



**PREMIER
MINISTRE**

*Liberté
Égalité
Fraternité*

**Secrétariat général de la défense
et de la sécurité nationale**

Agence nationale de la sécurité
des systèmes d'information

Rapport de certification ANSSI-CSPN-2022/09

S3Box Version 1.9

Paris, le 26 juillet 2022

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

Guillaume POUPARD

[ORIGINAL SIGNE]



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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification	ANSSI-CSPN-2022/09
Nom du produit	S3Box
Référence/version du produit	Version 1.9
Catégorie de produit	Anti-virus, protection contre les codes malicieux
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	HOGO BUSINESS SERVICES SAS Rue du Tram, 35520 La Meziere
Développeur	HOGO BUSINESS SERVICES SAS Rue du Tram, 35520 La Meziere
Centre d'évaluation	OPPIDA 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées	Contrôle des fichiers par rapport à une base d'anti-virus/malware Filtrage des fichiers Journalisation Authentification des administrateurs Mise à jour
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 www.ssi.gouv.fr.

TABLE DES MATIERES

1	Le produit.....	6
1.1	Présentation du produit.....	6
1.2	Description du produit évalué.....	7
1.2.1	Catégorie du produit.....	7
1.2.2	Identification du produit.....	7
1.2.3	Fonctions de sécurité.....	7
1.2.4	Configuration évaluée.....	7
2	L'évaluation.....	8
2.1	Référentiels d'évaluation.....	8
2.2	Travaux d'évaluation.....	8
2.2.1	Installation du produit.....	8
2.2.2	Analyse de la documentation.....	8
2.2.3	Revue du code source (facultative).....	8
2.2.4	Analyse de la conformité des fonctions de sécurité.....	8
2.2.5	Analyse de la résistance des mécanismes des fonctions de sécurité.....	8
2.2.6	Analyse des vulnérabilités (conception, construction, etc.).....	9
2.2.7	Analyse de la facilité d'emploi.....	9
2.3	Analyse de la résistance des mécanismes cryptographiques.....	9
2.4	Analyse du générateur d'aléa.....	9
3	La certification.....	10
3.1	Conclusion.....	10
3.2	Recommandations et restrictions d'usage.....	10
ANNEXE A.	Références documentaires du produit évalué.....	11
ANNEXE B.	Références liées à la certification.....	12

1 Le produit

1.1 Présentation du produit

Le produit évalué est « S3Box, Version 1.9 » développé par HOGO Business Services.

Ce produit est de type « station blanche » destiné à être utilisé pour permettre des transferts de données sécurisés d'un domaine non maîtrisé vers un domaine de confiance. Plus précisément, S3Box permet de :

- se protéger de l'introduction de virus et de code malveillants dans un système d'information sensible ;
- importer des données dans un système d'information sensible sans connecter directement une unité de stockage USB (type clé USB) ;
- valider l'utilisation de support de stockage USB selon une liste autorisée ;
- éviter les fuites d'informations *

Pour cela, S3Box se base sur trois fonctions :

- contrôle d'accès des périphériques utilisable sur le produit (sélection sur la base de liste-blanche) ;
- filtrage par type de fichier (extension, type MIME, signature...) ;
- contrôle anti-virus.

La figure ci-dessous explicite l'architecture globale de la solution à laquelle est intégrée le produit.

