COLLEGE DE L'AUTORITE DE REGULATION DES JEUX EN LIGNE

DECISION N° 2014-018 EN DATE DU 17 MARS 2014 PORTANT ADOPTION D'UN NOUVEAU REGLEMENT RELATIF A LA CERTIFICATION

Le collège de l'Autorité de régulation des jeux en ligne,

Vu la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, notamment ses articles 23 et 34-III ;

Vu la décision n° 2012-086 du collège de l'Autorité de régulation des jeux en ligne en date du 24 septembre 2012 portant modification du règlement de procédure d'inscription sur la liste des organismes certificateurs ;

Après en avoir délibéré le 17 mars 2014 ;

MOTIFS :

Considérant que les opérateurs agréés de jeux ou de paris en ligne sont soumis à une obligation de certification dans les conditions prévues à l'article 23 de la loi la loi n° 2010-476 du 12 mai 2010 susvisée ; que cette certification est réalisée par un organisme indépendant choisi par les opérateurs au sein d'une liste établie par l'Autorité de régulation des jeux en ligne ; qu'en vertu du III de l'article 34 de cette même loi, l'Autorité de régulation des jeux en ligne s'assure de la qualité des certifications réalisées en application de l'article 23 précité et peut procéder à la modification de la liste des organismes certificateurs ;

Considérant que, par sa décision n° 2012-086 du 24 septembre 2012, le collège de l'Autorité de régulation des jeux en ligne a modifié le règlement de procédure d'inscription sur la liste des organismes certificateurs adopté le 13 juillet 2010 ;

Considérant que les objectifs et besoins actuels de la régulation ainsi que le développement des moyens de contrôle de l'Autorité de régulation des jeux en ligne sont de nature à rendre opportune l'adoption d'un nouveau règlement relatif à la certification ayant vocation à se substituer au règlement de procédure d'inscription sur la liste des organismes certificateurs modifié en dernier lieu le 24 septembre 2012 ;

Considérant que les évolutions envisagées visent, en premier lieu, à clarifier les relations existantes entre les services de l'Autorité de régulation des jeux en ligne, les organismes certificateurs et les opérateurs agréés de jeux ou de paris en ligne ainsi que leurs rôles respectifs ; qu'elles tendent, ensuite, à définir plus précisément l'étendue et la nature des travaux attendus des organismes certificateurs pour mener à bien leur mission ; qu'elles répondent, en outre, à un besoin de clarification des périmètres respectifs de la certification annuelle initiale et de son actualisation ; qu'elles ont vocation, de surcroît, à permettre, dans la mesure du possible, un allègement des coûts liés aux opérations de certification ; qu'enfin, elles sont destinées à renforcer l'efficacité et la pertinence des procédures de certification ;

Considérant que la simplification, la transparence et l'allègement des procédures de certification ainsi recherchés impliquent notamment la suppression du pré-rapport qu'il appartenait jusqu'alors à l'organisme certificateur d'établir ; que, dans cette optique, il convient désormais que l'opérateur ayant été soumis à des travaux de certification soit considéré comme certifié, avec ou sans réserves ;

DECIDE :

Article 1er – Le règlement relatif à la certification prévue à l'article 23 de la loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne est adopté et fait corps avec la présente décision à laquelle il est annexé.

Article 2 – Est abrogée la décision n° 2012-086 du collège de l'Autorité de régulation des jeux en ligne en date du 24 septembre 2012 portant modification du règlement de procédure d'inscription sur la liste des organismes certificateurs.

Article 3 – La présente décision sera notifiée aux organismes inscrits sur la liste des organismes certificateurs ainsi qu'aux opérateurs agréés de jeux ou de paris en ligne et publiée sur le site Internet de l'Autorité de régulation des jeux en ligne.

Fait à Paris, le 17 mars 2014 ;

Le président de l'Autorité de régulation des jeux en ligne

Charles COPPOLANI

Décision mise en ligne sur le site officiel de l'ARJEL le 18 mars 2014

Autorité de régulation des jeux en ligne
RÉPUBLIQUE FRANÇAISE

RÈGLEMENT RELATIF À LA CERTIFICATION

PRÉVUE À L'ARTICLE 23 DE LA LOI N° 2012-476 DU 12 MAI 2010 RELATIVE À L'OUVERTURE À LA CONCURRENCE ET À LA RÉGULATION DU SECTEUR DES JEUX D'ARGENT ET DE HASARD EN LIGNE

Adopté par la décision n° 2014-018 du collège de l'Autorité de régulation des jeux en ligne en date du 17 mars 2014.

PREMIÈRE PARTIE : ORGANISMES CERTIFICATEURS

CHAPITRE 1er – PROCÉDURE D'INSCRIPTION

Article 1 – Objet de la procédure

La procédure d'inscription sur la liste des organismes certificateurs permet à l'Autorité de régulation des jeux en ligne de s'assurer que le demandeur à l'inscription :

a) est apte à certifier le respect, par les opérateurs de jeux ou de paris en ligne agréés par l'Autorité de régulation des jeux en ligne, de leurs obligations légales et réglementaires, conformément aux dispositions de l'article 23 de la loi n° 2010-476 du 12 mai 2010 ;

b) exercera en toute indépendance et impartialité les missions de certifications qu'il entend assumer ;

c) justifie d'une structure juridique et d'une organisation compatibles avec l'exercice des missions de certification qu'il souhaite mener.

L'évaluation des aptitudes de l'organisme demandeur s'effectue à partir d'une analyse du dossier de candidature décrit à l'article 5 du présent règlement.

Article 2 – Qualité du demandeur

Peut présenter une demande d'inscription sur la liste des organismes certificateurs toute entreprise, quelle que soit sa forme juridique, établie dans un État membre de l'Union européenne ou un État partie à l'accord sur l'Espace économique européen.

Article 3 – Recours à la sous-traitance

Le demandeur à l'inscription sur la liste des organismes certificateurs ou l'organisme certificateur qui entend recourir à la sous-traitance en informe l'Autorité de régulation des jeux en ligne.

Il communique à l'Autorité de régulation des jeux en ligne l'ensemble des pièces permettant de vérifier que le ou les sous-traitant(s) proposé(s) est/sont en mesure d'exécuter les missions qu'il envisage de lui/leur attribuer. Ces pièces sont celles exigées à l'article 5 du présent règlement.

L'évaluation des aptitudes du ou des sous-traitant(s) s'effectue à partir du dossier de candidature décrit à l'alinéa précédent.

Le ou les sous-traitant(s) n'exerce(nt) ses/leurs missions qu'à la condition d'avoir été préalablement accepté(s) par l'Autorité de régulation des jeux en ligne.

Le ou les sous-traitant(s) inscrit(s) sur la liste des organismes certificateurs est/sont soumis aux mêmes obligations que celles pesant sur les organismes certificateurs, en particulier celles prévues aux articles 10 et 11 du présent règlement.

L'organisme inscrit sur la liste des organismes certificateurs ne peut se prévaloir de ce qu'un ou plusieurs manquement(s) est/sont imputable(s) à son ou ses sous-traitant(s) pour se soustraire à ses obligations au titre du présent règlement.

Article 4 – Dépôt de la demande d'inscription

La demande d'inscription est adressée par courrier recommandé avec avis de réception ou déposée contre reçu à l'adresse suivante :

Autorité de régulation des jeux en ligne (ARJEL)
Direction générale déléguée à la régulation juridique et aux relations internationales
Département des agréments
99-101, rue Leblanc
75015 PARIS

L'Autorité de régulation des jeux en ligne en accuse réception par tout moyen et procède à son enregistrement.

Article 5 – Contenu du dossier de candidature

Le demandeur à l'inscription sur la liste des organismes certificateurs présente un dossier de candidature rédigé en langue française. Les pièces communiquées en langue étrangère sont traduites en français.

Le dossier de candidature peut être présenté sous forme dématérialisée. Il comporte pour le demandeur et, le cas échéant, pour chaque sous-traitant les éléments suivants :

- **<u>Une première partie consacrée à la présentation générale du demandeur et, le cas échéant, de son ou ses sous-traitant(s) comprenant les pièces suivantes</u>** :

- **Pièce n° 1** :
  - Un extrait *Kbis* de la société ou tout document équivalent pour les sociétés établies à l'étranger ;
  - Ou, s'il ne s'agit pas d'une personne morale, un justificatif de l'identité de son ou ses propriétaire(s) ;

- **Pièce n° 2** : Une présentation générale avec, le cas échéant, un ou des organigrammes présentant la place de la société dans le groupe si celle-ci appartient à un groupe de sociétés ;

- **Pièce n° 3** : Une déclaration concernant le chiffre d'affaires global et, le cas échéant, le chiffre d'affaires relatif à l'activité d'évaluation en vue de la délivrance d'une certification sur les trois derniers exercices clos ou, à défaut, pour les entreprises plus récentes, sur le ou les exercices clos ou en cours.

❖ **<u>Une deuxième partie constituée des éléments permettant d'apprécier les capacités professionnelles et les compétences techniques, juridiques et financières du demandeur et, le cas échéant, de son ou ses sous-traitant(s)</u> :**

Il convient en particulier de justifier que le personnel dédié dispose des compétences techniques nécessaires pour mener des activités d'évaluation et de certification de l'architecture et de la sécurité de systèmes d'information et/ou des aptitudes juridiques et financières lui permettant d'évaluer le respect par les opérateurs de jeux ou de paris en ligne de leurs obligations légales et réglementaires. Sur le plan technique, le personnel dédié doit être notamment qualifié et compétent en technologies de l'information, en audit de code et en évaluation de l'architecture de systèmes d'information et de leur sécurité.

Cette partie comporte les pièces suivantes :

- **Pièce n° 4** : Un document retraçant les expériences et les références nationales et internationales récentes de prestations similaires ainsi que les périodes de réalisation de ces prestations ;

- **Pièce n° 5** : La liste des personnes dédiées aux opérations de certification ainsi que leurs *curriculum vitae* détaillés. Ces documents devront notamment faire apparaître les éventuelles contributions ou publications de ces personnes ainsi que leur éventuelle participation à des colloques, conférences, formations spécialisées ou à des travaux de certification ;

- **Pièce n° 6** : Des rapports d'analyse « *type* » récents et conformes à l'état de l'art mettant en avant les méthodologies utilisées et le niveau de profondeur des analyses conduites dans des domaines d'expertise similaires à ceux abordés dans le cadre de la certification et plus particulièrement :

    - **Pièce n° 6-A** : Des audits applicatifs intrusifs, dont l'objectif est d'évaluer le niveau de sécurité d'une application par une approche combinant « audit de code » et « test d'intrusion » (en boîte blanche), afin d'identifier et d'exposer les vulnérabilités du composant et de déduire de cette analyse une liste de recommandations ;

    - **Pièce n° 6-B** : Des audits de configuration de plate-forme d'hébergement, dont l'objectif est d'évaluer le niveau de sécurité d'une architecture ou d'un composant (par exemple : équipement de commutation, routage, filtrage, système d'exploitation, serveur d'application ou encore application de type base de données).

❖ **<u>Une troisième partie permettant d'évaluer la capacité du demandeur ou, le cas échéant, de son ou ses sous-traitant(s) à satisfaire à ses obligations d'indépendance, d'impartialité et de confidentialité :</u>**

- **Indépendance et impartialité** :

Le demandeur ou, le cas échéant, son ou ses sous-traitant(s) justifie(nt), par une déclaration accompagnée de tout document utile, que les évaluations qu'il(s) sera/seront

amené(s) à mettre en œuvre seront faites en toute indépendance et en toute impartialité, conformément aux dispositions des articles 10 et 11 du présent règlement.

- **Pièce n° 7** : Déclaration d'impartialité et d'indépendance ;

  - **Confidentialité** :

    Le demandeur ou, le cas échéant, son ou ses sous-traitant(s) justifie(nt), par une déclaration accompagnée de tout document utile, qu'il(s) est/sont en mesure d'assurer la confidentialité des éléments portés à sa/leur connaissance pour les besoins des évaluations ainsi que celle des évaluations et de leurs résultats. Cette exigence ne porte que sur les informations qui ne sont pas publiques.

- **Pièce n° 8** : Déclaration de confidentialité**.**

Tout autre document comportant des informations jugées utiles par le demandeur ou, le cas échéant, par son ou ses sous-traitant(s), pourra également être produit.

Article 6 – Traitement du dossier de candidature

Le dossier de candidature fait l'objet d'un examen par l'Autorité de régulation des jeux en ligne dans un délai de deux mois à compter de sa date de réception.

Lorsque le dossier de candidature n'est pas complet, un courrier est adressé au demandeur l'invitant à transmettre, dans un délai qui ne peut être inférieur à quinze jours, le ou les pièce(s) faisant défaut.

L'instruction de la demande d'inscription est suspendue pendant ce délai.

Toute demande demeurée incomplète au terme du délai imparti entraîne le prononcé, par l'Autorité de régulation des jeux en ligne, d'une décision d'irrecevabilité de la demande d'inscription.

Au cours de l'instruction, le demandeur est tenu de fournir, à la demande des services de l'Autorité de régulation des jeux en ligne, toute information légalement justifiée de nature à éclairer ces derniers sur les éléments contenus dans le dossier déposé. En outre, le demandeur peut être auditionné par les services de l'Autorité de régulation des jeux en ligne s'ils l'estiment opportun.

Article 7 – Décision d'inscription

La décision d'inscription sur la liste des organismes certificateurs est délivrée *intuitu personae* par le collège de l'Autorité de régulation des jeux en ligne. L'inscription est valable cinq ans à compter de la date de sa notification.

La décision d'inscription énonce, le cas échéant, les obligations particulières auxquelles sont soumis les organismes certificateurs. Elle indique, le cas échéant, le ou les sous-traitant(s) acceptés par l'Autorité de régulation des jeux en ligne pour chaque organisme certificateur.

Toute décision de refus d'inscription est motivée et notifiée à l'intéressé par tout moyen propre à en établir la date de réception.

Article 8 – Publication de la liste des organismes certificateurs

La liste des organismes certificateurs est publiée sur le site Internet de l'Autorité de régulation des jeux en ligne.

Elle est mise à jour lors de chaque modification qui lui est apportée.

Elle mentionne les organismes certificateurs habilités par l'Autorité de régulation des jeux en ligne à réaliser les certifications prévues à l'article 23 de la loi n° 2010-476 du 12 mai 2010 ainsi que, le cas échéant, le ou les sous-traitant(s) déclaré(s) par eux et acceptés par l'Autorité de régulation des jeux en ligne.

Article 9 – Renouvellement de l'inscription

L'inscription sur la liste des organismes certificateurs est renouvelable.

L'instruction de cette demande se déroule selon les mêmes modalités que la demande initiale.

CHAPITRE 2 – SUIVI DES ORGANISMES INSCRITS SUR LA LISTE DES ORGANISMES CERTIFICATEURS

Article 10 – Obligations résultant de l'inscription sur la liste des organismes certificateurs

L'organisme inscrit sur la liste des organismes certificateurs :

- remplit les missions de certification qui lui sont confiées avec soin et diligence et en toute indépendance ;

- accomplit les opérations de certification qui lui sont confiées conformément à l'état de l'art ;

- conserve en toutes circonstances une attitude impartiale dans l'exercice de ses missions. Il fonde ses conclusions et son jugement sur une analyse objective de l'ensemble des données dont il a connaissance, sans préjugé ni parti pris. Il évite toute situation qui l'exposerait à des influences susceptibles de porter atteinte à son impartialité et s'engage à déclarer à l'Autorité de régulation des jeux en ligne toute pression qu'il subirait, quelle qu'en soit l'origine ;

- se conforme aux obligations légales de protection des données à caractère personnel et veille à la confidentialité des informations en sa possession ;

- rend compte immédiatement à l'Autorité de régulation des jeux en ligne de toute modification affectant la structure de son entreprise, son organisation ou son personnel et fournit les pièces justificatives de ces modifications. La liste et les *curriculum vitae* des

personnes dédiées aux missions de certification doit être maintenue à jour et communiquée à l'Autorité de régulation des jeux en ligne ;

- déclare à l'Autorité de régulation des jeux en ligne, préalablement à la réalisation de toute mission de certification qui lui est confiée, les termes de sa mission ainsi que l'identité de l'opérateur de jeux ou de paris en ligne concerné ;

- respecte les principes généraux et les différentes étapes du déroulement de la certification telles que précisées dans la seconde partie du présent règlement.

Article 11 – Prévention des conflits d'intérêts

L'organisme inscrit sur la liste des organismes certificateurs est indépendant de l'opérateur pour lequel il effectue une mission de certification.

Il ne peut mener aucune mission de certification pour un opérateur de jeux ou de paris en ligne dont il a été ou est le conseil ou le prestataire ou s'il a été ou est celui d'une société qui contrôle cet opérateur ou est contrôlée par cet opérateur au sens de l'article L. 233-16 du code de commerce.

La durée de l'incompatibilité prévue à l'alinéa précédent est de dix-huit mois. Elle court à compter du plus récent des deux événements suivants :

- la dernière prestation réalisée par l'organisme certificateur au profit de l'opérateur de jeux ou de paris en ligne ou des personnes ou entités qui le contrôlent ou qui sont contrôlées par lui au sens de l'article L.233-16 du code de commerce ;

- le dernier paiement réalisé au profit de l'organisme certificateur par l'opérateur de jeux ou de paris en ligne ou par des personnes ou entités qui le contrôlent ou qui sont contrôlées par lui au sens de l'article L.233-16 du code de commerce.

L'organisme inscrit sur la liste des organismes certificateurs avertit l'Autorité de régulation des jeux en ligne de la survenance de toute situation de conflit d'intérêts au regard de son activité de certification.

