Cecurity.com

PRESERVE DIGITAL TRUST

CFJL 3.0 CSPN - Cible de sécurité

Procédure Interne

+33 (0)1 56 43 37 37

75 rue Saint-Lazare
75009 Paris

www.cecurity.com

Paris, le 06 avril 2020

Version du document :	1.6	Nombre total de pages :	20
Statut du document :	☒ Validé	☐ Version finale	
Classification :	Restreint		
Objet :	CFJL V3.0 CSPN – Cible de sécurité		

Liste de diffusion :	☐ Externe - Clients	☒ Cecurity.com et auditeurs

Historique du document :

Date	Version	Rédacteur	Commentaires
19/07/2019	1.0	SLX	Sur la base de la cible de sécurité de la Version CFJL 2.5 datée 22/12/2014
22/07/2019	1.1	ABL	Mise en page et corrections éditoriales
22/07/2019	1.2	BRI	Proposition de compléments et corrections
23/07/2019	1.3	SLX	Prise en compte des remarques
30/07/2019	1.4	SLX	Finalisation
25/03/2020	1.5	SLX	Modifications
06/04/2020	1.6	SLX	Prise en compte des remarques

Sommaire

1. Identification du produit

Organisation éditrice	Cecurity.com
Lien vers l'organisation	https://www.cecurity.com/
Nom commercial du produit	Coffre-fort des jeux en ligne
Numéro de la version évaluée	3.0.0
Catégorie de produit	Stockage sécurisé

1.1. Références de documents publics utilisés

Référence	Clef	Nom de document
anssi-cspn-cer-p-01-certification_de_securite_de_premier_niveau_v2.0.pdf	CSPN	Certification de sécurité de premier niveau des technologies de l'information, ANSSI, version 2.0 du 6 sept. 2018
Arrêté du 27 mars 2015 : Cahier des charges opérateurs	ARRETE	Cahier des charges de l'Autorité de Régulation des Jeux en Ligne (ARJEL), NOR FCPB1505446A, Version de l'arrêté du 27 mars 2015
DET Version 1.2	DET	Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL), version 1.2 du 24 sept. 2012
Annexe DET Version 1.5.1	ANNEXE	Annexe au Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en

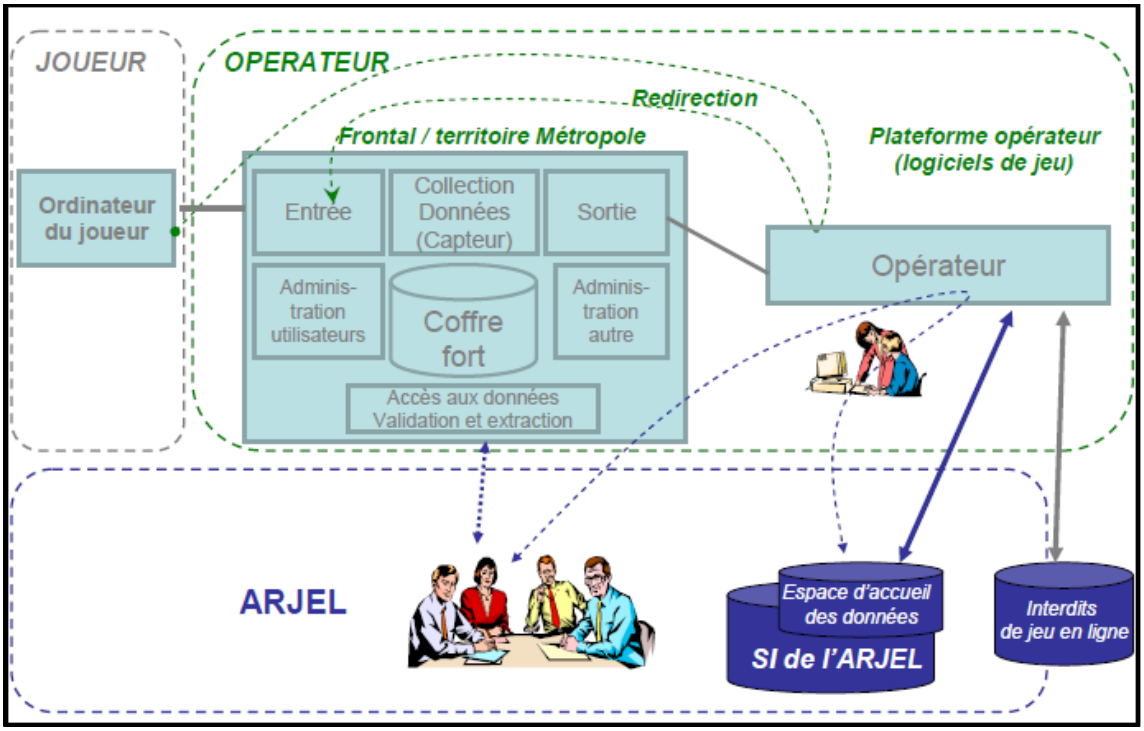
Référence	Clef	Nom de document
		Ligne (ARJEL), version 1.5.1 du 21 juin 2018
ISO 14721	OAIS	Norme ISO 14721:12
ETSI Portal	ETSI-POR	ETSI Portal Electronic Signatures and Infrastructures (ESI)
ETSI EN 319 132-1	ETSI-XAD1	XAdES baseline signatures
ETSI EN 319 132-2	ETSI-XAD2	Extended XAdES signatures