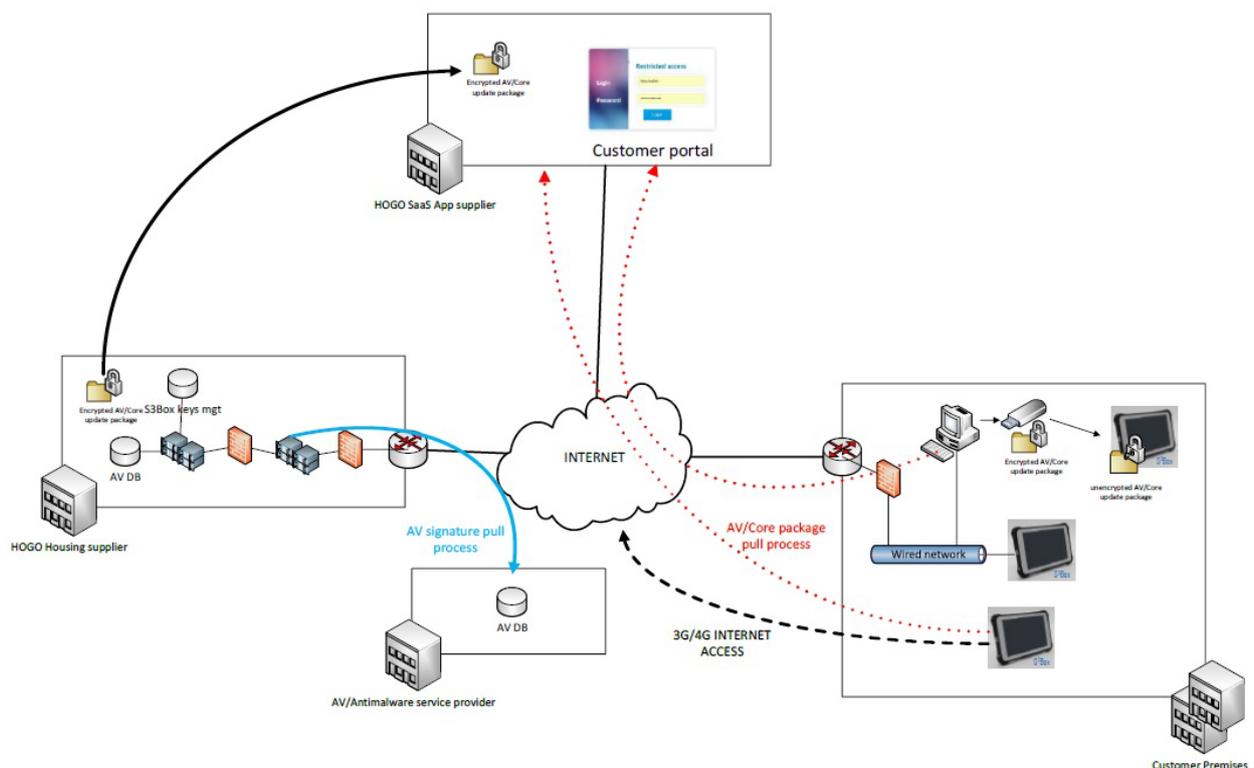


Figure 1 - Architecture globale de la solution.

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

<input type="checkbox"/>	1	détection d'intrusions
<input checked="" type="checkbox"/>	2	anti-virus, protection contre les codes malicieux
<input type="checkbox"/>	3	pare-feu
<input type="checkbox"/>	4	effacement de données
<input type="checkbox"/>	5	administration et supervision de la sécurité
<input type="checkbox"/>	6	identification, authentification et contrôle d'accès
<input type="checkbox"/>	7	communication sécurisée
<input type="checkbox"/>	8	messaging sécurisée
<input type="checkbox"/>	9	stockage sécurisé
<input type="checkbox"/>	10	environnement d'exécution sécurisé
<input type="checkbox"/>	11	terminal de réception numérique (<i>Set top box, STB</i>)
<input type="checkbox"/>	12	matériel et logiciel embarqué
<input type="checkbox"/>	13	automate programmable industriel
<input type="checkbox"/>	99	autre

1.2.2 Identification du produit

Produit	
Nom du produit	S3Box
Numéro de la version évaluée	Version 1.9
Référence	Build_2021082501

La version certifiée du produit peut être identifiée depuis la page d'accueil de l'interface du produit en allant dans le menu « Paramètres » puis « Mise à jour » et finalement « Informations de version ». Il est à noter que l'utilisateur doit rentrer le mot de passe d'administration de la tablette pour accéder au menu « Paramètres ».

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- contrôle des fichiers par rapport à une base d'anti-virus/*malware* ;
- filtrage des fichiers ;
- journalisation ;
- authentification des administrateurs ;
- mise à jour.

1.2.4 Configuration évaluée

La configuration évaluée, qui constitue également la plateforme de test, correspond à une station blanche « S3Box » sur laquelle l'évaluateur a appliqué les configurations décrites dans les guides d'utilisation [GUIDES].

Les caractéristiques techniques du produit sont décrites dans la section 1.6 de la cible de sécurité [CDS].

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

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

Le produit ne nécessite pas d'installation et est fonctionnel dès sa livraison.

2.2.1.3 Notes et remarques diverses

Sans objet.

2.2.2 Analyse de la documentation

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.

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

2.2.3 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.

2.2.4 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 inexploitable pour le niveau d'attaquant considéré 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

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

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

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

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 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.

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 a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. 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.

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 « S3Box, Version 1.9 » 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 : <ul style="list-style-type: none">- HR-CS-18-007 Cible de Sécurité CSPN, version 5, 12 juillet 2021.
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none">- Rapport Technique d'Evaluation CSPN, référence OPPIDA/CESTI/HOGO/RTE/2.2, version 2.2, 22 juin 2022.
[GUIDES]	Guides d'utilisation du produit : <ul style="list-style-type: none">- S3Box Manuel utilisateur, référence HR-MD-18-001, version 3.0 ;- Mise en place d'un serveur de dépôt minimaliste pour les bornes S3, référence NT-HR-21-093.

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 4.0, 3 mars 2022. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 4.0, 28 mars 2020. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 3.0, 6 septembre 2018.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1, 26 janvier 2021.
[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.