AMOSSYS

transfertpro
PARTAGE ET COLLABORATION SÉCURISÉE 100% FRANÇAIS

Cible de sécurité CSPN

Logiciel multi-tenant TransfertPro en tant que service (SaaS) version 10.2.0.2 en hébergement « *On Premise* » ou en hébergement Cloud non privé sur socle IaaS

Référence : CSPN-CDS-TransfertPro-1.10

Date : le 29/09/2025

Référence interne : TFP003

Siège : Immeuble Le Ouessant • Bâtiment B • 11 rue Maurice Fabre • 35000 Rennes • France • **www.amossys.fr**
SIRET : 493 348 890 00051 • **NAF** : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

FICHE D'EVOLUTIONS

Révision	Date	Description	Rédacteur
1.00	10/05/2023	Version finale approuvée (inchangée)	J. LEMETEYER
1.01	02/08/2023	Précisions sur la version et les attaquants, ajout de la FS2	J. LEMETEYER
1.02	17/10/2023	Mise à jour (précision sur HSM et évaluation de référence sur la version on premise)	J. LEMETEYER
1.03	03/01/2024	Mise à jour finale de mise en conformité avec la note 6 de l'ANSSI	J. LEMETEYER
1.04	17/09/2024	Prise en compte des résultats de l'évaluation CSPN « TRANSFERTPROv9 »	A. DELOUP TRANSFERTPRO
1.05	27/02/2025	Ajout d'informations concernant l'utilisation des OTP	TRANSFERTPRO
1.06	24/04/2025	Mise à jour en conformité avec la note d'application 9 de l'ANSSI	S. NZONGANI
1.07	27/06/2025	Mise à jour suite à la revue ANSSI	A. DELOUP
1.08	18/07/2025	Mise à jour suite à la revue ANSSI	A. DELOUP
1.09	21/07/2025	Mise à jour suite à la revue ANSSI	A. DELOUP
1.10	29/09/2025	Mise à jour des COTS	TRANSFERTPRO

Ce document a été validé par TransfertPro.

SOMMAIRE

1. INTRODUCTION 4
1.1. Objet du document 4
1.2. Identification du produit 4
1.3. Références 5
1.4. Glossaire 5
2. DESCRIPTION DU PRODUIT 6
2.1. Description générale 6
2.2. Principe de fonctionnement 8
2.2.1. Envoi sécurisé de fichiers 8
2.2.2. Stockage de fichiers 8
2.3. Description des COTS intégrés 9
2.4. Description de l'environnement technique de fonctionnement 9
2.4.1. Description des dépendances 9
2.4.2. Matériel compatible ou dédié 10
2.4.3. Système d'exploitation retenu 10
2.5. Périmètre de l'évaluation 10
2.5.1. Périmètre 10
2.5.2. Plateforme d'évaluation 11
3. PROBLEMATIQUE DE SECURITE 14
3.1. Description des utilisateurs 14
3.2. Description des biens sensibles 15
3.3. Description des hypothèses sur l'environnement 17
3.4. Description des menaces 19
3.5. Description des fonctions 21
3.5.1. Fonctions métier 21
3.5.2. Fonctions de sécurité 22
3.5.3. Fonctions désactivées 24
3.6. Surface d'attaque 25
3.7. Matrices de couvertures 26
3.7.1. Menaces et biens sensibles 26
3.7.2. Menaces et fonctions de sécurité 27
3.7.3. Menaces et moyens exploités par les agents menaçants 28

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de la réévaluation, selon le schéma CSPN promu par l'ANSSI, du produit « **TransfertPro** » développé par la société **TransfertPro**.

La TOE considérée est la gamme multi-tenant TransfertPro en tant que service (SaaS) version 10.2.0.2 :

- Produit de référence : en hébergement « *On Premise* »

- Produit décliné : en hébergement Cloud non privé (Orange) sur socle IaaS

Ce document est soumis au contrôle technique et qualité d'**AMOSSYS** ainsi qu'à la validation de **TransfertPro**. Les mises à jour de ce document sont effectuées par l'équipe projet d'**AMOSSYS**.

1.2. IDENTIFICATION DU PRODUIT

Éditeur	TransfertPro 32 Boulevard de Courcelles 75017 Paris
Lien vers l'organisation	https://www.transfertpro.com/
Nom commercial du produit	TransfertPro - « *On Premise* » (produit de référence) ; - SaaS.
Numéro de la version évaluée	10.2.0.2
Domaine d'agrément CSPN	Stockage sécurisé

1.3. REFERENCES

Le Tableau 1 liste les documents consultés par l'évaluateur pour l'établissement de la présente cible de sécurité.

Tableau 1 - Références consultées pour la rédaction de la cible de sécurité

Référence	Description	Version
	Document décrivant les fonctionnalités de TransfertPro https://www.transfertpro.com/nos-forfaits/#dearflip-df_12852/1/	
ANSSI-CSPN-NOTE-06	Note d'application « Méthodologie d'évaluation CSPN pour les logiciels déployés sur des infrastructures de *Cloud Computing* »	1.1
ANSSI-CC-NOTE-21	Note d'application « Méthodologie pour l'évaluation d'une gamme de produits »	1.0
ANSSI-CSPN-CER-P-01	Procédure « Certification de sécurité de premier niveau des produits des technologies de l'information »	5.0
ANSSI-CSPN-AGR-P-01	Procédure « Agrément des centres d'évaluation en vue de la certification de sécurité de premier niveau »	1.2
ANSSI-CSPN-NOTE-09	Note d'application « Contenu et structure de la cible de sécurité CSPN »	1.0
AID	Analyse d'Impact Différentielle et Stratégie de réutilisation des tests, « Transfertpro-Stratégie-Reutilisation-Tests-CSPN-1.0 »	1.0

1.4. GLOSSAIRE

Tableau 2 - Références documentaires

Référence	Description
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CESTI	Centre d'Évaluation de la Sécurité des Technologies de l'Information
COTS	*Commercial off-the-shelf*
CSPN	Certification de Sécurité de Premier Niveau
RDS	*Remote Desktop Services*
TOE	*Target Of Evaluation*
TSE	*Terminal Server Edition*
HSM	*Hardware Security Module*
SaaS	*Software as a Service*

2. DESCRIPTION DU PRODUIT

Ce chapitre présente le produit *TransfertPro*, son fonctionnement et son environnement. L'objectif de ce produit est de fournir un stockage sécurisé pour les utilisateurs, ainsi qu'un moyen de partager des fichiers volumineux de manière sécurisée. Les fichiers sont hébergés sous forme chiffrée.

