PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2020/34

MFT On Premise

Version 3.4.0.1 (release number : af42dac)

Paris, le 2 octobre 2020

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

Guillaume POUPARD

[ORIGINAL SIGNE]

SÉCURITÉ Ti CERTIFICATION

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2020/34**
Nom du produit **MFT On Premise**
Référence/version du produit **Version 3.4.0.1 (release number : af42dac)**
Catégorie de produit **Stockage sécurisé**
Critère d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Equisign** 76 route de la Demi-Lune 92057 Paris La Défense
Développeur **Equisign** 76 route de la Demi-Lune 92057 Paris La Défense
Centre d'évaluation **AMOSSYS** 11 rue Maurice Fabre 35000 Rennes, France
Fonctions de sécurité évaluées Identification et l'authentification des utilisateurs Protection des données utilisateurs Protection des communications Protection des éléments secrets Protection des journaux
Fonctions de sécurité non évaluées Néant
Restriction(s) d'usage Non

PREFACE

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification CSPN sont disponibles sur le site Internet www.ssi.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « MFT On Premise, Version 3.4.0.1 (release number : af42dac) » développé par *EQUISIGN*.

Managed File Transfer (MFT) est une solution de transfert de fichiers chiffrés en gros volume à destination des entreprises. La solution dispose d'une interface permettant à chaque utilisateur de déposer ses fichiers à destination d'une ou plusieurs personnes ou d'un groupe défini, en indiquant une durée de temps durant laquelle les fichiers seront accessibles aux destinataires.

La solution est également utilisable par des utilisateurs ne disposant pas de comptes. Ils sont alors des invités (*guests*) et peuvent simplement accéder aux fichiers qui leur ont été partagés ou alors déposer des fichiers après qu'un utilisateur leur ait au préalable fourni un « *token* ».

Le produit est disponible dans plusieurs offres : Cloud public, Cloud privé, ou *On Premise*. Le présent certificat n'est valable que pour la version *On Premise*.

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

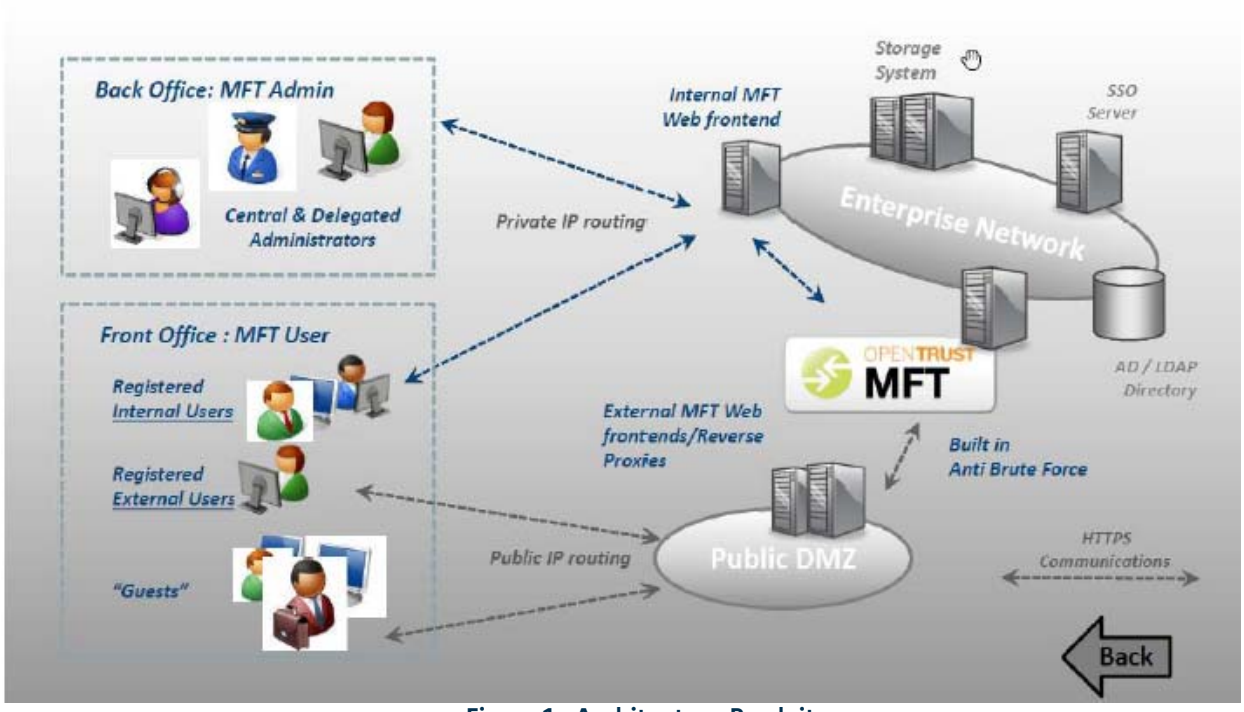

Figure 1 - Architecture Produit.

