Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CSPN-2017/08

TixeoServer Version 11.5.2.0

Paris, le 13 mars 2017

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

Guillaume POUPARD
[ORIGINAL SIGNE]

SÉCURITÉ 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-2017/08**
Nom du produit **TixeoServer**
Référence/version du produit **Version 11.5.2.0**
Catégorie de produit **Communication sécurisée**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **Tixeo SARL** **244 rue Claude François, 34080 Montpellier**
Centre d'évaluation **Amossys** **4 bis allée du bâtiment, 35000 Rennes, France**
Fonctions de sécurité évaluées **F1 : Chiffrement de bout en bout** **F2 : Protection des mots de passe des utilisateurs** **F3 : Authentification des utilisateurs** **F4 : HTTPS Tunneling**
Fonction(s) de sécurité non évaluées **Néant**
Restriction(s) d'usage **Oui (cf. §3.2)**

Préface

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 Premier ministre 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 matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la solution « TixeoServer, version 11.5.2.0 » développée par *TIXEO SARL*.

La solution TixeoServer est un système de vidéo conférence administré par le client. Il permet la communication voix et vidéo en multipoints, et offre des fonctions de partage d'écran et de documents. Le système a pour objectif de protéger la confidentialité des communications.
Il se compose de trois éléments :

- le serveur TMMS (*Tixeo Meeting Management Server*), assurant la gestion des utilisateurs, des réunions et de l'authentification ;
- le serveur TCS (*Tixeo Communication Server*), responsable de la gestion des communications temps réels, flux audio, vidéo et data pendant les réunions ;
- le client TCC (*Tixeo Communication Client*) est le logiciel coté utilisateur qui permet d'organiser, rejoindre et participer à des réunions en ligne.

Le client TCC communique avec le TCS et le TMMS en HTTPS sur le port 443.
Les principales fonctionnalités offertes par le produit sont les suivantes :

- les communications entre les différents TCC connectés à une même réunion sont protégées par un chiffrement de bout en bout. Les flux sont chiffrés localement sur le TCC et déchiffrés sur les TCC des autres participants à la réunion. Le serveur TCS manipule les flux de communication chiffrés sans avoir accès au contenu de ces communications ;
- les mots de passe des utilisateurs dans la base de données sont stockés sous forme de condensats salés. Le serveur n'a pas connaissance des mots de passe saisis par les utilisateurs ;
- les utilisateurs de la solution (invités, organisateurs et administrateurs) doivent s'authentifier sur le TMMS (par page web ou depuis le client TCC) en utilisant leur email et mot de passe. L'accès à une réunion est strictement réservé aux personnes y étant invitées ;
- les communications (audio, vidéo et données) entre le TCC et le serveur TCS sont encapsulées dans un flux HTTPS unique, identifié sur le réseau. Le lien de communication entre le client TCC et le serveur TMMS est également chiffré et protégé par l'utilisation du protocole HTTPS.

La figure ci-dessous illustre un déploiement typique de la solution.

