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-2011/04

Coffre-fort de jeux en ligne
Version 2.0

Paris, le 31 mars 2011

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

Patrick Pailloux
[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.anssi@ssi.gouv.fr

Référence du rapport de certification **ANSSI-CSPN-2011/04**
Nom du produit **Coffre-fort de jeux en ligne**
Référence/version du produit **Version 2.0**
Critères d'évaluation et version **CERTIFICATION DE SECURITE DE PREMIER NIVEAU** ***(CSPN, Phase expérimentale)***
Développeur(s) **Cecurity.com** **75, rue Saint-Lazare** **75009 Paris** **France**
Commanditaire **Cecurity.com** **75, rue Saint-Lazare** **75009 Paris** **France**
Centre d'évaluation **Oppida** **4-6, avenue du Vieil Etang - Bât B** **78180 Montigny Le Bretonneux** **Tél : +33 (0)1 30 14 19 00, Mél : cesti@oppida.fr**

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 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 « Coffre-fort de jeux en ligne**,** Version 2.0 **»** (CFJL) développé par Cecurity.com. Il s'agit d'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.

Ce coffre-fort électronique est évalué dans le contexte particulier de l'ouverture du marché français des jeux d'argent et de paris en ligne. Pour pouvoir proposer des offres de jeux aux consommateurs français, un « opérateur » doit, entre autre, permettre à une « autorité » (ARJEL[1]) de surveiller ses activités transactionnelles. Pour cela, un dispositif doit être installé chez l'opérateur pour recueillir et archiver les traces de certaines opérations au sein de son système d'information.

Ce dispositif est communément nommé coffre-fort électronique. C'est ce produit qui est la cible de l'évaluation en vue d'une Certification Sécurité de Premier Niveau.

Le système comporte également un capteur, hors du périmètre de cette certification, permettant de formater les données circulant entre le joueur et la plateforme de jeu, et de les transférer vers le module d'entrée du coffre-fort.

1.2. Description du produit évalué

La cible de sécurité [ST] 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 – firewall
☐ 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 - matériel et logiciel embarqué
☐ 99- Autres

[1] Autorité de Régulation des Jeux En Ligne

1.2.2. Identification du produit

Le coffre-fort est composé d'un ensemble de logiciels et de fichiers de configuration. Le produit certifié est identifiable par le numéro de version et l'empreinte de trois de ces éléments :

Élément	Version	Empreintes	
FrontService	2.0.2	**SHA1**	d5516b26ad2f29ad5aa527bfeb12b51f66e96d6d
		MD5	b37d2221bbd3a22203f3c2ef857900d6
ServerWS	2.0.2	**SHA1**	7f6a15b0feb1d3060aa7c1d39fe9451b6cc79bd8
		MD5	b3c9fbfaa72964d1aeda51b6fcdf2ac7
Fichier de configuration sudo	-	**SHA1**	ff7dbf8e8b72dcb4ad08288592f3b25019c6a151
		MD5	853619accca851ae25e048a90df13987

Les numéros de version de ces applications sont identifiables dans le fichier *META-INF/MANIFEST.MF* de chaque application.

Les empreintes sont celles des fichiers suivants :

FrontService	/usr/local/apache-tomcat-6.0.29/webapps/frontService.war
ServerWS	/usr/local/apache-tomcat-6.0.29/webapps/ServerWS.war
Fichier de configuration sudo	/etc/sudoers

Les autres logiciels dont dépend le produit ainsi que leurs versions sont identifiés dans le §2.3.2.2.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- le contrôle de l'accès au coffre-fort ;
- le chiffrement des dépôts (création de l'enveloppe) ;
- le scellement des dépôts (création de la trace) ;
- le chaînage des traces ;
- la signature de la configuration du coffre-fort.

1.2.4. Configuration évaluée

Le produit étant installé et configuré directement chez le client, la configuration dépend de l'architecture du système de l'opérateur. La plateforme de test est décrite dans le §2.3.2.1 du présent document.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément à la Certification de Sécurité de Premier Niveau en phase expérimentale. Les références des documents se trouvent en annexe 2.

