AUTORITE DE REGULATION DES JEUX EN LIGNE

OUVERTURE A LA CONCURRENCE ET A LA REGULATION DU SECTEUR DES JEUX D'ARGENT EN LIGNE

DOSSIER DES EXIGENCES TECHNIQUES

Visé par l'article 11 du Décret n° 2010-509 du 18 mai 2010
relatif aux obligations imposées aux opérateurs agréés de jeux ou de paris en ligne
en vue du contrôle des données de jeux par l'Autorité de régulation des jeux en ligne

Version 1.0

SOMMAIRE

1 INTRODUCTION : CONTEXTE ET PERIMETRE DU DOCUMENT

Le présent document décrit le dispositif technique à mettre en place par les opérateurs. Il comprend en particulier les volets archivage de données et fourniture de données par les opérateurs agréés. Il précise également les différents éléments techniques devant être fournis pour la demande d'agrément.

2 DEFINITIONS ET ACRONYMES

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information.

ARJEL : Autorité de régulation des jeux en ligne.

Capteur : le capteur est un élément constitutif du frontal, 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.

CCTP : Cahier des Clauses Techniques Particulières.

CERTA : Centre d'Expertise gouvernemental de Réponse et de Traitement des Attaques informatiques.

Certification : la certification permet à un client de s'assurer par l'intervention d'un professionnel indépendant, compétent et contrôlé, appelé organisme certificateur, de la conformité d'un produit à un référentiel.

Cible de sécurité : la cible de sécurité est le document décrivant en particulier les fonctionnalités de sécurité du produit qui font l'objet de l'évaluation et de la certification.

Coffre-fort : le coffre-fort est un élément constitutif du frontal, 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.

Compte joueur : un compte de joueur en ligne est le compte attribué à chaque joueur par un opérateur de jeux ou de paris en ligne pour un ou plusieurs jeux. Il retrace notamment les mises et les gains liés aux jeux et paris, les mouvements financiers qui leur sont liés, ainsi que le solde des avoirs du joueur auprès de l'opérateur.

CSPN : Certification (ou Certificat) de Sécurité de Premier Niveau : c'est le label de premier niveau pour les produits de sécurité des systèmes d'information, attestant que le produit a subi avec succès une évaluation par des centres d'évaluation agréés par l'ANSSI.

FAQ : Foire Aux Questions (Frequently Asked Questions) : c'est un ensemble structuré de questions et de réponses.

Frontal : support matériel prévu à l'article 31 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouvertu re à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne (« la Loi »). Le frontal est 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.

Joueur en ligne : un joueur ou un parieur en ligne s'entend de toute personne qui accepte un contrat d'adhésion au jeu proposé par un opérateur de jeux ou de paris en ligne.

Logiciel de jeu : le logiciel de jeu est l'application ou programme mis à disposition par l'opérateur aux utilisateurs afin d'interagir avec la plateforme de jeux. Il peut (ou non) comporter une composante logicielle chez l'utilisateur.

Opérateur : l'opérateur de jeux ou de paris en ligne est toute personne qui, de manière habituelle, propose au public des services de jeux ou de paris en ligne comportant des enjeux en valeur monétaire et dont les modalités sont définies par un règlement constitutif d'un contrat d'adhésion au jeu soumis à l'acceptation des joueurs.

Pare-feu : c'est le dispositif informatique qui filtre les flux d'informations entre un réseau interne à un organisme et un réseau externe en vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur.

Parieur en ligne : voir joueur en ligne.

Plateforme : la plateforme (de jeu) est le système d'information principal de l'opérateur dédié à une activité de jeu en ligne ou de pari en ligne, il s'agit des moyens matériels et logiciels qui assurent plus particulièrement la gestion complète des opérations de jeux ou de paris en ligne.

RSSI : Responsable de la Sécurité des Systèmes d'Information.

Sécurité des Systèmes d'Information : la sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information.

Site Internet : site Internet dédié, exclusivement accessible par un nom de domaine de premier niveau comportant la terminaison « .fr », mis en place par l'opérateur en vue des jeux ou paris en ligne faisant l'objet de l'agrément.

Source de temps fiable : une source de temps est fiable si l'écart avec le temps UTC est inférieur à une seconde, et si elle n'est pas modifiable.

SSI : voir à Sécurité des Systèmes d'Information.

Système d'Information (SI) : c'est l'ensemble des composants, aux niveaux système, réseau et applicatif et plus généralement, tout système ou application susceptible d'interagir avec les plates-formes de jeux de l'opérateur.

Terminal Internet : le moyen du joueur pour accéder à Internet. En général, il s'agit d'un ordinateur, mais il peut également par exemple être un téléphone, une télévision interactive, etc ; à la condition que le moyen permette un accès direct du joueur au site Internet.

3 PRESENTATION GENERALE DE L'ARCHITECTURE

3.1 BESOINS DE L'ARJEL

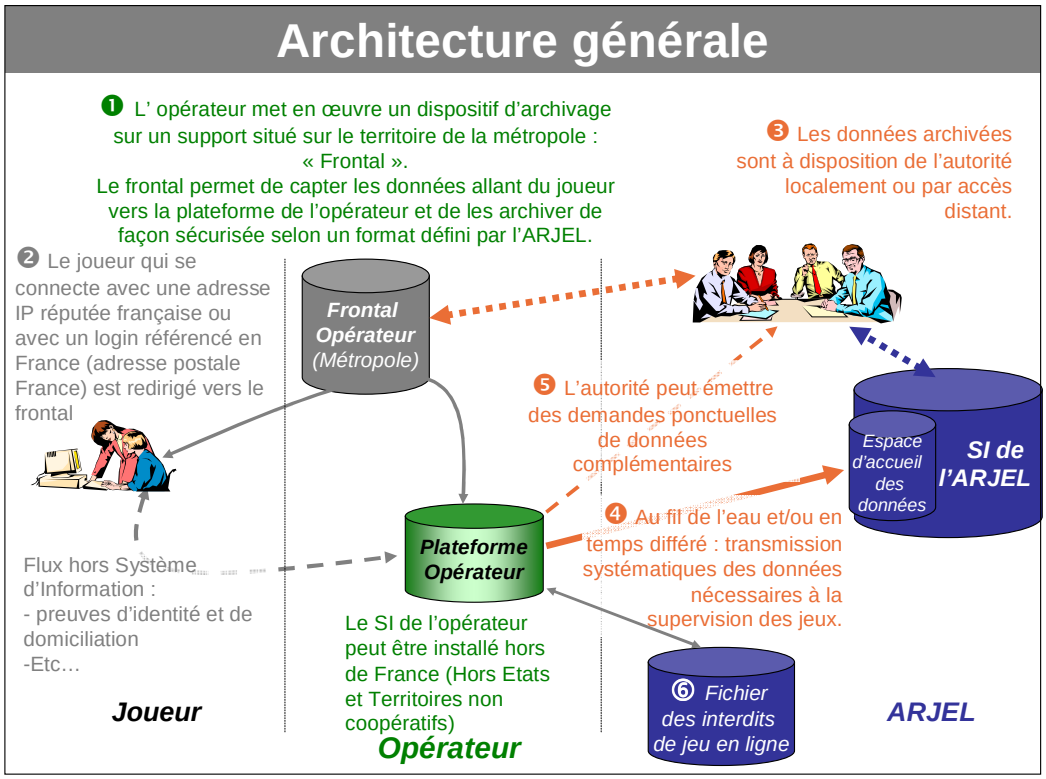
Pour accomplir sa mission de supervision et de contrôle du marché des jeux en ligne, l'ARJEL a besoin de s'appuyer sur des informations disponibles chez les opérateurs.
La loi prévoit que chaque agrément donne lieu à la mise en place d'un dispositif technique qui permet de garantir une traçabilité des opérations de jeu d'une part, et de générer et de transmettre des rapports sur l'activité de jeu d'autre part.

3.2 ARCHITECTURE GENERALE

Le schéma suivant présente les différents éléments de l'architecture et les principes d'archivage et de transmission des données :

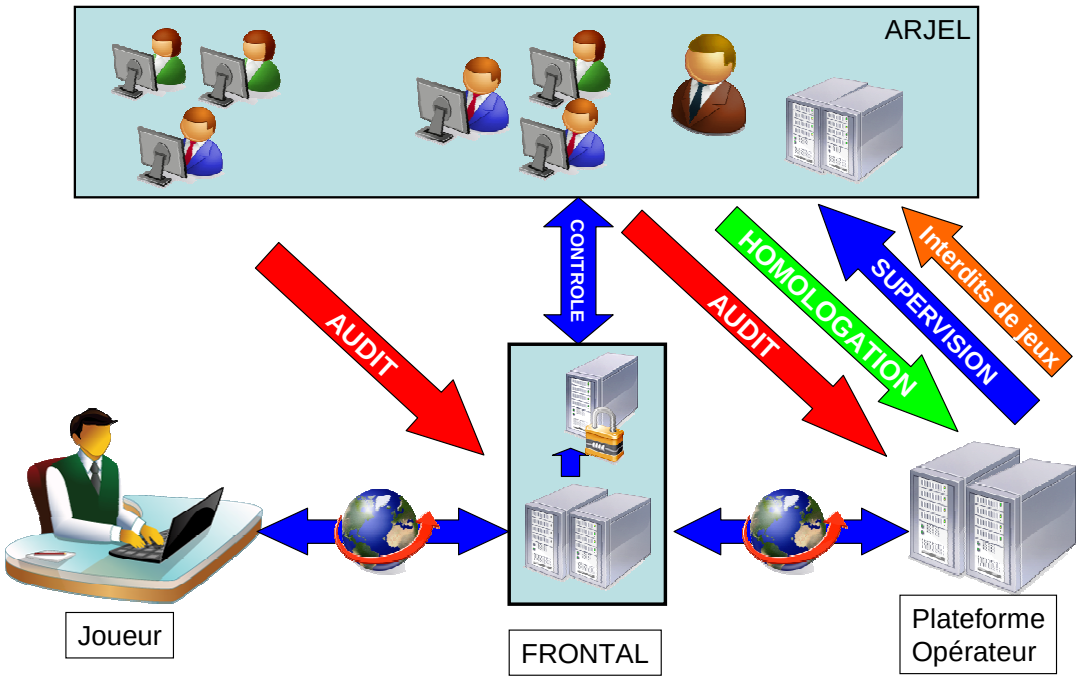
- l'opérateur met en place un dispositif appelé Frontal ❶ qui recueille et archive les transactions allant du joueur vers la plate-forme de jeu (dans ce sens exclusivement) de manière sécurisée (cf. partie 4.1) ;
- toute connexion d'un joueur réputé français à la plate-forme de jeu devra être redirigée vers ce Frontal, ainsi que les données échangées ultérieurement entre le joueur et la plate-forme ❷. Ces données devront être stockées dans un format spécifique défini par l'ARJEL (cf. Annexe 1) et restent à disposition de l'ARJEL localement ou par accès distant ❸ ;
- d'autre part l'opérateur devra transmettre à l'ARJEL, périodiquement ❹ (cf. partie 4.2 et Annexe 2) ou à la demande ❺ (cf. partie 4.3) des données nécessaires à la supervision des jeux ;
- finalement l'opérateur devra interroger le fichier des interdits de jeu ❻ et le cas échéant bloquer le compte de ses clients qui y figurent.

Chacun de ces éléments est détaillé dans les pages suivantes.



3.3 SCHEMA GENERAL D'INTERACTION ENTRE L'ARJEL ET LES OPERATEURS

Les différents éléments présentés sont détaillés dans les pages qui suivent.



Le schéma ci-dessus résume les interactions entre l'opérateur ayant obtenu un agrément et l'ARJEL :

- ✓ dans le cadre de la mission générale de contrôle de l'ARJEL, des audits périodiques ou à la demande seront réalisés au niveau du frontal et de la plate-forme opérateur. Ils seront effectués dans un cadre coopératif avec les opérateurs et des recommandations techniques ou organisationnelles leurs seront proposées afin de remédier aux vulnérabilités identifiées ;
- ✓ les logiciels de jeu seront soumis à une homologation afin de vérifier leur niveau de sécurité et le respect des règles du jeu concerné ;
- ✓ les éléments contenus dans le coffre-fort seront accessibles à distance et sur site à la demande afin d'effectuer les différentes opérations de contrôle nécessaires ;
- ✓ l'ARJEL demande la fourniture par l'opérateur de données de supervision, soit de façon systématique, soit à la demande ;
- ✓ l'ARJEL demande la fourniture par l'opérateur de données « à la demande » en fonction de ses différents besoins ;
- ✓ enfin, les opérateurs devront lors de la création de comptes joueurs vérifier que le demandeur n'est pas inscrit sur la liste des interdits de jeux en interrogeant l'ARJEL ; cette opération sera exécutée par la suite sur une base périodique pour chaque compte déjà créé.

4 ARCHITECTURE A METTRE EN PLACE

L'opérateur devra mettre en place un site Internet dédié, exclusivement accessible par un nom de domaine de premier niveau comportant la terminaison .fr. Toutes les connexions à destination d'un site de l'opérateur ou d'une de ses filiales et issues d'une IP française ou d'un compte joueur dont l'adresse est en France devront être redirigées vers ce site dédié.

4.1 FRONTAL ET DONNEES ARCHIVEES

4.1.1 Description générale

Le frontal est un dispositif de recueil et d'archivage des données échangées entre joueur et la plateforme de l'opérateur à l'occasion des opérations de jeux. Ce dispositif est développé et exploité sous la responsabilité de l'opérateur et est installé sur un support situé en France métropolitaine.
La plateforme ne peut être située dans un État ou un territoire non coopératif au sens de l'article 238-0 A du code général des impôts.

