PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2018/10

TransfertPro « On Premise »
Version 3.0.3.5

Paris, le 15/05/2018

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 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-2018/10**
Nom du produit **TransfertPro « On Premise »**
Référence/version du produit **TransfertPro, Version 3.0.3.5**
Catégorie de produit **Stockage sécurisé / Communication sécurisée**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **TransfertPro SAS** **32 Boulevard de Courcelles** **75017 Paris – France**
Développeur **TransfertPro SAS** **32 Boulevard de Courcelles** **75017 Paris, France**
Centre d'évaluation **Amossys** **4 bis allée du bâtiment** **35000 Rennes, France**
Fonctions de sécurité évaluées **Identification et Authentification** **Protection des données utilisateurs** **Communications sécurisées** **Intégrité des données de fonctionnement** **Protection des éléments secrets**
Fonction(s) de sécurité non évaluées **Sans objet**
Restriction(s) d'usage **Oui (cf. §3.2)**

Préface

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 Premier ministre 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est « TransfertPro « On Premise », version 3.0.3.5 » développé par *TRANSFERTPRO SAS*.

Ce produit vise à sécuriser le stockage et le transfert de documents. Dans sa version « On Premise », il est constitué d'un serveur Web, auquel les émetteurs et les destinataires de documents se connectent via un navigateur. Ce serveur inclut :

- un serveur de fichiers permettant de stocker les documents sous forme chiffrée ;
- un serveur SQL permettant de gérer les données de connexion des utilisateurs, les données métier, les évènements relatifs aux manipulations de fichiers, et les informations de session du serveur web.

Ce serveur s'interface avec un boîtier HSM *TRUSTWAY Proteccio* (développé par la société *BULL/ATOS*) permettant de stocker la clé de société. Il peut également s'interfacer avec un serveur *Collabora Online* permettant de modifier les fichiers, mais la version évaluée considère qu'un tel serveur n'est pas présent.

TransfertPro permet l'envoi sécurisé d'un fichier entre deux utilisateurs :

- dans un premier temps, l'émetteur se connecte sur TransfertPro par un identifiant (adresse email) et un mot de passe, puis télécharge un fichier en clair via un canal HTTPS ;
- dans un second temps, l'émetteur renseigne l'adresse email du destinataire et choisit son mode d'envoi. L'évaluation ne considère que les modes d'envoi assortis d'un mot de passe : pour récupérer le document, le destinataire doit saisir un mot de passe choisi conjointement avec l'émetteur. L'accès préalable au document se fait :
    - en se connectant sur son compte TransfertPro ;
    - si le destinataire ne dispose pas d'un compte, en suivant un lien envoyé par l'émetteur.

Pour l'échange du mot de passe, le destinataire et l'émetteur doivent au préalable s'accorder sur le moyen utilisé (SMS, téléphone, en direct, …).

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.

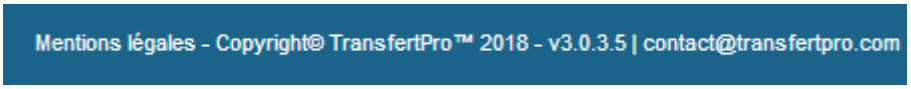
1.2.1. Catégorie du produit

☐ 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

Nom du produit	TransfertPro « On Premise »
Numéro de la version évaluée	3.0.3.5

La version est disponible sur la page de connexion du serveur web, comme le montre l'image ci-dessous :



