AMOSSYS

MFT

Cible de sécurité CSPN

Produit MFT *On Premise* version 3.4

Catégorie « stockage sécurisé »

Référence : CSPN-ST-MFT-1.05

Date : le 10/07/2020

Code interne : EQS001-2

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'ÉVOLUTIONS

Révision	Date	Description	Rédacteur(s)
1.00	01/07/2019	Création du document	A. DELOUP
1.01	04/07/2019	Ajout d'une précision sur les COTS	A. DELOUP
1.02	17/07/2019	Ajout de précisions	M. MOREAU
1.03	04/10/2019	Finalisation	A. DELOUP EQUISIGN
1.04	12/12/2019	Mise à jour de la version du produit en 3.4	A. DELOUP
1.05	10/07/2020	Précisions pour réévaluation du produit	M. VOGT

Ce document a été validé par Equisign.

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], du produit « MFT» développé par la société **Equisign**.

La TOE[3] considérée est la solution MFT, configuré en niveau de protection 2 (chiffrement par HSM)

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

1.2. IDENTIFICATION DU PRODUIT

Éditeur	**Equisign** 76 route de la Demi-Lune 92057 Paris La Défense
Lien vers l'organisation	https://www.opentrustmft.fr
Nom commercial du produit	MFT *On Premise*
Numéro de la version évaluée	3.4
Catégorie du produit	Stockage Sécurisé

1.3. RÉFÉRENCES

Pour l'établissement de la présente cible de sécurité, les documents suivants ont été consultés par le rédacteur :

- « Présentation MFT» ;
- « MFT_End_User_Guide.pdf » ;
- « release-notes.pdf ».

[1] Certification de Sécurité de Premier Niveau
[2] Agence Nationale de la Sécurité des Systèmes d'Information
[3] *Target Of Evaluation*

2. DESCRIPTION DU PRODUIT

2.1. DESCRIPTION GÉNÉRALE

MFT (*Managed File Transfer*) est une solution de transfert de fichiers chiffrés en gros volume à destination des entreprises. Le produit se présente comme une alternative à des solutions grand public, comme WeTransfer, Dropbox ou Google Drive.

La solution dispose d'une interface intuitive qui permet à chaque utilisateur de déposer ses fichiers à destination d'une ou plusieurs personnes ou d'un groupe, en indiquant une durée durant laquelle les fichiers seront accessibles aux destinataires. L'utilisateur a ensuite la possibilité de suivre ou de rechercher des messages. Les fichiers transférés sur MFT peuvent l'être avec des utilisateurs inscrits dans MFT, de l'entreprise ou non, ou avec des contacts ponctuels externes. Aucune restriction de taille ne s'applique aux fichiers téléversés sur la plateforme. Des notifications sont également disponibles pour alerter chaque utilisateur de la réception d'un fichier. La solution MFT permet également une traçabilité complète des échanges de fichiers (envoi et réception, hachage des fichiers, horodatage, etc.)

Enfin, les fichiers peuvent être partagés par des utilisateurs physiques (cas classique de l'envoi d'un fichier par Alice à Bob), ou par des systèmes automatisés logiciels (par exemple, partage automatique d'une facture par un applicatif de paiement).

Le produit est disponible dans plusieurs offres : Cloud public, Cloud privé, ou *On Premise*.

2.2. PRINCIPE DE FONCTIONNEMENT

Les utilisateurs ont la possibilité d'uploader leurs fichiers sur MFT au travers d'une interface Web. Dans celle-ci, ils peuvent définir un sujet et un message qui seront échangés par email avec le lien de téléchargement du fichier. Ils doivent également définir la liste des destinataires qui seront autorisés à accéder aux fichiers. Ces destinataires peuvent être internes à l'entité, ou externes. Enfin, l'expéditeur peut définir un mot de passe de chiffrement symétrique utilisé pour chiffrer les fichiers (voir précisions ci-après).

