

AUTORITÉ DE RÉGULATION DES JEUX EN LIGNE

MISSION DE PRÉFIGURATION

FAQ – FOIRE AUX QUESTIONS

Version du 12 mai 2010

LES QUESTIONS/RÉPONSES AJOUTÉES OU MODIFIÉES SONT EN BLEU

AVERTISSEMENT

La FAQ est un outil de dialogue, sans portée normative, mis à la disposition des utilisateurs du site de la mission de préfiguration de l'ARJEL.

Il contient des réponses aux questions les plus fréquemment posées et exclusivement relatives aux hypothèses de cahier des charges juridique et de dossier des exigences techniques, aujourd'hui en préparation.

Ces réponses sont donc formulées à partir du projet de loi en l'état et de documents de travail sans portée normative.

Ces réponses sont susceptibles de modifications pour tenir compte des évolutions que pourrait connaître le projet de loi, des textes d'application et des conditions de validation du cahier des charges et du dossier des exigences techniques par le Collège de l'ARJEL et s'agissant du cahier des charges, par les ministres compétents.

L'utilisation et l'exploitation de ces réponses ne sauraient engager la responsabilité de l'État.

Certaines réponses apportées aux questions posées ont pour conséquence la mise à jour du Dossier des exigences techniques, de ses annexes ainsi que des ressources techniques associées. Les réponses concernées sont signalées par une mention en rouge dans ce document.

Toutes les modifications seront réalisées en une seule fois. Les documents qui en résultent seront mis en ligne à l'arrêt de cette FAQ.

Seules les ressources techniques proprement dites seront modifiées en temps réel, de façon à en faciliter l'utilisation et l'intégration par les candidats à l'agrément.

QUESTIONS D'ORDRE GÉNÉRAL

Deux questions apparentées donnant lieu à une réponse commune :

1/ Les documents font référence à plusieurs décrets, est-il possible d'obtenir une version de travail ou à défaut les extraits qui sont référencés dans les documents ?

2/ Plusieurs articles (7.1.3, 7.2.2, 7.2.4 à 7.2.6, 7.3.1, 7.4.4, 9.2 et 9.3) du cahier des charges font référence à des projets de décrets. Des extraits de ces projets de décrets peuvent-ils être communiqués ?

La communication d'extraits des projets de décrets par l'ARJEL n'est pas prévue à ce jour.

* * *

Dans quelle mesure est-il possible de se rapprocher des membres ou experts de l'ARJEL concernant la constitution du dossier ?

A l'inverse, existe-t-il un partenaire compétent pour assister les futurs nouveaux entrants ?

La constitution d'un dossier de demande d'agrément relève de la seule responsabilité du demandeur. Dans le cadre du régime de délivrance des agréments, la mission de l'ARJEL consiste à délivrer ou non l'agrément demandé sur la base des éléments constitutifs de la demande d'agrément de l'entreprise candidate et ce, conformément aux dispositions de l'article 16 III du projet de loi et des textes réglementaires pris pour son application. En conséquence, l'ARJEL ne peut en aucune manière participer à la constitution du dossier de demande.

Le demandeur peut, s'il l'estime utile, requérir une assistance extérieure de son choix (avocat, consultant, ...) aux fins de l'aider à constituer son dossier.

* * *

A l'article 8 du projet de loi, quelles sont les règles pour évaluer la contre valeur des lots en nature ?

Les modalités d'évaluation de la contre valeur des lots en nature seront définies par décret.

* * *

A l'article 7 du projet de loi, quand l'ARJEL communiquera-t-elle la liste des compétitions sportives, les types de résultats, les phases de jeu ?

Conformément à l'article 7 du projet de loi, la liste des compétitions sportives, les types de résultats et les phases de jeu seront fixés pour chaque sport par l'ARJEL et ce, suivant des modalités définies par décret. Après la publication de ce décret, le collège de l'ARJEL se réunira donc pour arrêter ces listes par sport.

* * *

J'ai lu votre document « Ouverture à la concurrence et à la régulation du secteur des jeux d'argent en ligne - Projet de dossier des exigences techniques » et j'ai la question suivante : Le document est-il disponible en anglais ?

Les projets de cahiers des charges juridiques et dossier des exigences techniques sont disponibles uniquement en français.

* * *

Dans le développement de la plateforme de jeu, est-il possible d'utiliser pour la partie site web un CMS du type Joomla ou Drupal ?

Le choix des solutions techniques retenues pour composer la plate-forme de jeux relève uniquement de l'opérateur. L'historique des vulnérabilités d'une solution doit cependant constituer un critère de choix.

* * *

Nous avons développé des jeux de Casino (Black Jack et Stud Caribbean Poker) sous la forme de jeux de Cercle. A l'image des Cercles Français dans lesquels se pratique déjà ces jeux, les joueurs s'échangent la banque lors d'enchères organisées par l'opérateur. Ce dernier effectue un prélèvement sur le montant de l'adjudication qui donne droit à une session de x mains pour le joueur qui tient rôle de « Dealer ».

Notre ambition est de proposer aux joueurs Français cette variante en ligne, ainsi que l'organisation de tournois de Black jack et Stud Caribbean Poker (très comparables dans leurs caractéristiques aux tournois de Texas Hold'em). Quelle est la position de l'Arjel au regard de ces jeux ?

Un décret viendra préciser les jeux de cercle autorisés.

* * *

Jusqu'à quel niveau de granularité la comptabilité séparée devrait-elle descendre jusqu'au Net Gaming Revenue ou jusqu'aux coûts opérationnels ?

La tenue d'une comptabilité séparée par activité doit permettre de déterminer l'économie de chaque activité. Il convient donc d'y inclure l'ensemble des coûts directement affectables à l'activité faisant l'objet de la demande et d'utiliser des clés de répartition pour les coûts non directement affectables, cette analyse permettant d'estimer le résultat d'exploitation de l'activité en question.

* * *

Une société qui a pour activité le courtage de paris en ligne, c'est-à-dire qui propose à une communauté de parieurs des offres de paris de différents opérateurs agréés au terme de la nouvelle loi, qui gère les comptes des parieurs et qui place les paris, et qui est rémunéré par les parieurs, doit elle soumettre un dossier de licence ?

L'article 8-I du projet de loi dispose : « En matière de paris en ligne sur les épreuves hippiques ou sportives, sont seules autorisées l'organisation et la prise de paris enregistrés en compte par transfert de données numériques exclusivement par l'intermédiaire d'un service de communication au public en ligne, à l'initiative du joueur connecté directement au site de l'opérateur agréé ». L'article 9-III énonce : « Les mises sont enregistrées en compte par transfert de données numériques exclusivement par l'intermédiaire d'un service de communication au public en ligne, à l'initiative du joueur connecté directement au site de l'opérateur agréé ». Ces textes excluent clairement tout procédé d'intermédiation qui aboutirait à un contournement de l'exclusivité qui doit profiter aux opérateurs agréés. L'activité de courtage de paris en ligne est donc prohibée, d'où l'impossibilité de solliciter un agrément à l'effet de la pratiquer.

* * *

Sur un site offrant des jeux et paris autorisés par plusieurs agréments, le joueur doit il ouvrir un compte pour chaque jeux ou pari relevant d'un agrément ou peut il ouvrir un compte qui lui permet de jouer à tous les jeux et paris objets des différents agréments ?

Non, un compte joueur unique peut être proposé par un opérateur pour ses différents agréments.

* * *

Des joueurs « non français » peuvent-ils s'inscrire sur le site de l'opérateur et jouer contre les joueurs français. Si oui, doit-on tracer l'ensemble des événements liés à ces joueurs dans le coffre-fort ?

Toute personne est autorisée à jouer sur un site accessible depuis le territoire français, à la condition que celui-ci soit exploité par un opérateur agréé par l'ARJEL et ce, peu important l'Etat dont elle est ressortissante ou celui où elle a fixé sa résidence. Toute offre de jeux ou de paris en ligne d'un opérateur agréé doit être proposée conformément à toutes les exigences du droit français, exigences que l'opérateur s'oblige à respecter lors du dépôt de son dossier de demande d'agrément.

* * *

Nous savons que nous ne serons pas prêts pour l'ouverture. Nous aimerions néanmoins faire partie des premiers déposants. Une déclaration d'intention de postuler plus tard est-elle recevable par l'ARJEL ?

Le dépôt d'une "déclaration d'intention de postuler" amènera l'ARJEL à considérer comme incomplet le dossier du déposant, ce qui donnera lieu à application, notamment, de l'article 2.3.2. du projet de cahier des charges, aux termes duquel : "Lorsque le dossier de demande

est incomplet, l'ARJEL adresse au candidat un courrier lui demandant d'y remédier dans un délai qui ne peut être inférieur à quinze jours. L'instruction est interrompue pendant ce délai. Si à l'expiration du délai imparti, l'entreprise candidate n'a pas répondu à la demande de l'ARJEL, sa demande d'agrément est considérée comme incomplète et par suite, rejetée". Ce rejet obligera l'entreprise sollicitant l'agrément au dépôt d'un nouveau dossier de demande d'agrément, comprenant cette fois l'intégralité des pièces exigées, en ce compris celles qui avaient pu être fournies lors de la demande initiale.

* * *

Pourriez-vous nous confirmer qu'en accord avec les articles 13 et 14 du texte adopté, le taux de retour moyen maximal aux joueurs ne sera pas applicable aux jeux de cercle ?

En matière de jeux de cercle, la Loi ne prévoit aucune proportion maximale des sommes versées en moyenne aux joueurs. Il en va différemment en matière de paris sportifs et hippiques.

* * *

Entreprise de conseil, d'audit et de développement d'algorithme de jeu en ligne, nous souhaitons jouer le rôle de tiers de confiance auprès des opérateurs de jeu et d'expert auprès des instances de contrôle.

L'ARJEL délivre-t-elle des agréments ou des certifications aux instances d'audit et de contrôles des opérateurs de jeu en ligne ?

Si non, comment l'ARJEL s'assure-t-elle du sérieux et de l'indépendance des instances d'audit et de contrôles ?

Non, l'ARJEL ne délivre pas d'agrément ou de certification aux instances d'audit et de contrôle.

Les deux seules situations conduisant à l'établissement d'une liste d'entreprises sont : la liste des centres d'évaluation agréés pour la CSPN (http://www.ssi.gouv.fr/site_article7.html) et la liste des organismes pouvant procéder à la certification prévue à l'article 23 (anciennement 17) de la loi.

* * *

Conformément à l'article 17 de la loi lorsque l'opérateur ferme un compte joueur provisoire pour non-conformité entre les pièces d'identité et les données saisies par le joueur que doit-on faire des sommes que les joueurs ont versé sur leur compte « provisoire » ?

Doit-on les restituer ? Si oui à qui ? Les conserver ?

Le joueur qui finalement ouvre un compte après une première tentative infructueuse peut-il demander restitution des sommes versées précédemment?

Le joueur qui finalement n'ouvre pas de compte peut-il en demander remboursement ?

Les questions que vous posez trouveront leurs réponses dans le décret relatif à la mise à disposition de l'offre de jeux et de paris par les opérateurs agréés de jeux ou de paris en ligne. Ce décret sera publié prochainement.

* * *

Je suis le Conseil d'une entreprise qui, dans le cadre de la prochaine ouverture à la concurrence du secteur des jeux d'argent et de hasard en ligne, envisage de déposer un dossier de demande d'agrément. Je souhaite appeler votre attention sur le fait que les projets de formulaires qui ont été mis en ligne sur le site Internet de la mission de préfiguration de l'ARJEL sont des fichiers PDF dont les champs destinés à être complétés ne sont malheureusement pas modifiables. Afin d'être en mesure de respecter la présentation desdits formulaires, est-il envisagé de rendre ces documents disponibles sous un format - PDF ou autre - permettant de les remplir de façon électronique ?

Des formulaires renseignables ont été mis en ligne le 12 mai.

* * *

Représentant légal : le représentant en France auquel une notification des griefs pourrait être faite pourrait-il être toute personne agissant en vertu d'un mandat spécial?

Il s'agit du responsable mentionné à l'article 16 de la Loi.

* * *

<p style="text-align: center;">QUESTIONS RELATIVES AU CAHIER DES CHARGES</p>

CDC Partie 2.2.1

Quand le formulaire du dossier d'agrément sera-t-il disponible ? Quel délai doit-on anticiper pour mettre tous les documents qui auront été préparés et collectés dans un format conforme avec le formulaire ?

Comme précédemment pour le projet de cahier des charges et le projet de dossier des exigences techniques, la mission de préfiguration de l'ARJEL procèdera à la mise en ligne du projet de formulaire de demande d'agrément, lequel sera accompagné des projets de formulaires de tableaux financiers. La date de mise en ligne des projets de formulaires n'est pas fixée à ce jour. Nous espérons pouvoir y procéder dans le courant du mois d'avril.

CDC Partie 2.2.4

La traduction assermentée s'applique-t-elle uniquement aux documents officiels et aux contrats en langue étrangère ?

L'article 2.2.4 du projet de cahier des charges dispose : « Les pièces et documents fournis à l'appui de la demande d'agrément sont rédigés ou traduits en français. En cas de traduction, celle-ci devra être établie par un traducteur assermenté ».

L'article 2.2.4 ne distingue pas suivant la nature ou le caractère des pièces et documents produits.

Par suite, la traduction assermentée concerne tous les éléments joints au dossier de demande d'agrément.

* * *

Par qui les copies de documents doivent-elles être certifiées conformes ? Y a-t-il des exigences particulières pour certains documents, ex. pièce d'identité des dirigeants au 3.2.c du cahier des charges ?

L'article 2.2.4 du projet de cahier des charges dispose : « Les copies produites doivent être certifiées conformes à l'original. En cas de production d'une copie, l'ARJEL peut demander la présentation de l'original ».

Il appartient à l'entreprise sollicitant un agrément de certifier elle-même que la copie est conforme à l'original. Cette certification peut être réalisée, notamment, par l'opposition d'une formule du type « Certifiée conforme à l'original » apposée sur chacun des documents produits, en première page de ceux-ci.

Toutefois, les copies transmises doivent être lisibles.

En cas de doute sur l'authenticité du document original reproduit ou sur l'authenticité de la photocopie elle-même, l'ARJEL est fondée à demander la présentation de l'original.

* * *

Dans le cadre de la partie « homologation » les rapports fournis à l'ARJEL doivent-ils être rédigés en français ? Dans le cas où une traduction serait acceptée, quelles sont les exigences pour effectuer la traduction ?

Périmètre de la documentation en traduction assermentée : tous les documents traduits doivent-ils l'être par un traducteur assermenté ou s'agit-il seulement des documents majeurs (à définir) ou externes ?

Les traducteurs assermentés doivent-ils l'être nécessairement en France ?

La société qui effectue les audits doit-elle être française ?

Comme le prévoit l'article 2.2.4 du projet de cahier des charges au titre de ses dispositions générales, « le dossier de demande d'agrément est rédigé en langue française. Les pièces et documents fournis à l'appui de la demande d'agrément sont rédigés ou traduits en français. En cas de traduction, celle-ci devra être établie par un traducteur assermenté. »

Tous les documents communiqués à l'ARJEL qui ne sont pas rédigés en français doivent faire l'objet d'une traduction par un traducteur assermenté. Aucune exception à ce principe n'est posée.

Le traducteur visé à l'article 2.2.4 s'entend d'un traducteur assermenté en France ou habilité à intervenir auprès des autorités judiciaires ou administratives d'un autre État membre de l'Union européenne, ou d'un autre État partie à l'accord sur l'Espace économique européen

L'entreprise effectuant les audits n'a pas à être française, le rapport d'audit devant lui être communiqué en français.

CDC Partie 2.2.5

L'ARJEL prévoit-elle de mettre à disposition son certificat public afin de chiffrer les informations sur les supports informatiques qui seront remis (CD, DVD) ?

L'ARJEL mettra à disposition des opérateurs un certificat de chiffrement X.509v3 ainsi qu'un certificat PGP/GPG, pour assurer la transmission des informations les plus sensibles. Les mécanismes de chiffrement fondés sur la cryptographie à clef publique, et l'emploi de solutions logicielles éprouvées seront privilégiés (ex: GPG, etc.), même si des solutions alternatives peuvent être proposées (ex: Truecrypt, avec keyfile et mot de passe transmis par un mécanisme hors-bande, voire transmis via PGP ou S/MIME, etc.).

Les solutions de type « archive compressée, protégée par un mot de passe » sont proscrites.

L'emploi d'un logiciel évalué ou certifié par l'ANSSI serait un plus, mais ne constitue pas une obligation.

CDC Partie 2.3.2

Qu'en est-il dans le cadre d'une société qui se crée au moment de la demande d'agrément ? Quels sont les documents à fournir dans ce cas ?

Bien que n'étant pas constituée à la date du dépôt de son dossier de demande d'agrément, une société en formation peut déposer un dossier de demande d'agrément. Cependant, son dossier sera considéré comme incomplet au sens de l'article 2.3.2 du projet de cahier des charges. L'instruction de sa demande sera suspendue jusqu'au moment où elle aura communiqué le ou les documents établissant, au regard du droit applicable, qu'elle est définitivement constituée. La communication de ces documents devra intervenir dans un délai, qui ne peut être inférieur à quinze jours, fixé par l'ARJEL et ce, à peine de rejet de la demande d'agrément.

Une société en cours de formation ne peut, par nature, être titulaire d'un agrément.

CDC Partie 2.5

Cahier des charges/projet de Loi : pouvez-vous préciser la définition d'un plan d'affaires ?

Les projets de formulaires de tableaux financiers mentionnés au 2.5 du projet de cahier des charges seront prochainement mis en ligne sur le site de la mission de préfiguration de l'ARJEL, ceux-ci comprendront les formats détaillés de comptes sociaux (informations comptables, compte de résultat, bilan), de plans d'affaires et de tableaux de flux de trésorerie devant être renseignés par le demandeur.

Le plan d'affaires attendu intégrera :

- *les informations générales permettant de mieux comprendre les hypothèses de développement de la société ;*
- *les données financières permettant de comprendre l'économie propre au projet jusqu'au résultat d'exploitation ;*
- *les données financières prévisionnelles attendues du demandeur jusqu'au résultat net.*

CDC Partie 2.6

Est-ce-que, dans l'un et l'autre cas, le demandeur (s'agissant toujours d'un seul demandeur) doit le droit fixe pour la demande de délivrance et le droit annuel une seule fois (par typologie d'agrément) indépendamment du nombre de sites marque blanche ?

Les droits seront dus en fonction du nombre d'agréments demandés et obtenus. Un décret viendra préciser les montants.

CDC Partie 3

Deux questions apparentées donnant lieu à une réponse commune :

1/ Qu'entendez-vous par *équipement* dans « lieu de situation de ses équipements » ? (article 3.2.b du projet de cahier des charges)

2/ Pourriez-vous préciser les notions d'équipements (section 3.2.b) et de moyens matériels (section 3.3) ?

L'article 10 du projet de loi dispose que « l'entreprise sollicitant l'agrément ne peut avoir son siège social, une filiale ou un équipement dans un Etat ou territoire non coopératif au sens de l'article 238-0 A du code général des impôts. »

Au vu des travaux et débats parlementaires et en l'état des hypothèses de travail retenues, les équipements visés à l'article 3.2.b. du projet de cahier des charges sont compris comme tout équipement destiné à l'activité de jeux ou de paris en ligne, notamment tout matériel ou logiciel impliqué dans l'infrastructure de jeu ou de paris tels que les terminaux, les serveurs sur lesquels le site est hébergé et ceux sur lesquels les données de jeu et du compte joueur sont traitées etc.

S'agissant des moyens matériels dont le demandeur à l'agrément doit justifier au titre de l'article 10 du projet de loi, l'article 3.3 du projet de cahier des charges prévoit en l'état qu'il convient de fournir les éléments listés à cet article, à savoir liste des sous-traitants précisant la nature des prestations réalisées et informations relatives à l'usage, la localisation, le titre d'occupation, la superficie des locaux utilisés par le demandeur.

* * *

A l'article 10 du projet de loi, les Etats ou territoires non coopératifs au sens de l'article 238-0 du CGI sont-ils bien uniquement ceux visés récemment dans l'arrêté du 12 février 2010 ?

La liste des Etats et territoires mentionnée au deuxième alinéa du 1 de l'article 238-0 A du code général des impôts a effectivement été fixée au titre de l'année 2010 par arrêté du 12 février 2010 publié au JORF du 17 février 2010.

* * *

Informations personnelles : le comité stratégique fait-il part des organes de délibération au sens de cette question?

Non.

CDC Partie 3.1

Localisation des équipements du demandeur : le demandeur est une société française de nouvelle création, filiale d'un groupe étranger basé dans un autre pays CE. Est-il nécessaire de spécifier la localisation des équipements qui font part de la plateforme du groupe ou seulement les équipements sous le contrôle du demandeur?

Il est important de justifier le lieu de situation de tout équipement utilisé par l'opérateur.

* * *

Quels documents faut-il produire pour justifier de la localisation des équipements?

Tout document utile aux fins de justifier le lieu de situation des équipements.

CDC Partie 3.2

Que signifie *organique* dans « des liens organiques des sociétés du groupe... » ?

L'article 3.2 du projet de cahier des charges prévoit que lorsque l'entreprise qui demande l'agrément est une personne morale, elle doit justifier des liens organiques des sociétés du groupe auquel elle appartient le cas échéant.

Il s'agit de fournir une vision globale du groupe auquel le demandeur à l'agrément appartient le cas échéant, en précisant les liens entre les sociétés de ce groupe justifiant qu'une société fait partie dudit groupe. Cette information peut par exemple être fournie sous la forme d'un schéma de présentation du groupe faisant apparaître l'ensemble des sociétés et les participations des unes dans les autres (pourcentage de détention).

* * *

Je me permets de vous envoyer ce message pour vous poser une question relative aux conditions d'obtention de l'agrément sur les paris sportifs : supposons qu'un regroupement de personnes compétentes souhaitent créer une société pour opérer sur le secteur des paris sportifs en France. Ces personnes ont déjà développé le site de paris sportifs en respectant strictement les exigences techniques formulées par l'ARJEL. Pour autant, ces personnes n'ont pas encore créé leur société puisqu'elles ne peuvent pas exercer leur activité sans l'agrément délivré par l'ARJEL. Ces personnes, doivent-elles obligatoirement créer leur société avant de formuler leur demande d'agrément auprès de l'ARJEL ? Autrement dit, l'ARJEL peut-elle délivrer un agrément sur la base d'un examen de la plateforme (déjà créée), d'une vérification sur les personnes qui formulent la demande et d'une analyse du business plan qui garantirait la solidité financière de la future société ? Cette question se pose pour toutes les personnes physiques qui souhaitent créer une société de jeux en ligne payants en France. Ils se demandent s'ils doivent démissionner de leur fonction actuelle pour créer une société et ainsi pouvoir demander un agrément à l'ARJEL, ou s'ils peuvent formuler une demande en tant que personnes physiques pour ensuite décider de la création de leur société à partir du

moment où l'ARJEL leur aura donné la permission (éventuellement sous conditions) d'exercer leur activité ?

Une société en cours de formation peut déposer un dossier de demande d'agrément. Toutefois, son dossier doit être alors considéré comme incomplet au sens de l'article 2.3.2 du projet de cahier des charges. L'instruction de sa demande est suspendue jusqu'au jour de la communication du ou des documents établissant, au regard du droit applicable, la constitution définitive de la société. Cette communication doit intervenir dans un délai, prescrit à peine de rejet de la demande d'agrément, qui ne peut être inférieur à quinze jours et fixé par l'ARJEL.

Une société en cours de formation ne peut, par nature, être titulaire d'un agrément.

L'article 16, alinéa 1er, du projet de loi dispose que l'agrément « n'est pas cessible ». Par conséquent, une personne physique ne peut transférer l'agrément, qui lui a été délivré à titre personnel, à une société qu'elle aurait constituée pour l'exploiter.

* * *

Au point 3.2, d) il est indiqué :

« Si l'entreprise est une personne morale, elle informe l'ARJEL...des condamnations dont elle même, son ou ses propriétaires, ses dirigeants, ou ses mandataires sociaux fait l'objet depuis moins de 10 ans : »

Question :

Est-il nécessaire de produire un « Extrait de Casier Judiciaire » pour tout propriétaire, personne physique ou de personne morale, détenant plus de 5% du capital, ou bien la production de ce document peut-elle se limiter aux seuls dirigeants, mandataires sociaux ?

L'article 3.2, point d, du projet de cahier des charges énonce que l'entreprise sollicitant l'agrément informe l'ARJEL des condamnations suivantes dont "ses dirigeants ou ses mandataires sociaux ont, le cas échéant, fait l'objet depuis moins de dix ans, comme auteur ou complice". Le texte vise donc toute les personnes, physique ou morale, détenant un pouvoir de direction ou un mandat social au sein de la personne morale sollicitant l'agrément, peu important la fraction du capital social de cette dernière qu'elle détient.

CDC Partie 3.3

La description des moyens humains et matériels doit elle se limiter à l'activité internet de l'opérateur ou s'agit-il d'éléments concernant l'ensemble de l'activité d'un opérateur ?

L'article 12 du projet de loi dispose que « L'entreprise justifie de ses moyens humains et matériels et communique l'ensemble des informations comptables et financières de nature à attester sa solidité financière et sa capacité à assumer les investissements nécessaires au respect de ses obligations légales et réglementaires. »

Dans ce cadre, l'article 3.3 du projet de cahier des charges demande à l'entreprise de justifier des moyens humains et matériels affectés à l'ensemble de ses activités, mais uniquement par la fourniture des documents listés aux a, b) et c).

* * *

Deux questions apparentées donnant lieu à une réponse commune :

1/ Quel est le sens de sous-traitant à l'article 3.3 : s'agit-il uniquement des prestataires pour l'hébergement et l'exploitation du site internet de l'opérateur ?

2/ Pourriez-vous préciser la notion de sous-traitants (section 3.3 b) ?

