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-2024/09

Stormshield Data Security for Google Workspace

Version 4.1.2

Paris, le 21 Octobre 2024

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

Vincent STRUBEL

[ORIGINAL SIGNE]

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01.71.75.82.82

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-2024/09**
Nom du produit **Stormshield Data Security for Google Workspace**
Référence/version du produit **Version 4.1.2**
Catégorie de produit **Stockage sécurisé**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **STORMSHIELD** 1 place Verrazzano 69009 Lyon, France
Développeur **STORMSHIELD** 1 place Verrazzano 69009 Lyon, France
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Accord de reconnaissance applicable fixed time certification Ce certificat est reconnu dans le cadre du [BSZ_CSPN]
Fonctions de sécurité évaluées Identification, authentification et contrôle d'accès des utilisateurs Sécurité des communications Fonctions cryptographiques et de génération de nombres aléatoires Journalisation
Fonctions de sécurité non évaluées Sans objet
Restriction(s) d'usage Oui (cf. §3.2)

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 « *Stormshield Data Security for Google Workspace*, Version 4.1.2 » développé par STORMSHIELD.

Ce produit s'intègre de manière transparente dans l'infrastructure CSE (*Client-Side Encryption*, chiffrement côté client) de l'environnement *Google Workspace*, qui permet aux entreprises d'utiliser leurs propres clefs de chiffrement pour protéger les documents qu'elles stockent dans les environnements Google (présentations *Google Slides*, feuilles de calcul *Google Sheets* stockées dans *Google Drive*, vidéos *Google Meet*, rendez-vous *Google Calendar*).

Une infrastructure CSE est composée du *Google Workspace*, d'un fournisseur d'identité *(Identity Provider*), d'un système de gestion de clefs (*Key Management System* – KMS et HSM) et du *Stormshield Data Security (SDS) for Google Workspace* (le produit évalué).

Le *produit évalué* assure des communications sécurisées entre tous les utilisateurs dans l'environnement, ainsi que la protection des clefs de chiffrement des données sensibles.

Il est disponible dans deux modes de déploiement : *On Premise (*hébergé et maintenu par l'entreprise utilisatrice*),* ou bien dans le *Cloud* (en mode *SaaS - Software as-a-Service).*

Le présent certificat porte sur le *SDS for Google Workspace* dans son déploiement en mode *On Premise,* ainsi que sur ses communications avec les autres composants de l'infrastructure CSE (*Google Workspace*, *Identity Provider* et *KMS*).

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*

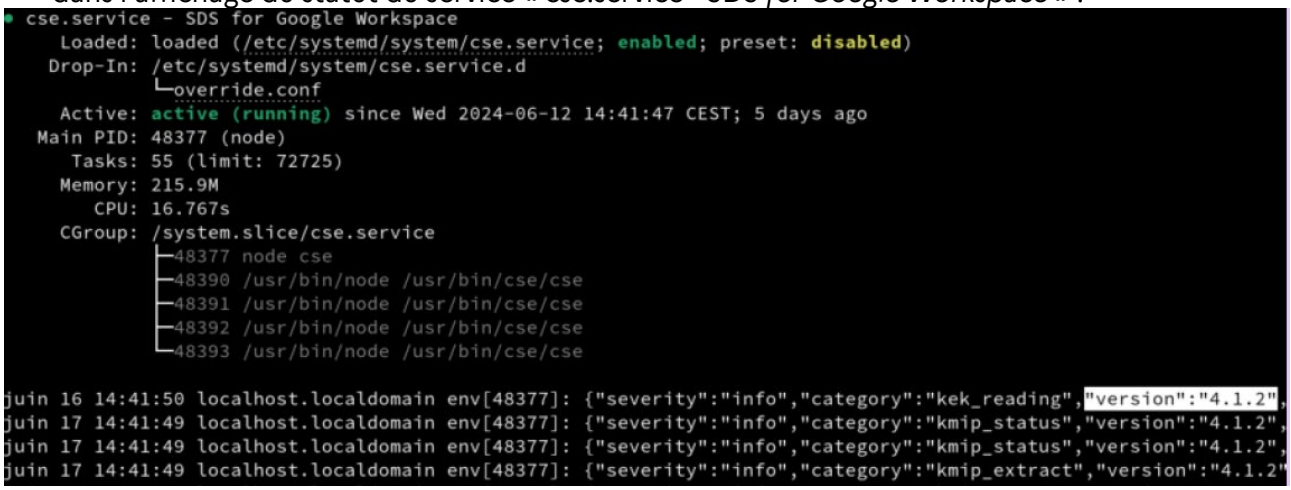
☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☒	**9**	**stockage sécurisé**
☐	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*

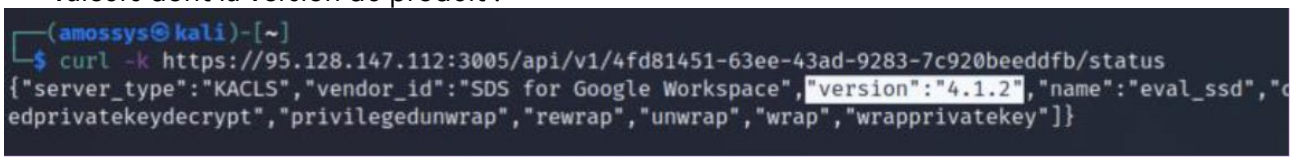
Produit	
Nom du produit	*Stormshield Data Security for Google Workspace*
Numéro de la version évaluée	Version 4.1.2