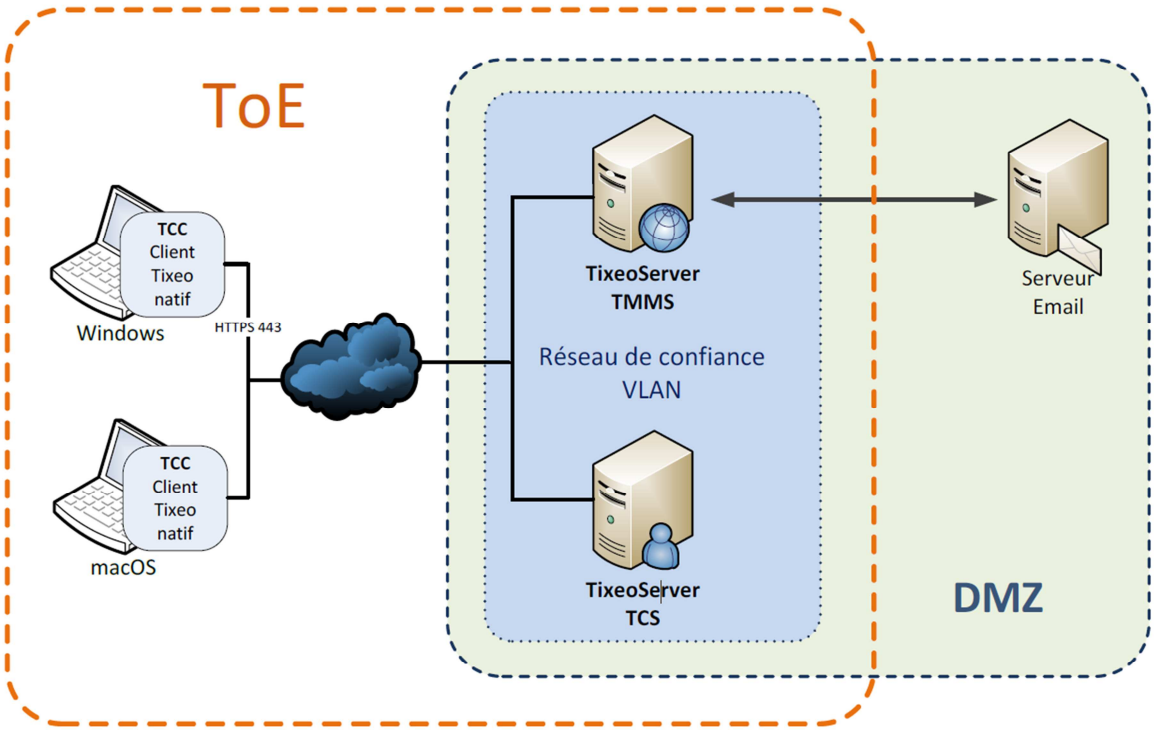

Figure 1 - Architecture de la solution TixeoServer.

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

Nom du produit	TixeoServer
Numéro de la version évaluée	11.5.2.0

Tous les éléments de la solution (TMMS, TCS, TCC Windows et Mac OS) portent le même numéro de version.
La version certifiée du produit peut être identifiée de la manière suivante :

- en se connectant sur le TMMS via un navigateur Web (Figure 2) ;
- dans les détails du fichier PE (`C:\Program Files (x86)\Tixeo Soft\Communication\Server\MetaServer\W3DMetaServer.exe`) sur le TCS (Figure 3) ;
- dans les paramètres de l'application TCC (Figure 4).

