HR-CS-18-007
Cible de Sécurité CSPN

Projet S3Box

Ce document constitue la cible de sécurité du produit S3Box dans le cadre d'une évaluation CSPN.

2021

Approbation du document

REDACTION	VERIFICATION	APPROBATION
Quentin RUILLERE	Franck DI NOCERA	Quentin RUILLERE

Historique des versions

Version	Date	Description
1	**18/06/2018**	Version initiale
2	**20/08/2020**	Mise à jour du document : • Changement du template • Mise à jour de la version du Core S3Box concerné • Modification du protocole de la méthode de mise à jour réseau (vers HTTPS)
3	**20/01/2021**	Modification de la mention « Smart Scan » conformément à la version V1.8 (Smart-Transfer) pour plus de clarté.
4	**08/02/2021**	Mention du Build en plus de la version du S3Core dans l'identification du produit
5	**12/07/2021**	Mise à jour du document suite au RTE V1.1 : • Mise à jour du visuel (photos) pour un rendu plus réaliste et précis • Mise en cohérence de la nomenclature des fonctions de sécurité, • Intégration de la fonction FS#03 à l'évaluation, mise à jour des menaces et de la description du produit en conséquence • Mise à jour de la version du S3Core • Ajout des hypothèses « Correct HTTPS configuration », « safe key ID management », « Safe Certificate management» , « Filtered archives » et « Controlled AV downgrade » • Basculement des biens [Update] « Environnement » vers « Produit »

Documents de référence

Référence	Nom du document	Description
1	**HR-NT-18-0113**	Spécifications Cryptographiques S3Box
2	**HR-MD-18-001**	S3Box Manuel utilisateur
3	**HR-DS-18-003**	Spécifications S3Box
4	**RTE/1.1**	Rapport OPPIDA/CESTI/HOGO/RTE/1.1
5	**DAT-NT-012/ANSSI/SDE/NP**	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation

Table des matières

1 Identification du produit

Editeur	HOGO Business Services
Site internet de l'éditeur	https://www.hogo.eu/
Nom commercial du produit	S3BOX
Version évaluée	**V1.9-build_2021082501**
Catégorie de produit	Station blanche - Passerelle de décontamination

1.1 Description générale du produit

Hogo Smart Secure Sanitizer Box (***S3BOX***) est un produit de type « station blanche » permettant :

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

L'objectif général de S3BOX est de permettre des transferts de données sécurisés d'un domaine non maitrisé vers un domaine sensible (de confiance).

La S3BOX se base pour cela sur les trois fonctions suivantes :

