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-2020/24

CFJL

Version 3.0

Paris, le 9 juin 2020

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

Guillaume POUPARD
[ORIGINAL SIGNÉ]

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-2020/24**
Nom du produit **CFJL**
Référence/version du produit **Version 3.0**
Catégorie de produit **Stockage sécurisé**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU (CSPN)**
Commanditaire **CECURITY.COM** 75 rue Saint-Lazare 75009 Paris
Développeur **CECURITY.COM** 75 rue Saint-Lazare 75009 Paris
Centre d'évaluation **Oppida** 4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Fonctions de sécurité évaluées **Authentification forte des utilisateurs déposants** **Chiffrement des événements** **Scellement des événements** **Chaînage des événements** **Horodatage de la signature** **Protection des secrets cryptographiques** **Protection des journaux d'évènements applicatifs**
Fonction(s) de sécurité non évaluées **Sans objet**
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 le « CFJL, version 3.0 » développé par *CECURITY.COM*.

Le Coffre-fort des Jeux en Ligne (CFJL) est une des composantes d'un frontal défini par [DET] comme *un dispositif de recueil et d'archivage sécurisé des données en vue du stockage d'une liste définie d'événements et de données clé issus des échanges entre joueur et plateforme* de jeux en ligne.
Le coffre-fort lui-même est un dispositif logiciel *dont la fonction est d'horodater, de chiffrer et d'archiver les données tracées par le capteur, afin d'en garantir l'intégrité et l'exhaustivité dans le temps*. Le capteur est quant à lui un composant *dont la fonction est la création de traces. La fonction de création de traces correspond au formatage des données circulant entre le joueur et la plateforme de jeu puis au transfert de ces données vers le module coffre-fort du frontal*.
La figure ci-dessous montre la mise en oeuvre de ces composants :

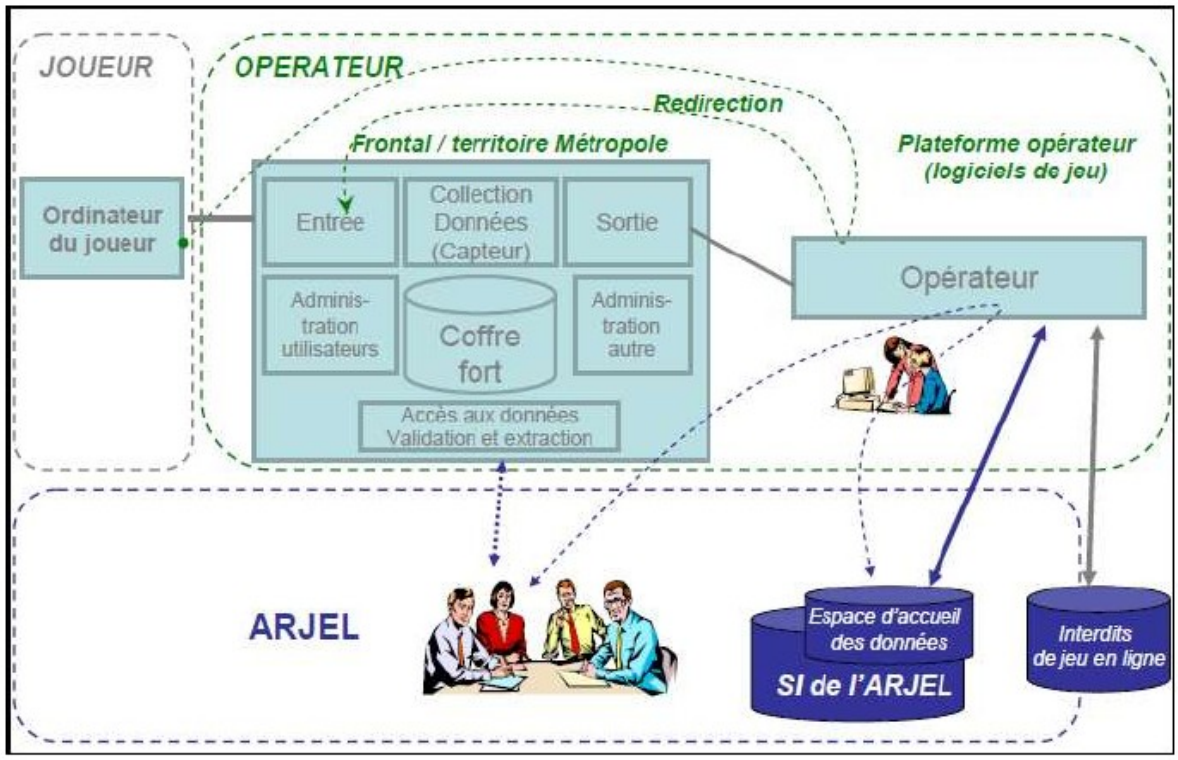

Figure 1 - Coffre-fort des jeux en ligne, frontal et capteur.