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

- dans l'affichage du statut du service « cse.service - SDS *for Google Workspace* » :



- ou encore par un appel à l'API (iP_address]/[tenant_ID]/status), qui retourne un ensemble de valeurs dont la version du produit :



- ou encore dans la console d'administration de Google, onglet « *Security/Client-side encryption* », en testant la connexion au service de chiffrement (*encryption service*) :

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'identification, l'authentification et le contrôle d'accès des utilisateurs ;
- la sécurité des communications ;
- les fonctions cryptographiques et de génération de nombres aléatoires ;
- la journalisation.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond au déploiement du produit en mode *On Premise*.

L'environnement de test est constitué des éléments suivants :

- une machine Rocky Linux 9 hébergeant le produit évalué ;
- pour le Google Workspace, un *Google Cloud Service* premium pour administrer les services tiers Google de l'entreprise (gdrive, gmail, gcalendar) ;
- pour le fournisseur d'identité, un compte OneLogin ;
- pour le KMS, un Thales CipherTrust ;
- une machine cliente pour effectuer les opérations dans le Google Workspace, protégées par l'utilisation du *SDS for Google Workspace* évalué.

La figure ci-dessous explicite la plateforme d'évaluation.

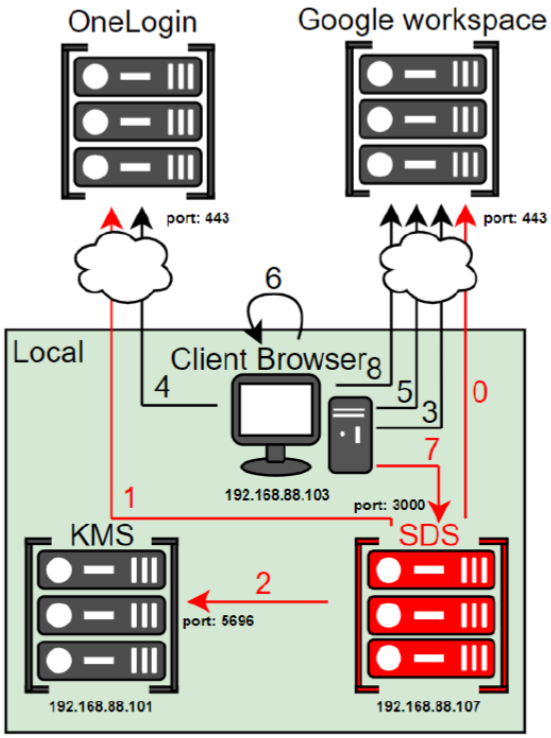


Figure 1 – Plateforme d'évaluation.

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

L'installation et la configuration complète de l'environnement d'évaluation du produit en mode *On Premise* est complexe et requiert l'assistance du développeur.

2.2.1.3 Notes et remarques diverses

Le mode de déploiement *On Premise* est destiné aux grandes entreprises qui disposent des ressources nécessaires.

2.2.2 *Analyse de la documentation*

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

2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques 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

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 inexploitables pour le niveau d'attaquant considéré.

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 [ANA_CRY].
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.

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 « Stormshield Data Security for Google Workspace, Version 4.1.2 » 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], notamment :

- L'installation devra être réalisée avec l'assistance du développeur ;
- Un mécanisme anti bruteforce devra être mis en place ;
- Les recommandations de l'ANSSI pour les systèmes de log devront être suivies, notamment : mise en place d'un espace dédié aux logs avec des droits d'accès restreints et implémentation d'une politique de rotation des logs.

3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ (*Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité de référence pour l'évaluation : - *Stormshield Data Security for Google Workspace– CSPN Security Target*, référence KAPUA/ST, version 1.3, 24 septembre 2024.
[RTE]	Rapport technique d'évaluation : - *CSPN Evaluation Technical Report - Product Stormshield Data Security for Google Workspace* - version 4.1.2, référence CSPN-ETR-KAPUA2-2.10, version 2.10, 24 septembre 2024.
[ANA_CRY]	Rapport d'expertise cryptographique : - *Analysis of Cryptographic Mechanisms - Product Stormshield Data Security for Google WorkSpace* - version 4.1.2, référence CSPN-CRY-KAPUA-2.00, version 2.00, 28 juin 2024.
[GUIDES]	Guide d'installation et d'administration du produit : - *Guide SDS encryption service for Google Workspace – Administration Guide*, référence sds-en-sds-for-gw-administration_guide, version 4.1.2, 22 mars 2024 - *SDS encryption service for Google Workspace – Release Notes*, référence sds-en-sds-for-gw-*release_notes*, version 4.1.2, 22 mars 2024 - *KMS configuration* - notice d'installation du KMS Thales

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 5.0, 12 janvier 2023. 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.
[BSZ_CSPN]	*Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence bsz_cspn_mutual_recognition_agreement, version 2.0, mai 2024.