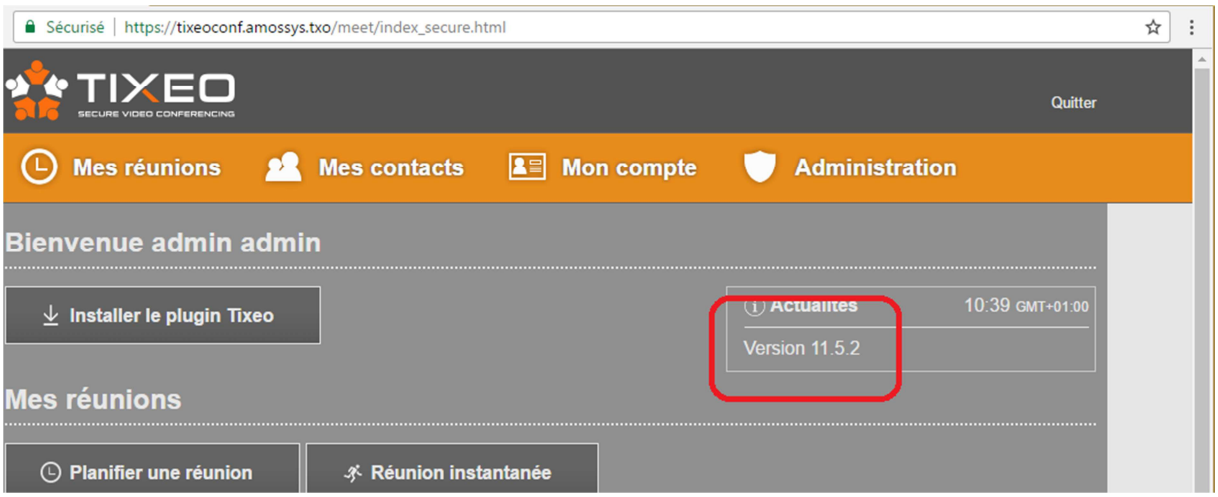

Figure 2 : Version du TMMS

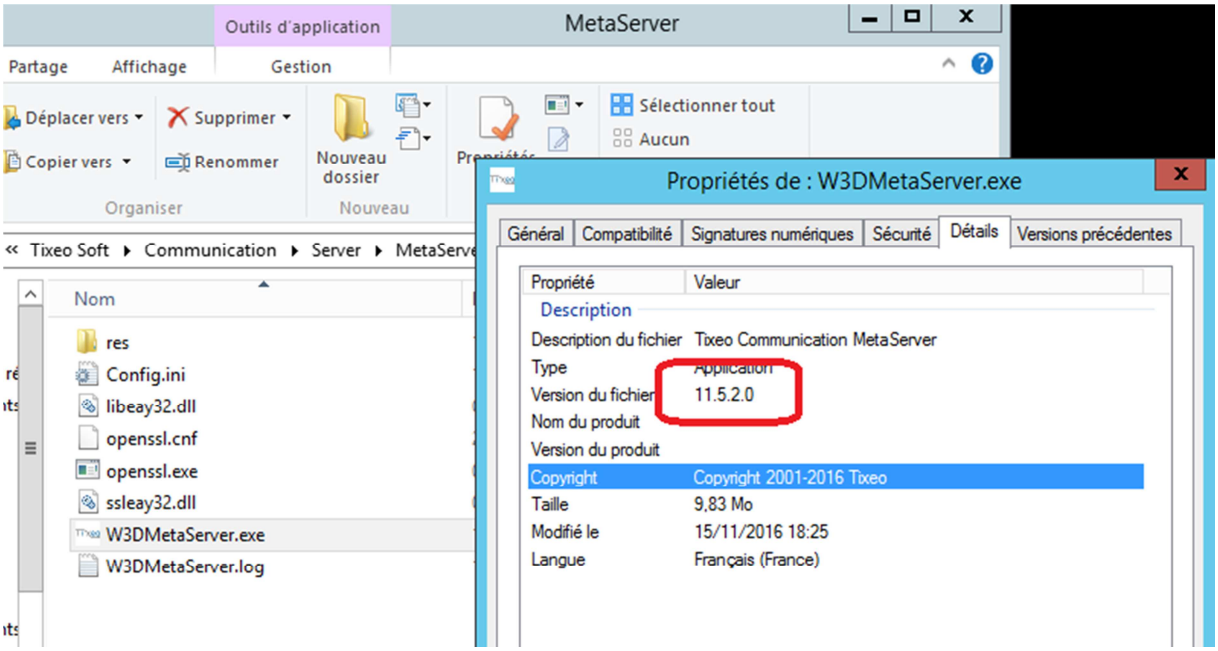

Figure 3 : Version du TCS

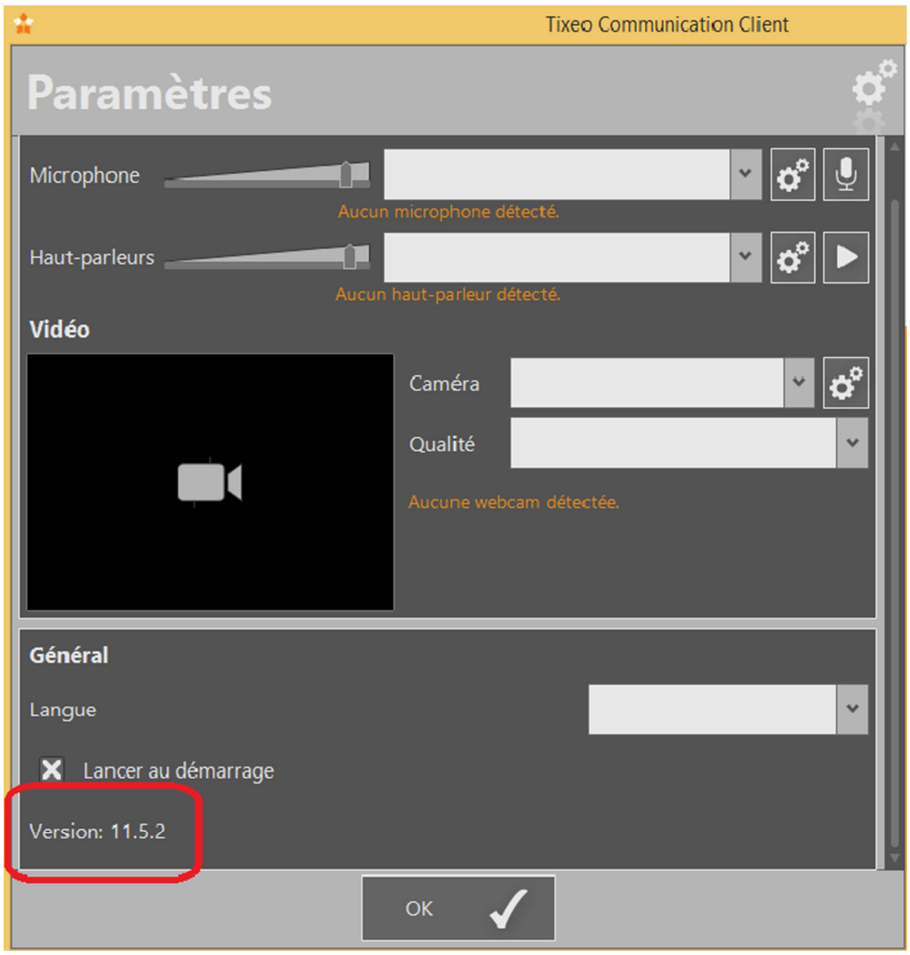

Figure 4 : Version du TCC

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :

- F1 : Chiffrement de bout en bout ;
- F2 : Protection des mots de passe des utilisateurs ;
- F3 : Authentification des utilisateurs ;
- F4 : HTTPS Tunneling.