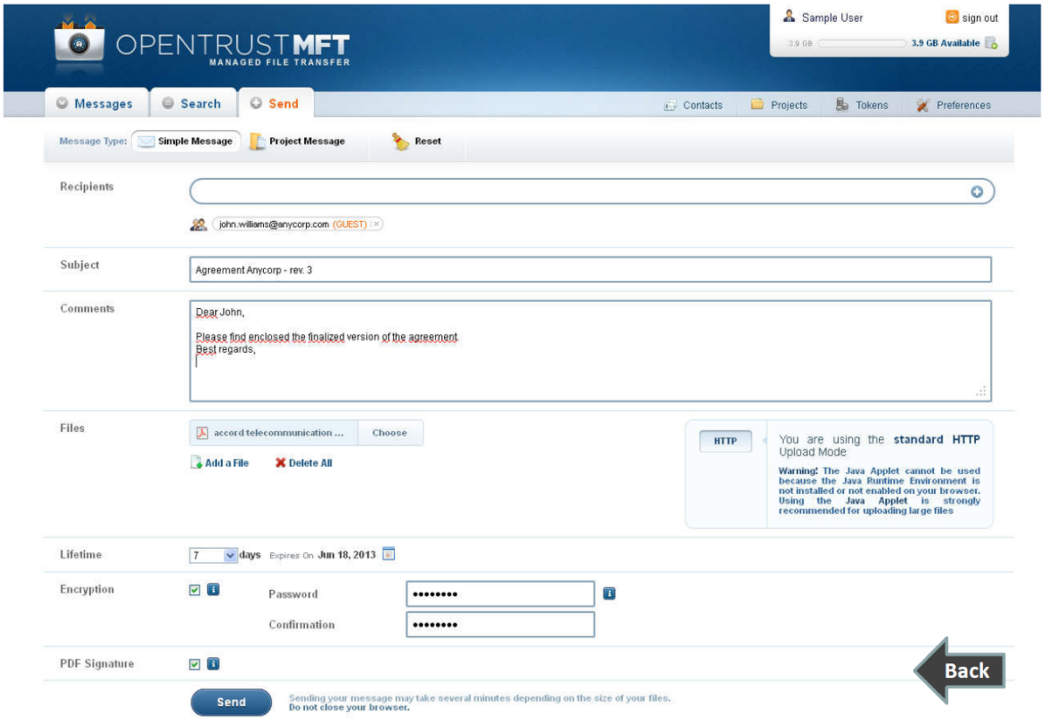

Figure 1 - Envoi d'un fichier par MFT

Les utilisateurs peuvent être des utilisateurs internes ou externes de l'entreprise et qui disposent d'un accès à MFT. Dans ce cas, ils peuvent déposer des fichiers, les partager avec toute personne (disposant ou non d'un compte sur la solution) et les administrateurs peuvent leur appliquer des politiques de sécurité (politique d'envoi (ce qu'il est possible envoyer), politique d'échange (à qui il est possible d'envoyer), politique d'authentification (règle d'authentification)), avec une segmentation par Domaine MFT. Par exemple, les utilisateurs d'un domaine A ne pourront envoyer des fichiers PDF qu'aux utilisateurs du domaine B, et pas aux invités. Les utilisateurs peuvent également être des utilisateurs externes à l'entreprise (par exemple, des prestataires). Ceux-ci disposent également d'un compte sur la plateforme, et l'administrateur peut leur appliquer des politiques restrictives (par exemple, possibilité de n'échanger des fichiers qu'avec les utilisateurs membres d'un groupe particulier sur la solution).

Enfin, les utilisateurs de la solution ne disposant pas de compte sont des invités et n'ont pas, par défaut, la possibilité de déposer des fichiers. Ils peuvent simplement accéder aux fichiers qui leur ont été partagés. Les utilisateurs inscrits sur la plateforme peuvent cependant leur envoyer, au travers de MFT, un « token », qui leur permet ensuite de déposer un fichier pendant un laps de temps donné (par exemple, pour déposer un contrat signé) à destination de l'émetteur du token.

