



**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-2022/07

Sentry ONE

Version Chipset firmware 3.05, Host device software 6.3.0

Paris, le 26 avril 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-2022/07
Nom du produit	Sentry ONE
Référence/version du produit	Version Chipset firmware 3.05, Host device software 6.3.0
Catégorie de produit	Stockage sécurisé
Critère d'évaluation et version	CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)
Commanditaire	DATALOCKER B.V. Dr. Nolenslaan 157 Unit 26 6136GM Sittard Pays-Bas
Développeur	DATALOCKER B.V. Backstugevägen 12 281 36 Suède
Centre d'évaluation	THALES/CNES 290 allée du Lac 31670 Labège France
Fonctions de sécurité évaluées	<i>Chiffrement matériel ; Politique de mots de passe ; Sécurité physique ; Protection du logiciel et firmware ; Auto-tests de sécurité.</i>
Fonctions de sécurité non évaluées	Sans objet
Restriction(s) d'usage	Sans objet

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.....	6
1.2.1	Catégorie du produit.....	6
1.2.2	Identification du produit.....	6
1.2.3	Fonctions de sécurité.....	8
1.2.4	Configuration évaluée.....	8
2	L'évaluation.....	9
2.1	Référentiels d'évaluation.....	9
2.2	Travaux d'évaluation.....	9
2.2.1	Installation du produit.....	9
2.2.2	Analyse de la documentation.....	9
2.2.3	Revue du code source (facultative).....	9
2.2.4	Analyse de la conformité des fonctions de sécurité.....	9
2.2.5	Analyse de la résistance des mécanismes des fonctions de sécurité.....	9
2.2.6	Analyse des vulnérabilités (conception, construction, etc.).....	10
2.2.7	Analyse de la facilité d'emploi.....	10
2.3	Analyse de la résistance des mécanismes cryptographiques.....	10
2.4	Analyse du générateur d'aléa.....	10
3	La certification.....	11
3.1	Conclusion.....	11
3.2	Recommandations et restrictions d'usage.....	11
ANNEXE A.	Références documentaires du produit évalué.....	12
ANNEXE B.	Références liées à la certification.....	13

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Sentry ONE, Version Host device software 6.3.0, Chipset firmware 3.05, » développé par DATALOCKER.

Ce produit est un périphérique de stockage sécurisé ayant le format d'une clef USB classique, qui effectue un chiffrement matériel automatique protégé par mot de passe des données qui s'y trouvent stockées, assurant par là-même un stockage et un transport sûrs des données.

Quand elle est branchée sur un ordinateur, la clef USB Sentry ONE se présente initialement, sur le système d'exploitation, comme un DVD-RW virtuel contenant le logiciel pour Linux, MacOS X et Windows (32 bits et 64 bits) ainsi qu'une partition de stockage non montée. Cette partition est montée après la saisie correcte du mot de passe (à travers l'application « unlocker.exe ») pour accueillir les données utilisateur.

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 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	messagerie sécurisée
<input checked="" type="checkbox"/>	9	stockage sécurisé
<input type="checkbox"/>	10	environnement d'exécution sécurisé
<input type="checkbox"/>	11	terminal de réception numérique (Set top box, STB)
<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	Sentry ONE
Numéro de la version évaluée	Chipset firmware 3.05 Host device software 6.3.0

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

- la version matérielle consiste en un numéro de série et un QR-code imprimés sur le produit :



Figure 1 – Version matérielle du produit

- la version du logiciel et du *firmware* est obtenue par le logiciel « unlocker.exe », lui-même stocké sur une partition en lecture seule du produit Sentry ONE :



Figure 2 – Version logicielle du produit

1.2.3 Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- la chiffrement matériel ;
- la politique de mots de passe ;
- la sécurité physique ;
- la protection du logiciel et *firmware* ;
- l'auto-test de sécurité.

1.2.4 Configuration évaluée

Deux modes de configuration sont possibles :

- configuration standard : Sentry ONE activé en mode *standalone* ;
- configuration managée : Sentry ONE activé avec un serveur *SafeConsole* ou *IronKey EMS*.

La configuration évaluée est la **configuration standard (non managée)**.

Cette configuration standard est obtenue en déroulant simplement le *wizard* de l'application *standalone* « *unlocker* », dans lequel l'utilisateur choisit son mot de passe, après quoi le disque est formaté.

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 processus d'installation est tel que décrit dans [GUIDES] et il est direct et facile à suivre et n'introduit pas de mauvaise configuration.

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'installer et 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'implémentation des mécanismes cryptographiques du produit et fourni les résultats de l'analyse dans le rapport d'analyse cryptographique [ANA_CRY].

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

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

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 et 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

Les risques identifiés lors de l'évaluation entraînent des recommandations et des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

2.2.7.2 Avis d'expert sur la facilité d'emploi

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

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 [ANA_CRY].

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 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 « Sentry ONE, Version *Host device software* 6.3.0, *Chipset firmware* 3.05 » 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">- <i>Sentry ONE CSPN Security Target</i>, 2021, version 1.6, 21 mai 2021.
[RTE]	Rapport technique d'évaluation : <ul style="list-style-type: none">- <i>Rapport Technique d'Évaluation CSPN – Project: SITTARD</i>, référence SITTARD_CSPN_ETR, version 1.0, 10 janvier 2022.
[ANA_CRY]	Rapport d'expertise cryptographique : <ul style="list-style-type: none">- <i>Analysis of Cryptographic Mechanisms - Project: SITTARD</i>, référence SITTARD_CRY, version 1.0, 11 janvier 2022.
[GUIDES]	Guides du produit : <ul style="list-style-type: none">- <i>Sentry One User Guide</i>, disponible sur le lien suivant : https://media.datalocker.com/manuals/sentry/DataLocker_Sentry_ONE_User_Guide.pdf ;- <i>Sentry One 2021 MAY Cryptographic Documentation CSPN</i>, version 1.5, 15 juin 2021 ;- <i>Password Authentication in AES Drive (DataLocker Sentry ONE)</i>, 15 novembre 2019 ;- <i>Password Authentication in AES Drive (DataLocker Sentry ONE) – Appendix</i>, 30 janvier 2020.

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.
[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.