Le commissaire aux comptes éventuellement inscrit sur la liste des organismes certificateurs ou agissant en qualité de sous-traitant se conforme aux termes de l'avis n° 2012-03 du 22 mars 2012 rendu par le Haut Conseil du Commissariat aux Comptes en application de l'article R. 821-6 du code de commerce relatif à la possibilité pour un commissaire aux comptes ou un membre de son réseau d'intervenir en qualité de certificateur au comptes au sens de la loi n° 2010-476 du 12 mai 2010. Cet avis figure à l'annexe III du présent règlement

Article 12 – Relations commerciales entre l'organisme certificateur et l'opérateur de jeux ou de paris en ligne sollicitant une certification

L'Autorité de régulation des jeux en ligne est désignée dans tout contrat de certification comme destinataire de l'ensemble des informations du processus d'évaluation, notamment des rapports d'évaluation.

Le contrat de certification mentionne les noms des personnes devant intervenir au titre des missions de certification prévues dans ledit contrat.

Une copie du contrat de certification conclu entre l'opérateur de jeux ou de paris en ligne et l'organisme certificateur est transmise à l'Autorité de régulation des jeux en ligne préalablement à l'exécution de la prestation de certification.

Article 13 – Non accomplissement de prestations par l'organisme certificateur ou l'un de ses sous-traitants

Lorsque l'organisme certificateur ou, le cas échéant, l'un de ses sous-traitants n'a/ont pas, au cours d'une période d'une année continue, exécuté de mission de certification, les services de l'Autorité de régulation des jeux en ligne peuvent lui/leur demander de produire tout document permettant de vérifier qu'il(s) demeure(nt) apte(s) à remplir ses/leurs fonctions.

L'organisme certificateur ou le sous-traitant qui refuse de communiquer ces documents peut être sanctionné dans les conditions et la mesure prévues aux articles 16 et suivants du présent règlement.

L'organisme certificateur ou le sous-traitant qui s'avère ne plus être apte à remplir ses fonctions peut être retiré de la liste des organismes certificateurs par le collège de l'Autorité de régulation des jeux en ligne.

Préalablement à ce retrait, le collège de l'ARJEL informe l'intéressé, par tout moyen propre à en établir la date de réception, qu'il envisage de le retirer cette liste et l'invite à présenter ses observations écrites dans un délai qui ne peut être inférieur à quinze jours.

La décision de retrait est prononcée par le collège de l'Autorité de régulation des jeux en ligne. Elle est motivée et notifiée à l'intéressé par tout moyen propre à en établir la date de réception.

La liste des organismes certificateurs est mise à jour en conséquence.

Article 14 – Cessation d'activité de l'organisme certificateur ou de l'un de ses sous-traitants

Article 14-1 – L'organisme certificateur qui entend cesser son activité de certificateur demande à l'Autorité de régulation des jeux en ligne à être retiré de la liste des organismes certificateurs par courrier recommandé avec avis de réception.

La cessation de l'activité de l'organisme certificateur entraîne le retrait de l'inscription sur la liste des organismes certificateurs établie par l'Autorité de régulation des jeux en ligne.

La décision de retrait est prononcée par le collège de l'Autorité de régulation des jeux en ligne. Elle est motivée et notifiée à l'organisme certificateur ainsi que, le cas échéant, à son ou ses sous-traitant(s), par tout moyen propre à en établir la date de réception.

La liste des organismes certificateurs est mise à jour en conséquence.

Article 14-2 – Le sous-traitant qui entend cesser son activité de certificateur demande à l'Autorité de régulation des jeux en ligne à être retiré de la liste des organismes certificateurs par courrier recommandé avec avis de réception.

Avant de se prononcer sur ce retrait, l'Autorité de régulation des jeux en ligne apprécie s'il est de nature à affecter la capacité de l'organisme certificateur dont dépend le sous-traitant à mener à bien sa mission de certification.

L'organisme certificateur dont dépend le sous-traitant est invité à présenter ses observations.

La décision de retrait est prononcée par le collège de l'Autorité de régulation des jeux en ligne. Elle est motivée et notifiée à l'intéressé par tout moyen propre à en établir la date de réception. Une copie de la décision est adressée à l'organisme certificateur dont dépend le sous-traitant concerné.

La liste des organismes certificateurs est mise à jour en conséquence.

Article 15 – Pouvoirs de contrôle des services de l'Autorité de régulation des jeux en ligne

Les services de l'Autorité de régulation des jeux en ligne peuvent s'assurer à tout moment, par un audit, que l'organisme certificateur et/ou, le cas échéant, son ou ses sous-traitant(s) continue(nt) de satisfaire aux obligations résultant de l'inscription sur la liste des organismes certificateurs.

Ils s'assurent de la qualité des certifications réalisées.

CHAPITRE 3 – SANCTION DES ORGANISMES INSCRITS SUR LA LISTE DES ORGANISMES CERTIFICATEURS

Article 16 – Procédure et sanctions encourues

L'organisme certificateur qui méconnaît ses obligations au titre du présent règlement s'expose, en fonction de la gravité de ses manquements, à l'une des sanctions suivantes :

1° L'avertissement ;
2° La suspension de l'inscription pour six mois au plus ;
3° Le retrait de la liste des organismes certificateurs.

La décision est prononcée par le collège de l'Autorité de régulation des jeux en ligne. Elle est motivée et notifiée à l'intéressé par tout moyen propre à en établir la date de réception.

Préalablement au prononcé de l'une de ces sanctions, l'organisme certificateur et, le cas échéant, son ou ses sous-traitant(s), est/sont informé(s), par tout moyen propre à en établir la date de réception, des manquements relevés à son/leur encontre et invité(s) à présenter ses/leurs observations écrites dans un délai qui ne peut être inférieur à quinze jours.

Article 17 – Règles spécifiques en cas de suspension

La décision de suspension fixe la durée et les modalités de celle-ci. Elle comporte, le cas échéant, l'énoncé de mesures correctives.

La suspension et sa durée sont mentionnées sur la liste des organismes certificateurs.

Si, à l'issue de cette période de suspension, les causes ayant entraîné la suspension de l'inscription sont corrigées, l'organisme certificateur est averti de la fin de sa suspension et la mention de la suspension de l'organisme certificateur est supprimée de la liste des organismes certificateurs.

Dans le cas contraire, l'Autorité de régulation des jeux en ligne notifie à l'organisme certificateur, par tout moyen propre à en établir la date de réception, les faits qui, relevés à son encontre, s'avèrent de nature à justifier son retrait de la liste des organismes certificateurs, et l'invite à présenter ses observations écrites dans un délai qui ne peut être inférieur à quinze jours.

Article 18 – Règles spécifiques en cas de retrait

Le retrait de l'inscription peut s'accompagner de l'interdiction de solliciter une nouvelle inscription pendant un délai maximal de trois ans.

La décision de retrait emporte interdiction de mener une nouvelle mission de certification. Elle met immédiatement fin à toute opération de certification en cours.

L'organisme certificateur retiré définitivement de la liste des organismes certificateurs doit remettre à l'Autorité de régulation des jeux en ligne l'ensemble des dossiers relatifs aux évaluations menées.

Il est tenu de notifier son retrait de la liste des organismes certificateurs aux opérateurs de jeux ou de paris en ligne pour lesquels il réalise, au jour de la décision de retrait, une mission de certification. Il justifie du respect de cette obligation auprès de l'Autorité de régulation des jeux en ligne. A défaut, l'Autorité se réserve le droit de prévenir les opérateurs agréés et les autres acteurs concernés par les évaluations en cours.

La liste des organismes certificateurs est mise à jour en conséquence.

SECONDE PARTIE : TRAVAUX DE CERTIFICATION

CHAPITRE 1er : PRINCIPES GÉNÉRAUX

Article 19 – Objectifs de la certification

La certification constitue un instrument d'évaluation de la situation de l'opérateur de jeux ou de paris en ligne qui complète la stratégie et les pouvoirs de contrôle de l'Autorité de régulation des jeux en ligne.

Elle ne lie pas l'Autorité de régulation des jeux en ligne.

La certification technique à six mois prévue au II de l'article 23 de la loi n° 2010-476 du 12 mai 2010 porte sur le respect, par l'opérateur de jeux et paris en ligne, de ses obligations techniques prévues aux articles 31 et 38 de cette loi.

La certification annuelle initiale prévue au premier alinéa du III de l'article 23 de la loi n° 2010-476 du 12 mai 2010 a pour but, plus particulièrement, de s'assurer que l'opérateur agréé met en œuvre correctement l'ensemble des moyens annoncés dans son dossier de demande d'agrément aux fins de respecter ses obligations légales et réglementaires.

La certification prévue au deuxième alinéa du III de l'article 23 de la loi n° 2010-476 du 12 mai 2010 a pour but, quant à elle, d'actualiser la certification annuelle initiale.

Article 20 – Principe de la mesure unique

Les opérations d'analyse conduites par l'organisme certificateur ou, le cas échéant, par son sous-traitant, ne sont pas itératives au cours d'une même certification : chaque exigence contrôlée fait l'objet d'une mesure unique.

Des échanges peuvent avoir lieu au moment de la mesure entre l'organisme certificateur ou son sous-traitant et l'opérateur dont il assure la certification. Toutefois, une fois la mesure effectuée, ces échanges ne peuvent en aucun cas conduire l'organisme certificateur ou son sous-traitant à effectuer une nouvelle mesure.

En particulier, les éventuelles modifications apportées par un opérateur en cours de certification sur un point de contrôle déjà mesuré ne peuvent pas modifier la constatation initiale qui doit figurer dans le rapport de certification.

CHAPITRE 2 : DÉROULEMENT DE LA CERTIFICATION

Article 21 – Réalisation des travaux conformément à des référentiels

Les travaux de certification sont réalisés conformément aux référentiels technique et juridique et financier annexés au présent règlement (annexes I et II).

Ces référentiels déterminent les différentes exigences devant faire l'objet d'un contrôle de la part de l'organisme certificateur ou, le cas échéant, de son ou ses sous-traitant(s) lors de la certification prévue

au II et au premier alinéa du III de l'article 23 de la loi n° 2010-476 du 12 mai 2010 et, le cas échéant, lors de celle prévue au deuxième alinéa du même texte. Ils précisent également la méthodologie à suivre et la nature des contrôles attendus.

Le référentiel technique précise en outre les niveaux de criticité retenus pour chaque exigence.

Article 22 – Périmètre de la certification

Le périmètre de la certification varie en fonction du type de certification mis en œuvre.

Pour les certifications prévues au II et au premier alinéa du III de l'article 23 de la loi n° 2010-476 du 12 mai 2010, l'organisme certificateur ou, le cas échéant, son ou ses sous-traitant(s) est tenu de contrôler l'ensemble des exigences listées dans les référentiels visés à l'article 21 du présent règlement.

S'agissant de l'actualisation de la certification annuelle initiale prévue au deuxième alinéa de l'article 23 de la loi n° 2010-476 du 12 mai 2010, le périmètre de la certification est susceptible de varier en fonction, notamment :

- de l'absence de modifications apportées par l'opérateur, depuis la dernière certification, aux exigences prévues par les référentiels visés à l'article 21 du présent règlement. Cette absence de modifications est attestée par une déclaration spécifique de l'opérateur annexée au rapport de certification ;

- des conclusions de la dernière certification.

Les référentiels visés à l'article 21 du présent règlement déterminent les conditions de variation du périmètre de l'actualisation de la certification annuelle.

Lorsque la certification est obtenue avec réserve(s) dans les conditions prévues à l'article 23 du présent règlement, les points de réserve doivent, en toute hypothèse, être mesurés à nouveau lors de l'actualisation de la certification.

Article 23 – Remise des travaux de certification

A l'issue de ses travaux, l'organisme certificateur établit un rapport faisant état des constats réalisés à partir des référentiels visés à l'article 21 du présent règlement. Ce rapport dresse la liste de l'ensemble des non-conformités constatées, quel que soit, au plan technique, leur niveau de criticité.

Ce rapport est rédigé ou traduit en langue française. Il est transmis à l'Autorité de régulation des jeux en ligne ainsi qu'à l'opérateur de jeux ou de paris en ligne concerné. Aucun pré-rapport n'est adressé ni à l'Autorité de régulation des jeux en ligne, ni à l'opérateur concerné.

Le rapport conclut soit à la certification sans réserve, soit à la certification avec réserve(s).

Sur le plan technique, la certification est faite avec réserve(s) lorsque une ou plusieurs exigences techniques présentant un niveau de criticité défini par le référentiel technique n'est/ne sont pas atteintes.

Sur le plan juridique et financier, la certification est faite avec réserve(s) lorsque une ou plusieurs exigences juridiques et financières n'est/ne sont pas atteintes.

Les exigences techniques, juridiques ou financières non atteintes constituent des non-conformités. Sur le plan technique, les non-conformités relatives aux exigences de sécurité sont également dénommées vulnérabilités.

L'organisme certificateur transmet à l'opérateur concerné le document attestant de l'obtention de la certification visé à l'article 23 de la loi n° 2010-476 du 12 mai 2010 afin que celui-ci procède à la transmission prévue à cet article. Ce document indique si la certification est obtenue avec ou sans réserve(s) et fait état, le cas échéant, de la ou des réserve(s) concernée(s).

Article 24 – Fiches d'anomalies

A l'issue de la remise du rapport de certification, l'opérateur réalise, s'il y a lieu, des fiches d'anomalies qu'il adresse à l'Autorité de régulation des jeux en ligne dans le délai d'un mois suivant la remise de ce rapport. Ces fiches d'anomalies sont adressées, pour information, à l'organisme certificateur.

Les fiches d'anomalies sont distinctes du rapport de certification.

Elles comportent la liste de l'ensemble des non-conformités relevées dans le rapport de certification, quel que soit, au plan technique, leur niveau de criticité.

Pour chaque non-conformité, l'opérateur propose, le cas échéant, des mesures correctives ainsi qu'un échéancier de mise en œuvre.

Ces fiches d'anomalies peuvent également permettre à l'opérateur de porter à la connaissance de l'Autorité de régulation des jeux en ligne toute information ou observation utile concernant le déroulement des opérations de certification et/ou de lui faire état de son éventuel désaccord avec les conclusions de ce rapport ou avec la méthodologie employée (erreur manifeste du certificateur, incomplétude du périmètre, mesure opérée inexacte, incomplète ou non-conforme à l'état de l'art, *etc.*). A cet égard, l'opérateur pourra, le cas échéant, faire procéder à une nouvelle mesure et produire le résultat de cette mesure dans le cadre des fiches d'anomalies.

Article 25 – Suites de la certification

Lorsque l'Autorité de régulation des jeux en ligne constate que des points de contrôle n'ont pas été correctement mesurés par l'organisme certificateur ou que ses appréciations sur la conformité ne semblent pas suffisamment fondées, elle peut demander à l'opérateur concerné toute information utile et, le cas échéant, mettre en œuvre une procédure de sanction à l'encontre de l'organisme certificateur, en application des articles 16 et suivants du présent règlement.

Lorsque l'Autorité de régulation des jeux en ligne estime que des points de contrôle de la certification révèlent des manquements à des obligations légales ou réglementaires prévues par la loi n° 2010-476 du 12 mai 2010 et ses textes d'application, elle est susceptible de demander à l'opérateur concerné toute explication utile, son éventuel plan d'action et, le cas échéant, sa mise en conformité dans un délai déterminé. L'Autorité de régulation des jeux en ligne est en outre susceptible de mettre en œuvre à son encontre une procédure de sanction, dans les conditions prévues aux articles 43 et suivants de la loi n° 2010-476 du 12 mai 2010.

ANNEXES

Annexe I : Référentiel technique

Annexe II : Référentiel juridique et financier

Annexe III : Avis n° 2012-03 rendu le 22 mars 2012 par le Haut Conseil du Commissariat aux Comptes en application de l'article R. 821-6 du code de commerce relatif à la possibilité pour un commissaire aux comptes ou un membre de son réseau d'intervenir en qualité de certificateur au comptes au sens de la loi n° 2010-476 du 12 mai 2010

Autorité de régulation des jeux en ligne
RÉPUBLIQUE FRANÇAISE

RÉFÉRENTIEL TECHNIQUE

ANNEXE I du Règlement relatif à la certification prévue à l'article 23 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne adopté par la décision n° 2014-018 du collège de l'Autorité de régulation des jeux en ligne en date du 17 mars 2014.

Guide méthodologique

Règles essentielles

- Le volet technique de la certification repose sur des exigences de conformité et de sécurité issues du DET et de ses annexes ;
- les exigences de conformité et de sécurité font l'objet de points de contrôle, regroupés dans un référentiel technique de certification ;
- le référentiel technique de certification est constitué du présent guide méthodologique et de deux matrices d'exigences, faisant l'objet de deux documents distincts :
    - la matrice d'exigences de la certification unique à 6 mois du composant frontal,
    - la matrice d'exigences de la certification annuelle ;
- les matrices d'exigences et les points de contrôle associés sont alimentés par :
    - les documents et attestations transmis par l'opérateur,
    - les analyses menées directement par l'organisme certificateur ;

- l'organisme certificateur effectue une mesure unique des différents points de contrôle ;
- l'organisme certificateur dresse, dans le rapport de certification, la liste de l'ensemble des vulnérabilités et non-conformités constatées quel que soit leur niveau de criticité.

- à l'issue de la remise du rapport de certification, l'opérateur réalise, s'il y a lieu, des fiches d'anomalies, reprenant l'ensemble des vulnérabilités et non-conformités soulevées par l'organisme certificateur. Ces fiches sont adressées à l'ARJEL et à l'organisme certificateur dans le délai d'un mois suivant la remise du rapport de certification ;
- les fiches d'anomalies font état, le cas échéant, des mesures correctives proposées par l'opérateur ainsi que de tout désaccord éventuel de l'opérateur avec les conclusions du rapport de l'organisme certificateur ;

- le référentiel technique de certification introduit trois niveaux de criticité des exigences, de la moins critique (1) à la plus critique (3) ;
- chaque exigence est liée, par défaut, à un niveau de criticité ;
- l'organisme certificateur peut moduler le niveau de criticité d'une exigence, à condition de justifier ses critères d'appréciation ;
- le rapport conclut à une certification sans réserve ou avec réserves, si une ou plusieurs exigences du référentiel ne sont pas atteintes ;
- les réserves concernent les exigences non atteintes dont le niveau de criticité est supérieur ou égal à 2 ;

- la certification unique à 6 mois du composant frontal repose sur un socle d'analyses obligatoires ;
- le composant frontal fait l'objet d'une analyse fonctionnelle et technique complète 6 mois après sa date de mise en production ;
- la certification annuelle repose sur un socle d'analyses susceptibles de faire, ou non, l'objet d'une actualisation, partielle ou totale ;
- une analyse non actualisable doit être effectuée dans son intégralité ;
- l'analyse du composant frontal fait l'objet d'une actualisation à chaque certification annuelle ;

- le rapport de certification technique est constitué de la matrice des exigences dûment complétée et des différents livrables et annexes issus des analyses techniques de l'organisme certificateur.

