Cible de sécurité CSPN

TransfertPro « On Premise »

Catégories « Stockage sécurisé » et « Communication sécurisée »

Référence : CSPN-ST-TransfertPro-3.00
Date : le 30/11/2017
Code interne : INO001

Siège : 4 bis allée du Bâtiment • 35000 Rennes • France • www.amossys.fr
SIRET : 493 348 890 00036 • **NAF** : 6202 A • RCS Rennes B 493 348 890 • SAS au capital de 38.000 Euros

FICHE D'ÉVOLUTIONS

RÉVISION	DATE	DESCRIPTION	RÉDACTEURS
1.00	24/02/2016	Création du document	François COURBIER
2.00	20/12/2016	Mise à jour suite à des modifications fonctionnelles de la solution	Alexandre DELOUP Antoine COUTANT
2.01	13/01/2017	Prise en compte des remarques de l'ANSSI	Antoine COUTANT
3.00	30/11/2017	Modifications suite à l'évaluation CSPN	Alexandre DELOUP

Ce document est validé par TransfertPro.

SOMMAIRE

1. INTRODUCTION

1.1. OBJET DU DOCUMENT

Ce document est réalisé dans le cadre de l'évaluation, selon le schéma CSPN[1] promu par l'ANSSI[2], de la solution TransfertPro « On Premise » développée par la société **TransfertPro**.

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™ TransfertPro SAS 1 Avenue de la gare - BP 16200 Alixan 26958 VALENCE CEDEX 9
Lien vers l'organisation	https://www.transfertpro.com
Nom commercial du produit	TransfertPro « On Premise »
Numéro de la version évaluée	3.0.3.5
Catégories du produit	Stockage sécurisé Communication sécurisée

1.3. RÉFÉRENCES

Pour l'établissement de la présente cible de sécurité, les liens suivants ont été consultés :

- site de l'éditeur : https://www.transfertpro.com ;
- aide en ligne : https://help.transfertpro.com.

[1] Certification de Sécurité de Premier Niveau
[2] Agence nationale de la sécurité des systèmes d'information

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GÉNÉRALE

TransfertPro est une suite de logiciels web permettant le stockage ainsi que le transfert de documents de manière sécurisée. Plusieurs versions de cette solution sont proposées par le développeur **TransfertPro** :

- *TransfertPro* version « Gratuite » : permet l'envoi de fichiers de façon chiffrée à un ou plusieurs destinataires ;
- *TransfertPro* version « Cloud » : intègre une fonctionnalité de stockage sécurisé. Ainsi, des fichiers peuvent être stockés de manière sécurisée sur une infrastructure cloud dont les serveurs sont hébergés en France. Un mécanisme de synchronisation avec un ordinateur est aussi disponible ;
- *TransfertPro* version « On Premise » : l'ensemble de la solution « Cloud » (serveurs compris) hébergée par un client ce qui lui permet ainsi de maîtriser l'intégralité des éléments de la solution.

La cible d'évaluation considérée est la version « On Premise » de la solution *TransfertPro*.

2.2. PRINCIPE DE FONCTIONNEMENT

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 :

- (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)). Pour les modes d'envois (1) et (3) qui sont considérés hors évaluation, le fichier est chiffré avec une clé générée aléatoirement et stockée sur le serveur *TransfertPro*. Dans l'offre « Cloud », les clés sont stockées soit sur un serveur physique distinct (serveur SQL) du serveur de stockage, soit sur un boîtier HSM (*Hardware Security Module*).

Pour l'échange du mot de passe, le destinataire et l'émetteur se mettent d'accord sur le moyen utilisé (SMS, téléphone, en direct, ...).