2.2. Charge de travail prévue et durée de l'évaluation

La charge de travail prévue lors de la demande de certification était conforme à la charge de travail préconisée dans [CSPN] pour un produit comportant des mécanismes cryptographiques, soit 35 hommes x jours. Une prolongation de 15 hommes x jours a exceptionnellement été accordée au centre d'évaluation afin de permettre au laboratoire d'évaluation de prendre en compte une modification de la solution faite par Cecurity.com durant l'évaluation. Cette dernière s'est déroulée de septembre à décembre 2010.

2.3. Travaux d'évaluation

Ce paragraphe apporte des précisions sur la cible de sécurité [CDS] fournie en entrée d'évaluation. Ces précisions sont issues du [RTE] élaboré par l'évaluateur suite à ses travaux.

2.3.1. Fonctionnalités, environnement d'utilisation et de sécurité

2.3.1.1. Spécification de besoin du produit

Conforme à la cible de sécurité [CDS] (chapitre 2 : « Argumentaire (description) du produit »).

2.3.1.2. Biens sensibles manipulés par le produit

Conforme à la cible de sécurité [CDS] (chapitre 4 : « Description des biens sensibles que le produit doit protéger »).

2.3.1.3. Description des menaces contre lesquelles le produit apporte une protection

Conforme à la cible de sécurité [CDS] (Chapitre 5 : « Description des menaces »).

2.3.1.4. Fonctions de sécurité

Conforme à la cible de sécurité [CDS] (chapitre 6 : « Description des fonctions de sécurité du produit »).

2.3.1.5. Hypothèses sur l'utilisation du produit

Les accès aux fonctionnalités du coffre-fort doivent être effectués au travers de canaux sécurisés (HTTPS). Ceux-ci doivent être configurés conformément à l'état de l'art notamment en termes de suites de chiffrement autorisées et de versions protocolaires.

2.3.1.6. Utilisateurs typiques

Conforme à la cible de sécurité [CDS] (chapitre « Argumentaire »).

2.3.2. Installation du produit

L'installation doit être réalisée par la société Cecurity.com.

2.3.2.1. Plate-forme de test

La plate-forme de test était composée :

- d'un processeur quadri cœur AMD Athlon II X4 635 (2.9Ghz) ;
- de 4 GB de mémoire vive ;
- d'un disque dur d'une capacité de 1 To ;
- de deux interfaces réseau ;
- carte HSM cryptographique Luna PCI.

L'évaluateur n'a pas assisté à l'installation du coffre-fort. Il constate que les logiciels suivants sont installés :

Logiciel	Version
Système d'exploitation GNU/Linux	RedHat Enterprise Linux Server 5.5
Apache HTTPd	httpd-2.2.3-43.el5_5.3
mod_ssl	mod_ssl-2.2.3-43.el5_5.3
mod_jk	mod_jk-ap20-1.2.28-2
openSSL	openssl-0.9.8e-12.el5_4.6
Java Runtime Environment	jre-1.6.0_21-fcs
Tomcat	apache-tomcat-6.0.29
PostgreSQL	postgresql-libs-8.4.4-2PGDG.el5 postgresql-server-8.4.4-2PGDG.el5 postgresql-8.4.4-2PGDG.el5 compat-postgresql-libs-4-1PGDG.rhel5
Bouncycastle	bcprov-jdk1.5-1.45.jar
Log4j	log4j-1.2.16.jar
Apache Commons Logging	commons-logging-1.1.jar
Serializer	serializer-2.7.1.jar
Xalan	Java xalan-2.7.1.jar
Apache XML Security	xmlsec-1.4.3-CC.jar

Cecurity.com a fourni trois utilitaires permettant de tester les fonctionnalités du CFJL :

- ClientBroker : permet l'envoi d'évènements pour stockage ;
- ClientWS : permet l'envoi de demandes de rapports contenant des ensembles d'évènements stockés dans le coffre-fort, ainsi que le téléchargement desdits rapports ;
- ReportExtractor : permet l'extraction des rapports téléchargés ainsi que la validation de la signature des évènements.