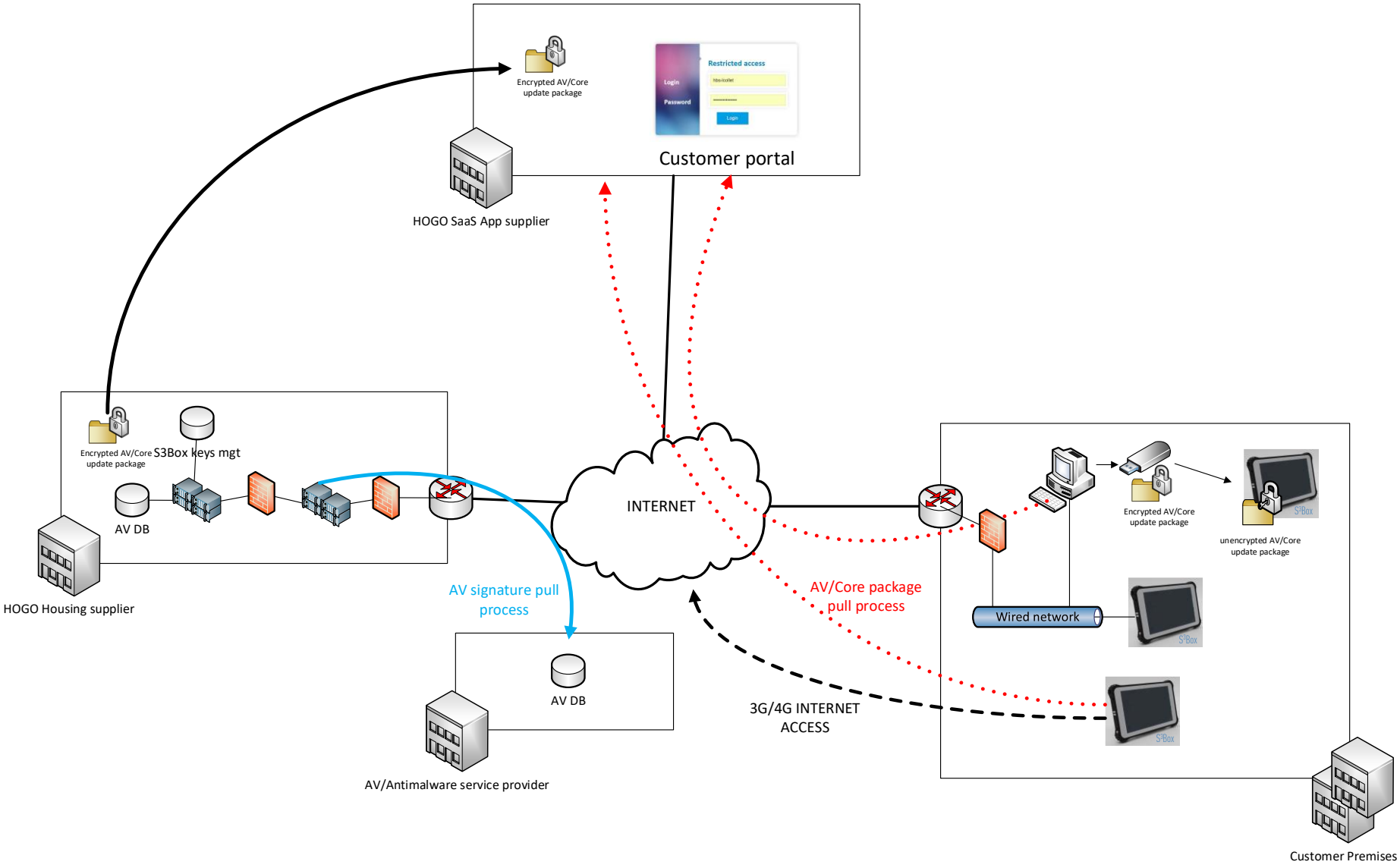
- Contrôle d'accès des périphériques utilisable sur le produit (sélection sur la base de liste-blanche) ;
- Filtrage par type de fichier (Extension, type MIME, signature…) ;
- Contrôle anti-virus.

Ces caractéristiques principales sont la robustesse, la stabilité, la mobilité, et la facilité d'intégration dans n'importe quel environnement client (pas de driver à installer, taille réduite du produit).

1.2 Visuel de la S3Box en version 8 pouces

1.3 Architecture globale

La S3Box est intégrée dans une architecture globale qui permet aux utilisateurs finaux de disposer d'un support technique et des mises à jour logicielles et antivirales.



Cette architecture autour du produit S3BOX contient les éléments suivants :

Le ***key management server*** qui fournit la gestion :

- Des clés publiques utilisées par les S3BOX afin de chiffrer les mises à jour reçues par l'utilisateur final sur sa propre S3B0X ;
- Des clés de signatures utilisées pour signer les données envoyées aux S3BOX.
- Des mises à jour antivirus (en lien direct avec les sites des fournisseurs de solutions anti-virus qui fournissent les fichiers de base mises à jour, qui sont récupérées puis sécurisées).

De plus, le **key management server** a pour fonction de préparer et mettre à disposition des utilisateurs finaux les mises à jour nécessaires au fonctionnement de S3BOX (anti-virus, S3BOX core software, système d'exploitation).

Le **customer portal** qui héberge et mets directement à disposition des utilisateurs finaux les mises à jour préparées par le **key management server**.

Il est à noter que les composants suivants : *key management server* et *customer portal* sont situés chez des hébergeurs.

1.4 Fonctions de sécurité du produit

Les fonctions de sécurité implémentées dans la S3Box sont les suivantes :

FS#01 Anti-virus/malware scan
La S3BOX met en œuvre une protection anti-virus/anti-malware sur la base de moteurs anti-virus (Clam-AV, Eset…) qui réalisent des analyses consécutives.