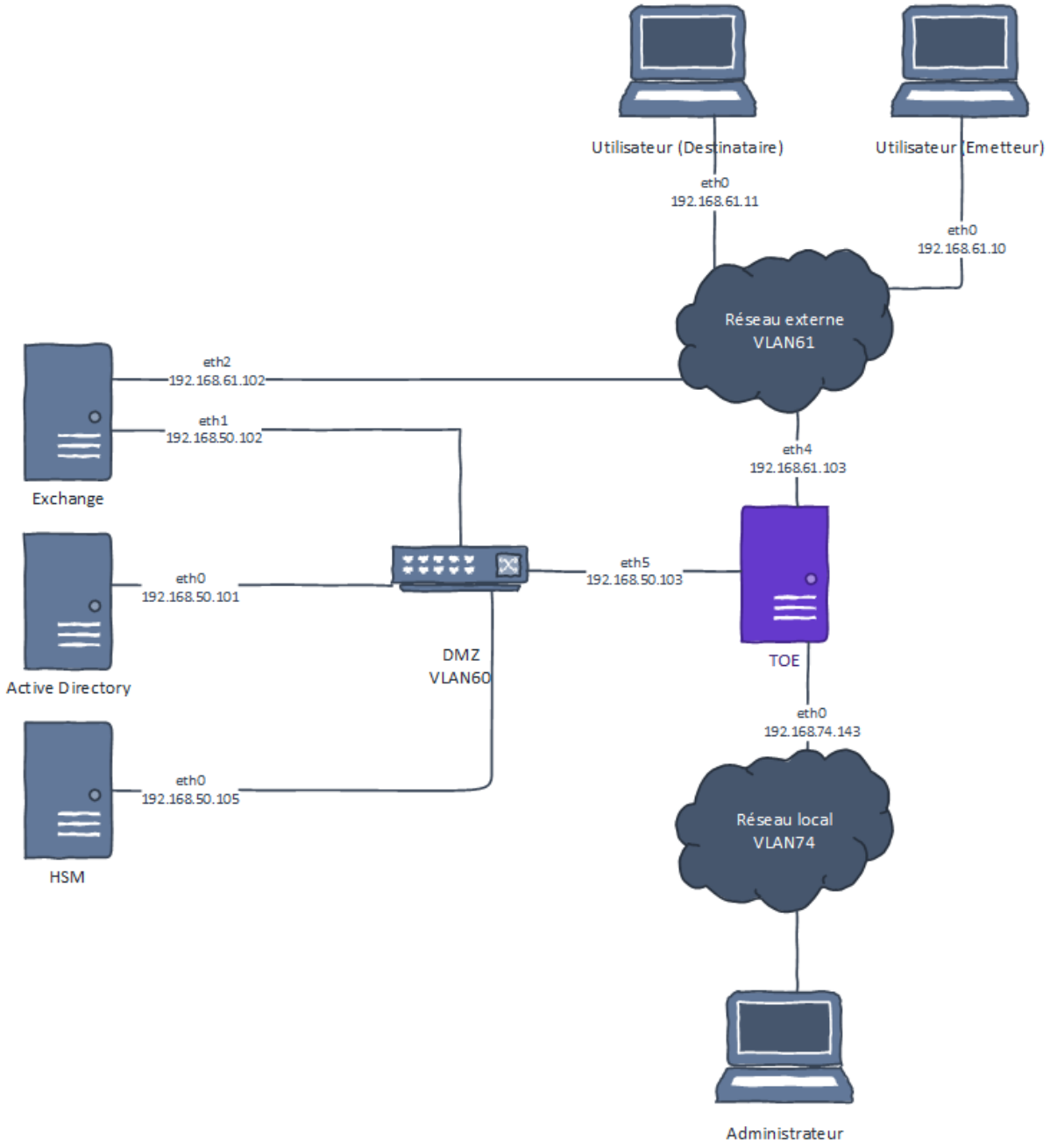
1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- identification et authentification ;
- protection des données utilisateurs ;
- communications sécurisées ;
- intégrité des données de fonctionnement ;
- protection des éléments secrets.

1.2.4. Configuration évaluée

La configuration évaluée est décrite dans le diagramme ci-dessous :



Trois VLAN sont présents sur la plate-forme de test :

- le VLAN d'administration de la TOE ;
- le VLAN correspondant à la DMZ qui héberge les services utilisés par la TOE (*Active Directory*, *Exchange* et HSM) ;
- le VLAN simulant le « monde extérieur ».

Les systèmes sont de types :

- *TRUSTWAY Proteccio* X140 PCA4L (version logicielle 16/01/2017) pour le HSM ;
- Linux Ubuntu 16.04 LTS pour Collabora Online ;
- *Windows* 7 SP1 Pro 64 bits pour les postes utilisateurs ;
- *Windows Server* 2012 R2 pour l'Active Directory, Exchange et la TOE.