1 Périmètre des certifications

1.1 Certification unique à 6 mois du composant frontal

1.1.1 Périmètre d'intervention technique

Prévue au II de l'article 23 de la loi n°2010-476 du 12 mai 2010, la certification unique à 6 mois porte sur le composant frontal et son infrastructure d'hébergement.

1.1.2 Couverture des exigences

Les exigences concernées sont celles issues du DET et de ses annexes : elles font l'objet des points de contrôle documentés dans le référentiel technique de la certification unique à 6 mois du composant frontal.

1.2 Certification annuelle

1.2.1 Périmètre d'intervention technique

Prévue au III de l'article 23 de la loi n°2010-476 du 12 mai 2010, la certification annuelle porte sur l'infrastructure globale du service de jeu en ligne ainsi que sur les modifications apportées aux logiciels homologués.

Ce périmètre inclut donc également le périmètre de la certification unique à 6 mois du composant frontal (partie 1.1).

1.2.2 Couverture des exigences

Les exigences concernées sont celles issues du DET et de ses annexes : elles font l'objet des points de contrôle documentés dans le référentiel technique de la certification annuelle.

2 Référentiel technique de certification

2.1 Matrice d'exigences

La certification unique à 6 mois du composant frontal et la certification annuelle font l'objet de matrices d'exigences techniques distinctes. Ces matrices d'exigences, tout comme le présent guide méthodologique, sont annexées au règlement de certification.

Chaque matrice regroupe les exigences de conformité et de sécurité issues du DET et de ses annexes. Les exigences font l'objet d'une numérotation et sont classées par thème.

La matrice d'exigences du référentiel de certification doit être complétée par l'organisme certificateur à l'issue de ses analyses. Elle synthétise les résultats obtenus à travers :

- les différentes opérations d'analyses techniques conduites par l'organisme certificateur (audits applicatifs, d'architecture, de configuration ou encore tests d'intrusion interne ou externe) ;

- l'analyse de la documentation remise par l'opérateur ;

- l'intégration des attestations d'absence de modification produites[1], le cas échéant, par l'opérateur. Remarque : cette absence de changement ne doit pas être incompatible avec un maintien en conditions de sécurité (gestion des mises à jour de sécurité, adaptation aux nouvelles attaques par des mesures de durcissement conformes à l'état de l'art, *etc.*).

2.2 Niveau de criticité d'une exigence

Un niveau de criticité, sur une échelle de 1 à 3 (criticité la plus élevée), est affecté à chaque exigence :

- ➔ le niveau de criticité 1 correspond essentiellement aux exigences liées à l'*existence* d'une documentation ou d'une procédure (ex : politique de sécurité, procédure de mise à jour, de durcissement d'un système, *etc.*) ;

- ➔ le niveau de criticité 2 correspond essentiellement aux exigences pour lesquelles une non-conformité a un impact *opérationnel* : défaut d'*application* d'une procédure, défaut de respect des exigences *opérationnelles* de conformité et de sécurité définies par l'ARJEL, ou encore défaut de suivi des règles de bonnes pratiques en sécurité des systèmes d'information ;

- ➔ le niveau de criticité 3 correspond aux exigences dont le non-respect est jugé très critique, le plus souvent en termes de conformité règlementaire ou en termes de sécurité (sur un composant exposé et/ou manipulant des données critiques).

Les niveaux de criticité ne sont pas figés : ils peuvent faire l'objet d'une réévaluation par l'organisme certificateur, après avis d'expert et échange éventuel avec l'opérateur au moment de la mesure du point de contrôle. L'organisme certificateur peut donc moduler le niveau de criticité d'une exigence, selon la nature exacte de la non-conformité identifiée et plus particulièrement de ses éléments de contexte : le cas échéant, il doit indiquer très précisément quels sont ses critères d'appréciation, afin de justifier de tout écart avec le niveau de criticité nominal d'une non-conformité[2].

A l'issue de ces opérations d'analyse, l'attestation de certification produite liste, le cas échéant, les réserves portant sur les non-conformités et vulnérabilités identifiées dont le niveau de criticité est supérieur ou égal à 2.

3 Méthodologie et livrables attendus

3.1 Méthodologie

[1] Attestation certifiant, par exemple, que la cinématique d'enregistrement mise en œuvre par le capteur n'a fait l'objet d'aucune modification depuis la précédente certification.
[2] Par exemple, une vulnérabilité applicative n'aura pas le même niveau de criticité (2, par défaut), selon l'exposition du composant impacté et sa proximité avec les données utilisateurs (cf. annexe I).

L'ensemble des rapports d'audits, documentations et attestations remises, le cas échéant, par l'opérateur permettent d'alimenter le référentiel technique de certification (cf. partie 2.1).

Pour chaque point de contrôle, l'organisme certificateur doit donc compléter la matrice des exigences, en renseignant la conformité de l'exigence évaluée et son niveau « définitif » de criticité (résultant de son analyse et prenant en compte les éléments communiqués par l'opérateur au cours de la réalisation de la mesure, cf. partie 2.2), ainsi que le ou les différents chapitres des rapports démontrant l'analyse effectuée.

Certaines mesures, dont l'analyse ne serait pas issue des rapports d'audits, peuvent être détaillées dans un rapport général intitulé « *Vérification des exigences* ».

Les opérations d'analyse conduites par l'organisme certificateur ne sont pas itératives au cours d'une même certification : l'organisme certificateur doit donc respecter le principe de la mesure unique de chaque point de contrôle. En particulier, les éventuelles modifications apportées par un opérateur, en cours de certification, sur un point déjà évalué ne peuvent pas modifier la constatation initiale qui doit figurer dans le rapport de certification.

, l'organisme certificateur énumère, le cas échéant, dans la synthèse du rapport, les réserves relatives aux vulnérabilités ou non-conformités découvertes lors de ses travaux. Seules les réserves de niveau 2 et 3 seront mentionnées.

Les vulnérabilités et non-conformités constatées font, indépendamment de leur niveau de criticité, l'objet d'une énumération exhaustive dans le rapport de synthèse. La liste de ces vulnérabilités et non-conformités est reprise, s'il y a lieu, dans les fiches d'anomalies. Ces fiches d'anomalies ne font pas partie du rapport de certification et doivent être communiquées à l'ARJEL et à l'organisme certificateur dans le délai d'un mois suivant la remise dudit rapport. Elles sont réalisées par l'opérateur, notamment afin qu'il propose des mesures correctives ainsi qu'un échéancier de mise en œuvre. Si l'opérateur souhaite par ailleurs apporter des précisions sur la mise en place éventuelle d'un correctif[3] qui serait postérieure à la mesure de l'organisme certificateur ou, plus généralement, s'il souhaite porter une information de toute nature à la connaissance de l'ARJEL, il peut formuler ses remarques et commentaires à travers ces fiches d'anomalies. Ces fiches d'anomalies peuvent également être l'occasion pour l'opérateur de préciser son éventuel désaccord avec les conclusions apportées par l'organisme certificateur sur certaines non-conformités ou vulnérabilités. Dans ce cas de figure, l'opérateur doit apporter une analyse contradictoire détaillée.

L'ARJEL détermine, en fonction des différents éléments apportés par l'opérateur et de la pertinence ou de la profondeur des analyses conduites par l'organisme certificateur, les éventuelles suites à donner. .

3.2 Certification à 6 mois du frontal

La certification unique à 6 mois du composant frontal, ainsi que la certification annuelle, sont à périmètre technique et couverture des exigences constants (cf. partie 1). Les deux certifications diffèrent néanmoins en termes de niveau d'analyse des opérations de vérification.

Les contrôles effectués lors de la certification unique à 6 mois du composant frontal reposent sur un socle d'analyses obligatoires.

L'audit applicatif du frontal, concentré sur le ou les composants « capteur(s) », est invariablement composé de deux volets :

- ➔ le premier volet correspond à l'analyse fonctionnelle et technique du code du capteur, permettant de présenter le fonctionnement de la vérification et de l'enregistrement des traces au coffre-fort et la mise en œuvre d'une cinématique conforme aux exigences du DET,

[3] Il est évident qu'en cas de vulnérabilité avérée, l'opérateur a intérêt à proposer un correctif dans les plus brefs délais. La mise en place de ce correctif ne saurait néanmoins annuler la non-conformité à l'exigence associée, ou encore en diminuer le niveau de criticité.

notamment en termes de mise en coupure et d'acquittement préalable par le joueur. L'organisme certificateur n'effectue pas l'analyse syntaxique et sémantique des enregistrements XML, mais s'assure que le positionnement du capteur est conforme aux exigences du DET et que l'ensemble des enregistrements sont correctement formés au sens de la norme XML et des schémas XSD publiés par l'ARJEL.

Lors de la certification annuelle, ce volet peut être actualisé si des modifications ont été apportées par l'opérateur. Si aucune modification n'a été effectuée et que l'opérateur déclare une absence totale de modification par le biais d'une attestation, les analyses spécifiques à ce périmètre peuvent être omises à l'occasion de la nouvelle certification : la matrice des points de contrôle peut alors reprendre à l'identique les résultats obtenus lors de la certification antérieure. Les rapports d'analyse pointés sont alors ceux de la certification antérieure, auxquels s'ajoute l'attestation d'absence de modification produite par l'opérateur pour l'année écoulée.

➔ Le second volet est relatif à la sécurité du capteur, mesurée par le biais d'un audit intrusif. Lors de cette analyse, l'organisme certificateur tente, aux travers de tests intrusifs, d'injecter des évènements spécialement formés dans le coffre afin d'en détourner les fonctions d'enregistrement et de sécurité (corruption des enregistrements, injection de faux évènements, prise de contrôle à distance du composant « capteur » ou encore du coffre-fort), ou encore de modifier les informations liées à ses paris ou à la gestion de son compte.

Lors de la certification annuelle, ce volet est non actualisable. Il est intégré à l'audit intrusif plus généralement conduit sur l'ensemble de la plate-forme. Il s'agit donc d'une nouvelle analyse, qui permet notamment de s'adapter – à implémentation constante – aux évolutions de l'état de l'art en sécurité des systèmes d'information et, à chaque itération, de pallier le manque d'exhaustivité intrinsèque aux tests d'intrusion.

La liste complète des autres analyses et donc livrables attendus dans le cadre de la certification unique à 6 mois du composant frontal figure dans l'annexe II.

3.3 Certification annuelle

Les contrôles effectués lors de la certification annuelle reposent sur des analyses dont les résultats peuvent, ou non, faire l'objet d'une actualisation, partielle ou totale. On parle, le cas échéant, d'une analyse actualisable.

Par actualisation, on entend la réitération, partielle ou totale, des contrôles effectués lors d'une certification antérieure sur un périmètre donné. En termes de livrables, il est donc principalement attendu une mise à jour des résultats obtenus[4] et des commentaires assortis, le cas échéant.
Une attestation d'absence de modification produite par l'opérateur (cf. partie 2.1) peut par ailleurs conduire l'organisme certificateur à ne pas effectuer d'analyse sur le périmètre concerné, sous réserve que cette absence de modification ne soit pas incompatible avec un maintien en conditions de sécurité.

Toutes les analyses ne sont pas actualisables et, à plus forte raison, ne peuvent pas être remplacées par une déclaration d'absence de modification par l'opérateur. En particulier, les points de contrôle qui auraient fait l'objet de réserves à l'occasion de la précédente certification doivent, en tout état de cause, faire l'objet d'une nouvelle analyse.

[4] Par exemple, pour un audit de configuration, les résultats de commande/outils, ainsi que les captures d'écran peuvent donc être mis à jour. Un rapport d'audit ne doit donc pas comporter le résultat de la commande « uname –a » de l'année antérieure, ou une capture d'écran dont la date ne correspond pas à la date de la mesure.

En règle générale, les opérations de vérification des points de contrôle liés à la sécurité *opérationnelle* des systèmes d'information sont actualisables mais ne peuvent pas faire l'objet d'une attestation d'absence de modification, dans la mesure où les vulnérabilités et l'état de l'art en sécurité des systèmes d'information sont en constante évolution :

- ➔ en pratique, les tests d'intrusion, internes ou externes, ne peuvent pas faire l'objet d'une actualisation et doivent donc être chaque année totalement réalisés. Il est d'ailleurs fortement recommandé que les auditeurs soient renouvelés à chaque réalisation d'un test d'intrusion et qu'ils n'aient pas accès, dans un premier temps, aux résultats précédents.

- ➔ en revanche, les audits de sécurité (audit technique de configuration, analyse d'architecture, *etc.*) peuvent faire l'objet d'une actualisation sur l'échantillon antérieur, ainsi que d'une nouvelle analyse sur un nouvel échantillon, complémentaire et introduite à des fins d'exhaustivité.

Les livrables suivants sont donc susceptibles de faire l'objet d'une actualisation ou, exceptionnellement, d'une substitution (en cas d'attestation d'absence de modification produite par l'opérateur) :

- ➔ analyse fonctionnelle et technique du capteur : cette analyse est actualisée si et seulement si l'implémentation du capteur a été modifiée ou afin de valider la correction d'anomalies précédemment identifiées.

  Si l'opérateur communique une attestation précisant que le capteur n'a pas été modifié et qu'aucune non-conformité n'a été relevée dans le précédent audit, l'organisme certificateur peut produire l'attestation dans les annexes et ne pas produire de nouvelle analyse du code source du capteur.

  En revanche, les tentatives de contournement du capteur doivent être dans tous les cas revérifiées annuellement, à l'occasion des audits intrusifs portant sur l'ensemble de la plate-forme de jeu (cf. partie 3.2).

  Pour rappel, l'analyse syntaxique et sémantique des évènements XML enregistrés au coffre ainsi que le fonctionnement du mécanisme d'interrogation des interdits de jeux ne sont pas à effectuer ;

- ➔ analyse d'architecture : le schéma réseau (niveau 3), la matrice de flux, les règles de filtrage ainsi que l'analyse des mécanismes d'administration peuvent faire l'objet d'une simple actualisation par l'organisme certificateur ;

- ➔ audit de configuration : l'organisme certificateur peut initialement, s'il le juge nécessaire, échantillonner les composants à auditer par rôle et/ou par criticité.

  Concernant les certifications ultérieures, la base de connaissances construite au gré des analyses doit permettre à l'organisme certificateur de revoir son échantillonnage et de recentrer son audit sur le fonctionnement d'un ou plusieurs composants qui n'auraient pas fait l'objet d'une analyse approfondie à l'occasion d'une précédente certification. Un travail d'actualisation peut donc être effectué sur les analyses de l'échantillon antérieur.

  Il est important que les contrôles relatifs à la sécurité des systèmes soient systématiquement effectués (état des mises à jour, gestion des comptes utilisateurs, gestion des droits, complexité des mots de passe, synchronisation horaire, *etc.*).

La liste complète des autres analyses et donc livrables attendus dans le cadre de la certification annuelle figure dans l'annexe III. Les livrables qui peuvent faire l'objet d'une actualisation sont indiqués en vert.

Annexe I – Exemples d'évaluation de niveau de criticité en fonction d'éléments de contexte.

Point de contrôle	Anomalie constatée	Contexte	Niveau de criticité initial	Niveau de criticité final
E1	Refus d'accès à un composant de la plate-forme	--	3	3
E5	Version non homologuée d'un logiciel de jeu en production	Des évolutions logicielles mineures ont été effectuées sur une version homologuée sans déclaration à l'ARJEL dans les délais prévus, mais sans impact sur la sécurité ou l'expérience de jeu	3	2
E7	Absence de politique de sécurité	Les équipes techniques présentent un défaut de sensibilisation et de compétences en sécurité informatique	1	2
E29	Back-office accessible depuis Internet, sans filtrage de niveau 3 (IP)	Aucune vulnérabilité découverte (mots de passe faibles, défaut d'implémentation du logiciel back-office [injection SQL, LFI/RFI, etc.])	2	2
E29	Backoffice accessible depuis Internet sans filtrage de niveau 3 (IP)	Vulnérabilité découverte (mot de passe trivial)	2	3
E33	Absence de mises à jour	Serveur wiki interne	2	2
E33	Absence de mises à jour	Serveur applicatif accessible depuis Internet, manipulant des données utilisateurs	2	3
E45	Présence d'un XSS ou d'une injection SQL	Serveur accessible depuis Internet	2	3
E59	Absence de synchronisation NTP	Relais-inverse HTTP en entrée	2	2
E59	Absence de synchronisation NTP	Serveur DNS responsable de l'interrogation des interdits de jeu	2	3

Les éléments ci-dessus ne constituent que des exemples fournis à titre d'illustration et en aucun cas un référentiel d'analyse. Seule l'expertise déployée par l'organisme certificateur peut permettre de moduler les niveaux de criticité.
La modification d'un niveau de criticité par l'organisme certificateur n'a bien entendu de sens que lorsque que l'exigence concernée n'est pas atteinte.

Annexe II – Livrables de la certification unique à 6 mois du composant frontal.

Le rapport de la certification à 6 mois se compose, pour chaque agrément, des 6 livrables suivants :

1. synthèse des rapports, avec mention des réserves ;
2. matrice des exigences ;
3. audit intrusif du capteur ;
4. audit de configuration de l'hébergement du frontal ;
5. rapport de vérification du respect des exigences ;
6. annexes techniques.