2.2.1. Principales fonctionnalités de TransfertPro

Les deux principales fonctionnalités mises en œuvre par *TransfertPro* sont le transfert et le stockage de fichiers. *TransfertPro* repose sur l'utilisation de deux mécanismes :

- l'utilisation de communications chiffrées (TLSv1.2) entre le client et le serveur pour le chargement et le téléchargement de fichiers ;
- l'utilisation d'un mécanisme de chiffrement afin de stocker les fichiers de façon sécurisée sur le serveur. Le chiffrement des fichiers est réalisé par l'utilisation de l'algorithme AES-256 en mode CBC, avec un vecteur d'initialisation généré aléatoirement. La clé utilisée est dérivée du mot de passe par la fonction PBKDF2. Le contrôle d'intégrité des fichiers est réalisé par l'utilisation de la fonction de hachage HMAC-SHA256. L'ensemble de ces opérations est réalisé par la bibliothèque cryptographique Bouncy Castle[3] (sources récupérées sur https://github.com/bcgit/bc-csharp.git, recompilées par **TransfertPro** et *dll*[4] intégrée dans les binaires *TransfertPro*).

Pour l'offre « On Premise », *TransfertPro* comprend 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[5], permettant de modifier les fichiers depuis l'application *TransfertPro* ;
- un boitier HSM Trustway Proteccio (développé par la société Bull/Atos) permettant de stocker la clé de société. Cette clé, unique par société, permet de chiffrer les clés de chiffrement avant leur stockage en base.

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

- serveur de messagerie Microsoft Exchange (*TransfertPro* propose un plugin Outlook facilitant le partage des fichiers) et serveur Active Directory (pour l'authentification des utilisateurs) ;
- API d'InWebo[6] pour réaliser une authentification multi-facteurs (dans ce cas, l'utilisateur doit enrôler son navigateur ou son téléphone mobile comme périphérique « de confiance ») ;
- API d'UniversSign[7] pour réaliser la signature électronique de documents.

---

[3] http://www.bouncycastle.org/csharp/
[4] *Dynamic Link Library*
[5] https://www.collaboraoffice.com/collabora-online-v1-engine
[6] https://www.inwebo.fr/
[7] https://www.universign.eu/en/

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

Enfin, la solution *TransfertPro* est administrable à distance par un accès en TSE/RDS (successeur du protocole RDP).

2.2.2. Processus de chiffrement et de déchiffrement de fichiers

Le processus de chiffrement d'un fichier est le suivant :

- génération d'une clé AES 256 bits, d'un vecteur d'initialisation (IV) et d'une clé HMAC-SHA256 par appel à la dll Bouncy Castle ;
- génération d'un GUID[8] pour anonymiser le fichier stocké chiffré ;
- génération de l'empreinte du fichier HMAC-SHA256 et chiffrement du fichier en AES 256 bits (mode CBC) ;
- concaténation de l'IV, du chiffré et du HMAC ;
- stockage de la concaténation sous le nom du GUID sur le serveur TransfertPro ;
- génération (par appel à la dll Bouncy Castle) d'un IV AES 256 bits et chiffrement de la clé de chiffrement du fichier avec la clé de la société contenue dans le HSM ;
- génération (par appel à la dll Bouncy Castle) d'un IV AES 256 bits et chiffrement de la clé du HMAC du fichier avec la clé de la société contenue dans le HSM ;
- stockage en base de données des deux IV de chiffrement, de la clé HMAC chiffrée, de la clé AES chiffrée et des informations du fichier (nom, taille...).

Pour résumer, par fichier chiffré, il y a une clé de chiffrement AES, une clé HMAC-SHA256 et deux vecteurs d'initialisation (IV).

Les fichiers chiffrés sont stockés sur le serveur et non pas en base de données.

2.3. DESCRIPTION DES DÉPENDANCES ET DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

Le serveur *TransfertPro* est compatible avec un environnement Windows Server 2012 R2.

2.4. PÉRIMÈTRE DE L'ÉVALUATION

Seule l'offre « On Premise » de la solution *TransfertPro*, avec l'envoi par mot de passe, est considérée dans le cadre de l'évaluation. Les liens HTTPS entre le serveur *TransfertPro* et les navigateurs Web font aussi partie du périmètre de l'évaluation.

Les options de la version « On Premise », *ie* l'édition en ligne et la signature électronique, ne sont pas présentes. Ce qui suppose donc l'exclusion de Collabora Online du périmètre de l'évaluation.

La TOE[9] considérée est le serveur *TransfertPro* de l'offre « On Premise » sous environnement Windows Server 2012 R2.

La figure suivante présente la plateforme d'évaluation.