L'article 11 alinéa 1^{er} du projet de loi dispose : « L'entreprise sollicitant l'agrément présente la nature, les caractéristiques et les modalités d'exploitation, d'organisation ou de sous-traitance du site de jeux en ligne et des opérations de jeu ou de pari en ligne qu'elle entend proposer au public, ainsi que les caractéristiques des plateformes et logiciels de jeux et de traitement de paris qu'elle compte utiliser ». L'alinéa 6 de ce texte ajoute : « Elle donne connaissance des contrats de fourniture ou de sous-traitance d'opérations de jeu ou de pari en ligne qu'elle a conclus ».

Les articles 3.3.b), 5.6 et 6.2 du projet de cahier des charges transcrivent ces dispositions.

La notion de « sous-traitance » doit être entendue ici dans son acception la plus large. Elle englobe tous les contrats par lesquels le candidat à l'agrément a ou entend conclure avec un prestataire de service pour la réalisation de son activité de jeu ou pari en ligne. Elle inclut, de surcroît, toutes les conventions par lesquelles ce prestataire confie l'exécution de ses propres obligations à une entreprise tierce.

Tous les contrats, sans exception, qui répondent à cette définition et se rapportent à ladite activité de jeu ou pari en ligne doivent être transmis.

* * *

A plusieurs reprises, il est demandé des informations concernant « les sous-traitants » (3.3.b, 5.6 et 6.2), pouvez-vous confirmer que l'information requise concerne uniquement les sous-traitants qui ont un rapport direct avec l'offre de paris et de jeux qui sera proposée ?

L'article 11 alinéa 1^{er} du projet de loi dispose : « L'entreprise sollicitant l'agrément présente la nature, les caractéristiques et les modalités d'exploitation, d'organisation ou de sous-traitance du site de jeux en ligne et des opérations de jeu ou de pari en ligne qu'elle entend proposer au public, ainsi que les caractéristiques des plateformes et logiciels de jeux et de traitement de paris qu'elle compte utiliser ». L'alinéa 6 de ce texte ajoute : « Elle donne connaissance des contrats de fourniture ou de sous-traitance d'opérations de jeu ou de pari en ligne qu'elle a conclus ».

Les articles 3.3.b), 5.6 et 6.2 du projet de cahier des charges transcrivent ces dispositions.

La notion de « sous-traitance » doit être entendue ici comme visant tous les contrats de prestation de services que le candidat à l'agrément a déjà ou a vocation à conclure pour la réalisation de son activité. Figurent parmi les contrats visés ceux par lesquels le prestataire de services confie, à son tour, l'exécution de sa propre mission à une entreprise tierce.

Tous les contrats qui répondent à cette définition et se rapportent spécifiquement à ladite activité de jeux ou de paris en ligne doivent, sans exception, être transmis à l'ARJEL.

* * *

Pouvez-vous préciser la définition d'un Dirigeant ainsi que celle d'un sous-traitant ?

Est un dirigeant la personne qui exerce, en toute indépendance, une activité positive de direction et de gestion.

La notion de « sous-traitance » doit être entendue ici comme visant tous les contrats de prestation de services concernant la réalisation de l'activité jeux et paris de l'opérateur. Sont donc visés, d'une part, tous les contrats conclus directement par l'opérateur avec un prestataire de services, et, d'autre part, tous ceux par lesquels ce dernier confie à son tour la mission qui lui a été attribuée à un tiers.

* * *

Est-il possible pour le titulaire de l'agrément de confier à une société tierce (voire de son groupe) le soin de gérer, en ses lieux et place mais sous sa responsabilité, l'ensemble des obligations relatives à la gestion des comptes clients (notamment perception des mises) ?

Le demandeur à l'agrément est fondé à confier à un tiers l'exécution de certaines des obligations mises à sa charge. Cela étant, la signature de ces contrats de prestation de services ne dispense pas l'opérateur de ses obligations au regard notamment, d'une part, de la future loi relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, de l'autre, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

* * *

S'agit-il de la société requérante ou du groupe dont elle est filiale ?

La personne visée à l'article 3.3. du projet de cahier des charges est celle qui requiert la délivrance d'un agrément. Les informations qu'elle communique en application de ce texte peuvent la conduire, le cas échéant, à fournir à l'ARJEL certaines données concernant le groupe dont elle constitue une filiale.

* * *

Moyens humains et matériels : quelle est la définition précise d'effectifs? S'agit-il nécessairement de salaires de la société qui demande l'agrément?

Oui. A noter toutefois que les moyens humains incluent par ailleurs les sous-traitants.

* * *

Dans le cas d' un demandeur qui est une société française de nouvelle création, filiale d' un groupe étranger basé dans un autre pays CE: au début le demandeur n'aura pratiquement pas d' effectifs directement affectés car le fonctionnement de l'activité sera assuré, d' une part par les ressources matérielles et humaines du groupe de provenance (pour les opérations de jeu) et, d'autre part, par les ressources des partenaires français (partenaires technologiques, conseils, partenaires en marque blanche pour l'activité commerciale, etc.) Faut-il décrire les effectifs affectés à l'activité par ces prestataires de service ?

Oui.

CDC Partie 3.4

Quid de la procédure de licence dans un Etat membre d'origine ? En quoi cela favorise-t-il la candidature d'un candidat à l'agrément en France ?

L'article 11, alinéa 6, du projet de loi dispose que l'entreprise sollicitant l'agrément « communique, à titre d'information, dans l'hypothèse où elle opère légalement dans son Etat d'établissement pour une même catégorie de jeux ou de paris en ligne, les exigences et, en général, la surveillance réglementaire et le régime des sanctions auxquelles elle est déjà soumise dans cet Etat ». Cette disposition est reprise dans la partie 3. 4 du projet de cahier des charges. L'obtention d'un agrément dans un autre Etat membre de l'Union européenne ne dispense donc pas son titulaire de demander un agrément à l'ARJEL s'il entend proposer en France des jeux d'argent et de hasard en ligne. La communication des règles de droit de l'Etat d'origine doit permettre à l'ARJEL de connaître, sans être liée par elle, l'appréciation qu'une autorité s'exprimant au nom d'un autre Etat membre a pu formuler.

* * *

Quelles documentations sont précisément requises comme « état du droit applicable et du régime de contrôle de l'activité de jeux ou de paris en ligne » dans le cas où l'entreprise opère légalement dans son Etat d'établissement ? La fourniture de ces éléments est-elle obligatoire ou facultative ?

L'article 3.4. du projet de cahier des charges reprend les dispositions de l'article 11, alinéa 6, du projet de loi, lequel dispose que l'entreprise sollicitant l'agrément « communique à titre d'information, dans l'hypothèse où elle opère légalement dans son Etat d'établissement pour une même catégorie de jeux ou de paris en ligne, les exigences et, en général, la surveillance réglementaire et le régime des sanctions auxquelles elle est déjà soumise dans cet Etat ». Cette communication est faite à titre d'information et, de ce fait, facultative. Les informations juridiques ainsi transmises doivent être suffisamment exhaustives et précises pour permettre à

l'ARJEL d'avoir une vision éclairée du système juridique duquel relève par ailleurs, à l'étranger, le candidat à l'agrément en France.

* * *

La présentation des modalités de licence dans pays d'établissement est-elle obligatoire lorsque la structure juridique agréée/ licenciée est différente mais que l'actionnaire est le même?

Conformément aux dispositions du cahier des charges, ces informations ne sont en toute hypothèse transmises qu'à titre d'information.

CDC Partie 4.1

Lorsque la société qui fait la demande de licence n'a pas eu d'activité avant l'obtention de la licence, nous comprenons que nous n'avons à produire que les états de trésorerie 2010 et 2011. Etes-vous d'accord ?

Conformément au projet de loi, l'entreprise sollicite un agrément et non une licence.

S'agissant des tableaux de trésorerie demandés à l'article 4.1.d du projet de cahier des charges, lorsque l'entreprise qui demande l'agrément n'a pas eu d'activité antérieurement à sa demande d'agrément, elle fournit effectivement au moins les états de trésorerie de l'année de la demande d'agrément et de l'exercice comptable suivant.

* * *

Plan d'affaires correspond selon notre interprétation à :

- **Mises**
- **Retour aux joueurs**
- **Bonus distribués aux joueurs**
- **Rake (poker)**
- **Nombre de joueurs actifs (ces éléments par type de jeu)**
- **Dépenses marketing,**

Est-ce conforme aux attentes de l'ARJEL ?

Les projets de formulaires de tableaux financiers mentionnés au 2.5 du projet de cahier des charges seront prochainement mis en ligne sur le site de la mission de préfiguration de l'ARJEL, ceux-ci comprendront les formats détaillés de comptes sociaux (informations comptables, compte de résultat, bilan), de plans d'affaires et de tableaux de flux de trésorerie devant être renseignés par le demandeur.

Le plan d'affaires attendu intégrera :

- *les informations générales permettant de mieux comprendre les hypothèses de développement de la société ;*

- les données financières permettant de comprendre l'économie propre au projet jusqu'au résultat d'exploitation ;
- les données financières prévisionnelles attendues du demandeur jusqu'au résultat net.

* * *

Informations économiques, financières et comptables ; pièces à fournir. Le plan d'affaires synthétiques des activités développées sur le site en .fr et le plan de trésorerie relatif est un document différent de ce qui est demandé dans le formulaire financier ?

Non.

CDC Partie 4.1g

il est demandé de fournir un « RIB justifiant l'ouverture d'un compte dans un établissement de crédit d'un Etat membre de la communauté européenne, (...), dédié exclusivement aux opérations d'encaissement et de paiement liées aux jeux ou paris, offerts à partir de son site .fr. ». Certaines banques françaises attendent la publication des décrets et du cahier des charges définitif pour apprécier les modalités exactes qui seront exigées par la législateur et/ou le régulateur sur le fonctionnement de ces comptes. Par conséquent il risque de ne pas être possible d'avoir le numéro du compte concerné lors du dépôt du dossier. Le numéro de marchand communiqué par cette même banque complété par un courrier de la banque précisant cette limitation peuvent-ils être jugés suffisants au regard de cette exigence? il ne faudrait pas que des banques d'autres pays de la Communauté européenne, peut-être plus habituées à cette industrie - créent une situation de distorsion en accordant l'ouverture de ces comptes à des opérateurs installés à l'étranger , avant publication de ces exigences.

L'article 18, alinéa 2, de la Loi énonce que l'entreprise sollicitant l'agrément "justifie de la disposition d'un compte ouvert dans un établissement de crédit établi dans un Etat membre de la Communauté européenne ou un Etat partie à l'accord sur l'Espace Economique Européen ayant conclu avec la France une convention d'assistance administrative en vue de lutter contre la fraude et l'évasion fiscales, sur lesquels sont exclusivement réalisées les opérations d'encaissement et de paiement liées aux jeux et paris qu'elle propose légalement en France". L'article 4.1, point g, du projet de cahier des charges reprend cette exigence qu'il concrétise en prévoyant la fourniture d'un document, en l'occurrence un RIB ou un IBAN, prouvant l'ouverture du compte requis. Il n'existe aucune dérogation à cette règle, qui ne porte, en elle-même, aucun risque de distorsion de concurrence.

CDC Partie 5

Les contrats dont il faut fournir des copies non-biffées se limitent-ils aux contrats de licences, d'affiliation, de sous-traitance d'opérations de jeu ou de paris, de sous-traitance pour l'exploitation du site et aux contrats liant l'entreprises à d'autres entreprises exerçant une activité de jeu ou de paris en ligne ?

Au titre des informations relatives au site de jeux en ligne et aux opérations de jeu des parties 5 et 6 du projet de cahier des charges, les contrats dont il faut fournir des copies non-biffées sont effectivement ceux listés.

CDC Partie 5.1

Il est indiqué dans le cahier des charges que l'opérateur doit fournir les certificats d'enregistrement des noms de domaine permettant l'accès à son site. Cela signifie-t-il qu'il doit en être propriétaire ?

La charte applicable aux noms de domaine en .fr (charte AFNIC) ne reconnaît pas des propriétaires mais des titulaires.

Le titulaire des noms de domaine permettant l'accès au site doit avoir un lien de droit avec l'opérateur.

Si l'opérateur n'est pas directement titulaire des noms de domaine, il doit indiquer à l'ARJEL la nature de ce lien et la façon dont il exerce ses prérogatives sur les noms de domaine qu'il utilise.

CDC Partie 5.2

Que signifie *nature* dans « nature du site » ?

Conformément à l'article 11 du projet de loi, « l'entreprise sollicitant l'agrément présente la nature, les caractéristiques et les modalités d'exploitation, d'organisation ou de sous-traitance du site de jeux en ligne et des opérations de jeu ou de pari en ligne qu'elle entend proposer au public, ainsi que les caractéristiques des plateformes et logiciels de jeux et de traitement de paris qu'elle compte utiliser. »

Dans ce cadre, le projet de cahier des charges précise au 5.2 que la présentation de la nature du site concerne notamment la présentation de l'ensemble des activités et des prestations proposées.

CDC Partie 5.3

En tant que sous-traitant pour une marque, sera-t-il nécessaire de demander une licence pour chacun des « white labels » ou existera-t-il une procédure de notification et de sous-agrément dans la même catégorie (par avenant par exemple) ?

Quel sera le coût de la demande d'agrément pour chacun des contrats de sous-traitance « white labels »

Seul un opérateur de jeux ou de paris en ligne, au sens de l'article 5 du projet de loi relatif à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, peut demander l'agrément prévu à l'article 16 dudit projet de loi. Le fait d'être opérateur de jeux ou de paris en ligne emporte la responsabilité juridique liée à l'activité de jeux ou de paris en ligne. Dans le cadre d'un dispositif en marque blanche, la question est de savoir lequel des cocontractants exerce l'activité d'opérateur de jeux ou de paris en ligne, en

particulier lequel s'engage contractuellement avec les joueurs. Si le cocontractant n'est qu'un prestataire technique de l'opérateur, il n'aura aucune obligation de demander un agrément. En effet, au terme du projet de loi, il n'existe aucune procédure particulière d'agrément ou de sous-agrément pour les prestataires techniques.

Par ailleurs, un opérateur agréé pourra opérer sous différents noms de domaine et marques dès lors, d'une part, qu'il les aura déclarés préalablement à l'ARJEL, d'autre part, que les joueurs seront pleinement informés de l'identité de l'opérateur agréé et responsable.

* * *

Informations relatives au site de jeu en ligne. Nous avons l'intention de demander l'agrément en tant qu'opérateur, pour mettre en œuvre un certain nombre de sites en marque blanche pour le compte de nos affiliés.

La dernière version de la FAQ récite à la p.15: Par ailleurs, un opérateur agréé pourra opérer sous différents noms de domaine et marques dès lors, d'une part, qu'il les aura déclarés préalablement à l'ARJEL, d'autre part, que les joueurs seront pleinement informés de l'identité de l'opérateur agréé et responsable. »

Pour nous permettre de mieux comprendre les possibles configurations, nous présenterons deux stratégies d'organisation des sites que nous voulons proposer.

Stratégie 1) : Il existe un domaine de premier niveau: « opérateur.fr » dont le demandeur est titulaire. Chaque affilié est titulaire du domaine de premier niveau de son propre site « marque blanche1 », « marque blanche2 », etc. L'activité de jeu (enregistrement, jeux et mises, gestion du compte joueur) se passe sur des sous-domaines du site de l'opérateur (www.opérateur.marqueblanche1.fr) ou le joueur est redirigé par le domaine de premier niveau de la marque blanche (www.marqueblanche.fr) site ou le joueur est recruté (mais ne joue pas). Chaque sous-domaine présenterait une graphique différente et, éventuellement, une structuration de l'offre différente. Les joueurs recrutés par chaque affilié joueraient donc sur un site de deuxième niveau dédié aux joueurs qu'il aura recruté.

Stratégie 2) : La titularité des domaines serait la même que dans le premier cas. La différence est que, dans ce deuxième cas, l'activité de jeu (inscription, jeux et mises, gestion du compte) se déroule sur le site de premier niveau de la marque blanche.

Dans les deux cas les joueurs sont tous enregistrés et signataires d'un contrat avec le seul opérateur agréé et responsable (notre société)

A condition de déclarer à l'ARJEL le nom de tous les sites et la modalité d'organisation et d'exploitation, et d'informer pleinement les joueurs de l'identité de l'opérateur, est-ce que les deux solutions sont conformes ?

Il convient de se reporter à la présentation du 12 avril dernier qui est disponible en ligne sur le site de la mission de préfiguration de l'ARJEL.

CDC Partie 5.5

Quels contrats de licence sont visés par cette question ?

Les contrats de licence visés par l'article 5.5 du projet de cahier de charges sont les contrats de licence de marques.

* * *

Qu'entend-on par contrats de licence et contrats d'affiliation ? Les contrats d'affiliation visés à l'article 5.5 concernent-ils les sites affiliés visés à l'article 6.3 ?

Oui.

CDC Partie 6

Informations relatives aux opérations de jeux ou de Paris en ligne proposées : la personne responsable du maintien de la conformité des jeux proposés au droit applicable dont les coordonnées en France doivent être communiquées à l'ARJEL peut-elle être un consultant (par exemple un avocat lié au demandeur par un contrat de service). Peut-elle être une employée d'une autre entité du groupe par exemple dans le pays CE d'origine? Au cas échéant, la personne serait joignable en France à travers l'adresse du siège social du demandeur.

Oui, à condition que cette activité soit compatible avec son statut.

CDC Partie 6.1

L'ARJEL demande la communication du règlement des jeux et paris. Est-ce à titre d'information ou de validation. S'il s'agit d'une validation, les TRJ par pari doivent-ils apparaître ? Dans ce cas quel est le délai de validation d'un règlement notamment pour la modification des TRJ des paris ?

Il s'agit d'une transmission pour information. Toutefois, si au regard des objectifs de régulation ce règlement appelle des remarques et questions de l'Autorité, cette dernière en ferait part au demandeur à l'agrément.

CDC Partie 6.3

Que signifie « sites affiliés » ?

Un site affilié est un site Internet rémunéré par un opérateur de jeux ou de paris en ligne en contrepartie du trafic ou de la clientèle qu'il lui apporte.

CDC Partie 6.4

Qu'entendez-vous par « *veille juridique* » et comment l'opérateur doit-il y répondre dans son dossier de demande d'agrément ?

Les jeux proposés en ligne doivent répondre à certaines obligations énoncées par des normes susceptibles de modifications dans le temps. Le respect de ces normes suppose qu'elles soient correctement comprises par l'opérateur. D'où la nécessaire mise en place d'une veille juridique chez l'opérateur, procédure qu'il incombe au candidat de décrire dans son dossier de demande d'agrément.

* * *

Le candidat doit-il avoir recruté une personne chargée de la veille juridique et en fournir la preuve ? Dans ce cas, le candidat doit-il produire un document particulier (contrat de travail...) ? Ou le candidat doit-il recruter ou nommer une personne chargée de la veille juridique après l'obtention de l'agrément?

L'entreprise sollicitant l'agrément est libre de la procédure qu'elle met en place pour assumer l'obligation de veille juridique qui pèse sur elle. Il lui appartient de décrire cette procédure dans son dossier de demande d'agrément, ce qui suppose qu'elle ait été déterminée au plus tard le jour du dépôt de celui-ci.

CDC Partie 6.5

Le candidat doit-il déjà avoir nommé une « personne responsable du maintien de la conformité des jeux » et donc produire à l'ARJEL une preuve? Dans ce cas, le candidat doit-il produire un document particulier (contrat de travail...) ? Ou le candidat doit-il recruter ou nommer cette personne après l'obtention de l'agrément?

La désignation d'une "personne responsable du maintien de la conformité des jeux" est prévue à l'article 6.5 du projet de cahier de charges. Ce dernier définissant "les éléments constitutifs de la demande d'agrément" en vertu de l'article 20, alinéa 2, de la Loi, la nomination de cette personne, et donc la communication de son identité et de ses coordonnées, doivent intervenir au plus tard lors du dépôt du dossier de demande d'agrément.

CDC Partie 7

Les prestataires de type Paypal sont-ils autorisés ?

L'article 12, alinéa 6, du projet de loi dispose que l'approvisionnement d'un compte joueur doit être réalisé au moyen de l'un des « instruments de paiement mentionnés au chapitre III du titre III livre Ier du code monétaire et financier ». Les prestataires susceptibles d'offrir de tels instruments de paiement, parmi lesquels ceux de type Paypal, sont autorisés.

* * *

La saisie de la date de naissance sera-t-elle obligatoire pour chaque visite sur le site ou pour chaque connexion au compte ? Idem pour l'affichage du message d'avertissement de l'interdiction du pari aux mineurs ?

Selon l'article 3 du projet de loi d'ouverture à la concurrence et à la régulation des jeux d'argent et de hasard en ligne, « Les opérateurs de jeux ou de paris en ligne mettent en place, lors de toute connexion à leur site, un message avertissant que les jeux d'argent et de hasard sont interdits aux mineurs. La date de naissance du joueur est exigée au moment de son inscription, ainsi qu'à chacune de ses visites sur le site de l'opérateur ».

* * *

Quand un joueur ayant ouvert un compte devenu définitif après vérification des pièces justificatives et saisie du code confidentiel envoyé par l'opérateur, voit un des paramètres d'authentification changer (changement d'adresse par exemple) retombe-t-il sous le coup de revalidation de ces documents entraînant une remise en compte du statut de son compte (qui de définitif redevient provisoire, sa limite de dépôt est-elle également remise en cause ?

En l'état des hypothèses de travail, dans le cas d'une telle modification, une nouvelle communication de pièces justificatives serait nécessaire ainsi que l'envoi d'un nouveau code d'activation à l'adresse postale lorsque cette dernière est modifiée. Il ne serait pas envisagé de revenir à un statut de compte provisoire. En revanche, à défaut de communication de pièces justificatives ou d'activation du code dans des délais déterminés, une procédure de désactivation puis de clôture du compte joueur pourrait être envisagée.

* * *

Au niveau international, il existe des systèmes de confiscation et de redistribution aux joueurs lésés des fonds des joueurs qui ont triché. Cette procédure a permis à la plupart des opérateurs de poker d'établir une véritable confiance avec ses joueurs. Le projet de cahier des charges ne prévoit que la suspension des versements aux joueurs en cas de suspicion de blanchiment, les opérateurs seront-ils également autorisés à mettre en place un système de suspension des versements et de séquestre des fonds des joueurs qui sont raisonnablement et objectivement suspectés de tricher. Serait-il également possible de prévoir une médiation par l'ARJEL dans les cas de tricherie suspectée ou avérée afin de permettre la redistribution des fonds des tricheurs entre les joueurs lésés en guise de compensation?

Le décret relatif à la mise à disposition de l'offre de jeux et de paris par les opérateurs agréés de jeux ou de paris en ligne sera publié prochainement.

* * *

Informations relatives au compte joueur - Communication des éléments d'identifications
Nous prévoyons que le joueur puisse envoyer des photocopies par courrier normal ou des scansions par courrier électronique ou en téléchargeant directement sur le site.les moyens électroniques sont ils acceptables?

Il a déjà été répondu à cette question dans la FAQ.

CDC Partie 7.1

La plupart des sites de poker offrent une version « Argent fictif » pour permettre aux utilisateurs d'apprécier, de tester et de se familiariser au logiciel. Les procédures d'inscription obligeant le joueur à saisir l'ensemble de ses coordonnées, peuvent-elles être déclenchées à partir du moment où l'utilisateur active la version « Argent réel » ? Si oui peut-on envisager que le basculement sur le site dédié soit déclenché également au moment de l'activation de la version « Argent réel » ?

Il résulte des termes du projet de loi, notamment de son article 1 B, que les jeux visés présentent un caractère payant. Ne relèvent pas de son champ d'application des jeux ou paris réalisés au moyen d' « Argent fictif ». Le basculement vers une version payante, en « Argent réel », emporte automatiquement application de la loi.

* * *

Deux questions apparentées donnant lieu à une réponse commune :

1/ Aux paragraphes 7.1.3 et 7.1.4, sont visés les pièces que le joueur doit adresser à l'opérateur pour vérifier son identité ainsi que les modalités d'envoi de ces pièces, serait-il possible pour les opérateurs de proposer aux joueurs « d'up-loader » les pièces (pièce d'identité et RIB) directement au moment de l'enregistrement sur le site dédié, le reste de la procédure restant inchangé ?

2/ Les moyens de transmission (par la voie d'une adresse postale ou électronique) des pièces justificatives d'identité par le joueur lors de son inscription doivent-ils être considérés comme limitatifs ? En particulier, la possibilité pour l'utilisateur de télécharger, sur le site de jeu de l'opérateur, une version électronique de ces pièces est-elle totalement écartée ?

En l'état, le projet de cahier des charges demande à l'entreprise sollicitant un agrément de préciser l'adresse d'envoi des documents et informations nécessaires à l'ouverture du compte joueur, en précisant qu'il peut s'agir d'une adresse physique ou électronique. Un téléchargement d'une version électronique de ces pièces pourrait être une hypothèse de travail à envisager. Elle est cependant en l'état exclue par le projet de cahier des charges. Cette hypothèse du cahier des charges pourra évoluer en fonction du projet de décret.

* * *

Protection des données personnelles : l'opérateur de jeu sera tenu de respecter le cahier des charges mais également la loi n°78-17 du 6 janvier 1978. Dans ce cadre, l'élaboration d'une norme simplifiée de déclaration de traitement de données est-elle envisagée ?

Le projet de loi impose à tout opérateur agréé de respecter la loi n° 78-17 du 6 janvier 1978. S'agissant de sa mise en oeuvre, les opérateurs sont invités à se rapprocher de la CNIL.

* * *

Dans le texte de loi art. 3 il est stipulé : « La date de naissance du joueur est exigée au moment de son inscription, ainsi qu'à chacune de ses visites sur le site de l'opérateur. » Ceci n'est pas repris dans le cahier des charges ou un code est requis mais sans allusion à la date de naissance. Nous n'avons donc pas prévu de rendre la saisie de la date de naissance obligatoire. Est ce acceptable ?