Tous les échanges entre un joueur réputé français et la plateforme de jeu devront transiter par ce frontal. Pour cela l'opérateur redirige les connexions provenant de joueurs réputés français vers son frontal qui se trouve en coupure de flux applicatif.

Les échanges de données suivants devront être sécurisés afin d'en garantir l'authentification ainsi que la confidentialité :

- ✓ les échanges entre le joueur et le frontal ;
- ✓ les échanges entre les différents modules du frontal ;
- ✓ les échanges entre le frontal et la plate-forme de jeux de l'opérateur ;
- ✓ les échanges entre le frontal et la plate-forme de l'ARJEL

Le flux des données échangées entre le joueur et la plateforme de jeux est déchiffré si nécessaire, puis une autre connexion sécurisée est établie entre le frontal et la plateforme opérateur.

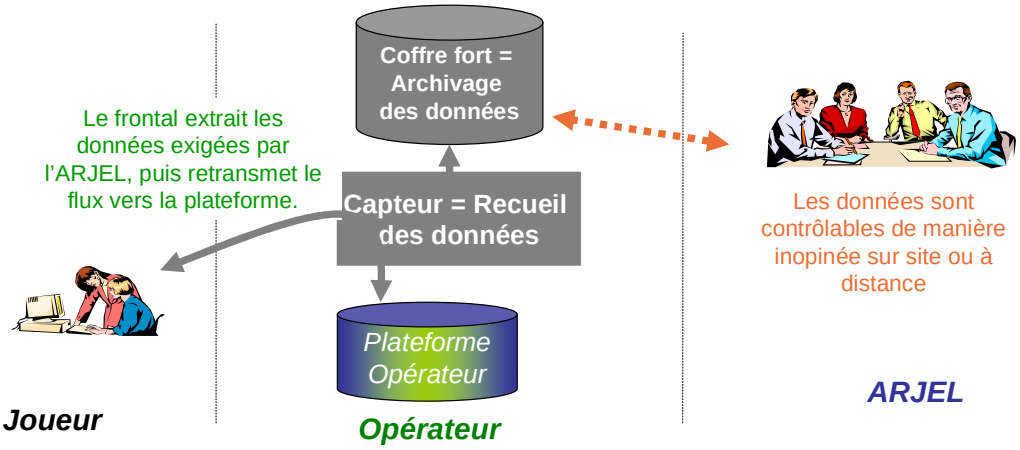
Sans implémenter de logique de jeu ou de fonction commerciale, le frontal extrait les données exigées par l'ARJEL, puis retransmet le flux vers la plateforme. Le frontal permet d'archiver les évènements de jeu entre le joueur et la plateforme de jeux, de manière sécurisée, à des fins de contrôle par l'ARJEL.

Les données archivées sont horodatées, chaînées, scellées et mises à disposition de l'ARJEL. Le dispositif d'archivage « frontal » est situé sur le territoire de la métropole.

Au moment du dépôt de son dossier de demande d'agrément, l'entreprise expose à l'ARJEL, de façon détaillée, les mesures qu'elle prend pour que son frontal permette la captation et la sauvegarde de la totalité des données qu'il doit servir à recueillir.
Elle fournit l'identité et les coordonnées du prestataire ayant réalisé le coffre-fort et du prestataire ayant réalisé le capteur.
Préalablement au début de son activité, l'entreprise ayant obtenu son agrément a l'obligation de déclarer à l'ARJEL que son frontal est en mode fonctionnement. Cette mise en fonctionnement n'implique pas, au moment où l'opérateur commence son activité, que ledit frontal soit en mesure de recueillir toutes les catégories de données qu'il doit permettre de collecter.
Le frontal devra ainsi être capable d'archiver, à l'ouverture de l'activité de jeu au moins deux catégories de données : les données compte joueur (hors données financières associées) [Annexes : partie 1.3.3 sauf 1.3.3.i] dans tous les cas ainsi que les données financières [Annexes : parties 1.3.3.i, 1.3.4.b et 1.3.5.b à f] ou les données de pari/jeu [Annexes : partie 1.3.4 sauf 1.3.4.b et partie 1.3.5 sauf 1.3.5.b à f].
L'accès distant devra impérativement être opérationnel sur les catégories de données qui seront déjà collectées. Un calendrier très précis de réalisation des différents travaux visant à rendre le frontal opérationnel sur l'ensemble des catégories de données devra être fourni à l'ARJEL lors de la demande d'agrément puis confirmé lors de la déclaration du frontal en mode fonctionnement. L'opérateur doit fournir un engagement écrit de respect de ce calendrier. Le frontal devra être en fonctionnement sur toutes ses fonctions et sur l'ensemble des données de l'Annexe 1 au plus tard pour la certification à 6 mois du frontal (II de l'article 23 de la Loi). Pour les catégories de données non encore stockées lors de la déclaration du frontal en mode fonctionnement, l'opérateur doit s'engager à les délivrer quotidiennement à l'ARJEL, dès la mise en fonctionnement du frontal, par le biais des données de supervision (Annexe 2) et selon le format XML définit à l'Annexe 1. En aucun cas cette phase intermédiaire ne pourra aller au delà de la certification à 6 mois.

Principe général du dispositif technique de recueil et d'archivage

L' opérateur met en œuvre un **dispositif d'archivage** « frontal » situé sur le territoire de la métropole.
Le frontal permet d'archiver les données échangées entre le joueur et la plateforme de jeu de manière sécurisée à des fins de contrôle.



Les éléments constitutifs du frontal

Le dispositif frontal à mettre en place se situe en rupture de flux applicatif, et comporte deux parties principales :

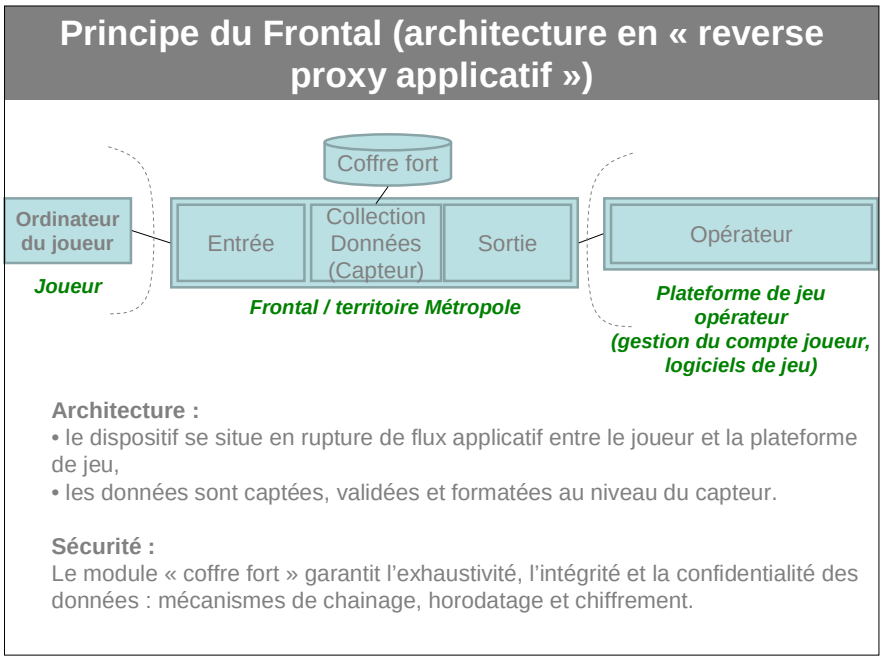
- une fonction de création de traces (capteur), qui assure la collecte, la validation et le formatage des données ;
- une fonction de stockage des traces (coffre-fort), qui assure un archivage sécurisé des données journalisées. Elle garantit l'exhaustivité, l'intégrité et la confidentialité des données journalisées, grâce à des mécanismes de chaînage, d'horodatage et de chiffrement.

Le coffre-fort devra obtenir, au minimum, une certification de sécurité de premier niveau (CSPN) délivrée par l'ANSSI (http://www.ssi.gouv.fr). Si cette certification n'est pas encore obtenue lors de la demande d'agrément, l'opérateur devra préciser le calendrier d'obtention de cette certification. Dans tous les cas, le dossier de demande devra avoir été déposé à l'ANSSI lors du dépôt de la demande d'agrément. Cette CSPN devra au minimum prendre en compte les éléments suivants :

- au niveau des menaces : le dépôt ou l'injection d'enregistrements, l'altération d'enregistrements, le vol de données, le déni de services ;
- au niveau des fonctions de sécurité : l'authentification forte des utilisateurs et administrateurs, le chaînage des évènements, le chiffrement et la signature des évènements.

À ces deux fonctions essentielles, il convient d'ajouter trois fonctions complémentaires :

- une fonction de redirection des connexions des joueurs (hors frontal, à mettre en place sur la plateforme elle-même) ;
- une fonction de consultation et d'extraction des données du frontal ;
- une fonction d'administration des utilisateurs du frontal.



NB : la solution consistant à une rupture au niveau applicatif (proxy applicatif) apparaît comme une solution cohérente et privilégiée. D'autres solutions pourront éventuellement être proposées sous réserve, bien entendu, de pouvoir répondre aux objectifs essentiels du frontal. Dans ce cas, la demande d'agrément devra clairement signaler l'emploi d'une solution alternative et définir très précisément la méthode employée ainsi que l'architecture mise en place (détail très précis sur les solutions systèmes et applicatives mises en place ou envisagées).

4.1.2 Fonctions de redirection de la plateforme

Les flux de données d'un joueur réputé français vers la plateforme de jeu doivent transiter par le dispositif technique du frontal. Ainsi, la plateforme de jeu doit refuser ou rediriger vers son frontal français les requêtes suivantes :

- avant authentification du joueur, si l'origine de la connexion est une adresse IP réputée française (pays d'attribution de l'adresse IP du terminal Internet depuis lequel il se connecte est la France dans la base RIPE NCC) ;
- après authentification du joueur, si le joueur a indiqué un domicile en France lors de l'ouverture de son compte de jeu.

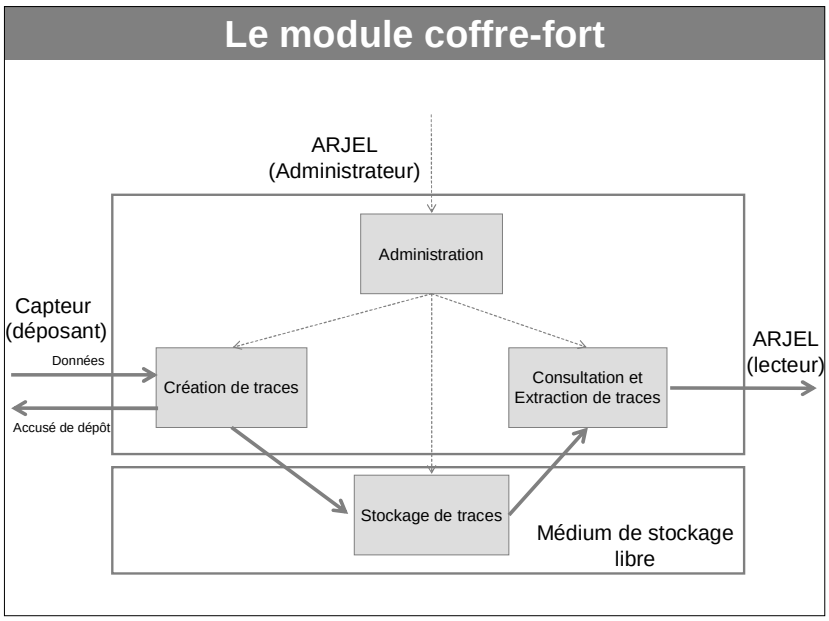
Le frontal repose sur cette fonction qui doit être implémentée sur la plateforme de l'opérateur.

4.1.3 Fonctions d'administration et de gestion des utilisateurs du coffre-fort

Les accès à la partie coffre-fort du frontal doivent s'appuyer sur des mécanismes d'authentification forte. Le coffre-fort est hébergé et exploité par l'opérateur, mais seule l'ARJEL peut déchiffrer le contenu des données archivées. Toute suppression ou altération des données archivées, de manière malveillante ou non, doit pouvoir être identifiée par l'ARJEL. L'ARJEL fournit les certificats utilisés pour son authentification au coffre. La conception du coffre doit garantir que seule l'ARJEL peut gérer les utilisateurs et leur accorder des droits.

Il faut distinguer quatre profils d'utilisateurs différents :

- profil « déposant » : profil attribué au module « capteur » du frontal de l'opérateur. Il permet uniquement d'écrire des traces dans le journal. Le module capteur du frontal s'authentifie à l'aide d'un certificat X.509v3 auprès de la partie 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, soit sur support amovible, soit via un dépôt de fichiers accessible à travers un service Web. Les certificats associés à ce profil sont utilisés :
  - soit par des personnes physiques, pour les contrôles réalisés sur site, avec des biclefs RSA et un certificat X.509v3 d'authentification conservés sur un support matériel (ex: carte à puce) fourni par l'opérateur,
  - 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 tunnel 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, par exemple :
  - arrêt/démarrage du coffre,
  - configuration du médium de stockage,
  - 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, 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.