FS#02 Filtrage des fichiers
La S3BOX réalise un filtrage des fichiers permettant de n'autoriser que ceux stockés sur une clef USB donnée, ou ayant un type MIME précis, ou encore ayant été signés (certificat PGP).

FS#03 Journalisation
La S3Box permet la journalisation locale des évènements de sécurité du produit. Il est également possible d'exporter les évènements sur une clé USB.

FS#04 Authentification des administrateurs
La S3Box intègre un mécanisme d'authentification par mot de passe, qui permet aux utilisateurs authentifiés (i.e. « administrateurs ») d'accéder à des fonctions spécifiques de la S3Box.

FS#05 Mise à jour
La S3Box intègre des fonctions de mise à jour sécurisées pour ses définitions antivirales et son logiciel « core ». Ces mises à jour peuvent être appliquées via une clef USB (mode « manuel »), via une connexion LAN via HTTPS (mode « LAN »), ou via Internet (mode « En ligne »).

Pour plus d'information sur les fonctions de sécurité considérées dans le cadre de l'évaluation CSPN, se reporter au chapitre **Erreur ! Source du renvoi introuvable.**.

1.5 Utilisation du produit

La S3Box est prévue pour être utilisée dans n'importe quel contexte où des utilisateurs souhaitent transférer des données entre un environnement non maîtrisé ou hostile et un environnement de confiance. Pour ces transferts, les utilisateurs souhaitent avoir la garantie que :

- Aucun virus ou malware n'est transmis avec les données ;
- Aucune donnée de l'environnement de confiance n'est divulguée vers l'environnement externe
- Seuls les périphériques de stockage USB autorisés peuvent être utilisés dans les transferts.

La S3BOX possède deux cas d'usage principaux :

- ***Scan only*** : dans ce cas, un seul périphérique de stockage est utilisé. La S3BOX effectue une analyse antivirus de ce périphérique et affiche un rapport :

- ***Smart-Transfer*** : dans ce cas d'usage deux périphériques sont utilisés, un sur l'environnement non maîtrisé ou hostile et un sur l'environnement de confiance. La S3Box effectue une analyse antivirus et un filtrage des fichiers. Seuls les fichiers autorisés et sains sont transférés sur le périphérique de confiance :

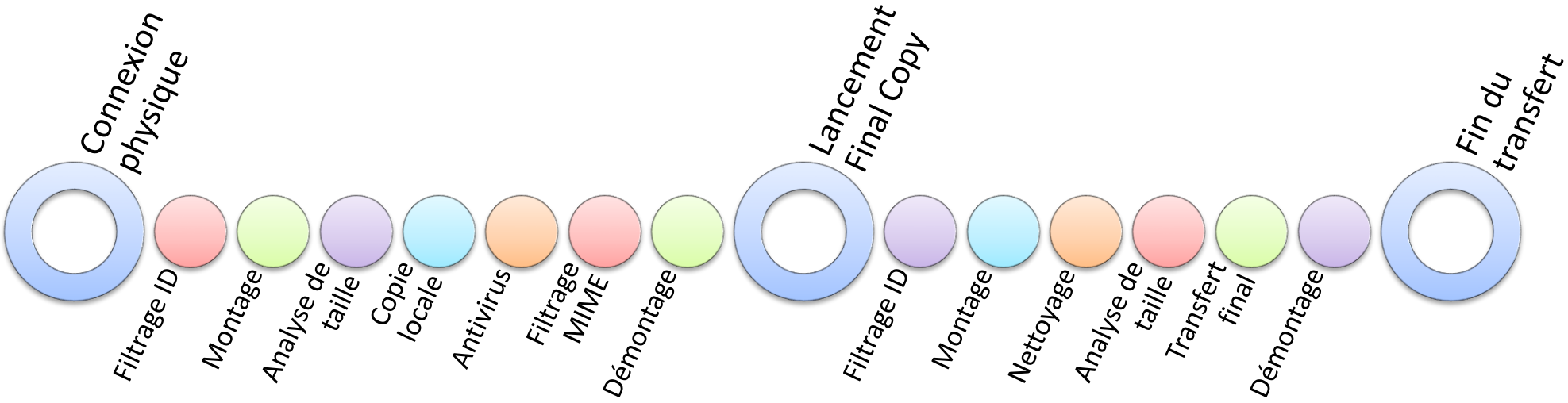
Cette fonction Smart-Transfer produit un journal d'analyse et de transfert qui est consultable sur la S3Box directement après le transfert. Ce journal peut, avec les autres journaux internes de la S3Box, être exporté sur un périphérique USB, chiffré et signé par le certificat interne propre à la S3Box.

