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-2020/35

Virtru Data Protection Platform - Browser plug-in and Secure Reader

Version 7.14.1

Paris, le 16 décembre 2020

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

Guillaume POUPARD

[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-2020/35**
Nom du produit **Virtru Data Protection Platform - Browser plug-in and Secure Reader**
Référence/version du produit **Version 7.14.1**
Catégorie de produit **Messagerie sécurisée**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Virtru Corporation** 1130 Connecticut Ave NW, Suite 210 Washington, DC 20036 Etats-Unis d'Amérique
Développeur **Virtru Corporation** 1130 Connecticut Ave NW, Suite 210 Washington, DC 20036 Etats-Unis d'Amérique
Centre d'évaluation **OPPIDA** 4-6 avenue du vieil étang, Bâtiment B 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées Chiffrement des messages Déchiffrement des messages pour les utilisateurs Virtru Déchiffrement des messages pour les utilisateurs ne disposant pas de Virtru Protection des clés de chiffrement
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 www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Virtru Data Protection Platform - Browser plug-in and Secure Reader, Version 7.14.1 » développé par Virtru Corporation.

Ce produit se présente sous la forme d'un *plug-in* au navigateur web qui s'interface avec le client web de messagerie électronique utilisé par l'émetteur pour chiffrer automatiquement les messages avant leur envoi.

Du côté du destinataire, deux modes de déchiffrement sont disponibles selon que l'utilisateur dispose ou non du *plug-in* Virtru ; dans le second cas, le contenu du message, conservé chiffré sur un serveur Amazon S3, peut être consulté par l'utilisateur après authentification via l'application Virtru Secure Reader.

La figure ci-dessous explicite l'architecture du produit.

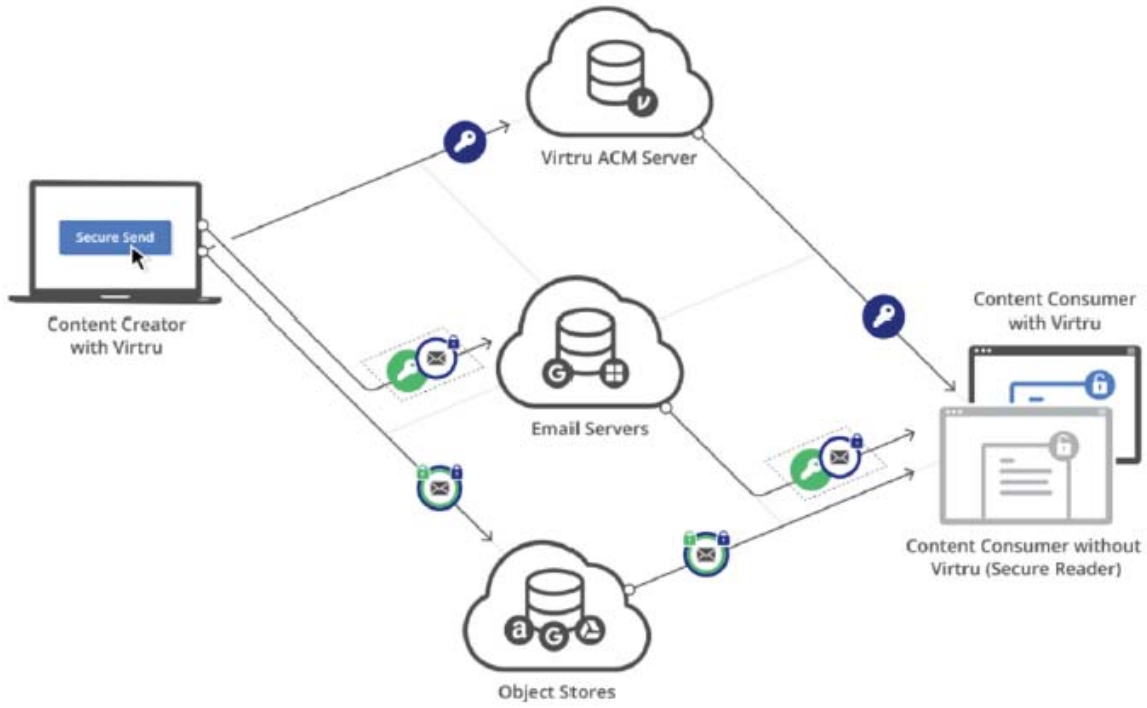

Figure 1 - Architecture de la solution Virtru.

