PREMIER
MINISTRE
*Liberté*
*Égalité*
*Fraternité*

Agence nationale de la sécurité
des systèmes d'information

**Secrétariat général de la défense**
**et de la sécurité nationale**

# Rapport de certification
# ANSSI-CSPN-2026/02

## MFT Online

### Version 4.4.1.0, hébergement on-premise

Paris, le 26/3/2026 | 23:04 CET

Vincent Strubel

# 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<br>**ANSSI-CSPN-2026/02** |
| Nom du produit<br>**MFT Online** |
| Référence/version du produit<br>**Version 4.4.1.0, hébergement on-premise** |
| Catégorie de produit<br>**Stockage sécurisé** |
| Critère d'évaluation et version<br>**CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)** |
| Commanditaire<br>**EQUISIGN**<br>Tour Opus 12 77 Esplanade du général de Gaulle<br>92081 Paris La Défense Cedex, France |
| Développeur<br>**EQUISIGN**<br>Tour Opus 12 77 Esplanade du général de Gaulle<br>92081 Paris La Défense Cedex, France |
| Centre d'évaluation<br>**ALMOND**<br>11 rue Maurice Fabre<br>35000 Rennes, France |
| Accord de reconnaissance applicable<br>fixed time certification<br>Ce certificat est reconnu dans le cadre du [BSZ_CSPN] |
| Fonctions de sécurité évaluées<br>Identification et authentification du bénéficiaire<br>Contrôle d'accès et gestion des droits/privilèges entre utilisateurs appartenant au bénéficiaire<br>Protection de données<br>Communication sécurisée<br>Journalisation |
| Fonctions de sécurité non évaluées<br>Sans objet |
| Restriction(s) d'usage<br>Oui |

# 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 cyber.gouv.fr.

## TABLE DES MATIERES

# 1 Le produit

## 1.1 Présentation du produit

Le produit évalué est « MFT Online, Version 4.4.1.0, hébergement on-premise » développé par EQUISIGN.

Ce produit est une solution de transfert de fichiers chiffrés en gros volume à destination des entreprises.

## 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 Online |
| Numéro de la version évaluée | Version 4.4.1.0, hébergement on-premise |

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

Un utilisateur connecté a la possibilité de récupérer la version de la TOE via les menus interactifs de l'UI End User. Après s'être rendu dans le menu [Preferences > About OpenTrust MFT], une fenêtre apparaît avec la version de la TOE. L'utilisateur obtient alors la version d'OpenTrust MFT

### 1.2.3 *Fonctions de sécurité*

Les fonctions de sécurité évaluées du produit sont :

- identification et authentification du bénéficiaire
- contrôle d'accès et gestion des droits/privilèges entre utilisateurs appartenant au bénéficiaire
- protection de données
- communication sécurisée
- journalisation

### 1.2.4 *Configuration évaluée*

La configuration évaluée correspond à

- Apache Tomcat, pour cette évaluation en version 9.0.112 ;
- Java OpenJDK-21, pour cette évaluation en version 21.0.9 ;
- PostgreSQL, pour cette évaluation en version 17.7 ;
- HAProxy, pour cette évaluation en version 3.0.6 ;
- ClamAV, pour cette évaluation en version 1.4.3 ;
- P7zip, pour cette évaluation en version 16.02 ;
- SoftHSM, pour cette évaluation en version 2.6.1 ;
- un serveur de mail local, utilisé uniquement par la TOE pour envoyer des mails à un serveur de messagerie est également préconisé. Postfix a été utilisé dans ce cadre en version 3.5.25 pour cette évaluation. L'agent postfix n'a été installé que sur le backend, il n'est pas directement utilisé par la TOE sur le frontend et le serveur de base de données.

La plateforme de test est constituée des éléments suivants :

- un serveur central « Backend » regroupe l'applicatif utilisateur et l'applicatif administratif ;
- un serveur « Frontend » fait office de relai pour les clients externes ;
- un serveur BDD expose une base de données qui gère l'ensemble de la configuration du produit ;
- une machine cliente permettant à l'administrateur ou un utilisateur de se connecter via les UI web ;
- une machine représentant un attaquant sur le réseau ;
- une machine hébergeant le serveur DNS et SMTP
- un export NFS a été mis en œuvre (sur le serveur « SMTP/DNS »), monté en suivant les instructions du guide sur le backend.