Non, ce n'est pas acceptable. Conformément à l'article 15 du projet de loi, le cahier des charges est un texte d'application de la loi qui établit les éléments constitutifs de la demande d'agrément. L'article 7.1.2 du projet de cahier des charges demande ainsi à l'entreprise sollicitant l'agrément de présenter la technique à laquelle elle recourt pour répondre à l'une des obligations prévues par la loi. L'opérateur agréé reste tenu en tout état de cause de respecter l'ensemble des obligations légales et notamment celle aux termes de laquelle « la date de naissance du joueur est exigée au moment de son inscription, ainsi qu'à chacune de ses visites sur le site de l'opérateur ».

* * *

En application de la section 7 du cahier des charges et de l'article 12 du projet de loi, l'opérateur ne sera autorisé qu'à reverser les fonds des joueurs sur leur compte bancaire déclaré et vérifié. Cependant, il existe des situations où les dépôts fait par un joueur sont involontaires soit, par exemple, du fait d'une utilisation frauduleuse de sa carte bancaire, soit du fait d'une erreur technique du prestataire ou encore du fait de l'annulation d'un tournoi ou du retrait du joueur d'un tournoi préalablement à son commencement. Dans ces conditions, sera-t-il possible d'exceptionnellement recréditer la carte bancaire ou l'autre moyen de paiement utilisé par le joueur pour le dépôt en cause ?

L'article 12, alinéa 7, du projet énonce que « les avoirs du joueur ne peuvent être reversés que sur un compte de paiement ».

L'article 7.4 réaffirme cette obligation.

Par suite, aucun versement ne peut être réalisé par un opérateur ailleurs que sur le compte de paiement dont le joueur est titulaire et dont il lui aura communiqué les références lors de son inscription.

La solution ne varie pas suivant la cause du versement accompli par l'opérateur ni selon la nature de l'instrument de paiement utilisé par le joueur.

* * *

Ces vérifications peuvent-elles être sous-traitées ? Si oui, par n'importe quelle entreprise dans n'importe quel pays ?

Les vérifications des informations personnelles évoquées peuvent être sous-traitées, sous la responsabilité de l'opérateur. Dans la mesure des missions qui lui sont confiées, le sous-traitant est tenu au respect des dispositions législatives et réglementaires qui régissent l'activité de l'opérateur, notamment de celles issues de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Peu importe le lieu d'établissement du sous-traitant, les textes en préparation ne comportant à cet égard aucune restriction. Néanmoins, lorsque le sous-traitant est établi à l'extérieur de l'Union européenne, des précautions s'imposent, notamment en cas de transfert de données personnelles, eu égard aux prescriptions des articles 68 et suivants de la loi précitée du 6 janvier 1978.

* * *

L'envoi du recto d'une pièce d'identité est-il suffisant ou faut-il envoyer le recto et verso ?

Le verso d'une carte nationale d'identité établie par les autorités française comporte la mention de sa date de délivrance, celle de sa date d'expiration et celle de l'autorité administrative qui l'a délivrée. En l'absence de ces informations, la régularité de la carte nationale d'identité ne peut être vérifiée.

CDC Partie 7.1.2

L'article 12 du projet de loi requiert l'entrée d'un code pour empêcher l'inscription et l'accès à des robots informatiques. Pour l'inscription, cela pourra passer par la saisie d'un CAPTCHA. En revanche, concernant l'accès, il nous semble que l'objectif de la loi est atteint via le système suivant : saisie du mot de passe du joueur et blocage du compte joueur suite à 3 saisies erronées. Est-ce acceptable ?

Oui. Le CAPTCHA peut cependant utilement être réintroduit, à la connexion, à partir du troisième essai infructueux, afin de laisser un nombre de tentatives plus élevé au joueur, tout en limitant les attaques par force brute.

CDC Partie 7.1.7

Des documents mis en ligne sur votre site de préfiguration <http://www.pre-arjel.fr>, il ressort la nécessité pour les opérateurs de jeux de vérifier l'identité du joueur, son adresse personnelle, ses coordonnées électroniques, son âge, ses références bancaires complètes et sa présence sur un fichier du ministère de l'Intérieur (fichier des interdits de jeu). Quelles sont les mesures de protection de ces données qui doivent être mises en œuvre, au plan juridique et au plan technique ?

La protection des données collectées doit être organisée suivant les modalités décrites par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et les textes pris pour son application, conformément aux dispositions de l'article 14 du projet qui y renvoient.

CDC Partie 7.1.10

Article 7.1.10 du projet de cahier des charges. Dans la mesure où les dispositions relatives aux données personnelles du joueur, selon le formalisme de la loi n° 78-17 du 6 janvier 1978 et leur communication aux fins de contrôles de l'ARJEL et de l'organisme certificateur, figureraient dans le règlement qui doit être expressément accepté par le joueur, il ne semble pas nécessaire de prévoir d'autre voie d'information du joueur. L'ARJEL partage-t-elle cette lecture ?

L'article 17 du projet de loi oblige l'opérateur à transmettre à l'ARJEL, dans un délai de six mois à compter de la date de mise en fonctionnement de son frontal, une attestation, établie par un certificateur, justifiant qu'il satisfait aux obligations énoncées aux articles 22 et 29. L'article 7.1.10 du projet de cahier des charges, qui décline l'obligation visée à l'article 17 du projet de loi, ne définit pas la manière selon laquelle l'opérateur informe les joueurs de la communication, à l'ARJEL ainsi qu'à l'organisme certificateur, des données personnelles les concernant. Quelle que soit la liberté dont l'opérateur jouit ici, l'information qu'il communique au joueur doit être apparente, complète et précise.

CDC Partie 7.2

Les comptes provisoires seront-ils limités en montant par joueur ? Si oui, avec quel plafond ? Auront-ils d'autres restrictions ?

Non.

Les restrictions qui s'attachent au compte provisoire seront précisées par Décret.

* * *

Les coordonnées bancaires du joueur doivent-elles être obligatoirement saisies par le joueur lors de l'inscription ou peuvent-elles être extraites du RIB envoyé pour la validation du compte ?

Les coordonnées du compte de paiement devront être saisies par le joueur lors de l'inscription, le document portant références du compte de paiement n'étant qu'un justificatif.

* * *

Au moment de l'activation définitive du compte provisoire, il n'est pas demandé de justificatif de domicile. Comment se fait la vérification de l'adresse du joueur ?

L'opérateur doit envoyer le code d'activation du compte définitif par voie postale, permettant ainsi une vérification effective de l'adresse à la réception de ce code.

* * *

La procédure d'envoi de code est-elle la même en cas de retrait d'argent du compte provisoire et d'activation du compte définitif ?

Il n'est pas possible d'ordonner le reversement de tout ou partie du solde créditeur du compte joueur provisoire sur le compte de paiement. La procédure d'envoi du code correspond uniquement à l'une des modalités d'activation du compte définitif.

* * *

Est-ce que la vérification de l'identité et du RIB peuvent suffire à débrider le montant du dépôt du compte provisoire ?

Le quatrième alinéa de l'article 12 du projet de loi dispose que la vérification des éléments mentionnés au premier alinéa de cet article et de la majorité du joueur conditionnent la validation du compte joueur et la restitution de son éventuel solde créditeur.

Le reversement de tout ou partie du solde créditeur du compte joueur en statut provisoire n'est pas possible.

Le compte joueur doit donc être validé. Cette validation impose dès lors la vérification des éléments d'identité du joueur, de son âge, de son adresse et de ses moyens de paiement et l'activation du code secret. La vérification de l'identité et du RIB ne peuvent donc pas suffire.

* * *

Les « contraintes » spécifiques au compte provisoire correspondent-elles bien uniquement à une limite dans le montant maximum de dépôt et à une interdiction de reverser son solde vers son compte de paiement ?

Concernant les délais laissés aux joueurs pour fournir leurs pièces justificatives, quelle est la date qui fait foi ? Date d'envoi (cachet de la Poste), date de réception par l'opérateur ou date de traitement par l'opérateur ?

Un compte provisoire ne permet pas à son titulaire d'ordonner le reversement de tout ou partie du solde créditeur de ce compte sur son compte de paiement. Par ailleurs, l'ensemble des pièces justificatives doivent être transmises dans le délai d'un mois à compter de la demande d'ouverture du compte joueur. A l'expiration de ce délai d'un mois, l'opérateur désactive le compte provisoire. A l'expiration d'un délai de trois mois, l'opérateur clôture le compte provisoire.

* * *

Les moyens de paiement suivants sont-ils autorisés : 1) carte de crédit (Visa, Mastercard, Amex, Diner's...) – 2) carte de débit immédiat – 3) cartes prépayées de multi-opérateurs ou cartes prépayées uniques ?

L'article 12, alinéa 1^{er}, du projet de loi dispose : « L'entreprise sollicitant l'agrément précise les modalités d'accès et d'inscription à son site de tout joueur et les moyens lui permettant de s'assurer de l'identité de chaque nouveau joueur, de son âge, de son adresse et de l'identification du compte de paiement sur lequel sont reversés ses avoirs ». L'alinéa 6 de ce même article ajoute que l'approvisionnement d'un compte joueur doit être réalisé au moyen de l'un des « instruments de paiement mentionnés au chapitre III du titre III livre Ier du code monétaire et financier ». Il convient donc de se reporter à ces dispositions du code monétaire et financier.

* * *

Doit-on comprendre que le solde créditeur est constitué du dépôt initial mouvementé des pertes et gains ? On ne fait pas de distinction avec les dépôts qui resteraient acquis en tout état de cause s'ils sont inférieurs au solde créditeur ?

Non. Le solde du compte joueur résulte des versements du joueur et de ses gains diminués de ses éventuelles pertes. Ce solde est le cas échéant créditeur ou nul. L'article 7.2.2 évoque la situation du statut provisoire du compte joueur. En effet ce statut provisoire du compte joueur ne permet pas à son titulaire d'ordonner le reversement, le cas échéant, du solde créditeur de ce compte.

CDC Partie 7.3.1

Les comptes doivent être clôturés si les données saisies par le joueur ne correspondent pas aux justificatifs envoyés. Quelles sont les champs sur lesquels la correspondance exacte est exigée ? Quelle est la latitude de tolérance ?

Une correspondance exacte est exigée sur au moins le nom, les prénoms, la date de naissance, l'adresse (vérification grâce à l'envoi du code d'activation par voie postale), et les coordonnées bancaires du joueur.

* * *

Peut-on demander au joueur une correction de certaines données personnelles sans clôturer le compte ?

L'opérateur doit clôturer immédiatement le compte joueur lorsque son titulaire lui communique des pièces dont les informations ne correspondent pas à celles qu'il a saisies lors de son ouverture. Les modalités de modifications du compte joueur définitif seront déterminées par décret.

* * *

Quels seront les éléments d'identification d'un joueur permettant de valider sa présence ou non dans le fichier d'interdits de jeux ?

Les critères d'identification d'un joueur seront précisés ultérieurement avec le ministère de l'Intérieur. Ces éléments d'identification seront a minima : nom, prénoms, date de naissance.

* * *

Nous comprenons qu'il s'agit d'une obligation de moyens étant donné qu'il n'est pas prévu de système permettant aux opérateurs d'avoir connaissance en temps réel de toute mise à jour du fichier des interdits de jeux. Est-ce conforme ?

Non. Les modalités d'interrogation du fichier des interdits de jeux seront précisées par décret.

* * *

Faut-il renvoyer au joueur un code de confirmation par courrier en cas de modification : d'adresse du joueur ? de nom ? de RIB ? (7.3.1.7 du projet de cahier des charges).

Lorsque la modification d'informations aura pour objet l'adresse postale du joueur, l'opérateur devrait communiquer à ce dernier, par courrier envoyé à cette adresse, un code secret dont la saisie par le joueur validerait sa nouvelle adresse postale. A défaut de saisine de ce code, le compte joueur serait désactivé.

Dans les autres cas de modification, il ne serait pas envisagé l'envoi d'un code de confirmation par courrier. En revanche, à défaut de communication de pièces justificatives à l'opérateur dans un délai déterminé, ce dernier devrait désactiver le compte joueur.

CDC Partie 7.4

Deux questions apparentées donnant lieu à une réponse commune :

1/ Nous interprétons « immédiat » comme : dans les délais les plus rapides possibles mais après avoir effectué les diligences nécessaires, le cas échéant (ex : lutte contre fraude / blanchiment etc ...). Est-ce conforme ?

2/ Le paragraphe 7.4.6 prévoit le reversement immédiat des sommes sur le compte bancaire du joueur à la clôture du compte joueur, l'emploi de l'adjectif « immédiat » signifie-t-il que la procédure de paiement doit être immédiatement déclenchée, permettant aux opérateurs de respecter leur procédure interne, y compris les contrôles de sécurité ? Cela signifierait que le compte bancaire du joueur ne serait crédité que 3 à 4 jours après la demande de clôture (délai de virement plus procédure interne). Merci pour vos clarifications.

L'article 7.4.6 du projet de cahier des charges concerne les reversements sur le compte de paiement du joueur des sommes dont ce dernier a demandé le reversement, automatique ou non. Cela concerne ainsi le reversement automatique sur le compte de paiement du joueur des crédits disponibles sur son compte joueur au-delà du montant qu'il aura lui-même fixé, mais également les demandes ponctuelles du joueur ainsi que le reversement du solde créditeur au moment de la clôture du compte joueur.

Dans tous les cas, le reversement doit être immédiat.

Cela signifie donc que l'opérateur doit y procéder sans délai. Toutefois, le reversement peut être différé par l'opérateur en cas de soupçon de blanchiment de capitaux en application de l'article L.561-16 du code monétaire et financier. Il lui appartient donc de mettre en place les procédures nécessaires au respect de ses obligations en matière de lutte contre le blanchiment. En tout état de cause, l'opérateur ne doit pas indûment retarder le reversement des sommes. Il doit, le cas échéant, pouvoir justifier des soupçons différant le reversement. Le compte du joueur est ensuite crédité par virement selon les délais usuels.

* * *

Au paragraphe 7.4.7 concernant la traçabilité de l'historique des transactions sur le compte joueur, la génération de codes informatiques séparés pour chaque transaction constatée suffira-t-elle à répondre aux exigences de l'ARJEL ou les données historiques indiquées devront-elle clairement apparaître sur le compte joueur ?

Le compte joueur doit retracer l'historique, sur un an, des mises, des gains, des pertes et des événements de jeu qui leur sont associés ainsi que l'historique, sur un an, des mouvements financiers affectant ledit compte. Ces informations doivent pouvoir ainsi être visualisées par le joueur en accédant à son compte joueur. Elles devront donc clairement apparaître sur le compte joueur. Cette exigence est distincte de la génération de codes informatiques séparés pour chaque transaction.

* * *

En ce qui concerne les fournisseurs de solutions de paiement électronique, avons-nous l'obligation de traiter uniquement avec les organismes agréés par la Banque de France ? a. si oui, aurons-nous communication de la liste de ces organismes agréés ? b. si non, y a-t-il un moyen d'obtenir l'assurance par une institution indépendante que les partenaires que nous choisirons ne poseront aucun problème ?

L'article 12, alinéa 6, du projet de loi dispose : « L'approvisionnement d'un compte joueur par son titulaire ne peut être réalisé qu'au moyen d'instruments de paiement mis à disposition par un prestataire de services de paiement établi dans un État membre de la Communauté européenne ou un État partie à l'accord sur l'Espace économique européen ayant conclu avec la France une convention contenant une clause d'assistance administrative en vue de lutter contre la fraude et l'évasion fiscales ».

Ce texte définit strictement les établissements susceptibles autorisés à émettre des instruments de paiement pouvant être utilisés par les joueurs pour alimenter leur compte. Ces établissements ont nécessairement la qualité de « prestataire de services de paiement ».

* * *

Quelles sont les méthodes de paiement acceptées pour participer a. cartes de crédit et de débit ? b. cartes délivrées par les banques locales uniquement, ex. banques françaises ? c. virements/transferts bancaires ? Si oui, uniquement en provenance de banques françaises ? d. cartes prépayées ? e. portefeuilles électroniques (eWallets) ?

Aux termes de l'article 12, alinéa 6, du projet de loi : « L'approvisionnement d'un compte joueur par son titulaire ne peut être réalisé qu'au moyen d'instruments de paiement mis à disposition par un prestataire de services de paiement établi dans un État membre de la Communauté européenne ou un État partie à l'accord sur l'Espace économique européen ayant conclu avec la France une convention contenant une clause d'assistance administrative en vue de lutter contre la fraude et l'évasion fiscales. Seuls peuvent être utilisés les instruments de paiement mentionnés au chapitre III du titre III du livre Ier du code monétaire et financier ».

Ce texte définit précisément, d'une part, les instruments de paiement permettant d'approvisionner les comptes joueurs, par renvoi aux articles L.133-1 et suivants du Code monétaire et financier, et, d'autre part, le lieu où doivent être établis les établissements susceptibles de les émettre.

CDC Partie 7.4.1

7.4.1 CDC , il est dit : « L'entreprise fait état des moyens garantissant que le compte joueur est approvisionné par son titulaire ». Quelles sont les exigences requises lorsque l'entreprise passe par des intermédiaires de paiement (type Moneybooker, Paypal) ou par des cartes pré-payées ?

L'article 12, alinéa 1er, du projet de loi dispose : « L'entreprise sollicitant l'agrément précise les modalités d'accès et d'inscription à son site de tout joueur et les moyens lui permettant de s'assurer de l'identité de chaque nouveau joueur, de son âge, de son adresse et de l'identification du compte de paiement sur lequel sont reversés ses avoirs ». L'alinéa 6 précise : « Le compte joueur ne peut être crédité que par son titulaire au titre des approvisionnements qu'il réalise dans les conditions définies au présent article ou par l'opérateur agréé qui détient le compte, soit au titre des gains réalisés par le joueur, soit à titre d'offre promotionnelle ».

L'entreprise sollicitant l'agrément doit donc indiquer la manière, qu'il lui appartient de déterminer, dont elle s'assurera que le compte joueur est crédité par son titulaire, quels que soient les instruments de paiement utilisés.

CDC Partie 7.4.6

Il est fait référence à un mécanisme de retrait automatique, de quelle nature est-il ? Est-il obligatoire ? A partir de quel moment ?

Lors de la validation du compte définitif, l'opérateur devrait demander au joueur de déterminer un montant au-delà duquel les crédits disponibles inscrits sur son compte joueur seraient automatiquement reversés sur son compte de paiement. Aucune opération ne pourrait être réalisée tant que le joueur n'aurait pas déterminé ce montant.

CDC Partie 7.4.7

Y a-t-il des règles d'affectation du bonus lorsqu'il est attribué à un titulaire de compte lui permettant d'accéder à la fois aux paris hippiques, sportifs et au poker ?

Les bonus alloués pour une catégorie de jeux spécifique sont exclusivement utilisés pour cette catégorie. Les bonus présentant un caractère générique peuvent recevoir toute destination. Le calcul du taux de retour au joueur (TRJ) est réalisé en prenant en compte la part de bonus générique utilisée par catégorie de jeux.

* * *

Bilan : les participants ont fait part de difficultés d'interprétations quant au point 7.4.7 2°. L'ouverture, sur l'espace de jeu, d'une rubrique dédiée mettant à disposition du joueur divers éléments tels que la date de création du compte joueur, l'historique des gains et pertes satisfait-elle à cette obligation ?

En l'état des hypothèses de travail, le compte joueur doit retracer non seulement la date de création, l'historique sur un an des mises, des gains, des pertes et des événements de jeu qui leur sont associés, l'historique sur un an des mouvements financiers affectant ledit compte, mais également le solde des avoirs du joueur auprès de l'opérateur, visé à l'article 7.4.7. 2° du projet de cahier des charges.

Ce solde des avoirs du joueur doit distinguer les sommes versées par le joueur, les sommes versées par l'opérateur sous forme de gains et les sommes versées par l'opérateur à titre promotionnel.

Cette exigence n'est satisfaite que dès lors que dans son compte joueur, le joueur a accès à l'ensemble des informations ainsi énoncées et ce, de manière clairement distinguée.

CDC Partie 10

Articles 10.2 et 10.6 CDC : ces obligations sont elles identiques ou complémentaires (déclaration de l'entreprise et clauses du règlement intérieur ou du contrat de travail type) ?

Ces obligations sont complémentaires. L'article 10.2 du projet de cahier des charges impose au demandeur à l'agrément de procéder à des déclarations auprès de l'ARJEL relatives à des intérêts du propriétaire de l'entreprise, d'un de ses dirigeants, mandataires sociaux ou membres du personnel. L'article 10.6 pour sa part impose la communication des documents mis en place par le demandeur à l'agrément afin que les personnes ainsi visées aient l'obligation de lui déclarer de tels intérêts.

CDC Partie 10.1

La partie 10 parle des contrats de partenariat avec les fédérations sportives. Il sera difficile d'avoir des contrats finalisés quelques jours après le vote de la loi. Une simple lettre d'intention suffit-elle ?

La partie 10 du cahier des charges prévoit que « l'entreprise transmet à l'ARJEL les contrats de partenariat qu'elle a, le cas échéant, conclus avec des personnes physiques ou morales organisant des courses hippiques, compétitions ou manifestations sportives ou y prenant part ». Les contrats ainsi visés sont ceux qui ont été conclus sous la condition suspensive, expresse ou tacite, de la délivrance de l'agrément par l'ARJEL. Par ailleurs, selon l'article 23-II du projet de loi, postérieurement à la délivrance de l'agrément, l'opérateur « transmet à l'Autorité de régulation des jeux en ligne les contrats de partenariats conclus avec des personnes physiques ou morales organisant des courses hippiques, compétitions ou manifestations sportives ou y prenant part dès le moment où il propose des jeux ou paris sur lesdites courses hippiques, compétitions ou manifestations sportives ».

Il convient de ne pas confondre ces contrats avec ceux visés à l'article 52 du projet de loi et conclus entre opérateurs agréés et fédérations sportives ou organisateurs de manifestations sportives. Conformément à l'alinéa 5 de ce texte, ces projets de contrats de commercialisation du droit d'organiser des paris doivent être transmis pour avis à l'ARJEL ainsi qu'à l'Autorité de la concurrence, ces dernières devant se prononcer dans un délai de quinze jours à compter de leur réception.

CDC Partie 11

Point 11 du cahier des charges et dossier des exigences techniques :

Afin d'être en mesure d'offrir ses services dès l'ouverture du marché, un opérateur peut se trouver dans l'obligation de mener en même temps des négociations avec plusieurs prestataires techniques pour la mise en place dans les temps de sa plate-forme. Dans ces conditions, l'opérateur peut-il préciser dans son dossier de demande d'agrément que le prestataire auquel il fera finalement appel sera l'un d'entre eux, dès lors que, dans son dossier, il aura fourni pour chacun d'entre eux l'ensemble des informations requises ?

Non. Cette solution n'est clairement pas envisageable.

CDC Partie 11.2

Quelle est l'intention de l'ARJEL vis-à-vis des opérateurs qui ne peuvent pas effectuer la mise en place de toutes les plateformes techniques exigées dans les délais prévus, ex. y-aura-t-il une période de grâce après l'accord de l'agrément pendant laquelle l'opérateur aura un engagement de réaliser les étapes techniques dans un délai imparti ?

Avant de débiter son activité, l'opérateur agréé doit déclarer à l'ARJEL que son frontal est en mode fonctionnement.

L'article 11.2 du projet de cahier des charges envisage néanmoins le cas de l'opérateur dont le frontal n'est pas en mesure de recueillir l'ensemble des données qu'il doit permettre de collecter lors de cette mise en fonctionnement.

Cet article détaille les données devant alors obligatoirement être archivées et les modalités de transmission à l'ARJEL des autres catégories de données.

Dans une telle hypothèse, l'opérateur doit en outre s'engager sur un calendrier indiquant précisément la date à laquelle les mesures restant à adopter pour le fonctionnement du frontal seront prises ; l'adoption de ces mesures devant intervenir au plus tard le jour de la première certification prévue au II de l'article 17 du projet de loi, soit au plus tard 6 mois après la mise en fonctionnement du frontal.

* * *

A l'article 17 du projet de loi, l'obligation de mise en fonctionnement d'un support dans un délai de 6 mois à compter de la date de mise en fonctionnement du support signifie elle qu'un opérateur n'est pas obligé de mettre en fonctionnement un support dès l'agrément ?

L'opérateur agréé ne peut pas débiter son activité sans mettre en fonctionnement son frontal. Il doit d'ailleurs déclarer à l'ARJEL que son frontal est en mode fonctionnement avant de débiter son activité. Cette mise en fonctionnement n'implique pas, au moment où l'opérateur débute son activité, que ledit frontal soit en mesure de recueillir toutes les catégories de données qu'il doit permettre de collecter. L'article 11.2 du projet de cahier des charges précise dans ce cas les obligations de l'opérateur. En tout état de cause, le frontal doit respecter l'ensemble des exigences techniques et permettre de collecter la totalité des éléments qu'il est destiné à recueillir au plus tard le jour de la première certification prévue au II de l'article 17 du projet de loi.

* * *

Dans le cas spécifique du poker, la capture des données pourrait elle être faite à l'étranger sachant que le coffre serait situé en France ?

Non, le capteur doit être situé en France métropolitaine.

Si toutes les données ne peuvent pas être archivées dès le début, les opérateurs doivent envoyer les données agrégées quotidiennement selon les exigences définies dans l'annexe 2? Et est ce que ça veut dire que nous devons avoir ce qui est en annexe 2 seulement si le frontal ne permettra pas, au commencement de son activité, la collecte de la totalité des éléments qu'il est destiné à recueillir? Ou alors devons-nous encore envoyer les données agrégées à l'ARJEL une fois que le frontal sera tout à fait opérationnel, en parallèle aux traces ?

Conformément à l'encadré de la page 9 du DET, les données du frontal qui ne pourraient être archivées lors de sa déclaration en mode fonctionnement devront être transmises à l'ARJEL par le biais des données de supervision.

Cette souplesse ne peut en aucun cas aller au delà de la certification à 6 mois du frontal.

Dès que le frontal est opérationnel sur toutes ses fonctions, cet envoi par les données de supervision s'arrête.