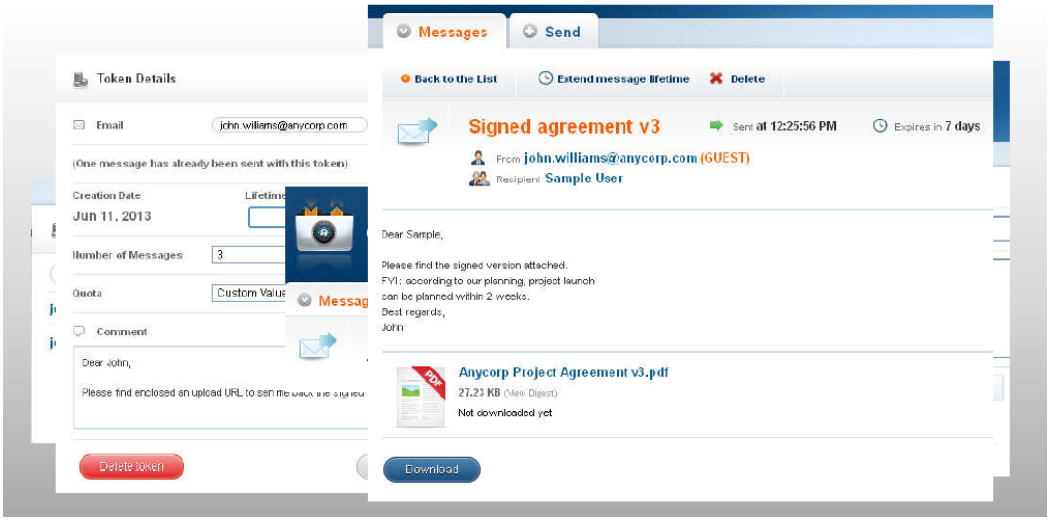

Figure 2 - Partage de fichier par « token »

Plusieurs modes de protection sont disponibles sur le serveur MFT. Ces modes peuvent être activés par configuration d'un administrateur sur le serveur :

- Niveau 0 (par défaut) : les fichiers sont anonymisés avant d'être stockés sur le serveur (le nom du fichier sur le disque est remplacé par un identifiant unique, stocké dans la base de données) ;
- Niveau 1 : les fichiers sont chiffrés en AES-256 avant d'être stockés sur le serveur. La clé de chiffrement est propre à chaque fichier, et est générée aléatoirement pour l'occasion.
- Niveau 2 : les fichiers sont chiffrés en AES-256 en utilisant une clé aléatoire et unique. Cette clé est stockée en base de données après chiffrement par une clé AES-256 stockée dans le HSM (*Hardware Security Module*) du serveur.

Un mode de chiffrement supplémentaire est disponible à la discrétion de l'utilisateur qui uploade les fichiers. Ceux-ci sont alors encapsulés dans une archive 7-zip chiffrée en AES-256. Dans ce cas, l'utilisateur défini le mot de passe utilisé dans l'interface Web du serveur, au moment où il dépose les fichiers. Celui-ci doit également être renseigné par les destinataires lors de l'accès aux fichiers. Le chiffrement est réalisé par le serveur lors de l'envoi des fichiers, et la clé n'est pas conservée sur le serveur.

La plateforme complète est composée de plusieurs serveurs (physiques ou virtualisés) :

- Un ou plusieurs serveurs Apache servant uniquement de Reverse-Proxy « External/Internal MFT Web », peuvent être placés en DMZ ou en zone serveur interne ; Un ou plusieurs serveurs applicatifs, supports d'un serveur Tomcat, sur lesquels les utilisateurs se connectent via le reverse-Proxy Apache, pour déposer ou accéder à des fichiers ;
- Un serveur « MFT-Admin », qui peut être installé sur un des serveurs applicatifs, sur lequel sont démarrés :
    - L'applicatif principal de MFT, en charge du contrôle d'accès et de la gestion des fichiers ;
    - Le module de journalisation ;
- Un serveur de base de données, qui stocke les données de la TOE ;
- Un relai SMTP pour l'envoi des emails de notification ;
- Un système de stockage des fichiers ;

- Une fédération d'identités pour la gestion des droits d'accès (MFT utilise le protocole SAML) ;
- MFT pourra également être connecté à un annuaire Active Directory ou LDAP, pour la gestion des utilisateurs internes (provisioning, mots de passe, etc.). Les utilisateurs externes sont nécessairement gérés par l'application depuis l'interface administrateur.

