : – *Déploiement On-Premises, Guide de déploiement, LockSelf. Ubuntu 16.04 LTS.*

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 des produits des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.