2.1. DESCRIPTION GENERALE

La solution *TransfertPro* est une suite de logiciels web permettant le stockage, l'édition collaborative, la signature électronique, ainsi que le transfert de documents de manière sécurisée. Elle se compose des modules logiciels suivants :

- **Tsend** : solution d'envoi sécurisé de fichier (sans stockage à long terme[1]) de toute taille ;
- **Tsafe** : solution de coffre-fort numérique permettant l'archivage sécurisé (en confidentialité et intégrité) de documents ;
- **Troom** : solution de stockage collaboratif permettant le partage de dossiers et l'édition en ligne de fichiers (Word, Excel et PowerPoint) ;
- **Tbox** : solution équivalente à Troom offrant la fonctionnalité supplémentaire d'envoi de fichiers et de stockage à long terme (pas de limite de rétention) ;
- **TAE** : solution d'archivage électronique permettant de classifier et d'archiver des fichiers en fonction d'un code, d'une famille et une durée de conservation associée.

Le produit offre également la possibilité d'accéder aux services suivants :

- Serveur de messagerie Microsoft Exchange (Tsend propose un plugin Outlook facilitant le partage des fichiers) et serveur Active Directory (pour l'authentification des utilisateurs) ;
- API d'InWebo[2] pour réaliser une authentification multi-facteurs (dans ce cas, l'utilisateur doit enrôler son navigateur ou son téléphone mobile comme périphérique « de confiance ») ;
- API Okta[3] ou Microsoft Azure AD[4] pour réaliser une authentification unique (SSO) ;
- API d'UniversSign[5] pour réaliser la signature électronique de documents.

TransfertPro est aussi compatible SAMLv2 (protocole de fédération d'identité). Si un utilisateur a un provider type (Auth0, OneLogin) alors il peut utiliser ses identifiants d'entreprises pour se connecter à la solution.

La solution *TransfertPro* est administrable via le portail d'administration TAdmin.

Seules les fonctionnalités d'envoi de fichiers et de stockage sont considérées pour l'évaluation.

Comme indiqué, l'envoi de fichiers à un destinataire peut se faire :

- Depuis Tbox garantissant l'authentification mutuelle de l'expéditeur et du destinataire. L'expéditeur peut inviter gratuitement des destinataires à recevoir des fichiers ;

[1] Les fichiers sont supprimés après 30 jours maximum de rétention par défaut (configurable). Il est possible de définir une période d'expiration du téléchargement et d'activer la suppression immédiate du document après téléchargement (non activé par défaut).
[2] https://www.inwebo.fr/
[3] https://www.okta.com/
[4] Service de gestion des identités et des accès basée sur le cloud.
[5] https://www.universign.eu/en/

- Depuis TSend. L'expéditeur depuis Tsend ne doit pas être forcément authentifié pour faire les envois. Il doit alors valider l'envoi via un mail de validation. Le destinataire ne s'identifie pas non plus mais dois saisir le mot de passe partagé afin d'obtenir les fichiers.

Le stockage de fichiers est offert dans Tbox. L'utilisateur stocke des fichiers (pour lui-même ou partagés sur le serveur Transfert Pro).

Pour assurer ces fonctionnalités, *TransfertPro* intègre les éléments suivants :

- Un serveur Web qui est le point de connexion pour l'émetteur et le destinataire (via un navigateur) comprenant :
    - Un serveur de fichier sur lequel sont stockés les fichiers chiffrés ;
    - Un serveur SQL qui comprend les bases de données suivantes :
        - La base *FileUpload* dédiée aux données relatives à la connexion des utilisateurs (noms d'utilisateurs, mots de passe, rôles),
        - La base *FileUploadBackArchive* dédiée aux données métiers (données des sociétés, des fichiers, des dossiers, des partages, des envois, etc.),
        - La base *FileUploadFlow* dédiée aux évènements relatifs aux manipulations de fichiers et aux dossiers que les utilisateurs stockent dans leur espace,
        - La base *ASPState* qui sert à stocker les informations de session des serveurs Web (qui sont éventuellement répartis en charge),
- Une machine virtuelle Ubuntu hébergeant un serveur Collabora Online[6] ou OnlyOffice, permettant de modifier les fichiers depuis l'application *TransfertPro* ;
- Un boitier HSM Trustway Proteccio (développé par la société Bull/Atos) assurant la protection des clés de chiffrement.

La solution est toujours administrée et infogérée par l'éditeur, qui peut la déployer sous 3 formes :

- **SaaS** : l'ensemble des modules (serveurs compris) de la solution est déployée dans le Cloud par TransfertPro (sur des serveurs hébergés en France), qui met en place un HSM Trustway Proteccio, mutualisé entre tous les clients et bénéficiaires. Ces clients et bénéficiaires disposent d'un accès d'administration métier sur l'applicatif uniquement.
- **Dédiée** : contrairement au déploiement SaaS, l'installation est ici dédiée pour un seul client. Néanmoins, l'éditeur TransfertPro est toujours en charge de l'installation et de l'infogérance pour son client. Ce mode de déploiement peut être réalisé « *On Premise* » ou (plus généralement) sur des plateformes IaaS. Dans les deux cas, le HSM est dédié à ce client.
- **Hybride** : une partie de la solution est hébergée « *On Premise* », le reste est hébergé dans l'infrastructure SaaS de TransfertPro.

Dans les trois modes de déploiement, les composants logiciels installés sont strictement identiques, seul le nombre de machines virtuelles utilisées peut varier selon les besoins de performance.