Informations relatives au frontal / certification : auprès de quels organismes l'opérateur doit il faire certifier le frontal ? Y a-t-il une liste préconisée ?

La certification de sécurité de premier niveau (CSPN) concerne le seul coffre-fort.

Cette certification est à obtenir auprès de l'agence nationale de sécurité des systèmes d'information (voir modalités sur le site de l'ANSSI : www.ssi.gouv.fr)

* * *

Informations relatives à l'architecture du SI. 11.2 description détaillée du frontal. Dans les procédures contre les accès non autorisés, parlez-vous d'accès au site ou d'accès aux machines ?

Les réponses doivent porter à la fois sur les mécanismes de sécurité logique et physique.

CDC Partie 11.3

CDC 11.3 stipule que l'entreprise requérant l'agrément doit produire :

- **3 rapports d'analyse de code source des logiciels de jeux et paris**
- **1 rapport d'analyse des vulnérabilités techniques de la plate-forme de jeu**

Question : les rapports d'analyse cités au chapitre 11.3 du projet de Cahier des Charges doivent-ils être obligatoirement communiqués lors de la demande d'agrément, ou seulement avant ouverture de la plate-forme de jeux et paris ?

Les rapports sont impérativement à fournir lors de la demande d'agrément.

* * *

Est-ce que les codes sources doivent être notifiés à la demande? Si un code source est toujours en développement, est-ce que les informations fournies conformément aux articles 5 et 6 sont suffisantes pour que l'Autorité rende un avis préliminaire, sachant que le code source modifié serait communiqué par la suite, dès sa finalisation ?

Les codes sources doivent être fournis dans le dossier de demande d'agrément. C'est sur la base des codes sources fournis que le dossier sera étudié : ils doivent donc nécessairement être fonctionnels.

* * *

Es-ce-que l'ARJEL peut octroyer l'agrément sur la base de ces activités en cours, sous condition de la présentation (et acceptation) des rapports avant le début de l'activité?

Nous soulignons aussi que, dans notre cas, il s'agit de logiciels déjà opératifs sans problèmes dans le contexte du plus grand marché régulé du jeu en ligne.

Théoriquement, l'agrément pourrait être délivré avant l'homologation puisqu'il s'agit de décisions distinctes. Toutefois, la demande d'homologation doit être faite lors de la demande d'agrément.

CDC Partie 11.3.1

S'agissant de la communication des codes sources telle que prévue par l'article 11.3.1 du CDC, dont l'opérateur serait propriétaire et considérant le caractère critique de ceux-ci, qui touche au secret des affaires, la pré-Arjel serait elle d'accord pour que l'opérateur les dépose auprès d'un tiers de confiance auquel l'Arjel pourrait accéder dans des conditions garantissant la sécurité et la confidentialité des codes sources. Si la pré-Arjel ne marque pas son accord, quelles mesures de sécurité entend-elle mettre en œuvre en vue de protéger les codes sources communiqués par l'opérateur. Des mécanismes de protection unilatérales par l'opérateur peuvent-ils être envisagés (mot de passe, etc ..) ?

La disposition évoquée stipule que « L'entreprise communique le code source de chaque logiciel de jeux et de paris destiné à être utilisé par les joueurs et les parieurs français ainsi que le code source de l'éventuel générateur de nombre aléatoire ». L'entreprise doit donc communiquer le code source à l'ARJEL.

En confiant ses codes sources à l'ARJEL, l'entreprise ne s'adresse pas à un tiers mais à une autorité administrative indépendante de l'État français dont les agents et titulaires sont soumis à des obligations de secret professionnel.

Des mécanismes de protection sont bien entendu envisageables, et seront mis en place avec les candidats à l'agrément : chiffrement du support, etc.

* * *

Pour le générateur de nombres aléatoires, quid de l'audit de la librairie (dont les sources peuvent ne pas être publiques) du HSM utilisé pour générer les seeds ?

L'audit du PRNG, et des mécanismes cryptographiques en général, se rapprocheront de la méthodologie préconisée dans le cadre d'une certification de sécurité de premier niveau : elle est décrite dans la partie 11 du document « Méthodologie d'évaluation en vue de la CSPN et contenu attendu du RTE » (partie dédiée à la cryptographie), disponible sur le site de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), depuis l'adresse http://www.ssi.gouv.fr/site_article80.html.

* * *

Pour les applications recourant à des progiciels du marchés ou à des services de type SAAS (exemple : Poker), est-il prévu des aménagements quant à la fourniture des codes sources et des rapports d'audit de la sécurité des codes (contraintes relatives à la protection de la propriété intellectuelles) :

Les mesures - exigées par contrats - seraient-elles satisfaisantes du point de vue de l'Arjel :

i. la fourniture d'un rapport d'audit de la sécurité du code des applications réalisées par un tiers indépendant sur une fréquence à définir (annuelle, à chaque release majeure).

ii. la réalisation de test d'intrusion directement sur les plateformes transactionnelles pour les tiers fournissant un service de type « Saas ».

iii. Certification de type SAS 70 avec un volet sécurité reprenant les exigences de l'Arjel en matière de sécurité.

iv. Certifications s'adossant sur des normes de référence pour le générateur de nombre aléatoire (type FIPS (USA),...).

Aucun aménagement de ce type n'est prévu.

* * *

Questions SI : les codes sources sont souvent susceptibles de comporter des savoir faire dont la divulgation pourrait porter atteinte aux intérêts stratégiques de l'entreprise qui serait donc légitimement réticente à confier le stockage de ce genre d'information à des tiers. Quel mode de consultation de ces sources sans transfert pourrait être envisagé?

En confiant ses codes sources à l'ARJEL, l'entreprise ne s'adresse pas à un tiers mais à une autorité administrative indépendante de l'État français dont les agents et titulaires sont soumis à des obligations de secret professionnel.

Aucun mode de consultation "sans transfert" n'est prévu.

* * *

Quid de l'entiercement des codes sources ? l'APP est-elle validée par l'ARJEL?

La disposition évoquée stipule que "L'entreprise communique le code source de chaque logiciel de jeux et de paris destiné à être utilisé par les joueurs et les parieurs français ainsi que le code source de l'éventuel générateur de nombre aléatoire." L'entreprise doit donc communiquer le code source à l'ARJEL, et non à un tiers avec lequel l'Autorité n'a pas de lien de droit. L'ARJEL est un organisme administratif qui agit au nom de l'État : il est donc un correspondant de confiance.

* * *

Dans l'hypothèse où un demandeur de licence n'est pas propriétaire des codes sources de ses logiciels et que la plateforme de jeu qu'il utilise ne souhaite pas divulguer ses codes sources, est-il possible de recourir à un contrat d'entiercement tel que celui proposé par l'Agence de Protection Programme. Voir <http://app.legalis.net/>

La disposition évoquée stipule que « L'entreprise communique le code source de chaque logiciel de jeux et de paris destiné à être utilisé par les joueurs et les parieurs français ainsi que le code source de l'éventuel générateur de nombre aléatoire. » L'entreprise doit donc communiquer le code source à l'ARJEL, et non à un tiers avec lequel l'Autorité n'a pas de lien de droit. L'ARJEL est un organisme administratif qui agit au nom de l'État : il est donc un correspondant de confiance.

* * *

« L'ARJEL rend une décision sur l'homologation des logiciels de jeux distincte de celle relative à la demande d'agrément.

Un opérateur agréé ne peut pas débiter son activité de jeu sans homologation des logiciels de jeu et de paris. »

Comprenant que l'ARJEL, avant tout début d'activité, procédera à une homologation des logiciels de jeu ;

Comprenant que les rapports mentionnés en 11.3.1 et 11.3.2 seront un des éléments de l'homologation ;

Comprenant que l'agrément et l'homologation sont des éléments distincts ;

Une demande d'agrément ne contenant pas les rapports mentionnés en 11.3.1 et 11.3.2 serait-elle recevable par l'ARJEL ?

Ces rapports seraient fournis lors de l'homologation de la plateforme et du logiciel de jeu, préalablement au début de l'activité.

Par extension, est-il acceptable que les codes source :

- du Frontal (capteur et coffre), mentionné au chapitre 11.2

- du site .fr, mentionné au chapitre 11.2

- du logiciel de jeu, mentionné au chapitre 11.3.1

ne soient pas fournis lors de la demande d'agrément, mais lors de l'homologation de la plateforme et du logiciel de jeu ?

NON. L'ensemble des éléments demandés pour l'homologation doivent être fournis lors de la demande d'agrément.

* * *

Ci-jointe une question concernant le CDC : s'agissant de la communication des codes sources telle que prévue par l'article 11.3.1 du CDC, dont l'opérateur ne serait pas propriétaire, l'Arjel serait elle d'accord pour que l'opérateur les communique à l'Arjel sous forme cryptée, les clés étant directement échangées entre le tiers et l'opérateur ? Quels dispositifs techniques l'Arjel souhaite t elle que les opérateurs mettent en place, concernant le cryptage et les clés ?

L'ARJEL mettra à disposition des certificats afin de chiffrer les DVD. Ces certificats seront transmis aux candidats opérateurs qui pourront alors les transmettre aux éditeurs. Les DVD chiffrés seront alors transmis par les éditeurs aux candidats opérateurs afin que ces derniers présentent un dossier de demande d'agrément complet à l'ARJEL.

* * *

Codes source et rapports d'analyse des logiciels : que se passe-t-il dans le cas (assez commun) où un logiciel (déjà employé par le demandeur) est exploité en vertu d'un contrat de licence qui (comme dans presque tous ces accords) ne prévoit pas la disponibilité des codes sources pour des exigences de protection des droits de propriété intellectuelle (de la part du producteur du logiciel envers l'opérateur et non de la part de l'opérateur envers l'ARJEL, cette dernière problématique étant déjà adressée dans la FAQ). Que faire si l'opérateur n'a pas accès aux codes sources ? Est-il possible de substituer dans ce cas une certification d'un tiers de confiance?

Il a déjà été répondu à cette question dans la FAQ.

* * *

CDC Partie 11.3.1

Rapport d'analyse des logiciels : nous avons remarqué les phrases suivantes introduites dans la dernière version du cahier des charges : « l'ARJEL rend une décision sur l'homologation des logiciels de jeux distincte de celle relative à la demande d'agrément. Un opérateur agréé ne peut pas débiter son activité de jeu sans homologation des logiciels de jeu et de Paris. » Est-ce que cela signifie que la demande d'agrément peut être déposée en présentant les contrats avec les prestataires de service chargés des analyses, sans toutefois avoir encore les résultats ?

Non.

CDC Partie 11.3.2

Les bibliothèques tierces utilisées (frameworks php, message queuing, XML...) doivent-elles être comprises dans le cadre de l'audit, et si oui, dans quelle mesure (je suppose en effet par exemple que libmysql peut être exclue) ?

A priori non, l'analyse des bibliothèques tierces pourra classiquement s'appuyer sur les règles de l'art (niveau de mise à jour, configuration conforme à l'état de l'art, etc.), pour les composants les plus communs (libmysql, par exemple).

En revanche, les composants plus spécifiques et moins connus en termes de sécurité pourront faire l'objet d'une analyse plus détaillée. Ainsi, un serveur d'applications ou d'un framework Java complexe et relativement peu répandu est susceptible de faire l'objet d'une analyse, si les experts techniques en sécurité jugent cette analyse intéressante.

CDC Partie 11.4.2

Evolutions (article 11.4.2 du CDC) : la pré-Arjel marquerait elle son accord pour une communication annuelle des évolutions fonctionnelles et techniques du logiciel et de la plate-forme de jeu ?

Non, la communication de ces évolutions doit dépendre de leur nature et de leur importance, et non d'une périodicité.

CDC Partie 11.4.4

La prise en compte des aspects réglementaires et notamment des données personnelles au titre des systèmes d'information n'est elle pas redondante avec la prise en compte des contraintes de la loi n° 78-17 aux articles 7.1.7 à 7.1.10 ?

L'article 14 du projet de loi relatif à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne dispose : « L'entreprise sollicitant l'agrément décrit les moyens qu'elle met en œuvre pour protéger les données à caractère personnel et la vie privée des joueurs, conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».

Les articles 7.1.7 à 7.1.10 reprennent cette exigence à propos des informations relatives au compte joueur, tandis que l'article 11.4.4 la décline s'agissant de l'architecture du système d'information.

Il n'y a donc pas redondance : les dispositions de la loi n° 78-17 du 6 janvier 1978 doivent donc être respectées successivement à ces deux niveaux.

* * *

Propositions de corrections : Marchés publics. Le point 11.4.4 du cahier des charges impose que l'opérateur communique « des extraits du Cahier des Clauses Techniques Particulières (CCTP) ainsi que les clauses relatives à la sécurité ». Cette obligation est spécifique aux marchés publics et ne concerne pas le secteur des jeux d'argent en ligne. Nous proposons dès lors de supprimer cette référence.

Un CCTP est effectivement un document plus spécifique aux marchés publics. L'ARJEL souhaite ainsi disposer d'extraits de documents contractuels liant l'opérateur à ses prestataires concernés par le pilotage du système d'information que ce document contractuel soit appelé CCTP ou autrement.

CDC Partie 11.5

Il est dit que la partie technique comporte 4 sous-parties. L'ARJEL veut-elle voir traité les éléments du 11.5 (Informations détaillées) dans la partie "maturité SSI" ?

Oui. Les éléments de la partie 11.5 du cahier des charges, tout comme ceux de la partie 11.4 sont rattachés à la partie maturité (ces parties sont directement liées à la partie 5.7 du DET.)

CDC Partie 11.5.2

Journalisation : il est mentionné que les journaux techniques doivent être archivés 3 mois. Nous comprenons dans ce contexte, archivage des journaux tel qu'ils sont produits, c'est-à-dire sans notion d'empreinte et de scellement, est-ce conforme ?
Par rapport à la question précédente, est-ce que l'ensemble des journaux respecte les mêmes règles de conservation.

*Oui, le scellement des journaux techniques ne fait pas partie des exigences.
Oui, également pour la seconde question.*

CDC Partie 11.5.2.1

Le terme « Procédures de veille technologique » correspond-il au terme « Procédures de veille vulnérabilités » ?

Oui. Il s'agira, par exemple, de décrire les procédures mises en œuvre afin d'assurer le suivi et le traitement des alertes et avis de sécurité publiés par le CERTA, comme mentionné dans la partie 5.7.3.d relative à la gestion des mises à jour.

CDC Partie 11.5.2.7

Gestion de la sécurité dans les cycles de développement : est-il possible d'utiliser un référentiel de code externalisé et accédé via internet ?

Si par « référentiel de code externalisé », on entend des objets métiers type EJB appelés via RMI, ou encore des services web appelés via SOAP/REST/etc. (par exemple), il n'y a pas d'objection à en faire usage (à condition que ces appels distants respectent les bonnes pratiques de sécurité).

<p style="text-align: center;">QUESTIONS RELATIVES AU DOSSIER DES EXIGENCES TECHNIQUES</p>

Questions générales relatives au Dossier des Exigences Techniques :

J'ai lu votre document « Ouverture à la concurrence et à la régulation du secteur des jeux d'argent en ligne - Projet de dossier des exigences techniques » et j'ai la question suivante : Le document est-il disponible en anglais ?

Les projets de cahiers des charges juridiques et dossier des exigences techniques sont disponibles uniquement en français.

DET Partie 3.1.1

Le cahier des charges précise que le frontal doit être situé en France métropolitaine. Par ailleurs, l'annexe 3 §3.1.1. indique p83 la remarque suivante : « (1) Remarque sur le positionnement du capteur : la mise en oeuvre du capteur peut également s'insérer dans la logique de présentation de l'application, en amont de la logique de jeu, par exemple au niveau des serveurs d'applications effectuant le traitement des requêtes en provenance du logiciel client. Dans ce cas, la requête ne fera pas l'objet d'une interception au sens protocolaire du terme (interception d'une requête HTTP par exemple, et extraction des paramètres pertinents afin de former l'enregistrement XML conforme à la DTD fournie en annexe) mais d'un filtre dans la logique de traitement. ». Est-il acceptable pour un opérateur ayant sa plateforme de jeu dans un pays de l'UE que le capteur s'insère dans la logique de présentation (c'est-à-dire sur la plateforme qui n'est pas sur le territoire français) et qu'elle déverse le produit de la capture dans un coffre qui lui soit sur situé sur le territoire français ?

Cette même annexe mentionne explicitement que « [l']ensemble coffre + capteur étendu aux serveurs doit, conformément au projet de loi, être localisé en France métropolitaine ».

Nous avons démarré la conception d'un frontal complet pour un opérateur et souhaitons confirmer le déroulement des étapes décrites dans le document « Projet d'Annexe au DET chapitre 3.1.1 ». Nous avons compris que : • Le retour à l'internaute (étape 5) est conditionné par deux acquittements : un premier en provenance de la plateforme de jeux (étape 3), un second en provenance du coffre (retour de l'étape 4), le capteur doit donc « mémoriser » le flux capté avant de l'enregistrer dans le coffre. Pourriez-vous confirmez que dans le cas d'un acquittement négatif du coffre : 1/ le capteur doit produire un acquittement négatif vers l'internaute et par conséquent altérer le flux applicatif produit par la plateforme de jeu 2/ le capteur ne doit pas indiquer à la plateforme de jeu que le flux applicatif produit a été ignoré.

Non, le mode de fonctionnement décrit dans le DET présente la logique à implanter afin d'éviter l'enregistrement par le coffre d'évènements non valides. Le cas d'un acquittement négatif n'est pas traité.

Dans le cas d'un acquittement négatif du coffre, le frontal mettra donc en œuvre la logique applicative que l'opérateur jugera nécessaire à l'avertissement du joueur, d'une part, et de la plate-forme, d'autre part.

Comme cité par ailleurs, il est important que l'évènement journalisé au niveau du coffre soit validé par la plate-forme, et que sa traçabilité participe au traitement de la requête, comme tout autre processus métier dont la réussite conditionne celle de la transaction dans son ensemble.

Localisation des composants du frontal : pour des raisons d'exploitation et de performance, un opérateur envisage de déployer les composants capteur et coffre-fort du frontal sur des sites différents. La partie capteur sur le site de la plateforme de jeu, et la partie coffre-fort sur un site tier. Les flux entre capteur et coffre-fort sont sécurisés conformément aux exigences du DET. Un tel déploiement sera-t-il autorisé par l'ARJEL.

Oui. Cette configuration est valide sous réserve que "[l']ensemble coffre + capteur étendu aux serveurs [soit], conformément au projet de loi, [...] localisé en France métropolitaine".

DET Partie 3.1.3.a

Plusieurs coffre-forts pour une même licence : pour des raisons d'exploitation et de performance, un opérateur utilise plusieurs infrastructures disjointes pour ses plateformes de jeux et gère de manière distincte les back-offices associées. Dans l'hypothèse où une seule licence de jeu est nécessaire (les différentes plateformes opèrent le même type de pari au sens de l'ARJEL), est-il envisageable d'avoir plusieurs instances du coffre-fort indépendantes. Les traces de jeux seront collectées et chaînées de manière indépendantes par chaque des coffre-fort (afin d'éviter la synchronisation entre les sites et la dégradation des performances). L'opérateur mettra à disposition de l'ARJEL plusieurs services Web d'accès comme cela est précisé dans la section 3.1.3a de l'annexe du DET.

Oui.

DET Partie 4

Je me demandais pour les futurs opérateurs étrangers, si vous aviez une liste d'accréditation pour le serveur frontal?

NON, il n'y a aucune liste « d'accréditation » concernant la définition ou la mise en oeuvre du FRONTAL.

En tant que fournisseur de centres de données, nous mettons des environnements physiques à disposition des opérateurs de jeux et paris en ligne pour y faire fonctionner leurs applications et systèmes informatiques.

Pouvons nous obtenir un « agrément site d'hébergement » ou un « référencement en tant que site éligible d'hébergement » auprès de l'ARJEL (comme il existe pour le coffre une certification de sécurité de premier niveau délivrée par l'ANSSI) ?

Si oui, quelles sont/seraient les modalités pour l'obtenir ?

L'ARJEL ne met en place aucune sélection formelle ou informelle de prestataires pour la mise en œuvre du frontal par les opérateurs.

DET Partie 4.1

Archivage : le coffre-fort devra-t-il respecter la norme NF Z 42-013 ?

Non.

Acceptation de l'utilisateur : Peut-on implémenter des actions hors ligne/asynchrones dans les systèmes back-end avant que l'utilisateur les accepte? Par exemple, un utilisateur remporte le pari. Est-ce que le compte utilisateur est crédité avec le montant avant que l'utilisateur ait accepté que l'événement ait eu lieu?

Cette acceptation doit-elle se produire dans tous les produits qui fonctionnent dans un portefeuille unique de back-end? Par exemple, lorsqu'un utilisateur se connecte à un jeu de poker, doivent-ils voir et accepter tous leur pari avec l'opérateur depuis la dernière fois qu'ils ont été connectés ?

Que se passe-t-il si l'utilisateur ne se connecte pas de nouveau ? Quel est le délai maximum que le système de l'opérateur peut supporter sans en informer le Capteur / Coffre fort?

Oui, les actions dont la réussite n'est pas conditionnée par une confirmation de l'utilisateur peuvent être implantées au niveau des systèmes en back-end. En particulier, le crédit du compte joueur suite à un gain peut-être effectué sans que le joueur n'ait à l'acquitter.

En revanche, une notification devra être signalée au joueur à sa reconnexion, et devra lui être présentée tant qu'elle n'aura pas été acquittée.

Si l'utilisateur ne se connecte pas à nouveau, cette notification ne sera donc jamais tracée au niveau du frontal.

L'implantation d'un système de notification propre ou commun à plusieurs types de jeu en ligne est laissée à l'appréciation de l'opérateur.

* * *

Coffre fort : dans le cas d'une offre multiple en marque blanche où création de compte et PMV sont intégrés par l'opérateur mais les solutions de jeu (trois) sont fournies par des éditeurs (Playtech, Sportingbet...), comment devons-nous organiser l'archivage ? Est-ce un capteur par brique du dispositif (3 solutions de jeux et plateforme gestion compte du joueur et transactionnel) qui adresse un même coffre fort ou faut-il fonctionner à partir des coffres-forts des éditeurs ?

L'ARJEL pourra, pour un même agrément, interroger plusieurs coffres.

Il est donc possible d'imaginer un dispositif à n capteurs (un capteur pour la plate-forme gestion du compte joueur, et n-1 capteurs éditeurs pour les solutions de jeu fournies) et m coffres (un coffre gestion du compte joueur, m-1 coffres éditeurs, voire un seul et même coffre - modulo la redondance - pour n capteurs...).

* * *

Comment pourra-t-on garantir l'exactitude des données si le frontal et les serveurs de jeux ne sont pas en synchronisation? Par exemple, pour des paris rejetés pour des raisons de sécurité qui seront enregistrés dans le frontal mais pas acceptés.

L'annulation d'un pari rejeté pour des raisons de sécurité devra faire l'objet d'une notification auprès du joueur. Le projet de dossier des exigences techniques décrit explicitement les événements PANNUL et POANNUL (partie 1.3.4.c du projet d'annexe au projet de dossier des exigences techniques) relatifs aux paris sportifs et au poker. Ces événements référencent le pari ou le tournoi cibles de l'annulation, ainsi que la raison de l'annulation.

* * *

Comment peut-on arrêter un jeu en cas de défaillances d'écriture, étant donné que le serveur du jeu ne saura pas s'il y a eu une défaillance du frontal (peu probable) ou s'il y a eu une défaillance/une coupure de la ligne du côté du client ?

Il convient d'intégrer convenablement le capteur à la plate-forme de jeu en ligne, afin de traiter ce cas d'erreur comme tout autre dysfonctionnement d'un composant de la plate-forme.

* * *

Un opérateur peut-il avoir les droits administrateurs (« root ») sur ces machines ? Utiliser des solutions de type 'boîtes noires' ?

Non, les chapitres 4.1.3 et 4.1.5 introduisent la notion d'"administrateurs techniques et opérationnels". Ces utilisateurs possèdent des privilèges qui leur permettront d'administrer et de superviser techniquement le coffre (arrêt/redémarrage, configuration réseau, analyse de la journalisation, etc.). Un accès à distance via SSH ou sur la console n'est donc pas proscrit : en revanche, la réalisation de ces accès système avec le niveau de privilège de root n'est pas souhaitée, à moins de mettre en oeuvre des mécanismes de restriction de type

securelevel/capabilities (par exemple) pour limiter les droits de l'uid 0. Le coffre-fort est donc, un système compartimenté.

* * *

Il est indiqué que toutes les actions du joueur doivent être stockées. Pouvez-vous préciser le contenu de cette obligation : vise-t-elle les seules actions 'humaines', générées par un clic ? Et les actions automatiques asynchrones (validation d'un pari, envoi d'un mail...) ? En cas de double action et de solde insuffisant, les deux paris seront indiqués en cours de traitement, mais un seul sera validé. Faut-il enregistrer les deux demandes ? Le rejet de l'un ? La validation de l'autre ? Transformer ces traitements automatiques en actions humaines (confirmation d'information) afin de les loguer ?

Seuls les événements spécifiés dans l'annexe au dossier des exigences techniques doivent être stockés. Chaque enregistrement d'évènement doit résulter d'une action humaine. En particulier, un enregistrement ne peut résulter de l'emploi d'une méthode asynchrone comme la méthode AJAX XmlHttpRequest.

* * *

Le cahier des charges indique qu'une marge de 'tolérance' existera concernant des solutions alternatives (bloc NB de la page 11 du Dossier des Exigences techniques). Quelle est la pérennité éventuelle sur cette tolérance ?

Sauf indication contraire spécifiquement indiqué dans le DET, les aménagements cités sont permanents.

* * *

Dans plusieurs documents est décrit comment les données doivent être correctement « enchaînées ». Qu'est ce que cela implique? Est-ce simplement que les événements doivent être dans l'ordre approprié, ou est- il nécessaire que toutes les actions soient regroupées au nom d'un utilisateur particulier?