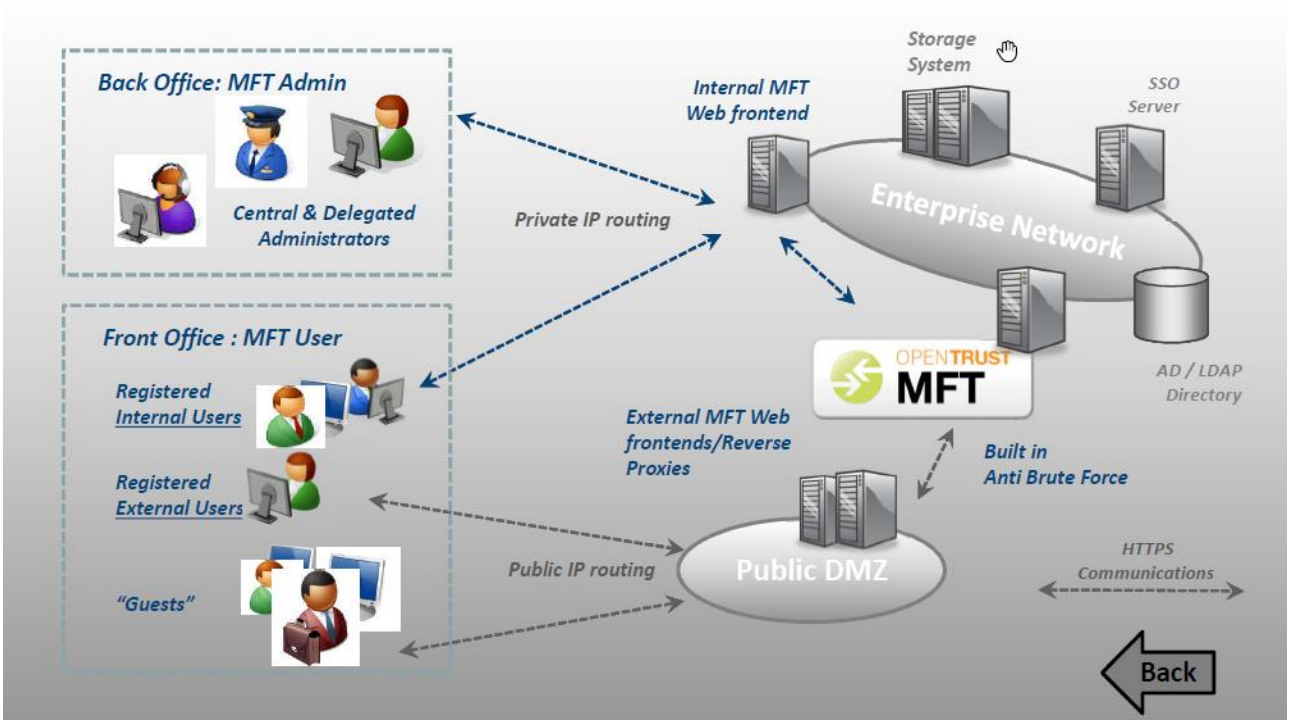

Figure 3 - Schéma d'architecture de la plateforme MFT

2.3. DESCRIPTION DES DÉPENDANCES

Le produit est *standalone* et n'a pas de dépendance externe.

Néanmoins, pour fonctionner il requiert les éléments suivants :

- Apache (version 2.4.6), pour l'interface Web accessible aux utilisateurs ;
- Tomcat (version 7.0.76), pour l'applicatif du serveur ;
- PostgreSQL (version 9.2.24), pour le stockage des données ;
- 7-zip (version 16.02), pour l'encapsulation des fichiers chiffrés sur demande de l'utilisateur.

Ces COTS sont installés sur une base RedHat 7, ce qui induit que les dépendances, bien qu'anciennes, sont toujours maintenues en conditions de sécurité par RedHat, qui applique des patchs de sécurité nécessaires[4].

2.4. DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

2.4.1. Matériel compatible ou dédié

La plateforme nécessite 4 serveurs pour faire fonctionner les différentes briques de la solution :

[4] https://access.redhat.com/security/updates/backporting

- Le serveur *Frontend* ;
- Le serveur *Backend* (applicatif MFT) ;
- Un système de stockage des fichiers (serveur NAS ou dérivé) ;
- Un serveur de base de données ;
- Un serveur SMTP pour l'envoi des emails de notification.