La cible d'évaluation considérée est la version **dédiée** installée « *On Premise* » et la version **SaaS** de la solution *TransfertPro* (multi-tenant).

[6] https://www.collaboraoffice.com/collabora-online-v1-engine

2.2. PRINCIPE DE FONCTIONNEMENT

Via son module Tsend ou Tbox, *TransfertPro* permet l'envoi sécurisé d'un fichier entre plusieurs utilisateurs.

2.2.1. Envoi sécurisé de fichiers

Pour déposer un fichier, l'émetteur se connecte sur *TransfertPro* par un identifiant (adresse email) et un mot de passe puis y dépose son fichier en clair. *TransfertPro* se charge de le chiffrer. L'authentification peut se faire au moyen d'un Active Directory.

Puis, l'émetteur renseigne l'adresse email du destinataire et choisit son mode d'envoi :

- (1) envoi par lien simple : le destinataire n'a pas besoin de compte *TransfertPro*, le fichier est accessible directement en cliquant sur le lien contenu dans le courriel ;
- (2) envoi par lien avec mot de passe : le destinataire n'a pas besoin de compte TransfertPro mais il doit connaître le mot de passe choisi conjointement avec l'émetteur ;
- (3) envoi *TransfertPro* : le destinataire a besoin d'un compte TransfertPro (s'il n'en a pas alors un compte gratuit est créé et le destinataire devient un utilisateur « Tiers ») ;
- (4) envoi *TransfertPro* avec mot de passe : le destinataire doit se connecter sur son compte TransfertPro et saisir le mot de passe choisi conjointement avec l'émetteur.

Seuls les envois avec mot de passe sont retenus dans le périmètre d'évaluation (modes d'envoi (2) et (4)). L'échange du mot de passe entre les correspondants est géré en dehors de la solution (usage d'un SMS, partage par téléphone, en direct, …).

Le transfert (dépôt du fichier sur le serveur TransfertPro et téléchargement par le destinataire) est réalisé via HTTPS. Les communications sont chiffrées selon le protocole TLSv1.2 entre le client et le serveur. TBox supporte également l'accès aux fichiers via un client FTP (hors périmètre de l'évaluation).

Le fichier déposé est stocké temporairement[7] sur le serveur de manière sécurisée, au moyen d'un chiffrement AES-256 en mode CBC dont la clé est dérivée du mot de passe (modes d'envoi (2) et (4)).

À titre indicatif, pour les modes d'envois (1) et (3), qui ne font pas intervenir de mot de passe, (et qui sont considérés hors évaluation) le fichier est chiffré avec une clé générée aléatoirement et stockée sur le serveur *TransfertPro*. L'ensemble des clés est stocké en base de données (serveur SQL distinct du serveur de stockage). L'offre « SaaS » offre la possibilité de protéger ces clés en les chiffrant avec une clé (unique pour chaque société) elle-même stockée dans un boîtier HSM (*Hardware Security Module*).

2.2.2. Stockage de fichiers

Tbox offre à l'utilisateur la fonctionnalité supplémentaire de stockage sécurisé de fichiers :

- Pour lui-même ;
- Au sein de dossiers partagés s'il souhaite les partager avec d'autres utilisateurs.

Dans ce cas, les fichiers sont conservés sur le serveur sans limite de rétention.

[7] Dans Tbox et Tsend, les fichiers envoyés sont conservés jusqu'à 30 jours par défaut.

2.3. DESCRIPTION DES COTS INTEGRES

Les composants tiers intégrés au produit (COTS) sont présentés dans le Tableau 3.

Tableau 3 - COTS intégrés au produit

COTS	Version utilisée	Dernière version	Patch ou modifications appliquées	A jour	Toujours maintenu
Framework .NET [8]	4.8.04161	4.8.04161	**Non**	**Oui**	**Oui**
SQL Server 2022	16.0.4205.1	16.0.4205.1 (10/07/2025)	**Non**		**Oui**
IIS	10.0.20348.1	10.0.20348.1	Script PowerShell[9] de durcissement de IIS	**Oui**	**Oui**
Bouncycastle	BouncyCastle.Cryptography.dll (2.6.2)	2.6.2 (31/07/2025) Tags – bcgit/bcsharp	**Non**	**Oui**	**Oui**
Framework .NET Standard	2.0	2.1 (Non applicable dans notre cas, car doit faire le pont avec la version .net 4.8)	**Non**	**Oui**	**Oui**
LayerCommon	10.2.0.2	10.2.0.2	**Non**	**Oui**	**Oui**

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

2.4.1. Description des dépendances

Une dépendance est un composant nécessaire à la TOE pour fonctionner, mais non fourni directement par la TOE. Le maintien en condition de sécurité de cet élément doit être assuré par l'administrateur de la plate-forme. Ces dépendances peuvent être liées ou non au système hôte.

En version « *On Premise* », la solution *TransfertPro* est fournie sous forme de serveurs virtuels, embarquant les dépendances :

- Framework .NET 4.8 et .Net Standard 2.0 pour la librairie LayerCommon ;
- SQL Server 2022 ;
- IIS 10.

[8] .NET Framework net prenant pas en charge .NET Standard 2.1.

[9] https://www.hass.de/content/setup-microsoft-windows-or-iis-ssl-perfect-forward-secrecy-and-tls-12

2.4.2. Matériel compatible ou dédié

Dans le cadre de l'évaluation, un HSM logiciel (SoftHSM2) sera utilisé (à la place du Trustway Proteccio développé par la société Bull/Atos) afin de stocker et protéger les clés de chiffrement.

2.4.3. Système d'exploitation retenu

Les composants constituant le serveur TransfertPro sont compatibles avec un environnement Windows Server 2022.

2.5. PERIMETRE DE L'EVALUATION

2.5.1. Périmètre

La TOE[10] considérée est le serveur *TransfertPro* de l'offre « *On Premise* » et « SaaS ». Dans le cadre de l'évaluation de gamme, le produit de référence sur lequel les tests seront joués est l'offre « *On Premise* ». Le seul produit décliné de l'évaluation de gamme est l'offre « SaaS ».