La configuration de ces rôles aura lieu sous contrôle de l'ARJEL, lors d'une cérémonie de clés initialisant le coffre-fort. Cette cérémonie doit comporter les grandes étapes suivantes :

- étape 1 : génération de la clé de signature (« cachet serveur ») pour le scellement des dépôts au coffre. Le biclef RSA de signature est soit généré dans le HSM (*Hardware Security Module*), soit injecté dans ce dernier. Le quorum de l'ARJEL ou des personnes désignées par l'ARJEL est constitué. Les éléments caractéristiques sont les suivants
    - l'ARJEL est administrateur de la clé de signature,
    - l'opérateur a uniquement un droit d'usage de la clé publique de chiffrement,
    - la demande de certificat au format PKCS#10 fait l'objet d'une certification par une autorité désignée par l'ARJEL. Le certificat X.509v3 généré à l'issue de cette étape sert à la validation de l'horodatage des données transmises par l'opérateur à l'ARJEL ;
- étape 2 : configuration des utilisateurs au profil « administrateur fonctionnel », avec les certificats X.509v3 fournis par l'ARJEL ;
- étape 3 : configuration de la source fiable de temps ;
- étape 4 : scellement logiciel de la configuration et des binaires ;
- étape 5 : durcissement du logiciel du serveur afin de n'autoriser les accès qu'aux fonctions exposées par le coffre ;
- étape 6 : configuration des utilisateurs au profil « administrateur opérationnel », avec les certificats X.509v3 fournis par l'ARJEL ;
- étape 7 : configuration du profil « déposant », avec la partie publique avec les certificats X.509v3 fournis par l'opérateur ;
- étape 8 : configuration du profil « lecteur », avec les certificats X.509v3 fournis par l'ARJEL ;
- étape 9 : configuration de la clé de chiffrement, avec le certificat X.509v3 fourni par l'ARJEL.

À l'issue de la cérémonie d'initialisation, la partie publique des biclefs, dont la partie secrète est conservée dans le HSM, sera donc certifiée par une autorité désignée par l'ARJEL. L'utilisation d'un HSM est obligatoire pour la génération de la clé de signature et les opérations de signature. En revanche, les opérations de chiffrement des données peuvent indifféremment être réalisées par des moyens matériels ou logiciels. Les boîtiers de type NetHSM sont autorisés.

Les tailles de clefs doivent être conformes aux règles énoncées dans le Référentiel général de sécurité disponible sur le site de l'ANSSI. Ainsi, si l'algorithme asymétrique utilisé est l'algorithme RSA, une taille de clef de 2048 octets est acceptable ("RegleFact-1 : la taille minimale du module est de 2048 bits, pour une utilisation ne devant pas dépasser l'année 2020", règle mentionnée dans le document RGS_B_1 intitulé "Mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques" en version 1.20).

Un emplacement protégé, la mise en place d'un contrôle d'accès et de procédures de suivi des interventions assureront la sécurité physique des accès au coffre.

Toutes les opérations de configuration du coffre-fort feront l'objet d'un suivi.

4.1.4 Fonctions de création de traces du capteur

La fonction de création de traces correspond à l'écriture de données liées à un évènement de jeu ou à un compte joueur dans le module coffre-fort du frontal. Cette fonction intercepte voire relaie le flux applicatif entre le joueur et l'opérateur. Elle est implantée en amont de la logique de jeu.

Cette fonction doit être appelée systématiquement à chaque échange de données, entre le joueur et la plate-forme de jeux de l'opérateur, dont les traces sont exigées : en particulier, les demandes de contenu statique (images, pages HTML, etc.), ou encore les pages dynamiques sans rapport avec les évènements de jeux dont la traçabilité est exigée, n'ont pas à faire l'objet d'une analyse par le capteur. Cette fonction s'insère donc en coupure dans la chaîne de traitement des requêtes émises par le joueur vers la plateforme de jeux.

Dans l'idéal, le flux ne devrait être relayé vers le SI de l'opérateur que si et seulement si la trace a été déposée avec succès dans le coffre. Étant donné les difficultés potentielles à mettre en œuvre cette solution dans certains cas, des solutions plus souples peuvent être envisagées (traitements par lots par exemple). Le frontal doit cependant absolument offrir une architecture dotée d'une très haute disponibilité avec redondance de mécanismes afin de strictement limiter les incidents potentiels de stockage. Le principe d'une annulation d'un jeu concerné par un incident de stockage d'un des évènements doit être retenu.

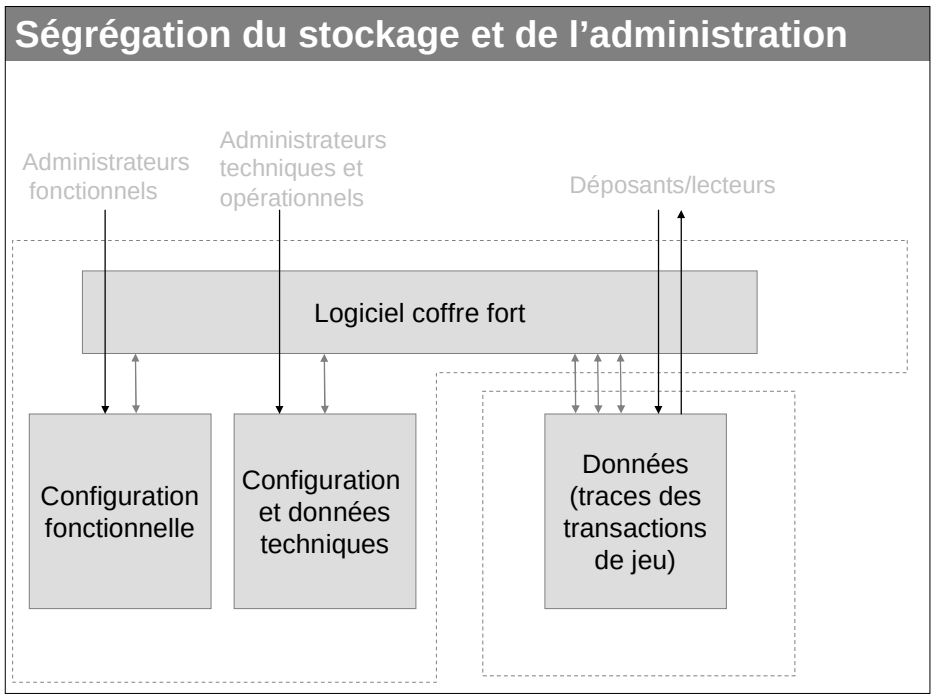
Le catalogue de ces données figure en annexe 1.

La partie 3.1.1 des Annexes apporte des éclaircissements et illustrations utiles sur la fonction de création des traces.

4.1.5 Fonctions de stockage des traces du coffre-fort

Les données tracées sont archivées dans un coffre-fort numérique afin d'en garantir l'intégrité et l'exhaustivité dans le temps. Avant que les données ne soient transmises au système d'information métier de l'opérateur, le coffre-fort enregistre les données, et les scelle de manière à ce qu'elles ne puissent être altérées, en rendant tout ajout, suppression ou modification de transaction détectable.

Le coffre-fort met en œuvre une ségrégation entre l'espace de stockage destiné aux données de son administration et celui ou ceux destinés aux données de jeu tracées : en effet, dans le cadre d'un coffre mutualisé entre plusieurs agréments, chaque agrément doit faire l'objet d'un espace de stockage spécifique. Cette ségrégation des espaces de stockage doit, *a fortiori*, être implantée dans le cadre d'une mutualisation inter-opérateurs, le cas échéant.

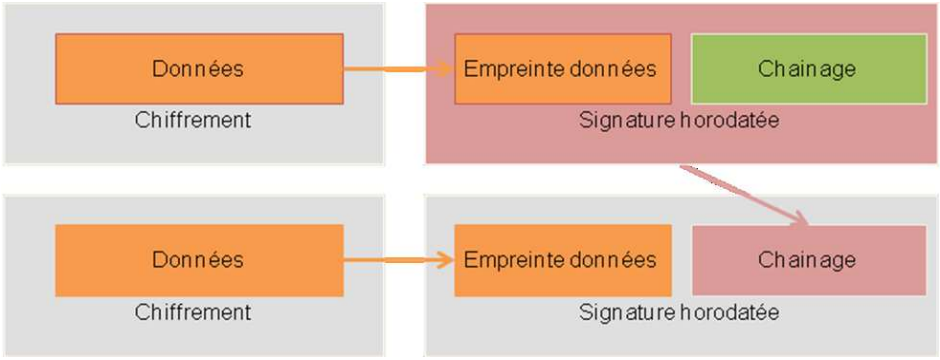


Le stockage des données consiste en les étapes suivantes :

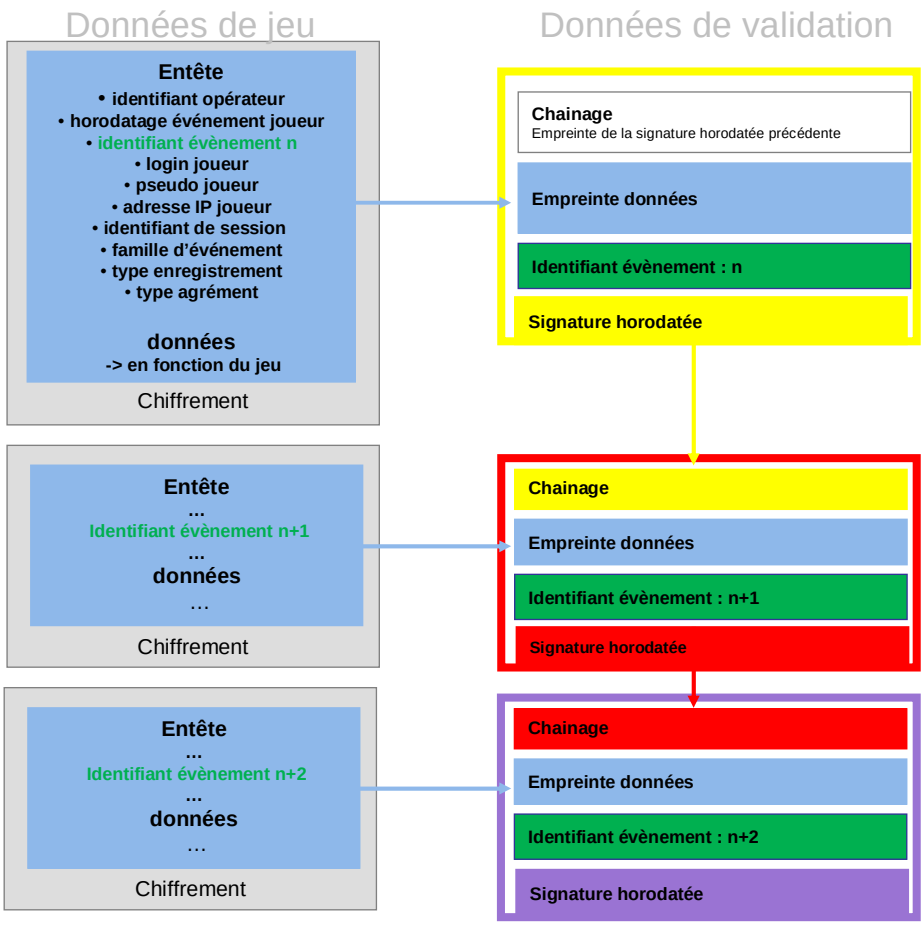
- étape 1 : établissement d'un canal sécurisé, suite à l'authentification mutuelle du déposant avec le coffre, via une session TLS mutuellement authentifiée par certificat X.509v3, et vérification de l'habilitation du profil à déposer des traces ;
- étape 2 : dépôt des données :
    - chaînage avec la trace précédente en liant l'empreinte des données à une empreinte de la signature de la trace précédente (cf. figure ci-dessous) et en incluant l'identifiant d'évènement unique à l'opérateur. L'empreinte est calculée à l'aide d'une fonction de hachage. Elle ne doit pas être calculée au moment de l'ajout, mais être conservée en mémoire depuis l'opération précédente,
    - scellement des données par signature horodatée incluant l'élément de chaînage pour en garantir l'intégrité, et les lier à une heure précise. La clé de signature est celle présente dans le HSM. La source de temps doit être fiable. Le format de signature est XADES-T avec un jeton d'horodatage RFC 3161,
    - chiffrement des données au moyen de la clé publique de l'ARJEL pour en assurer la confidentialité. La méthode de chiffrement pourra faire intervenir un algorithme de chiffrement symétrique, suivant des opérations qui seront précisément décrites à l'ARJEL. Seule l'ARJEL, détentrice de la clef privée associée à la clef publique, pourra les déchiffrer ;
- étape 3 : en cas de succès, un accusé de dépôt est retourné au capteur pour « débloquer » la poursuite de la transaction.

La cryptographie mise en œuvre en termes de générateurs de nombres pseudo-aléatoires, fonctions de hachage, algorithmes symétriques et asymétriques devra respecter les règles de bonnes pratiques spécifiées dans le référentiel général de sécurité (RGS, cf.http://www.ssi.gouv.fr/site_rubrique57.html).

Ainsi les traces constituées dans le coffre sont construites selon le modèle suivant :



La structure chaînée sera donc la suivante, pour un seul et unique événement traité par enveloppe XML chiffrée et horodatée :



NB : l'emploi du format de signature XADES-T est privilégié et devra dans tous les cas constituer la solution à terme. En phase transitoire, des solutions basées sur d'autres formats peuvent éventuellement être proposées, notamment pour des questions de performance. Dans ce cas, la demande d'agrément déposée par l'opérateur devra très précisément expliquer le recours provisoire à une autre solution et bien entendu préciser la solution retenue.

