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-2026/18

PARSEC

VERSION 3.7.10

Paris, le 27/7/2026 | 12:09 CEST

Vincent Strubel

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-2026/18**
Nom du produit **PARSEC**
Référence/version du produit **VERSION 3.7.10**
Catégorie de produit **Stockage sécurisé**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **SCILLE SAS** 11 chemin de Jalès 33160 SAINT-MEDARD-EN-JALLES, France
Développeur **SCILLE SAS** 21, rue de la Division du Général Leclerc 94250 GENTILLY, France
Centre d'évaluation **OPPIDA** 6 - 8 rue Firmin Gillot 75015 - Paris, France
Fonctions de sécurité évaluées Confidentialité des données Intégrité des données, non répudiation et authenticité Authentification des utilisateurs Transmission sécurisée des informations lors de l'enrôlement et authentification des terminaux Sécurité de contrôle d'accès et rotation de la clé de chiffrement d'un espace de travail Gestion des utilisateurs et de leurs droits Administration du serveur de métadonnées Sécurité des données de séquestre
Fonctions de sécurité non évaluées Sans objet
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 cyber.gouv.fr.

TABLE DES MATIERES

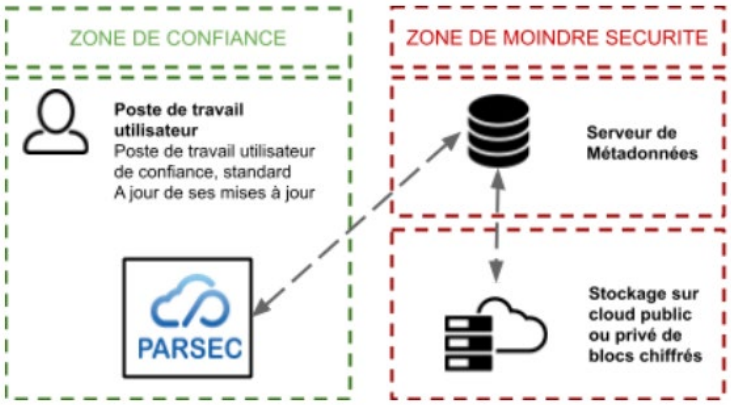
1 Le produit

1.1 Présentation du produit

Le produit évalué est « PARSEC, VERSION 3.7.10 » développé par SCILLE SAS.

Ce produit est un ensemble de composants logiciels libres disponible sous forme de logiciel desktop pour la gestion collaborative de fichiers. Le partage sécurisé est effectué par point de montage ou via une interface utilisateur dédiée. Le produit sécurise les données sensibles avant qu'elles ne soient stockées sur les *clouds* publics.

La figure ci-dessous explicite l'architecture du 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 malveillants
☐	3	Pare-feu
☐	4	Passerelle-multiniveau
☐	5	Effacement de données
☐	6	Administration et supervision de la sécurité
☐	7	Moyen d'authentification numérique
☐	8	Système de contrôle d'accès physique
☐	9	Communication sécurisée
☐	10	Messagerie sécurisée
☒	**11**	**Stockage sécurisé**
☐	12	Environnement d'exécution sécurisé
☐	13	Matériel avec logiciel embarqué
☐	14	SCADA
☐	15	Automate programmable industriel
☐	16	Système de vidéoprotection
☐	99	Autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	PARSEC
Numéro de la version évaluée	VERSION 3.7.10

La version certifiée du produit peut être identifiée de la manière suivante :

- Afin d'identifier la version installée du produit, l'évaluateur démarre le client lourd. Il peut alors accéder à un onglet « A propos » permettant d'identifier la version évaluée

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- confidentialité des données ;
- intégrité des données, non répudiation et authenticité ;
- authentification des utilisateurs ;
- transmission sécurisée des informations lors de l'enrôlement et authentification des terminaux ;
- sécurité de contrôle d'accès et rotation de la clé de chiffrement d'un espace de travail
- gestion des utilisateurs et de leurs droits ;
- administration du serveur de métadonnées ;
- sécurité des données de séquestre.

1.2.4 *Configuration évaluée*

L'installation de la plateforme d'évaluation a consisté en l'installation de plusieurs machines Windows servant d'hôte aux clients Parsec et en l'installation d'une machine Ubuntu servant d'hôte au serveur

Client :PARSEC

2 machines Windows, :

- Windows 10 Enterprise LTSC 21H2
- Windows 11 Enterprise LTSC 24H2

Serveur :

Une machine Ubuntu 24.04 a servi d'hôte au serveur.

L'installation du serveur de métadonnée requiert de déployer une base de données, un serveur SMTP, d'installer ou d'acheter du stockage cloud, et de connecter tous ces éléments entre eux.

L'installation a été réalisée via docker. Il y a 2 BDD, celle contenant la configuration, qui est un postgreSQL, et celle hébergeant les données, qui est un S3 minio. Le STMP est un mailhog v1.0.1.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN] et aux dispositions de [NOTE-06].

2.2 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].

2.2.1 *Installation du produit*

2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation

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

2.2.1.2 Description de l'installation et des non-conformités éventuelles

Sans objet

2.2.1.3 Notes et remarques diverses

La documentation d'installation est claire et indique bien que la configuration utilisée pour l'évaluation sert uniquement dans le cadre de tests.

2.2.2 *Analyse de la documentation*

L'installation du client lourd a été réalisée en moins de 5 minutes selon les [GUIDE] fournis par le développeur. Il peut être suivi sans difficulté par un utilisateur grand public.

L'installation du serveur de métadonnée, quant à elle, requiert des compétences en administration de systèmes informatiques. En effet, il est nécessaire de déployer une base de données, un serveur SMTP, d'installer ou d'acheter du stockage cloud, et de connecter tous ces éléments entre eux.

2.2.3 *Revue du code source (facultative)*

Le code source n'a pas fait l'objet d'une revue dans le cadre de cette l'évaluation.

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.

2.2.4 *Analyse de la conformité des fonctions de sécurité*

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

2.2.5 *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.

2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

2.2.6.1 Liste des vulnérabilités connues

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS].

2.2.6.2 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.

2.2.7 *Analyse de la facilité d'emploi*

2.2.7.1 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.

2.2.7.2 Avis d'expert sur la facilité d'emploi

L'installation du serveur de métadonnée requiert des compétences en administration de systèmes informatiques. En effet, il est nécessaire de déployer une base de données, un serveur SMTP, d'installer ou d'acheter du stockage cloud, et de connecter tous ces éléments entre eux.

2.2.7.3 Notes et remarques diverses

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

2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

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 3.7.10 » 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.

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 suivre les recommandations se trouvant dans les guides fournis [GUIDES].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - Cible de Sécurité CSPN PARSEC, référence : PARSEC-CSPN-CDS-01_v1.4, version 1.4, 02/02/2026
[RTE]	Rapport technique d'évaluation : - Rapport Technique d'Evaluation CSPN PARSEC version 3.7.10 - PARSEC3, référence : OPPIDA/CESTI/2026/PARSEC3/RTE, version 1.1, 15/06/2026
[GUIDES]	Guide d'utilisation et d'installation du produit : - Documentation en ligne à l'adresse https://docs.parsec.cloud/en/v3.7.10/

ANNEXE B. Références liées 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, version 7.0,12 mai 2026. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, 12 juillet 2024 Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0, 12 juillet 2024.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.2, 18 mars 2025.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[NOTE-06]	Note d'application - Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de *cloud computing*, référence ANSSI-CSPN-NOTE-06, version 1.0, 2 mars 2021.