Le dossier d'exigences techniques de l'ARJEL [DET] stipule qu'en production, chaque opérateur doit intégrer les appels à l'API du CFJL au code de son capteur [DET]. Ces outils ne font pas partie du périmètre de ce certificat.

2.3.2.2. Particularités de paramétrage de l'environnement

L'environnement d'exécution des utilitaires fournis durant l'évaluation est composé de :

Logiciel	Version
Système d'exploitation GNU/Linux	GNU/Linux Ubuntu 10.04 « Lucid »
Java Runtime Environment	1.6.0.22
Boucycastle	1.45
Apache Commons Logging	1.1
Log4j	1.2.16
Serializer	2.7.1
Xalan Java	2.7.1
XML Security	1.4.3-CC (version modifiée par Cecurity.com)

2.3.2.3. Options d'installation retenues pour le produit

La configuration du produit suivante a été retenue pour l'évaluation :

- un seul espace de stockage a été créé sur le disque dur local ;
- toutes les clés de signature sont des clés RSA de taille 2048 bits ;
- toutes les clés de signature utilisent le SHA256 comme algorithme de hachage ;
- quatre profils d'administrateurs (opérationnel et technique, fonctionnel, mise à jour, contrôle du HSM) ont été créés, chacun étant identifié par un bi-clef RSA 2048 bits unique ;
- deux profils d'utilisateurs (dépôt et consultation) ont été configurés ;
- le produit a été configuré pour utiliser deux interfaces réseau physiques (administrative et applicative) séparées.

Cette configuration est conforme à [DET].

2.3.2.4. Description de l'installation et des non-conformités éventuelles

L'évaluateur n'a pas assisté à l'installation du produit sur la machine hôte. Seule la configuration relative à l'installation du produit au sein de la plateforme de test a été supervisée.

La configuration du produit est décrite dans le « Manuel d'installation du logiciel CFJL » [GUIDES]. Elle est jugée simple et rapide.

2.3.2.5. Durée de l'installation

Le temps nécessaire à l'installation complète du produit n'a pas été communiqué à l'évaluateur. La configuration du produit sur la plateforme de test a duré une demi-journée et a été effectuée par un développeur de Cecurity.com.

2.3.2.6. Notes et remarques diverses

L'installation du coffre-fort pour l'évaluation a été effectuée par Cecurity.com. L'évaluateur n'a supervisé aucune étape du processus d'installation car le produit ne doit être livré aux opérateurs de jeux qu'une fois la configuration initiale effectuée. Ce processus de livraison assure que le produit est utilisé dans un contexte compatible avec la cible de sécurité [CDS].

2.3.3. Analyse de la documentation

L'évaluateur a eu accès à la documentation technique du produit [GUIDES] :

- le manuel d'installation du logiciel CFJL décrit clairement la procédure d'installation et de configuration du produit ;
- les manuels d'utilisation relatifs aux profils « dépôt » et « consultation » sont jugés succincts et incomplets ;
- le manuel d'exploitation n'est pas assez universel. Il présente l'intégration du coffre-fort à une infrastructure spécifique et ne permet pas d'intégrer le produit à un autre type d'infrastructure.

2.3.4. Revue du code source (facultative)

Les évaluateurs n'ont pas eu accès au code source.

2.3.5. Fonctionnalités testées

Fonctionnalité	Résultat
Authentification forte des déposants	**Réussite**
Authentification forte des administrateurs	**Réussite**
Chiffrement des évènements	**Réussite**
Signature des évènements	**Réussite**
Chaînage des évènements	**Réussite,** toutefois, voir chapitre 2.3.9.

2.3.6. Synthèse des fonctionnalités testées / non testées et des non-conformités

Les tests de conformité ont permis de tester la plupart des fonctionnalités offertes par le produit « Coffre-fort de jeux en ligne ».