La partie 3.1.2 des Annexes apporte des précisions et des éclaircissements utiles pour le traitement par lots.

4.1.6 Fonctions d'accès aux traces et d'extraction

Les traces conservées dans le coffre sont accessibles par l'ARJEL qui peut se déplacer sur site et y saisir les données, ou les télécharger depuis ses plateformes techniques installées dans ses propres locaux.

L'opérateur agréé doit fournir les éléments suivants pour chaque agrément :

- un mécanisme d'accès aux données permettant :
  - la saisie des données sur site (copie de tout ou partie du coffre fort),
  - l'interrogation des données à distance, par l'intermédiaire d'un outil de collecte ;
- un outil de validation des données du frontal et d'extraction des traces des opérations de jeu : extraction des événements de jeu après validation de l'intégrité des données copiées depuis le frontal :
  - utilisable sur le site du frontal,
  - utilisable dans les laboratoires de l'ARJEL.

L'architecture de la partie coffre-fort du frontal doit ainsi distinguer :

- un espace de stockage des données situé dans une zone réseau sécurisée ;
- une couche d'accès à l'espace de stockage accessible. Cette couche doit elle-même être sécurisée, aux niveaux applicatif et réseau, vis-à-vis de l'extérieur, notamment contre les attaques de déni de service, et les accès autres que ceux par l'ARJEL. La couche d'accès expose un service web doté des deux principales interfaces suivantes :
  - une interface de consultation : elle permet l'extraction d'une trace ou d'un ensemble de traces à partir d'une date ou d'une tranche caractérisée par une date de début et une date de fin. À une même date peuvent correspondre aucun, un ou plusieurs évènements,
  - une interface de synchronisation : elle permet l'extraction d'une trace et ou d'un ensemble des traces à partir de l'identifiant d'un évènement ou d'une tranche d'évènements. L'identifiant devra prendre la forme d'un numéro de séquence unique à chaque coffre, implanté comme un compteur incrémenté à chaque événement enregistré. Il devra donc être fixé par le coffre lui-même. Cette interface est bijective : à un identifiant doit correspondre un et un seul événement. Le compteur ne doit souffrir d'aucune discontinuité. Le cas échéant, la détection et la reprise sur erreur devront être traitées par l'outil de validation et d'extraction.

Les données doivent rester accessibles sur site sur toute la durée de conservation exigée.

Les données accessibles à distance doivent couvrir au moins les 12 derniers mois d'opération (période glissante).

La partie 3.1.3 des Annexes apporte des illustrations et des éclaircissements sur les outils de collecte à distance et de validation.

4.1.6.a Saisie des données sur site

Un représentant de l'ARJEL peut se rendre sur le site d'hébergement du frontal pour saisir l'ensemble ou un sous-ensemble des données copiées depuis le coffre-fort. Préalablement à la saisie, l'agent de l'ARJEL vérifie que les protections physiques du frontal sont intactes, et que le médium de stockage est bien lié au frontal dont il veut saisir les données en inspectant le journal des changements de configuration.

L'ensemble des données du journal de traces contenues dans le frontal doit pouvoir être copié sur un support amovible. Le mécanisme de copie des données dépendra du médium de stockage choisi par l'opérateur. La protection de la confidentialité des données lors du transport entre le site d'hébergement du frontal et le laboratoire de l'ARJEL est assurée par leur chiffrement.

- étape 1 : accès au site d'hébergement du frontal ;
- étape 2 : vérification du sceau physique du module coffre-fort ;

- étape 3 : vérification de la configuration du coffre-fort et des média de stockage utilisés pendant la période concernée par la saisie ;
- étape 4 : mécanisme d'export des données vers le support amovible :
    - o authentification de l'agent de l'ARJEL avec son certificat client X.509v3. Le biclef d'authentification associé est stocké sur un périphérique sécurisé (carte à puce, par exemple) qui sera fourni par l'opérateur à l'ARJEL. L'ARJEL assurera la génération de son biclef d'authentification, et la signature de la clef publique associée,
    - o validation de l'habilitation de l'agent ARJEL. Ce mécanisme d'autorisation s'appuie sur les champs de base du certificat X.509v3 généré et signé par l'ARJEL, sur le support fourni par l'opérateur,
    - o choix des paramètres d'export,
    - o journalisation de la requête,
    - o export,
    - o journalisation du succès ou de l'échec de l'export.

L'outil d'extraction mis à disposition par l'opérateur doit donc permettre aux agents de l'ARJEL, munis de leur secret d'authentification et d'un médium amovible, d'extraire les évènements pour les tranches d'évènements ou d'horaires.

4.1.6.b Accès à distance

Les données stockées dans le coffre doivent être accessibles à distance, depuis les locaux de l'ARJEL, i.e. depuis une ou plusieurs adresses IP identifiées qui seront communiquées à l'opérateur. L'autorité doit pouvoir extraire du coffre une tranche de données, correspondant à une période d'activité ou une tranche d'identifiants d'évènements, sans avoir à se déplacer, et dans des conditions de sécurité logique équivalentes.

Seule la validation de l'intégrité du sceau physique ne peut être effectuée à distance. Cet accès est principalement réalisé au travers d'un service web, décrit par une interface WSDL. Il est effectué par l'outil de collecte à distance mis à disposition par l'opérateur.

Cet outil doit répondre aux exigences techniques énoncées dans l'introduction de la partie 4.1.6. Les options en ligne de commande qu'il implante doivent permettre d'interagir avec le service Web SOAP décrit par l'interface WSDL.

La partie 3.1.3.a des Annexes apporte des précisions et des éclaircissements utiles pour la mise en œuvre de l'architecture d'accès distant.

4.1.6.c Validation des données du frontal et extraction des traces (évènements de jeu)

L'opérateur fournit à l'ARJEL les moyens de valider les données extraites du coffre-fort. Ces outils prennent en entrée les données telles qu'elles ont été copiées depuis un coffre-fort, et les secrets de l'ARJEL pour effectuer les validations nécessaires à prouver l'intégrité des données et en extraire les traces des opérations de jeu. Ces outils d'extraction et de validation font partie du dispositif d'ensemble appelé coffre-fort.

Les étapes suivantes peuvent être effectuées sur place lors d'une saisie sur site ou par l'ARJEL dans ses locaux, après téléchargement du fichier de traces par le biais de son agent de collecte.

Si les outils d'extraction et de validation peuvent être intégrés au coffre, il faut également prévoir une version de ces outils que l'ARJEL pourra utiliser indépendamment dans son laboratoire, dans un mode de fonctionnement hors-ligne (déconnecté d'Internet) et opérer sur les traces récupérées soit localement sur un support amovible, soit à distance par interrogation du service web SOAP.

Les fonctionnalités suivantes sont implantées par l'outil de validation :

- étape 1 : déchiffrement des données avec la clé privée de l'ARJEL ;
- étape 2 : vérification des signatures et de l' horodatage avec la clé publique du coffre-fort ;
- étape 3 : validation du chaînage ;
- étape 4 : fourniture des données en clair (non chiffrées au format spécifié dans le paragraphe « Nature et format des données » ;

- étape 5 : fourniture des données de validation au format défini dans l'annexe 1.

La partie 3.1.3.b des Annexes fournit des précisions et éclaircissements utiles sur l'outil de validation.

4.1.7 Nature et format des données

Ce chapitre présente globalement la nature des événements à tracer, donc les données à archiver sur le frontal. Les données sont détaillées en ***annexe 1.***

D'une façon systématique, les données sont archivées sur le frontal lors des échanges entre le joueur et la plateforme de jeu ; dans certains cas, la plateforme doit cependant « pousser » les informations vers le joueur et l'archivage est fait une fois que le joueur a pu prendre connaissance des informations. Ce sera ainsi le cas, selon les logiciels de jeu, pour les opérations sur le compte joueur ainsi que pour les mouvements financiers. Dans ces cas, un affichage des modifications intervenues depuis la dernière connexion devra être réalisé en direction d'un joueur puis accepté par ce dernier afin que l'enregistrement soit réalisé.
Du point de vue technique, la trace ne doit être enregistrée que lorsque frontal reçoit une forme de confirmation de lecture par le joueur, donc toujours dans le sens d'échange joueur vers plateforme, jamais dans l'échange plateforme vers joueur.

a. Gestion du compte joueur
   Ouverture et fermeture du compte,
   Gestion des paramètres du compte (identification et adresse, acceptation des conditions contractuelles,...),
   Gestion des modérateurs personnels (autolimitations...),
   Clôture du compte (quand le joueur se connecte a posteriori).
b. Mouvements financiers d'alimentation ou retrait sur le compte joueur
   Chaque compartiment du compte joueur est identifié et tracé.
c. Evénements de jeu / paris : mise sur un pari, gain/perte,
d. Evénements de jeu / poker : selon le périmètre qui sera choisi,
   Inscription à un tournoi (mise), déroulement des parties du tournoi,
   Participation à une partie en cash-game.

Certains événements peuvent être annulés ou refusés par la plateforme de jeu pour des raisons fonctionnelles ou techniques.

⇨ Il convient d'enregistrer l'annulation de l'événement de façon à pouvoir le relier facilement à l'événement père. (Ex : refus de la mise car non réponse du serveur.).

Format des échanges.
Utilisation d'un **format XML** offrant une grande souplesse et une grande évolutivité.

Evolutivité des exigences sur les données à tracer
La liste et de la description des exigences de données à tracer évoluera au fur et à mesure que le marché des jeux va se développer, il sera donc nécessaire d'adapter les exigences.
Une procédure permettra aux opérateurs de proposer à l'ARJEL une évolution des exigences. Tant qu'une telle proposition n'est pas discutée et validée, l'opérateur ne peut pas modifier les formats ni ajouter de nouveaux types d'enregistrements dans son frontal.

4.1.8 Eléments attendus dans le dossier de demande d'agrément

Ce paragraphe recoupe les éléments réclamés dans le dossier de demande d'agrément pour la partie relative au « frontal » (ces éléments sont repris dans le cahier des charges).

Les éléments spécifiques ci-dessous sont à compléter par les éléments génériques demandés au paragraphe 5, exigences sur les systèmes et les logiciels de jeu **:**

Dans le cas où le frontal ne serait pas encore opérationnel lors de la demande d'agrément, les différents éléments demandés ci-dessous devront donc se focaliser sur la stratégie qu'il a été décidé d'employer et sur le niveau de réalisation du frontal au moment du dépôt du dossier. Un calendrier détaillé des différents travaux de mise en œuvre devra être fourni ; ce calendrier précisera les dates de remise des différentes pièces demandées.

- un point de contact technique pour toute question sur l'ensemble du frontal ;
- la description générale du frontal (stratégie employée, architecture générale, localisation physique du frontal, type d'hébergement réalisé, précisions sur les contrats d'hébergement, politique de sécurité) ;
- la description détaillée du frontal (partie génération des traces) (stratégie détaillée employée (proxy applicatif, interception IP,…), architecture technique et fonctionnelle détaillée, désignation des sous-traitants éventuels ayant développé les différents modules du frontal, spécification des interfaces et relais front-end, stratégie employée vis-à-vis de la très haute disponibilité demandée, fourniture des codes sources, politique de sécurité réalisée, analyse de risques réalisée, liste et résultats des tests d'audits effectués, documents d'exploitation, procédures mises en place notamment en terme de protection contre les accès non autorisés) ;
- la description détaillée du frontal (partie stockage sécurisé des traces) (stratégie détaillée employée, architecture technique et fonctionnelle détaillée, désignation des sous-traitants ou fournisseurs éventuels, précision des différents algorithmes employés, stratégie employée vis-à-vis de la très haute disponibilité demandée, spécification précise du déroulement de la cérémonie de clés nécessaire, spécification et rôle des bi-clés utilisées, politique de sécurité, analyse de risques effectuée, rapports de tests effectués, codes sources, documents d'administration et d'exploitation, procédures mises en place notamment en terme de protection contre les accès non autorisés) ;
- la fourniture du certificat de sécurité de premier niveau (ou mieux) du coffre-fort (ou le calendrier d'obtention) ;
- la description détaillée des mécanismes d'authentification et de confidentialité mis en place (entre le joueur et le frontal, entre les différents modules du frontal, entre le frontal et la plate-forme) ;
- la description détaillée de la cérémonie envisagée pour l'initialisation du coffre ;
- la description détaillée des mécanismes d'authentification des personnes physiques au coffre ;
- la description détaillée de l'outil de collecte à distance des fichiers de traces ;
- la description détaillée de l'outil de validation et d'extraction des fichiers de traces ;
- la description détaillée des mesures de sécurisation du frontal ;
- la description détaillée des fonctions d'administration des utilisateurs du frontal (spécifications détaillées, code source, rapports de tests) ;
- la description détaillée des fonctions de redirection des connexions de joueurs ;
- la description détaillée du site .fr mis en place (hébergeur, localisation, code source, politique de sécurité, analyse de risques, procédures mises en place…).