2. Argumentaire (description) du produit

2.1 Description générale du produit

Le Coffre-fort des Jeux en Ligne (CFJL) 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* » [DET, Page 5]

Le coffre-fort est une des composantes du frontal définit 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 frontal comporte également un capteur « *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* ».



Coffre-fort des jeux en ligne, frontal et capteur. Source : [DET]

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 produites 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.

Une instance du coffre-fort des jeux en ligne est limitée à un seul opérateur, identifié par son numéro unique.

Ce numéro unique est un élément des ressources de services déployés et est utilisé dans la convention de nommage de la base de données relationnelle.

Il ne peut pas être changé après le déploiement ou pendant le fonctionnement du service.

Les éléments de preuve produits par le Coffre-fort des Jeux en Ligne incluent les métadonnées d'archivage (notablement les dates d'archivage et les empreintes

des données archivées ...) ainsi que la journalisation des événements applicatifs ayant lieu dans le coffre-fort des jeux en ligne lors des échanges avec ses clients (versement d'événements de jeu, archivage, demandes et consultations de rapports …).

Les traitements réalisés par le coffre-fort des jeux en ligne vont permettre de :

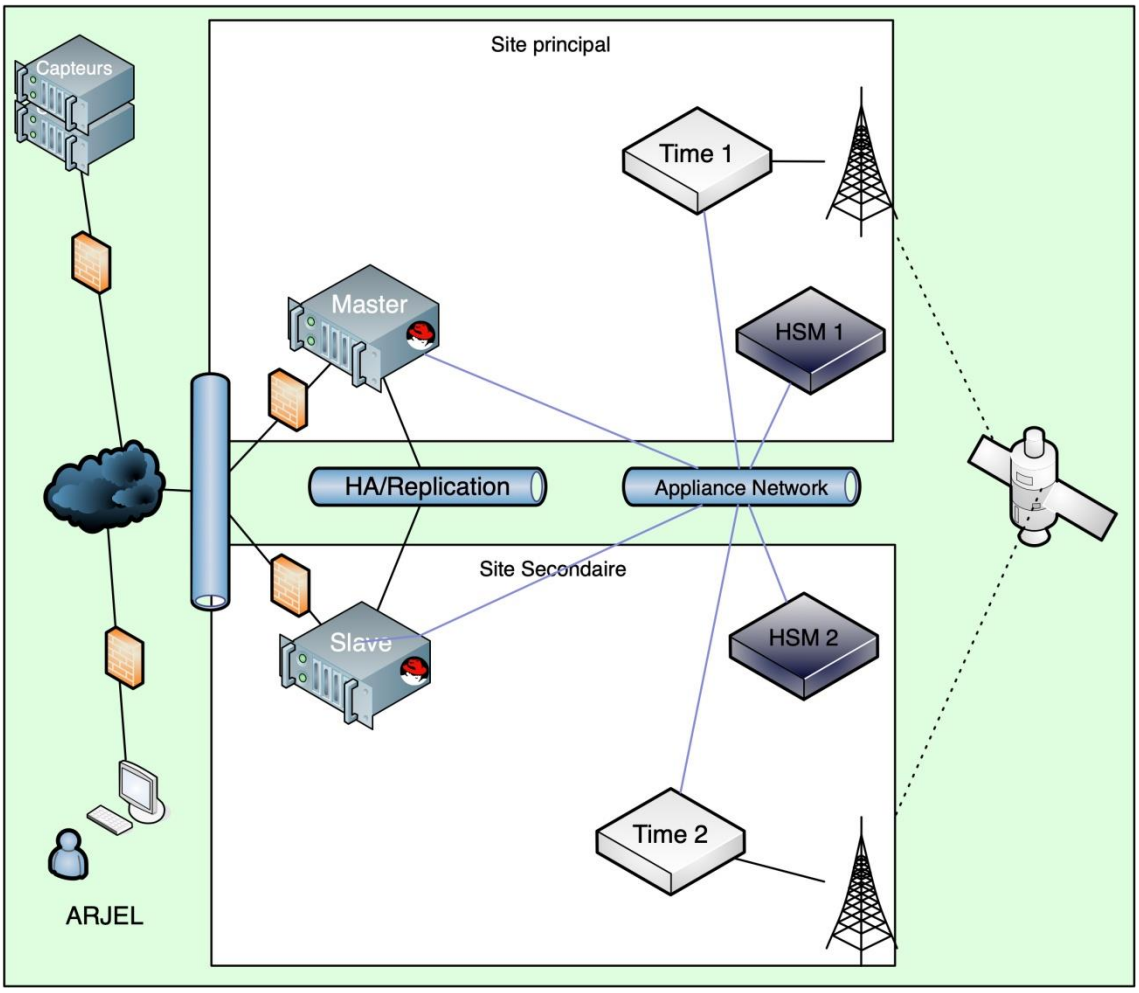
- fournir des éléments justificatifs dans un contexte de contrôle diligenté par les autorités publiques ;
- fournir des éléments de preuve dans un contexte de contentieux.

Le Coffre-fort des Jeux en Ligne a vocation à être utilisé dans un contexte global comprenant :