Le Coffre-fort des Jeux en Ligne permet donc la conservation, à des fins de contrôle, d'évènements de jeu nativement électroniques déposés par un opérateur de jeux et paris en ligne client du système.
Le coffre-fort des jeux en ligne permet :

- d'archiver les événements de jeu produits par les plateformes de l'opérateur de jeu en ligne, et collectés par le capteur ;
- d'obtenir des attestations d'archivage des événements de jeu ;
- d'obtenir des copies électroniques conformes des événements de jeu archivés;

- de conserver ses propres éléments de preuve relatifs à l'archivage sécurisé des événements de jeu archivés.

Le produit doit protéger l'accès aux données archivées ainsi que leur complétude et leur intégrité.

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	CFJL
Numéro de la version évaluée	3.0

La version certifiée du produit peut être identifiée via la commande « cfjl version » :

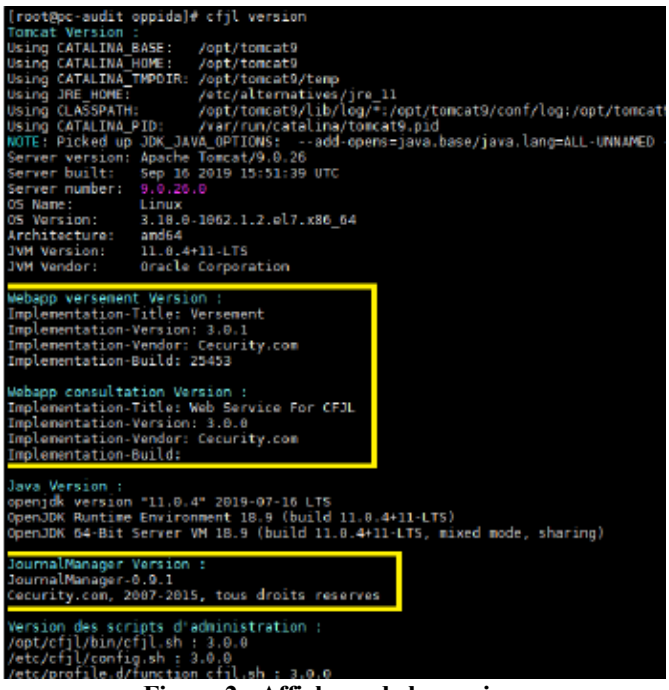

Figure 2 - Affichage de la version.

1.2.3. Fonctions de sécurité

Les fonctions de sécurité évaluées du produit sont :
- Authentification forte des utilisateurs déposants ;
- Chiffrement des événements ;
- Scellement des événements ;
- Chaînage des événements ;
- Horodatage de la signature ;
- Protection des secrets cryptographiques ;
- Protection des journaux d'évènements applicatifs.

1.2.4. Configuration évaluée

La configuration évaluée est déployée directement par CECURITY.COM. Elle se compose des éléments suivants :
- un serveur RedHat 7.7 contenant les différents applicatifs CFJL ;
- un serveur NTP ;
- un HSM Safenet ;
- toutes les clés de signature sont des clés RSA de taille 2048 bits, comme spécifié lors des différentes procédures de création des espaces clients ;
- toutes les clés de signature utilisent le SHA256 comme algorithme de hachage comme spécifié lors de la procédure de création des espaces clients ;
- quatre types d'administrateurs ont été créés :
  - administrateur opérationnel et technique : dispose du compte Unix « admin », identifié par une bi-clef RSA 2048 bits,
  - administrateur fonctionnel : dispose du compte Unix « admincfjl » identifié par une bi-clef RSA 2048 bits,
  - administrateur de mise à jour : dispose du compte Unix « adminupdates » identifié par une bi-clef RSA 2048 bits,
  - administrateur de contrôle du HSM : dispose d'un compte Unix « adminhsm » identifié par une bi-clef RSA 2048 bits,
- le produit a été configuré pour utiliser deux interfaces réseau physiques séparées :
  - l'interface d'administration utilisée pour :
    - SSH : connexion entrante,
  - l'interface applicative utilisée pour :
    - HTTPS : connexion entrante,
    - JMS/SSL : connexion entrante.