[8] *Globally Unique IDentifier*
[9] *Target Of Evaluation*

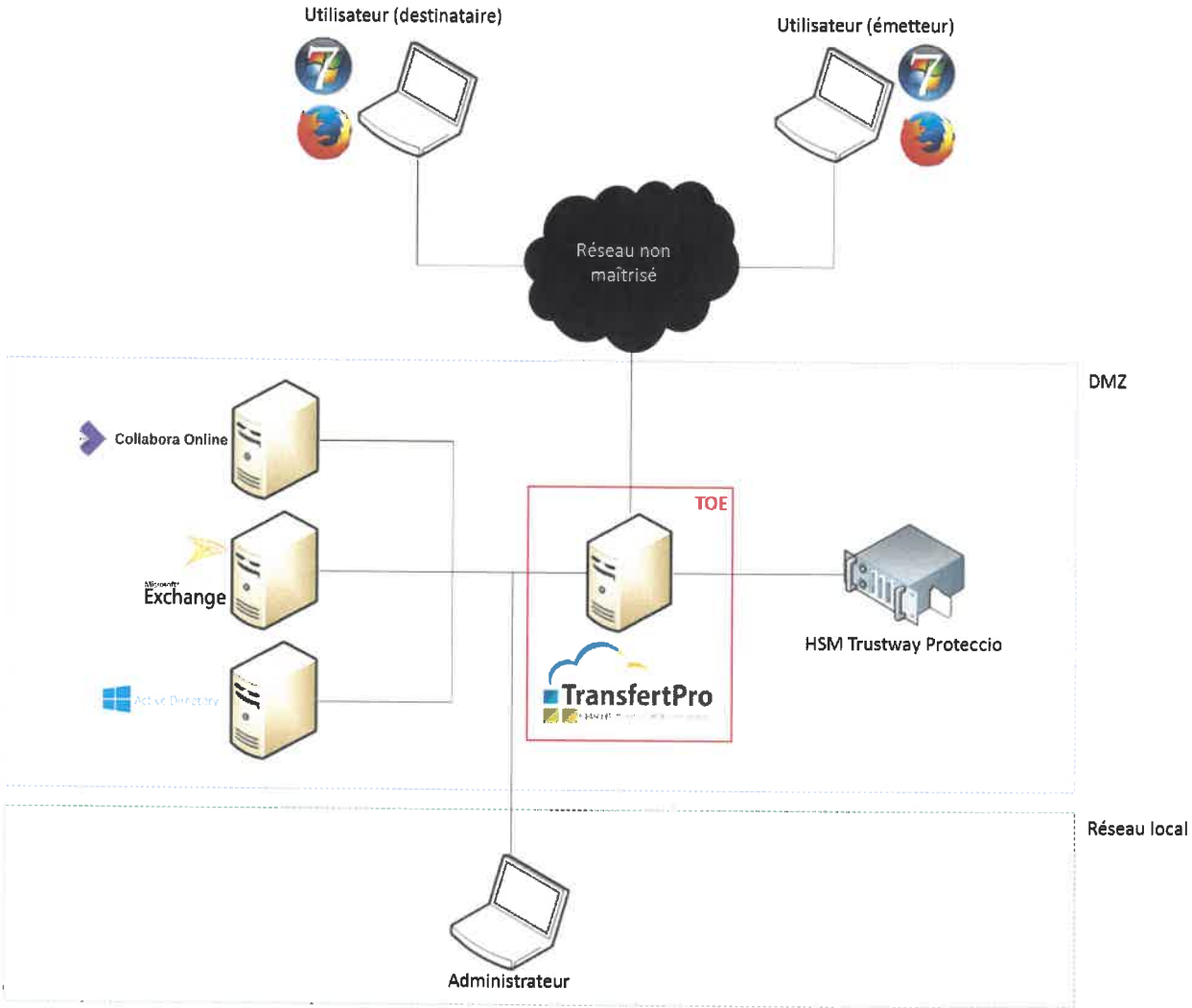

Figure 1 : Plateforme d'évaluation

Les liens avec les smartphones (application et notifications « push » via l'utilisation d'un serveur Parse) ne font pas partie de l'évaluation. De même, la machine physique et le système d'exploitation où sont installés les serveurs de la solution, le serveur de messagerie ainsi que le HSM Trustway Proteccio et les services tiers (accès aux services InWebo et UniversSign), sont en dehors du périmètre de l'évaluation.