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	Virtru Data Protection Platform - Browser plug-in and Secure Reader
Numéro de la version évaluée	Version 7.14.1

La version certifiée du *plug-in* pour le navigateur peut être identifiée via le menu contextuel accessible depuis l'icône Virtru du navigateur, en sélectionnant « Gérer les extensions » (*manage extensions*) :

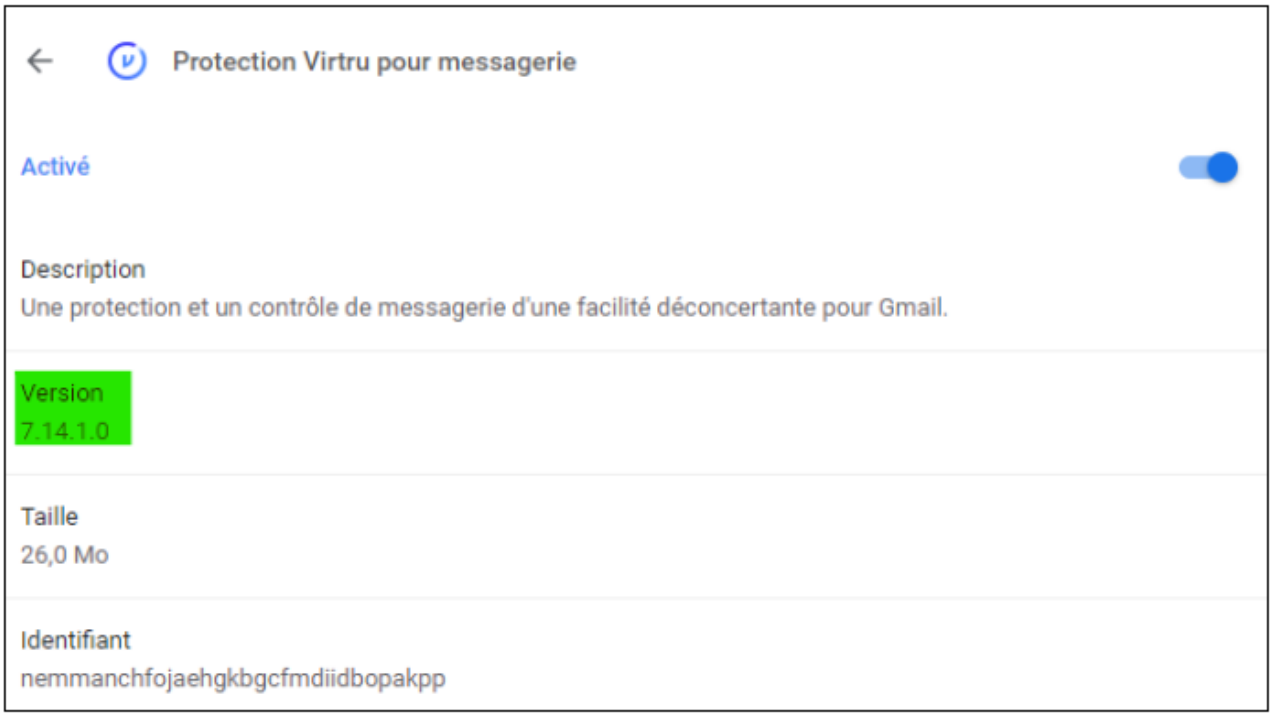

Figure 2 - identification de la version du plug-in

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- le chiffrement des messages ;
- le déchiffrement des messages pour les utilisateurs Virtru ;
- le déchiffrement des messages pour les utilisateurs ne disposant pas de Virtru ;
- la protection des clés de chiffrement.

