20 septembre 2010

CIBLE DE SECURITE CSPN – COFFRE-FORT DES JEUX EN LIGNE

Sommaire

1. Identification du produit

Organisation éditrice	Cecurity.com
Lien vers l'organisation	http://www.cecurity.com/
Nom commercial du produit	Coffre-fort des jeux en ligne
Numéro de la version évaluée	V 2.0
Catégorie de produit	Stockage sécurisé

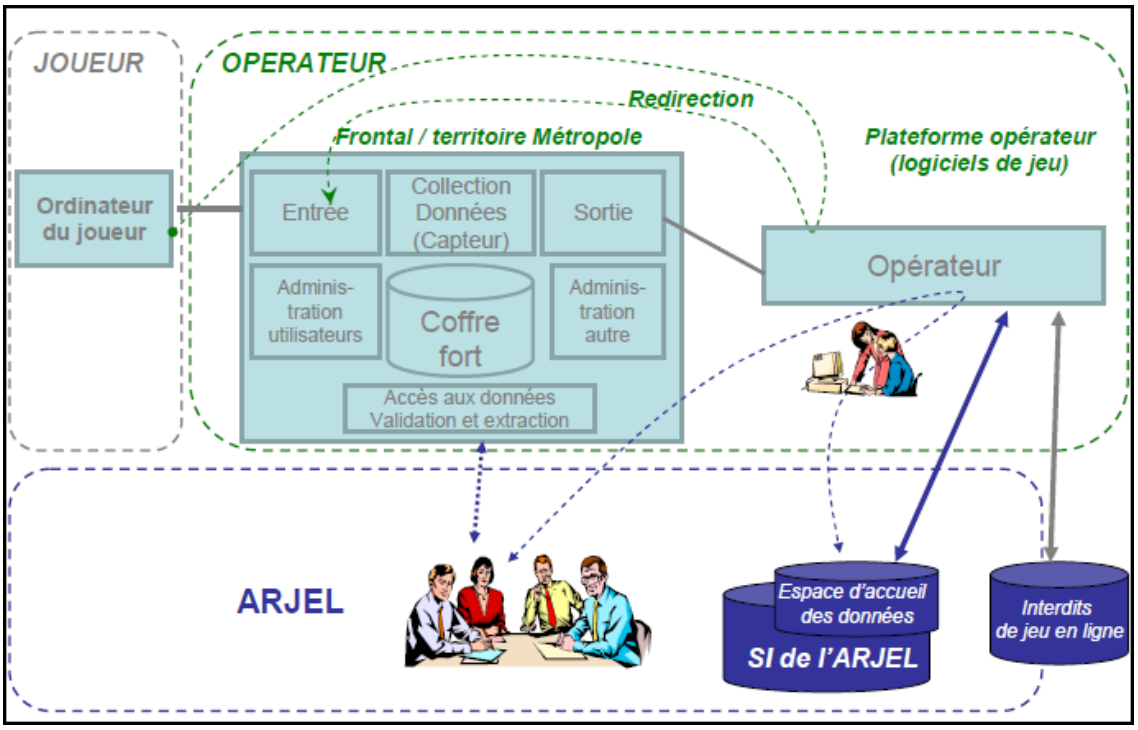
Références de documents publics utilisés	
Référence	**Nom de document**
N°915/SGDN/DCSSI/SDR du 25 avril 2008	Certification de sécurité de premier niveau des technologies de l'information, ANSSI
Version diffusée sur le site http://www. arjel.fr/	Cahier des charges de l'Autorité de Régulation des Jeux en Ligne (ARJEL)
Version 1.0	Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL)
Version 1.0	Annexe au Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL)
V.2006-11-29	ANSSI Archivage électronique sécurisé - L'état de l'art juridique, technique, organisationnel et des offres - ArchivageSecurise-EtatDeLArt-2006-11-29.pdf
Norme NF Z42-013 : 2009	Norme AFNOR pour l'archivage électronique
Référentiel FNTC V 11-5	Fédération Nationale des Tiers de Confiance - Référentiel définissant un coffre-fort électronique pour l'archivage à vocation probatoire d'objets numériques

2. Argumentaire (description) du produit

a. Description générale du produit

Le coffre-fort des jeux en ligne 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* » (source : Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL))

Le coffre-fort est une des composante 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 : Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL))

Le coffre-fort des jeux en ligne permet donc la conservation à des fins de contrôle d'éléments de preuves nativement électroniques déposés par un opérateur de jeux et paris en ligne client du système.