1.2 Description du produit évalué

La cible de sécurité [CDS] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

1.2.1 *Catégorie du produit*

☐	1	détection d'intrusions
☐	2	anti-virus, protection contre les codes malicieux
☐	3	pare-feu
☐	4	effacement de données
☐	5	administration et supervision de la sécurité
☐	6	identification, authentification et contrôle d'accès
☐	7	communication sécurisée
☐	8	messagerie sécurisée
☒	**9**	**stockage sécurisé**
☐	10	environnement d'exécution sécurisé
☐	11	terminal de réception numérique (*Set top box*, STB)
☐	12	matériel et logiciel embarqué
☐	13	automate programmable industriel
☐	99	autre

1.2.2 *Identification du produit*

Produit	
Nom du produit	MFT On Premise
Numéro de la version évaluée	Version 3.4.0.1 (release number : af42dac)

La version certifiée du produit peut être identifiée de la manière suivante :

- par un utilisateur connecté, via le menu Preferences > About OpenTrust MFT (voir Figure 2) ;
- par un administrateur, via l'interface d'administration en cliquant sur le logo « OpenTrust MFT » (voir Figure 3).

Figure 2 - Fenêtre "About OpenTrust MFT" pour un utilisateur connecté

Figure 3 - Fenêtre "A propos de OpenTrust MFT" pour un administrateur

1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- l'identification et l'authentification des utilisateurs ;
- la protection en confidentialité et en intégrité des données utilisateurs ;
- la protection en intégrité et confidentialité des communications ;
- la protection en confidentialité et intégrité des éléments secrets ;
- la protection en intégrité des journaux.

1.2.4 *Configuration évaluée*

Le schéma suivant détaille l'architecture déployée par le CESTI, en utilisant les guides d'administration du développeur ([GUIDES]).

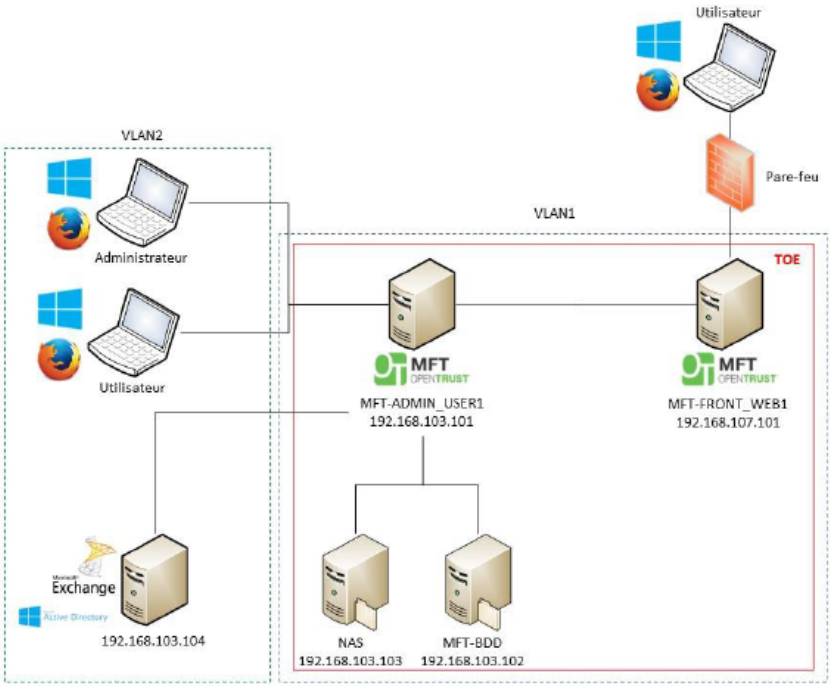

Figure 4 - Architecture de la plateforme de test

La plateforme de test est constituée des éléments suivants :

- un serveur d'administration (ici MFT-ADMIN_USER1) :
  - OS : CentOS 7.7,
  - VLAN : VLAN1,
  - services : Apache 2.4.6, Tomcat 7.0.76 et SoftHSM 2.4.1[1] ;

- un serveur frontal (ici MFT-FRONT_WEB1) :
  - OS : CentOS 7.7,
  - VLAN : VLAN1,
  - service Apache 2.4.6 ;

- un serveur de base de données (ici MFT-BDD) :
  - OS : CentOS 7.7,
  - VLAN : VLAN1,
  - service : PostgreSQL 9.2.24 ;

[1] Ce service est installé pour émuler un HSM matériel.