Un HSM est nécessaire pour utiliser le niveau 2 de chiffrement des fichiers (voir §2.2, page 7).

Les serveurs nécessitent le système d'exploitation CentOS 7 ou RedHat 7.

2.4.2. Système d'exploitation retenu

Les systèmes d'exploitation suivants ont été retenus pour l'évaluation :

- Serveurs : CentOS 7 ;
- Poste client : Windows 10.

2.5. PÉRIMÈTRE DE L'ÉVALUATION

2.5.1. Périmètre

L'évaluation porte sur la plateforme MFT, installé en mode de protection « Niveau 2 », dans lequel tous les fichiers sont chiffrés avec un HSM tiers (bien que le choix du HSM soit laissé libre, l'éditeur recommande Trustway Proteccio NetHSM[5] ou le HSM logiciel SoftHSM[6]).

Seuls les serveurs spécifiques à MFT, et les communications réseaux (entre les composants des serveurs MFT, et entre les serveurs MFT et les navigateurs Web des utilisateurs) sont considérés dans le périmètre de l'évaluation. Les serveurs de mail, AD et HSM, et le navigateur Web du client, sont considérés hors périmètre.

2.5.2. Plateforme d'évaluation

La plateforme d'évaluation sera composée de 3 serveurs et un NAS :

- MFT-FRONT_WEB1, pour héberger le serveur frontal utilisateurs ;
- MFT-ADMIN_USER1, pour héberger les rôles suivants :
  - Serveur frontal administrateurs ;
  - Serveur d'Application administrateurs ;
  - Serveur d'Application Utilisateurs ;
  - Module de journaux d'audit
- MFT-BDD, pour héberger les données de la TOE ;
- Serveur NAS, pour le stockage des fichiers.

Les utilisateurs se connecteront à la plateforme depuis des navigateurs Mozilla Firefox (en dernière version), sur des postes Windows 10. L'administrateur utilisera un poste dédié à cet usage. Les flux réseaux entre les composants de la plateforme et les navigateurs Web font également partie du périmètre de la TOE.

[5] https://atos.net/fr/produits/cybersecurite/chiffrement-donnees/hsm-trustway-proteccio-nethsm
[6] https://www.opendnssec.org/softhsm/

Les utilisateurs internes seront intégrés à la plateforme au travers d'un annuaire Active Directory, porté par un serveur Windows Server 2016. Ce serveur sera aussi support d'un serveur mail Exchange pour l'envoi des emails de la TOE et support d'un serveur NTP. Les utilisateurs externes sont gérés directement par le serveur MFT. Les invités utilisent le mode « jeton » (voir page 6).