> NB : Afin de simplifier la lecture du présent document, les éléments de preuve déposés par le client dans le coffre-fort seront notés éléments de preuves externes (EPE) afin de les distinguer des éléments de preuves internes (EPI) mis en place nativement par le coffre-fort à des fins de traçabilité et de conservation sécurisée des EPE archivés.

Le coffre-fort des jeux en ligne permet :

- d'archiver des éléments de preuve externes (EPE);
- d'obtenir des copies électroniques conformes des éléments de preuve externes (EPE) archivés ;
- d'archiver ses propres éléments de preuve internes (EPI) relatifs à la conservation sécurisée des EPE archivés.

Le produit doit protéger l'accès à tous les éléments de preuves (EPE et EPI) ainsi que leur complétude et leur intégrité.

Les éléments de preuve externes sont liés aux clients et/ou aux applications clientes du coffre-fort des jeux en ligne.

Les éléments de preuve internes (EPI) sont liés au coffre-fort des jeux en ligne lui-même. Ils correspondent aux événements ayant lieu concernant coffre-fort des jeux en ligne et les échanges avec ses clients (dépôt, retrait de copie conforme, création d'utilisateurs, attributions de rôles, …).

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

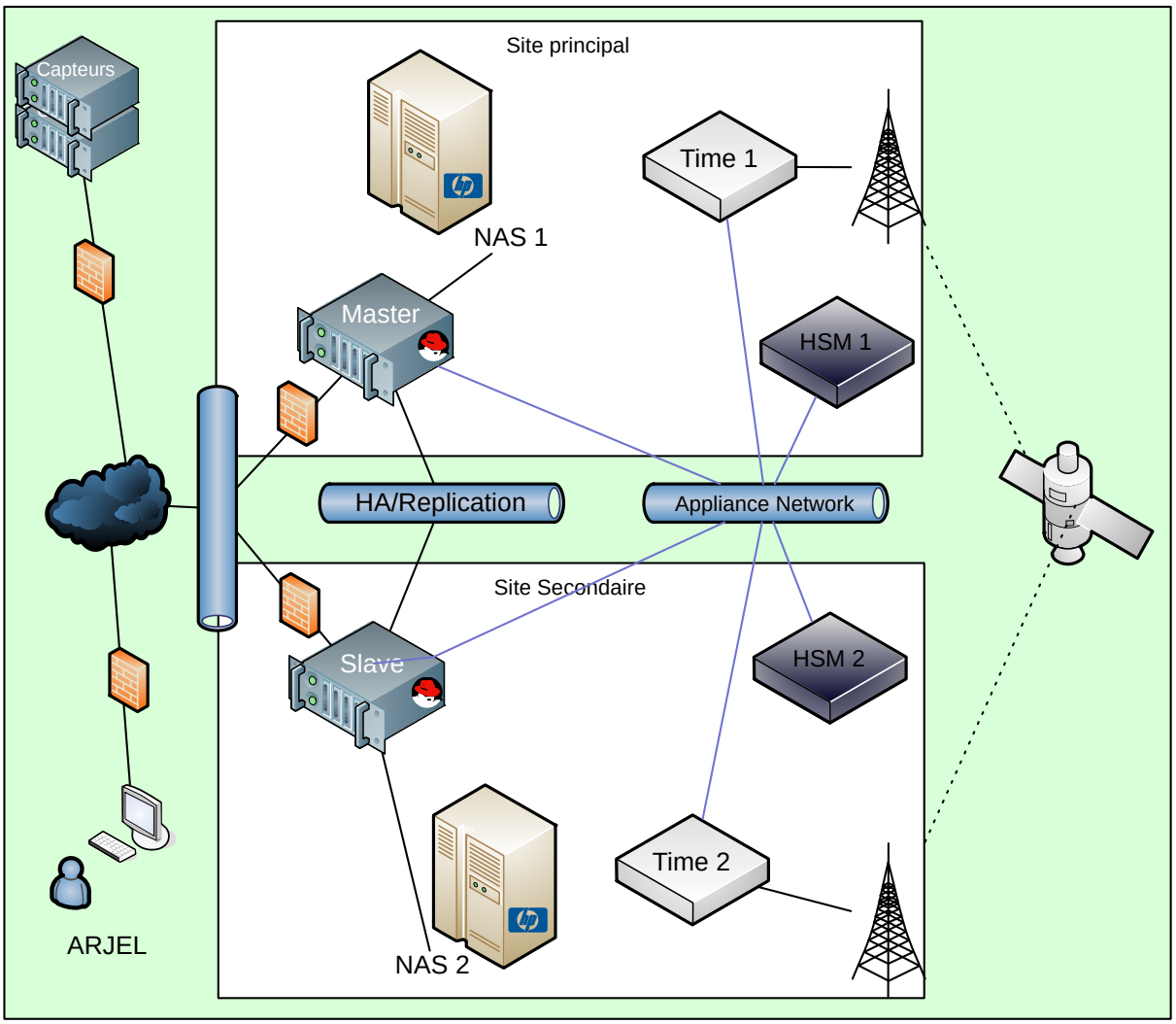
- Fournir des éléments justificatifs dans un contexte de contrôle diligenté par les autorités publiques.
- Fournir des éléments de preuve dans un contexte de contentieux ;