- la plateforme technique de jeux et son ou ses capteurs ;
- le coffre-fort lui-même ;
- la plateforme technique de l'ARJEL pour le contrôle puis le recueil des événements de jeu a posteriori ;
- l'autorité de certification de l'ARJEL pour la délivrance et la révocation des certificats.

Le contexte de production doit aussi être sécurisé et doit fonctionner avec un niveau élevé de fiabilité de sorte que la présence des fonctions d'archivage n'impacte pas de manière significative la disponibilité du service de l'opérateur de jeu.

Le schéma de la page suivante illustre la mise en œuvre d'un tel contexte de déploiement :



2.2 Description de la manière d'utiliser le produit

Toute entité utilisatrice du service d'archivage proposé par la plateforme du Coffre-fort des Jeux en Ligne doit être référencée par celui-ci. Un utilisateur doit donc être défini au niveau du coffre-fort. Cet utilisateur doit être associé à un rôle. Ce rôle définit les actions élémentaires autorisées vis-à-vis du coffre-fort : dépôt, consultation.

Pour utiliser le coffre-fort des jeux en ligne, l'entité utilisatrice s'authentifie auprès du Coffre-fort des Jeux en Ligne à travers un certificat électronique conforme à la norme X.509 v3 puis accède au Coffre-fort des Jeux en Ligne auprès duquel elle pourra, en fonction de son rôle et des droits qui lui ont été accordés :

- déposer un nouvel événement de jeu pour archivage ;
- recevoir des attestations de l'archivage des éléments versés ;
- obtenir une copie électronique conforme d'un ensemble d'événements de jeu archivés dans le Coffre-fort des Jeux en Ligne, accompagné des éléments de preuve correspondants ;

- obtenir des informations sur le statut du service et des requêtes effectuées précédemment.