4.2 DONNEES MISES A DISPOSITION SYSTEMATIQUEMENT

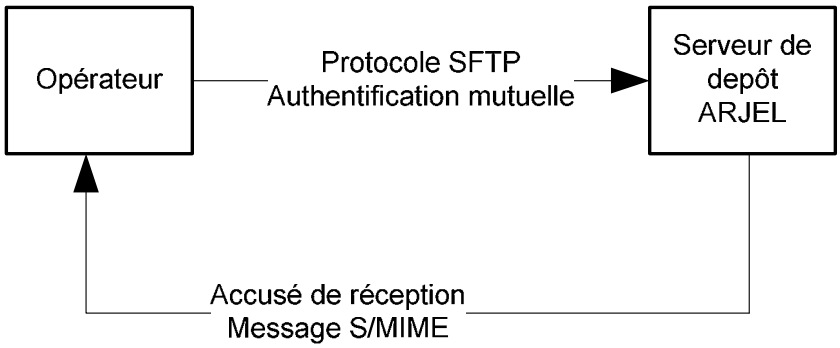
4.2.1 Fonctions de production de rapports

L'autorité exige des opérateurs l'envoi systématique de données. Ces données sont extraites des systèmes métier des opérateurs et envoyées sous forme de rapport de données agrégées. Si le format et le contenu des rapports exigés par l'autorité à l'ouverture du marché seront identifiés, ils pourront évoluer par la suite. La fonction de production de rapport devra donc pouvoir évoluer avec les exigences de l'autorité.

4.2.2 Fonctions de dépôt de données

L'ARJEL mettra à disposition des opérateurs un service de dépôt de données fondé sur le protocole SFTP . La mise à disposition des données se fait selon plusieurs étapes :

- étape 1 : authentification mutuelle de l'opérateur et de l'ARJEL, par le biais de clefs publiques client et serveur. L'empreinte de la clef publique SSH sera transmise par l'ARJEL. L'opérateur fournira à l'ARJEL sa clef publique SSH ;
- étape 2 : établissement d'un canal sécurisé entre l'ARJEL et l'opérateur, assurant authentification des parties, confidentialité et authenticité des données ;
- étape 3 : transmission des données vers le serveur de l'ARJEL ;
- étape 4 : preuve de dépôt par le biais d'un message d'acquittement signé, accusant de la bonne réception des données sous la forme d'un message S/MIME signé, transmis via le protocole SMTP à destination d'une adresse électronique qui sera communiquée par l'opérateur.



4.2.3 Nature et format des données

Ce chapitre présente globalement la nature des données à transmettre depuis la plateforme vers l'espace d'échange du système d'information de l'ARJEL.
Les données sont détaillées en ***Annexe 2.***

D'une façon générale, les données concernées sont des données globales ou agrégées.
Elles sont transmises de façon périodique à l'ARJEL. La périodicité est réglable.
Pour certaines compétitions majeures ou événements sensibles, le rythme de transmission pourra être augmenté mais cela sur une durée limitée et sur un périmètre limité.

4.3 DONNEES A LA DEMANDE

Au-delà des données tracées dans le frontal, ou mises à disposition systématiquement, l'ARJEL peut ponctuellement exiger des rapports ou données plus détaillés, ou établis avec des critères de recherche précis, qui notamment peuvent être nominatifs.

L'opérateur doit pouvoir exécuter des requêtes sur ses systèmes métier afin d'en extraire des données correspondant à des critères imposés par l'ARJEL dans des délais impartis.
Ces rapports complèteront les informations qui peuvent être obtenus sur le frontal et les informations remontées systématiquement et automatiquement vers le système d 'information de l'ARJEL.

La nature et le format spécifique des données seront spécifiés au cas par cas par l'ARJEL, selon ses besoins.

A ce stade, on peut citer :

- la fourniture à l'ARJEL de toutes les données techniques et non techniques liées à un évènement particulier ;
- des demandes d'enquête de la part de l'ARJEL concernant des évènements détectés et considérés comme anormaux ;
- le détail de l'identité d'un joueur ;
- le détail des coordonnées du compte de paiement d'un joueur ;

- le détail d'une partie de poker, incluant une visibilité complète sur tous les joueurs ayant participé (toutes cartes, quelque soit l'opérateur de rattachement des joueurs dans le cas de réseaux d'opérateurs de mise en commun de joueurs) ;
- certaines statistiques non prévues dans les données de supervision ;
- le détail d'un pari particulier ;
- la fourniture de données techniques (journaux) concernant certains éléments de l'architecture de jeu (frontal, plate-forme, …).

4.4 INTERFACES

4.4.1 Interdits de jeux

L'opérateur devra interroger l'ARJEL pour les interdits de jeux. Les interrogations menées par les opérateurs obtiendront une réponse binaire : absence ou présence dans la liste. Les procédures suivantes devront être mises en œuvre par l'opérateur :

- à chaque demande d'ouverture de compte, l'opérateur interroge le fichier des interdits sur la base d'une identification de la personne ; si la personne est inscrite, l'ouverture est bloquée ;
- périodiquement (ordre de grandeur mensuel) chaque opérateur doit contrôler pour chaque joueur ayant un compte ouvert s'il est inscrit au fichier des interdits de jeu en ligne. Si un joueur a été inscrit, son compte joueur est bloqué.

La partie 3.2 des Annexes précise les modalités techniques de mise en œuvre de cette interrogation.

5 AUTRES EXIGENCES SUR LES SYSTEMES ET LES LOGICIELS DE JEU

En dehors des exigences du dispositif spécifique qu'est le frontal, afin d'assurer la protection des joueurs et permettre à l'ARJEL de remplir sa mission, l'ensemble du système d'information de l'opérateur devra être décrit et répondre à certaines exigences techniques.

Par système d'information, nous entendons :
- **les différents modules du Frontal** ;
- l'ensemble des composants aux niveaux système, réseau et applicatif et plus généralement tout système ou application (outils de gestion de relation client, logiciels de jeux, etc.) **susceptible d'interagir avec les plates-formes de jeux de l'opérateur**.

Ces exigences techniques précisent les critères auxquels l'opérateur devra répondre, afin de s'assurer du respect des bonnes pratiques du jeu en ligne retenues par l'ARJEL, en particulier celles relatives à l'intégrité, la sécurité et la fiabilité des jeux.

Dans la suite de ce document les éléments précédés de [E*] sont à considérer comme des exigences impérativement opérationnelles lors de l'ouverture de l'activité de jeu, les éléments précédés de [E] sont à considérer comme des exigences à atteindre (objectifs), les éléments précédés de [P] sont à considérer comme des précisions à apporter.

5.1 AUDITS DE SECURITE

L'ARJEL réalisera dans le cadre de sa mission générale de contrôle des audits de sécurité afin de vérifier les niveaux de maturité SSI des opérateurs ainsi que les niveaux de sécurité atteints par les frontaux et les plates-formes de jeux. Ces audits seront effectués dans un cadre coopératif et des recommandations techniques ou organisationnelles seront proposées aux opérateurs afin de remédier aux vulnérabilités identifiées.

- [E] ces audits et contrôles porteront sur :
  - la sécurité physique et les contrôles devant être réalisés sur site : un accès au site ainsi qu'à l'ensemble des équipements et des données de la ou des plates-formes de jeux devra être accordé à l'ARJEL ou aux organismes mandatés,
  - la sécurité logique, par des tests pratiqués à distance ou depuis les locaux de l'opérateur, qu'ils soient intrusifs ou non ;
- [E] ces audits et contrôles seront essentiellement prévus à l'avance ;
- [E] l'opérateur devra mettre à disposition des personnes mandatées par l'ARJEL les moyens et ressources nécessaires à ces audits et contrôles. Ceux-ci pourront comprendre, par exemple :
  - ✓ des jours de présentations technique et fonctionnelle, assurées par l'opérateur, des dispositifs mis en place sur les plates-formes de jeux,
  - ✓ des jours consacrés à l'analyse technique et détaillée de ces systèmes dans des environnements mis à disposition par l'opérateur ;
- [E] l'opérateur devra corriger les éventuelles anomalies majeures constatées à l'issue des audits de sécurité. Si aucune mesure de sécurité ne permet de les corriger directement, l'opérateur devra proposer des mesures de contournement provisoire afin d'éviter l'exploitation de ces vulnérabilités majeures. Le plan d'action associé et établi par l'opérateur devra être communiqué à l'ARJEL ;
- [E] l'opérateur devra informer l'ARJEL de la mise en place d'une nouvelle technologie au sein de sa plate-forme ;
- [E] l'opérateur devra communiquer à l'ARJEL les résultats des audits de sécurité réalisés sur ses plates-formes de jeux, le cas échéant, par des organismes tiers.

5.2 HOMOLOGATIONS

- [E*] Les logiciels de jeu seront systématiquement homologués ;
- [E] les mises à jour et évolutions des logiciels qui ont fait l'objet d'homologations, devront suivre les mêmes procédures d'homologation ;
- [E*] dans le cadre de l'homologation du logiciel de jeu et afin de permettre à l'ARJEL de prononcer ou non à cette homologation, l'opérateur devra impérativement remettre à l'ARJEL le code source du logiciel destiné à être utilisé par les joueurs français ainsi que le code source de l'éventuel générateur de nombre aléatoire. L'opérateur devra également remettre trois rapports spécifiques d'analyse des codes sources fournis réalisés par des prestataires experts de son choix dont les coordonnées seront fournies à l'ARJEL :
  - ✓ un rapport d'analyse détaillée des vulnérabilités de sécurité du code source ; ce rapport devra détailler la méthode utilisée pour l'analyse du code, lister l'ensemble des vulnérabilités identifiées, détailler chaque vulnérabilité techniquement et expliquer l'impact précis de l'exploitation de chaque vulnérabilité identifiée ; le plan d'actions associé à la prise en compte des vulnérabilités identifiées devra être fourni ;
  - ✓ un rapport d'analyse spécifique du générateur de nombre aléatoire détaillant les éventuelles vulnérabilités du code et indiquant le niveau de qualité intrinsèque de ce générateur aléatoire. Les caractéristiques suivantes liées au caractère aléatoire du générateur (selon Bruce Schneier) devront être démontrées :
    - les mécanismes de génération doivent avoir subi avec succès différents tests statistiques démontrant leur caractère aléatoire,
    - les données aléatoires générées doivent être non prévisibles : il doit être impossible de prédire la donnée générée suivante même si l'on a connaissance de l'algorithme ou du matériel de génération et de toutes les données précédemment générées,
    - les séries de données générées ne doivent pas être reproductibles : si le générateur aléatoire est activé avec les mêmes paramètres en entrée, il doit générer une nouvelle séquence de données ;
  - ✓ un rapport d'analyse certifiant que les règles implémentées dans le logiciel de jeu sont bien conformes au jeu tel qu'il est présenté au joueur ; les règles seront jointes au rapport.

  L'ARJEL remettra sa décision sur l'homologation des logiciels de jeux dans les deux mois à compter de la date de remise des différents éléments demandés pour cette homologation.

La partie 3.3 des Annexes précise les modalités techniques de transmission sécurisée de ces informations.

5.3 VERIFICATION INITIALE DE LA PLATE-FORME DE JEU

[E*] La plate-forme de jeu devra avoir subi, avant ouverture, une première analyse de ses vulnérabilités techniques. Les coordonnées précises du prestataire choisi par l'opérateur devront être précisées. Le rapport issu de cette analyse devra être fourni à l'ARJEL. Il indiquera la liste des vulnérabilités identifiées, l'impact de chaque vulnérabilité ainsi que le plan d'actions associé à la prise en compte des vulnérabilités. L'opérateur ne pourra ouvrir son activité de jeux que si l'ARJEL estime que le niveau de sécurité de la plate-forme de jeux est suffisant.

5.4 CERTIFICATION

Conformément à l'article 23 de la Loi, l'opérateur de jeux ou de paris en ligne doit se soumettre à une certification portant sur le respect par ses soins des clauses générales et spécifiques du cahier des charges prévu à l'article 20 de la Loi. Cette certification est réalisée par un organisme choisi par l'opérateur au sein d'une liste établie par l'ARJEL. Le coût de cette certification est à la charge de l'opérateur.
La certification n'est pas spécifique aux aspects techniques qui n'en constituent qu'une partie.

5.5 MISE EN ŒUVRE OPERATIONNELLE DU FRONTAL

Au moment du dépôt de son dossier de demande d'agrément, l'entreprise expose à l'ARJEL, de façon détaillée, les mesures qu'elle prend pour que son frontal permette la captation et la sauvegarde de la totalité des données qu'il doit servir à recueillir.
Elle fournit l'identité et les coordonnées du prestataire ayant réalisé le coffre-fort et du prestataire ayant réalisé le capteur.

Préalablement au début de son activité, l'entreprise ayant obtenu son agrément a l'obligation de déclarer à l'ARJEL que son frontal est en mode fonctionnement. Cette mise en fonctionnement n'implique pas, au moment où l'opérateur commence son activité, que ledit frontal soit en mode fonctionnement.
Le frontal devra ainsi être capable d'archiver, à l'ouverture de l'activité de jeu au moins deux catégories de données : les données compte joueur (hors données financières associées) [Annexes : partie 1.3.3 sauf 1.3.3.i] dans tous les cas ainsi que les données financières [Annexes : parties 1.3.3.i, 1.3.4.b et 1.3.5.b à f] ou les données de pari/jeu [Annexes : partie 1.3.4 sauf 1.3.4.b et partie 1.3.5 sauf 1.3.5.b à f].
L'accès distant devra impérativement être opérationnel sur les catégories de données qui seront déjà collectées. Un calendrier très précis de réalisation des différents travaux visant à rendre le frontal opérationnel sur l'ensemble des catégories de données devra être fourni à l'ARJEL lors de la demande d'agrément puis confirmé lors de la déclaration du frontal en mode fonctionnement. L'opérateur doit fournir un engagement écrit de respect de ce calendrier. Le frontal devra être en fonctionnement sur toutes ses fonctions et sur l'ensemble des données de l'Annexe 1 au plus tard pour la certification à 6 mois du frontal (II de l'article 23 de la Loi). Pour les catégories de données non encore stockées lors de la déclaration du frontal en mode fonctionnement, l'opérateur doit s'engager à les délivrer quotidiennement à l'ARJEL, dès la mise en fonctionnement du frontal, par le biais des données de supervision (Annexe 2) et selon le format XML définit à l'Annexe 1. En aucun cas cette phase intermédiaire ne pourra aller au delà de la certification à 6 mois.