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 jeux 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 traitement :



b. Description de la manière d'utiliser le produit

Toute entité utilisatrice du service de conservation 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 élément de preuve externe pour archivage ;
- obtenir une copie électronique conforme d'un ensemble d'éléments de preuve externes archivés dans le coffre-fort des jeux en ligne, accompagné des éléments de preuve internes correspondants ;
- obtenir des informations sur le statut du service et des requêtes effectuées précédemment.

c. 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 en version 5.4 ou 5.5 en fonction de la compatibilité du matériel utilisé pour le déploiement.

Une autre distribution (CentOS 5.4 ou 5.5) a été validée.

Le coffre-fort fonctionnera en connexion avec une appliance HSM Luna SA de la société SafeNet. Ce boitier contient une carte HSM cryptographique Luna PCI.

Les versions 4.1 et 4.4 du logiciel du boitier Luna SA.

Le coffre fort des jeux en ligne est connecté au HSM par un lien applicatif chiffré (SSL) 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.

d. 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 SSL/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 clefs de signature, 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 (c'est-à-dire des éléments de preuve interne - EPI) générés par le journal de traçabilité 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 du 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 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 (protocole NTPv4).

e. 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 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 le runtime java 1.6 et d'un environnement capteur pour déposer des événements.

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

- Java Runtime Environnement 1.6.0_18 ou version ultérieure
- Apache 2.2.3 avec mod_ssl 2.2.3 et mod_jk 1.2.28
- OpenSSL version 0.98 ou ultérieure
- Tomcat 6.0.28 ou version ultérieure

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. L'installation du coffre-fort des jeux en ligne nécessite la présence des jars des packages de Cecurity.com et des tierces.
Parmi les dépendances notables, les composants opensource suivants sont utilisés par le coffre-fort des jeux en ligne.

- Bouncycastle 1.43
- Xerces java 2.9.1
- Xalan java 2.7.1
- XMLSecurity java 1.4.3
- Apache CXF 2.2.9
- Apache ActiveMQ 5.3.2

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 SGBD PostgreSQL V8.4.3 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 en liste blanche sur le port 6163 en openwire/SSL (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.

f. 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 d'écrire des éléments de preuves externes 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.

g. 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.

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 EPE fournis par l'utilisateur.
- Les éléments de preuves internes (EPI) (authentification du déposant de l'archive, horodatage de l'archivage, empreinte calculée par le coffre-fort du fichier archivé).