Sont considérés dans le périmètre de l'évaluation :

- L'authentification simple (l'authentification via Active Directory est supportée mais non considérée pour l'évaluation) ;
- Les fonctionnalités d'envoi/réception de documents dan Tbox et Tsend, sécurisés par mot de passe ;
- Les communications HTTPS entre le serveur *TransfertPro* et les navigateurs Web des utilisateurs ;
- Les communications entre les différents serveurs de la solution *TransfertPro* (cf schéma en Figure 1) ;
- Le stockage des fichiers dans Tbox et Tsend ;
- Le stockage des clés de chiffrement en base de données SQL ;
- Les interactions avec le HSM ;
- L'administration via TAdmin.

Sont considérés en dehors du périmètre de l'évaluation :

- La fonctionnalité d'édition de fichiers en ligne. Le serveur Collabora Online n'est donc pas déployé ;
- La fonctionnalité de signature électronique (service UniverSign) ;
- L'authentification multi-facteurs (service InWebo) ;
- La fonctionnalité d'envoi de documents sans mot de passe ;
- Le HSM ;
- La machine physique et le système d'exploitation où sont installés les serveurs de la solution ;
- Le serveur de messagerie Exchange et ses communications.

[10] *Target Of Evaluation*

La configuration du produit évalué est présentée dans le Tableau 4.

Tableau 4 - Composants du système

Composant du système global		Inclus dans la cible de l'évaluation (TOE)	Non évalué (environnement de la TOE)	
			Supposé de confiance	Est un attaquant potentiel
Serveur TransfertPro	Système d'exploitation Windows Server 2022		√	
	Serveur web IIS	√		
	Fonctions cryptographiques	√		
	Base de données SQL Server	√		
Client	Système d'exploitation Windows 10		√	
HSM	Fonctions cryptographiques		√	
Serveur de messagerie	Serveur Exchange		√	

2.5.2. Plateforme d'évaluation

La figure suivante présente la plateforme d'évaluation. L'installation sera effectuée « *On Premise* ».

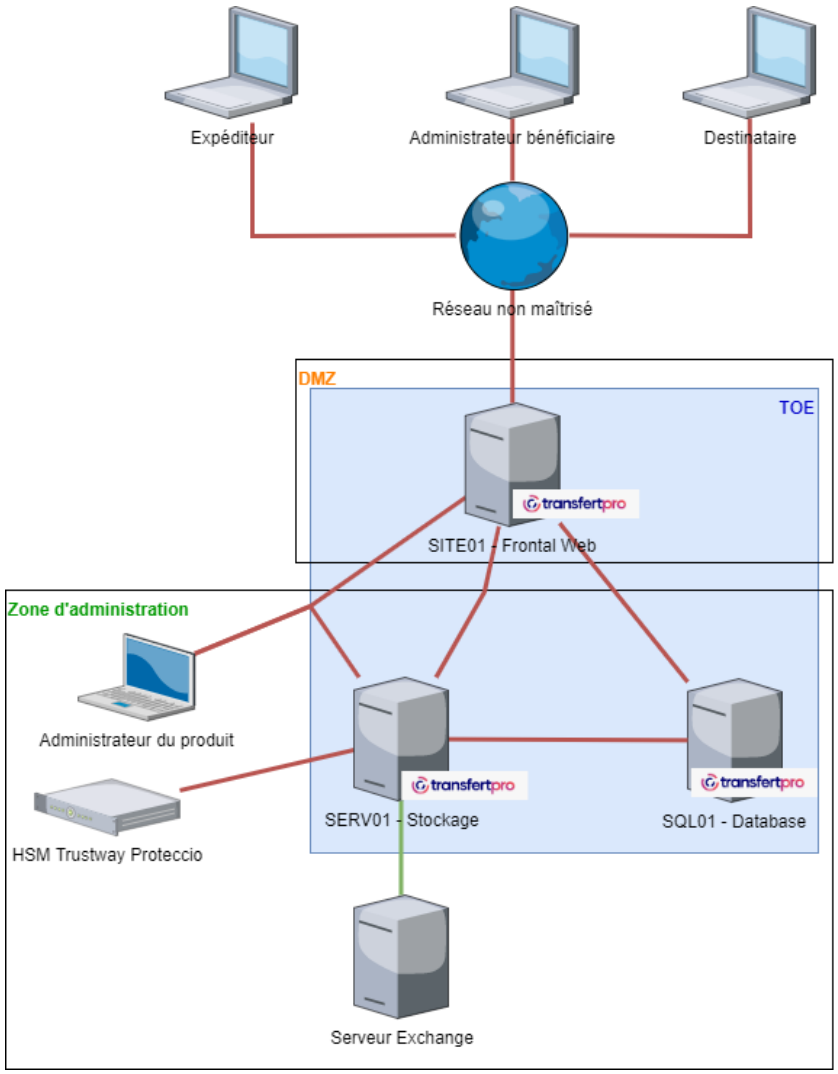

Figure 1 : Plateforme d'évaluation

Le serveur de messagerie Microsoft Exchange est installé sur un poste Windows Server 2022.

La solution *TransfertPro* est composée de trois serveurs, hébergeant chacun un composant dédié :

- Un serveur Web frontal, accessible par les utilisateurs finaux et les administrateurs bénéficiaires ;
- Un serveur de stockage, contenant l'applicatif *TransfertPro* et en charge du stockage des fichiers et des données ;
- Un serveur de base de données.

Le serveur Web frontal est installé dans une DMZ, accessible depuis Internet. Les deux autres serveurs sont installés dans un réseau dédié à ces composants (protégé conformément à l'hypothèse H3).

Le boîtier HSM, utilisé par le serveur de stockage, et le serveur Exchange sont également installés dans cette zone du SI. L'administration des serveurs se fait à partir de ce même réseau local dédié.