Les utilitaires permettant le test du produit par les évaluateurs ainsi que le capteur permettant la création de traces sont hors périmètre de la cible de sécurité [CDS] et n'ont donc pas été analysés.

2.3.7. Avis d'expert sur le produit

Le produit est fonctionnellement conforme à la cible de sécurité [CDS]. Son installation n'a pu être évaluée par l'évaluateur, tandis que sa configuration ainsi que son utilisation sont jugées simples et efficaces.

D'un point de vue fonctionnel, le coffre-fort est conforme aux exigences de l'ARJEL décrites dans [DET], bien que celles-ci souffrent d'une erreur de conception en ce qui concerne la suppression des derniers évènements sauvegardés (cf. §2.3.9).

2.3.8. Analyse de la résistance des mécanismes et des fonctions

2.3.8.1. Liste des fonctions et des mécanismes testés - résistance

L'avis sur la résistance des mécanismes est donné au §2.3.8.2.

Fonction et mécanisme
Mécanisme d'authentification SSL par certificat des utilisateurs
Mécanisme de chiffrement des documents
Mécanisme d'authentification SSH par bi-clef RSA des administrateurs

2.3.8.2. Avis d'expert sur la résistance des mécanismes

La résistance des mécanismes de sécurité est conforme à l'état de l'art. Il n'a pas été mis en évidence de vulnérabilités exploitables dans le cadre de l'évaluation du produit. Les mécanismes de sécurité qui s'appuient sur la cryptographie font l'objet d'une analyse théorique particulière dont les principales conclusions sont données au chapitre 2.4.

2.3.9. Analyse des vulnérabilités (conception, construction…)

2.3.9.1. Liste des vulnérabilités connues

La cible de sécurité [CDS] stipule que les correctifs de sécurité des différents logiciels utilisés par le produit doivent être appliqués dès leur publication (cf. §2.3.10.2).

Les vulnérabilités publiques de ces logiciels recensées pendant l'évaluation sont donc supposées corrigées après la mise à jour du coffre-fort.

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

Aucune.

2.3.10. Analyse de la facilité d'emploi et préconisations

2.3.10.1. Cas où la sécurité est remise en cause

Sans Objet.

2.3.10.2. Recommandations pour une utilisation sûre du produit

Compte « root »
Il est fortement recommandé que seule l'« autorité » possède le login / mot de passe d'accès au compte *root* qui permet d'accéder à l'ensemble des fonctions du système. Ce mot de passe doit suivre une politique de création et une politique de gestion conformes à la note du CERTA (No CERTA-2005-INF-001).

La plate-forme doit pouvoir être mise à jour. Il est préconisé que les mises à jour se fassent sous la responsabilité de l'« autorité ». La mise à jour pourrait, par exemple, être réalisée directement par l'« autorité » (le développeur fournit à l'« autorité » l'ensemble de la

procédure de mise à jour, ainsi que les logiciels si besoin), ou indirectement (l'« autorité » s'authentifie en tant que « root », et laisse le développeur effectuer la mise à jour sous sa surveillance).

Quel que soit le mode d'intervention, la présence de l'« autorité » est préconisée afin de s'assurer de la non-altération des dépôts et des traces déjà stockés.

Compte « admin »
Le compte « admin » possède un accès logique au socle système avec les droits d'un utilisateur de base, plus certaines fonctions d'administration accessibles via les commandes « *sudo* ».
La gestion des vulnérabilités du socle système doit faire l'objet d'une vigilance particulière. En effet, une élévation de privilège pourrait donner des informations sensibles à un utilisateur du compte « admin », comme les identifiants de connexion à la base de données.

Accès physique au poste
Aucun système de chiffrement du disque n'étant mis en place, l'équipement hébergeant l'application devrait être scellé afin de détecter toute ouverture physique illégitime du boîtier. Ce scellé devrait être vérifié lors de chaque audit de la plate-forme.

De plus, il est recommandé de protéger la séquence de démarrage du poste (BIOS et gestionnaire de démarrage) afin d'empêcher les élévations de privilèges.