L'évaluateur a fourni la source de temps (service NTP).

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

Sans objet.

2.3.1.3. Durée de l'installation

Sans objet : l'installation est effectuée par le développeur.

2.3.1.4. Notes et remarques diverses

Sans objet.

2.3.2. Analyse de la documentation

L'évaluateur a eu accès aux documents [GUIDES] dans le cadre de cette évaluation.
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 de l'implémentation des mécanismes cryptographiques du produit. L'analyse a été effectuée manuellement.
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

Des vulnérabilités publiques existent sur le produit ou sur ses briques logicielles tierces, mais se sont révélées inexploitables pour le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité [CDS].
Il est à noter que la version de système d'exploitation (RedHat 7.7) utilise des composants logiciels qui ne sont plus maintenus que par RedHat, et non par leurs éditeurs originels (par exemple OpenSSL). Bien qu'aucune vulnérabilité publique exploitable n'ait été détectée lors de l'évaluation, il n'est pas impossible que des vulnérabilités exploitables non publiques existent, et puissent être utilisées contre le produit

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 le niveau d'attaquant considéré et dans le contexte défini par la cible de sécurité.

2.3.7. Accès aux développeurs

Sans objet.

2.3.8. Analyse de la facilité d'emploi

2.3.8.1. Cas où la sécurité est remise en cause

Les risques identifiés lors de l'évaluation entraînent des recommandations pour l'utilisateur (voir chapitre 3.2).

2.3.8.2. 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.

2.3.8.3. Notes et remarques diverses

Sans objet.

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 vulnérabilité exploitable.

2.5. Analyse du générateur d'aléas

L'analyse du générateur aléatoire du produit n'a pas identifié 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 « CFJL, version 3.0 » 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. 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 mettre en œuvre, lorsqu'elles sont pertinentes au regard du contexte d'utilisation du produit, les recommandations et restrictions suivantes.
Bien que le produit soit censé être correctement configuré lors de sa livraison, les administrateurs doivent s'assurer que les fichiers *.properties* fournis sont conformes aux [GUIDES], afin de s'assurer que l'intégralité des services de sécurité (horodatage, signature...) sont bien activés.
Les conditions de déploiement prévues dans la cible de sécurité [CDS] doivent être respectées et les utilisateurs doivent se conformer aux [GUIDES] fournis.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cecurity_CFJL_V30_CibleSecurite* Date : *6 avril 2020.* *Cecurity_CFJL_V30_Moyens cryptographiques* Date : *6 avril 2020.* *Cecurity_CFJL_V30_Annexe XADES-E-T* *Date : 31 mars 2020.*
[RTE]	*Rapport Technique d'Evaluation CSPN Coffre-Fort des Jeux en Ligne* Référence : : OPPIDA/CESTI/CECURITY2/RTE ; Version : 3.0 ; Date : *13 mai 2020.*
[GUIDES]	*Cecurity_CFJL_V30_API Versement* Date : *23 septembre 2019.* *Cecurity_CFJL_V30_Cartographie des répertoires* Date : *4 octobre 2019.* *Cecurity_CFJL_V30_Manuel d'exploitation* Date : *4 octobre 2019.* *Cecurity_CFJL_V30_Manuel d'installation* Date : *6 avril 2020.* *Cecurity_CFJL_V30_Manuel utilisateur de l'outil d'accès aux traces* Date : 4 octobre 2019. *Cecurity_CFJL_V30_Manuel utilisateur de l'outil de validation des traces* Date : *4 octobre 2019.*
[DET]	*Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL)* Référence : *DET* ; Version : *1.2* ; Date : *24 septembre 2012.*

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 des technologies de l'information, référence ANSSI-CSPN-CER-P-01/2.0 du 6 septembre 2018. Critères pour l'évaluation en vue d'une certification de sécurité de premier niveau, référence ANSSI-CSPN-CER-P-02/2.0 du 6 septembre 2018. 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.