Un poste Windows 10 est choisi pour les machines de l'émetteur, du destinataire et de l'administrateur des bénéficiaires, sur lesquelles est installé le navigateur Web Mozilla Firefox (utilisé comme client) à jour. Le poste utilisé par les administrateurs du produit est un PC Windows 10.

Le HSM étant en dehors de l'évaluation, il a été décidé d'utiliser SoftHSM2 en lieu et place du HSM physique afin de simplifier les travaux, tout en conservant strictement la même chaîne de connexion. L'évaluation des communications réseaux entre la solution *TransfertPro* et le HSM physique sont réalisés depuis l'environnement de production, selon un plan de tests défini au préalable par le CESTI, sous la supervision de l'éditeur.

3. PROBLEMATIQUE DE SECURITE

Ce chapitre décrit le panorama sécuritaire de la TOE. Il consiste en une présentation des acteurs, des ressources stratégiques et des hypothèses.

3.1. DESCRIPTION DES UTILISATEURS

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec le produit évalué. Les rôles devant être pris en considération dans le cadre de l'évaluation de sécurité sont présentés dans le

Tableau **5**.

Tableau 5 - Utilisateurs de la TOE

ID	Description de l'acteur	Degré de confiance
A.1	**Utilisateur principal** Individu disposant d'un compte TransfertPro et effectuant des opérations d'envoi ou de réception d'un fichier, ou de stockage de fichiers	Attaquant potentiel
A.2	**Utilisateur tiers** Individu disposant seulement d'un compte TransfertPro gratuit créé lorsqu'il est destinataire d'un fichier (par envoi ou dossier partagé), via la solution *TransfertPro,* en provenance d'un individu détenant le rôle « Utilisateur principal »	Attaquant potentiel
A.3	**Externe** Individu dit « Open », ne disposant pas de compte TransfertPro et recevant un fichier transmis sous la forme d'un lien téléchargeable par une personne détenant le rôle « Utilisateur principal »	Attaquant potentiel
A.4	**Administrateur bénéficiaire** Individu en charge d'administrer le *tenant TransfertPro* de son organisation (accès aux mécanismes de journalisation des opérations, de gestion des utilisateurs) via le portail TAdmin	Utilisateur de confiance
A.5	**Super-Administrateur** Individu en charge d'administrer la solution *TransfertPro* (accès aux mécanismes de journalisation des opérations, de gestion des utilisateurs, de configuration de la solution, gestion des bénéficiaires, configuration du HSM) via le portail TAdmin	Utilisateur de confiance
A.6	**Administrateur système** Individu en charge d'administrer le système support sur lequel est installée la solution *TransfertPro*. Il a également en charge l'administration locale du HSM	Utilisateur de confiance

Avec l'accord de la société cliente qui héberge le serveur TransfertPro « *On Premise* », une administration à distance peut aussi être faite par un profil « host » d'un collaborateur de la société TransfertPro. Ce rôle est exclu de la cible de sécurité.

Pour le déploiement SaaS, la répartition des rôles est présentée dans le Tableau 6.

Tableau 6 - Répartition des rôles

Rôle	Socle	Tenue du rôle
Utilisateur final (Utilisateur principal, tiers, externe)	Utilisation métier	Bénéficiaire
Administrateur métier (Administrateur bénéficiaire, Super-Administrateur)	Paramétrage métier	Bénéficiaire
Administrateur système	Logiciel et données	Éditeur
	Intergiciels et autres logiciels de base	Éditeur
	Système d'exploitation	Éditeur
	Ressources virtualisées	Fournisseur du socle
Administrateur de l'infrastructure technique	Couche de virtualisation	Fournisseur du socle
	Machines physiques, réseau et stockage	Fournisseur du socle
Officier de sécurité	Sécurité des locaux et du personnel	Fournisseur du socle

Pour le déploiement « *On Premise* », ces rôles sont assurés par le bénéficiaire (client).

3.2. DESCRIPTION DES BIENS SENSIBLES

Par définition, un bien sensible est une donnée (ou fonction) jugée comme ayant de la valeur par la TOE. Sa valeur est estimée selon des critères de sécurité (aussi appelés besoins de sécurité) : disponibilité, intégrité, confidentialité et authenticité.

Les biens à protéger sont les présentés dans le Tableau 7.

Tableau 7 - Biens sensibles

ID	Description du bien sensible	Besoin de protection
B.1	**Données d'identification et d'authentification** Ce bien concerne les données relatives à la connexion des utilisateurs permettant l'accès à un compte *TransfertPro*. Ces données peuvent être stockées sur un système ou transiter sur le réseau.	Confidentialité Intégrité
B.2	**Données utilisateur** Ce bien concerne les données métiers qui sont stockées chiffrées sur le serveur *TransfertPro*et qui peuvent être partagées (envoyées via Tsend/Tbox	Confidentialité Disponibilité Intégrité

	sur le réseau, ou stockées dans Tbox) à différents utilisateurs via la solution *TransfertPro*.	
B.3	**Données de journalisation** Ce bien concerne les évènements relatifs aux opérations des utilisateurs de *TransfertPro*.	Intégrité
B.4	**Eléments secrets** Ce bien concerne les clés cryptographiques utilisées pour assurer la protection des fichiers envoyés ou stockés.	Confidentialité Intégrité
B.5	**Données de configuration** Ce bien concerne les données utiles pour assurer le fonctionnement de la TOE (fichiers de configuration des serveurs Web, de fichiers et SQL du serveur *TransfertPro*).	Confidentialité Intégrité
B.6	**Flux réseau** Ce bien concerne les flux réseaux manipulés par la TOE (communications entre les différents serveurs *TransfertPro*, communications liées aux accès utilisateurs, communications liées aux accès administrateurs, communications avec le HSM).	Confidentialité Disponibilité Intégrité
B.7	**Système hôte** Ce bien concerne le système et les serveurs sur lesquels sont installés les applicatifs *TransfertPro*.	Intégrité

Les besoins de sécurité de chacun des biens à protéger sont synthétisés dans le Tableau 8.