5.6 CONTROLE DES JEUX ET PARIS REALISE PAR L'OPERATEUR

En complément des éléments strictement techniques, l'opérateur devra décrire précisément les différents mécanismes de suivi, de supervision et de contrôle des jeux et paris mis en place. Il indiquera notamment les différents indicateurs et seuils d'alerte retenus ainsi que les procédures de réaction à chaud ou à froid qui ont été définies.
Il est clair que le franchissement d'un seuil d'alerte doit s'accompagner de la transmission de données dites systématiques à l'ARJEL.

5.7 EXIGENCES ORGANISATIONNELLES ET TECHNIQUES

Cette partie a pour but de donner à l'ARJEL toutes les informations utiles pour évaluer :

- l'organisation générale de l'opérateur ;
- l'organisation mise en place par l'opérateur pour l'acquisition et la mise en œuvre de ses systèmes d'information ;
- les systèmes d'information mis en œuvre par l'opérateur et par les structures qui relèvent de sa responsabilité ;
- l'architecture de ces systèmes et les réseaux utilisés ;
- l'organisation et les moyens mis en œuvre dans le domaine de la sécurité des systèmes d'information.

Les différents éléments demandés ci-après concernent l'ensemble des systèmes d'information de l'opérateur au sens indiqué dans l'introduction du §5. Si certaines briques de ces systèmes n'étaient pas opérationnelles lors de la demande d'agrément, le demandeur devra en indiquer les raisons et préciser le calendrier de mise en œuvre de ces systèmes ainsi que celui de remise des différents éléments demandés ci-dessous.

5.7.1 Présentation générale

5.7.1.a Organisation générale de l'opérateur

- [P] L'opérateur détaillera :
  - ✓ les différentes directions qui le composent, avec leurs missions précises,
  - ✓ les éventuels services déconcentrés qui lui sont rattachés, avec leurs fonctions respectives et leurs implantations géographiques.

5.7.1.b Politique et organisation dans le domaine des systèmes d'information de l'opérateur

- [P] L'opérateur détaillera et fournira, si les éléments cités existent :
  - ✓ son organisation pour la conduite des projets et pour la mise en œuvre des systèmes d'information,
  - ✓ sa politique générale informatique,
  - ✓ son schéma directeur informatique.

5.7.1.c Systèmes d'information de l'opérateur

- [P] L'opérateur détaillera :
  - ✓ les centres d'exploitation et de supervision informatiques et réseau (localisation, application, personnel),
  - ✓ les centres d'hébergement (localisation, type d'hébergement),
  - ✓ les centres d'interconnexion (types),
  - ✓ les centres opérationnels ;
- [P] pour chacune des plates-formes de jeux, des frontaux, et l'ensemble des systèmes d'information afférents à celles-ci, l'opérateur indiquera :
  - ✓ la ou les fonctions qu'il assure,
  - ✓ le type de données traitées,
  - ✓ l'autorité responsable de son exploitation,
  - ✓ le fournisseur d'accès,
  - ✓ l'hébergeur ;
- [P] l'opérateur fournira la liste des principales applications en service au niveau des plates-formes de jeux ;
- [P] pour chacune de ces applications, l'opérateur indiquera :
  - ✓ la ou les fonctions qu'elle assure,
  - ✓ le type de données traitées,
  - ✓ l'autorité d'exploitation désignée,
  - ✓ ses implantations, son architecture et les réseaux utilisés (Internet ou réseau dédié),
  - ✓ les éventuels moyens de chiffrement mis en œuvre,
  - ✓ l'importance de sa fonction (de « outil facilitant le travail» à « outil indispensable »),
  - ✓ l'importance de sa disponibilité (de « aucun effet » à « effet bloquant » en cas d'arrêt total ou partiel du système),

- ✓ l'importance de l'intégrité des données (de « aucun effet » à « effet bloquant » en cas de modification de données),
- ✓ l'importance de la confidentialité des données (de « aucun effet » à « effet bloquant » en cas de divulgation de données),
- ✓ la durée de vie prévue ;

- [P] si des projets sont en cours, l'opérateur fournira les mêmes renseignements que pour ceux en service et précisera les maîtrises d'ouvrage et les maîtrises d'œuvre.

5.7.1.d Organisation humaine de l'opérateur

- [P] L'opérateur décrira l'organisation mise en place pour assurer la sécurité des systèmes d'information, ainsi que la sécurité physique des locaux ;
- [P] l'opérateur précisera si les fonctions citées ci-dessous sont prévues, et indiquera pour chacune les informations demandées :
  - ✓ RSSI, avec la définition précise de ses responsabilités, si elles sont formalisées, le d'adjoints et le rattachement hiérarchique,
  - ✓ autorité d'exploitation du SI, ou fonction équivalente (définition précise de ses responsabilités, si elles sont formalisées. Préciser en particulier si elle a des responsabilités en matière de SSI),
  - ✓ responsables juridiques experts en SSI (nombre et rattachement hiérarchique),
  - ✓ auditeurs internes en SSI (nombre et rattachement hiérarchique),
  - ✓ fonction de contrôle interne en SSI (nombre et rattachement hiérarchique),
  - ✓ fonction support en SSI (nombre et rattachement hiérarchique),
  - ✓ fonction opérationnelle en SSI (nombre et rattachement hiérarchique),
  - ✓ fonction de conception en SSI (nombre et rattachement hiérarchique) ;
- [P] l'opérateur précisera s'il existe des tableaux de bord SSI. Si oui, il en fournira un exemplaire ;
- [P] l'opérateur précisera s'il existe un budget spécifique SSI. Si oui, il l'indiquera. Si non, il évaluera si possible son montant, ou son pourcentage par rapport au budget des SI.

5.7.1.e Pilotage des systèmes d'information (SI) chez l'opérateur

Les points suivants seront décrits pour l'opérateur dans son ensemble et, le cas échéant, pour chacun des systèmes d'information qui le composent.

- [P] L'opérateur indiquera dans quelles phases du cycle de vie des systèmes la sécurité des systèmes d'information est prise en compte. Il précisera notamment si la sécurité est prise en compte en amont dans les expressions de besoins rédigés pour le développement (en interne ou sous-traité) et pour le maintien en condition des systèmes d'information et des applications (application des correctifs notamment). Il précisera également si les applications développées ont une durée de vie estimée. Il fournira quelques exemples caractéristiques : extraits de CCTP, par exemple, incluant les clauses de sécurité éventuellement fixées ;
- [P] l'opérateur indiquera s'il est prévu une recette SSI des projets de systèmes d'information avant leur mise en service. Il indiquera la proportion des systèmes d'information ayant réellement fait l'objet d'une telle recette ;
- [P] l'opérateur indiquera s'il est prévu un examen formalisé de l'impact, sur la sécurité d'un SI, de la mise en exploitation d'un nouvel composant (modèle de serveur, système d'exploitation, application, données, etc.) et en précisera les modalités ;
- [P] l'opérateur indiquera si les livrables incluent le code source en pleine propriété ;
- [P] l'opérateur indiquera si des études des risques ont été réalisées. Si oui, il en fournira une copie. Il en précisera le nombre, le périmètre et la méthode utilisée, et fournira quelques exemples caractéristiques ;
- [P] l'opérateur précisera si les composants sensibles sont identifiés (y compris les données). Si oui, il en précisera les modalités d'identification et de classification, et notamment la méthodologie employée ;
- [P] l'opérateur indiquera s'il est fait recours à des évaluations ou certifications. Si oui, il en précisera les périmètres, conditions, modalités et résultats ;
- [P] l'opérateur indiquera les métiers faisant appel à la sous-traitance ou à l'externalisation (hébergement web, infogérance, sécurité, …) ;
- [P] l'opérateur indiquera si des audits SSI périodiques sont réalisés sur les systèmes d'information et applications. Si oui, il en précisera la nature, le nombre annuel, les acteurs et la méthodologie employée. Il en fournira les comptes-rendus, et donnera la liste des principales recommandations effectuées. Il précisera les modalités de décision des mesures correctrices, et celles de leur mise en œuvre et du contrôle de leur bonne exécution. Il

indiquera la proportion des mesures réellement appliquées ;

- [P] l'opérateur indiquera le taux de personnel ayant été sensibilisé ou formé à la SSI dans les chaînes SI et SSI et parmi les utilisateurs. Il précisera s'il existe une gestion et un suivi régulier de la compétence de chacun ;
- [P] l'opérateur indiquera comment les aspects réglementaires sont pris en compte, notamment en termes de données personnelles [CNIL].

5.7.1.f Fonction SSI opérationnelle chez l'opérateur

- [P] L'opérateur indiquera s'il dispose d'un centre opérationnel chargé de la SSI. Si oui, il indiquera son rattachement hiérarchique, son régime de veille et l'effectif de permanence. Si non, il indiquera les modalités de veille et de déclenchement des alertes ;
- [P] l'opérateur indiquera s'il existe une astreinte SSI. Si oui, il en précisera l'organisation, le régime, le niveau du personnel l'assurant, les modalités de contact ;
- [P] l'opérateur indiquera si des procédures ou des consignes sont en place pour les cas d'incident et de détection de fraude, jusqu'à quel niveau ces documents sont diffusés, et s'ils prévoient les modalités de remontée des incidents. Si oui, il en fournira un exemplaire ;
- [P] l'opérateur précisera si des incidents de SSI ou des fraudes ont déjà été rapportés. Si oui, il indiquera par quelle voie, jusqu'à quel niveau, et quelles suites ont été données ;
- [P] l'opérateur détaillera sa gestion de la continuité des services, et précisera les plans de reprise en cas de dysfonctionnement de SI, et s'ils existent, si ces plans ont été testés.

5.7.2 Exigences organisationnelles

5.7.2.a Politique et schéma directeur en sécurité des systèmes d'information de l'opérateur

- [E] L'opérateur devra posséder un schéma directeur en SSI, ou un document équivalent. Il en précisera la date de son début d'application, et la périodicité de ses mises à jour. Il précisera également s'il est intégré dans le schéma directeur informatique et en fournira la dernière version et, si possible, la version précédente ;
- [P] l'opérateur indiquera les orientations stratégiques décidées, et le niveau de réalisation des actions en découlant ;
- [E] l'opérateur devra posséder une politique de sécurité des systèmes d'information. Il précisera son périmètre d'application et en fournira un exemplaire. Si un tel document n'existe pas, il indiquera, si un ou des documents remplissent une fonction similaire, et en fournira une copie. Cette politique de sécurité devra aborder les sujets suivants :
  - ✓ des éléments stratégiques :
    - le périmètre d'application de la politique de sécurité, par exemple en termes de domaines d'activités ou de systèmes d'information,
    - les enjeux et orientations stratégiques, à travers la formalisation des enjeux liés au périmètre précédemment défini,
    - les aspects légaux et réglementaires liés au périmètre d'application de la politique de sécurité,
    - une échelle de besoins qui comportera une pondération et des valeurs de référence selon les critères de sécurité choisis, ainsi qu'une liste d'impacts enrichis d'exemples,
    - une description des besoins de sécurité des domaines d'activité de l'opérateur, selon l'échelle de besoins présentée dans la partie précédente,
    - une analyse des menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications,
  - ✓ de règles de sécurité, classées par thème :
    - organisation: organisation de la SSI, gestion des risques, sécurité et cycle de vie, assurance et certification, évolution de la PSSI,
    - mise en oeuvre : aspects humains, plan de secours, gestion des incidents, sensibilisation et formation, exploitation, sécurité physique,
    - technique : identification / authentification, contrôle d'accès logique, journalisation, chiffrement ;
- [E] l'opérateur devra posséder des déclinaisons techniques détaillées des éléments exigés par sa politique de sécurité. Elles feront faire le lien entre la politique de sécurité et toutes les procédures liées aux systèmes d'information, en établissant des moyens de sécurisation et du suivi de ces moyens dans le temps. Ces moyens seront aussi bien organisationnels que

techniques ;

- [E] l'opérateur devra imposer des exigences de sécurité aux divers sous-traitants avec lesquels des relations contractuelles sont établies, il les fournira si possible ;
- [P] l'opérateur précisera les contrôles qu'il exerce auprès de ses sous-traitants, le cas échéant, afin d'assurer un maintien du niveau de sécurité au cours du temps de ses plates-formes et systèmes d'information.