1.2.4. Configuration évaluée

La configuration évaluée correspond à un TCC Windows communiquant avec un TCC MacOS. Les composants TCS et TMMS sont hébergés sur un serveur unique, lui-même installé sur un réseau maîtrisé.

La plateforme de test est constituée des éléments suivants :

- un domaine AMOSSYS.TXO comprenant le serveur hébergeant :
  - le TMMS ;
  - le TCS ;
  - le « Serveur Email », comprenant :
    - le contrôleur du domaine Active Directory AMOSSYS.TXO,

  - un serveur SMTP pour la validation des comptes clients,
  - une autorité de certification pour la génération des certificats nécessaires au chiffrement des communications,
  - le serveur DNS pour le domaine AMOSSYS.TXO;
- un PC sous Windows 10 contenant un TCC ;
- un PC sous MacOS X contenant un TCC.

La figure ci-dessous décrit la plateforme de tests.

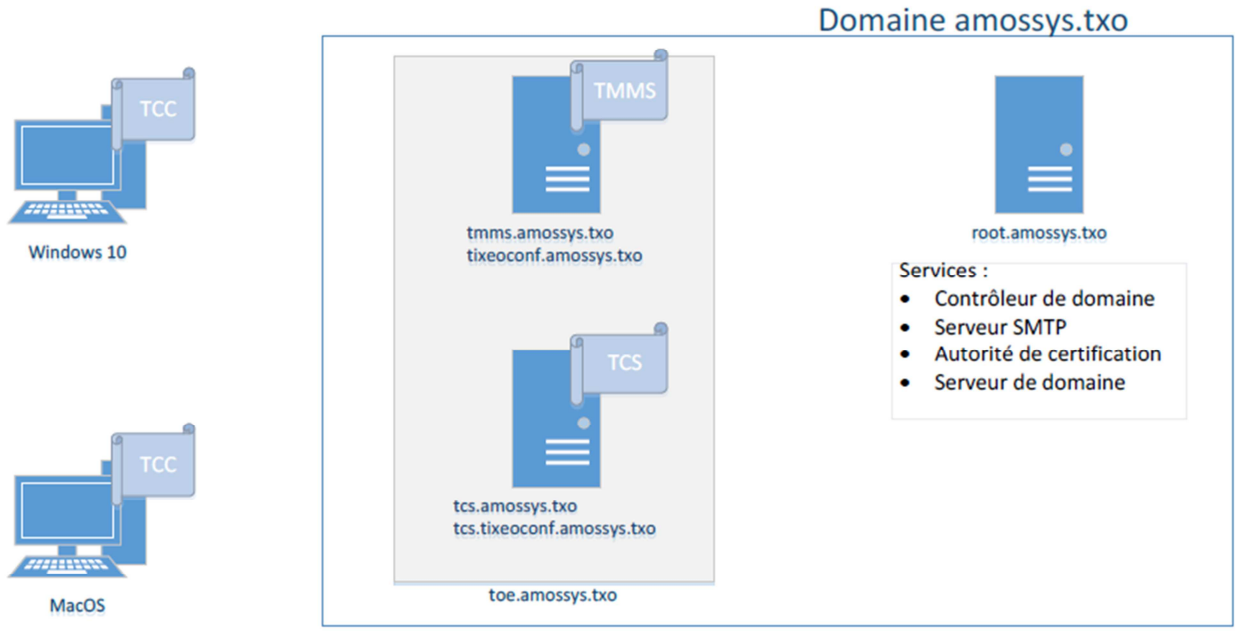

Figure 5 : plateforme de tests

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 2.

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 suit la documentation [GUIDES] et s'effectue selon les étapes suivantes :

- installation du TMMS à partir de l'exécutable disponible sur le site internet du développeur : cette phase requiert l'installation de *Java SE Development Kit*, du TMMS, des certificats et enfin de la licence ;
- installation du TCS à partir de l'exécutable disponible sur le site internet du développeur : cette phase requiert l'installation du TCS, des certificats associés et l'association du TCS au TMMS ;
- téléchargement et installation des TCC à partir de l'exécutable disponible sur le site internet du développeur.