Enfin, il est recommandé d'introduire dans la procédure de déchiffrement et de vérification de la signature des documents un contrôle de leur intégrité avant la validation du padding. A défaut de pouvoir mettre en place une telle mesure, il est recommandé de n'autoriser que les postes de confiance à envoyer des requêtes à l'oracle de validation du padding.

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

Afin d'assurer une utilisation sûre du produit, il doit être installé et configuré par Cecurity.com. Une fois ces opérations effectuées, l'utilisation du coffre-fort est simple et correctement décrite dans les guides fournis [GUIDES].

2.4. Analyse de la résistance des mécanismes cryptographiques

Le produit évalué offre les services cryptographiques suivants :
- authentification forte des déposants ;
- authentification forte des administrateurs ;
- chiffrement des événements ;
- signature des événements ;
- chaînage des événements.

Lors de l'installation du produit, le choix des protocoles et le paramétrage de certains algorithmes permettent de mettre en œuvre des algorithmes non-conformes au référentiel de l'ANSSI [REF-CRY].

Le développeur doit donc vérifier que la configuration qu'il met en place est conforme à ce référentiel.

Par ailleurs, certains mécanismes cryptographiques mis en œuvre par le produit ne sont pas conformes au référentiel [REF-CRY]. Cependant, les écarts constatés ne remettent pas en cause le niveau de résistance aux attaques visé par la CSPN.
Il est recommandé que ces mécanismes soient mis en conformité et qu'ils soient évalués lors d'une prochaine certification du produit. Des mesures organisationnelles doivent provisoirement être mises en place pour pallier ce manquement (§2.3.10.2).

2.5. Analyse du générateur d'aléas

Le générateur d'aléas a fait l'objet d'une analyse et est conforme au référentiel [REF-CRY] de l'ANSSI.

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 « Coffre-fort de jeux en ligne**,** Version 2.0 **»** soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [CDS].

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 d'exploitation spécifiés dans la cible de sécurité [CDS] et suivre les recommandations énoncées dans le chapitre 2.3.10.2 du présent rapport.

Annexe 1. Références documentaires du produit évalué

[CDS]	*Cible de sécurité CFJL ;* Référence : *Cecurity_CSPN_CibleSecurite_CFJL_Cecurity_100920.pdf* ; Date : *2010-20-09*
[RTE]	*CSPN : Rapport Technique d'Évaluation (RTE) ;* Référence *: OPPIDA/CESTI/CFJL/RTE/1.0*; Date : *17/12/2010*
[ANA-CRY]	*Rapport d'analyse des mécanismes crypotographiques ;* Référence *: OPPIDA/CESTI/CFJL/CRYPTO/1.0* ; Date : *19/12/2010*
[DET]	*Dossier des Exigences Techniques de l'ARJEL ;* Référence *: version 1.0* ; Date : *19/05/2010*
[GUIDES]	Manuel d'installation : *Manuel d'installation du logiciel CFJL ;* Référence : *CFJL_Manuel_Installation_20100927_Validé.pdf* ; Date : 27/09*/2010* Manuel d'exploitation : *Manuel d'exploitation du produit CFJL ;* Référence : *CC_CFJL_Exploitation_Generique_20101117validé.pdf* ; Date : *17/11/2010* Manuel d'utilisation : *Descriptif de l'API du service de versement d'évènements fourni par le logiciel CFJL* Référence : *CC_CFJL201_API_V1.0.pdf*

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 (CSPN) des technologies de l'information, version 2. 4, phase expérimentale, n° 915/SGDN/DCSSI/SDR/CCN du 25 avril 2008. Critères pour l'évaluation de sécurité de premier niveau des technologies de l'information, phase expérimentale, version 1. 4. Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE, phase expérimentale, version 1. 3. Documents disponibles sur www.ssi.gouv.fr
[REF-CRY]	Référentiel général de sécurité, version 1.0, annexe B1 : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20. Documents disponibles sur www.ssi.gouv.fr