5.7.2.b Procédures d'administration et d'exploitation

- [E*] L'organisation mise en place pour gérer les systèmes d'information de l'opérateur devra s'appuyer sur une documentation et des procédures permettant de suivre leurs évolutions. Outre la politique de sécurité, la documentation comportera les éléments suivants :
  - ✓ une description fonctionnelle du SI (elle peut être intégrée dans la politique de sécurité) précisant les composants de l'interconnexion (cf. description fonctionnelle de l'architecture) et les flux devant transiter au travers de celle-ci,
  - ✓ une description technique du SI issue de l'étude d'architecture (composants techniques, adressage/nommage, flux techniques (protocoles) nécessaires avec leur sens, etc.) et comprenant des éléments factuels (licences des logiciels utilisés, contrats de maintenance, configurations à jour des équipements, état des modifications effectuées),
  - ✓ une liste de procédures d'exploitation des composants de l'interconnexion (qui peuvent être incluses ou non dans une déclinaison technique de politique de sécurité),
  - ✓ des procédures d'exploitation classiques comme la gestion des comptes et mots de passe, la gestion de la configuration des composants, la gestion de sauvegardes,
  - ✓ des procédures spécifiques liées à la sécurité ;
- [E*] les procédures d'exploitation suivantes seront notamment transmises par l'opérateur :
  - ✓ procédures de gestion des journaux,
  - ✓ procédures de gestion des alertes,
  - ✓ procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.),
  - ✓ procédures de gestion des composants à mise à jour fréquente (anti-virus, systèmes de détection d'intrusion, le cas échéant),
  - ✓ procédures de mise à jour en cas d'édition d'un correctif de sécurité critique,
  - ✓ procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent,
  - ✓ procédures d'exploitation des composants du SI (serveurs, routeurs),
  - ✓ procédures d'exploitation des comptes et mots de passe,
  - ✓ procédures de gestion des composants infogérés,
  - ✓ procédures relative à la sécurité physique (gardiennage, etc.),
  - ✓ procédures de gestion des sauvegardes et des restaurations,
  - ✓ procédures de veille technologique,
  - ✓ procédures pour la télé-administration,
  - ✓ procédures de gestion des tableaux de bord SSI.

5.7.3 <u>Exigences techniques</u>

5.7.3.a Description générale des systèmes d'information

Pour chacun des systèmes mentionnés dans la partie « systèmes d'information des opérateurs », les points suivants seront décrits, si applicable :

- [P] l'opérateur fournira l'architecture du réseau, et précisera comment elle a été définie et quel est son historique ;
- [P] l'opérateur fournira une description détaillée de l'architecture :
  - ✓ fournir un schéma technique du réseau,
  - ✓ lister les différents flux associés,
  - ✓ lister les zones de sensibilités différentes,
  - ✓ lister les interconnexions de ces zones, et comment elles ont été interconnectées,
  - ✓ lister les liens vers l'extérieur (lignes dédiées, interconnexions de réseaux, …) et les accès distants possibles depuis l'extérieur (modem analogiques, RNIS, Internet, etc.),
  - ✓ préciser les fournisseurs d'accès et le type de contrat passé avec eux,
  - ✓ préciser comment les diverses fonctions et les services sont implantés,
  - ✓ indiquer les technologies mises en œuvre ;

- **[E*] les informations techniques, notamment les spécifications concernant l'architecture du système, les documentations des matériels ou des logiciels, les configurations (règles de filtrage, DNS, pare feu, messagerie, etc.) et le plan d'adressage seront regroupés dans un dossier appelé « dossier de définition ». Ce dossier devra également contenir la liste descriptive précise de tous les éléments (matériels et logiciels, versions, contrat de maintenance) ;**
- [E] l'opérateur sera responsable, sur toute la durée de validité de l'agrément, de la tenue à jour et de la cohérence de ce dossier. Chaque modification de l'un de ces dossiers devra faire l'objet d'une nouvelle remise de document à l'ARJEL ;
- [E] l'opérateur donnera dans sa réponse le plan détaillé des dossiers de définition et décrira l'ensemble des informations qui y seront consignées.

5.7.3.b Architecture réseau

- [E] Les systèmes d'information de l'opérateur devront faire l'objet d'une segmentation et d'un filtrage réseau en accord avec le principe de défense en profondeur, notamment au niveau des réseaux de services, d'administration et de supervision des plates-formes. Ce cloisonnement réseau sera conforme aux descriptions fonctionnelles et techniques décrites dans la partie « description générale des systèmes d'information » ;
- [E] l'opérateur assurera un cloisonnement du réseau, mis en oeuvre à l'aide de mécanismes de filtrage de niveau 3 au minimum, au moins entre les zones suivantes :
    - ✓ les zones dédiées aux serveurs, avec un cloisonnement supplémentaire en fonction du niveau de sensibilité identifié pour chacun par la politique de sécurité :
        - les serveurs métiers (serveurs d'applications, systèmes de gestion de base de données),
        - les serveurs d'infrastructure (serveurs d'authentification, serveurs de messagerie, serveurs de fichiers, serveurs de distribution de logiciels),
        - les équipements d'infrastructure réseau (routeurs, commutateurs),
        - les serveurs de tests, de développement et de préproduction,
    - ✓ la zone des équipements dédiés à la l'administration, l'exploitation et la supervision du système d'information. Cette zone qui héberge notamment les postes de travail des administrateurs et les serveurs de supervision devra faire l'objet d'une attention particulière compte tenu des accès privilégiés qu'ils sont susceptibles d'accorder sur les ressources les plus critiques du SI,
    - ✓ la ou les zones dédiées aux postes de travail des utilisateurs, avec un découpage supplémentaire dont la granularité pourra varier selon les missions des différents services métiers et la criticité de l'information dont ils ont la responsabilité ;
- [E] la politique de filtrage réseau adoptée devra respecter le principe du moindre privilège : les règles de filtrage seront élaborées suivant un principe de liste blanche ;
- [P] l'opérateur détaillera les mécanismes de cloisonnement réseau déployés (filtrage IP, filtrage applicatif, VLAN, 802.1X, NAP/NAC, etc.).

5.7.3.c Gestion de la disponibilité

- [P] l'opérateur précisera sa politique vis-à-vis de ses fournisseurs tant de matériels que de logiciels : contrat de maintenance systématique, délai maximum d'intervention en cas d'incident, délai maximal d'approvisionnement en cas de défaillance matériel de l'un des équipements, ou en cas d'ajout de matériel sur la plate-forme, etc. ;
- [E*] l'opérateur mettra en oeuvre des mécanismes de sécurité afin d'assurer une défense contre les attaques classiques sur IP et les protocoles associés, en particulier par rapport aux attaques en déni de service réseau ;
- [P] l'opérateur détaillera les mesures techniques prises en termes de résilience réseau de ses systèmes d'information, notamment au regard de la lutte contre les attaques en déni de service (distribuées ou non, par épuisement de bande passante, ou encore de ressources système) au niveau des plates-formes de jeux et du frontal. Cette description s'attachera à décrire les procédés techniques mis en oeuvre (équilibrage de charge, ajustement des TTL DNS, réadressage IP dynamique des plates-formes, et du frontal) et les mesures organisationnelles associées (remontée d'alerte en cas d'attaque, protocole d'accord avec les FAI pour la lutte contre les DDOS, etc.) ;
- [P] l'opérateur décrira les solutions qu'il met en oeuvre pour éviter ou détecter, le cas échéant, les attaques et intrusions sur ses systèmes d'information.

5.7.3.d Gestion des mises à jour

- [E*] L'opérateur devra au moins surveiller les avis et les alertes du CERTA ;
- [E*] l'opérateur devra appliquer les correctifs de sécurité qui sont proposés par les éditeurs, dans les documents du CERTA ou demandés explicitement par l'ARJEL, le cas échéant :
- [E*] si aucun correctif de sécurité n'est disponible auprès de l'éditeur, l'opérateur devra suivre les recommandations de ce dernier ou du CERTA dans le cadre d'un contournement provisoire. Si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, l'opérateur s'engagera à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité ;
- [P] l'opérateur décrira le processus d'application des correctifs, et notamment en cas de régression vis-à-vis des systèmes ou vis-à-vis des applications. Ce processus devra inclure des procédures techniques permettant un retour arrière dans le cas où le correctif provoquerait une éventuelle régression. En cas d'incompatibilité avérée entre un correctif et les applications existantes, le titulaire devra documenter l'incompatibilité rencontrée et les risques engendrés ;
- [E*] l'opérateur devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer à l'ARJEL la version actualisée du document.

5.7.3.e Gestion des échanges

5.7.3.e.1 Confidentialité et authenticité des flux d'administration

- [E] L'intégralité des échanges de données devra être sécurisée à l'aide de procédés cryptographique permettant de garantir l'authentification des composants, la confidentialité et l'authenticité des communications. Tous les échanges de fichiers – données d'administration, et mise à jour de contenu, etc. – devront se faire en utilisant des mécanismes reposant sur des algorithmes de chiffrement reconnus et des protocoles normalisés par l'IETF (IPsec, TLS, SSH, etc.). Ces échanges comprennent principalement les communications suivantes :
  - ✓ les communications entre opérateur et l'ARJEL,
  - ✓ les communications réseaux entre joueurs et opérateur,
  - ✓ les communications réseaux entre les modules au sein du frontal ;
- [P] l'opérateur indiquera l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux au sein de ses plates-formes de jeux et du frontal : ces flux concernent les administrateurs faisant partie du personnel de l'opérateur tels les exploitants par exemple, les administrateurs externes tels ceux qui assurent la télémaintenance des matériels, etc.

La sécurisation des échanges entre l'ARJEL et l'opérateur s'appuiera sur des certificats X509v3 émis par l'ARJEL.

5.7.3.e.2 Authentification des administrateurs

- [E*] Les accès d'administration aux équipements des plates-formes de jeux et du frontal devront être protégés à l'aide des mécanismes suivants :
  - ✓ en priorité, une authentification par certificat X.509v3, par clef publique RSA ou par système à deux facteurs (dont un mot de passe à usage unique), si les applications et les systèmes le supportent,
  - ✓ ou bien une authentification par mot de passe, avec des règles de composition et de renouvellement conforme aux bonnes pratiques recommandées par le CERTA, que l'opérateur détaillera ; ces mots de passe devront être employés dans le cas de protocoles d'authentification par défi/réponse. Les authentifications en clair seront prohibées, et en l'absence de mode défi/réponse un chiffrement des communications sera obligatoire,
  - ✓ en complément de méthodes d'authentification précédentes, un contrôle d'accès basé sur les adresses IP sera réalisé ;
- [P] pour ses personnels exploitants, l'opérateur indiquera les mesures mises en œuvre lui permettant de garantir un haut niveau de sécurité dans la gestion des secrets d'authentification : robustesse des mots de passe et changement périodique, ou mieux authentification forte, etc.
- [P] l'opérateur indiquera si ses personnels exploitants utilisent régulièrement ou occasionnellement (astreintes par exemple) des accès distants pour administrer tout ou partie des systèmes. En cas de réponse positive, le soumissionnaire décrira précisément les

mécanismes mis en œuvre pour garantir la sécurité de ces accès distants, et le périmètre d'actions des intervenants accédant depuis l'extérieur.

5.7.3.f Gestion des configurations

- [E*] Au titre de la maintenance et du maintien en conditions de sécurité, l'opérateur devra suivre les évolutions logicielles des éditeurs de façon à être en mesure de se procurer les correctifs de sécurité mis à disposition régulièrement ;
- [E] l'opérateur devra au moins prohiber l'utilisation sur ses plates-formes des systèmes et logiciels obsolètes référencés par le CERTA ;
- |P] l'opérateur décrira dans sa proposition les moyens prévus permettant d'identifier et de prendre en compte les évolutions logicielles des constructeurs ;
- [E] à l'issue de la mise en œuvre d'un nouvel équipement ou de l'installation d'une nouvelle application, l'opérateur mettra à disposition de l'ARJEL la version à jour du dossier de définition incluant toutes les informations relatives à la configuration de ce nouvel élément ;
- [E] les composants systèmes, réseau et applicatifs mis en oeuvre par l'opérateur devront avoir fait l'objet d'une minimalisation de leur configuration et d'un durcissement en termes de sécurité : restriction des applications exécutées au démarrage, limitation du nombre d'applications en écoute sur le réseau, désactivation des fonctionnalités inutiles voire dangereuse (interface d'administration de serveurs d'application), suppression des comptes et mots de passe constructeurs, etc. ;
- [P] l'opérateur indiquera dans sa réponse les mesures de sécurisation adoptées sur chacun des composants de sa plate-forme ;
- [P] l'opérateur indiquera dans sa réponse les moyens prévus pour gérer les différentes versions des fichiers de configuration ainsi que leur sauvegarde ;
- [E*] afin de détecter d'éventuelles erreurs de manipulation mais aussi le résultat d'attaques, l'intégrité des fichiers de configuration des équipements devra être vérifiée régulièrement. Cette vérification devra pouvoir être faîte sur demande de l'ARJEL, et un rapport de diagnostic devra pouvoir lui être transmis.

5.7.3.g Gestion de la sécurité dans les cycles de développement

- [E] L'opérateur devra gérer la sécurité à chaque étape du cycle de développement de ses systèmes, dans les phases de définition, de développement, d'exploitation et d'utilisation, puis de maintenance et d'évolution ;
- [P] l'opérateur présentera les mesures de contrôle et méthodes d'évaluation de ses développements à chaque étape d'un projet de développement. S'il dispose d'un guide d'intégration de la sécurité des systèmes d'information dans les projets, il en fournira un exemplaire à l'ARJEL ;
- [E] l'opérateur devra respecter un référentiel de développement sécurisé pour les projets dont il assure le développement ;
- [E] l'opérateur devra contractualiser avec ses prestataires le respect d'un référentiel de développement sécurisé pour les projets dont il externaliserait la prise en charge ;
- [E] le référentiel de développement sécurisé devra en particulier aborder le problème de la validation des paramètres, notamment :
  - ✓ vérifier toutes les données transmises par l'utilisateur selon des critères de taille, type et caractères autorisés, et selon un mécanisme de liste blanche,
  - ✓ vérifier les données en entrée et en sortie,
  - ✓ utiliser une fonction de vérification des données identique et centralisée ;
- [E*] l'opérateur devra pouvoir transmettre à l'ARJEL l'ensemble de codes sources des logiciels de jeux utilisés sur ses plates-formes.