Pour simplifier la visualisation des journaux à l'écran (journaux de scan et autres journaux internes de la S3Box, accessible dans l'interface d'administration), Hogo s'est basé sur les recommandations de l'ANSSI pour sélectionner les évènements affichés, conformément au document [5]. De plus nombreux messages peuvent être exportés sur le périphérique USB dans les fichiers chiffrés.

A noter : L'administrateur a la possibilité de « purger » les journaux de la S3Box. Cette action de suppression est irréversible. Il s'agit d'une fonction authentifiée (demandant le code d'administration de la S3Box), donc considéré comme protégé dans le cadre de l'hypothèse [Admins are not evil], cf. chapitre 2.2.

La fonction Smart-Transfer peut être réalisée soit sur l'intégralité du contenu du périphérique USB venant de l'environnement non maîtrisé ou hostile, soit sur un sous-ensemble de ce contenu, après une sélection manuelle des données à analyser et à transférer.

La fonction Smart-Transfer réalise le chronogramme de traitement suivant (les ronds évidés représentent les actions utilisateur, les ronds pleins celles de la S3Box) :



Dans le cadre de l'évaluation CSPN, seul le cas d'usage "Smart-Transfer" est considéré.

Les fonctions de sécurité suivantes **sont dans le périmètre d'évaluation :**

- FS#01 Anti-virus/malware scan
- FS#02 Filtrage des fichiers, sous-fonctions :
  - FS#0201 Filtrage par type MIME
  - FS#0202 Filtrage par clef USB Support (key_ID)
  - FS#0203 Filtrage par signature (certificat PGP)
- FS#03 Journalisation
- FS#04 Authentification des administrateurs
- FS#05 Mise à jour de la S3BOX, sous-fonctions :
  - FS#0501 Mise à jour du core mode Manuel via USB
  - FS#0502 Mise à jour Anti-Virus mode Manuel via USB
  - FS#0503 Mise à jour du core mode LAN (réseau local)
  - FS#0504 Mise à jour Anti-Virus mode LAN (réseau local)

Les fonctions suivantes **ne font pas partie du périmètre d'évaluation** :

- FS#02 Filtrage des fichiers, sous-fonction :
  - Sélection manuelle des fichiers
- FS#05 Mise à jour de la S3BOX, sous-fonctions :
  - Mise à jour du core mode « En ligne » (via Internet)
  - Mise à jour Anti-Virus mode « En ligne » (via Internet)

L'efficacité de la fonction anti-virus est également exclue (il n'est vérifié pour cette fonction que la mise en œuvre : configuration, utilisation des bases de signature…).

Pour plus d'information sur les fonctions de sécurité considérées dans le cadre de l'évaluation CSPN, se reporter au chapitre **Erreur ! Source du renvoi introuvable.**.

1.6 Environnement d'utilisation

La S3BOX qui est testée dans le cadre de la certification CSPN a pour version V1.9-build_2021082501.
Elle possède les caractéristiques suivantes :

Matériel :

- Security:
  - Embedded chipset TPM - capable
  - BIOS – secure boot capable
- Screen:
  - Multipoint touchscreen (reco. 1280x800 resolution)
  - High Glass protection (anti-scratch)
- CPU/Memory:
  - Intel architecture CPU
  - Minimum RAM 2GB and ROM flash (internal memory) 64 GB
- Network and connectivity:
  - Wi-Fi b/g/n
  - 4G LTE
- Connectors:
  - one USB connector and one micro USB for OTG USB (on-the-go)
  - one SD-card slot
- Certification:
  - CE / FCC / RoHS / Reach
  - Industrial version: MIL-STD810G

Logiciel :

- Operating system: Linux Ubuntu 20.04 (version LTS, supportée jusqu'en Avril 2025)
- Main software packages
  - GnuPG2 (logiciel permettant la gestion des routines de cryptage PGP, version 2.2.19)
  - ClamAV (logiciel antivirus, version 0.103.2)
  - Python3.9 (gestion du langage Python – version LTS, supportée jusqu'en Octobre 2025)

2 Environnement de sécurité

2.1 Utilisateurs

Les utilisateurs qui peuvent interagir avec la S3BOX sont :

Administrateur	Utilisateur authentifié sur la S3BOX qui possède des droits pour modifier la politique de sécurité ainsi que des paramètres généraux de la S3BOX.
Utilisateur	Une personne ayant un accès physique à la S3BOX et qui l'utilise pour transférer des données.