Tableau 8 - Besoins de sécurité des biens sensibles

Biens sensibles	Disponibilité	Intégrité	Confidentialité
B1. Données d'identification et authentification		√	√
B2. Données utilisateur	√	√	√
B3. Données de journalisation		√	
B4. Eléments secrets		√	√
B5. Données de configuration		√	√
B6. Flux réseaux	√	√	√
B7. Système hôte		√	

Dans le cas du déploiement SaaS, l'appartenance des biens sensibles devant être protégés est présentée dans le tableau suivant.

Tableau 9 - Appartenance des biens sensibles

Bien sensible	Appartenance à l'utilisateur final (Sur le poste utilisateur)	Appartenance à l'administrateur métier (Dans le cloud)	Appartenance à la TOE
B1. Données d'identification et authentification		√	
B2. Données utilisateur		√	
B3. Données de journalisation		√	
B4. Eléments secrets			√
B5. Données de configuration		√	
B6. Flux réseaux		√	
B7. Système hôte		√	

Dans le cas du déploiement « *On Premise* », les biens sensibles sont stockés dans l'infrastructure du bénéficiaire.

3.3. DESCRIPTION DES HYPOTHESES SUR L'ENVIRONNEMENT

Par définition, les hypothèses sont des déclarations portant sur le contexte d'emploi de la TOE ou de son environnement. Les hypothèses sur l'environnement de la TOE à considérer sont présentées dans le

Tableau 10.

Tableau 10 - Hypothèses sur l'environnement

ID	Type de mesure	Description de la mesure	Acteurs en charge de la mesure
H.1	Organisationnelle	**Administrateurs TOE formés et de confiance** Les administrateurs de la TOE (serveur TransfertPro) sont considérés de confiance et formés à l'utilisation et à l'administration de la TOE. Le poste de l'administrateur de la TOE est situé dans le réseau séparé et dédié. L'administration à distance est désactivée par défaut (pour le profil « host »).	A.4 A.5 A.6
H.2	Organisationnelle	**Administrateurs système formés et de confiance** Les administrateurs système ou d'infrastructure sont considérés de confiance et formés à l'utilisation ainsi qu'à l'administration du système support sur lequel est installé la TOE et des systèmes supports des serveurs participant à la mise en œuvre de la solution *TransfertPro*. Les composants du serveur TransfertPro (serveur web, serveur de fichiers, serveur SQL) sont configurés et administrés comme préconisés par la documentation de l'éditeur (permissions, services, protocoles et algorithmes selon les recommandations de l'éditeur, etc.).	A.5 A.6
H.3	Sécurité logique et physique	**Environnement sécurisé** Le serveur TransfertPro ainsi que les serveurs participant à la mise en œuvre de la solution sont installés sur des systèmes d'exploitation sains et correctement mis à jour. Les services et partages inutiles sont désactivés. Le socle IaaS est considéré de confiance. Les serveurs de la solution *TransfertPro* sont installés au sein d'une DMZ et d'une zone d'administration (protégées selon les recommandations de l'éditeur). En particulier, des moyens techniques sont mis en place en entrée de la DMZ (pare-feu, anti-DDOS, etc.). Les serveurs de la solution *TransfertPro* sont déployés dans un local dont les accès sont nominativement contrôlés.	A.5 A.6
H.4	Sécurité logique	**Environnement clients sain** Les postes client sont dotés d'un système d'exploitation et d'un navigateur Web sains et correctement mis à jour, en particulier concernant les correctifs liés à la sécurité.	A.6

H.5	Sécurité logique	**HSM à l'état de l'art** Seul le serveur *TransfertPro* accède au HSM dont l'administration est effectuée en local. Le HSM implémente des mécanismes cryptographiques à l'état de l'art, est qualifié par l'ANSSI et utilisé selon les recommandations d'usage de la décision de qualification.	A.6

Dans le cas du déploiement SaaS :

- L'hypothèse H.1 est associée à l'**administrateur métier** de la TOE ;
- L'hypothèse H.2 est associée à l'**administrateur système** ;
- Les hypothèses H.2, H.3 et H.5 sont associées à **l'administrateur d'infrastructure technique** et à l'**officier de sécurité**.

3.4. DESCRIPTION DES MENACES

Par définition, une menace est une action ou un événement susceptible de porter préjudice à la sécurité de la cible évaluée.

Le Tableau 5 donne le degré de confiance associé aux utilisateurs de la TOE.

Les agents menaçants à considérer pour l'évaluation de sécurité doivent être les suivants :

- Un attaquant humain ou entité qui interagit ou non avec la TOE mais ne disposant pas d'accès légitime à celle-ci (attaquant **hors-bénéficiaire**) ;
  - Utilisateur A.3
- Un utilisateur légitime (muni d'un compte TransfertPro) qui souhaite contourner certaines restrictions d'accès (attaquant **bénéficiaire**) :
  - Un attaquant cherchant à compromettre des biens sensibles de la TOE ou d'un autre utilisateur du même bénéficiaire (attaquant **intra-bénéficiaire**) ;
  - Un attaquant provenant d'un bénéficiaire cherchant à compromettre des biens sensibles d'un autre bénéficiaire (attaquant **inter-bénéficiaire**).
    - Utilisateurs A.1, A.2 et A.4

Les attaquants peuvent être situés sur le réseau non maîtrisé, dans la DMZ ou dans la zone d'administration (liens indiqués en rouge dans le schéma de la plateforme d'évaluation en Figure 1. Les liens en vert sont supposés de confiance).

Par conséquent, la TOE doit résister à ces agents menaçants ainsi qu'aux moyens logiciels et matériels mis en œuvre par ces derniers. Ces moyens sont les suivants :

Tableau 11 - Moyens exploités par les attaquants

Moyens exploités par les agents menaçants	Moyen mis en œuvre		TOE résistante à un attaquant	
	Logiciel	Matériel	Local	Distant
Vulnérabilité de la session utilisateur	√			
Vol d'authentifiants	√	√		
Vulnérabilité du cloisonnement utilisateur	√			

Vulnérabilité réseau	√		√	

Les menaces qui portent sur les biens sensibles de la TOE sont présentées dans le Tableau 12.