Le serveur de messagerie Microsoft Exchange ainsi que l'Active Directory sont installés sur un poste Windows Server 2012 R2.

Le serveur TransfertPro ainsi que le boîtier HSM, les serveurs Collabora Online, Exchange et Active Directory sont installés dans une DMZ (protégée selon les règles de l'état de l'art). L'administration des serveurs se fait à partir d'un réseau local dédié.

Un poste Windows 7 est choisi pour la machine de l'émetteur et du destinataire sur lequel est installé le navigateur Web Mozilla Firefox (utilisé comme client) version 44 au minimum. Le poste utilisé par les administrateurs est un PC Windows 7.

3. PROBLÉMATIQUE DE SÉCURITÉ

3.1. DESCRIPTION DES UTILISATEURS TYPIQUES

Par définition, les utilisateurs concernent les personnes et services applicatifs qui interagissent avec le produit évalué.

Les rôles suivants doivent être pris en considération dans le cadre de l'évaluation de sécurité :

- ***Utilisateur principal :*** personne disposant d'un compte *TransfertPro* et effectuant des opérations d'envoi ou de réception d'un fichier.
- ***Utilisateur tiers :*** personne disposant seulement d'un compte *TransfertPro* gratuit créé lorsqu'elle est destinatrice d'un fichier par envoi TransfertPro en provenance d'une personne détenant le rôle « Utilisateur principal ».
- ***Externe :*** personne dite « 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 ».
- ***Administrateur TOE :*** personne en charge d'administrer la solution *TransfertPro* (accès aux mécanismes de journalisation des opérations, de gestion des utilisateurs, de configuration de la solution).
- ***Administrateur système :*** personne en charge d'administrer le système support sur lequel est installée la solution *TransfertPro*.

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.

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 suivants :

- **B.Données d'identification et d'authentification**

  Ce bien concerne les données relatives à la connexion des utilisateurs permettant l'accès à un compte *TransfertPro*.

  Besoin de sécurité : confidentialité.

- **B.Données utilisateur**

  Ce bien concerne les données métiers (*ie* les fichiers) qui sont stockées chiffrées sur le serveur *TransfertPro*.

  Besoin de sécurité : intégrité, confidentialité.

- **B.Données de journalisation**

  Ce bien concerne les évènements relatifs aux fichiers et aux dossiers que les utilisateurs stockent dans leur espace *TransfertPro*.

  Besoin de sécurité : intégrité.

- **B.Éléments secrets**

  Ce bien concerne les clés cryptographiques utilisées pour assurer la protection des fichiers (ces clés sont chiffrées par une clé disponible dans le boîtier HSM Trustway Proteccio et stockées chiffrées sur le serveur *TransfertPro*).

  Besoin de sécurité : intégrité, confidentialité.

- **B.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*).

  Besoin de sécurité : intégrité.

3.3. DESCRIPTION DES HYPOTHÈSES 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 suivantes doivent être considérées :

- **H1.Administrateurs**

  Les administrateurs système 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 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.

  Les composants du serveur *TranfertPro* (serveur web, serveur de fichiers, serveur SQL) sont correctement configurés et administrés (permissions, services, protocoles et algorithmes à l'état de l'art, etc.).

  L'administration à distance est désactivée par défaut (pour le profil « host »).

- **H2.Environnement sécurisé**

  Le serveur *TranfertPro* 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.

  Les serveurs de la solution *TranfertPro* sont installés au sein d'une DMZ (protégée selon les règles de l'état de l'art et réputée de confiance). En particulier, des moyens techniques sont mis en place en entrée de la DMZ (pare-feu, anti-DDOS, etc.).

  Les serveurs de la solution *TranfertPro* sont déployés dans un local dont les accès sont nominativement contrôlés.

- **H3.Environnement clients**

  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.