Non, les événements n'ont pas à être regroupés en fonction de leur contenu. Ils doivent être simplement chaînés/signés par le coffre dans l'ordre de réception -- ainsi la liste chaînée des événements pourra comporter une séquence d'évènements générés par plusieurs capteurs (dans le cas d'une configuration multi-capteurs et multi-coffres).

* * *

Est-ce que l'estampille d'un fichier xml écrit dans le coffre-fort reflète le temps de l'action demandée par l'utilisateur, ou l'heure à laquelle il a signé dans le coffre-fort?

L'horodatage figurant dans les entêtes de l'évènement XML (données de jeu) doit être positionné par le capteur. L'horodatage figurant dans la signature de l'évènement ou du lot (données de validation) doit être positionné par le coffre.

* * *

La relation du Capteur et du coffre-fort est-elle toujours 1-à-1 ? Par exemple un Capteur peut-il écrire à plusieurs coffres-forts, ou un coffre-fort écrire à plusieurs Capteurs?

Non, il peut y avoir n capteurs et m coffres, ne serait-ce que pour des raisons de disponibilité. L'ARJEL interrogera autant de coffres que nécessaire, par agrément.

* * *

Est-ce que nous redirigeons uniquement des demandes de traçage vers le Capteur?

Oui.

* * *

Existe-il une liste de sociétés recommandées pour la mise en œuvre et l'installation du « coffre fort » et du « capteur » ?

Non.

* * *

Est-ce que l'XML doit être envoyé à l'ARJEL via la méthode « push », ou « récupérée » par l'ARJEL via la méthode « pull » ?

Le frontal doit intégrer une interface de consultation au niveau de laquelle l'ARJEL se connectera de façon discrétionnaire afin de télécharger les traces de jeu.

* * *

Est-ce qu'un correspondant technique de l'ARJEL sera disponible pendant la période de test pour nous certifier que les données sont bien transmises comme il le faut ? (données des opérateurs transmises par XML)

Oui.

* * *

Quelle partie de ce qui est décrit est obligatoire et quelles « paroles » sont optionnelles (ou au moins dans un premier temps)? Il y a quelques exigences sans beaucoup d'utilité, par exemple, le traçage de fichiers et leur disponibilité pour l'agent de collecte de l'ARJEL par accès à distance. Annexe 3. 3.1.1, 3.1.2, 3.1.3.

L'ensemble des messages décrits dans l'annexe au dossier des exigences techniques est obligatoire, sauf mention explicite. Il n'y a pas de sous-ensemble à respecter, dans un premier temps, concernant ces enregistrements.

La disponibilité des traces pour l'agent de collecte est au coeur du dispositif de contrôle mis en oeuvre dans le cadre du projet de loi.

* * *

Que se passe-t-il en cas de surcharge du système ?

Le dimensionnement du système doit permettre de prévenir tout problème de surcharge, en prenant en compte les aménagements proposés (traitement par lot, écriture différée au sein du coffre-fort, etc.) dans le dossier des exigences techniques et, le cas échéant, la FAQ.

* * *

Que se passe-t-il en cas de défaillance du système ?

Une défaillance du système, frontal y compris, doit être prise en compte comme pour tout autre composant du système d'information.

* * *

Devons-nous synchroniser les données des joueurs avec le frontal en temps réel ?

Le capteur étant en coupure, lui-même et le coffre sont synchronisés en temps réel. Seule l'écriture au sein du coffre peut être différée, ainsi que la mise à disposition des traces au niveau de l'interface de consultation de l'ARJEL.

* * *

Est-ce que le protocole requiert un accusé de réception (acknowledgement)?

Oui.

* * *

Le frontal peut-il traiter des flux émanant de différentes sources ? En effet, dans le cadre de [nom anonymisé d'un site de jeux.fr], notre SI va traiter de l'inscription du client mais pas des opérations de jeux.

Oui.

* * *

Le cryptage 256 bits pour les échanges du frontal vont demander beaucoup de ressources CPU, d'électricité et d'énergie. Pourquoi ne pas réduire cette clé ?

La taille de clef minimale recommandée par le RGS est de 128 bits pour un algorithme de chiffrement symétrique : il est donc possible de configurer des algorithmes de chiffrement utilisant des clefs de 128 bits. L'utilisation de clefs de chiffrement de 256 bits correspond néanmoins à une pratique usuelle et à la configuration par défaut de nombreux serveurs SSL/TLS.

* * *

Un opérateur peut-il gérer lui-même son coffre-fort et son capteur ou doit-il recourir à un tiers de confiance ?

L'opérateur peut lui-même gérer son capteur et son coffre-fort.

* * *

Que faire en cas d'identification d'une utilisation de proxy ? Et dans le cas où l'adresse source n'a pas été masquée par le proxy ?

L'utilisation d'un relais applicatif (HTTP/HTTPS, Socks, etc.) ou d'un rebond (serveur hébergé, VPN avec tête de tunnel hors de France, etc.) fait naturellement partie des techniques de contournement classiques identifiées. Cette pratique d'utilisateurs avertis constitue un risque résiduel accepté contre lequel il n'est techniquement pas réaliste de lutter efficacement.

En revanche, la collecte de ces informations (identification de l'appartenance d'une adresse IP à un netblock connu, enregistrement de l'adresse IP d'origine transmise par l'entête X-Forwarded-For ou équivalent, ou encore discordance entre la localisation de l'adresse IP et le langage demandé par la navigateur) font partie d'éléments techniques effectivement susceptibles d'être analysés par l'opérateur à des fins de contrôle.

* * *

Fonctionnalités :

- Est-ce que le streaming sera autorisé pour nos clients?
- Si nous l'autorisons pour nos clients, alors nous devons envoyer ce xml au frontal, dans le cas où il est payant ?

Oui, à condition que le capteur soit à même de prélever les événements dans ce flux, suivant le principe d'acquiescement vis-à-vis de la plate-forme de jeu et du coffre-fort qui est exposé dans le dossier des exigences techniques.

* * *

Est-ce que le capteur est la seule application qui peut écrire des données dans le coffre-fort, ou ces données pourraient également être poussées par les systèmes back-end?

Seul le capteur possède un profil déposant. Les systèmes back-end, potentiellement installés en dehors de la France métropolitaine, n'ont pas vocation à écrire dans le coffre, dans la mesure où les données enregistrées doivent provenir du joueur et non de la plate-forme de jeu.

Mutualisation des ressources : notre solution est dotée de 2 niveaux de service : le premier niveau, service « d'accueil » a en charge la réception d'une transaction (depuis un capteur). Notre solution mutualise les ressources physiques (serveurs), des flux de différents opérateurs peuvent alors transiter via les mêmes serveurs. La ségrégation est assurée au niveau de l'espace de stockage, est-ce conforme ?

La ségrégation doit également garantir l'étanchéité des environnements dans lesquels s'exécutent les processus en charge de la signature et du chiffrement des données. Plus généralement, la réponse sera apportée par l'analyse technique qui sera réalisée dans le cadre de la CSPN.

Taille des clés : nous prévoyons de fixer la taille des clés asymétriques à 2048 octets. Est-ce conforme ? Dans le cas contraire pouvez-vous nous donner la taille des clés ?

Les tailles de clés doivent être conformes aux règles énoncées dans le Référentiel général de sécurité disponible sur le site de l'ANSSI. Si l'algorithme asymétrique utilisé est l'algorithme RSA, une taille de clé 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).

Taux de disponibilité des fonctions d'accès du coffre-fort par l'ARJEL : nous envisageons une architecture du coffre-fort dans laquelle la disponibilité des fonctions de collecte et scellement vis-à-vis des capteurs est indépendante de la disponibilité des fonctions d'accès et d'extraction à distance vis-à-vis de l'ARJEL. Ces deux fonctions sont traités par des sous-systèmes distincts. Nous comprenons que le capteur doit attendre l'acquiescement du coffre avant de retourner les acquiescements de la plateforme de jeux vers le client. Ainsi, si la fonction de collecte et scellement (conformément aux cahiers des charges, calcul d'empreinte, chainage, signature) n'est pas disponible, le capteur ne doit pas relayé les flux applicatifs de la plateforme de jeux vers le joueur. En revanche, si les fonctions d'accès à distance ne sont pas disponibles, peut on accepter que les capteurs et les fonctions de collecte et scellement puisse continuer à fonctionner sans interruption de service pour la plateforme de jeux vis-à-vis des joueurs.

La priorité doit effectivement être donnée à la fonction de collecte et de scellement : la défaillance de la fonction d'accès à distance ne doit pas provoquer d'interruption de service pour la plate-forme vis-à-vis des joueurs.

Scellement du hardware : nous envisageons de sceller physiquement les boîtiers HSM en cadenassant les baies (cadenas accessible via un coffre-fort (physique) accessible par 1 ou 2 personnes habilitées). Est-ce conforme ?

Oui, avec la mise en place d'un système de scellement physique pour le cas spécifique des supports de stockage, afin d'identifier que des accès à ces derniers ont été effectués. Le DET sera mis à jour pour prendre en compte cette évolution.

Est-il envisageable que l'opérateur ait accès en lecture seule aux données stockées dans le coffre-fort mis à disposition de l'ARJEL ? Cet accès ne remet pas en question l'intégrité des données archivées mais permettrait de s'assurer de leur cohérence.

Non.

Initialisation du coffre : l'initialisation d'un coffre suppose de tirer un certain nombre de secrets cryptographiques et de les stocker dans un HSM. Nous considérons que cette cérémonie se déroulera dans les locaux de l'ARJEL, en présence des représentants de l'opérateur. Quand pourra-t-on disposer de la procédure que l'ARJEL souhaite mettre en place pour cette initialisation ?

Cette cérémonie sera réalisée en vue de la certification initiale du composant frontal, au maximum 6 mois après sa mise en oeuvre opérationnelle.

L'ARJEL transmettra en amont son certificat de chiffrement et les certificats clients nécessaires à la collecte à distance.

Dans ce délai, le coffre pourra fonctionner avec des clefs (de signature, notamment) temporaires.

Faut-il plusieurs Frontaux, s'il y a plusieurs segments de jeux ?

Non, un frontal peut être mutualisé.

Définition de métadonnées : l'ARJEL prévoit d'extraire les données à partir des tranches d'événements ou d'horaires. Dans l'hypothèse où ces données seraient chiffrées, il faudrait les gérer non chiffrées sous forme de métadonnées pour en permettre la sélection. Y aurait-il d'autres métadonnées à prendre en compte pour faciliter l'extraction et la consultation de l'ARJEL ?

Non, ces données de validation sont les seules données à constituer en métadonnées.

La gestion des certificats : notre plateforme d'archivage comporte une Autorité de Certification Technique constituée selon les meilleures pratiques (HSM, cérémonie des clés, partage de secrets ...). Etait-il possible d'utiliser cet environnement de confiance ? Sinon, quel délai pourrait être accordé, après lancement, pour intégrer les certificats de l'ARJEL ?

Oui, cet environnement pourra être utilisé.

Le certificat de chiffrement des événements sera transmis par l'ARJEL et devra être intégré dès la mise en oeuvre opérationnelle initiale du coffre.

L'intégration de l'ensemble des certificats dûment signés s'effectuera en vue de la certification du composant frontal, au maximum 6 mois après sa mise en oeuvre opérationnelle.

La confidentialité des informations : en tant que tiers-archivageur nous prenons des engagements forts concernant la confidentialité des données qui nous sont confiées. La confidentialité des informations est assurée par la gestion d'habilitations et de droits d'accès complétées par une traçabilité complète de l'ensemble des accès. Dans ce contexte, le chiffrement des archives au moment du dépôt et le déchiffrement au moment de la consultation apportent peu de sécurité supplémentaire et beaucoup de risque en terme de performance (streaming, parallélisation temps de calcul) et de fiabilité du processus (pas de garantie de lisibilité si les clés sont non disponibles). Dans ce contexte de tiers-archivageur, le chiffrement est-il nécessaire ? Si oui est-il envisageable de le faire à la source, c'est à dire de chiffrer la trace XML avant dépôt, le chaînage et le scellement portant alors sur des traces chiffrées ? Et de déchiffrer après consultation ou extraction ?

Le chiffrement des informations est obligatoire.

Du point de vue de la sécurité cryptographique, il convient de ne pas signer des messages chiffrés (cf. "Robustness Principles for Public Key Protocols", R. Anderson and R. Needham).

De plus, certains paramètres comme l'identifiant d'évènement ou l'identifiant de coffre, doivent être fixés par le coffre, et non par le capteur. A moins d'être dans une configuration mono-capteur et mono-coffre, il n'est donc pas possible de chiffrer les enregistrements avant dépôt au coffre.

Accès physique sur site non autorisé à des tiers : compte tenu des exigences, en terme de sécurité, de nos clients et de notre modèle de coffre-fort en mode hébergé, l'accès aux locaux contenant les machines est réservé aux personnels techniques habilités. Dans le cadre d'un Audit ou d'une requête judiciaire, les intervenants seraient systématiquement accompagnés par le personnel de CDC Arkhinéo. L'ARJEL a toujours la possibilité d'accéder aux données à distance y compris pour effectuer des extractions pour des tranches d'évènements ou d'horaires. Si malgré tout une procédure

d'extraction sur site devait être nécessaire, pourrait-elle être effectuée, à la demande de l'ARJEL, par le personnel du tiers-archiviste ?

L'extraction sur site pourra être effectuée par le tiers-archiviste mais impérativement en présence et sous le contrôle de l'ARJEL.

Doit-on obligatoirement utiliser un module HSM interne ou peut-on utiliser un HSM réseau type « nshield connect » de Thales ?

L'utilisation d'un HSM réseau est conforme au DET.

Pour le chiffrement des données, faut-il nécessairement utiliser un moyen matériel, comme par exemple le HSM ?

Non, le HSM (qui est obligatoire) doit être utilisé pour la génération de la clé de signature et les opérations de signature, mais pas nécessairement pour le chiffrement des données (ce qui pourrait être lent et donc pénalisant). Ce chiffrement peut être réalisé par des moyens matériels ou logiciels.

DET Partie 4.1.

Est ce que, dans l'un et l'autre cas, l'opérateur sera tenu à déposer les données dans un seul coffre-fort ou devra-t-il aménager un coffre-fort pour chaque site marque blanche?

Un seul coffre-fort. Il convient de se reporter aux réponses d'ores et déjà communiquées à travers la FAQ.

DET Partie 4.1.1

Dans la partie 4.1.1 du DET, il est écrit que le coffre devra obtenir une certification CSPN de 1er niveau délivrée par l'ANSSI. Nous prévoyons de faire installer et intégrer ce coffre par un éditeur de coffre électronique certifié CSPN (ou en cours de certification). Fournir une copie de la certification de l'éditeur répond-il aux exigences de l'ARJEL concernant cet article ? ET 4.1.1

Le coffre-fort doit faire l'objet d'une certification de sécurité de premier niveau délivrée par l'ANSSI. Le candidat devra fournir soit cette certification, soit une note délivrée par l'ANSSI indiquant qu'une CSPN a bien été lancée pour le coffre-fort. Dans tous les cas, la cible de sécurité devra également être fournie.

* * *

Serait-il possible de continuer à envoyer uniquement les données agrégées à l'ARJEL, de la même façon que dans le cas où le frontal n'est pas encore opérationnel à 100%, et d'utiliser cette méthode pour toujours ?

Les données agrégées correspondent aux données dites de supervision qui doivent être transmises systématiquement. Ces données correspondent à l'Annexe partie 2.

Conformément à l'encadré de la page 9 du DET, les données du frontal qui ne pourraient être archivées lors de sa déclaration en mode fonctionnement devront être transmises à l'ARJEL par le biais des données de supervision.

Cette souplesse ne peut en aucun cas aller au delà de la certification à 6 mois du frontal.

* * *

Le coffre fort devra obtenir une certification de sécurité de premier niveau (CSPN). Selon l'ANSSI, cette certification est expérimentale et s'adresse plus vers un code open source. Est-ce que les opérateurs seront tenus d'utiliser une certification de sécurité qui est toujours en phase expérimentale (à compter du 15/02/10, il n'y avait que 6 produits certifiés sur le site de l'ANSSI - http://www.ssi.gouv.fr/site_rubrique54.html)?

Le caractère expérimental de la CSPN ne gêne en rien l'ARJEL.

Le périmètre de la cible de la certification CSPN est décrit en points clés au paragraphe 4.1.1 du DET. Quel sera le processus pour que l'ARJEL s'assure que les cibles de certification CSPN sont bien en ligne avec ses attentes ? Pour que l'ARJEL soit impliqué formellement en amont du processus CSPN pour en valider la cible, est-ce que le processus de l'ANSSI dénommé « Qualification Élémentaire » pourrait être envisagé ?

Le processus de « Qualification Élémentaire » pourrait être envisagé, mais l'ARJEL attend en premier lieu que lui soit communiquée, par l'éditeur de la solution de coffre-fort, la cible de certification CSPN qui sera proposée à l'ANSSI.

Sous quel format et comment doit-on transférer les données que l'on n'est pas en mesure de transmettre via le frontal à l'ouverture mais que l'on doit tout de même mettre à la disposition de l'ARJEL?

L'opérateur pourra déposer un lot, au niveau du dépôt mis à disposition par l'ARJEL :

- journalier, couvrant 24 heures d'activité (à partir de 6 heures du matin) ;*
- dont les événements, séquentiels, disposent d'un identifiant de coffre unique et propre à la supervision (par exemple : 9999) ;*
- respectant le format XML présenté dans le DET, signé avec la clef temporaire du coffre (avant mise en place des clefs définitives), compressé et chiffré avec la clef publique de l'ARJEL.*

DET Partie 4.1.3

Si une intervention technique sur le coffre-fort requiert de briser les scellés physiques posés lors de la cérémonie des clés, quel serait le protocole à suivre avant la remise en service ? Exclusion du système concerné de la solution coffre-fort et mise en place d'une nouvelle cérémonie pour la réintégration du système dans la solution ?

Oui, une nouvelle cérémonie devra être effectuée.

* * *

Le chapitre 4.1.3 exclut-il bien la possibilité pour les équipes d'administration technique (ingénieurs systèmes ou middleware) d'un opérateur de se connecter via le réseau ou localement aux machines liées au coffre-fort et donc d'administrer ces dernières ? Le coffre-fort est-il bien dans l'esprit une boîte noire pour ses équipes ? (ex: impossibilité pour un administrateur système Unix de se connecter root à distance via SSH ou sur la console sur les machines coffre-fort) ?

Non, les chapitres 4.1.3 et 4.1.5 introduisent la notion « d'administrateurs techniques et opérationnels ». Ces utilisateurs possèdent des privilèges qui leur permettront d'administrer et de superviser techniquement le coffre (arrêt/redémarrage, configuration réseau, analyse de la journalisation, etc.).

Un accès à distance via SSH ou sur la console n'est donc pas proscrit : en revanche, la réalisation de ces accès système avec le niveau de privilège de root n'est pas souhaitée, à moins de mettre en oeuvre des mécanismes de restriction de type securelevel/capabilities (par exemple) pour limiter les droits de l'uid 0.

Le coffre-fort est donc un système compartimenté.

* * *

A partir de quel étape du processus et dans quel timing seront disponibles les certificats de l'Arjel afin de permettre de réaliser des tests de fonctionnement du frontal ?

L'IGC de l'ARJEL est en cours de réalisation, et les informations nécessaires seront diffusées dans les meilleurs délais aux opérateurs. Les certificats seront conformes au standard X.509v3, et leur profil conforme au RFC 3280.

L'implémentation de référence sera celle de la bibliothèque cryptographique OpenSSL.

Deux questions apparentées donnant lieu à une réponse commune :

1/ Instanciation du coffre-fort : pour chaque coffre-fort à instancier, nous envisageons de valider le fonctionnement du coffre-fort en environnement de production avant la cérémonie des clés. Est-ce envisageable ?

2/ Instanciation du coffre-fort : pour chaque coffre-fort à instancier, nous envisageons de valider le fonctionnement du coffre-fort en environnement de production en utilisant les boîtiers HSM de production. Est-ce envisageable ?

Oui. L'ARJEL publiera prochainement dans la rubrique « ressources techniques », des certificats X.509v3 et des biclefs RSA à des fins de tests d'interopérabilité.

Cérémonie des clés : nous envisageons de « mutualiser » les cérémonies des clés (ex: faire 1 cérémonie pour 1 opérateur avec plusieurs coffres). Est-ce envisageable ?

Oui.

Certificats : quelle est la différence entre le certificat « authentification coffre » et le certificat « HSM auth. Matérielle »?

Le certificat « HSM auth. Matérielle » est le certificat de signature de la configuration du coffre (fichiers de configuration, binaires, bibliothèques partagées, etc).

Le certificat d'authentification du coffre par rapport au capteur est un certificat X.509v3 serveur permettant une authentification SSL/TLS (encapsulant HTTP, MQ, etc.).

Le certificat « HSM signature » est le certificat de signature permettant le scellement des évènements de jeu.

DET Partie 4.1.4 - Fonctions de création de traces du capteur

Notre solution s'appuie sur un module de type sonde réseau, posée en dérivation (et non en coupure) et qui capte l'ensemble du flux réseau pour ensuite l'analyser et en extraire les données destinées au coffre-fort électronique pour archivage. Un tel dispositif en dérivation est-il acceptable ?

Une telle solution peut être envisagée sous réserve d'être très clairement décrite et de respecter strictement les contraintes spécifiées dans le paragraphe 3.1.1 du document annexe, notamment à propos de la notion d'acquiescement (en provenance de la plate-forme de jeu) qui conditionne la journalisation de la transaction.

Si le capteur est indisponible tandis que les opérations de jeu continuent, mais que le système est capable de fournir les tranches horaires des indisponibilités, cela est-il acceptable pour vous ?

L'indisponibilité n'est pas un état envisageable du capteur. Les éléments à retenir sont énoncés dans l'encadré du §4.1.4 du DET. Envisager des tranches horaires d'indisponibilité du capteur pendant que des opérations de jeu se déroulent, est ainsi totalement en opposition avec le DET.

* * *

Est-il possible de traiter la mise au coffre de manière asynchrone ?

Capteur et coffre doivent fonctionner de façon synchrone, mais l'écriture de l'évènement (et son traitement cryptographique) au sein du coffre peut être différée, dès lors que le capteur a bien reçu l'accusé de réception du coffre.

* * *

Si dans une pile d'évènements destinés à être enregistrés dans le coffre, l'un d'entre eux échoue, doit-il tout de même être enregistré ?

Ce cas de figure ne peut pas se produire puisqu'un évènement échoué doit être, en amont, rejeté par le capteur.

* * *

Vous indiquez qu'une trace ne doit être enregistrée que lorsque le frontal reçoit une confirmation de lecture par le joueur. Mais si un joueur ne répond pas (déconnexion ou autre), l'information ne sera pas vue par le capteur. Que faut-il faire alors ?

Il convient de rediriger le joueur (dès sa reconnexion) vers une page qui l'oblige à valider la bonne prise en compte de l'évènement (évènement financier notamment). Sauf cas particuliers expliqués dans l'annexe au DET, cette validation par le joueur est nécessaire au stockage de l'élément et à la poursuite de son activité de jeu : elle devra donc lui être représentée jusqu'à acquittement. Sans une forme d'acquiescement, l'évènement de jeu ne peut pas être pris en compte et ne doit donc pas être stocké.

* * *

Nous ne comprenons pas que l'indisponibilité du capteur doive entraîner un arrêt de l'activité des joueurs. Ce principe nous semble contraire à l'efficacité de la plate-forme de jeu et ne paraît pas se justifier dans la mesure où l'ensemble des moyens sont mis en oeuvre afin d'assurer une disponibilité maximale (ces moyens étant par ailleurs certifiés). Est-il envisageable, dans un souci de transparence, de fournir les SLAs associés à cette plate-forme et d'éviter ainsi un point de coupure technique en cas d'incident ?

L'ensemble des opérations effectuées par le capteur font partie intégrante du traitement de la requête, comme tout autre processus métier dont la réussite conditionne celle de la transaction dans son ensemble.

La plate-forme doit donc mettre en oeuvre des mécanismes de détection et de reprise sur erreur, afin qu'une indisponibilité du capteur -- comme l'indisponibilité de tout autre composant de la plate-forme -- n'entraîne pas un arrêt de l'activité des joueurs.

* * *

Projet de DET point 4.1.4 (fonction de création de traces du capteur) et projet d'annexe au DET point 3.1.1 (fonctions de création de traces du capteur (1) Remarque sur le positionnement du capteur) : la mise en oeuvre du capteur peut également s'insérer dans la logique de présentation de l'application, en amont de la logique de jeu, par exemple au niveau des serveurs d'applications effectuant le traitement des requêtes en provenance du logiciel client. Dans ce cas, la requête ne fera pas l'objet d'une interception... »

- Question 1 : est-ce que serait conforme au cahier des charges, l'implémentation du capteur consistant en une api java à intégrer dans la logique de présentation de nos logiciels de jeux, sachant que cette api (partie cliente du capteur) et sa partie serveur respecteraient les contraintes d'intégrité des données, d'acquiescement de dépôt ?

- Question 2 : est-ce que serait conforme au cahier des charges, l'implémentation du capteur utilisant le protocole syslog pour la génération de traces, plus précisément, l'utilisation du daemon rsyslog implémentant la RFC 3195 assurant un transport et dépôt garanti, sachant que ce protocole de mécanismes de reprise sur erreur serait doublé avec une double écriture dans des fichiers pour reprise et que cette implémentation permettrait également de transmettre en crypté, et entre systèmes « authentifiés ». ?

Ces deux exemples d'implantation sont conformes au DET.

DET Partie 4.1.5

S'agissant des fonctions de stockage des traces du coffre-fort, un opérateur peut-il, lorsqu'il dispose de plusieurs agréments, scinder logiquement le coffre (par exemple, les données de compte joueur, les données financières communes à tous les jeux dans le même espace puis les données de jeu, chacune dans un espace dédié à un jeu)

Oui.