2.3 Description de l'environnement prévu pour son utilisation

- Le coffre-fort des jeux en ligne fonctionne sous le système d'exploitation Linux sur l'architecture x86-64. En standard, la distribution retenue est la distribution *Red Hat Enterprise Linux Server* en dans la dernière révision disponible de la branche 7 (version 7.6 au moment de la rédaction de ce document) en fonction de la compatibilité du matériel utilisé pour le déploiement. Cet environnement est réputé avoir accès au service de diffusion des mises à jour de l'éditeur de la distribution, permettant la mise en œuvre des éventuels correctifs de sécurité et de stabilité.
- Le coffre-fort fonctionnera en connexion avec une *appliance* SafeNet Luna Network HSM proposé par la division SafeNet de la société Thales-Gemalto (Luna SA *firmware* 7.4, HSM firmware version 7.4.0). Ce boîtier contient un module HSM Luna PCIe.
- Le coffre-fort des jeux en ligne est connecté au HSM par un lien applicatif chiffré (TLS) utilisant une interface physique dédiée, soit à cette fonction seule, soit aux flux non applicatifs incluant les accès aux *appliances*, le monitoring et les accès administratifs.

2.4 Description des hypothèses sur l'environnement

Le coffre-fort des jeux en ligne doit être installé sur une plateforme technique (serveur informatique) dédié à cet usage.

Sur cette plateforme, le système d'exploitation doit être sain ; il doit être correctement et régulièrement mis à jour, avec un soin tout particulier concernant les correctifs liés à la sécurité et aux failles potentielles recensées.

Les utilisateurs du coffre-fort accèdent au service à travers un canal TLS et sont authentifiés au travers d'un certificat électronique conforme à la norme X.509 v3. Les administrateurs du Coffre-fort des Jeux en Ligne sont considérés comme de confiance et non hostiles.

- Initialisation

Il est supposé qu'une cérémonie d'initialisation du coffre-fort a été réalisée. Cette cérémonie a permis la génération des bi-clefs utilisées pour le scellement, la délivrance des certificats correspondant par l'ARJEL et leur mise en place, la configuration des accès pour les différents rôles avec leurs certificats électroniques respectifs.

- Audit

Il est supposé que l'auditeur peut consulter en permanence les événements de l'application inscrits dans le journal du coffre-fort des jeux en ligne.

- Alarme

Il est supposé que l'administrateur de sécurité analyse et traite les alertes de sécurité transmises par le diffuseur de la distribution linux pour les composants concernés.

- Administrateur

Les administrateurs sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration du Coffre-fort des Jeux en Ligne.

- Local

Les équipements (serveurs, baies techniques, …) sur lesquels est installé le coffre-fort des jeux en ligne ainsi que tous supports contenant les biens sensibles se trouvent dans des locaux sécurisés dont l'accès est contrôlé et restreint.

- Maîtrise de la configuration

L'administrateur dispose des moyens de contrôle de la configuration matérielle du Coffre-fort des Jeux en Ligne ce qui garantit la maîtrise du dispositif.

- Maîtrise du système

Le système d'exploitation supportant le Coffre-Fort des Jeux en Ligne et les différents constituants logiciels utilisés dans la solution sont correctement administrés et configurés. En particulier, les accès aux différents composants du Coffre-fort des Jeux en Ligne ne sont accessibles qu'aux seuls administrateurs autorisés. Seuls ces administrateurs désignés disposent des accès au système d'exploitation de la plate-forme technique dédiée à l'hébergement du coffre-fort des jeux en ligne.

- Source de temps

Le système utilise une source de temps de confiance. D'une part, une source de temps existe et elle dispose d'une référence temporelle considérée comme de confiance et d'autre part, le protocole utilisé entre cette source de temps et le système est sécurisé (réseau privé et protocole NTPv4).

2.5 Description des dépendances par rapport à des matériels, des logiciels et/ou des microprogrammes du système qui ne sont pas fournis avec le produit.

La source de temps de confiance accessible en NTPv4 doit être disponible. Le rôle de la PKI de l'ARJEL doit être assumé de manière externe pour la délivrance des certificats de chiffrement, de signature, d'horodatage, d'accès pour consultation et la fourniture des CRLs correspondantes.

Le rôle de la PKI de l'opérateur de jeu doit être assumé de manière externe pour la délivrance des certificats d'accès pour le déposant.

Outre le serveur hébergeant la solution, on doit disposer d'un environnement poste

client distinct pour la consultation, supportant une machine virtuelle java 11 et d'un environnement capteur pour déposer des événements.