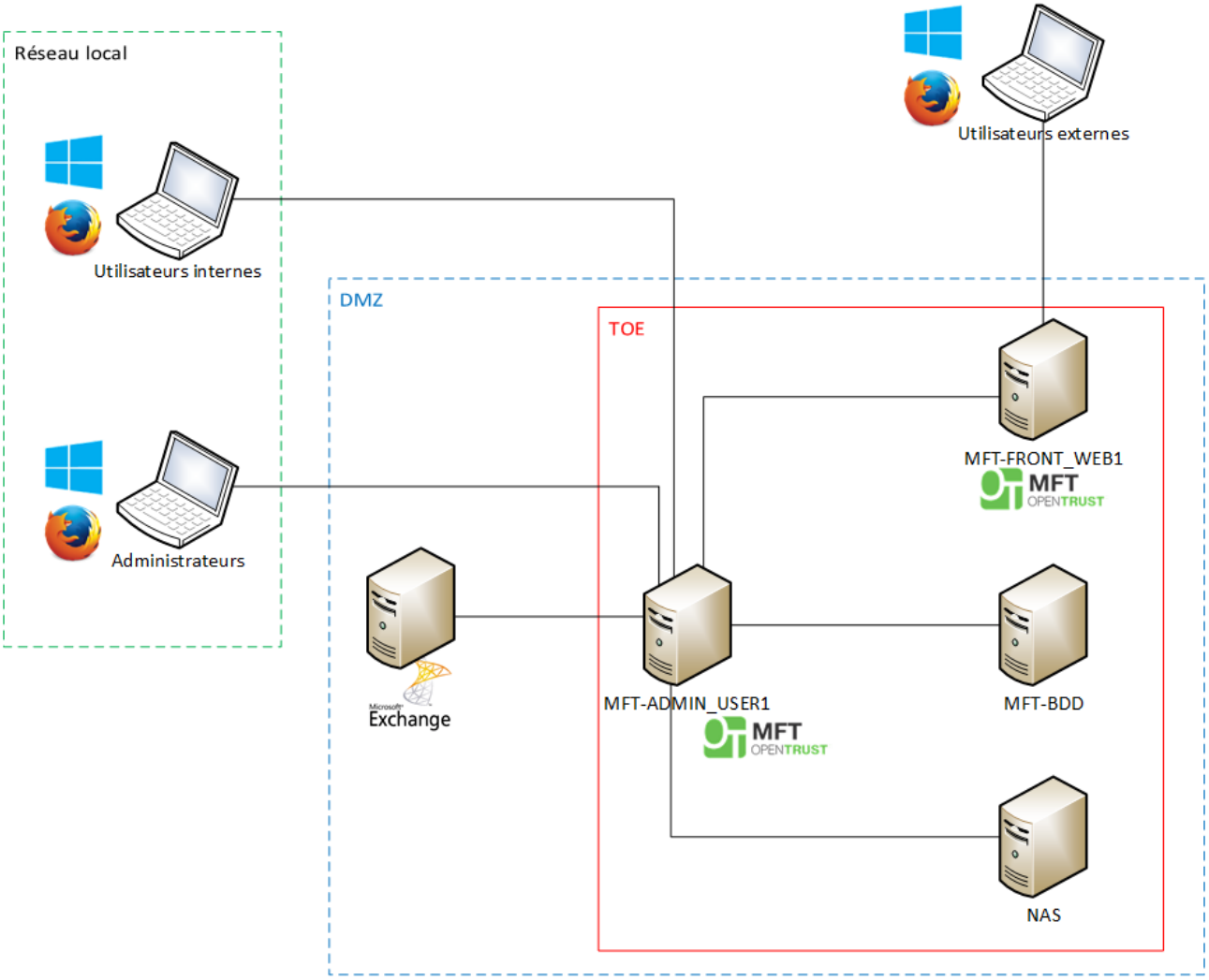

Figure 4 - Schéma de l'architecture utilisée pour l'évaluation

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 interne :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant des droits suffisants pour échanger des fichiers avec tout utilisateur (avec ou sans compte) ;
- ***Utilisateur externe :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant de droits restreints ne lui permettant d'échanger des fichiers qu'avec les utilisateurs internes ;
- ***Invité :*** utilisateur de la solution ne disposant pas de compte utilisateur. Il peut accéder aux fichiers qui lui ont été partagés par des utilisateurs internes, et déposer des fichiers s'il dispose d'un *token* ;
- ***Administrateur :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant de droits privilégiés lui permettant d'administrer la solution ;
- ***Auditeur :*** utilisateur de la solution, disposant d'un compte utilisateur, et disposant de droits privilégiés lui permettant d'accéder aux journaux de la solution. Il ne dispose pas de droits pour administrer la solution ;
- ***Administrateur système :*** personne en charge d'administrer le système support sur lequel est installée la solution MFT.

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 :

- **B1.FICHIERS ECHANGES**

  MFT doit protéger les fichiers échangés par ses utilisateurs.

  Besoin de sécurité : intégrité et confidentialité.

- **B2.MATERIEL CRYPTOGRAPHIQUE**

  Les clés cryptographiques utilisées pour chiffrer les fichiers partagés, et les communications réseau.

  Besoin de sécurité : intégrité et confidentialité.

- **B3.JOURNAUX**

  Les évènements générés lors des processus d'authentification, de partage de fichiers, d'accès à un partage, ou de déchiffrement, sont journalisés. Ces données ne sont accessibles que par les auditeurs ou les administrateurs après s'être authentifiés.

  Besoin de sécurité : intégrité.

- **B4.CONFIGURATION**

  Les données utiles pour assurer le fonctionnement de la TOE (fichiers de configuration des serveurs Web, de fichiers et SQL du serveur *MFT*).

  Besoin de sécurité : intégrité.