* * *

S'agissant des fonctions de stockage des traces du coffre-fort, un opérateur peut-il, lorsqu'il dispose de plusieurs agréments, scinder logiquement le coffre, par exemple, les données de compte joueur, les données financières communes à tous les jeux dans le même espace puis les données de jeu, chacune dans un espace dédié à un jeu ?

Oui, l'ARJEL interrogera ensuite indifféremment les coffres suivant les indications transmises par l'opérateur.

* * *

Est-il possible de gérer la fonction de stockage des traces à travers plusieurs coffres-forts, éventuellement chez plusieurs prestataires ?

Si oui, comment faire une extraction continue puisque la numérotation sera gérée de façon distincte par chaque coffre ?

La fonction de stockage des traces peut-être gérée à travers plusieurs coffres-forts (cf. 3.1.2 de l'annexe), éventuellement chez plusieurs prestataires, à charge pour l'exploitant de gérer correctement les identifiants (notamment identifiant de coffre et identifiant d'évènement) pour lui permettre de satisfaire les exigences de l'ARJEL.

En pratique, l'annexe mentionne que l'ARJEL pourra interroger autant de services web qu'il y aura de coffres. Chaque coffre pourra donc entretenir un séquençement continu qui lui sera local. L'unicité au sein de la plate-forme de l'opérateur sera assurée par la notion d'identifiant de coffre, nouvellement introduit dans les entêtes d'évènements, et documentés dans les schémas XML détaillés dans l'annexe au DET.

L'unicité d'un évènement sera donc assurée :

- au sein d'un coffre, par son numéro de séquence.*
- chez un opérateur, par la combinaison du numéro de séquence et de l'identifiant de coffre.*
- sur l'ensemble des opérateurs, par la combinaison du numéro de séquence, de l'identifiant de coffre et de l'identifiant d'opérateur.*

DET Partie 4.1.6.b

Lien réseau entre les opérateurs et l'ARJEL : quelles connexions réseaux l'ARJEL considère-t-elle utiliser pour extraire à distance les traces collectées par les opérateurs : une ligne spécialisée ouverte entre l'ARJEL et le frontal de l'opérateur ou une liaison à travers Internet.

Le lien établi entre l'ARJEL et l'opérateur sera un tunnel SSL/TLS mutuellement authentifié par certificats, et réalisé à travers Internet. Une protection par filtrage IP complètera le dispositif.

DET Partie 4.1.7 – Nature et format des données

Il est écrit « 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 ». Merci de confirmer que cette exigence de confirmation s'applique à ces données « poussées » seulement. Si cette exigence devait s'appliquer à toutes les données, merci d'indiquer ce qu'il est attendu de l'opérateur.

Sauf exception clairement indiquée (par exemple pour les parties de poker, cf. section 1.3.5.g de l'annexe au Dossier des exigences techniques), tous les événements enregistrés dans le coffre le sont après que le frontal ait obtenu une confirmation de lecture par le joueur (voir partie 1.1.3 du document annexe). Cette confirmation de lecture peut consister en une simple action de jeu (partie de Poker par exemple) ou en un acquittement plus formel dans le cas de données poussées vers le joueur (gain sur pari par exemple).

DET Partie 4.2

Informations relatives à l'architecture du SI. 4.2 du dossier des exigences techniques données mises à disposition systématiquement. Une fois le code transmis à l'ARJEL, est-ce que nous avons la possibilité d'effectuer des changements mineurs (par exemple pour correction d'anomalies) ?

Oui. Il conviendra néanmoins de maintenir un historique des changements apportés à chaque version mineure (documentation technique et fonctionnelle, journaux du système de changement de version utilisé, par exemple), à des fins de traçabilité, en vue notamment du renouvellement de l'homologation, ou encore d'un audit technique qui serait réalisé de façon ponctuelle par l'ARJEL.

DET Partie 4.4

Une société peut-elle être directement certifiée auprès de l'ARJEL en tant qu'éditeur/fournisseur de logiciel afin d'éviter que chaque opérateur utilisant sa plateforme doive demander une certification pour l'utiliser ?

Non, chaque opérateur doit déposer un dossier complet.

* * *

Nous avons examiné la solution proposée par l'ARJEL dans la FAQ du 30 Mars pour la consultation des interdits de jeux.

Dans le contexte de notre SI, une solution de type Web service et/ou API Java comme mode de consultation de la black list, pourrait-elle être envisageable ? En effet, nous n'avons pas connaissance d'utilisation de protocole DNS directement par des applications métiers.

Une autre solution pourrait elle consister en un téléchargement de la black-list mise à disposition par l'ARJEL ? Est-ce acceptable ?

Dans le cadre de la solution DNS proposée par l'ARJEL, serait-il possible pour les opérateurs de contacter directement le DNS ARJEL sans passer par une infrastructure en local ?

Pour des raisons de robustesse et de sécurité, l'ARJEL ne déploiera pas de service Web pour l'interrogation du fichier des interdits de jeu, mais s'appuiera sur un protocole et une implantation logicielle robustes, éprouvés et adaptés à ce type d'interrogation binaire.

De même, pour des raisons de confidentialité, l'ARJEL ne mettra pas à disposition la liste noire. Quant à la liste des empreintes cryptographiques, elle devra faire l'objet d'une interrogation à chaque ouverture de connexion d'un joueur : la journalisation des interrogations DNS par l'ARJEL permettra de s'assurer que l'opérateur effectue bien cette vérification systématiquement. Ainsi, les zones DNS configurées disposeront donc de TTL à zéro, afin d'éviter toute mise en cache des enregistrements par des relais DNS intermédiaires..

Les opérateurs pourront contacter les serveurs DNS de l'ARJEL à leur convenance, à condition de respecter la mise en oeuvre du protocole TSIG, permettant de s'assurer de l'authenticité des échanges, de bout-en-bout, à l'aide d'un secret partagé.

DET Partie 4.4.1

Huit questions apparentées donnant lieu à une seule réponse :

1/ Concernant les interrogations des interdits de jeux, il n'est pas précisé quels sont les moyens techniques à mettre en oeuvre. Quels seront les moyens d'accès, les protocoles et interfaces supportés pour ces interrogations ? La mise en oeuvre de cette solution est-elle un pré-requis au démarrage de l'activité ?

2/ La loi actuelle ou à venir ne prévoit pas l'accès au fichier du ministère de l'Intérieur par des tiers : comment faut-il procéder ?

3/ Fichiers des interdits de jeu : le DET indique que la consultation du fichier des interdits de jeu se fera au travers d'un système informatique opéré par l'ARJEL. Serait-il possible d'avoir plus de précisions sur ce point ? S'agit-il d'un web-service SOAP ? Quelles données seront requises en entrée ? Quel niveau de disponibilité sera garanti par l'ARJEL ? Quel temps de réponse sera garanti par l'ARJEL ? Si le web-service est indisponible, l'opérateur peut-il continuer le processus d'ouverture du compte provisoire et tenter à nouveau la vérification plus tard ? En s'inspirant du fonctionnement des serveurs d'autorisation bancaire, est-il possible de définir que une non-réponse en moins de 3s équivaut à une autorisation ?

4/ Quelles sont les modalités d'interfaçage et contrôle d'accès pour la consultation de la base des interdits de jeux hébergée au sein du système d'information de l'Arjel ? i. Quelle est l'engagement de service de l'Arjel ? ii. Que faire en cas d'indisponibilité du service Arjel ? iii. Quelles sont les modalités de reprise sur erreur ? iv. Pouvez - vous préciser l'ensemble des attributs permettant le contrôle (fourni par l'Arjel) ?

5/ Le DET indique que la consultation du fichier des interdits de jeu se fera au travers d'un système informatique opéré par l'ARJEL. Serait-il possible d'avoir plus de précisions sur ce point ?

6/ Quelle sera la procédure précise pour accéder à la liste des interdits de jeu ?

7/ Article 4.4.1 du DET (interdits de jeu) : Quels sont les éléments identifiant un joueur et permettant à l'opérateur d'interroger les interdits de jeux : nom prénom ... Un mode intermédiaire de contrôle manuel est-il acceptable au démarrage de l'activité ? Quelles seront les modalités d'inscription pour un joueur sur le fichier des interdits (les mêmes que pour les casinos ?) ? Comment sera mise en œuvre la consultation de l'interface ARJEL ?

8/ Retours d'expertise : Interdiction de jeu. Les participants prennent acte du processus défini en matière de gestion des interdits de jeu et souhaitent vous faire part des éléments suivants. 1/ Les opérateurs de jeu ont besoin d'une visibilité concernant la réglementation applicable et notamment la coexistence ou non d'une liste d'interdiction de casino et d'une future liste d'interdiction de jeux. 2/ Un échange réalisé auprès des opérateurs de casinos physiques participant aux travaux du Geste révèle que le processus de consultation des listes interdictions de casino soulève un important risque d'homonymie et donc d'identification de la personne à interdire. Il conviendra de

définir un mode de consultation de la liste d'interdiction de jeux permettant de lever cette difficulté.

Afin de concilier robustesse, extensibilité et sécurité (authentification des parties, authenticité, confidentialité et traçabilité des transactions), le protocole d'interrogation s'inspirera de la technique de la liste noire DNS (DNS Blacklist). Le protocole DNS sera donc mis en oeuvre, ainsi que l'extension de sécurité TSIG afin d'assurer l'authenticité des réponses -- sans recourir à DNSSEC. Ainsi :

- *l'ARJEL mettra en oeuvre une infrastructure DNS sécurisée et particulièrement redondante. Une plate-forme sera mise en oeuvre prochainement afin de permettre aux opérateurs déclarés candidats à un agrément de recevoir les paramètres (adresses IP, clefs partagées TSIG, etc.) qui leur permettront d'effectuer les tests d'interopérabilité et de charge, le cas échéant, nécessaires ;*
- *la vocation de cette plate-forme n'est pas de constituer un point de défaillance unique ; dans le cas très hypothétique où une résolution se solderait par un échec, celui-ci ne devra donc pas être bloquant pour l'accès à la plate-forme. En revanche, l'opérateur devra renouveler ses interrogations, par exemple au cours de la navigation du joueur, afin de pouvoir bloquer à tout moment son accès ;*
- *les attributs permettant le contrôle seront, dans une première phase, les nom, prénoms et date de naissance des joueurs. Ces informations ne seront pas utilisées en clair : après une mise sous forme canonique (suppression des diacritiques, passage à la case supérieure, suppression des caractères pour conformité à la classe [A-Z]), une empreinte cryptographique HMAC-SHA1, indexée par une clef secrète, sera calculée et permettra à l'opérateur de former le nom de domaine pleinement qualifié qui fera l'objet d'une interrogation ;*
- *pour l'opérateur, la mise en oeuvre consistera donc :*
 - *en termes d'infrastructure : à installer un ou plusieurs relais DNS récursifs supportant l'extension de sécurité TSIG, avec les secrets partagés appropriés ;*
 - *au niveau de l'application : à mettre en place une fonction d'interrogation d'un enregistrement de ressources de type TXT, portant sur le FQDN formé à partir de la zone réservée à l'opérateur, et d'un préfixe (ou nom d'hôte) construit à partir du condensât HMAC-SHA1 des paramètres précédemment cités.*

L'ARJEL publiera prochainement, sur son site Internet de préfiguration, dans la rubrique dédiée aux ressources techniques, les éléments techniques expliquant en détail la mise en oeuvre de ce dispositif (fichiers de configuration DNS pour l'implantation Bind et autres serveurs DNS cache récursifs avec support de l'extension TSIG, PoC pour la normalisation des chaînes de caractères, avec une visualisation à l'octet pour éviter toute ambiguïté dans le calcul des empreintes, etc.).

L'annexe au DET sera donc mise à jour sur ce point, ainsi que les ressources techniques associées.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

DET Partie 5

Quand doivent être fournies les précisions de type P ? Quelles sont les attentes de l'ARJEL sur les précisions à fournir ?

Les éléments de réponse de type P doivent être fournis dans le dossier de demande d'agrément. Ces éléments sont destinés à étoffer notre compréhension de la façon dont l'opérateur gère la sécurité de ses systèmes d'information.

* * *

Les exigences de type E sont à fournir ultérieurement, le dossier de demande d'accréditation doit-il préciser à quelle date ces documents pourront être fournis ? ou bien préciser que ces documents sont des tâches identifiées et qu'ils seront fournis au fur et à mesure de leur production ?

Conformément à ce qui est indiqué dans la partie 5 du DET, les exigences de type [E] correspondent à des objectifs à atteindre. Si ces objectifs sont atteints d'ores et déjà lors de la demande d'agrément, les éléments liés à ces exigences devront être fournis par l'opérateur. Dans le cas contraire, un calendrier de mise en oeuvre devra être fourni et justifié et les documents devront être fournis dès que les objectifs correspondants seront atteints.

* * *

La définition du SI (définition reprise dans tout le document) présentée dans l'art 5 des exigences techniques : les modules du frontal et l'ensemble des composants susceptible d'interagir avec les plates-formes de jeu de l'opérateur. Pouvez-vous préciser de quels types de composants et d'interactions il s'agit ?

Afin d'illustrer cette définition, le SI devra comporter a minima :

- *l'infrastructure système et réseau d'hébergement de la plate-forme de jeux, dont le frontal ;*
- *l'ensemble des réseaux d'administration et de supervision ;*
- *l'ensemble des réseaux sous la responsabilité (technique ou non) de l'opérateur, par exemple les réseaux bureautiques, interconnectés directement ou indirectement à la plate-forme et plus généralement susceptibles de constituer un point d'entrée vers celle-ci.*

Ainsi :

- *pour un réseau dont le maintien en conditions de sécurité fait l'objet d'une sous-traitance, une copie du contrat devra être transmise à l'ARJEL ;*
- *concernant l'internet, cette vérification s'appuiera sur des audits applicatifs intrusifs réalisés par des experts du domaine choisi par l'opérateur.*

Plus généralement, il est important que tout point d'entrée/sortie de la plate-forme de jeux soit identifié, et fasse l'objet de contrôles de sécurité, par le biais :

- *d'opérations prises en charge par l'opérateur : audits de sécurité, certifications, etc. ;*
- *d'exigences contractualisées, déclinées de la politique de sécurité SI de l'opérateur et imposées à l'ensemble des sous-traitants, pouvant aller jusqu'à la réalisation d'audits sur les SI des sous-traitants (en particulier si les plates-formes d'hébergement sont externalisées).*

DET Partie 5.1

Quelle est la définition d'anomalies majeures pour l'ARJEL (section 5.1) ?

La partie 5.1 correspond aux audits réalisés par l'ARJEL. Cette dernière appréciera chaque vulnérabilité détectée en fonction de l'impact associé et la caractérisera. D'une façon générale, les vulnérabilités majeures sont celles qui remettent en cause l'intégrité ou la disponibilité de la plateforme de jeu ainsi que la confidentialité ou l'intégrité des données qu'elle manipule.

DET Partie 5.2

L'article 5.2 des ET précise que les mises à jour et évolutions des logiciels qui ont fait l'objet d'homologations devront suivre les mêmes procédures d'homologations. Pour des raisons évidentes de cycles applicatifs courts, peut-on considérer que seules les modifications majeures feront l'objet d'un nouveau processus d'homologation ?

Oui. Il conviendra néanmoins de maintenir un historique des changements apportés à chaque version mineure (documentation technique et fonctionnelle, journaux du système de changement de version utilisé, par exemple), à des fins de traçabilité, en vue notamment du renouvellement de l'homologation, ou encore d'un audit technique qui serait réalisé de façon ponctuelle par l'ARJEL.

Y a-t-il d'autres moyens de fournir des informations pour la certification des logiciels de jeux? Ces informations pourraient être mises à disposition en ligne au moyen d'outils de surveillance automatisés.

*Il n'y a aucune certification de logiciel de jeux mais bien une homologation.
Non, il n'y a aucun autre moyen de procéder à cette homologation.*

Dans ce contexte, comment ARJEL prévoit-il que les opérateurs gèrent les exigences ci-dessous? 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. Certains opérateurs développent en méthodologie dite agile (SCRUM / sprint), ayant des équipes logicielles (une vingtaine si ce n'est plus) travaillant en parallèle et développant de nouveaux produits et/ou fonctionnalités toutes les trois semaines en moyenne. L'ARJEL exige de donner son aval à tout changement, y compris un changement d'urgence pour répondre à un incident de sécurité ou de fraude, avant que celui-ci ne soit déployé, ce qu'elle fera dans un délai de deux mois. Cette demande est impossible à satisfaire. Une suggestion serait d'envoyer un "change log" quelques jours en avance.

Cette procédure exclue naturellement les changements mineurs réalisés au niveau des logiciels, et en particulier les correctifs de sécurité, le cas échéant. Seules les mises à jour majeures sont concernées, et il convient effectivement de maintenir un historique précis des changements apportés à chaque version mineure (documentation technique et fonctionnelle, journaux du système de changement de version utilisé, par exemple), à des fins de traçabilité.

Remise des codes source – cela peut-il se faire via « escrow mechanism » (à savoir, dépôt consigné auprès d'un tiers) ?

La disposition évoquée stipule que « L'entreprise communique le code source de chaque logiciel de jeux et de paris destiné à être utilisé par les joueurs et les parieurs français ainsi que le code source de l'éventuel générateur de nombre aléatoire. » L'entreprise doit donc communiquer le code source à l'ARJEL.

En confiant ses codes sources à l'ARJEL, l'entreprise ne s'adresse pas à un tiers mais à une autorité administrative indépendante de l'État français dont les agents et titulaires sont soumis à des obligations de secret professionnel.

Source code requis par ARJEL: a. Est-ce le code source de l'application entière ou seulement par exemple le « moteur de pari » ? b. Comment doit-il être livré ?

a. Il s'agit du code source du moteur de pari et de l'ensemble des briques logicielles en interaction avec les données des utilisateurs. L'ARJEL souhaite en effet pouvoir apprécier la sécurité de la plate-forme de jeu vis-à-vis d'un utilisateur potentiellement malveillant. Le code source des applications web, par exemple, qui interagissent avec les entrées utilisateurs, est donc demandé ;

b. le code source devra être livré sous la forme d'une archive sécurisée, intégrant fichiers de projets, etc.

Comment les opérateurs sont-ils censés appliquer les exigences techniques à des logiciels de jeux qu'ils n'ont pas conçus eux-mêmes ?

Le choix du logiciel de jeu proposé à l'agrément est un choix qui appartient au candidat à l'agrément. Il convient donc de choisir des logiciels conformes, ou adaptés aux exigences techniques demandées.

Rapport d'analyse des codes sources : l'ARJEL peut-elle préciser les attendus en matière de revue des vulnérabilités, les fonctions et la profondeur d'analyse ? Ces analyses sont-elles limitées aux seules fonctions de sécurité ou à l'ensemble des fonctions des applications ? Si oui, l'ARJEL peut-elle préciser les fonctions à auditer ?

Comme indiqué dans la partie 5.2 du DET, le code source du logiciel doit être analysé dans sa totalité et pas seulement pour ses seules fonctions de sécurité. Toutes les vulnérabilités identifiées doivent être explicitées en termes d'impact (conséquences). Le plan d'actions visant à remédier à ces différentes vulnérabilités devra être fourni.

Un test d'intrusion externe est tout à fait insuffisant puisqu'il est habituellement mené en boîte noire. Il convient clairement d'effectuer une analyse en boîte blanche permettant une plus grande exhaustivité en termes de vulnérabilités. Le recours exclusif à des outils d'analyse automatique est également proscrit.

Rapport d'analyse des codes sources : l'ARJEL peut-elle préciser les attendus en matière de revue des vulnérabilités, les fonctions et la profondeur d'analyse ? Ces analyses sont-elles limitées aux seules fonctions de sécurité ou à l'ensemble des fonctions des applications ?

Comme indiqué dans la partie 5.2 du DET, le code source du logiciel doit être analysé dans sa totalité et pas seulement pour ses seules fonctions de sécurité. Toutes les vulnérabilités identifiées doivent être explicitées en termes d'impact (conséquences). Le plan d'actions visant à remédier à ces différentes vulnérabilités devra être fourni.

Le poker fonctionne souvent de la façon suivante : une application coté serveur, un client lourd coté client (souvent avec une fonction d'affichage uniquement), un générateur de nombre aléatoire, un protocole de communication spécifique et propriétaire pour la transmission des données.

Dans ce cadre là, quels sont les audits de code et tests d'intrusion attendus par l'ARJEL ? (liste non exhaustive) : audit du code coté serveur, audit de code du générateur de nombre aléatoire, audit de code du client lourd, audit du protocole de communication, test d'intrusion sur le protocole de communication (usurpation, insertion de données fausses...).

A première vue, cette démarche générale est complète et devrait couvrir l'ensemble des vulnérabilités, en fonction du niveau de profondeur de l'analyse. Le périmètre de l'analyse pourra être adapté après qualification par un expert technique en sécurité, sur la base d'une analyse des risques élémentaire, par exemple.

Une attention plus particulière devrait néanmoins être apportée aux prestations d'audit de code côté serveur, d'audit de code du générateur de nombres aléatoires et de test d'intrusion sur le protocole de communication (par injection de code dans le client lourd, par exemple).

* * *

Pari en ligne : le pari fonctionne souvent de la façon suivante : un serveur qui gère les informations relatives aux paris, d'une part, et une interface web pour afficher les résultats. Il y a dans ce cas aucune interaction entre le client et le serveur autre que la sélection du pari concerné. Parfois il n'y a pas même de formulaire (sauf pour l'inscription). Les audits attendus dans ce cas sont-ils : 1/ audit de code du jeu de pari, coté serveur ? 2/ test d'intrusion sur l'interface web de jeu ? 3/ y en a-t-il d'autre ?

La démarche attendue est effectivement celle d'un audit applicatif intrusif, combinant « audit de code » (portant sur les aspects sécurité : il ne s'agit pas d'évaluer la qualité du code), « audit de configuration », côté serveur, et « tests d'intrusion externes en boîte blanche » afin de simuler les actions d'un utilisateur malveillant et techniquement compétent.

L'objectif de ces audits sera de présenter un plan d'actions à court, moyen et long terme, ainsi qu'une liste de recommandations détaillées, classées en termes d'urgence et de coût de mise en œuvre, selon une classification qui sera à préciser. Le rapport d'analyse devra également lister les vulnérabilités identifiées, précisément décrites en des termes techniques et classées par ordre de criticité. L'opérateur décrira précisément le calendrier de mise en œuvre des recommandations.

L'ARJEL réalisera également des audits de sécurité sur les plates-formes de jeux des opérateurs. Ces analyses permettront de mesurer la pertinence et la technicité des audits réalisés dans le cadre de la certification, ou initialement dans le cadre de l'agrément.

* * *

En référence du point 5.2 du DET, en tant que fournisseur de logiciel, pouvons-nous fournir le code source sur un DVD encrypté / chiffré avec un md5 hash des fichiers? A chaque fois que l'ARJEL aura besoin d'accéder au code source nous vous enverrons un employé pour déverrouiller l'accès au code et superviser la revue du code. Nous sommes concernés qu'au moment de sa demande d'agrément l'opérateur doit vous faire part du code source de la plateforme de poker et aura besoin de notre code source pour cela faire. Quelles sont nos options?

Non. Les codes sources doivent être transmis sur supports chiffrés à l'ARJEL à partir de certificats transmis par cette dernière. Les tests menés par l'ARJEL ne se feront pas sous présence d'un représentant de l'éditeur.

* * *

Le code applicatif évolue souvent : retouches cosmétiques, améliorations, évolutions majeures, correction de bogues et de vulnérabilités. Faut-il systématiquement signaler ces modifications à l'ARJEL ? Dans quel délai ?

Oui, toute modification du code doit être signalée à l'ARJEL, étant entendu que ces modifications doivent respecter le cadre légal et réglementaire. Les différentes évolutions doivent ainsi notamment être signalées dans le cadre des données de supervision et des mises à jour du dossier de définition. Par contre, une modification majeure, une modification urgente pour faire face à une nouvelle vulnérabilité, et plus généralement toute modification substantielle, doivent être portées à la connaissance de l'ARJEL sans délai.

DET Partie 5.4

Deux questions apparentées donnant lieu à une réponse commune :

1/ Quand sera disponible la liste des organisations de certification ?

2/ Certification : l'article 17 du projet de loi impose à l'opérateur de jeu diverses obligations de certification, celles-ci devant être réalisées par un organisme indépendant choisi par l'opérateur au sein d'une liste déterminé par l'ARJEL. Pouvez-vous nous communiquer cette liste ?

La liste des organismes retenus pour les certifications (à 6 mois et annuelle) sera précisée ultérieurement et dans un délai compatible avec l'exécution de la certification à 6 mois.

DET Partie 5.7.1.

Pourquoi est-il demandé de produire un CCTP ? (il s'agit d'un document qui est spécifique aux marchés publics) ?

Un CCTP est effectivement un document plus spécifique aux marchés publics. L'ARJEL souhaite ainsi disposer d'extraits de documents contractuels liant l'opérateur à ses prestataires concernés par le pilotage du système d'information que ce document contractuel soit appelé CCTP ou autrement.

DET Partie 5.7.3

Au chapitre 5.7.3, il est demandé de synchroniser les plates-formes sur une source de temps fiable. L'ARJEL émet-elle une préconisation sur le choix de la source ?

Par source de temps fiable, on entend une synchronisation des horloges via un ou plusieurs serveurs NTP de strate 1, qui s'appuient sur des signaux GPS ou encore DCF 77 (par exemple).

Au chapitre 5 des exigences techniques, les éléments en [P] sont des précisions à apporter. Pour la disponibilité, il semble qu'il faille démontrer les moyens mis en oeuvre pour la continuité de la plate forme de jeux globalement et non pas seulement de la fonction de traçage vis à vis de la plate forme. Est-ce exact ?

Les exigences de sécurité portent effectivement sur l'ensemble de la plate-forme, et pas uniquement sur le composant frontal. Elles permettent d'estimer le niveau de maturité de l'opérateur en termes de sécurité des systèmes d'information.