Les composants suivants et leurs dépendances sont nécessaires au fonctionnement du service :

- Java Runtime Environnement version 11 LTS, version 11.0.4;
- Apache httpd 2.4.6, mod_ssl 2.4.6 et mod_jk 1.2.46;
- OpenSSL version 1.0.2k;
- OpenSSH 7.4p1;
- Tomcat 9.0.26.

Le Coffre-fort des Jeux en Ligne intègre des briques logicielles et des applications *open-source* existantes. Celles-ci servent de base pour les fonctionnalités attendues du dispositif. Les services applicatifs déployés incluent dans les mêmes packages les modules développés par Cecurity.com et des frameworks tiers.

Parmi les dépendances notables, les composants *open source* suivants sont utilisés par le Coffre-fort des Jeux en Ligne.

- Bouncycastle 1.62
- SD-DSS 5.4.3
- Apache ActiveMQ Artemis version 2.10.1
- Apache CXF 3.3.2
- Xerces java 2.11

Le Coffre-fort des Jeux en Ligne utilise également un gestionnaire de base de données relationnelle comme support des données prises en compte. En standard, le SGBDR PostgreSQL v11 (version 11.4 ou ultérieure) est utilisé.

On suppose que les composants énumérés ci-dessus sont installés dans des versions packagées par la distribution incorporant les correctifs de sécurité publiés ou dans la sous version mineure connue pour incorporer les correctifs de sécurité. En matière d'environnement réseau, le serveur sur lequel est installé le Coffre-fort des Jeux en Ligne doit disposer au minimum de deux liens physiques distincts, permettant de séparer les flux applicatifs des autres accès.

Il doit :

- être accessible depuis les serveurs et les postes clients en liste blanche, HTTPS (443/tcp); (flux applicatif) ;
- être accessible depuis les serveurs de l'opérateur de jeu en liste blanche sur le port 6163 en openwire/TLS (flux applicatif) ;
- doit pouvoir effectuer des requêtes vers des services de temps et recevoir des réponses (protocole NTP, port 123/udp) ;
- accéder au HSM ;
- disposer d'un accès SSH avec authentification par clef uniquement.

A l'exclusion de ces besoins, tous les autres ports d'accès TCP/IP peuvent être fermés ce qui par là même va permettre de limiter les conséquences d'éventuelles failles de sécurité et les risques d'intrusion sur la plateforme. Le filtrage IP peut-être porté par un équipement externe dédié pour un logiciel intégré au système d'exploitation, selon les modalités de déploiement choisies.

2.6 Description des utilisateurs typiques concernés (utilisateurs finaux, administrateurs, experts …) et de leur rôle particulier dans l'utilisation du produit.

Utilisateurs dans le contexte d'usage du secteur des jeux d'argent en ligne (d'après le Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL) page 11)

- profil « déposant » : profil attribué au module « capteur » du frontal de l'opérateur. Il permet uniquement de verser des événements dans le coffre-fort Serveur de preuves. Le module « capteur» du frontal s'authentifie à l'aide d'un certificat X.509v3 auprès du coffre-fort avec une identité associée à ce profil ;
- profil « lecteur » : profil attribué aux agents de l'ARJEL dotés des pouvoirs de contrôle et d'audit, qui permet l'extraction des données enregistrées. Les certificats associés à ce profil sont utilisés :
    - soit par des personnes physiques, pour les contrôles réalisés sur site, avec des bi clefs RSA et un certificat X.509v3 d'authentification ;
    - soit par des agents de collecte, pour les consultations réalisées à distance, avec une authentification fondée sur un certificat X.509v3 client SSL/TLS, dans le cadre de la négociation d'un canal SSL/TLS mutuellement authentifié ;
- profil « administrateur technique et opérationnel » : profil attribué au personnel technique de l'opérateur, responsable de l'administration et de la supervision technique du coffre-fort (authentifié par bi clef RSA), par exemple : arrêt/démarrage, consultation des journaux techniques, notamment en termes de traçabilité des accès locaux et distants, de gestion des erreurs, etc;
- profil « administrateur fonctionnel » : profil attribué aux personnes physiques de l'ARJEL ou désignées par l'ARJEL, authentifié par bi-clef RSA, qui peuvent définir des rôles et leur associer un certificat d'authentification. Cette opération est nécessaire à l'initialisation des coffres, puis lors des renouvellements ou des révocations des certificats.