- **B5.FLUX RÉSEAU**

  Les flux réseau de la TOE entre les postes clients et le serveur doivent être protégés.

  Besoin de sécurité : intégrité et confidentialité.

- **B6.DONNÉES D'AUTHENTIFICATION**

  Les données relatives à la connexion des utilisateurs permettant l'accès à un compte MFT.

  Besoin de sécurité : confidentialité.

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.

  Les administrateurs de la TOE (serveur *MFT*) sont considérés de confiance et formés à l'utilisation et à l'administration de la TOE.

  Les auditeurs sont considérés de confiance et formés à l'utilisation de la TOE.

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

- **H2.Environnement sécurisé**

  Le serveur MFT 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 *frontend* de la solution MFT 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 MFT 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 MFT sur le boitier HSM sont sécurisées selon les règles de l'état de l'art. Seul le serveur MFT accède au HSM (physiquement relié au serveur) 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 MFT, ou non (invité)) qui souhaite contourner certaines restrictions d'accès.

Les administrateurs ne sont pas considérés comme des attaquants.

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 MFT.

- **M2.ACCÈS ILLÉGITIME AUX DONNÉES**

  Un attaquant parvient à accéder aux fichiers chiffrés d'un utilisateur, stockés sur le serveur MFT 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 MFT 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 MFT) est protégé par un système d'authentification des utilisateurs internes avec utilisation d'un serveur Active Directory tiers. Les utilisateurs externes sont gérés par un serveur d'authentification interne à la TOE. Enfin, les invités sont authentifiés par un jeton unique.

- **F2.PROTECTION DES DONNÉES UTILISATEURS**

  Le produit protège en confidentialité et en intégrité les données de l'utilisateur de deux façons :

  - Par défaut, dans le mode de protection de niveau 2, par un mécanisme de chiffrement robuste et non prédictible (utilisation de l'algorithme AES-256 en mode CBC avec une clé de 256 bits dérivée via PBKDF2 d'une autre clé générée aléatoirement par le serveur à l'aide de la classe `SecureRandom` du JDK).
  - Si l'expéditeur choisit l'encapsulation des fichiers échangés, ceux-ci sont chiffrés en AES-256 dans une archive 7-zip, avec un mot de passe défini par l'utilisateur.

  Dans les deux cas, le chiffrement est réalisé par le serveur MFT. Les fichiers temporaires téléchargés sont supprimés systématiquement à la fin du processus de chiffrement. Aucun contrôle d'intégrité n'est effectué. Les empreintes SHA-256 des fichiers sont stockées et affichées lors de la réception. C'est à la charge du destinataire de vérifier l'intégrité.

- **F3.COMMUNICATIONS SÉCURISÉES**

  Le flux entre les navigateurs Web des clients et le serveur MFT sont protégés en intégrité et confidentialité (TLS v1.2).

- **F4.PROTECTION DES ÉLÉMENTS SECRETS**

  Le produit assure la protection en confidentialité et intégrité d'une clé nécessaire au chiffrement du niveau 2 en utilisant un HSM pour la stocker.

- **F5.PROTECTION DES JOURNAUX**

  Le produit assure la protection des journaux en les protégeant par un mécanisme de signature et chaînage. Le chaînage est effectué en ajoutant le haché des journaux précédents aux journaux à chaîner. La signature s'effectue via XMLSig.

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) :

	B1.FICHIERS ECHANGES	B2.MATERIEL CRYPTOGRAPHIQUE	B3.JOURNAUX	B4.CONFIGURATION	B5.FLUX RÉSEAU	B6.DONNÉES D'AUTHENTIFICATION
M1.VOL DES DONNÉES D'AUTHENTIFICATION					**C**	**C**
M2.ACCÈS ILLÉGITIME AUX DONNÉES	**C**				**C**	
M3.ALTÉRATION DES DONNÉES UTILISATEURS	**I**				**I**	
M4.ALTÉRATION DES DONNÉES DE JOURNALISATION			**I**			
M5.ALTÉRATION DES ÉLÉMENTS SECRETS		**IC**				**IC**
M6.ALTÉRATION DES DONNÉES DE CONFIGURATION				**C**		

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.PROTECTION DES ÉLÉMENTS SECRETS	F5.PROTECTION DES JOURNAUX
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