2.2 Hypothèses

Event log viewing	Il est considéré que les administrateurs consultent régulièrement les évènements de sécurité enregistrés par la S3BOX.
Trained user	Les utilisateurs de la S3BOX sont formés à son utilisation.
Administrators not evil	Les administrateurs de la S3Box sont formés aux tâches d'administration qu'ils doivent réaliser. Par ailleurs il est considéré que les administrateurs sont de confiance.
Safe filtering policy	Il est considéré que la politique de sécurité (filtrage Mime, contrôle USB,…) est adaptée au cas d'usage de l'utilisateur final de la S3BOX.
Safe key ID management	Le client final de Hogo doit s'assurer de la confidentialité des numéro de série "key_ID" de ses clefs USB, utilisés dans le cadre de la fonction FS#0202.
Deactivated services	Les services de la S3BOX qui ne sont pas utilisés dans le cadre de la certification CSPN sont considérés comme étant désactivés (ex : scan only mode).
Key Manager secure	Le Key Manager server fournit des clés cryptographiques robustes et adaptées au cas d'usage de la S3BOX.
Filtered archives	Dans le cadre de la fonction de filtrage MIME FS#0201, les archives sont par défaut rejetées par la S3BOX.
Controlled AV downgrade	Dans le cadre des fonctions de mise à jour AV FS#0502 et FS#0504, une descente de version des bases de définitions virales est possible, jusqu'à 3 jours, pour permettre un retour à une base antérieure ponctuellement.
Customer portal secure	Le portail utilisateur (customer portal) est considéré comme de confiance, ne permettant pas la corruption des mises à jour qui y sont préparées et fournies aux S3BOX.
A/V service provider	Les fournisseur d'anti-virus mettent à disposition du key manager server des mises à jour saines et pertinentes.

Physical integrity	La S3box est physiquement intègre (pas de dégradation des témoins d'intégrité pouvant laisser penser à une ouverture de la S3Box).
Correct HTTPS configuration	Le paramétrage du serveur HTTPS est pris en charge par le client final de Hogo en accord avec la documentation [2].
Safe Certificate management	La gestion des certificats PGP utilisés pour la fonction FS#0203 est pris en charge par le client final de Hogo en accord avec la documentation [2].

3 Biens sensibles

3.1 Biens sensibles de l'environnement

User files Fichiers de l'utilisateur qui doivent être transférés.

Bien sensible	Disponibilité	Confidentialité	Intégrité	Authenticité
Users files		●	●	

3.2 Bien sensibles du produit

Admin credentials Mot de passe de l'administrateur permettant d'accéder à la configuration de S3BOX.

Core Application S3BOX.

Control Policy Politique de contrôle d'accès (règles de filtrage des types Mime, listes blanches ou noires des périphériques autorisés).

Configuration Configuration et paramètres généraux de la S3BOX.

Logs Fichiers d'enregistrement des évènements de sécurité.

Certificats PGP Certificats de signature permettant de vérifier qu'un fichier signé est bien autorisé à être transmis.

Core update Mises à jour de l'application S3BOX téléchargée depuis le portail utilisateur.

A/V update Mises à jour anti-virus qui sont téléchargées depuis le portail utilisateur de la S3BOX.

Bien sensible	Disponibilité	Confidentialité	Intégrité	Authenticité
Admin Credentials		●	●	
Core		●	●	
Control policy	●		●	
Configuration			●	
Logs	●		●	
Certificats PGP			●	●
Core update		●	●	●
A/V update	●		●	●

3.3 Profils des attaquants

Evil end-device:	Périphérique malicieux connecté à la S3BOX et contrôlé par un individu malveillant.
External attacker:	Un attaquant qui tente de modifier une mise à jour lors de son téléchargement depuis le portail utilisateur.
Internal attacker:	Un utilisateur qui tente de modifier le comportement de la TOE (modification de la configuration).