2.7 Définition du périmètre de l'évaluation, à savoir les caractéristiques de sécurité du produit concernées par l'évaluation.

L'évaluation portera sur les fonctionnalités d'authentification forte, de chiffrement des données et de vérification de l'intégrité et de l'exhaustivité des données archivées dans le coffre-fort des jeux en ligne. L'exhaustivité des données archivées sera notamment évaluée au niveau des outils de recueil et d'extraction

à usage de l'ARJEL. Voir courrier du président de l'ARJEL aux opérateurs de jeu agréés en date du 15 mai 2014.

3. Description de l'environnement technique dans lequel le produit doit fonctionner

- Matériel compatible ou dédié - Système d'exploitation compatible : type, version, correctifs…

Le Coffre-fort des Jeux en Ligne est implémenté sur un serveur dédié dont les caractéristiques sont les suivantes : processeurs de type Intel x86_64, disques SATA ou SAS, stockage en DAS (*Direct Attachment Storage*), SAN (*Storage Area Network*) ou NAS (*Network Attachment Storage*).

C'est un programme automatique de dépôt (mode API) qui procède au dépôt des données dans le coffre-fort.

4. Description des biens sensibles que le produit doit protéger

Il y a deux types de biens sensibles à protéger :

Les biens sensibles utilisateurs :

- les événements de jeu versés par l'opérateur de jeu de ligne. Ceux-ci doivent être protégés en intégrité, confidentialité et seuls les utilisateurs habilités peuvent y accéder ;
- les éléments de preuves (authentification du déposant de l'archive, horodatage du dépôt, empreintes d'intégrité des données fichier archivé, scellement, journaux probants de l'application). Ceux-ci doivent être protégés en intégrité, confidentialité et seuls les utilisateurs habilités peuvent y accéder.

Les biens sensibles du produit :

- les informations d'authentification des utilisateurs (identifiant, habilitations). Ceux-ci doivent être protégés en confidentialité et seuls les utilisateurs habilités peuvent y accéder ;
- la base de temps du système. Elle doit être protégée en intégrité;
- les secrets cryptographiques. Ceux-ci doivent être protégés en intégrité, confidentialité et seuls les utilisateurs habilités peuvent y accéder.

5. Description des menaces

Dans le contexte d'usage du secteur des jeux d'argent en ligne, les agents de l'ARJEL ne sont pas considérés comme des attaquants potentiels.

5.1 Agents menaçants

Dans ce cadre, les agents menaçants sont :

- les attaquants internes à un opérateur de jeux en ligne à l'exclusion des administrateurs opérationnels et techniques considérés comme de confiance ;
- les attaquants externes (utilisateurs/joueurs des services de jeux en ligne proposés par l'opérateur ou autres) ne disposant pas d'accès direct à la plateforme du coffre-fort des jeux en ligne.

5.2 Menaces

- dépôt ou injection d'événement de jeu ;
- perte des données archivées ou des preuves d'intégrité ;
- altération d'enregistrements ;
- vol de données;

6. Description des fonctions de sécurité du produit

Dans le contexte d'usage du secteur des jeux d'argent en ligne, les fonctions de sécurité sont les suivantes :

- Authentification forte des utilisateurs déposants

Le Coffre-fort des Jeux en Ligne met en place un mécanisme d'authentification lui permettant de s'assurer que les utilisateurs déposants sont biens autorisés à y accéder. Ceux-ci sont détenteurs d'un certificat d'authentification client et de la clef privée associée. Ce certificat doit être validé par les autorités de certification configurées sur le serveur pour accéder au service. Le sujet du certificat doit correspondre à ceux référencés sur le serveur pour le profil déposant.

- Chiffrement des événements

La confidentialité des événements de jeu conservés par le système est assurée par un dispositif de chiffrement électronique. Le mécanisme de chiffrement s'appuie sur la mise en place d'un algorithme de chiffrement asymétrique. Pour cette fonctionnalité, une bi-clef contenant une clef publique et une clef privée est produite par l'autorité de régulation (ARJEL) destinataire finale et utilisatrice du système. La clef publique est utilisée pour le chiffrement des événements qui sont conservés sous forme chiffrée. Seule l'ARJEL qui possède la clef privée est en mesure de les déchiffrer et d'accéder au contenu en clair.