- **H4.Services tiers**

  Les connexions réalisées par le serveur *TransfertPro* sur les services tiers (InWebo, UniversSign) sont désactivées. Les connexions réalisées par le serveur *TransfertPro* sur le boitier HSM sont sécurisées selon les règles de l'état de l'art. Seul le serveur *TransfertPro* accède au HSM (physiquement relié au serveur par liaison filaire) dont l'administration est effectuée en local.

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.

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 ;
- un utilisateur légitime (muni d'un compte *TransfertPro*) qui souhaite contourner certaines restrictions d'accès.

Les administrateurs ne sont pas considérés comme des attaquants.

Les attaquants peuvent être situés sur le réseau non maîtrisé, la DMZ ou le réseau local d'où est opérée l'administration de la solution *TransfertPro*.

Les menaces qui portent sur les biens sensibles de la TOE sont les suivantes :

- **M1.Vol des données d'authentification**

  Un attaquant arrive à récupérer les données d'identification et/ou d'authentification d'un utilisateur muni d'un compte *TransfertPro*.

- **M2.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.

- **M3.Altération des données utilisateurs**

  Un attaquant parvient à modifier les données utilisateurs à l'insu de l'utilisateur légitime.

- **M4.Altération des données de journalisation**

  Un attaquant parvient à modifier les données de journalisation afin de masquer des actions illégitimes.

- **M5.Altération des éléments secrets**

  Un attaquant parvient à modifier les clés cryptographiques utilisées pour le chiffrement des fichiers.

- **M6.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.

3.5. DESCRIPTION DES 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 suivantes :

- **F1.Identification et Authentification**

  L'accès aux fonctionnalités du produit (compte *TransfertPro*) est protégé par un système d'authentification avec utilisation d'un serveur Active Directory.

- **F2.Protection des données utilisateurs**

  Le produit protège en confidentialité et en intégrité les données de l'utilisateur par un mécanisme de chiffrement robuste et non prédictible (utilisation de l'algorithme AES 256 en mode CBC avec un clé utilisée dérivée par la fonction PBKDF2 à partir du mot de passe échangé entre les utilisateurs ainsi qu'un vecteur d'initialisation généré aléatoirement) et de contrôle d'intégrité (fonction de hachage HMAC-SHA256).

  Les fichiers temporaires téléchargés sont supprimés systématiquement : soit à la fin du processus de chiffrement, soit (si le traitement est interrompu, par exemple, suite à une perte de connexion lors d'un envoi d'un fichier volumineux) par un batch de nettoyage.

- **F3.Communications sécurisées**

  Le flux entre les applications clientes (navigateur Web) et le serveur *TransfertPro* sont protégés en intégrité et confidentialité (TLS v1.2).

- **F4.Intégrité des données de fonctionnement**

  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) ainsi que des données de configuration.

- **F5.Protection des éléments secrets**

  Le produit assure la protection en confidentialité et intégrité des clés utilisées lors des opérations de chiffrement et de déchiffrement des fichiers en les chiffrant, au moyen d'une clé de société stockée sur le HSM, avant leur stockage en base de données.

3.6. MATRICES DE COUVERTURES

3.6.1. 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) :

	B.Données d'identification et d'authentification	B.Données utilisateur	Données de journalisation	B.Éléments secrets	B.Données de configuration
M1.Vol des données d'authentification	C				
M2.Accès illégitime aux données		C		C	
M3.Altération des données utilisateurs		I			
M4.Altération des données de journalisation			I		
M5.Altération des éléments secrets				I	
M6.Altération des données de configuration					I

Tableau 1 - Couverture des biens sensibles par les menaces

3.6.2. Menaces et fonctions de sécurité

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

	F1.Identification et Authentification	F2.Protection des données utilisateurs	F3. Communications Sécurisées	F4.Intégrité des données de fonctionnement	F5.Protection des éléments secrets
M1.Vol des données d'authentification	√		√		
M2.Accès illégitime aux données	√	√	√		
M3.Altération des données utilisateurs		√	√		
M4.Altération des données de journalisation				√	
M5.Altération des éléments secrets					√
M6.Altération des données de configuration				√	

Tableau 2 - Couverture des menaces par les fonctions de sécurité

Fin du document