3.4 Menaces

Filtering policy bypassing	Un attaquant réussit à contourner la politique de contrôle d'accès en transmettant des fichiers non autorisés.
Filtering policy compromising	Un attaquant tente de modifier le comportement de la S3BOX en modifiant sa politique de sécurité.
Core hacking	Un attaquant tente d'injecter ou d'exécuter une mise à jour malicieuse de l'application S3BOX.
A/V update hacking	Un attaquant tente d'injecter une mise à jour anti-virus corrompue dans la S3BOX.
Configuration alteration	Un attaquant modifie la configuration générale de la S3BOX.
Credential stealing	Un attaquant récupère l'authentifiant de l'administrateur afin de modifier le comportement de la S3BOX.
Authentication bypassing	Un attaquant contourne la procédure d'authentification de l'administrateur afin de pouvoir modifier le comportement de la S3BOX.
Log or Event deletion	Un attaquant réussit à supprimer tout ou partie d'un journal afin de masquer un évènement.
Log or Event modification	Un attaquant réussit à modifier tout ou partie d'un journal afin de masquer un évènement.

4 Fonctions de sécurité

Seules les fonctions de sécurité suivantes sont considérées dans le cadre de l'évaluation CSPN.

4.1 FS#01 Anti-virus/malware scan

La S3Box active une fonction de contrôle anti-virus sur les fichiers à transférer. Cette fonction se base sur le(s) anti-virus intégré(s). Les fichiers infectés ne sont pas transférés sur la clé de sortie.

4.2 FS#02 Filtrage des fichiers

4.2.1 FS#0201 Filtrage par type MIME

La fonction de filtrage MIME est appelée dans le cadre du « Smart-Transfer » pour chaque fichier à transférer.

Cette fonction va récupérer le type MIME de chaque fichier, et chercher dans la bibliothèque des « règles MIME » le traitement à appliquer.

Ce traitement peut être :

- Copie normale : Le type est autorisé, le fichier est transféré ;
- Pas de copie : Le type n'est pas autorisé, le fichier n'est pas transféré.

Si le type MIME n'est pas reconnu (ou s'il n'est pas possible d'obtenir le type MIME d'un fichier), le cas « par défaut » est appliqué. Celui-ci est défini dans les paramètres de la box, il peut être :

- Copie normale : Le type est autorisé, le fichier est transféré ;
- Copie « unsecure » : le fichier est copié dans un sous dossier « unsecure » ;
- Pas de copie : Le type n'est pas autorisé, le fichier n'est pas transféré.

4.2.2 FS#0202 Filtrage par clef USB Support (key_ID)

La fonction de filtrage par key_ID est appelée dans le cadre du « Smart-Transfer » avant l'analyse des fichiers (clef dite « d'entrée ») et avant le transfert final des fichiers (clef dite « de sortie ») selon le paramétrage de la box. Ce paramétrage peut-être :

- Filtrer les clefs d'entrée uniquement ;
- Filtrer les clefs de sortie uniquement ;
- Filtrer les clefs d'entrée et de sortie.

Cette fonction va récupérer le numéro de série de chaque clef USB, et chercher dans la bibliothèque des « clefs autorisées » le traitement à appliquer :

- Si la clef est autorisée, la clef est montée ;
- Sinon, la clef n'est pas montée et le traitement est arrêté.

Les clefs USB peuvent être ajoutées ou supprimées de la liste d'autorisation dans le « Gestionnaire de clefs USB ».

4.2.3 FS#0203 Filtrage par signature (certificat PGP)

La fonction de filtrage par signature PGP est une routine de vérification supplémentaire qui peut être appelée dans le cadre du « Smart-Transfer ».

Cette fonction va récupérer sur la clef USB d'entrée les signatures ainsi que les fichiers à vérifier, et chercher si ces fichiers et ces signatures sont bien concordants. Elle se base pour cela sur une librairie de certificats PGP enregistrés par l'utilisateur dans la S3Box.

Seuls les fichiers validés (i.e. dont la signature est présente, nommée -nom_du_fichier.sig-, et est correctement vérifiée) sont alors transférés dans le cadre du Smart-Transfer. Les fichiers sans signatures sur la clef d'entrée ou avec une signature incorrecte ne sont pas transférés.