1.2.4 *Configuration évaluée*

La configuration évaluée correspond au *plug-in* identifié au 1.2.2 installé sur un navigateur Chrome, déployé côté emmetteur et destinataire. Les différents serveurs nécessaires au fonctionnement de la solution ne font pas partie du périmètre de l'évaluation ; la gestion et la distribution des clés cryptographiques ont par contre été évaluées au titre de l'analyse des mecanismes cryptographiques.

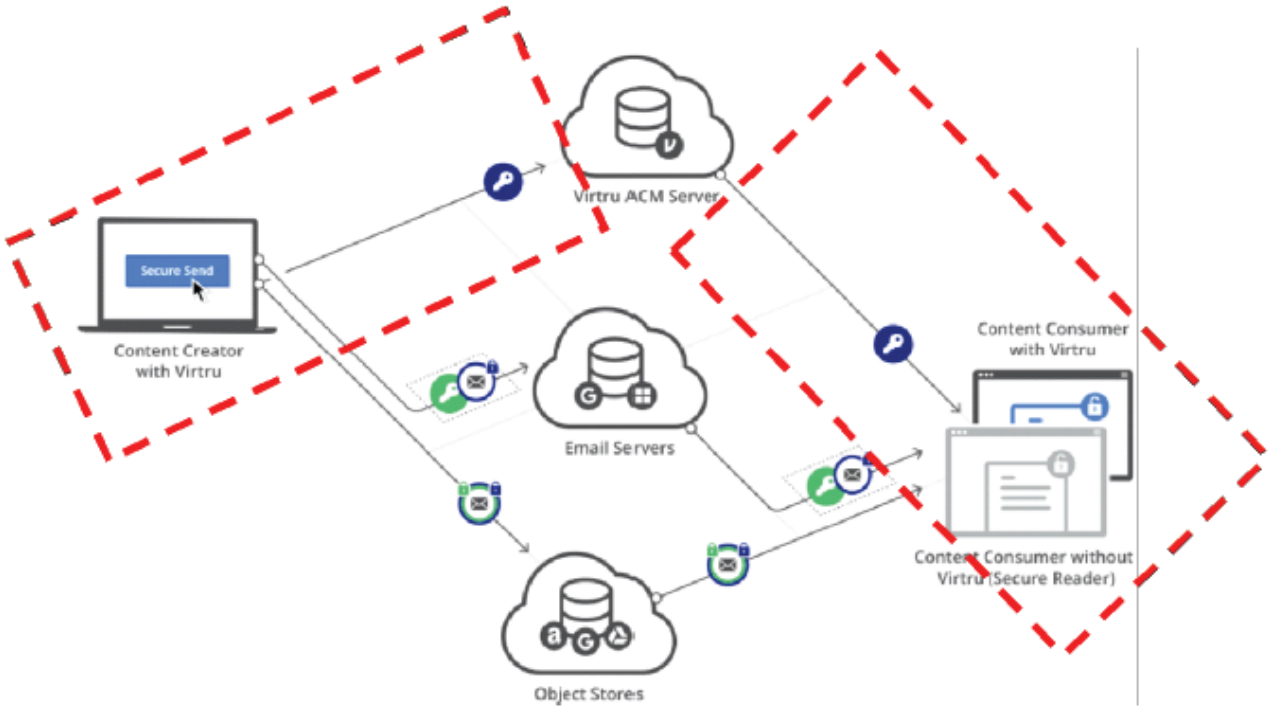

Figure 3 - périmètre de l'évaluation

La plateforme de test est constituée des éléments suivants :

- un PC fonctionnant sous *Windows 10* ;
- le navigateur *Chrome* en version 79.0.39 ;
- la version 7.14.1 du *plug-in* Virtru interfacée avec le client web de messagerie *gmail*.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN]. Les références des documents se trouvent en Annexe 2.