Synthèse des rapports :

1. présentation du candidat opérateur ;
2. nombres de jour/homme consacrés à chaque point ;
3. dates des différentes prestations ;
4. date de mise en œuvre opérationnelle du frontal ;
5. synthèse stratégique des résultats obtenus par point ;
6. liste des réserves.

Matrice des exigences.

Audit du capteur :

1. synthèse :
    a. synthèse de l'analyse fonctionnelle et technique,
    b. synthèse technique de l'audit intrusif,
    c. synthèse des vulnérabilités, classées par criticité et impact,
    d. synthèse des recommandations, classées par priorité et coût de mise en œuvre;

2. analyse fonctionnelle et technique :
    a. présentation de la solution :
        i. mécanismes d'enregistrement des traces,
        ii. mécanismes de vérification et de filtrage des données,
        iii. mécanismes de sécurité du capteur,
    b. analyse de code des fonctions les plus importantes du capteur ;

3. audit intrusif du capteur : déroulement linéaire de l'audit, avec description explicite de la méthodologie employée pour détecter les vulnérabilités et les exploiter, le cas échéant.

Audit de configuration du frontal et de son infrastructure d'hébergement :

1. synthèse :
    a. synthèse technique de l'audit de configuration,
    b. synthèse des vulnérabilités, classées par criticité et impact,
    c. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;

2. rapport d'audit :
    a. analyse de la stratégie de sécurité (politique de sécurité technique, procédures, …),
    b. analyse de l'architecture technique (matrices de flux, règles du pare-feu, …),
    c. analyse des configurations, aux niveaux système, réseau et applicatif.

Vérification du respect des exigences : rapport regroupant les différentes analyses n'ayant pas été abordées dans les précédents livrables ;

Annexes techniques :

1. attestations, le cas échéant ;
2. documentation opérateur.

Les fiches d'anomalies sont transmises directement par l'opérateur à l'ARJEL ainsi qu'à l'organisme certificateur. Ces fiches d'anomalies doivent reprendre l'intégralité des vulnérabilités et non conformités pointées par l'organisme certificateur (associées au contenu rédigé par l'organisme certificateur) et intégrer les différentes réponses de l'opérateur (cf. partie 3.1). Chaque fiche doit intégrer au minimum les éléments suivants :

- Numéro et détail de l'exigence ;
- Libellé exact de la vulnérabilité ou non-conformité constatée par l'organisme certificateur ;
- Réponse de l'opérateur.

Annexe III – Livrables de la certification annuelle.

Les éléments actualisables sont présentés en vert. Le rapport de la certification annuelle se compose, pour chaque agrément, des 9 livrables suivants,:

1. synthèse des rapports, avec mention des réserves ;
2. matrices des exigences ;
3. tests intrusifs internes et externes de la plate-forme ;
4. audit fonctionnel du capteur ;
5. analyse de l'architecture technique ;
6. audit de configuration des équipements de la plate-forme ;
7. audit des évolutions des différents logiciels de jeu ;
8. vérification du respect des exigences ;
9. annexes techniques.

Synthèse des rapports :

1. présentation du candidat opérateur ;
2. nombres de jour/homme consacrés à chaque point ;
3. dates des différentes prestations ;
4. synthèse stratégique des résultats obtenus par point ;
5. liste des réserves.
6. liste de l'ensemble des vulnérabilités et non-conformités constatées.

Matrice des exigences.

Audit fonctionnel et technique du capteur :

1. synthèse :
    a. synthèse de l'audit fonctionnel et technique,
    b. synthèse technique de l'audit intrusif,
    c. synthèse des non conformités, classées par criticité et impact,
    d. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;

2. analyse fonctionnelle et technique :
    a. présentation de la solution :
        i. mécanismes d'enregistrement des traces,
        ii. mécanismes de vérification et de filtrage des données,
        iii. mécanismes de sécurité du capteur ;
    b. analyse de code des fonctions les plus importantes du capteur.

Tests intrusifs externes et internes de la plate-forme de jeu

1. synthèse technique des tests intrusifs ;
2. synthèse des vulnérabilités, classées par criticité et impact ;
3. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;

4. rapport du test d'intrusion :
    a. analyse de risques techniques synthétique,
    b. déroulement linéaire du test d'intrusion, avec description explicite de la méthodologie employée pour détecter les vulnérabilités et les exploiter, le cas échéant,
    c. déroulement linéaire du test d'intrusion du capteur.

Analyse de l'architecture technique

1. synthèse technique de l'audit d'architecture ;
2. synthèse des vulnérabilités, classées par criticité et impact ;
3. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;
4. rapport d'analyse :
    a. présentation de l'architecture technique,
    b. analyse de l'architecture technique (matrices de flux, règles de filtrage…),
    c. analyse du cloisonnement,
    d. mécanismes d'administration.

Audit de configuration des équipements principaux des plate-formes

1. synthèse technique de l'audit des équipements ;
2. synthèse des vulnérabilités, classées par criticité et impact ;
3. synthèse des recommandations, classées par priorité et coût de mise en œuvre ;
4. rapport d'analyse : analyse des configurations au niveau système, réseau et applicatif.

Audit des évolutions des différents logiciels de jeu

1. synthèse technique de l'analyse ;
2. rapport d'analyse :
    a. liste des différents logiciels de jeux utilisés (clients et serveur),
    b. analyse des changements apportés.

Vérification du respect des exigences : rapport regroupant les différentes analyses n'ayant pas été abordées dans les précédents livrables.

Annexes techniques :

1. attestations éventuelles ;
2. documentations opérateur.

Les fiches d'anomalies sont transmises directement par l'opérateur à l'ARJEL ainsi qu'à l'organisme

certificateur. Ces fiches d'anomalies doivent reprendre l'intégralité des vulnérabilités et non conformités pointées par l'organisme certificateur (associées au contenu rédigé par l'organisme certificateur) et intégrer les différentes réponses de l'opérateur (cf. partie 3.1). Chaque fiche doit intégrer au minimum les éléments suivants :

- Numéro et détail de l'exigence ;
- Libellé exact de la vulnérabilité ou non-conformité constatée par l'organisme certificateur ;
- Réponse de l'opérateur.

Matrice des exigences de la certification unique à 6 mois du composant frontal
Version du 17 mars 2014

Notice	
Point de contrôle	Point de contrôle noté « En ». Remarque : la numérotation du point de contrôle est propre à ce document.
Référence	Référence au document (DET, Annexe au DET, voire Loi ou décret) et de la partie renseignant le point de contrôle. DET : dossier des exigences techniques http://www.arjel.fr/IMG/pdf/det.pdf ANN : annexe au dossier des exigences techniques http://www.arjel.fr/IMG/pdf/annexe.pdf
Libellé	Description du point de contrôle, selon les termes du document de référence.
Niveau de criticité	Niveau de criticité du point de contrôle : - le niveau de criticité 1 correspond essentiellement aux exigences liées à l'existence d'une documentation ou d'une procédure (ex : politique de sécurité, procédure de mise à jour, de durcissement d'un système, etc.) ; - le niveau de criticité 2 correspond essentiellement aux exigences pour lesquelles une non-conformité a un impact opérationnel : défaut d'application d'une procédure, défaut de respect des exigences opérationnelles de conformité et de sécurité définies par l'ARJEL, ou encore défaut de suivi des règles de bonnes pratiques en sécurité des systèmes d'information ; - le niveau de criticité 3 correspond aux exigences dont le non-respect est jugé très critique, le plus souvent en termes de conformité règlementaire, ou en termes de sécurité (sur un composant exposé et/ou manipulant des données critiques).
Éléments d'analyse	Éléments sur lesquels l'analyse s'appuie : 1. documents remis par l'opérateur, par exemple : - dossier de définition de la plate-forme d'hébergement du frontal, - documentation fonctionnelle et technique du logiciel capteur, - rapport de certification CSPN réalisé à l'occasion de la certification du coffre-fort, et la cible de sécurité de cette certification, - rapports d'audits de sécurité déjà réalisés par l'opérateur – en particulier si le capteur est intégré à la plate-forme de jeu – ou encore d'analyse de la maturité SSI de l'opérateur ; 2. audits réalisés par le certificateur, visant à comprendre et valider techniquement les points de contrôle, et apprécier les éléments déclaratifs décrits par l'opérateur dans sa documentation, en particulier : - l'audit applicatif intrusif du composant logiciel capteur. Ce rapport est noté « audit applicatif de type 'intrusif' de l'application capteur » dans la suite du document ; - l'audit de configuration de premier niveau de l'infrastructure d'hébergement du frontal. Ce rapport est noté « audit de configuration des plates-formes d'hébergement » dans la suite du document. Le niveau d'analyse demandé peut être précisé : « analyse de premier niveau » signifie qu'une analyse pragmatique et de bon sens est attendue. Au contraire, un « avis d'expert » sera plus technique et étayé (élément de configuration, extrait de code, etc.).
Commentaires	Précisions apportées par l'ARJEL, afin d'aider à la compréhension du point de contrôle ;
Rapports concernés	Références du ou des documents ainsi que des chapitres sur lesquels l'analyse a été effectuée, le cas échéant.
Conformité	Constat de l'analyse

Point de Contrôle	Référence		Libellé		Niveau de criticité	Éléments d'analyse	Commentaires	Rapports concernés	Conformité
Exigences organisationnelles									
			Procédures d'administration et d'exploitation						
			L'organisation mise en place pour gérer les systèmes d'information de l'opérateur doit s'appuyer sur une documentation et des procédures permettant de suivre ses évolutions. La documentation comporte :						
E1	DET	5.7.2.a 5.7.2.b		- la politique de sécurité, ou un document remplissant une fonction similaire ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E2	DET	5.7.2.b		- une description fonctionnelle de l'infrastructure d'hébergement du composant frontal, précisant les différents composants, leurs fonctions et les flux transitant par ces derniers.	**1**	Documentation remise par l'opérateur + avis d'expert.			
E3	DET	5.7.3.a	La documentation des infrastructures d'hébergements du composant frontal et de la plate-forme de jeu qui intègre un volet technique et procédural fait l'objet d'un dossier appelé « dossier de définition ».		**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E4	DET	5.7.3.d	L'opérateur sera responsable, sur toute la durée de validité de l'agrément, de la tenue à jour et de la cohérence de ce dossier. Chaque modification de l'un de ces dossiers devra faire l'objet d'une nouvelle remise de document à l'ARJEL ; L'opérateur doit mettre à jour le « dossier » de définition avec la liste des correctifs de sécurité appliqués sur les serveurs, et doit communiquer à l'ARJEL la version actualisée du document.		**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
			La documentation des infrastructures d'hébergement du composant frontal et de la plate-forme de jeu qui intègre un volet technique et procédural comporte :						
E5	DET	5.7.2.b		- une description de l'architecture, en termes de composants techniques, plan d'adressage et de nommage, de flux, en mentionnant les protocoles associés, sens d'établissement des connexions, règles de filtrage, etc. ;	**2**	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.			
E6	DET	5.7.2.b		- les spécifications techniques du système, en particulier les configurations à jour des équipements qui le compose ;	**2**	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.			
E7	DET	5.7.2.b		- la liste descriptive précise de tous les composants, avec le recensement d'éléments factuels, comme les versions des logiciels utilisés, les contrats de maintenance, les configurations et l'état des modifications effectuées, etc. ;	**2**	Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.			

E8	DET	5.7.2.b		- une liste de procédures d'exploitation, notamment : - procédures de gestion des journaux ; - procédures de gestion des alertes ; - procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.) ; - procédures de gestion des composants à mise à jour fréquente (anti-virus, systèmes de détection d'intrusion, le cas échéant) ; - procédures de mise à jour en cas d'édition d'un correctif de sécurité critique ; - procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent ; - procédures d'exploitation des composants du SI (serveurs, routeurs) ; - procédures d'exploitation des comptes et mots de passe ; - procédures de gestion des composants infogérés ; - procédures relative à la sécurité physique (gardiennage, etc.) ; - procédures de gestion des sauvegardes et des restaurations ; - procédures de veille technologique ; - procédures pour la télé-administration ; - procédures de gestion des tableaux de bord SSI.	**1**	Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.			
			Gestion de la disponibilité et des mises à jour						
E9	DET	5.7.3.c	L'opérateur met en œuvre des mécanismes de sécurité afin d'assurer une défense contre les attaques classiques sur IP et les protocoles associés, en particulier par rapport aux attaques en déni de service réseau.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E10	DET	5.7.3.f	- Au titre de la maintenance et du maintien en conditions de sécurité, l'opérateur suit les évolutions logicielles des éditeurs de façon à être en mesure de se procurer les correctifs de sécurité mis à disposition régulièrement. - L'opérateur surveille au moins les avis et les alertes d'un CERT, comme le CERTA (http://www.certa.ssi.gouv.fr) par exemple. - L'opérateur applique les correctifs de sécurité qui sont proposés par les éditeurs, dans les documents du CERT ou demandés explicitement par l'ARJEL, le cas échéant.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E11	DET	5.7.3.f	L'opérateur devra au moins prohiber l'utilisation sur ses plates-formes des systèmes et logiciels obsolètes référencés par le CERTA.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Si aucun correctif de sécurité n'est disponible auprès de l'éditeur, l'opérateur suit :						
E12	DET	5.7.3.d		- les recommandations de ce dernier ou d'un CERT, dans le cadre d'un contournement provisoire ;	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E13	DET	5.7.3.d		- si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, l'opérateur s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E14	DET	5.7.3.d	L'opérateur devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer à l'ARJEL la version actualisée du document.		**1**				
E15	DET	5.7.3.c	L'opérateur met en œuvre des mécanismes de sécurité afin d'assurer une défense contre les attaques classiques sur IP et les protocoles associés, en particulier par rapport aux attaques en déni de service réseau.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Authentification des accès d'administration						
			Les accès d'administration aux équipements du frontal doivent être protégés à l'aide des mécanismes suivants :						
E16	DET	5.7.3.e.2		- en priorité, une authentification par certificat X.509v3, par clef publique RSA ou par système à deux facteurs (dont un mot de passe à usage unique), si les applications et les systèmes le supportent ;	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E17	DET	5.7.3.e.2		- ou bien une authentification par mot de passe, avec des règles de composition et de renouvellement conforme aux bonnes pratiques recommandées par le CERTA, que l'opérateur détaillera ; ces mots de passe devront être employés dans le cas de protocoles d'authentification par défi/réponse ;	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.	Les authentifications en clair seront prohibées, et en l'absence de mode défi/réponse un chiffrement des communications sera obligatoire. La mesure doit permettre de prouver la robustesse des mots de passe		
E18	DET	5.7.3.e.2		- un contrôle d'accès basé sur les adresses IP est réalisé, le cas échéant.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Gestion des configurations						
E19	DET	5.7.3.f	À l'issue de la mise en œuvre d'un nouvel équipement ou de l'installation d'une nouvelle application, l'opérateur mettra à disposition de l'ARJEL la version à jour du dossier de définition incluant toutes les informations relatives à la configuration de ce nouvel élément.		**1**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E20	DET	5.7.3.f	Les composants systèmes, réseau et applicatifs mis en œuvre par l'opérateur devront avoir fait l'objet d'une minimalisation de leur configuration et d'un durcissement en termes de sécurité : restriction des applications exécutées au démarrage, limitation du nombre d'applications en écoute sur le réseau, désactivation des fonctionnalités inutiles voire dangereuse (interface d'administration de serveurs d'application), suppression des comptes et mots de passe constructeurs, etc.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E21	DET	5.7.3.f	Afin de détecter d'éventuelles erreurs de manipulation mais aussi le résultat d'attaques, l'intégrité des fichiers de configuration des équipements devra être vérifiée régulièrement. Cette vérification devra pouvoir être faîte sur demande de l'ARJEL, et un rapport de diagnostic devra pouvoir lui être transmis.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Gestion de la sécurité dans les cycles de développement						
E22	DET	5.7.3.g	L'opérateur devra gérer la sécurité à chaque étape du cycle de développement de ses systèmes, dans les phases de définition, de développement, d'exploitation et d'utilisation, puis de maintenance et d'évolution.		**2**	Documentation remise par l'opérateur.	Cette exigence couvre, outre la vérification de la procédure technique liée à cette transmission, le droit de l'opérateur de l'effectuer.		
E23	DET	5.7.3.g	L'opérateur devra contractualiser avec ses prestataires le respect d'un référentiel de développement sécurisé pour les projets dont il externaliserait la prise en charge.		**1**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
			Le référentiel de développement sécurisé devra en particulier aborder le problème de la validation des paramètres, notamment :						
E24	DET	5.7.3.g		- vérifier toutes les données transmises par l'utilisateur selon des critères de taille, type et caractères autorisés, et selon un mécanisme de liste blanche ;	**2**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E25	DET	5.7.3.g		- vérifier les données en entrée et en sortie ;	**2**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E26	DET	5.7.3.g		- utiliser une fonction de vérification des données identique et centralisée.	**2**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E27	DET	5.7.3.g	L'opérateur devra pouvoir transmettre à l'ARJEL l'ensemble de codes sources des logiciels de jeux utilisés sur ses plates-formes.		**3**	Documentation remise par l'opérateur.			
E28	DET	5.7.3.g	L'opérateur devra gérer la sécurité à chaque étape du cycle de développement de ses systèmes, dans les phases de définition, de développement, d'exploitation et d'utilisation, puis de maintenance et d'évolution.		**2**	Documentation remise par l'opérateur.	Cette exigence couvre, outre la vérification de la procédure technique liée à cette transmission, le droit de l'opérateur de l'effectuer.		
			Gestion des sauvegardes des données						