Les biens sensibles du produit :

- Les informations d'authentification des utilisateurs (identifiant, habilitations) ;
- La base de temps du système ;
- Les secrets cryptographiques.

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.

Agents menaçants

Dans ce cadre, les agents menaçants sont :

- Les attaquants internes à un opérateur de jeux en ligne ;
- Les attaquants externes utilisateurs des services de jeux en ligne proposés par l'opérateur (joueurs) ne disposant pas d'accès direct à la plateforme du coffre-fort des jeux en ligne.

Menaces

- Dépôt ou injection d'enregistrements (EPE dans le contexte de la présente cible de sécurité) ;
- Altération d'enregistrements ;
- Vol de données ;
- Déni de service.

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 (Source : Dossier des Exigences Techniques de l'Autorité de Régulation des Jeux en Ligne (ARJEL) page 11) :

- Authentification forte des déposants

  Le coffre fort des jeux en ligne met en place un mécanisme d'authentification lui permettant de s'assurer que les déposants qui se présentent au coffre-fort des jeux en ligne sont bien autorisés à y accéder.

- Authentification forte des administrateurs

  Le coffre fort des jeux en ligne met en place un mécanisme d'authentification lui permettant de s'assurer que les administrateurs qui se présentent au coffre-fort des jeux en ligne sont bien autorisés à y accéder.

- Chiffrement des événements

  La confidentialité des événements produits et conservés par le système est assurée par un dispositif de chiffrement électronique des événements. Le mécanisme de chiffrement s'appuie sur la mise en place d'un algorithme de chiffrement asymétrique. Pour cette fonctionnalité, un bi-clef contenant une clef publique et une clef privée est produit 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 ;

- Signature des événements

  Afin de sécuriser la production et el suivi des événements, le coffre-fort des jeux en ligne intègre un dispositif de signature électronique des événements. Au travers de cette fonctionnalité l'intégrité individuelle de chaque événement peut être vérifiée. Le mécanisme de signature électronique utilisé s'appuie sur la norme de signature XML étendue XAdES-T. La signature électronique réalisée est horodatée et l'horodatage utilise un jeton conforme à la norme RFC 3161 ; Les certificats de signature et d'horodatage sont délivrés par l'ARJEL.

- Chaînage des événements

  Le coffre-fort des jeux en ligne intègre une fonctionnalité permettant de s'assurer de l'exhaustivité des événements EPE produits et conservés. Cette fonctionnalité s'appuie sur le chaînage sécurisé des événements EPE. Comme indiqué dans le paragraphe concerné, chaque événement produit est signé (processus de signature électronique XAdES-T). Par le processus mis en place, la signature en question protège à la fois le contenu de l'événement mais également le lien avec l'événement précédent. En effet, pour chaque événement, une empreinte est produite à partir des champs descriptifs dudit événement et de l'empreinte de la signature électronique de l'EPE précédent. Ce processus conduit donc à la mise en place d'un chaînage sécurisé des

événements. Par construction la sécurisation est double : à la fois individuelle au travers le la signature et globale au travers du lien inter-événements. L'exhaustivité et l'intégrité du stock des EPE sont donc assurés puisque tout ajout, suppression ou modification d'un ou de plusieurs EPE serait détectable au moment de la consultation ;

Fonctions de sécurité et moyens cryptographiques

Fonction de sécurité protégeant les biens utilisateurs	
Fonction de sécurité	**Moyens cryptographiques**
Authentification forte des utilisateurs	Certificat électronique X.509v3
Authentification forte des administrateurs	bi-clef RSA
Chaînage des évènements	Algorithme de hachage SHA256
Chiffrement des évènements	Algorithmes de chiffrement RSA et AES256
Signature des évènements	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 XAdES-T
Protection des secrets cryptographiques	Encapsulation PKCS#12, HSM.

Annexe - Cadre d'utilisation

Le schéma ci-après expose le cadre d'utilisation typique du coffre-fort des jeux en ligne