Tableau 12 - Menaces

ID	Description	Interfaces d'attaque	Acteur de la menace	Bien impacté
M.1	**Vol des données d'authentification** Un attaquant parvient à récupérer les données d'identification et/ou d'authentification d'un utilisateur muni d'un compte TransfertPro.	I1	A.1 A.2 A.3 A.4	B.1 B.6
M.2	**Accès illégitime aux données** Un attaquant parvient à accéder aux fichiers chiffrés ou temporaires d'un utilisateur, stockés sur le serveur TransfertPro ou envoyés à un destinataire.	I1	A.1 A.2 A.3 A.4	B.2 B.4 B.6
M.3	**Altération des données utilisateurs** Un attaquant parvient à modifier les données utilisateurs à l'insu de l'utilisateur légitime.	I1	A.1 A.2 A.3 A.4	B.2 B.6
M.4	**Altération des données de journalisation** Un attaquant parvient à modifier les données de journalisation afin de masquer des actions illégitimes.	I1	A.1 A.2 A.3 A.4	B.3 B.6
M.5	**Compromission des éléments secrets** Un attaquant parvient à modifier/lire les clés cryptographiques utilisées pour le chiffrement des fichiers.	I2	A.1 A.2 A.3 A.4	B.4 B.5 B.6
M.6	**Altération des données de configuration** Un attaquant parvient à modifier les données de configuration du produit dans le but d'abaisser le niveau de sécurité du serveur TransfertPro ou d'exfiltrer des données sensibles.	I2	A.1 A.2 A.3 A.4	B.5 B.6
M.7	**Déni de service** Un attaquant parvient à rendre le service inopérant et non disponible pour les utilisateurs légitimes.	I1	A.1 A.2 A.3 A.4	B.2 B.6
M.8	**Contrôle du produit à distance** Un attaquant parvient à prendre le contrôle du produit, à distance, pour s'accorder des droits supplémentaires.	I1	A.1 A.2 A.4	B.2 B.5 B.7

3.5. DESCRIPTION DES FONCTIONS

3.5.1. Fonctions métier

Les fonctions métiers sont l'ensemble des fonctions actives et mises en œuvre par la TOE pour assurer son fonctionnement et répondre au besoin pour lequel elle a été développée. Ces fonctions métiers ne seront pas évaluées en conformité mais uniquement en robustesse.

Pour l'évaluation, ces fonctions sont considérées comme des fonctions de sécurité.

3.5.2. Fonctions de sécurité

Par définition, les fonctions de sécurité sont l'ensemble des mesures techniques et mécanismes mis en œuvre dans la TOE pour protéger de façon proportionnée les biens sensibles de la TOE contre les menaces identifiées.

Les fonctions de sécurité essentielles de la TOE sont les présentées dans le Tableau 13.

Tableau 13 - Fonctions de sécurité

ID	Description	Argumentaire de couverture des menaces
FS.1	**Identification, authentification** L'accès aux fonctionnalités du produit (compte TransfertPro) est protégé par un système d'authentification par mot de passe. Lorsqu'un utilisateur dont le compte a été verrouillé tente de se connecter avec un mot de passe valide la connexion doit être validée par l'envoi d'un code (TOTP) par email. Le TOTP (« Time-Based One-Time Password ») est un mot de passe à usage unique généré à partir d'un secret et de l'heure actuelle. Contrairement à un OTP classique (« One-Time Password »), le TOTP est calculé localement et change toutes les 30 secondes, et n'a donc pas besoin d'être stocké lors de sa génération, renforçant ainsi la sécurité. Le secret est généré à partir de l'email de l'utilisateur et de sa date de fin de blocage de compte (correspondant à la date du 25ème mot de passe erroné à laquelle est ajouté 5 minutes), le tout hashé ensuite via l'algorythme SHA512.	La fonction interdit aux acteurs A.1, A.2, A.3 et A.4 de mettre en œuvre les menaces M.1 et M.2. Il n'existe pas d'autres acteurs potentiellement malveillants. Le reste des acteurs (A.5 et A.6) sont de confiance.
FS.2	**Contrôle d'accès et gestion des droits/privilèges entre utilisateurs** Un contrôle d'accès aux données est assuré pour garantir le cloisonnement entre les différents bénéficiaires du service TransfertPro. Suivant les droits d'accès positionnés sur les dossiers, l'utilisateur peut partager ou non ses fichiers à d'autres utilisateurs. Les privilèges des utilisateurs sont segmentés pour garantir que seuls les administrateurs peuvent modifier la configuration du produit ou les permissions des bénéficiaires.	La fonction interdit aux acteurs A.1, A.2, A.3 et A.4 de mettre en œuvre les menaces M.2, M.3, M.4, M.5, M.6 et M.8. Il n'existe pas d'autres acteurs potentiellement malveillants. Le reste des acteurs (A.5 et A.6) sont de confiance.
FS.3	**Protection des données utilisateurs** Le produit protège en confidentialité et en intégrité les données de l'utilisateur (fichiers échangés via Tsend ou Tbox, et fichiers stockés dans Tbox).	La fonction interdit aux acteurs A.1, A.2, A.3 et A.4 de mettre en œuvre les menaces M.2 et M.3. Il n'existe pas d'autres acteurs potentiellement malveillants. Le reste des acteurs (A.5 et A.6) sont de confiance.
FS.4	**Communications sécurisées** Les flux avec le serveur TransfertPro sont protégés en intégrité et confidentialité via l'encapsulation TLS. HSTS est activé.	La fonction interdit aux acteurs A.1, A.2, A.3 et A.4 de mettre en œuvre les menaces M.1, M.2, M.3 et M.5. Il n'existe pas d'autres acteurs potentiellement malveillants. Le reste des acteurs (A.5 et A.6) sont de confiance.