E29	DET	5.7.3.h	L'opérateur fournit les moyens de mettre en œuvre un service d'archivage afin d'assurer la conservation de l'ensemble de ses données de traitement, et en particulier celles stockées dans le coffre-fort du frontal.	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E30	DET	5.7.3.h	Ces sauvegardes sont mises à disposition de l'ARJEL par l'opérateur pour consultation et archivage.	**2**	Documentation remise par l'opérateur.			
E31	DET	5.7.3.h	Le type de support et le format de la sauvegarde sont indiqués pour permettre à l'ARJEL de vérifier l'exploitabilité de ces sauvegardes et de leurs contenus.	**3**	Documentation remise par l'opérateur.			
E32	DET	5.7.3.h	La durée de conservation des informations, définie par le code du commerce, doit être de 5 ans, suivant la fermeture du compte de jeu.	**3**	Documentation remise par l'opérateur.			
			Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :					
E33	DET	5.7.3.h	- être protégées en intégrité ;	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E34	DET	5.7.3.h	- être accessibles aux personnes autorisées seulement ;	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E35	DET	5.7.3.h	- pouvoir être relues et exploitées.	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E36	DET	5.7.3.h	Le niveau de protection des sauvegardes des archives doit être au moins équivalent au niveau de protection des archives : l'opérateur présentera dans sa réponse les mécanismes d'archivage ainsi que les moyens sécurisés de protection des archives qu'il est capable de mettre en œuvre.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			La précision de l'horloge par rapport à laquelle les systèmes d'information se synchronisent pour dater les événements journalisés ou archivés doit :					
E37	DET	5.7.3.h	- être inférieure à une seconde par rapport au temps UTC ; - la source de temps doit être fiable.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.	L'auditeur devra démontrer le respect de l'exigence		
E38	DET	5.7.3.h	Une totale intégrité des données et des traitements est requise pour l'ensemble des données sur le frontal.	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Gestion de la journalisation technique et fonctionnelle					
			L'opérateur doit maintenir, et pouvoir fournir à l'ARJEL, les journaux des traces techniques pour les évènements clé. Une première liste des événements concernés :					
E39	DET	5.7.3.k	- accès aux modules du frontal ; - opérations de maintenance effectuées ; - ouverture et fermeture de la prise de paris, mises poker, etc.	**2**	Documentation remise par l'opérateur.			
E40	DET	5.7.3.k	Si des personnes physiques sont à l'origine des évènements tracés : - la journalisation doit permettre d'établir un lien entre l'identifiant technique utilisé dans la trace et la personne physique responsable des actions ; - les évènements seront journalisés en s'appuyant sur une source de temps fiable.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E41	DET	5.7.3.k	Concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un package Linux, …). toutes les traces disponibles au niveau des équipements seront activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E42	DET	5.7.3.k	L'opérateur consolidera l'ensemble des traces issues de la journalisation technique des différents équipements (réseau, système, applicatifs et sécurité), par exemple via l'application et le protocole syslog.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E43	DET	5.7.3.k	Les traces de sécurité issues de la journalisation technique des plates-formes seront analysées périodiquement par l'opérateur afin d'identifier les anomalies éventuelles.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E44	DET	5.7.3.k	Les journaux techniques produits par les différents équipements doivent être conservés au minimum pendant trois mois en tant qu'archive.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E45	DET	5.7.3.k	L'opérateur pourra mettre à disposition de l'ARJEL ces journaux bruts produits par les différents équipements ou logiciels.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E46	DET	5.7.3.k	Les incidents ou les comportements anormaux pouvant avoir un impact sur la sécurité du service devront être traités et systématiquement faire l'objet d'une alerte et d'un compte-rendu écrit qui pourra être communiqué à l'ARJEL.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			L'opérateur doit maintenir, et pouvoir fournir à l'ARJEL, les journaux des traces techniques pour les évènements clé. Une première liste des événements concernés :					
E47	DET	5.7.3.k	- accès aux modules du frontal ; - opérations de maintenance effectuées ; - ouverture et fermeture de la prise de paris, mises poker, etc.	**2**	Documentation remise par l'opérateur.			
E48	DET	5.7.3.k	Si des personnes physiques sont à l'origine des évènements tracés : - la journalisation doit permettre d'établir un lien entre l'identifiant technique utilisé dans la trace et la personne physique responsable des actions ; - les évènements seront journalisés en s'appuyant sur une source de temps fiable.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E49	DET	5.7.3.k	Concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un package Linux, …). toutes les traces disponibles au niveau des équipements seront activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E50	DET	5.7.3.k	L'opérateur consolidera l'ensemble des traces issues de la journalisation technique des différents équipements (réseau, système, applicatifs et sécurité), par exemple via l'application et le protocole syslog.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Frontal					
E51	DET	4	L'opérateur devra mettre en place un site Internet dédié, exclusivement accessible par un nom de domaine de premier niveau comportant la terminaison .fr.	**3**	Documentation remise par l'opérateur (informations techniques sur le nom de domaine pleinement qualifié : Whois, résolutions DNS, etc. sur l'ensemble des noms de domaine déclarés auprès de l'ARJEL)			
E52	DET	4	Toutes les connexions à destination d'un site de l'opérateur ou d'une de ses filiales et issues d'une IP française ou d'un compte joueur dont l'adresse est en France devront être redirigées vers ce site.	**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
			Le frontal est un dispositif de recueil et d'archivage des données échangées entre joueur et la plateforme de l'opérateur à l'occasion des opérations de jeux. Ce dispositif est :					
E53	DET	4.1.1	- développé et exploité sous la responsabilité de l'opérateur ;	**2**	Documentation remise par l'opérateur (identification des prestataires : développeurs, exploitants, etc.).			
E54	DET	4.1.1	- installé sur un support situé en France métropolitaine.	**3**	Description de l'infrastructure d'hébergement. Cette exigence s'applique au coffre et au capteur.			
E55	DET	4.1.2	Tous les échanges entre un joueur réputé français et la plate-forme de jeu devront transiter par le frontal.					
			Les connexions provenant de joueurs réputés français doivent être redirigées vers le frontal qui se trouve en coupure de flux applicatif. La plateforme de jeu doit refuser ou rediriger vers son frontal français les requêtes suivantes :					
E56	DET	4.1.2	- avant authentification du joueur, si l'origine de la connexion est une adresse IP réputée française (pays d'attribution de l'adresse IP du terminal Internet depuis lequel il se connecte est la France dans la base RIPE NCC) ;	**3**	Audit de configuration de la plate-forme d'hébergement, en particulier la description des dispositifs techniques mis en place par l'opérateur côté frontal/plate-forme de jeu (ex : description du module de géolocalisation mis en place au niveau HTTP, ou encore au niveau DNS), étayée par des extraits de configuration (ex : module Apache de géolocalisation) et portion de code (redirection en post-authentification).			
E57	DET	4.1.2	- ou, après authentification du joueur, si le joueur a indiqué un domicile en France lors de l'ouverture de son compte de jeu.	**3**				
E58	Décret N° 2010-509	Art.6	L'opérateur doit permettre à l'ARJEL de se rendre, à tout moment, sur le site d'hébergement du support matériel d'archivage pour saisir l'ensemble ou un sous-ensemble des données qui y sont conservées. À cette fin, l'ARJEL informe au moins deux heures à l'avance le représentant de l'opérateur de son intention d'accéder à ce site et de l'heure à laquelle cet accès devra leur être donné.	**3**	Procédures mises en place par l'opérateur et l'hébergeur du frontal, le cas échéant, pour autoriser un tel accès.			
			Les échanges de données suivants devront être sécurisés afin d'en garantir l'authentification ainsi que la confidentialité :					

E59	DET	4.1.1		- les échanges entre le joueur et le frontal ;	**3**	Audit de configuration de la plate-forme d'hébergement, en particulier la description technique des protocoles de sécurité mis en place (ex : algorithmes, certficats X.509, le cas échéant, etc.).	Avis d'expert sur les interactions HTTP/HTTPS pour les applications Web, notamment pour l'accès au formulaire d'authentification, et la gestion des identifiants de session, etc.		
E60	DET	4.1.1		- les échanges entre les différents modules du frontal ; - les échanges entre le frontal et la plate-forme de jeux de l'opérateur ; - les échanges entre le frontal et la plate-forme de l'ARJEL.	**2**	Audit de configuration de la plate-forme d'hébergement, notamment le schéma d'architecture.	Description technique des flux et protocoles impliqués, en mentionnant les moyens de chiffrement/authenticité des flux (transport IPsec, SSL/TLS, ou colocation des équipements, par exemple) et d'authentification des parties mis en place.		
			Le frontal doit comporter des fonctionnalités de sécurité visant à le protéger des attaques par saturation, qu'elles agissent :						
E61	ANN	3.1.1		- au niveau transport, si ce composant termine les connexions TCP initiées par les clients : protection contre les dénis de service réseau, qui visent un épuisement de ressources TCP par des attaques de type SYN Flood, ou des attaques qui s'appuient sur un établissement complet de connexion TCP (Naphta, Sockstress, etc.) ;	**2**	Audit de configuration de la plate-forme d'hébergement, notamment la description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration, ou encore des procédures de gestion d'incident mises en place avec le fournisseur d'accès en amont, le cas échéant, par exemple.			
E62	ANN	3.1.1		- au niveau applicatif, avec l'envoi de multiples requêtes HTTP qui viseraient la saturation du frontal, qui constitue potentiellement un point de défaillance unique de l'architecture, afin de le protéger : - d'un épuisement de ressources (saturation des enregistrements temporairement mis en tampon et en attente d'un acquittement) ; - d'une saturation du coffre avec des enregistrements mal formés.	**2**	Audit de configuration de la plate-forme d'hébergement, audit applicatif de type 'intrusif' de l'application capteur, notamment la description des dispositifs techniques mis en place par l'opérateur appuyée par des éléments de configuration.			
			Frontal : coffre-fort						
E63	DET	4.1.1	Le coffre-fort doit détenir une certification de sécurité de premier niveau (CSPN) délivrée par l'ANSSI (http://www.ssi.gouv.fr).		**3**	L'absence de certification CSPN est rédhibitoire pour l'obtention de la certification du frontal.			
			La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des menaces :						
E64	DET	4.1.1		- le dépôt ou l'injection d'enregistrements non autorisés ;	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E65	DET	4.1.1		- l'altération d'enregistrements ;	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E66	DET	4.1.1		- le vol de données ;	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E67	DET	4.1.1		- le déni de service.	**3**	Rapport et cible de la certification ANSSI/CSPN.			
			La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des fonctions de sécurité :						
E68	DET	4.1.1		- l'authentification forte des utilisateurs et administrateurs ;	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E69	DET	4.1.1		- le chiffrement, la signature et l'horodatage des évènements ;	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E70	DET	4.1.1		- le chaînage des évènements.	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E71	DET	4.1.3	Toute suppression ou altération des données archivées, de manière malveillante ou non, doit pouvoir être identifiée par l'ARJEL.		**3**	Audit de configuration de la plate-forme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
			Quatre profils d'autorisation doivent pouvoir être définis :						
E72	DET	4.1.3		- profil « déposant » : profil attribué au module « capteur » du frontal de l'opérateur. Il permet uniquement d'écrire des traces dans le journal. Le module capteur du frontal s'authentifie à l'aide d'un certificat X.509v3 auprès de la partie coffre-fort avec une identité associée à ce profil ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E73	DET	4.1.3		- profil « lecteur » : profil attribué aux agents de l'ARJEL dotés des pouvoirs de contrôle et d'audit, qui permet l'extraction des données enregistrées, soit sur support amovible, soit via un dépôt de fichiers accessible à travers un service Web ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E74	DET	4.1.3		- profil « administrateur technique et opérationnel » : profil attribué au personnel technique de l'opérateur, responsable de l'administration et de la supervision technique du coffre-fort ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E75	DET	4.1.3		- profil « administrateur fonctionnel » : profil attribué aux personnes physiques de l'ARJEL ou désignées par l'ARJEL, qui peuvent définir des rôles et leur associer un certificat d'authentification. Cette opération est nécessaire à l'initialisation des coffres, puis lors des renouvellements ou des révocations des certificats.	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
			Les certificats associés au profil « lecteur » sont utilisés :						
E76	DET	4.1.3		- soit par des personnes physiques, pour les contrôles réalisés sur site, avec des biclefs RSA et un certificat X.509v3 d'authentification, par exemple conservé sur un support matériel (ex : carte à puce) fourni par l'opérateur ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E77	DET	4.1.3		- soit par des agents de collecte, pour les consultations réalisées à distance, avec une authentification fondée sur un certificat X.509v3 client SSL/TLS, dans le cadre de la négociation d'un tunnel SSL/TLS mutuellement authentifié.	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
			En termes de gestion des clefs de chiffrement, de signature, et d'horodatage :						
E78	DET	4.1.3		- les tailles de clefs doivent être conformes aux règles énoncées dans le référentiel général de sécurité de l'ANSSI (http://www.ssi.gouv.fr/) ;	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E79	DET	4.1.5		- la cryptographie mise en œuvre en termes de générateurs de nombres pseudo-aléatoires, fonctions de hachage, algorithmes symétriques et asymétriques doit respecter les règles de bonnes pratiques spécifiées dans le référentiel général de sécurité de l'ANSSI (http://www.ssi.gouv.fr/);	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E80	DET	4.1.3		- un HSM est utilisé pour les opérations de signature ; le biclef de signature peut être soit injecté dans le HSM, soit injecté dans ce dernier	**3**	Rapport et cible de la certification ANSSI/CSPN.	Dans l'hypothèse où le biclef ferait l'objet d'une injection, un avis d'expert est attendu sur la sécurité de la méthode de génération du biclef hors HSM.		
E81	DET	4.1.3		- les données chiffrées le sont au moyen de la clef publique du certificat transmis par l'ARJEL : seule l'ARJEL peut déchiffrer le contenu des données archivées. Remarque : les opérations de chiffrement des données peuvent indifféremment être réalisées par des moyens matériels ou logiciels.	**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E82	DET	4.1.5	En termes de stockage des traces du coffre-fort, le coffre-fort met en œuvre une ségrégation entre l'espace de stockage destiné aux données de son administration et celui ou ceux destinés aux données de jeu tracées : en effet, dans le cadre d'un coffre mutualisé entre plusieurs agréments, chaque agrément doit faire l'objet d'un espace de stockage spécifique. Cette ségrégation des espaces de stockage doit, a fortiori, être implantée dans le cadre d'une mutualisation inter-opérateurs, le cas échéant.		**3**	Rapport et cible de la certification ANSSI/CSPN.			
			La sécurité physique des accès au coffre sera assurée par :						
E83	DET	4.1.3		- l'hébergement dans un emplacement protégé ;	**2**	Audit de configuration de la plate-forme d'hébergement : une analyse de premier niveau de la sécurité physique de			
E84	DET	4.1.3		- la mise en place d'un contrôle d'accès ;	**2**				

E85	DET	4.1.3		- la mise en place de procédures de suivi des interventions (toutes les opérations de configuration du coffre-fort doivent notamment faire l'objet d'un suivi).	**2**	l'infrastructure d'hébergement est attendue.			
E86	DET	4.1.6.a		- la mise en oeuvre de protections physiques	**2**	La méthode de scellement du coffre doit faire l'objet d'une procédure qui, quelle que soit la méthode, doit être probante et garantir l'inocuité d'une intervention qui aurait pour conséquence de rompre ledit dispositif.			
			Frontal : capteur						
E87	ANN	3.1.1	Le capteur doit implanter des mécanismes de défense afin de protéger sa mémoire tampon et éviter toute saturation à destination de cette dernière ou du coffre lui-même.		**2**	Audit applicatif de type 'intrusif' de l'application capteur. Documentation remise par l'opérateur.			
			Le module capteur doit :						
E88	ANN	3.1.1		- être authentifié par certificat auprès du coffre, au niveau duquel une session avec le profil « déposant » est ouverte ;	**2**	Documentation remise par l'opérateur, appuyée par des éléments issus de l'audit applicatif de type 'intrusif' de l'application capteur.	L'analyse doit être étayée par des extraits de code du capteur		
E89	ANN	3.1.1		- attendre du coffre un acquittement, sous la forme d'une preuve du dépôt.	**2**	Documentation remise par l'opérateur, appuyée par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur. Voir les exigences dédiées aux fonctions de création et de stockage des traces.			
E90	DET	4.1.5	L'ensemble des composants doivent être synchronisés en temps, auprès d'une source de temps fiable.		**3**	Audit de configuration de la plate-forme d'hébergement.			
			Frontal : fonctions de création et de stockage des traces						
			La fonction de création de traces du capteur doit respecter les principes suivants :						
E91	DET	4.1.4		- la fonction de création de traces correspond à l'écriture de données liées à un évènement de jeu ou à un compte joueur dans le module coffre-fort du frontal intercepte voire relaie le flux applicatif entre le joueur et l'opérateur. Elle doit donc être réalisée au niveau applicatif : - soit par interception protocolaire du flux HTTP ; - soit par insertion dans la logique de présentation de l'application.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E92	DET	4.1.4		- la fonction de création de traces est implantée en amont de la logique de jeu : elle s'insère en coupure dans la chaîne de traitement des requêtes émises par le joueur vers la plateforme de jeux.	**3**				
E93	DET	4.1.4		- le frontal doit offrir une architecture dotée d'une très haute disponibilité avec redondance de mécanismes afin de strictement limiter les incidents potentiels de stockage.	**3**				
E94	DET	4.1.4		- le principe d'une annulation d'un jeu concerné par un incident de stockage d'un des évènements doit être retenu.	**2**				
			La fonction de création de traces d'un événement doit :						
E95	ANN	3.1.1		- être invoquée suite à une requête émise par le joueur (si celle-ci requiert un enregistrement). Cette requête peut résulter : - d'une action du joueur, à son initiative, comme une prise de pari ; - d'un acquittement par le joueur, suite à message transmis à l'initiative de la plate-forme, comme l'annonce d'un gain sur un pari.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E96	ANN	3.1.1		- reposer sur un module applicatif à état qui respecte la cinématique de création décrite dans le schéma 3.1.1 de l'annexe du DET, et en particulier donner lieu à un enregistrement temporaire, conservé au niveau du capteur dans une mémoire tampon ou un dispositif de stockage temporaire équivalent (ex: base de données, par exemple), avant toute transmission au niveau du coffre et dans l'attente d'un acquittement de la plate-forme de jeux validant la bonne et due forme de cet événement.	**3**	Le respect de mode de fonctionnement à état assure que les évènements transmis au coffre sont générés à l'initiative du joueur (action ou acquittement), mais sont validés, avant stockage au coffre, par la plate-forme.	Tout écart par rapport à ce mode de fonctionnement doit être techniquement justifié (ex : évènements POPARTIE générés par la plate-forme de jeu, et transmis pour acquittement au joueur avant stockage). Une analyse technique de la sécurité du processus de validation des évènements par le capteur est attendue, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur. Un mode de fonctionnement dans lequel les données transmises par le joueur seraient directement journalisées par le coffre est rédhibitoire pour la certification du frontal. Idem pour des données transmises directement de la plate-forme de jeu vers le coffre, sans acquittement préalable par le joueur.		
E97	ANN	3.1.1		- gérer un acquittement de la plate-forme de jeux, afin de limiter les risques d'attaques qui viseraient à saturer le coffre d'évènements aléatoires, ou à enregistrer des évènements falsifiés générés par un joueur malveillant.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E98	ANN	3.1.1		- en cas d'acquittement négatif de la part de la plate-forme de jeux, l'évènement pré-enregistré au niveau du capteur doit être détruit. Une erreur doit être générée et faire l'objet d'un message dans la journalisation technique du capteur.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E99	ANN	3.1.1		- en cas d'acquittement positif de la part de la plate-forme de jeux, l'évènement présent en mémoire tampon au niveau du capteur peut être transformé au format exigé par l'ARJEL, pour son stockage par le coffre.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E100	ANN	3.1.1		- gérer les cas d'acquittements négatifs de la part du coffre, en cas de défaillance d'enregistrement.	**2**		Des mécanismes de reprise sur erreur peuvent être implantés au niveau du capteur, par exemple par des tentatives de retransmission au coffre d'un l'évènement.		