Remarque : en termes de précision [P], la fourniture des SLA (ou "contrats de niveau de service") constituera une réponse partielle au volet concernant la gestion de la disponibilité. Une description technique des mécanismes de protection réseau mis en oeuvre est attendue, afin de mesurer si les attaques par déni de service (distribuées ou non) sont prises en compte de façon effective dans les risques d'atteinte à la continuité de service.

DET Partie 5.7.3.m

Est-il nécessaire d'avoir deux unités de climatisation dans chaque salle de serveur ?

Le dossier des exigences techniques prévoit : "un système de climatisations redondantes et indépendantes par salle". La solution technique retenue doit permettre la continuité du service attendu.

Comment les opérateurs pourront-ils informer l'ARJEL des changements apportés à des configurations (pare feu, règle de filtrage, DNS, etc), de les en informer à chaque changement, et d'en obtenir l'autorisation au moins 2 mois au préalable ? Ne serait-il pas plus raisonnable d'en informer l'ARJEL une fois par an ?

Un dossier technique référençant l'ensemble des configurations techniques de la plate-forme devra être maintenu à jour. Ce dossier est introduit dans la partie 5.7.3.a "Description générale des systèmes d'information" sous la dénomination de "dossier de définition".

Ce dossier pourra être mis à disposition des prestataires en charge de la certification, au cours des opérations d'audit planifiées, ou encore des auditeurs du département évaluation et contrôle de l'ARJEL, à l'occasion des opérations d'audit techniques ponctuels ou encore des demandes d'information inopinées qui seront émises.

**QUESTIONS RELATIVES À L'ANNEXE AU
DOSSIER DES EXIGENCES TECHNIQUES**

Questions générales relatives à l'Annexe au Dossier des Exigences Techniques :

Voici une question sur les XML de session: doit-on avoir un XML de session par session utilisateur ou par intervalle de temps sur l'intégralité des connexions clients ?

Les lots d'évènements ne sont pas liés aux sessions des utilisateurs, mais portent sur l'intégralité des connexions des clients, sur un intervalle de temps donné.

* * *

Le chiffre '.' est interdite dans le XSD mais l'exemple au contraire «greg.dupont@monmail.tld » et « SuperJeu.fr » Exemple: ... SuperJeu.fr 091015144800 1987501 greg.dupont@monmail.tld ... Common.xsd – « fr »

La classe de caractères "fr" a été étendue, afin d'accepter le caractère "." et des caractères de ponctuation susceptibles d'apparaître dans les différents libellés des évènements. Cette modification fera l'objet d'une mise à jour de la page dédiée aux ressources techniques, notamment au niveau des définitions du schéma XSD.

* * *

<xs:element minOccurs="5" maxOccurs="5" ref="TabCarte" />

Vous spécifié: minOccurs="5", mais un fin est possible avec 0 (Acune flop), 3 (Seulement flop), 4 (Flop et River) ou 5 (Flop et Turn et River)

Je propose:

<xs:element minOccurs="0" maxOccurs="5" ref="TabCarte" />

Cette modification sera prise en compte dans les prochaines versions des schémas qui seront publiées.

* * *

On a du vous le dire déjà cent fois mais il manque le '.' dans la regexp ('\.') de simpleType « fr » pour que IDOper qui est string-32 elle même fr admette votre exemple « SuperJeu.fr »

La classe des caractères autorisés sera modifiée afin de notamment prendre en compte ce besoin.

* * *

Comme souvent les apostrophe sont problématiques : dans votre xml exemple Accessrefuse-07.xml l'apostrophe n'est pas la même que celle employée dans la regexp... '!= ' On peut admettre les deux ou seulement celle de la regexp ?

Oui. La classe des caractères autorisés sera modifiée afin de notamment prendre en compte ce besoin.

* * *

Dans les xsd fournis dans le projet de ressources techniques, il est indiqué que les emails doivent être de type string-64. Or ce type refuse le caractère « point ». Nous en déduisons qu'il serait nécessaire de faire évoluer les xsd sur ce point. Notre compréhension est-elle correcte ?

Oui. La classe des caractères autorisés sera modifiée afin de notamment prendre en compte ce besoin.

Annexe DET Partie 1

La définition d'un « évènement » conformément à la procédure définie par l'ARJEL peut-elle être clarifiée (notamment la raison pour laquelle chaque évènement doit recevoir un numéro unique généré par le coffre-fort)

La notion de numéro unique, dont l'enregistrement doit être séquentiel et continu, est introduite à des fins d'identification des évènements au sein d'un coffre (sans ambiguïté, comme avec la date par exemple), de synchronisation entre l'opérateur et l'ARJEL lors du téléchargement des traces.

Pouvons-nous changer les XML messages ?

Non. Sauf indication contraire indiquée dans les annexes, les enregistrements XML sont à reprendre strictement selon le format défini.

Annexe DET Partie 1.1.3

Question (en 2 parties) :

Enregistrement de trace sous réserve de confirmation du joueur : il est dit que « Du point de vue technique, la trace ne doit être enregistrée que lorsque le frontal reçoit une forme de confirmation de lecture par le joueur » qu'est-il entendu par « forme de confirmation » : est-ce qu'un cookie montrant que la page s'est bien affichée sur l'ordinateur du joueur suffirait, ou faut-il un acquiescement explicite de la part du joueur (click) ?

Dans le même esprit, il est dit au même endroit que pour le poker, « en fin de partie : que le joueur soit resté actif ou pas, le système doit afficher au joueur le résultat de la partie avec précision du montant de son gain ou de sa perte, avec obligation pour le joueur d'accuser réception de cette information; c'est à ce moment que l'enregistrement final est déclenché. » Si l'on parle d'enregistrement final, c'est qu'il y a un enregistrement provisoire : qu'en est-il de cet enregistrement provisoire et que fait-on si le joueur n'accuse pas réception de son gain ou sa perte ?

Réponse (en 2 parties) :

Pour qu'une trace soit enregistrée lorsque l'opérateur transmet au joueur une information, il faut qu'il y ait un acquiescement explicite de la part du joueur qui l'exprime en effectuant une action.

On entend par enregistrement final l'enregistrement de "Conclusion de la partie" comme décrit au paragraphe 1.3.5.1. Cet enregistrement ne se fait que si le joueur accuse réception du résultat. Le joueur ne peut passer à la partie suivante que s'il accuse réception du résultat de la dernière partie à laquelle il a participé. Il n'y a donc pas d'enregistrement provisoire.

* * *

Conformément à la section 1.1.3 de l'annexe technique, l'opérateur doit immédiatement sauvegarder toutes les transactions sur le serveur frontal. Cette obligation ne va pas sans présenter de sérieux risques pour la sécurité si les transactions sont sauvegardées immédiatement, soit avant la fin de la main. Cette approche était précisément à l'origine de la fameuse défaillance

des supers utilisateurs d'Absolute Poker & Ultimate Bet. Certains opérateurs pensent que le risque sécuritaire pour l'intégrité des opérations de poker est avéré, y compris dans l'hypothèse où les plus grandes précautions seraient prises. Dans ces conditions, serait-il envisageable de prévoir que les transactions seront enregistrées à la fin de chaque main seulement par opposition à immédiatement?

L'annexe au DET va être modifiée afin de permettre l'enregistrement à la fin de chaque main.

* * *

Dans le cadre de la nécessaire confirmation par le joueur, qu'en est-il d'un joueur ayant perdu au poker et s'étant déconnecté sans confirmation et ne se reconnectant jamais ? Qu'advient-il de sa perte (non confirmée donc non enregistrée pour le site) alors que le gagnant devra être payé par le site ?

*La perte du joueur qui se déconnecte et ne se reconnecte jamais n'est en effet pas enregistrée dans le frontal en tant qu'évènement vu par ce joueur là.
Elle est en revanche enregistrée en tant qu'évènement vu par les autres joueurs de la main, notamment celui qui a gagné, qui eux peuvent confirmer.
La somme perdue par le joueur déconnecté doit donc bien lui être retirée et le joueur gagnant devra être payé.*

Annexe DET Partie 1.3.4.a

Vous trouverez ci-après une question ayant trait aux documents que vous avez bien voulu mettre en ligne.

« Dans le message PASPMISE pare exemple, quelle donnée doit être mentionnée dans le segment « Code technique du pari » TECH : Est-ce l'identifiant du pari tel que géré par l'opérateur (et commun à tous les joueurs) ou celui que l'opérateur attribue à la prise de pari d'un joueur donné (et donc spécifique a chaque joueur) ?

Le code technique du pari est bien l'identifiant du pari tel que géré par l'opérateur et commun à tous les joueurs pariant sur la même combinatoire d'évènements.

Annexe DET Partie 1.2

Identifiant d'évènements : notre solution de coffre-fort génère un identifiant unique et incrémental préfixé (préfixe + année + incrément ex: 1112010000000001), Chaque année, la partie incrément est remise à 0, est-ce conforme ?

Des identifiants croissants, et contiguës sur une même année, sont conformes aux exigences.

Remarque : le format des évènements sera prochainement modifié, afin que figure un identifiant de coffre dans les entêtes de l'évènement. Cet entête sera fixé par le coffre lui-même. Cette modification sera documentée dans les prochaines versions du DET et de l'annexe au DET.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

* * *

Identifiant d'évènements : nous n'envisageons pas de modifier le contenu de la transaction délivrée par le capteur. Ceci pour garantir l'intégrité des données fournies au coffre-fort. Cet identifiant sera associé à la transaction, est-ce conforme au fait que c'est le coffre-fort qui fixe cet identifiant d'évènement?

Le projet de dossier des exigences techniques suggérait que cet identifiant d'évènement soit fixé par le coffre, afin d'éviter un échange préliminaire entre capteur et coffre, avec des risques d'accès concurrents dans des configurations multi-capteurs et multi-coffres.

Si cette transaction n'est pas jugée pénalisante en termes de délai de traitement de la requête, et que son implantation permet de respecter le séquençement incrémental des évènements au niveau d'un même coffre, elle est a priori conforme aux exigences techniques.

* * *

Identifiant d'évènements : le coffre-fort fixant l'identifiant, doit-il également fixer la date permettant d'effectuer des extractions?

Oui.

Annexe DET Partie 1.3

Les messages portent tous le même nom, « Evt », ils sont non typés, or ces messages n'ont pas du tout la même signature, peut on avoir des messages typés, ex :

<xs:element name="EvtLOTNATURE"/>

<xs:element name="EvtCLOTUREDEM"/>

<xs:element name="EvtXXXXXX"/>

Ceci permettrait d'automatiser plus simplement la validation des messages et d'éviter les erreurs de format.

Ce typage sera proposé dans la prochaine version du dossier des exigences techniques.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

* * *

Les mêmes énumérations sont redéfinies dans chaque définition de message, ne peut on pas avoir une seule énumération comprenant toutes les valeurs possibles qui seraient dans le fichier common.xsd ? la validité de la valeur de l'enum serait en fonction d'une facet définie dans le xsd du message, les définitions seraient donc factorisées et les restrictions faites pour chaque type de message.

Exemple pour l'événement « Accès refusé » typage de message plus factorisation de l'énumération evenement :

```

<xs:element name="EvtACCESREFUSE">
  <xs:complexType>
    <xs:sequence minOccurs="1" maxOccurs="1">

      <!-- Entete -->
      <xs:element minOccurs="1" maxOccurs="1" ref="IDOper"/>
      <xs:element minOccurs="1" maxOccurs="1" ref="DateEvt"/>
      <xs:element minOccurs="1" maxOccurs="1" ref="IDEvt"/>
      <xs:element minOccurs="1" maxOccurs="1" ref="Login"/>
      <xs:element minOccurs="1" maxOccurs="1" ref="Pseudo"/>
      <xs:element minOccurs="1" maxOccurs="1" ref="IPJoueur"/>
      <xs:element minOccurs="1" maxOccurs="1" ref="IDSession"/>
      <xs:element minOccurs="1" maxOccurs="1" ref="FamEvt"/>

      <!-- /Entete -->

      <!-- ACCESREFUSE -->
      <xs:element minOccurs="1" maxOccurs="1" ref="CauseRefus"/>
      <!-- /ACCESREFUSE -->

    </xs:sequence>
  </xs:complexType>
</xs:element>

<xs:element name="FamEvt" type="evenementACCESREFUSE"/>
<!-- Inclut dans chaque definition de message pour restreindre la valeur possible pour
ce type de message-->
<xs:simpleType name="evenementACCESREFUSE">
  <xs:restriction base="evenement">
    <xs:enumeration value="CJ"/>
  </xs:restriction>
</xs:simpleType>

<!--Devrait être definit une seule fois dans le common.xsd -->
<xs:simpleType name="evenement">
  <xs:restriction base="xs:string">
    <xs:enumeration value="CJ"/>
    <xs:enumeration value="EJ"/>
  </xs:restriction>
</xs:simpleType>

```

Cette modification sera proposée dans la prochaine version du dossier des exigences techniques.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

Annexe DET Partie 1.3.3.a

Deux questions apparentées donnant lieu à une réponse commune :

1/ Processus d'inscription en ligne : l'opérateur de jeu doit-il exiger obligatoirement du joueur qu'il communique sa date de naissance, sa ville et son pays de naissance, sexe, numéros de téléphone fixe ou mobile ? Certains de ces éléments sont-ils facultatifs ?

2/ Sont indiqués dans l'annexe du CDC, en information à envoyer à la création du compte joueur les numéros de téléphone fixe et mobile. Sont-elles obligatoires ou facultatives? Même question pour les départements et pays de naissance ?

Les numéros de téléphone sont facultatifs. Le département et le pays de naissance sont obligatoires. Par contre l'ensemble des champs doivent être demandés au joueur qui peut cependant ignorer les deux champs facultatifs.

* * *

La ville, le département et le pays de naissance font ils partie des informations obligatoires à collecter lors de l'inscription et à afficher dans le compte de joueur ?

Ces éléments sont obligatoires. Ils sont à collecter lors de l'inscription et à vérifier lors de la fourniture des pièces justificatives.

* * *

Sur un site offrant des jeux et paris autorisés par plusieurs agréments, le joueur doit il ouvrir un compte pour chaque jeux ou pari relevant d'un agrément ou peut il ouvrir un compte qui lui permet de jouer à tous les jeux et paris objet des différents agréments ?

Pour un site offrant des jeux et paris associés à différents agréments, il est possible, pour un joueur, de n'ouvrir qu'un seul compte joueur pour l'ensemble des jeux et paris proposés. Les éléments demandés dans la partie 1.3.2.a de l'annexe au DET (notamment concernant les bonus) devront être respectés.

* * *

Tous les champs sont ils obligatoires ? Quel est l'intérêt d'ajouter à la ville de naissance, le département et le pays ? Idem pour le téléphone fixe, le mobile et l'adresse e-mail ?

Tous les champs sont obligatoires sauf les champs téléphones fixe et mobile qui sont facultatifs. Par contre l'ensemble de ces champs sont à demander au joueur, les deux cités précédemment pouvant être ignorés par ce dernier.

* * *

Les champs suivants sur l'inscription, semblent obligatoires : Genre Ville de la naissance Département de la naissance Pays de la naissance Numéro de téléphone fixe et mobile Carte d'identité nationale ou # de passeport ou # du permis de conduire Compte bancaire pour les retraits. D'après les FAQ, tous les champs sont obligatoires, à l'exception du numéro de téléphone fixe et du mobile. Tous les champs doivent être posés au joueur ; cependant les numéros de téléphone mobile et fixe peuvent être ignorés par le joueur. Dans notre système le numéro de téléphone fixe est aussi obligatoire. Ceci pourrait-il être appliqué aux clients français aussi?

Oui. Le format XML présenté page 10 correspond aux informations demandés par l'ARJEL. Si l'opérateur souhaite demander aux joueurs d'autres informations, il peut le faire. ces éléments ne seront tout simplement pas pris en compte lors de la création des enregistrements XML.

Remarque importante : Les enregistrements XML n'ont pas à refléter de façon bijective les éléments pris en compte par la plateforme de jeux.

* * *

Veillez confirmer si nous devons ajouter ces 3 paramètres à notre système : pays, ville et département de naissance. En outre, xml a pour l'ouverture de compte une Session ID comme paramètre. Nous créons une session après la connexion, et la connexion se produit après l'enregistrement. Cela signifie que lors d'une inscription nous n'avons pas de Session ID.

Oui, ces trois paramètres doivent être renseignés, de préférence en respectant les codes officiels géographiques fournis par l'INSEE et disponible à l'adresse <http://www.insee.fr/fr/methodes/nomenclatures/cog/telechargement.asp>.

* * *

Propriété DptN (département) est répertorié comme obligatoire et nous n'avons pas cela dans notre système. Peut-être CountyOrStateOrProvince (Pays, ville ou région) peut être utilisé. ?

Le lieu de naissance fera partie des éléments discriminants pour la consultation des interdits de jeu.

Le département est donc une donnée nécessaire afin de lever une éventuellement ambiguïté sur la ville de naissance.

* * *

Annexe DET Partie 1.3.3.i

Les bonus attribués dans le cadre d'un jeu ou d'un pari autorisé dans le cadre d'un agrément spécifique, peuvent-ils être utilisés par le joueur dans le cadre d'un autre jeu ou pari relevant d'un autre agrément dont est titulaire le même opérateur, sous réserve qu'on assure leur traçabilité notamment dans le cadre du calcul de l'assiette des prélèvements et du calcul du TRJ maximum moyen ?

Les bonus alloués pour une catégorie de jeux spécifique sont exclusivement utilisés pour cette catégorie. Les bonus présentant un caractère générique peuvent recevoir toute destination. Le calcul du taux de retour au joueur (TRJ) est réalisé en prenant en compte la part de bonus générique utilisée par catégorie de jeux.

* * *

Alimentation/retrait sur le compte joueur Les types de bonus autorisés sont précisément décrits : crédit de jeu offert, mise apportée par l'opérateur, gain apporté par l'opérateur. Ces contraintes sont-elles facultatives ou obligatoires ?

Les événements liés au compte joueur et plus spécifiquement ceux liés aux aspects financiers (1.3.3.i de l'annexe au DET) sont obligatoires.

L'opérateur n'a pas l'obligation de faire appel à tous ces enregistrements, mais les mouvements financiers qu'il prend en compte doivent s'inscrire dans ceux autorisés.

* * *

D'après les échantillons xml le client peut définir des limites pour des types de paris spécifiques, pour les paris sportifs (en surbrillance ci- dessous). Est-il nécessaire d'avoir des limites par type de pari ?

Oui.

Annexe DET Partie 1.3.4.a – Mise par un joueur sur un pari

A quoi sert de fournir le « Solde du compte avant la prise de pari » sachant qu'il se déduit des autres valeurs par ailleurs ? De plus ceci pose un problème de faisabilité technique lorsque plusieurs moteurs de jeu sont intégrés autour d'un unique porte-monnaie. Est-il possible de considérer ce champ comme facultatif ou de le supprimer des exigences ?

Fournir le « solde du compte avant la prise de pari » (et autres informations) permet une bonne information du joueur et facilite la prise de décisions éclairées. Si plusieurs moteurs de jeu sont intégrés autour d'un unique compte, le solde doit être convenablement géré au risque de dépasser la capacité du compte joueur. Ce champ n'est donc pas facultatif.

Cette question concerne la section 1.3.4.a (« Mise par un joueur sur un pari »). Il nous semble que la balise <Type> identifiant le Type de pari devrait se situer à un niveau plus bas de la hiérarchie XML (à savoir sous la balise <Pari>). En effet, dans les types de combinatoire « Combiné » ou « Multiple » un joueur doit pouvoir combiner des paris de types différents au sein d'une même prise de jeu. Si l'on se réfère à l'exemple de Pari Combiné présenté page 44 comment aurait-on du structurer un pari combiné sur Nice/Lyon en 1N2 et sur Paris SG Bordeaux en Résultat exact ?

En effet, la configuration actuelle trop rigide de la structure XML, ne permet de combiner des paris de type différent.

Le champ relatif au type de pari « Type » sera donc placé plus bas au niveau du sous-groupe « Lig » mais cependant pas au niveau du sous-groupe « pari » comme vous le proposez.

La réponse à cette question va provoquer une modification de l'annexe au DET dans le § 1.3.4.a où le champ « Type » sera déplacé au niveau du sous-groupe « lig ».

Les exemples de la partie 1.4.2 seront modifiés de la même façon ainsi que les ressources techniques.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

Deux questions apparentées donnant lieu à une réponse commune :

1/ Dans les annexes du Dossier des Exigences Techniques, p.20 il est établi une distinction entre pari multiple et pari combiné. Quelle est-elle ?

2/ Est-il possible d'explicitier, à la page 45, l'exemple de paris multiple sur 3 matchs/Terminologie utilisée pour le type de combinatoire « Multiple » ? Habituellement, la combinatoire multiple X/Y est interprétée comme suit :

- Y : Nombre de pronostics effectués par le joueur dans sa prise de jeu (et non le nombre de combinaisons)

- X : Nombre de pronostics pris en compte dans chaque combinaison unitaire (le nombre total de combinaisons unitaires validées par le joueur étant alors égal à CxY)

Par exemple, pour un multiple 2/3 si le joueur a choisi les pronostics A, B et C sur 3 paris différents, les 3 combinaisons unitaires suivantes seront considérées pour déterminer un éventuel gain : AB -> Gain potentiel : Mise unitaire x Cote pronostic A x Cote pronostic B BC -> Gain potentiel : Mise unitaire x Cote pronostic B x Cote pronostic C AC -> Gain potentiel : Mise unitaire x Cote pronostic A x Cote pronostic C Dans cet exemple, cela revient à valider en une fois l'équivalent de 3 paris combinés indépendants.

Dans le cas d'un pari Multiple 2/3 tel que défini ci-dessus, nous transmettrions le type de combinatoire précis dans le descriptif de la prise de jeu (balise <Clair>) et les cotes associées aux pronostics choisis par le joueur (cf exemple dans la pièce jointe ci-dessous). Cette approche est-elle correcte ? Sélectionner plusieurs pronostics d'un même pari reviendrait à valider plusieurs paris simples indépendants au niveau du calcul des gains. Le flux XML présenté page 45 aurait donc été envoyé lors de la validation par le joueur de 6 paris simples indépendants (en précisant le code S dans la balise indiquant le type de combinatoire (<Combi>S</Combi>)) et non lors de la validation d'un pari multiple.

Dans la partie 1.3.4.a de l'annexe au DET, nous définissons trois types courants de paris :

- *le pari simple consiste à pronostiquer un résultat concernant un match; le pari est gagnant si le résultat pronostiqué correspond au résultat une fois le résultat officiel du match annoncé ;*
- *le pari combiné consiste à pronostiquer un résultat pour une série de n matchs, chaque match recevant un pronostic élémentaire. Le pari est gagnant lorsque le pronostic global correspond aux résultats en fin de matchs, c'est à dire que tous les pronostics élémentaires sont bons.*
- *le pari X sur Y consiste à pronostiquer Y résultats élémentaires portant sur Y matchs. Le pari est gagnant lorsqu'au moins X des Y pronostics élémentaires sont bons. Le pari X sur Y consiste ainsi à effectuer plusieurs combinaisons dans un pari.*

Par ailleurs, la notion de multiple peut être associée à un pari simple, un pari combiné ou un pari X sur Y. L'extension multiple permet d'effectuer plusieurs pronostics pour un même match. Par exemple pour un pari simple multiple en IN2, le joueur cochera 1 et N. Dans l'enregistrement XML correspondant, le champ « pari » sera donc multiple.

Cette liste de types de pari n'est pas restrictive, si nécessaire d'autres types de pari peuvent être ajoutés selon la procédure explicitée dans la partie 1.3.4, sous réserve que ces types de paris figurent sur la liste édictée par l'ARJEL pour la discipline sportive concernée.

Dans la partie 1.3.4.a de l'annexe au DET, l'enregistrement correspondant aux paris sportifs sera donc modifié :

- *en remplaçant dans le champ « type combinatoire » S ou M ou C par S ou C ou XY, le caractère multiple se déduisant du groupe « pari » qui pourra être multiple;*
- *lorsque le type de combinatoire XY est sélectionné. Un champ X sera ajouté au groupe <Desc>. Le champ Y représente le nombre de pronostics élémentaires effectués par le joueur dans son pari (donc de ligne) et le champ X représente le nombre minimum de pronostics gagnants nécessaires pour remporter le pari.*

Les éléments suivants du DET et de l'Annexe au DET seront donc modifiés afin de correspondre aux éléments portés ci-dessus:

§ 1.3.4.a de l'annexe au DET sur la structure des paris sportifs

§ 1.4.2.a de l'annexe au DET portant sur les exemples d'enregistrement XML

Les ressources techniques associées.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

* * *

Mise par un joueur sur un pari – Page 20 Concernant un pari sportif, faut-il enregistrer la cote présentée au joueur au moment où il a effectué son pari ? Faut-il prévoir un rafraîchissement régulier de la cote sur l'écran du joueur ? S'agissant d'une cote mutuelle, doit-on enregistrer la cote juste avant ou celle juste après ?

La cote apparaissant dans l'enregistrement XML "PASPMISE", correspond à la cote d'un pronostic effectué par un joueur sur une rencontre qu'il a sélectionnée. Un rafraîchissement peut être possible sur l'écran du joueur mais la cote inscrite dans l'enregistrement XML doit correspondre à la cote affichée sur l'écran du joueur au moment où il valide son pari.

* * *

Y a-t-il un format spécifique requis pour le code technique du pari (ENUM, etc...) ? Ou alors, peut-on utiliser notre mécanisme de code actuel ?

Aucun format n'est requis. L'opérateur peut utiliser ses propres conventions de nommage.