Ces serveurs sont répartis sur un VLAN. Le niveau de protection du produit est défini de niveau 2 ce qui implique l'utilisation d'un HSM. Un SoftHSM a donc été installé sur la machine Backend.

# 2 L'évaluation

## 2.1 Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de sécurité de premier niveau [CSPN].

## 2.2 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].

### 2.2.1 *Installation du produit*

#### *2.2.1.1 Particularités de paramétrage de l'environnement et options d'installation*

Le produit a été évalué dans la configuration précisée au paragraphe 1.2.4.

#### *2.2.1.2 Description de l'installation et des non-conformités éventuelles*

L'installateur a fait appel au développeur pendant l'installation. Cet échange a apporté une modification de guide.

#### *2.2.1.3 Notes et remarques diverses*

Sans objet

### 2.2.2 *Analyse de la documentation*

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

### 2.2.3 *Revue du code source (facultative)*

L'évaluateur a revu le code source de l'implémentation des mécanismes cryptographiques du produit.

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

### 2.2.4 *Analyse de la conformité des fonctions de sécurité*

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

### 2.2.5 *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.

### 2.2.6 *Analyse des vulnérabilités (conception, construction, etc.)*

#### *2.2.6.1 Liste des vulnérabilités connues*

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

#### *2.2.6.2 Liste des vulnérabilités découvertes lors de l'évaluation et avis d'expert*

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

### 2.2.7 *Analyse de la facilité d'emploi*

#### *2.2.7.1 Cas où la sécurité est remise en cause*

Les risques identifiés lors de l'évaluation entraînent des recommandations [ET/OU] des restrictions d'usage pour l'utilisateur (voir chapitre 3.2).

#### *2.2.7.2 Avis d'expert sur la facilité d'emploi*

Une fois installé, le produit est très intuitif à utiliser via ses deux UI web.

#### *2.2.7.3 Notes et remarques diverses*

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

## 2.3 Analyse de la résistance des mécanismes cryptographiques

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [CDS]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto]. L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

## 2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport au référentiel [ANSSI Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

# 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 Online, Version 4.4.1.0, hébergement on-premise » 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], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- Il est nécessaire de suivre le guide concernant le point de montage du NFS.
- Il est nécessaire, pour un nouvel utilisateur, de modifier le mot de passe.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement spécifiés dans la cible de sécurité [CDS], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

## 3.3 Reconnaissance du certificat

Ce certificat est émis dans les conditions du [BSZ_CSPN].

Cet accord permet la reconnaissance mutuelle des certificats de sécurité pour les schémas CSPN (Certification de Sécurité de Premier Niveau) et BSZ *(Beschleunigte Sicherheitszertifizierung* ou Certification de sécurité accélérée).

# ANNEXE A. Références documentaires du produit évalué

| | |
|---|---|
| [CDS] | Cible de sécurité de référence pour l'évaluation :<br>- Logiciel *single-tenant* MFT online en tant que service (SaaS) version 4.4.1.0 en hébergement *On Premise*, CSPN-CDS-MFT online-2.21, 15 décembre 2025<br>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :<br>- Logiciel *single-tenant* MFT *online* en tant que service (SaaS) version 4.4.1.0 en hébergement On Premise référence EQS006P, version 2.22, 09 Mars 2026. |
| [RTE] | Rapport technique d'évaluation :<br>- Rapport technique d'évaluation CSPN MFT Online version 4.4.1.0, référence CSPN-RTE-MFT ONLINE-2.11, version 2.11, 4 mars 2026 |
| [GUIDES] | Guide d'installation du produit :<br>- MFT 4.4.1.0 Server Installation and Upgrade Guide<br><br>Guide d'utilisation du produit :<br>- MFT 4.4.1.0 End_User_Guide |

# ANNEXE B. Références liées 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, version 5.0, 12 janvier 2023.<br><br>Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02, version 5.0, 12 juillet 2025.<br><br>Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01, version 4.0,6 mars 2024. |
| [CRY-P-01] | Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.2, 18 mars 2025. |
| [ANSSI Crypto] | Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020. |
| [BSZ_CSPN] | *Mutual Recognition Agreement of cybersecurity evaluation certificates issued under fixed time certification process, BSI/ANSSI,* référence bsz_cspn_mutual_recognition_agreement,version 2.0, mai 2024. |