- un serveur de stockage (ici NAS) :
    - VLAN : VLAN1,
    - disque dur monté sur le serveur d'administration via fstab ;

- un serveur Active Directory/Exchange :
    - OS : Windows Server 2016,
    - VLAN : VLAN2
    - services : Active Directory et Exchange 2016.

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 B.

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 est à faire en suivant les guides d'installation du développeur (voir [GUIDES]).

2.3.1.3 Durée de l'installation

L'installation du produit en lui-même est rapide. La mise en place de toute la plateforme décrite en section 1.2.4 est plus longue. Le temps total a été de deux jours.

2.3.1.4 Notes et remarques diverses

Sans objet.

2.3.2 *Analyse de la documentation*

Les guides du produit permettent d'installer et d'utiliser le produit sans causer de dégradation accidentelle de la sécurité.

2.3.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source du produit. L'analyse a été effectuée manuellement ainsi qu'avec l'outil *checksec*.

Cette analyse a contribué à l'analyse de conformité et de résistance des fonctions de sécurité du produit.

2.3.4 *Analyse de la conformité des fonctions de sécurité*

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

2.3.5 *Analyse de la résistance des mécanismes des fonctions de sécurité*

Toutes les fonctions de sécurité ont subi des tests de pénétration et aucune ne présente de vulnérabilité exploitable dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé.

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

2.3.6.1 Liste des vulnérabilités connues

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

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

Des vulnérabilités potentielles ont été identifiées, mais se sont révélées inexploitables pour les vulnérabilités résiduelles pour le niveau d'attaquant considéré.

2.3.7 *Accès aux développeurs*

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

2.3.8 *Analyse de la facilité d'emploi*

2.3.8.1 Cas où la sécurité est remise en cause

L'évaluateur n'a pas identifié de cas où la sécurité de la TOE est remise en cause.

2.3.8.2 Avis d'expert sur la facilité d'emploi

Le produit est globalement bien documenté, et sa mise en œuvre ne présente pas de difficulté pour un administrateur familier des environnements décris en section 1.2.4.

Il n'a pas été identifié de moyen par lequel l'utilisateur risque de remettre en cause la sécurité du produit.

2.3.8.3 Notes et remarques diverses

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

2.4 Analyse de la résistance des mécanismes cryptographiques

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

2.5 Analyse du générateur d'aléas

Le produit utilise le générateur d'aléas fourni par l'environnement Java. Cependant l'analyse n'a pas identifié de non-conformité au RGS (voir [RGS]) ni 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 « MFT On Premise, Version 3.4.0.1 (release number : af42dac) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS] pour le niveau d'évaluation attendu lors d'une certification de sécurité de premier niveau.

3.2 Recommandations et restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS] ainsi que les conditions de déploiement prévues dans les [GUIDES].

ANNEXE A. Références documentaires du produit évalué

[CDS]	Cible de sécurité CSPN Produit MFT On Premise version 3.4 Référence : CSPN-ST-MFT-1.05 ; Version : 1.05 ; Date : 10 juillet 2020.
[RTE]	Rapport Technique d'Évaluation CSPN Produit Opentrust MFT - version 3.4.0.1 Référence : CSPN-RTE-EQUISIGN-2.00 ; Version : 2.0 ; Date : 11 septembre 2020.
[GUIDES]	Guide utilisateur *MFT 3.4.0.1 End User Guide* Date : 19 novembre 2019. Guide technique programmeur *MFT 3.4.0.1 Connectors Developer Guide* Date : 19 novembre 2019. Guide d'administration Guide d'installation *MFT 3.4.0.1 Server Installation and Upgrade Guide* Date : 19 novembre 2019. Guide de configuration *MFT 3.4.0.1 Server Configuration Guide* Date : 19 novembre 2019. Guide de maintenance *MFT 3.4.0.1 System Maintenance Guide* Date : 19 novembre 2019. Guide de la gestion des journaux *Managed File Transfer3.4.0.1 Audit Logs Guide* Date : 19 novembre 2019.

ANNEXE B. Références à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CSPN]	Certification de sécurité de premier niveau des produits des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.1 du 13 janvier 2020. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/3.0 du 18 mars 2019. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/3 du 6 septembre 2018. Documents disponibles sur www.ssi.gouv.fr.
[RGS]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.