FS.5	**Journalisation** La TOE assure l'intégrité des données de journalisation (celles relatives à l'enregistrement des événements correspondant aux fichiers et aux dossiers que les utilisateurs stockent).	La fonction interdit aux acteurs A.1, A.2, A.3 et A.4 de mettre en œuvre les menaces M.4 et M.6 Le reste des acteurs (A.5 et A.6) sont de confiance.
FS.6	**Fonctions cryptographiques** Pour assurer la protection des fichiers dans Tbox, le produit génère des éléments aléatoires stockés en base de données. Il peut assurer la protection des clés en confidentialité en les chiffrant au moyen d'un HSM avant leur stockage en base. Le chiffrement assuré par le HSM est hors périmètre.	La fonction interdit aux acteurs A.1, A.2, A.3 et A.4 de mettre en œuvre la menace M.5. Le reste des acteurs (A.5 et A.6) sont de confiance.
FS.7	**Autoprotection** La TOE met en œuvre des mécanismes de protection pour contrer des attaques portées contre son fonctionnement (par exemple pour empêcher le déni de service ou l'atteinte au système hôte).	La fonction interdit aux acteurs A.1, A.2, A.3 et A.4 de mettre en œuvre les menaces M.7 et M.8. Le reste des acteurs (A.5 et A.6) sont de confiance.

3.5.3. Fonctions désactivées

Les fonctions désactivées sont les fonctions considérées comme étant en dehors du périmètre de l'évaluation (hors TOE). Ces fonctions ne seront pas évaluées, mais seront prises en compte en tant que vecteurs d'attaque potentiels sur la TOE (protection vis-à-vis d'une activation par un attaquant). Les fonctions désactivées de la TOE sont présentées dans le Tableau 14.

Tableau 14 - Fonctions désactivées

ID	Description
FD.1	**Services tiers** Les connexions réalisées par le serveur TransfertPro sur les services tiers (InWebo, UniversSign) sont désactivées. Ces services sont optionnels.

3.6. SURFACE D'ATTAQUE

Cette section décrit l'ensemble des moyens par lesquels il est possible d'interagir avec le produit (interfaces physiques, logiques, locales ou distantes).

Tableau 15 - Interfaces avec la TOE

Type de surface d'attaque	Interfaces (accessibles ou non accessibles)	Fonction concernée (évaluée ou non évaluée)	Acteurs ayant accès aux interfaces
Interfaces logiques	Interface réseau du HSM	Non évaluée (H.3)	
	I1. Interface web – SITE01 Port 443 HTTPS	FS.1 FS.2 FS.4	A.1 A.2 A.3 A.4
	I2. Console (tty) d'un serveur de la TOE	Non évaluée (H.3)	A.6
	Interface RPC – SQL01 Port 1433	Non évaluée (H.3)	
	Interface web – SERV01 Port 443 HTTPS	Non évaluée (H.3)	
	Interface SMB2 – SERV01 Port 445	Non évaluée (H.3)	
	Interface WebDeploy – SERV01 Port 8172	Non évaluée (H.3)	
	Interface NetBios – ALL Port 135 (tcp) – 137 (udp) -138 (udp)	Non évaluée (H.3)	
	Interface MSDTC – ALL Port 5000 à 5100	Non évaluée (H.3)	
	Interface RDP – ALL Port 3389	Non évaluée (H.3)	

La TOE ne dispose pas d'interfaces physiques.

3.7. MATRICES DE COUVERTURES

3.7.1. Menaces et biens sensibles

La matrice suivante présente la couverture des menaces sur les biens sensibles (les lettres "D", "I", "C" et "A" représentent respectivement les besoins de Disponibilité, Intégrité, Confidentialité et Authenticité) :

Tableau 16 - Couverture des biens sensibles par les menaces

	B1. Données d' identification et d' authentification	B2. Données utilisateur	B3. Données de journalisation	B4. Éléments secrets	B5. Données de configuration	B6.Flux réseaux	B7. Système hôte
M1.Vol des données d'authentification	**C**					**C**	
M2.Accès illégitime aux données		**C**		**C**		**C**	
M3.Altération des données utilisateurs		**I**				**I**	
M4.Altération des données de journalisation			**I**			**I**	
M5.Compromission des éléments secrets				**IC**	**C**	**CI**	
M6.Altération des données de configuration					**I**	**C**	
M7.Déni de service		**D**				**D**	
M8.Contrôle du produit à distance		**CI**			**I**		**I**

3.7.2. Menaces et fonctions de sécurité

La matrice suivante présente la couverture des menaces par les fonctions de sécurité :

Tableau 17 - Couverture des menaces par les fonctions de sécurité

	FS1.Identification et Authentification	FS2. Contrôle d' accès et gestion des droits/privilèges entre utilisateurs	FS3.Protection des données utilisateurs	FS4. Communications Sécurisées	FS5.Journalisation	FS6.Fonction cryptographique	FS7.Autoprotection
M1.Vol des données d'authentification	√			√			
M2.Accès illégitime aux données	√	√	√	√			
M3.Altération des données utilisateurs		√	√	√			
M4.Altération des données de journalisation		√			√		
M5.Compromission des éléments secrets		√		√		√	
M6.Altération des données de configuration		√			√		
M7.Déni de service							√
M8.Contrôle du produit à distance		√					√

3.7.3. Menaces et moyens exploités par les agents menaçants

La matrice suivante présente la couverture des moyens exploités par rapport aux menaces retenues.

Tableau 18 - Couverture des moyens exploités par rapport aux menaces

	M1.Vol des données d' authentification	M2.Accès illégitime aux données	M3.Altération des données utilisateurs	M4.Altération des données de journalisation	M5.Compromission des éléments secrets	M6.Altération des données de configuration	M7.Déni de service	M7.Déni de service
Vulnérabilité de la session utilisateur	√							√
Vol d'authentifiants	√							
Vulnérabilité du cloisonnement utilisateur		√	√	√	√	√		√
Vulnérabilité réseau		√	√	√	√	√	√	

Fin du document