PREMIER MINISTRE

Liberté
Égalité
Fraternité

Agence nationale de la sécurité
des systèmes d'information

Secrétariat général de la défense et de la sécurité nationale

Rapport de certification ANSSI-CSPN-2021/08

PARSEC

Version 2.0.0

Paris, le 16 avril 2021

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti 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-2021/08**
Nom du produit **PARSEC**
Référence/version du produit **Version 2.0.0**
Catégorie de produit **Stockage sécurisé**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **SCILLE** 11 chemin de Jalès 33160 Saint-Médard-en Jallès, France
Développeur **SCILLE** 11 chemin de Jalès 33160 Saint-Médard-en Jallès, France
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Stockage sécurisé en confidentialité et intégrité des données Non répudiation et l'authenticité des données stockées Contrôle d'accès aux données Authentification des utilisateurs Protection en confidentialité des workspaces Gestion des utilisateurs Vérification de la chaine de confiance Non répudiation des terminaux Authentification des terminaux Transfert sécurisé du compte vers un nouveau terminal
Fonctions de sécurité non évaluées Néant
Restriction(s) d'usage Non

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information 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 MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « PARSEC, Version 2.0.0 » développé par SCILLE.

PARSEC est une solution *open-source* pour le partage sécurisé de données sensibles dans le nuage (*cloud)*. Pour cela le produit apporte une couche de protection sous forme d'enclave (ou *workspace*), permettant la segmentation des utilisateurs, et de chiffrement des données.

La solution PARSEC se décompose en trois parties :
- le client PARSEC ;
- le serveur de métadonnées ;
- le serveur de stockage.

Le logiciel client PARSEC va sécuriser les données sensibles avant qu'elles ne soient stockées sur les *clouds*, en procédant en trois étapes :
- le découpage en blocs des fichiers avant chiffrement ;
- le chiffrement de chaque bloc par une clé symétrique différente ;
- le chiffrement des métadonnées par la clé privée de l'utilisateur.

Les serveurs de métadonnées et de stockage vont ensuite agir comme un disque dur. Le serveur de métadonnées stocke les métadonnées permettant la reconstruction des fichiers. Le serveur de stockage lui va stocker les blocs chiffrés.

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

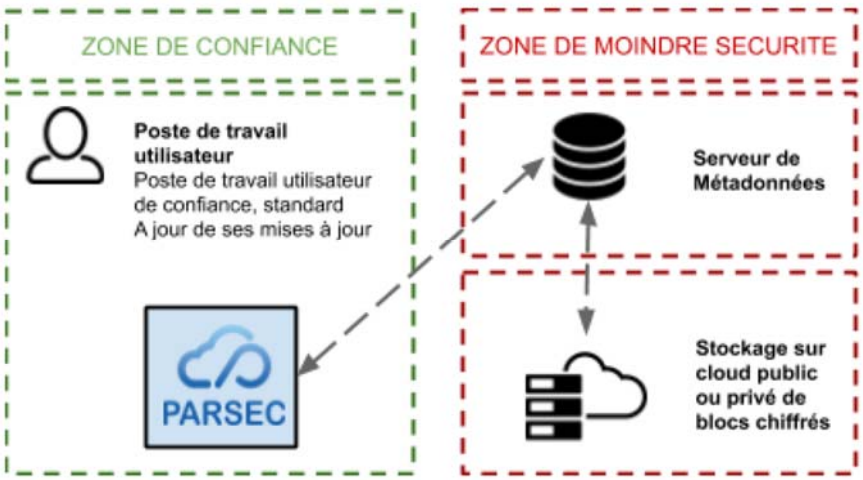

Figure 1 - Architecture Produit.

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*

Produit	
Nom du produit	PARSEC
Numéro de la version évaluée	Version 2.0.0

La version certifiée du produit peut être identifiée dans le menu « A propos » :

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le stockage sécurisé en confidentialité et intégrité des données ;

- la non répudiation et l'authenticité des données stockées ;
- le contrôle d'accès aux données ;
- l'authentification des utilisateurs ;
- la protection en confidentialité des *workspaces* ;
- la gestion des utilisateurs ;
- la vérification de la chaine de confiance ;
- la non répudiation des terminaux ;
- l'authentification des terminaux ;
- le transfert sécurisé du compte vers un nouveau terminal.

1.2.4 *Configuration évaluée*

Le client lourd Parsec doit être exécuté par un système d'exploitation mono-utilisateur.

La plateforme de test est constituée des éléments suivants :

- le client lourd Parsec en version 2.0.0, exécuté dans une machine virtuelle Windows 10 Pro x64 ;
- le serveur de métadonnées en version 2.0.0, exécutant Ubuntu 18.04.5.

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 B.

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 a été faite en suivant les guides du développeur [GUIDES]. Ces guides décrivent les étapes d'installation du serveur de métadonnées et de son environnement ainsi que du client.

2.3.1.3 Durée de l'installation

Le temps d'installation du produit est relativement court.

2.3.1.4 Notes et remarques diverses

Néant.

2.3.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'intégralité du produit.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS] et pour le niveau d'attaquant considéré.

2.3.7 *Analyse de la facilité d'emploi*

2.3.7.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.7.2 Avis d'expert sur la facilité d'emploi

Le client lourd n'a aucune option de configuration par l'utilisateur et l'évaluateur n'a identifié aucune configuration non sécurisée pouvant résulter d'une mauvaise manipulation de l'utilisateur.

2.3.7.3 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 (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) pouvant être exploitable.

2.5 Analyse du générateur d'aléas

Le générateur aléatoire du produit mis en œuvre par le produit a fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [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 « PARSEC, Version 2.0.0 » 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 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de Sécurité CSPN Date : 16 mars 2021.
[RTE]	Rapport Technique d'Évaluation CSPN PARSEC - PARSEC Référence : OPPIDA/CESTI/PARSEC/RTE/1.1 ; Version : 1.1 ; Date : 28 janvier 2021.
[GUIDES]	Guide d'installation : Parsec-v2_0_0-GuideInstallation-MetadataServer ; Version : 3 ; Date : 10 mars 2021. Guide d'utilisation : Parsec-v2_0_0-Guide-Utilisation ; Date : 23 février 2021.

ANNEXE B. 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, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. 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.