E101	ANN	3.1.1		- garantir l'enregistrement d'un évènement de jeu au niveau du coffre, sous peine d'annulation de l'opération de jeu.	**2**	Cette exigence repose, dans le DET, sur un fonctionnement synchrone entre capteurs et coffres. Le capteur, dans ce modèle, doit attendre un acquittement positif du coffre avant de poursuivre la transaction.	Dans la pratique : - l'introduction d'un traitement par lots, le cas échéant, proscrit un fonctionnement synchrone au sens strict, - l'approbation de l'utilisation de mécanismes basés sur des files d'attente entre capteurs et coffres proscrit également ce mode de fonctionnement. Il est donc notamment attendu un avis d'expert technique sur : - le synchronisme entre le capteur et le mécanisme de dépôt au coffre, en décrivant files d'attente, mécanismes de détection et de reprise sur erreur (ex : retransmission par le capteur), - la redondance et la fiabilité du dispositif assurant le traitement des évènements entre leur émission par le capteur, et leur stockage *in fine* par le coffre (ex : analyse du mécanisme de file d'attente de type ActiveMQ, par exemple).		
			Le stockage des données consiste en les étapes suivantes :						
E102	DET	4.1.5		- l'établissement d'un canal sécurisé, suite à l'authentification mutuelle du déposant avec le coffre, via une session TLS mutuellement authentifiée par certificat X.509v3 ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E103	DET	4.1.5		- la vérification de l'habilitation du profil à déposer des traces ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.	- l'approbation de l'utilisation de mécanismes basés sur des files d'attente entre capteurs et coffres proscrit également ce mode de fonctionnement.		
E104	DET	4.1.5		- le chaînage avec la trace précédente, en liant l'empreinte des données à une empreinte de la signature de la trace précédente, et en incluant l'identifiant d'évènement unique à l'opérateur ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E105	DET	4.1.5		- le calcul de l'empreinte, à l'aide d'une fonction de hachage. L'empreinte ne doit pas être calculée au moment de l'ajout, mais être conservée en mémoire depuis l'opération précédente ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E106	DET	4.1.5		- le scellement des données, par signature horodatée incluant l'élément de chaînage pour en garantir l'intégrité, et les lier à une heure précise ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E107	ANN	1.1.5		- l'horodatage, qui doit être effectué sur l'évènement **(**ou le lot d'évènements**)** en clair.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
			Concernant les opérations de signature et de chiffrement :						
E108	DET	4.1.5		- le format de signature est XADES-T avec un jeton d'horodatage RFC 3161.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.	Un autre format de signature peut être implanté, à condition d'être justifié.		
E109	DET	4.1.5		- le chiffrement des données est réalisé au moyen de la clé publique de l'ARJEL pour en assurer la confidentialité.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.	La méthode de chiffrement pourra faire intervenir un algorithme de chiffrement symétrique, suivant des opérations qui seront précisément décrites.		
			Concernant le traitement par lots :						
E110	ANN	1.1.5		- le traitement par lot doit être paramétrable pour une durée ou un nombre maximal d'évènements.	**1**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E111	ANN	1.1.5		- la granularité du traitement par lot doit être l'évènement.	**1**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
			Frontal : fonctions d'accès aux traces						
			L'opérateur agréé doit fournir les éléments suivants pour chaque agrément :						
E112	DET	4.1.6		- un mécanisme d'accès aux données permettant la saisie des données sur site (copie de tout ou partie du coffre fort) ;	**3**	Documentation remise par l'opérateur.			
E113	DET	4.1.6		- un mécanisme d'accès aux données permettant l'interrogation des données à distance, par l'intermédiaire d'un outil de collecte ;	**3**	Documentation remise par l'opérateur.			
E114	DET	4.1.6		- un outil de validation des données du frontal et d'extraction des traces des opérations de jeu utilisable sur le site du frontal, et dans les laboratoires de l'ARJEL (mode hors-ligne).	**3**	Documentation remise par l'opérateur.			
			L'architecture de la partie coffre-fort du frontal doit distinguer :						
E115	DET	4.1.6		- un espace de stockage des données situé dans une zone réseau sécurisée ;	**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.			
E116	DET	4.1.6		- une couche d'accès à l'espace de stockage accessible.	**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.			
E117	DET	4.1.6.a	Les données stockées dans le coffre doivent être en permanence accessibles à distance, depuis les locaux de l'ARJEL, *i.e.* depuis une ou plusieurs adresses IP identifiées.		**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E118	DET	4.1.6.a	L'extraction du coffre doit pouvoir se faire sur une tranche de données, correspondant à une période d'activité ou une tranche d'identifiants d'évènements avec l'outil de collecte à distance mis à disposition par l'opérateur.		**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E119	DET	4.1.6	La couche d'accès à l'espace de stockage doit elle-même être sécurisée, aux niveaux applicatif et réseau, vis-à-vis de l'extérieur, notamment contre les attaques de déni de service, et les accès autres que ceux initiés par l'ARJEL.		**2**	Audit de configuration de la plate-forme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur + avis d'expert.			
			La couche d'accès expose un service web doté des deux principales interfaces suivantes :						
E120	DET	4.1.6		- une interface de consultation : elle permet l'extraction d'une trace ou d'un ensemble de traces à partir d'une date ou d'une tranche caractérisée par une date de début et une date de fin. À une même date peuvent correspondre aucun, un ou plusieurs évènements ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E121	DET	4.1.6		- une interface de synchronisation : elle permet l'extraction d'une trace et ou d'un ensemble des traces à partir de l'identifiant d'un évènement ou d'une tranche d'évènements.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E122	DET	4.1.6	Les données doivent rester accessibles sur site sur toute la durée de conservation exigée par la loi (article 10 du Décret n° 2010-509 du 18 mai 2010).		**3**	Documentation remise par l'opérateur.			
E123	DET	4.1.6	Les données accessibles à distance doivent couvrir au moins les 12 derniers mois d'opération (période glissante).		**3**	Documentation remise par l'opérateur.			
			L'outil réalisé par l'opérateur doit permettre :						
E124	ANN	3.1.3		- d'interroger à distance le coffre de l'opérateur pour télécharger les traces demandées (outil de collecte) ;	**3**	Documentation remise par l'opérateur.			
E125	ANN	3.1.3		- d'extraire les traces ainsi téléchargées pour ensuite les déchiffrer et vérifier l'intégrité des données (outil d'extraction et de validation). Cette extraction doit pouvoir être réalisée hors-ligne.	**3**	Documentation remise par l'opérateur.			
			L'outil doit implanter :						
E126	ANN	3.1.3.c		- l'interface WSDL définie par l'ARJEL, ou proposer une interface d'interrogation équivalente notamment basée sur l'identifiant d'opérateur, de coffre, sur l'agrément, et une tranche d'évènements ou de dates ;	**1**	Documentation remise par l'opérateur.			
E127	ANN	3.1.3		- les options en ligne de commande décrites dans la partie 3.1.3 de l'annexe au DET (fonctionnalités d'interrogation à distance) ;	**1**	Documentation remise par l'opérateur.			
E128	ANN	3.1.3		- le protocole TLS v1.1 au niveau du protocole de transport, et si possible, le triple d'algorithmes DHE-RSA-AES256-SHA ;	**2**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.			

E129	ANN	3.1.3		- des algorithmes cryptographiques manipulant des clefs dont la taille doivent être conformes aux règles énoncées dans le Référentiel général de sécurité disponible sur le site de l'ANSSI.	**3**	Documentation remise par l'opérateur.			
			L'accès réseau de l'accès à distance doit :						
E130	ANN	3.1.3		- faire l'objet d'un filtrage implanté sous la forme d'une liste blanche au niveau d'un équipement de sécurité périmétrique de type pare-feu ;	**2**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.	Un autre format de signature peut être implanté, à condition d'être justifié.		
E131	ANN	3.1.3		- faire l'objet d'une journalisation, et l'objet de procédures de traitement d'incident, le cas échéant.	**2**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.			
E132	ANN	3.1.3.a	L'outil d'extraction et de validation des traces doit implanter les options décrites dans la partie 3.1.3.a de l'annexe au DET (fonctionnalités d'extraction des traces et de vérification).		**1**	Documentation remise par l'opérateur.			
			Évènements XML : généralités						
			Les enregistrements XML sont :						
E133	ANN	1.1.1		- encodés au format UTF-8. On veillera en particulier au respect des caractères accentués (é, è, à) ;	**3**	Audit de code	L'analyse devra démontrer l'usage de filtres dans le code source		
E134	ANN	1.1.1		- conformes à la norme XML (en particulier en termes d'encodage des entités XML) ;	**3**				
E135	ANN	1.1.1		- conformes au schéma XSD publié par l'ARJEL ;	**3**				
E136	ANN	1.3		- filtrés, en termes de contenu, conformément aux expressions régulières (facette *pattern*) décrites dans le schéma XSD ;	**3**				
E137	ANN	1.3		- filtrés, en termes de contenu, afin de prévenir des attaques web classiques par injection (injections SQL, XPath, voire XSS, en complément d'un encodage des sorties par entités HTML, par exemple, etc.) ;	**3**				

Matrice des exigences de la certification annuelle
Version du 17 mars 2014

Notice	
Point de contrôle	Point de contrôle noté « E**n** ». Remarque : la numérotation du point de contrôle est propre à ce document.
Référence	Référence au document (DET, Annexe au DET, voire Loi ou décret) et de la partie renseignant le point de contrôle. DET : dossier des exigences techniques http://www.arjel.fr/IMG/pdf/det.pdf ANN : annexe au dossier des exigences techniques http://www.arjel.fr/IMG/pdf/annexe.pdf
Libellé	Description du point de contrôle, selon les termes du document de référence.
Niveau de criticité	Niveau de criticité du point de contrôle : - le niveau de criticité 1 correspond essentiellement aux exigences liées à l'existence d'une documentation ou d'une procédure (ex : politique de sécurité, procédure de mise à jour, de durcissement d'un système, etc.) ; - le niveau de criticité 2 correspond essentiellement aux exigences pour lesquelles une non-conformité a un impact opérationnel : défaut d'application d'une procédure, défaut de respect des exigences opérationnelles de conformité et de sécurité définies par l'ARJEL, ou encore défaut de suivi des règles de bonnes pratiques en sécurité des systèmes d'information ; - le niveau de criticité 3 correspond aux exigences dont le non-respect est jugé très critique, le plus souvent en termes de conformité règlementaire, ou en termes de sécurité (sur un composant exposé et/ou manipulant des données critiques).
Éléments d'analyse	Éléments sur lesquels l'analyse s'appuie : 1. documents remis par l'opérateur, par exemple : - dossier de définition, mis à jour, de la plate-forme d'hébergement du frontal et de la plate-forme de jeu, - documentation fonctionnelle et technique actualisée du logiciel capteur et de la plate-forme de jeu, - rapport de certification initiale à 6 mois du composant frontal , - rapports d'homologation effectués sur les logiciels de jeu, - rapports d'audits de sécurité réalisés par l'opérateur indépendamment des certifications prévues par la réglementation, - attestation(s) de d'absence de modification d'un composant (ex: capteur) ; 2. audits, réalisés par le certificateur, visant à comprendre et valider techniquement les points de contrôle, et d'apprécier les éléments déclaratifs décrits par l'opérateur dans sa documentation, en particulier : - les rapports d'audit de configuration de premier niveau de l'infrastructure d'hébergement du frontal et de la plate-forme de jeu. Ces rapports sont notés « audits de configuration des plates-formes d'hébergement » dans la suite du document ; - les rapports d'audit applicatif qui portent sur les composants logiciels de la plate-forme de jeu qui ne font pas l'objet d'homologation. Ces rapports sont notés « audits applicatif » dans la suite du document ; Le niveau d'analyse demandé peut être précisé : « analyse de premier niveau » signifie qu'une analyse pragmatique et de bon sens est attendue. Au contraire, un « avis d'expert » sera plus approfondi, technique – si le sujet s'y prête – et étayé. La certification annuelle repose sur un socle d'analyses obligatoires, pouvant faire l'objet d'une actualisation. Le guide méthodologique de la certification, pour la partie technique, indique les analyses pour lesquelles cette actualisation peut être réalisée.
Commentaires	Précisions apportées par l'ARJEL, afin d'aider à la compréhension du point de contrôle ;
Rapports concernés	Référence du ou des documents ainsi que des chapitres sur lesquels l'analyse a été effectuée, le cas échéant.
Conformité	Constat de l'analyse

Point de Contrôle	Référence		Libellé	Niveau de criticité	Éléments d'analyse	Commentaires	Rapports concernés	Conformité
Exigences organisationnelles								
			Suivi des audits de sécurité, certifications et homologations					
E1	DET	5	L'ARJEL réalisera dans le cadre de sa mission générale de contrôle des audits de sécurité afin de vérifier les niveaux de maturité SSI des opérateurs ainsi que les niveaux de sécurité atteints par les frontaux et les plates-formes de jeux. Un accès au site ainsi qu'à l'ensemble des équipements et des données de la ou des plates-formes de jeux devra être accordé à l'ARJEL ou aux organismes mandatés.	**3**	Documentation remise par l'opérateur. Audit de configuration des plates-formes d'hébergement.	L'opérateur devra notamment donner aux certificateurs l'ensemble des accès et éléments de configuration requis par ce dernier afin qu'il puisse procéder aux contrôles attendus dans le cadre de sa mission d'audit.		
E2	DET	5.1	L'opérateur devra corriger les éventuelles anomalies majeures constatées à l'issue des audits de sécurité. Si aucune mesure de sécurité ne permet de les corriger directement, l'opérateur devra proposer des mesures de contournement provisoire afin d'éviter l'exploitation de ces vulnérabilités majeures. Le plan d'action associé et établi par l'opérateur devra être communiqué à l'ARJEL.	**3**	Documentation remise par l'opérateur, notamment : - rapports d'homologation des logiciels de jeu ; - rapports d'audit de configuration réalisés dans le cadre de la certification initiale à 6 mois du composant frontale ou dans le cadre des certifications annuelles antérieures, le cas échéant ; - rapports d'audits de sécurité effectués sur les systèmes d'information de l'opérateur, qu'ils soient réalisés par l'ARJEL ou un organisme mandaté par l'ARJEL.	Il s'agira de s'assurer que les recommandations les plus pertinentes sont bien appliquées.		
E3	DET	5.1	L'opérateur devra informer l'ARJEL de la mise en place d'une nouvelle technologie au sein de sa plate-forme.	**2**	Documentation remise par l'opérateur.	L'opérateur devra notamment présenter au certificateur la liste des changements effectués au niveau de ses systèmes d'information (capteur + plates-formes de jeu, aussi bien au niveau des logiciels que des infrastructures) et les éléments communiqués à l'ARJEL, depuis le dépôt de la demande d'agrément ou la dernière certification annuelle effectuée, le cas échéant.		
E4	DET	5.1	L'opérateur devra communiquer à l'ARJEL les résultats des audits de sécurité réalisés sur ses plates-formes de jeux, le cas échéant, par des organismes tiers.	**1**				
E5	DET	5.2	Les nouveaux logiciels de jeu seront systématiquement homologués avant mise en exploitation ;	**3**	Documentation remise par l'opérateur.	L'opérateur devra lister les versions des logiciels de jeu qu'il emploie (côté client comme côté serveur), et les rapports d'homologations correspondants. Cette exigence inclut notamment les éventuels logiciels clients déployés sur *smartphones* ou les interfaces correspondantes côté serveur. Un avis d'expert est attendu de la part du certificateur sur les homologations réalisées au regard de l'historique des modifications apportées aux logiciels, côté client comme côté serveur.		
			Politique et schéma directeur en sécurité des systèmes d'information de l'opérateur					