Tous ces éléments, à l'exception du HSM, sont virtualisés.

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 s'est déroulée en plusieurs temps :

- le CESTI a préinstallé un serveur *Windows Server 2012 R2* (pour l'installation du produit) et des postes clients *Windows 8* suivant le document [PRE] fourni par l'éditeur ;
- l'éditeur s'est déplacé dans les locaux du CESTI afin d'installer le produit sur le serveur. De plus, l'éditeur a intégré :
  - des machines virtuelles préconfigurées : *Active Directory* et *Exchange* ;
  - le HSM *TRUSTWAY Proteccio*.

  Durant cette phase d'installation par l'éditeur, un évaluateur du CESTI été présent pour observer les opérations effectuées ;
- pour des raisons techniques la fin de l'installation a été réalisée par le CESTI (raccordement du HSM et *Exchange*).

L'évaluateur signale que l'éditeur est en charge de l'installation du produit auprès de ses clients. Il est à noter par ailleurs que l'utilisateur final doit conserver la maîtrise de la configuration du serveur hôte (voir chapitre 2.3.8.2).

2.3.1.3. Durée de l'installation

L'installation de la TOE ainsi que du système hôte a duré 2 jours.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation, accompagnée de l'aide en ligne, sont jugées suffisamment complètes pour permettre une prise en main efficace du produit.

2.3.3. Revue du code source (facultative)

L'évaluation n'a pas fait l'objet d'une revue de code source.

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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces. Cependant dans le contexte définit par la cible de sécurité [CDS] et les conditions d'utilisation du produit par le développeur aucune d'entre elles n'est exploitable.

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

Il n'a pas été découvert de vulnérabilité propre au produit, ni dans son implémentation, qui puisse remettre en cause la sécurité du produit.

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 et préconisations

2.3.8.1. 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.

2.3.8.2. Recommandations pour une utilisation sûre du produit

L'utilisateur du produit devra mettre en œuvre la(es) mesure(s) suivante(s) :

- fermer le port SQL (TCP n°1433) et préférer le port RDP s'il est nécessaire d'administrer la base de données à distance ;
- ne pas mettre en place de rupture protocolaire vers le serveur TransfertPro ou de sécuriser sa mise en place au niveau du serveur ;

- s'assurer que la configuration du serveur hôte du produit est maîtrisée.

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

2.3.8.3. **Avis d'expert sur la facilité d'emploi**

L'évaluateur n'a pas relevé de problème majeur relatif à la facilité d'emploi.

2.3.8.4. **Notes et remarques diverses**

Sans objet.

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. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le produit utilise les fonctionnalités *.Net* et *BouncyCastle C#* afin d'obtenir des aléas. Celles-ci ne présentent pas de vulnérabilité exploitable.

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 « TransfertPro « On Premise », version 3.0.3.5 » 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. 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 recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Cependant l'évaluation a mis en avant que, pour une utilisation sécurisé du produit, L'administrateur du produit doit mettre en place une politique de mots de passe par défaut correspondant a minima à une force « moyenne » ainsi que préconisé par l'ANSSI (voir [MdP]).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – TransfertPro « On Premise »* *Référence : CSPN-ST-TransfertPro ;* *Version : 3.00 ;* *Date : 30 novembre 2017*
[RTE]	*Rapport Technique d'Évaluation CSPN - Produit TransfertPro « On Premise » version 3.0.3.5* Référence : CSPN-RTE-TransfertPro ; Version : 2.01 ; Date : 27 avril 2018
[PRE]	*Prérequis d'installation de la version On-Premise de TransfertPro 2.0* *Prérequis d'installation de la version On-Premise de TransfertPro 2.0, TransfertProv3.0.3.5-PreRequis-Installation-OnPremise-12012018.docx* Référence : n.c. ; Version : n.c. ; Date : n.c.

Annexe 2. 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, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr.
[MdP]	Note technique – Recommandations de sécurité relatives aux mots de passe, 5 juin 2012, ANSSI. https://www.ssi.gouv.fr/administration/guide/mot-de-passe/