- Scellement des événements

Afin de sécuriser la production et le suivi des événements, le Coffre-fort des Jeux en Ligne intègre un dispositif de scellement électronique des données archivées. Au travers de cette fonctionnalité l'intégrité individuelle de chaque événement peut être vérifiée. Le mécanisme de signature électronique utilisé s'appuie sur le format de signature XML avancée de type XAdES-T. La fonction cryptographique de calcul de la signature value avec la clef RSA est effectuée au sein du HSM à l'aide de la clef privée et du certificat de signature associé qui y sont conservés.

- Chaînage des événements

Le Coffre-fort des Jeux en Ligne intègre une fonctionnalité permettant de s'assurer de l'exhaustivité des événements de jeu archivés. Cette fonctionnalité s'appuie sur le chaînage sécurisé des éléments archivés. Chaque lot d'événements archivé est scellé (processus de signature électronique XAdES-T). Le scellement permet d'assurer la complétude et l'intégrité du ou des événement(s) conservé(s) dans le lot. Tous les événements de jeu sont numérotés avec des entiers naturels consécutifs, conformément aux exigences du [DET]. De plus, le scellement d'un lot incorpore l'empreinte de la signature du lot antérieur. L'omission d'une partie des événements de jeu archivés serait donc détectable lors de la consultation de la période concernée, à l'extérieur du service d'archivage, à la fois par l'absence des numéros de série d'événements correspondants et l'invalidité des signatures utilisées pour le scellement. Il est possible de vérifier l'intégralité des données

archivées en consultant le stock par segments avec un recouvrement pour vérifier la cohérence de la restitution.

- Horodatage de la signature

La signature électronique réalisée est horodatée. Cet horodatage utilise un jeton conforme à la norme RFC 3161 ; Les certificats de signature et d'horodatage sont délivrés par la PKI du régulateur. Selon les dispositions de ETSI EN 319 132-1 V1.1.1 §5.3, le jeton d'horodatage sur le contenu de la signature value est créé par une autorité d'horodatage embarquée et inclus dans la structure XAdES sous l'élément <SignatureTimeStamp>. L'opération de signature du jeton d'horodatage est effectuée au sein du HSM à l'aide de la clef privée et du certificat d'horodatage qui y sont conservés. La source de temps utilisée pour l'horodatage est délivré par l'horloge du système, dans un contexte dans lequel sa dérive fait l'objet d'un contrôle direct par le composant d'horodatage.

- Protection des secrets cryptographiques

Les bi-clefs utilisées pour la signature et l'horodatage de la signature sont générées et conservées au sein du HSM.

- Protection des journaux d'évènements applicatifs

Les événements applicatifs du coffre-fort des jeux en ligne sont écrits dans un journal. Celui-ci est constitué d'une série de fichiers journaux successifs, qui sont clôturés à intervalles réguliers par une tâche planifiée. Les fichiers journaux clôturés sont scellés au moyen d'une signature CMS insérée dans un fichier XML de métadonnées d'archivage associé à chaque fichier journal.

- Fonctions de sécurité et moyens cryptographiques

Fonction de sécurité protégeant les biens utilisateurs	
Fonction de sécurité	**Moyens cryptographiques**
Authentification forte des utilisateurs déposants	Certificat électronique X.509v3
Chaînage des évènements	Algorithme de hachage SHA256

Chiffrement des événements	Algorithmes de chiffrement RSA et AES256
Scellement des événements	Signature électronique XAdES-T
Horodatage de la signature	Jeton d'horodatage RFC 3161
Fonction de sécurité protégeant les biens du produit	
Fonction de sécurité	**Moyens cryptographiques**
Protection des journaux d'événements du coffre-fort des jeux en ligne	Signature électronique CMS
Protection des secrets cryptographiques	Encapsulation PKCS#12, HSM.

7. Annexe - Cadre d'utilisation

Le schéma ci-après expose l'architecture applicative du service Coffre-fort.