* * *

L'attribut <type>au niveau du pari se réfère effectivement au type de marché dans notre système. Il y a quelques questions à propos de cet attribut. Pour un prix identique parier le xml signifie : <Type>1N2</Type> Pour le score exact : <Type>Score</Type> 1. Devons nous faire correspondre tous nos types de paris à ces types ? Nous avons un grand nombre d'entre eux. Pourrions-nous utiliser éventuellement notre nom de pari comme valeur de cette base xml ? C'est-à-dire <type>Prix Match</type> <type>Score exact</type> ou <type>Over/Under 2.5</type>... En outre, dans notre système nous n'avons pas la contrainte que pour plusieurs paris le client doit choisir les sélections du même type de marque. C'est-à-dire il peut combiner correspondent au prix sélection (par exemple Arsenal) d'un match de football avec une sélection de Score exact (c'est-à-dire 2-1) d'un autre match. 2. Ce xml peut-il être modifié? Une option consiste à mettre des balises xml <type> au sein de la balise xml de <lig> (cf mail).

1/ La balise Type est un champ libre, il peut contenir n'importe quel type de pari préalablement validé par l'ARJEL. Vous pouvez donc utiliser le nom de vos types de paris comme valeur de cette balise sous réserve de les avoir déclarés et fait valider en amont auprès de l'ARJEL.

2/ Le champ relatif au type de pari « Type » sera placé plus bas au niveau du sous-groupe "Lig".

La réponse à cette question va provoquer une modification de l'annexe au DET dans le § 1.3.4.a où le champ "Type" sera déplacé au niveau du sous-groupe "lig".

Les exemples de la partie 1.4.2 seront modifiés de la même façon ainsi que les ressources techniques.

* * *

Le cahier des charges Arjel semble ne pas intégrer la possibilité de paris « combinés ». Faut-il par conséquent se cantonner à des paris de même typologie sur chaque ticket ?

Les paris "combinés" en tant que paris portant sur des types d'agréments différents ne peuvent effectivement pas être pris en compte.

Les paris sportifs combinés portant sur plusieurs rencontres sont autorisés.

* * *

Dans les annexes du Dossier des Exigences Techniques, p.20 il est établi une distinction entre pari multiple et pari combiné. Quelle est- elle ?

Dans la partie 1.3.4.a de l'annexe au DET, nous définissons trois types de paris :

- *le pari simple consiste à pronostiquer un résultat concernant un match; le pari est gagnant si le résultat pronostiqué correspond au résultat annoncé par l'organisateur de la compétition sportive ;*
- *le pari combiné consiste à pronostiquer un résultat pour une série de n matchs, chaque match recevant un pronostic élémentaire. Le pari est gagnant lorsque le pronostic global correspond aux résultats annoncé par l'organisateur de la compétition sportive, c'est à dire que tous les pronostics élémentaires sont bons.*
- *le pari X sur Y consiste à pronostiquer Y résultats élémentaires portant sur Y matchs, c'est-à-dire correspondant aux résultats annoncés par l'organisateur de la compétition sportive. Le pari est gagnant lorsqu'au moins X des Y pronostics élémentaires sont bons. Le pari X sur Y consiste ainsi à effectuer plusieurs combinaisons dans un pari.*

Par ailleurs, la notion de multiple peut être associée à un pari simple, un pari combiné ou un pari X sur Y. L'extension multiple permet d'effectuer plusieurs pronostics pour un même match. Par exemple pour un pari simple multiple en IN2, le joueur cochera 1 et N. Dans l'enregistrement XML correspondant, le champ « pari » sera donc multiple.

Cette liste de types de pari n'est pas restrictive, si nécessaire d'autres types de pari peuvent être ajoutés selon la procédure explicitée dans la partie 1.3.4, sous réserve que ces types de paris soient autorisés en vertu de la liste édictée par l'ARJEL pour la discipline sportive concernée.

Dans la partie 1.3.4.a de l'annexe au DET, l'enregistrement correspondant aux paris sportifs sera donc modifié :

- *en remplaçant dans le champ « type combinatoire » S ou M ou C par S ou C ou XY, le caractère multiple se déduisant du groupe « pari » qui pourra être multiple;*
- *lorsque le type de combinatoire XY est sélectionné. Un champ X sera ajouté au groupe <Desc>. Le champ Y représente le nombre de pronostics élémentaires effectués par le joueur dans son pari (donc de ligne) et le champ X représente le nombre minimum de pronostics gagnants nécessaires pour remporter le pari.*

Les éléments suivants du DET et de l'Annexe au DET seront donc modifiés afin de correspondre aux éléments portés ci-dessus:

§ 1.3.4.a de l'annexe au DET sur la structure des paris sportifs

§ 1.4.2.a de l'annexe au DET portant sur les exemples d'enregistrement XML

Les ressources techniques associées.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

Annexe DET Partie 1.3.4.b

Gain pour un joueur sur un pari : Page 23 Je comprends que dans notre cas de paris mutualisés, nous devons pour chaque pari qu'il a effectué indiquer au joueur, le montant de la masse des enjeux sur ce pari : au global ou choix par choix ?

L'enregistrement de la page 23 vise à décrire le gain et non des informations relatives aux enjeux.

Annexe DET Partie 1.3.4.c

Annulation d'une prise de pari : Page 24 Je comprends qu'en cas d'annulation d'un événement, tous les joueurs doivent acquitter cette information. Pour cette opération et pour les gains, l'acquiescement par le joueur est-il obligatoire avant qu'il puisse effectuer toute opération sur le site (nouveau site, action sur le compte...) ? Que se passe-t-il pour les opérations que le joueur n'a jamais acquittées ? L'acquiescement peut-il être pour le joueur global : on lui présente une liste de gains et il acquiesce ou doit-il acquiescer chaque opération individuellement?

Oui, il est demandé que le joueur acquiesce une action avant de pouvoir poursuivre sa navigation sur le site. L'acquiescement du joueur peut être commun à plusieurs gains, en termes d'interface. En revanche, autant d'événements qu'il y aura de gains devront être générés par le capteur et enregistrés au niveau du coffre.

Annexe DET partie 1.3.5.

Dans le cadre de la nécessaire confirmation par le joueur, qu'en est-il d'un joueur ayant perdu au poker et s'étant déconnecté sans confirmation ? Qu'advient-il de sa perte (non confirmée donc non enregistrée pour le site) alors que le gagnant devra être payé par le site ?

Quand un joueur de poker se déconnecte sans confirmation : on enregistre la transaction correspondant au dernier tour auquel il a participé.

L'enregistrement "Conclusion de la partie" n'est stocké dans le coffre que si le joueur valide le résultat. Le site, dans le sens système d'information de l'opérateur, doit en revanche stocker toutes les informations dont il a besoin pour le bon déroulement du jeu. Le gagnant doit donc être payé par le site et l'enregistrement de son gain doit lui être affiché pour confirmation.

Le joueur qui a été déconnecté peut toujours reprendre le jeu quelques parties plus tard en confirmant le résultat de la partie de laquelle il a été déconnecté.

* * *

La section 1.3.5 des exigences techniques évoque « Le partage des joueurs entre plusieurs opérateurs » et précise « Les données sont archivées sur le frontal de l'opérateur qui gère le compte du joueur ».....dans ces conditions peut-il y avoir un partage des joueurs entre des opérateurs étrangers et Français ?

Conformément à l'article 9 du projet de loi relatif à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, il ne pourra pas y avoir de partage de joueurs entre opérateurs non agréés en France et opérateurs agréés en France. Des opérateurs étrangers ayant obtenu leur agrément en France pourront en revanche partager leurs joueurs avec d'autres opérateurs agréés en France (français ou non).

Annexe DET Partie 1.4.2

Cette question concerne la section 1.4.2.a page 42 dans l'exemple de pari simple. Dans le cadre de notre offre, si un joueur effectue 3 paris simples de façon groupée il ne doit renseigner qu'une seule mise unitaire qui sera appliquée à chacun des paris. Une seule prise de jeu est dans ce cas envoyée à nos serveurs et il ne sera pas possible de générer trois enregistrements différents au niveau du coffre fort car cela reviendrait à modifier la logique transactionnelle. Par contre, la fourniture de la mise totale et la connaissance du nombre de paris dans l'enregistrement permettront de remonter aisément à la mise unitaire. Cette approche est-elle acceptable ?

Oui cette approche est acceptable. L'enregistrement correspondant devra bien être spécifié comme un pari simple (champ « combi » égal à « S ») et contenir plusieurs sous-groupes « ligne » correspondant à chaque pari simple. Le montant renseigné dans le champ « Mise » devra représenter la mise totale du pari effectué par le joueur. Dans ce format, la mise de chacun des paris simples est nécessairement égale au montant de la mise totale divisée par le nombre de paris simples.

* * *

Le calcul du gain d'un joueur pour un pari combiné s'effectue habituellement en faisant le produit de sa mise par les différentes cotes qu'il a sélectionnées. Est-ce que, dans l'exemple donné page 50, le gain attribué au joueur ne serait-il pas de 38,7 euros (4 x 4,5 x 2,15) au lieu de 26,6 euros ?

Effectivement, l'exemple donné page 50 présente une erreur au niveau du gain attribué au joueur. Le montant est bien de 38,70 euros et non de 26,60 euros.

Attention : la réponse à cette question a entraîné une mise à jour du document mentionné (cf. avertissement spécifique en tête de document)

Annexe DET Partie 2

Dans les annexes du Dossier des Exigences Techniques, p.79 il est fait référence à des événements ? Quelle réalité le terme d'événement recouvre-t-il ?

Par « évènement » nous entendons - dans le contexte du projet d'annexe n°2 - une compétition sportive servant de support à un ou plusieurs paris. Ainsi, sous réserve que ces évènements fassent partie de la liste des compétitions sportives figurant sur la liste édictée par l'ARJEL, l'opérateur fournit chaque semaine à l'ARJEL les données relatives aux paris proposés.

* * *

Est-ce que les données agrégées devront être envoyées en parallèle avec les données en temps réel ?

*Les données enregistrées en temps réel seront récupérées par l'ARJEL (PULL) en temps différé.
Les données agrégées seront donc transmises (PUSH) indépendamment.*

* * *

Annexe 2 – Description des Données Transmises Systématiquement à l'ARJEL : compte tenu de l'ampleur des données à transmettre nous prévoyons une transmission csv ; est ce acceptable?

Oui.

* * *

Trois questions apparentées donnant lieu à une réponse commune :

Annexe DET Partie 2

1/ Données agrégées relatives à l'activité de l'opérateur-données relatives aux événements - combien de temps après la fin de la semaine écoulée ce rapport est-il dû ? Quid en cas de jour(s) férié(s) : le nombre de jours est-il à considérer en jours ouvrables?

2/ Données agrégées relatives aux opérations de jeux ou paris réalisés par les joueurs : combien de temps après la fin du mois ce rapport est-il dû? Quid en cas de jour(s) férié(s) : le nombre de jours est-il à considérer en jours ouvrables?

3/ Données agrégées relatives aux contrôles menés par l'opérateur : combien de temps après la fin du mois ce rapport est-il dû? Quid en cas de jour(s) férié(s) : le nombre de jours est-il à considérer en jours ouvrables?

Conformément à l'Annexe 2 modifiée du DET, [mise en ligne le 12 mai 2010], dès le commencement de son activité d'offre de jeux ou de paris en ligne, l'opérateur transmet périodiquement à l'Autorité de régulation des jeux en ligne les données, exhaustives ou agrégées, portant sur ce qui suit, et selon les délais ci-après énoncés :

- ❖ *Recueil de données mensuel, à transmettre à l'ARJEL au plus tard le 15 du mois suivant :*
 - *Les opérations de compte réalisées par les joueurs (voir le détail dans l'Annexe 2 du DET);*
 - *Les offres commerciales comportant une gratification financière des joueurs et leur utilisation par ces derniers.*
 - *Le tirage des cartes réalisé par le générateur de nombres aléatoires pour l'organisation des jeux de cercle (voir le détail dans l'Annexe 2 du DET);*
 - *Les contrôles menés par ses soins et leurs résultats (voir le détail dans l'Annexe 2 du DET).*

- ❖ *Recueil de données hebdomadaire, à transmettre à l'ARJEL au plus tard le mercredi de la semaine suivante :*
 - *Les opérations de jeu réalisées par les joueurs ainsi que toute donnée concourant à la formation du solde du compte joueur (voir le détail dans l'Annexe 2 du DET);*
 - *Les profils des joueurs et leurs comportements de jeu (voir le détail dans l'Annexe 2 du DET);*
 - *Les différents éléments techniques (voir le détail dans l'Annexe 2 du DET).*

- ❖ *Le catalogue des jeux et paris proposés :*

Ce catalogue est transmis mensuellement, au plus tard, le 15 du mois précédant la mise en ligne des jeux et paris proposés. Dans le cas où, des modifications à la hausse du catalogue auraient lieu, la transmission d'éléments additionnels du catalogue peut s'effectuer jusqu'à 48 heures avant la mise en ligne des jeux et paris concernés.

* * *

Données agrégées relatives à l'activité de l'opérateur : catalogue des jeux et paris. Quid des modifications ultérieures éventuelles à la hausse ou à la baisse sur ce catalogue ?

Conformément à l'Annexe 2 modifiée du DET (voir notre mise en ligne du 12 mai 2010) :

"Ce catalogue est transmis mensuellement, au plus tard, le 15 du mois précédent la mise en ligne des jeux et paris proposés. Dans le cas où, des modifications à la hausse du catalogue auraient lieu, la transmission d'éléments additionnels du catalogue peut s'effectuer jusqu'à 48 heures avant la mise en ligne des jeux et paris concernés."

Les modifications à la baisse du catalogue ne doivent pas obligatoirement être communiquées à l'ARJEL.

* * *

Données agrégées relatives à l'activité de l'opérateur - catalogue des jeux et paris - liste des tournois de poker etc. : ce reporting est-il obligatoirement à fournir par l'opérateur ou peut-il être fourni directement et sans intervention de l'opérateur par le fournisseur du service en cas de sous-traitance de ce service?

Le recueil des données peut être réalisé par un prestataire de l'opérateur agréé à condition que ce prestataire respecte les obligations relatives aux sous-traitants.

Toutefois, seul l'opérateur agréé pourra transmettre à l'ARJEL les données agrégées dont la description figure en Annexe 2 du DET (voir notre mise en ligne de l'Annexe au DET du 12 mai 2010).

* * *

Dans les annexes du Dossier des Exigences Techniques, p.79, il est demandé des tris par origine géographique du joueur, quel est le critère retenu (adresse IP, adresse postale..) ?

Conformément aux termes de l'annexe 2 au DET, l'origine géographique du joueur s'entend "par pays et par département pour les résidents français".

* * *

Dans les annexes du Dossier des Exigences Techniques, p.79, quelle est la formule retenue pour calculer la durée de connexion ?

La durée de connexion correspond à la durée effective de présence du joueur sur le site. Cette durée est délimitée par l'authentification du joueur à son début, et par la clôture de sa session applicative, résultant soit d'une déconnexion volontaire, soit de l'expiration de sa session.

* * *

Dans les annexes du Dossier des Exigences Techniques, p.79, pour définir le nombre de joueurs faut-il considérer comme joueur sur la période celui qui a réalisé une action de pari ou de jeu sur la période, ou celui qui a des paris en cours par exemple ?

Pour chaque opération de jeu réalisée par joueur, les données agrégées devant être transmises correspondent à l'ensemble des paris clos et débouclés d'un élément du catalogue, que ce soit terminé ou non (voir Annexe 2 modifiée au DET mise en ligne le 12 mai 2010).

Annexe DET Partie 3.1.1

Est-il possible d'utiliser une fonction de « gestion de messages » pour transmettre les informations au coffre (simplifie la gestion du traitement des erreurs d'enregistrement au sein du coffre ainsi que la reprise (utilisation d'un *middleware* de type *MQ Series*).

Oui. Le protocole HTTPS était cité en exemple dans le dossier des exigences techniques. Il peut tout à fait être substitué par un autre protocole offrant un niveau de sécurité équivalent, a fortiori un middleware comme IBM MQSeries, dont le canal de communication (ou channel) supporte le protocole de sécurité standardisé SSL/TLS.

* * *

Dans l'annexe 3 du Projet d'annexe au DET, il est précisé qu'en cas de capteur intégré aux plates-formes de services, le périmètre de la certification s'étendra à ces serveurs. De quelle certification parle-t-on dans ce chapitre ? Annexe DET

Il s'agit de la certification telle que décrite dans l'article 17 du projet de Loi et non de la certification au sens CSPN.

* * *

Est-il possible pour le flux retour (plate-forme de jeux vers le joueur) de ne pas attendre l'acquittement du coffre fort pour relayer le flux au joueur ? :

- pour la portion de traitement visant à enregistrer l'information conservée dans le tampon du capteur au sein du coffre
- si le traitement de la transaction de jeux n'a pas généré d'erreurs.

Cela permet de limiter l'*overhead* lié aux traitements cryptographiques et d'enregistrement des informations tout en conservant principe de la rupture protocolaire dans le cas de l'utilisation d'un *proxy*. Cela permet également en cas d'erreur d'enregistrement des données au sein du coffre, de resoumettre le message conservé dans le tampon du capteur sans impacter la « qualité de service perçue » par le joueur (message conservé dans le tampon du coffre dans l'attente d'un acquittement du coffre).

Le capteur et le coffre doivent fonctionner de façon synchrone, mais l'écriture de l'évènement et son traitement cryptographique au sein du coffre peuvent être différés, dès lors que le capteur a bien reçu l'accusé de réception du coffre. Dans la situation décrite, la surcharge

induite par les traitements cryptographiques n'a donc pas lieu d'impacter la qualité de service perçue par le joueur. Dès lors, l'attente de l'acquiescement du coffre-fort est nécessaire et doit être intégrée au traitement de la requête comme tout autre processus métier dont la réussite conditionne celle de la transaction dans son ensemble.

* * *

Frontal : quelles sont les conséquences pour l'opérateur de jeu d'un incident dans l'opération de stockage ? L'opérateur de jeu devra-t-il interrompre les opérations de jeu en cours ? Annuler les paris déjà engagés ? Les participants souhaitent rappeler que n'ayant qu'un accès limité à la partie haute du « frontal », ils ne pourront pas effacer les données de jeu afférentes à ces opérations une fois stockées au sein de cette partie haute.

Un évènement échoué doit être, en amont, rejeté par le capteur, et non transmis au coffre : le coffre a pour fonction essentielle d'effectuer des traitements cryptographiques sur la file d'évènements qui lui est poussée. La logique réside au niveau du capteur et uniquement au niveau de celui-ci.

Les conséquences pour l'opérateur de jeu d'un incident dans l'opération de stockage doivent être traitées comme tout autre incident susceptible de se produire sur l'ensemble des éléments de sa plate-forme et pouvant conduire à un échec de la transaction.

* * *

Coffre-fort : l'annexe au DET suggère un lien HTTPS entre le capteur et le coffre-fort (voir par exemple schéma p84). Est-il possible d'utiliser un protocole de type Active MQ sur un lien IP sécurisé en SSL à la place ? Ce protocole permet une meilleure fiabilisation de l'envoi des messages (en particulier en gérant nativement l'accusé de réception et la journalisation des actions). Est-il possible d'avoir confirmation de la possibilité d'héberger plusieurs instances de coffre-fort sur une même infrastructure matériel, moyennant l'implémentation de mécanismes de cloisonnement stricts (ex : partitionnement du stockage et des traitements, utilisation de serveurs virtuels, utilisation de bi-clés différents par agrément) ?

Oui. Le protocole HTTPS est cité à titre d'exemple dans le dossier des exigences techniques. Il peut tout à fait être substitué par un autre protocole offrant un niveau de sécurité équivalent, a fortiori un middleware comme IBM MQSeries, dont le canal de communication (ou channel) supporte le protocole de sécurité standardisé SSL/TLS.

L'hébergement de plusieurs instances de coffre-fort sur une même infrastructure matérielle est autorisé, sous réserve que les mécanismes de sécurité mis en oeuvre pour assurer ce cloisonnement soient précisément documentés et fassent l'objet d'un audit de sécurité technique.

* * *

Est-il possible d'héberger le domaine en .fr sur un relais ou un équipement de gestion de charges distinct du serveur web à qui il est associé ?

Cette configuration est mentionnée dans le projet d'annexe au dossier des exigences techniques, dans la partie 3.1.1 « Fonctions de création de traces du capteur ».

Dans le cas d'une architecture dont le protocole d'accès est basé sur HTTPS, la session sécurisée SSL/TLS peut être établie avec l'un des équipements d'infrastructure, assurant par exemple l'équilibrage de charge ou encore le filtrage réseau et/ou applicatif des flux, en amont du frontal (dans le sens « capteur d'évènements ») et de la plate-forme de services.

En revanche, il est essentiel que les transactions entre ces équipements, le frontal puis la plate-forme de services soient sécurisés, par le biais :

- *de mécanismes cryptographiques éprouvés au niveau réseau, transport ou applicatif (ex: IPSec, SSL/TLS, etc.) ;*
- *ou bien d'une colocalisation des équipements, prémunissant quasi de fait contre les attaques en écoute passive ou par interception dont pourrait faire l'objet un réseau de transport non maîtrisé.*

* * *

A quelle fréquence les données doivent elles être envoyées/récupérées ? En temps réel ou en masse a certaines intervalles ?

Ces aspects sont expliqués dans l'annexe au dossier des exigences techniques, notamment dans la partie relative au traitement par lot.

* * *

Traitement par lot : y a-t-il une « latence » maximale à ne pas dépasser pour enregistrer les données au sein du coffre ? Si oui, laquelle ? En seconde ? Est-il envisageable que le coffre-fort intègre une notion de file d'attente ? Cette file serait intégrée à l'environnement sécurisé du coffre et permettrait de résoudre les problèmes de performance. Actuellement aucun fournisseur n'est en mesure de proposer de systèmes suffisamment performants pour répondre aux exigences de l'ARJEL, sans file d'attente.

La durée de 300 secondes correspond à un délai raisonnable dans le projet d'annexe du dossier des exigences techniques, dans la partie "3.1.2 Fonctions de stockage des traces du coffre-fort". L'ARJEL laissera néanmoins à l'opérateur la latitude de choisir ce paramètre, afin de concilier au mieux robustesse du stockage, disponibilité et réactivité de la plate-forme, et optimisation du mécanisme de compression des lots, le cas échéant. En toute hypothèse, la granularité de l'enregistrement unitaire (i.e. à l'évènement) doit être techniquement implantée, à défaut de constituer le mode de fonctionnement nominal.

* * *

Tel qu'énoncé en note(1) page 83 de l'annexe au DET, il est possible de placer le capteur du frontal dans « la logique de présentation de l'application » plutôt qu'en coupure. Le schéma accompagnant cette explication indique clairement plusieurs couches au dessus de la plateforme de jeu : serveurs d'applications et de présentations. La question est de savoir jusqu'où porte cette désolidarisation au niveau du code : notre implémentation est basée autour d'un framework mvc, est il possible d'insérer la couche de capteurs au sein même de la plateforme de jeux : càd au niveaux des contrôleurs / vues ? Cette couche étant chargée de réceptionner les requêtes utilisateurs et d'envoyer la réponse adéquate mais sans logique de jeu. Une petite précision : dans notre cas la plateforme de jeu est hébergée en France.

Oui, ce mode de fonctionnement est conforme au DET. L'implantation du capteur au niveau des contrôleurs/vues permettra un traitement de la requête émise par le client au niveau applicatif, et une meilleure intégration à la plate-forme de jeux en ligne (notamment pour la gestion des erreurs de stockage des évènements de jeu), tout en étant situé en dehors de la logique de jeu.

* * *

Acquittement : l'acquittement synchrone que notre solution propose au capteur est un acquittement technique de réception. Est-ce conforme à la notion de « preuve » indiquée dans l'annexe p81 ?

Cela dépend de la nature de l'acquittement technique, qui sera à préciser dans la description technique du coffre figurant dans la demande d'agrément.

Annexe DET Partie 3.1.2

Traitement par lot : y a-t-il une « latence » maximale à ne pas dépasser pour enregistrer les données au sein du coffre ? Si oui, laquelle en seconde ?

La durée de 300 secondes correspond à un délai raisonnable dans le projet d'annexe du dossier des exigences techniques, dans la partie « 3.1.2 Fonctions de stockage des traces du coffre-fort ». L'ARJEL laissera néanmoins à l'opérateur la latitude de choisir ce paramètre, afin de concilier au mieux robustesse du stockage, disponibilité et réactivité de la plate-forme, et optimisation du mécanisme de compression des lots, le cas échéant. En toute hypothèse, la granularité de l'enregistrement unitaire (i.e. à l'évènement) doit être techniquement implantée, à défaut de constituer le mode de fonctionnement nominal.

Annexe DET Partie 3.1.3

Protocole d'accès au coffre-fort par l'ARJEL : le chapitre 4.2.2 du DET présente les principes de transfert des données remontées systématiquement vers l'ARJEL, basé sur des transferts périodique FTPS de l'opérateur vers l'ARJEL. Le chapitre 3.1.3 de l'annexe du DET présente les principes d'accès et d'extraction des traces de jeux collectées dans le coffre, basé sur des appels à la demande SOAP et HTTPS de l'ARJEL vers l'opérateur. Pourriez-vous confirmez que les traces de jeux seront exclusivement extraites à la demande suivant les principes établies dans le chapitre 3.1.3 de l'annexe du DET. Il ne sera pas demandé aux opérateurs de transmettre vers l'ARJEL de manière systématique.

Les traces de jeux seront exclusivement extraites à la demande de l'ARJEL suivant les principes établies dans le chapitre 3.1.3 de l'annexe du DET.

Le dépôt de données via le protocole FTPS correspond principalement aux données de supervision que l'opérateur soumettra à l'ARJEL, et non des traces de jeux dans un format brut. Le protocole de transfert décrit au chapitre 4.2.2 ne concerne donc pas le coffre-fort.

Annexe DET Partie 3.1.3.c

Certificats : les certificats dont le signataire n'est pas l'ARJEL doivent-ils être obligatoirement délivrés par une autorité de certification ?

Si la question porte sur une autorité de certification reconnue, la réponse est non ; les certificats déployés au sein de la plate-forme n'ont pas, a priori, à être émis par une autorité reconnue. L'opérateur pourra donc déployer sa propre IGC. Seul le certificat X.509v3 EV présenté aux joueurs doit être émis par une autorité reconnue dont le certificat est présent dans les navigateurs grand public.