2.2 Charge de travail prévue et durée de l'évaluation

La durée de l'évaluation est conforme à la charge de travail prévue dans le dossier d'évaluation.

2.3 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].

2.3.1 *Installation du produit*

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

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

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

L'installation n'a nécéssité aucune manipulation ou option particulière.

2.3.1.3 Durée de l'installation

L'installation du *plug-in* par l'utilisateur ne nécessite que quelques minutes.

2.3.1.4 Notes et remarques diverses

L'administrateur doit contacter le support Virtru pour l'activation ou la désactivation de certaines fonctionnalités nécessaire à une mise en œuvre sécurisée de la solution (voir 2.3.8.1).

2.3.2 *Analyse de la documentation*

L'évaluateur a eu accès aux documents identifiés dans [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, à condition de bien prendre en compte les éléments identifiés au 2.3.8.1.

2.3.3 *Revue du code source (facultative)*

Aucune analyse du code source n'a été effectuée dans le cadre de cette évaluation.

2.3.4 *Analyse de la conformité des fonctions de sécurité*

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

2.3.5 *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.

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

2.3.6.1 Liste des vulnérabilités connues

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

2.3.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables dans le contexte défini par la cible de sécurité [CDS]

2.3.7 *Accès aux développeurs*

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit.

2.3.8 *Analyse de la facilité d'emploi*

2.3.8.1 Cas où la sécurité est remise en cause

Par défaut, le service de messagerie *gmail* de *Google* fournit à l'utilisateur des services de « rédaction intelligente » (*Google predictive services*), comme par exemple la suggestion de texte prédictif. Ces services, pour fonctionner, nécessitent que le texte saisi par le rédacteur soit envoyé aux serveurs *Google* au fur et à mesure de la rédaction, constituant une fuite de données en clair s'ils sont utilisés avec la solution de chiffrement Virtru.
Les utilisateurs de la solution doivent donc s'assurer auprès de leur administrateur (dans le cadre d'une utilisation en contexte professionnel) et/ou de leur correspondant Virtru de la désactivation de ces services, comme indiqué dans le guide [Admin Google].

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

2.3.8.2 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 l'utilisateur.

2.3.8.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par le produit ont fait l'objet d'une analyse au titre de cette évaluation CSPN (voir [RTE]). Celle-ci n'a pas identifié de non-conformité au RGS (voir [RGS]) ni de vulnérabilité exploitable.

2.5 Analyse du générateur d'aléas

Le produit n'implémente pas de générateur d'aléas et utilise les API exposées par le navigateur pour la génération des clés cryptographiques. L'analyse n'a pas mis en évidence de faiblesse exploitable liée à la génération d'aléas.

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 « Virtru Data Protection Platform - Browser plug-in and Secure Reader, version Version 7.14.1 » 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit.

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

En particulier, les utilisateurs de la solution Virtru doivent s'assurer que les services de « rédaction intelligente » de *Google* (*Google predictive services*) sont bien désactivés, en contactant, au besoin, le support client Virtru (voir [Google Predictive Services]).

ANNEXE A. Références documentaires du produit évalué

[CDS]	*Security Target – Virtru Data Protection Platform – Browser plug-in and Secure Reader – Version 7.14.1* Version : 1.4 ; Date : 19 décembre 2019.
[RTE]	*CSPN Evaluation Technical report VEMAN2 – Virtru Data Protection Platform* Référence : OPPIDA/CESTI/VEMAN2/RTE/1.0 ; Version : 1.0 ; Date : 1 septembre 2020.
[GUIDES]	*Virtru Support Center* https://support.virtru.com/hc/en-us
[Google Predictive Services]	*Virtru & Google Predictive Services* https://support.virtru.com/hc/en-us/articles/360049729653-Virtru-Google-Predictive-Services

ANNEXE B. Références 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-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.