4.3 FS#03 Journalisation

La fonction de Journalisation enregistre les actions réalisées sur la S3BOX, que ce soit dans le cadre d'une utilisation pour un Smart-Transfer par exemple, ou lors des actions d'administration comme une mise à jour Core par exemple.

Il est possible pour l'Utilisateur de la S3BOX de visualiser le Journal de ses actions de scan ou de transfert à la fin de ceux-ci sur l'interface directement, ou dans un fichier « HTML » sur la clef USB de sortie.

Il est possible pour l'Administrateur de la S3BOX de visualiser le Journal des actions d'utilisation (hors journaux de scan et de transfert) et d'administration, directement sur la S3BOX dans une IHM dédiée.

Il est également possible pour l'Administrateur d'exporter la totalité des journaux, y compris des journaux de scan et de transfert, dans un fichier chiffré avec les certificats « Hogo » (GnuPG, algorithme RSA, clef de 4096 bits).

Enfin, il est possible pour l'Administrateur de supprimer les journaux présents sur la S3BOX, directement via l'interface dédiée de gestion des journaux (cf. [2]).

4.4 FS#04 Authentification des administrateurs

La S3Box implémente une fonction d'authentification des administrateurs du produit.

Cette fonction de sécurité implémente un mécanisme d'authentification par mot de passe, qui permet aux utilisateurs authentifiés d'accéder à des fonctions spécifiques de la S3Box.

A noter : les administrateurs du produit S3Box n'ont aucun privilège d'administration au sens du système d'exploitation. Les droits des utilisateurs est géré directement par le core software S3Box.

4.5 FS#05 Mise à jour de la S3BOX

4.5.1 FS#0501 et FS#0503 - Mise à jour du core

Le core software de S3Box est mis à jour en recevant des fichiers depuis le Customer Portal.

L'intégrité et l'authenticité de la mise à jour reçue sont basées sur le cryptage et la signature des fichiers envoyés. Le cryptage et la signature sont effectués grâce à un mécanisme asymétrique (PGP). La S3BOX vérifie le cryptage et la signature des fichiers avant installation de la mise à jour.

La mise à jour peut s'effectuer :

- FS#0501 - Mise à jour Core en mode « manuel » : hors ligne via une clef USB
- FS#0503 - Mise à jour Core en mode « LAN » : via une connexion LAN en HTTPS

Pour rappel, la fonction « Mise à jour Core - Mode en ligne » n'est pas considérée dans le cadre de cette évaluation.

4.5.2 FS#0502 et FS#0504 - Mise à jour Anti-Virus

Les bases de signature anti-virus sont mises à jour en recevant des fichiers depuis le Customer Portal.

L'intégrité et l'authenticité de la mise à jour reçue sont basées sur le cryptage et la signature des fichiers envoyés. Le cryptage et la signature sont effectués grâce à un mécanisme asymétrique (PGP). La S3BOX vérifie le cryptage et la signature des fichiers avant installation de la mise à jour.

La mise à jour peut s'effectuer :

- FS#0502 – Mise à jour AV en mode « manuel » : hors ligne via une clef USB
- FS#0504 - Mise à jour AV en mode « LAN » : via une connexion LAN en HTTPS

Pour rappel, la fonction « FS# Mise à jour AV - Mode en ligne » n'est pas considérée dans le cadre de cette évaluation.

5 Argumentaire

Le tableau ci-dessous présente la couverture des menaces par les fonctions de sécurité

	Filtering Policy bypassing	Filtering Polycy compromising	Core hacking	A/V update hacking	Configuration alteration	Credential stealing	Authentication bypassing
FS#01 Antivirus/malware scan	●						
FS#0201 Filtrage Mime	●						
FS#0202 Filtrage USB Key ID	●						
FS#0203 Filtrage signature PGP	●						
FS#03 Journalisation		●	●	●	●	●	●
FS#04 Authentification administrateur		●	●	●	●	●	●
FS#0501 Mise à jour CORE – mode Manuel		●	●		●		
FS#0502 Mise à jour AV – mode Manuel				●			
FS#0503 Mise à jour CORE – mode LAN		●	●		●		
FS#0504 Mise à jour AV – mode LAN				●			