E6	DET	5.7.2.a	L'opérateur devra posséder un schéma directeur en sécurité des systèmes d'information, ou un document équivalent. Il en précisera la date de son début d'application, et la périodicité de ses mises à jour. Il précisera également s'il est intégré dans le schéma directeur informatique et en fournira la dernière version et, si possible, la version précédente.		**1**	Documentation remise par l'opérateur + analyse de premier niveau.	L'analyse devra plus généralement porter sur la plate-forme d'hébergement du frontal et la plate-forme de jeu.		
E7	DET	5.7.2.a	l'opérateur devra posséder une politique de sécurité des systèmes d'information. Si un tel document n'existe pas, il indiquera, si un ou des documents remplissent une fonction similaire. Cette politique de sécurité devra aborder les sujets suivants :		**1**				
E8	DET	5.7.2.a	- des éléments stratégiques :	- le périmètre d'application de la politique de sécurité, par exemple en termes de domaines d'activités ou de systèmes d'information ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E9	DET	5.7.2.a		- les enjeux et orientations stratégiques, à travers la formalisation des enjeux liés au périmètre précédemment défini ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E10	DET	5.7.2.a		- les aspects légaux et réglementaires liés au périmètre d'application de la politique de sécurité ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E11	DET	5.7.2.a		- une échelle de besoins qui comportera une pondération et des valeurs de référence selon les critères de sécurité choisis, ainsi qu'une liste d'impacts enrichis d'exemples ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E12	DET	5.7.2.a		- une description des besoins de sécurité des domaines d'activité de l'opérateur, selon l'échelle de besoins présentée dans la partie précédente ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E13	DET	5.7.2.a		- une analyse des menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications.	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E14	DET	5.7.2.a	- de règles de sécurité, classées par thème :	- organisation: organisation de la SSI, gestion des risques, sécurité et cycle de vie, assurance et certification, évolution de la PSSI ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E15	DET	5.7.2.a		- mise en oeuvre : aspects humains, plan de secours, gestion des incidents, sensibilisation et formation, exploitation, sécurité physique ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E16	DET	5.7.2.a		- technique : identification / authentification, contrôle d'accès logique, journalisation, chiffrement.	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E17	DET	5.7.2.a	L'opérateur devra posséder des déclinaisons techniques détaillées des éléments exigés par sa politique de sécurité. Elles feront faire le lien entre la politique de sécurité et toutes les procédures liées aux systèmes d'information, en établissant des moyens de sécurisation et du suivi de ces moyens dans le temps. Ces moyens seront aussi bien organisationnels que techniques.		**2**	Documentation remise par l'opérateur + analyse de premier niveau.			
E18	DET	5.7.2.a	L'opérateur devra imposer des exigences de sécurité aux divers sous-traitants avec lesquels des relations contractuelles sont établies, il les fournira si possible.		**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
			Procédures d'administration et d'exploitation						
			L'organisation mise en place pour gérer les systèmes d'information de l'opérateur doit s'appuyer sur une documentation et des procédures permettant de suivre ses évolutions. La documentation comporte :						
E19	DET	5.7.2.a 5.7.2.b		- la politique de sécurité, ou un document remplissant une fonction similaire ;	**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E20	DET	5.7.2.b		- une description fonctionnelle de l'infrastructure d'hébergement du composant frontal, précisant les différents composants, leurs fonctions et les flux transitant par ces derniers.	**1**	Documentation remise par l'opérateur + avis d'expert.			
E21	DET	5.7.3.a	La documentation des infrastructures d'hébergements du composant frontal et de la plate-forme de jeu qui intègre un volet technique et procédural fait l'objet d'un dossier appelé « dossier de définition ».		**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
E22	DET	5.7.3.d	L'opérateur sera responsable, sur toute la durée de validité de l'agrément, de la tenue à jour et de la cohérence de ce dossier. Chaque modification de l'un de ces dossiers devra faire l'objet d'une nouvelle remise de document à l'ARJEL ; L'opérateur doit mettre à jour le « dossier » de définition avec la liste des correctifs de sécurité appliqués sur les serveurs, et doit communiquer à l'ARJEL la version actualisée du document.		**1**	Documentation remise par l'opérateur + analyse de premier niveau.			
			La documentation des infrastructures d'hébergement du composant frontal et de la plate-forme de jeu qui intègre un volet technique et procédural comporte :						
E23	DET	5.7.2.b		- une description de l'architecture, en termes de composants techniques, plan d'adressage et de nommage, de flux, en mentionnant les protocoles associés, sens d'établissement des connexions, règles de filtrage, etc. ;	**2**	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.			
E24	DET	5.7.2.b		- les spécifications techniques du système, en particulier les configurations à jour des équipements qui le compose ;	**2**	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.			
E25	DET	5.7.2.b		- la liste descriptive précise de tous les composants, avec le recensement d'éléments factuels, comme les versions des logiciels utilisés, les contrats de maintenance, les configurations et l'état des modifications effectuées, etc. ;	**2**	Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.			
E26	DET	5.7.2.b		- une liste de procédures d'exploitation, notamment : - procédures de gestion des journaux ; - procédures de gestion des alertes ; - procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.) ; - procédures de gestion des composants à mise à jour fréquente (anti-virus, systèmes de détection d'intrusion, le cas échéant) ; - procédures de mise à jour en cas d'édition d'un correctif de sécurité critique ; - procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent ; - procédures d'exploitation des composants du SI (serveurs, routeurs) ; - procédures d'exploitation des comptes et mots de passe ; - procédures de gestion des composants infogérés ; - procédures relative à la sécurité physique (gardiennage, etc.) ; - procédures de gestion des sauvegardes et des restaurations ; - procédures de veille technologique ; - procédures pour la télé-administration ; - procédures de gestion des tableaux de bord SSI.	**1**	Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.			
			Architecture réseau						
E27	DET	5.7.3.b	Les systèmes d'information de l'opérateur devront faire l'objet d'une segmentation et d'un filtrage réseau en accord avec le principe de défense en profondeur, notamment au niveau des réseaux de services, d'administration et de supervision des plates-formes. Ce cloisonnement réseau sera conforme aux descriptions fonctionnelles et techniques décrites dans la partie « description générale des systèmes d'information ».		**2**	Documentation remise par l'opérateur +avis d'expert	Un schéma de niveau 3 doit impérativement être réalisé par le certificateur. Ce schéma devra faire apparaitre les adresses IP des machines les plus importantes.		
			L'opérateur assurera un cloisonnement du réseau, mis en oeuvre à l'aide de mécanismes de filtrage de niveau 3 au minimum, au moins entre les zones suivantes :						

E28	DET	5.7.3.b		- les zones dédiées aux serveurs, avec un cloisonnement supplémentaire en fonction du niveau de sensibilité identifié pour chacun par la politique de sécurité : . les serveurs métiers (serveurs d'applications, systèmes de gestion de base de données), . les serveurs d'infrastructure (serveurs d'authentification, serveurs de messagerie, serveurs de fichiers, serveurs de distribution de logiciels), . les équipements d'infrastructure réseau (routeurs, commutateurs), . les serveurs de tests, de développement et de préproduction ;	**2**	- Documentation remise par l'opérateur, en particulier : . les rapports d'audits de configuration des plates-formes d'hébergement réalisés dans le cadre de la vérification initiale de la plate-forme de jeu, . les rapports d'audits de configuration de la certification à 6 mois du composant frontal, . les rapports d'audit de configuration des certifications annuelles antérieures, le cas échéant ; - Audit de configuration des plates-formes d'hébergement.			
E29	DET	5.7.3.b		- la zone des équipements dédiés à la l'administration, l'exploitation et la supervision du système d'information. Cette zone qui héberge notamment les postes de travail des administrateurs et les serveurs de supervision devra faire l'objet d'une attention particulière compte tenu des accès privilégiés qu'ils sont susceptibles d'accorder sur les ressources les plus critiques du SI ;	**2**		Le filtrage de ces interfaces d'administration doit s'effectuer au niveau 3 (IP) et non pas au niveau 7 (applicatif)		
E30	DET	5.7.3.b		- la ou les zones dédiées aux postes de travail des utilisateurs, le cas échéant, avec un découpage supplémentaire dont la granularité pourra varier selon les missions des différents services métiers et la criticité de l'information dont ils ont la responsabilité.	**2**				
E31	DET	5.7.3.b	La politique de filtrage réseau adoptée devra respecter le principe du moindre privilège : les règles de filtrage seront élaborées suivant un principe de liste blanche.		**2**		L'analyse devra prendre en compte le filtrage en entrée et en sortie		
			Gestion de la disponibilité et des mises à jour						
E32	DET	5.7.3.c	L'opérateur met en œuvre des mécanismes de sécurité afin d'assurer une défense contre les attaques classiques sur IP et les protocoles associés, en particulier par rapport aux attaques en déni de service réseau.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E33	DET	5.7.3.f	- Au titre de la maintenance et du maintien en conditions de sécurité, l'opérateur suit les évolutions logicielles des éditeurs de façon à être en mesure de se procurer les correctifs de sécurité mis à disposition régulièrement. - L'opérateur surveille au moins les avis et les alertes d'un CERT, comme le CERTA (http://www.certa.ssi.gouv.fr) par exemple. - L'opérateur applique les correctifs de sécurité qui sont proposés par les éditeurs, dans les documents du CERT ou demandés explicitement par l'ARJEL, le cas échéant.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E34	DET	5.7.3.f	L'opérateur devra au moins prohiber l'utilisation sur ses plates-formes des systèmes et logiciels obsolètes référencés par le CERTA.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Si aucun correctif de sécurité n'est disponible auprès de l'éditeur, l'opérateur suit :						
E35	DET	5.7.3.d		- les recommandations de ce dernier ou d'un CERT, dans le cadre d'un contournement provisoire ;	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E36	DET	5.7.3.d		- si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, l'opérateur s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E37	DET	5.7.3.d	L'opérateur devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer à l'ARJEL la version actualisée du document.		**1**				
			Authentification des accès d'administration						
E38	DET	5.7.3.e.1	L'intégralité des échanges de données devra être sécurisée à l'aide de procédés cryptographiques permettant de garantir l'authentification des composants, la confidentialité et l'authenticité des communications. Tous les échanges de fichiers – données d'administration, et mise à jour de contenu, etc. – devront se faire en utilisant des mécanismes reposant sur des algorithmes de chiffrement reconnus et des protocoles normalisés par l'IETF (IPsec, TLS, SSH, etc.). Ces échanges comprennent principalement les communications suivantes : - les communications entre opérateur et l'ARJEL ; - les communications réseaux entre joueurs et opérateur ; - les communications réseaux entre les modules au sein du frontal.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Les accès d'administration aux équipements du frontal doivent être protégés à l'aide des mécanismes suivants :						
E39	DET	5.7.3.e.2		- en priorité, une authentification par certificat X.509v3, par clef publique RSA ou par système à deux facteurs (dont un mot de passe à usage unique), si les applications et les systèmes le supportent ;	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E40	DET	5.7.3.e.2		- ou bien une authentification par mot de passe, avec des règles de composition et de renouvellement conforme aux bonnes pratiques recommandées par le CERTA, que l'opérateur détaillera ; ces mots de passe devront être employés dans le cas de protocoles d'authentification par défi/réponse ;	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.	Les authentifications en clair seront prohibées, et en l'absence de mode défi/réponse un chiffrement des communications sera obligatoire. La mesure doit permettre de prouver la robustesse des mots de passe		
E41	DET	5.7.3.e.2		- un contrôle d'accès basé sur les adresses IP est réalisé, le cas échéant.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Gestion des configurations						
E42	DET	5.7.3.f	À l'issue de la mise en œuvre d'un nouvel équipement ou de l'installation d'une nouvelle application, l'opérateur mettra à disposition de l'ARJEL la version à jour du dossier de définition incluant toutes les informations relatives à la configuration de ce nouvel élément.		**1**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E43	DET	5.7.3.f	Les composants systèmes, réseau et applicatifs mis en œuvre par l'opérateur devront avoir fait l'objet d'une minimalisation de leur configuration et d'un durcissement en termes de sécurité : restriction des applications exécutées au démarrage, limitation du nombre d'applications en écoute sur le réseau, désactivation des fonctionnalités inutiles voire dangereuse (interface d'administration de serveurs d'application), suppression des comptes et mots de passe constructeurs, etc.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E44	DET	5.7.3.f	Afin de détecter d'éventuelles erreurs de manipulation mais aussi le résultat d'attaques, l'intégrité des fichiers de configuration des équipements devra être vérifiée régulièrement. Cette vérification devra pouvoir être faîte sur demande de l'ARJEL, et un rapport de diagnostic devra pouvoir lui être transmis.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Gestion de la sécurité dans les cycles de développement						
E45	DET	5.7.3.g	L'opérateur devra gérer la sécurité à chaque étape du cycle de développement de ses systèmes, dans les phases de définition, de développement, d'exploitation et d'utilisation, puis de maintenance et d'évolution.		**2**	Documentation remise par l'opérateur.	Cette exigence couvre, outre la vérification de la procédure technique liée à cette transmission, le droit de l'opérateur de l'effectuer.		
E46	DET	5.7.3.g	L'opérateur devra contractualiser avec ses prestataires le respect d'un référentiel de développement sécurisé pour les projets dont il externaliserait la prise en charge.		**1**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
			Le référentiel de développement sécurisé devra en particulier aborder le problème de la validation des paramètres, notamment :						
E47	DET	5.7.3.g		- vérifier toutes les données transmises par l'utilisateur selon des critères de taille, type et caractères autorisés, et selon un mécanisme de liste blanche ;	**2**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E48	DET	5.7.3.g		- vérifier les données en entrée et en sortie ;	**2**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E49	DET	5.7.3.g		- utiliser une fonction de vérification des données identique et centralisée.	**2**	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E50	DET	5.7.3.g	L'opérateur devra pouvoir transmettre à l'ARJEL l'ensemble de codes sources des logiciels de jeux utilisés sur ses plates-formes.		**3**	Documentation remise par l'opérateur.			
			Gestion des sauvegardes des données						
E51	DET	5.7.3.h	L'opérateur fournit les moyens de mettre en œuvre un service d'archivage afin d'assurer la conservation de l'ensemble de ses données de traitement, et en particulier celles stockées dans le coffre-fort du frontal.		**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			

E52	DET	5.7.3.h	Ces sauvegardes sont mises à disposition de l'ARJEL par l'opérateur pour consultation et archivage.		**2**	Documentation remise par l'opérateur.			
E53	DET	5.7.3.h	Le type de support et le format de la sauvegarde sont indiqués pour permettre à l'ARJEL de vérifier l'exploitabilité de ces sauvegardes et de leurs contenus.		**3**	Documentation remise par l'opérateur.			
E54	DET	5.7.3.h	La durée de conservation des informations, définie par le code du commerce, doit être de 5 ans, suivant la fermeture du compte de jeu.		**3**	Documentation remise par l'opérateur.			
			Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :						
E55	DET	5.7.3.h		- être protégées en intégrité ;	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E56	DET	5.7.3.h		- être accessibles aux personnes autorisées seulement ;	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E57	DET	5.7.3.h		- pouvoir être relues et exploitées.	**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E58	DET	5.7.3.h	Le niveau de protection des sauvegardes des archives doit être au moins équivalent au niveau de protection des archives : l'opérateur présentera dans sa réponse les mécanismes d'archivage ainsi que les moyens sécurisés de protection des archives qu'il est capable de mettre en œuvre.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			La précision de l'horloge par rapport à laquelle les systèmes d'information se synchronisent pour dater les événements journalisés ou archivés doit :						
E59	DET	5.7.3.h		- être inférieure à une seconde par rapport au temps UTC ; - la source de temps doit être fiable.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.	L'auditeur devra démontrer le respect de l'exigence		
			Gestion de la journalisation technique et fonctionnelle						
			L'opérateur doit maintenir, et pouvoir fournir à l'ARJEL, les journaux des traces techniques pour les évènements clé. Une première liste des événements concernés :						
E60	DET	5.7.3.k		- accès aux modules du frontal ; - opérations de maintenance effectuées ; - ouverture et fermeture de la prise de paris, mises poker, etc.	**2**	Documentation remise par l'opérateur.			
E61	DET	5.7.3.k	Si des personnes physiques sont à l'origine des évènements tracés : - la journalisation doit permettre d'établir un lien entre l'identifiant technique utilisé dans la trace et la personne physique responsable des actions ; - les évènements seront journalisés en s'appuyant sur une source de temps fiable.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E62	DET	5.7.3.k	Concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un package Linux, …). toutes les traces disponibles au niveau des équipements seront activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E63	DET	5.7.3.k	L'opérateur consolidera l'ensemble des traces issues de la journalisation technique des différents équipements (réseau, système, applicatifs et sécurité), par exemple via l'application et le protocole syslog.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E64	DET	5.7.3.k	Les traces de sécurité issues de la journalisation technique des plates-formes seront analysées périodiquement par l'opérateur afin d'identifier les anomalies éventuelles.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E65	DET	5.7.3.k	Les journaux techniques produits par les différents équipements doivent être conservés au minimum pendant trois mois en tant qu'archive.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E66	DET	5.7.3.k	L'opérateur pourra mettre à disposition de l'ARJEL ces journaux bruts produits par les différents équipements ou logiciels.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E67	DET	5.7.3.k	Les incidents ou les comportements anormaux pouvant avoir un impact sur la sécurité du service devront être traités et systématiquement faire l'objet d'une alerte et d'un compte-rendu écrit qui pourra être communiqué à l'ARJEL.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Gestion des accès physiques						
E68	DET	5.7.3.l	Les locaux techniques doivent être accessibles aux seules personnes habilitées par l'opérateur.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			L'opérateur doit :						
E69	DET	5.7.3.l		- être en mesure d'identifier parfaitement les personnes ayant à intervenir dans ses locaux et sur ses équipements ;	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E70	DET	5.7.3.l		- les fonctions et les autorisations d'accès de ces personnes devront être connues et maintenues à jour.	**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E71	DET	5.7.3.l	Les personnes ayant à intervenir sur les équipements des plates-formes devront avoir été sensibilisées à la sécurité des systèmes d'information (confidentialité des mots de passe et des données hébergées, etc.).		**1**	Documentation remise par l'opérateur.			
E72	DET	5.7.3.l	L'opérateur fournira à l'ARJEL les dispositions prises en matière de contrôle de la situation, notamment la vérification de l'absence de conflits d'intérêts, des candidats postulant pour un poste sensible, ainsi que les modalités de mise en sécurité de l'information lors de leur départ de la société (récupération des badges, gestion des mots de passe, etc.).		**1**				
E73	DET	5.7.3.l	Les locaux abritant les équipements devront être sécurisés : serrure haute sécurité, alarme d'ouverture, enregistrement des accès, video-surveillance, etc.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E74	DET	5.7.3.l	L'accès physique à ces locaux devra être limité : filtrage des personnes, contrôle des accès physiques, etc.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Gestion de l'environnement physique						
E75	DET	5.7.3.m	Les matériels et supports informatiques (support de sauvegarde, ...) devront être placés dans des zones de sécurité physiques, conçues pour lutter contre les tentatives d'intrusion et de lutter contre les sinistres et accidents liées à l'environnement.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E76	DET	5.7.3.m	La structure d'hébergement devra répondre disposer de mesure de protection incendie.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E77	DET	5.7.3.m	Le centre d'hébergement devra disposer, pour sa sécurité électronique, d'une double alimentation, d'onduleurs et d'un système de groupe électrogène principal et secondaire.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E78	DET	5.7.3.m	Un système de climatisations redondantes et indépendantes par salle devra assurer la stabilité des températures et du taux d'humidité.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E79	DET	5.7.3.m	Tous les matériels (climatiseurs, panneaux électriques, ...) utilisés par l'opérateur devront faire l'objet d'un contrat de maintenance.		**1**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E80	DET	5.7.3.m	Les sites d'exploitation devront être surveillés 24h/24 et 7j/7.		**2**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Équipe sécurité						
E81	DET	5.7.3.n	L'opérateur devra justifier d'une "équipe sécurité" chargée de surveiller tous les équipements réseau, systèmes et les applications. La sécurité logique des équipements sera réalisée sous le contrôle de cette équipe.		**1**	Documentation remise par l'opérateur.			
			Interdits de jeu						
E82	ANN	3.2.5	Le serveur DNS doit faire l'objet d'une sécurisation, plus particulièrement en termes de : - mise à jour, - durcissement du système d'exploitation sous-jacent, - durcissement de la configuration (en particulier avec la limitation de la récursivité aux seuls hôtes autorisés de la plate-forme de jeu, par le biais d'une liste de contrôle d'accès). Les adresses IP des serveurs DNS de l'opérateur sont communiquées à l'ARJEL, afin de mettre en œuvre des règles de filtrage réseau et listes de contrôle d'accès au niveau applicatif.		**3**	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.	L'exigence relative à la synchronisation horaire s'applique en particulier aux serveurs DNS effectuant les interrogations, afin d'assurer le bon fonctionnement de l'extension de sécurité TSIG		
			Données à la demande						