Aucune non-conformité n'a été relevée lors de l'installation.

2.3.1.3. Durée de l'installation

L'installation de la TOE a requis une demi-journée.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

La documentation est jugée suffisamment complète pour permettre une prise en main efficace du produit, malgré certains manques ou incohérences relevés dans [RTE].

2.3.3. Revue du code source (facultative)

L'évaluateur a effectué une revue de la partie propriétaire du code source et estime que le code est lisible et correctement documenté.

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] à l'exception d'une non-conformité mineure (seule la connexion par e-mail, et non par login, est possible).

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

Toutes les fonctions de sécurité ont subi des tests de pénétration ; aucune ne présente, dans le contexte d'utilisation du produit et pour le niveau d'attaquant visé, de vulnérabilité exploitable mettant en défaut le problème de sécurité défini dans la cible [CDS].

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

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

2.3.7. Accès aux développeurs

Le centre d'évaluation a eu accès aux développeurs pour répondre à des questions sur le produit. Ces questions ont principalement visé à clarifier l'implémentation des mécanismes cryptographiques.

2.3.8. Analyse de la facilité d'emploi et préconisations

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. Recommandations pour une utilisation sûre du produit

Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.
De plus, l'utilisateur du produit devra mettre en œuvre les mesures suivantes :

- désactiver le stockage des mots de passe par le navigateur Web sur le TCC ;
- limiter au maximum l'utilisation de la messagerie instantanée hors-réunion ;
- mettre en place des dispositifs de type *Web-Application Firewall* ou *fail2ban* sur le serveur Web TMMS pour empêcher les attaques par force brute ;
- imposer une politique de mots de passe forte aux utilisateurs ;
- rejoindre des réunions depuis des postes dédiés ou, a minima, peu sensibles pour limiter l'impact d'une élévation de privilèges d'un autre participant ;

- restreindre les noms de domaines et adresses IP accessibles par le client TCC via une politique locale de pare-feu ;
- utiliser des mots de passe uniques pour l'application ;
- placer le TCS et le TMMS dans un réseau dédié et maîtrisé, afin d'éviter une interception des communications entre ces deux serveurs.

2.3.8.3. Avis d'expert sur la facilité d'emploi

Aucun avis d'expert du CESTI n'a été donné quant à la facilité d'emploi du produit.

2.3.8.4. 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. Celle-ci n'a pas identifié de non-conformité au RGS ni de vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

Le produit utilise les générateurs fournis par les bibliothèques *OpenSSL* et *mORMot*.
Dans le premier cas, l'évaluateur a relevé une non-conformité mineure à [REF] (utilisation de SHA-1 pour le retraitement d'aléa). Dans le second cas, l'évaluateur n'a pu s'assurer de l'utilisation d'une mémoire non volatile pour le retraitement.
Toutefois, l'évaluateur estime que l'utilisation de ces générateurs d'aléa n'entraîne pas de vulnérabilité sur le produit.

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 « TixeoServer, version 11.5.2.0 » 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. 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations énoncées dans le présent rapport (voir 2.3.8.2).

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CSPN – Tixeo* *Version 161025* Date : *25 octobre 2016*
[RTE]	*Rapport Technique d'Évaluation CSPN - Produit TixeoServer version 11.5.2.0* Référence : *CSPN-RTE-TixeoServer* Version : 1.01 Date : *27 février 2017*
[ANA-CRY]	*Expertise des mécanismes cryptographiques - Produit TixeoServer - version 11.5.2.0* Référence : *CSPN-CRY-TixeoServer* Version : 1.0 Date : *30 janvier 2017*
[SPEC-CRY]	*Fournitures nécessaires à l'analyse de mécanismes cryptographiques – Tixeo* *Version 161025* Date : *25 octobre 2016*
[GUIDES]	*TixeoServer Admin Guide – TixeoServer.pdf* *version 11.5.2 et plus.*

Annexe 2. 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 (CSPN) des technologies de l'information, version 1.1, référence ANSSI-CSPN-CER-P-01/1.1 du 07 avril 2014. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, version 1.1, référence ANSSI-CSPN-CER-I-02/1.1 du 23 avril 2014. Méthodologie pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-NOTE-01/2 du 23 avril 2014. Documents disponibles sur www.ssi.gouv.fr/
[REF]	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_B_1), voir www.ssi.gouv.fr/.