5.7.3.h Gestion des sauvegardes des données

- [E*] L'opérateur fournira les moyens de mettre en œuvre un service d'archivage afin d'assurer la conservation de l'ensemble de ses données de traitement, et en particulier celles stockées dans le coffre-fort du frontal. Ces sauvegardes seront mises à disposition de l'ARJEL par l'opérateur pour consultation et archivage. Le type de support et le format de la sauvegarde seront indiqués pour permettre à l'ARJEL de vérifier l'exploitabilité de ces sauvegardes et de leurs contenus ;
- [E*] la durée de conservation des informations est définie par le code du commerce, soit 5 ans suivant la fermeture du compte de jeu ;
- [E*] pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :
  - ✓ être protégées en intégrité,

- ✓ être accessibles aux personnes autorisées seulement,
- ✓ pouvoir être relues et exploitées ;

- [E] le niveau de protection des sauvegardes des archives doit être au moins équivalent au niveau de protection des archives : l'opérateur présentera dans sa réponse les mécanismes d'archivage ainsi que les moyens sécurisés de protection des archives qu'il est capable de mettre en œuvre ;
- [E*] la précision de l'horloge par rapport à laquelle les systèmes d'information se synchronisent pour dater les événements journalisés ou archivés doit être inférieure à 1 seconde par rapport au temps UTC. La source de temps doit être fiable ;
- [E*] une totale intégrité des données et des traitements est requise pour l'ensemble des données sur le frontal, et celles qui stockées dans le système d'information de l'opérateur sont liées aux activités de jeu, et sont identifiées comme auditables ;
- [P] l'opérateur détaillera dans sa réponse les modalités de son plan de sauvegarde : il précisera en particulier les modalités et les délais de restauration d'une sauvegarde suite à un incident et le ou les lieux de stockage des sauvegardes ainsi que les mesures de sécurité appliquées à ce(s) lieux.

5.7.3.i Gestion des données sensibles

- [P] l'opérateur décrira quelles sont les procédures et mécanismes mis en place afin de protéger les données qu'il traite, et notamment :
  - ✓ les données nominatives et personnelles de ses clients,
  - ✓ les données et statistiques de jeu ou de certains joueurs dont la connaissance pourrait avantager un joueur,
  - ✓ les données de jeu « secrètes » (par exemple les cartes des autres joueurs, ou celles qui n'ont pas été retournées lors d'une partie de poker).

5.7.3.j Gestion du générateur de nombres aléatoires

- [P] Parmi les systèmes qu'il décrira, l'opérateur attachera une attention particulière à la description des procédures et mécanismes mis en place afin de protéger le générateur de nombres aléatoires, et notamment
  - ✓ la surveillance de la série de nombres,
  - ✓ la protection d'une éventuelle graine de l'algorithme de génération de nombres aléatoires,
  - ✓ la protection de l'intégrité du logiciel.

5.7.3.k Gestion de la journalisation technique et fonctionnelle

- [E*] L'opérateur devra maintenir, et pouvoir fournir à l'ARJEL, les journaux des traces techniques pour les évènements clé. Une première liste des événements concernés :
  - ✓ accès aux modules sensibles de la plateforme de l'opérateur,
  - ✓ accès aux modules du frontal,
  - ✓ opérations de maintenance effectuées,
  - ✓ séquence des évènements aléatoires et des jeux issus de la séquence aléatoire,
  - ✓ ouverture et fermeture de la prise de paris ;
- [E*] si des personnes physiques sont à l'origine des évènements tracés, la journalisation permettra d'établir un lien entre l'identifiant technique utilisé dans la trace et la personne physique responsable des actions. Les évènements seront journalisés en s'appuyant sur une source de temps fiable ;
- [E*] concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un *package* Linux, …), toutes les traces disponibles au niveau des équipements seront activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté ;
- [E] l'opérateur consolidera l'ensemble des traces issues de la journalisation technique des différents équipements (réseau, système, applicatifs et sécurité), par exemple via l'application et le protocole syslog ;
- [E] les traces de sécurité issues de la journalisation technique des plates-formes seront analysées périodiquement par l'opérateur afin d'identifier les anomalies éventuelles ;
- [P] l'opérateur décrira d'une part les traces sécurité qu'il peut activer, et d'autre part les modalités d'analyse des traces qu'il met en œuvre (périodicité, outils d'analyse utilisés …) ;
- [E] les journaux techniques produits par les différents équipements doivent être conservés au minimum pendant trois mois en tant qu'archive ;
- [E] l'opérateur pourra mettre à disposition de l'ARJEL ces journaux bruts produits par les

différents équipements ou logiciels :

- [P] l'opérateur précisera le mode opératoire et la liste des journaux auxquels l'ARJEL aura accès (journaux de connexion locale ou des accès distants, journaux systèmes, journaux Web, journaux fonctionnels des applications, ou encore journaux générés par les SGBD, etc.) ;
- [E] les incidents ou les comportements anormaux pouvant avoir un impact sur la sécurité du service devront être traités et systématiquement faire l'objet d'une alerte et d'un compte-rendu écrit qui pourra être communiqué à l'ARJEL ;
- [P] l'opérateur présentera les moyens prévus pour la détection, le traitement et la notification des incidents, ainsi que leurs modalités de gestion (y compris les procédures d'escalade).

5.7.3.l Gestion des accès physiques

- [E*] Les locaux techniques devront être accessibles aux seules personnes habilitées par l'opérateur ;
- [E*] l'opérateur devra être en mesure d'identifier parfaitement les personnes ayant à intervenir dans ses locaux et sur ses équipements. Les fonctions et les autorisations d'accès de ces personnes devront être connues et maintenues à jour ;
- [E] les personnes ayant à intervenir sur les équipements des plates-formes devront avoir été sensibilisées à la sécurité des systèmes d'information (confidentialité des mots de passe et des données hébergées, etc.) ;
- [E] l'opérateur fournira à l'ARJEL les dispositions prises en matière de contrôle de la situation, notamment la vérification de l'absence de conflits d'intérêts, des candidats postulant pour un poste sensible, ainsi que les modalités de mise en sécurité de l'information lors de leur départ de la société (récupération des badges, gestion des mots de passe, etc.) ;
- [P] l'opérateur présentera dans sa réponse l'ensemble des mesures de sécurité concernant le personnel ;
- [E] les locaux abritant les équipements devront être sécurisés : serrure haute sécurité, alarme d'ouverture, enregistrement des accès, video-surveillance, etc.
- [E] l'accès physique à ces locaux devra être limité : filtrage des personnes, contrôle des accès physiques, etc.
- [P] l'opérateur présentera dans sa réponse les moyens de protection des locaux techniques mis en oeuvre.

5.7.3.m Gestion de l'environnement physique

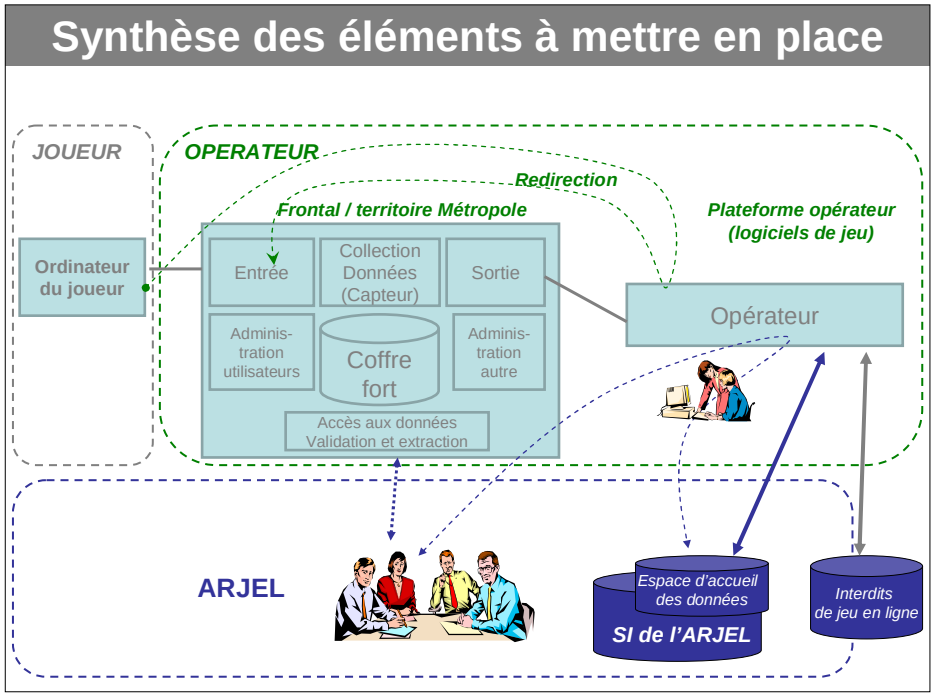
- [E] Les matériels et supports informatiques (support de sauvegarde, …) devront être placés dans des zones de sécurité physiques, conçues pour lutter contre les tentatives d'intrusion et de lutter contre les sinistres et accidents liées à l'environnement ;
- [E] la structure d'hébergement devra répondre aux normes de protection incendie établies par l'APSAD (Assemblée Plénière des Sociétés d'Assurance Dommage). L'opérateur détaillera les principes de détection et d'extinction incendie. Un incendie pourra faire l'objet d'une procédure de bascule sur un éventuel site de secours que l'opérateur décrira ;
- [E] le centre d'hébergement devra disposer, pour sa sécurité électronique, d'une double alimentation, d'onduleurs et d'un système de groupe électrogène principal et secondaire ;
- [E] un système de climatisations redondantes et indépendantes par salle devra assurer la stabilité des températures et du taux d'humidité. L'opérateur tiendra à disposition de l'ARJEL les caractéristiques techniques de ses installations de froid ;
- [E] tous les matériels (climatiseurs, panneaux électriques, …) utilisés par l'opérateur devront faire l'objet d'un contrat de maintenance ; l'opérateur en précisera les caractéristiques ;
- [P] l'opérateur précisera la nature du dispositif anti-foudre mis en œuvre ainsi que la vulnérabilité du centre d'hébergement au risque d'inondation ;
- [E] les sites d'exploitation devront être surveillés 24h/24 et 7j/7 ;
- [P] l'opérateur précisera les plans de continuité d'activité et plans de reprise d'activité qu'il aura pu élaborer dans le cadre de son activité et les modalités qu'il prévoit pour les adapter au contexte du frontal.

5.7.3.n Équipe sécurité

- [E] L'opérateur devra justifier d'une "équipe sécurité" chargée de surveiller tous les équipements réseau, systèmes et les applications. La sécurité logique des équipements sera réalisée sous le contrôle de cette équipe ;
- [P] l'opérateur fournira dans sa réponse l'ensemble des dispositions mises en œuvre

concernant l’équipe sécurité, ainsi que le plan de la charte de sécurité qui en encadre l'activité.

6 SYNTHESE DES ELEMENTS ATTENDUS DANS LE DOSSIER D'AGREMENT



Dans le cadre de la demande d'agrément, les différentes pièces à fournir sur le plan technique sont précisées dans le cahier des charges.

D'une façon synthétique, les éléments clés par domaine sont les suivants :

Pour ce qui concerne la mise en œuvre du frontal (partie 4.1 du dossier des exigences techniques) :
- fourniture de l'ensemble des éléments précisés dans la partie 4.1.8 du dossier des exigences techniques.

Pour ce qui concerne le logiciel de jeu (partie 5.2 du dossier des exigences techniques) :
- fourniture du code source du logiciel de jeu ;
- fourniture d'un rapport d'analyse détaillée des vulnérabilités de sécurité du code source ;
- fourniture d'un rapport d'analyse spécifique du générateur de nombre aléatoire ;
- fourniture d'un rapport d'analyse certifiant que les règles implémentées dans le logiciel de jeu sont bien conformes au jeu tel qu'il est présenté au joueur.

Pour ce qui concerne la plateforme de jeu (partie 5.3 du dossier des exigences techniques) :
- fourniture d'un rapport d'analyse détaillée des vulnérabilités de la plateforme de jeu.

Pour ce qui concerne les exigences organisationnelles et techniques (maturité SSI de l'opérateur, partie 5.7 du dossier des exigences techniques) :
- fourniture de l'ensemble des éléments répondant aux questions de la partie 5.7.

Le cahier des charges précise également le format des réponses (sous forme papier et sous forme électronique). Ces éléments, qui doivent être scrupuleusement respectés, sont rappelés ci-dessous :

- pour le dossier papier, les différents documents techniques devront être physiquement séparés des autres documents. Les sous parties correspondants aux 4 thèmes présentés ci-dessus ne devront pas être reliées mais constituer 4 éléments cohérents et correctement identifiés (frontal, logiciel de jeu, plateforme de jeu, maturité SSI) ;
- pour les versions électroniques (5 DVD), un répertoire spécifique baptisé « Eléments techniques » correspondant à la partie 11 du cahier des charges devra être créé. Dans ce répertoire, 4 sous répertoires devront être créés (« Frontal », « Logiciel de jeu », « Plateforme de jeu », « Maturité SSI »). Ces 4 répertoires engloberont les différents éléments demandés ci-dessus (sauf les codes sources qui seront fournis sur deux supports chiffrés dédiées, selon les modalités décrites dans la partie 3.3 des Annexes). Des sous répertoires explicites pourront utilement être créés.