E83	DET	4.3	L'ARJEL peut ponctuellement exiger des rapports ou données plus détaillés, ou établis avec des critères de recherche précis, qui notamment peuvent être nominatifs. L'opérateur doit pouvoir exécuter des requêtes sur ses systèmes métier afin d'en extraire des données correspondant à des critères imposés par l'ARJEL dans des délais impartis. Ces rapports complèteront les informations qui peuvent être obtenus sur le frontal et les informations remontées systématiquement et automatiquement vers le système d 'information de l'ARJEL. On peut citer : - la fourniture à l'ARJEL de toutes les données techniques et non techniques liées à un évènement particulier ; - des demandes d'enquête de la part de l'ARJEL concernant des évènements détectés et considérés comme anormaux ; - le détail de l'identité d'un joueur ; - le détail des coordonnées du compte de paiement d'un joueur ; - le détail d'une partie de poker, incluant une visibilité complète sur tous les joueurs ayant participé (toutes cartes, quelque soit l'opérateur de rattachement des joueurs dans le cas de réseaux d'opérateurs de mise en commun de joueurs) ; - certaines statistiques non prévues dans les données de supervision ; - le détail d'un pari particulier ; - la fourniture de données techniques (journaux) concernant certains éléments de l'architecture de jeu (frontal, plate-forme, ...).		**3**	Documentation remise par l'opérateur.	Pour chacun des éléments cités à titre d'exemple dans le DET, l'opérateur devra spécifier la nature des données conservées, la période de rétention correspondante et les procédures mises en place pour leur mise à disposition de ces informations à l'ARJEL.		
			Frontal					
E84	DET	4	L'opérateur devra mettre en place un site Internet dédié, exclusivement accessible par un nom de domaine de premier niveau comportant la terminaison .fr.		**3**	Documentation remise par l'opérateur (informations techniques sur le nom de domaine pleinement qualifié : Whois, résolutions DNS, etc. sur l'ensemble des noms de domaine déclarés auprès de l'ARJEL)		
E85	DET	4	Toutes les connexions à destination d'un site de l'opérateur ou d'une de ses filiales et issues d'une IP française ou d'un compte joueur dont l'adresse est en France devront être redirigées vers ce site.		**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.		
			Le frontal est un dispositif de recueil et d'archivage des données échangées entre joueur et la plateforme de l'opérateur à l'occasion des opérations de jeux. Ce dispositif est :					
E86	DET	4.1.1		- développé et exploité sous la responsabilité de l'opérateur ;	**2**	Documentation remise par l'opérateur (identification des prestataires : développeurs, exploitants, etc.).		
E87	DET	4.1.1		- installé sur un support situé en France métropolitaine.	**3**	Description de l'infrastructure d'hébergement. Cette exigence s'applique au coffre et au capteur.		
E88	DET	4.1.2	Tous les échanges entre un joueur réputé français et la plate-forme de jeu devront transiter par le frontal.					
			Les connexions provenant de joueurs réputés français doivent être redirigées vers le frontal qui se trouve en coupure de flux applicatif. La plateforme de jeu doit refuser ou rediriger vers son frontal français les requêtes suivantes :					
E89	DET	4.1.2		- avant authentification du joueur, si l'origine de la connexion est une adresse IP réputée française (pays d'attribution de l'adresse IP du terminal Internet depuis lequel il se connecte est la France dans la base RIPE NCC) ;	**3**	Audit de configuration de la plate-forme d'hébergement, en particulier la description des dispositifs techniques mis en place par l'opérateur côté frontal/plate-forme de jeu (ex : description du module de géolocalisation mis en place au niveau HTTP, ou encore au niveau DNS), étayée par des extraits de configuration (ex : module Apache de géolocalisation) et portion de code (redirection en post-authentification).		
E90	DET	4.1.2		- ou, après authentification du joueur, si le joueur a indiqué un domicile en France lors de l'ouverture de son compte de jeu.	**3**			
E91	Décret N° 2010-509	Art.6	L'opérateur doit permettre à l'ARJEL de se rendre, à tout moment, sur le site d'hébergement du support matériel d'archivage pour saisir l'ensemble ou un sous-ensemble des données qui y sont conservées. À cette fin, l'ARJEL informe au moins deux heures à l'avance le représentant de l'opérateur de son intention d'accéder à ce site et de l'heure à laquelle cet accès devra leur être donné.		**3**	Procédures mises en place par l'opérateur et l'hébergeur du frontal, le cas échéant, pour autoriser un tel accès.		
			Les échanges de données suivants devront être sécurisés afin d'en garantir l'authentification ainsi que la confidentialité :					
E92	DET	4.1.1		- les échanges entre le joueur et le frontal ;	**3**	Audit de configuration de la plate-forme d'hébergement, en particulier la description technique des protocoles de sécurité mis en place (ex : algorithmes, certficats X.509, le cas échéant, etc.).	Avis d'expert sur les interactions HTTP/HTTPS pour les applications Web, notamment pour l'accès au formulaire d'authentification, et la gestion des identifiants de session, etc.	
E93	DET	4.1.1		- les échanges entre les différents modules du frontal ; - les échanges entre le frontal et la plate-forme de jeux de l'opérateur ; - les échanges entre le frontal et la plate-forme de l'ARJEL.	**2**	Audit de configuration de la plate-forme d'hébergement, notamment le schéma d'architecture.	Description technique des flux et protocoles impliqués, en mentionnant les moyens de chiffrement/authenticité des flux (transport IPsec, SSL/TLS, ou colocation des équipements, par exemple) et d'authentification des parties mis en place.	
			Le frontal doit comporter des fonctionnalités de sécurité visant à le protéger des attaques par saturation, qu'elles agissent :					
E94	ANN	3.1.1		- au niveau transport, si ce composant termine les connexions TCP initiées par les clients : protection contre les déni de service réseau, qui visent un épuisement de ressources TCP par des attaques de type SYN Flood, ou des attaques qui s'appuient sur un établissement complet de connexion TCP (Naphta, Sockstress, etc.) ;	**2**	Audit de configuration de la plate-forme d'hébergement, notamment la description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration, ou encore des procédures de gestion d'incident mises en place avec le fournisseur d'accès en amont, le cas échéant, par exemple.		
E95	ANN	3.1.1		- au niveau applicatif, avec l'envoi de multiples requêtes HTTP qui viseraient la saturation du frontal, qui constitue potentiellement un point de défaillance unique de l'architecture, afin de le protéger : - d'un épuisement de ressources (saturation des enregistrements temporairement mis en tampon et en attente d'un acquittement) ; - d'une saturation du coffre avec des enregistrements mal formés.	**2**	Audit de configuration de la plate-forme d'hébergement, audit applicatif de type 'intrusif' de l'application capteur, notamment la description des dispositifs techniques mis en place par l'opérateur appuyée par des éléments de configuration.		
			Frontal : coffre-fort					
E96	DET	4.1.1	Le coffre-fort doit détenir une certification de sécurité de premier niveau (CSPN) délivrée par l'ANSSI (http://www.ssi.gouv.fr).		**3**	L'absence de certification CSPN est rédhibitoire pour l'obtention de la certification du frontal.		
			La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des menaces :					
E97	DET	4.1.1		- le dépôt ou l'injection d'enregistrements non autorisés ;	**3**	Rapport et cible de la certification ANSSI/CSPN.		
E98	DET	4.1.1		- l'altération d'enregistrements ;	**3**	Rapport et cible de la certification ANSSI/CSPN.		
E99	DET	4.1.1		- le vol de données ;	**3**	Rapport et cible de la certification ANSSI/CSPN.		
E100	DET	4.1.1		- le déni de service.	**3**	Rapport et cible de la certification ANSSI/CSPN.		
			La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des fonctions de sécurité :					
E101	DET	4.1.1		- l'authentification forte des utilisateurs et administrateurs ;	**3**	Rapport et cible de la certification ANSSI/CSPN.		
E102	DET	4.1.1		- le chiffrement, la signature et l'horodatage des évènements ;	**3**	Rapport et cible de la certification ANSSI/CSPN.		
E103	DET	4.1.1		- le chaînage des évènements.	**3**	Rapport et cible de la certification ANSSI/CSPN.		
E104	DET	4.1.3	Toute suppression ou altération des données archivées, de manière malveillante ou non, doit pouvoir être identifiée par l'ARJEL.		**3**	Audit de configuration de la plate-forme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.		
			Quatre profils d'autorisation doivent pouvoir être définis :					

E105	DET	4.1.3		- profil « déposant » : profil attribué au module « capteur » du frontal de l'opérateur. Il permet uniquement d'écrire des traces dans le journal. Le module capteur du frontal s'authentifie à l'aide d'un certificat X.509v3 auprès de la partie coffre-fort avec une identité associée à ce profil ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E106	DET	4.1.3		- profil « lecteur » : profil attribué aux agents de l'ARJEL dotés des pouvoirs de contrôle et d'audit, qui permet l'extraction des données enregistrées, soit sur support amovible, soit via un dépôt de fichiers accessible à travers un service Web ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E107	DET	4.1.3		- profil « administrateur technique et opérationnel » : profil attribué au personnel technique de l'opérateur, responsable de l'administration et de la supervision technique du coffre-fort ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E108	DET	4.1.3		- profil « administrateur fonctionnel » : profil attribué aux personnes physiques de l'ARJEL ou désignées par l'ARJEL, qui peuvent définir des rôles et leur associer un certificat d'authentification. Cette opération est nécessaire à l'initialisation des coffres, puis lors des renouvellements ou des révocations des certificats.	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
			Les certificats associés au profil « lecteur » sont utilisés :						
E109	DET	4.1.3		- soit par des personnes physiques, pour les contrôles réalisés sur site, avec des bi-clefs RSA et un certificat X.509v3 d'authentification, par exemple conservé sur un support matériel (ex : carte à puce) fourni par l'opérateur ;	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E110	DET	4.1.3		- soit par des agents de collecte, pour les consultations réalisées à distance, avec une authentification fondée sur un certificat X.509v3 client SSL/TLS, dans le cadre de la négociation d'un tunnel SSL/TLS mutuellement authentifié.	**1**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
			En termes de gestion des clefs de chiffrement, de signature, et d'horodatage :						
E111	DET	4.1.3		- les tailles de clefs doivent être conformes aux règles énoncées dans le référentiel général de sécurité de l'ANSSI (http://www.ssi.gouv.fr/) ;	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E112	DET	4.1.5		- la cryptographie mise en œuvre en termes de générateurs de nombres pseudo-aléatoires, fonctions de hachage, algorithmes symétriques et asymétriques doit respecter les règles de bonnes pratiques spécifiées dans le référentiel général de sécurité de l'ANSSI (http://www.ssi.gouv.fr/);	**3**	Rapport et cible de la certification ANSSI/CSPN.			
E113	DET	4.1.3		- un HSM est utilisé pour les opérations de signature ; le biclef de signature peut être soit injecté dans le HSM, soit injecté dans ce dernier	**3**	Rapport et cible de la certification ANSSI/CSPN.	Dans l'hypothèse où le biclef ferait l'objet d'une injection, un avis d'expert est attendu sur la sécurité de la méthode de génération du biclef hors HSM.		
E114	DET	4.1.3		- les données chiffrées le sont au moyen de la clef publique du certificat transmis par l'ARJEL : seule l'ARJEL peut déchiffrer le contenu des données archivées. Remarque : les opérations de chiffrement des données peuvent indifféremment être réalisées par des moyens matériels ou logiciels.	**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E115	DET	4.1.5	En termes de stockage des traces du coffre-fort, le coffre-fort met en œuvre une ségrégation entre l'espace de stockage destiné aux données de son administration et celui ou ceux destinés aux données de jeu tracées : en effet, dans le cadre d'un coffre mutualisé entre plusieurs agréments, chaque agrément doit faire l'objet d'un espace de stockage spécifique. Cette ségrégation des espaces de stockage doit, a fortiori, être implantée dans le cadre d'une mutualisation inter-opérateurs, le cas échéant.		**3**	Rapport et cible de la certification ANSSI/CSPN.			
			La sécurité physique des accès au coffre sera assurée par :						
E116	DET	4.1.3		- l'hébergement dans un emplacement protégé ;	**2**	Audit de configuration de la plate-forme d'hébergement : une analyse de premier niveau de la sécurité physique de l'infrastructure d'hébergement est attendue.			
E117	DET	4.1.3		- la mise en place d'un contrôle d'accès ;	**2**				
E118	DET	4.1.3		- la mise en place de procédures de suivi des interventions (toutes les opérations de configuration du coffre-fort doivent notamment faire l'objet d'un suivi).	**2**				
E119	DET	4.1.6.a		- la mise en oeuvre de protections physiques	**2**	La méthode de scellement du coffre doit faire l'objet d'une procédure qui, quelle que soit la méthode, doit être probante et garantir l'inocuité d'une intervention qui aurait pour conséquence de rompre ledit dispositif.			
			Frontal : capteur						
E120	ANN	3.1.1	Le capteur doit implanter des mécanismes de défense afin de protéger sa mémoire tampon et éviter toute saturation à destination de cette dernière ou du coffre lui-même.		**2**	Audit applicatif de type 'intrusif' de l'application capteur. Documentation remise par l'opérateur.			
			Le module capteur doit :						
E121	ANN	3.1.1		- être authentifié par certificat auprès du coffre, au niveau duquel une session avec le profil « déposant » est ouverte ;	**2**	Documentation remise par l'opérateur, appuyée par des éléments issus de l'audit applicatif de type 'intrusif' de l'application capteur.	L'analyse doit être étayée par des extraits de code du capteur		
E122	ANN	3.1.1		- attendre du coffre un acquittement, sous la forme d'une preuve du dépôt.	**2**	Documentation remise par l'opérateur, appuyée par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur. Voir les exigences dédiées aux fonctions de création et de stockage des traces.			
E123	DET	4.1.5	L'ensemble des composants doivent être synchronisés en temps, auprès d'une source de temps fiable.		**3**	Audit de configuration de la plate-forme d'hébergement.			
			Frontal : fonctions de création et de stockage des traces						
			La fonction de création de traces du capteur doit respecter les principes suivants :						
E124	DET	4.1.4		- la fonction de création de traces correspond à l'écriture de données liées à un évènement de jeu ou à un compte joueur dans le module coffre-fort du frontal intercepte voire relaie le flux applicatif entre le joueur et l'opérateur. Elle doit donc être réalisée au niveau applicatif : - soit par interception protocolaire du flux HTTP ; - soit par insertion dans la logique de présentation de l'application.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E125	DET	4.1.4		- la fonction de création de traces est implantée en amont de la logique de jeu : elle s'insère en coupure dans la chaîne de traitement des requêtes émises par le joueur vers la plateforme de jeux.	**3**				
E126	DET	4.1.4		- le frontal doit offrir une architecture dotée d'une très haute disponibilité avec redondance de mécanismes afin de strictement limiter les incidents potentiels de stockage.	**3**				
E127	DET	4.1.4		- le principe d'une annulation d'un jeu concerné par un incident de stockage d'un des évènements doit être retenu.	**2**				
			La fonction de création de traces d'un événement doit :						
E128	ANN	3.1.1		- être invoquée suite à une requête émise par le joueur (si celle-ci requiert un enregistrement). Cette requête peut résulter : - d'une action du joueur, à son initiative, comme une prise de pari ; - d'un acquittement par le joueur, suite à message transmis à l'initiative de la plate-forme, comme l'annonce d'un gain sur un pari.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			

E129	ANN	3.1.1		- reposer sur un module applicatif à état qui respecte la cinématique de création décrite dans le schéma 3.1.1 de l'annexe du DET, et en particulier donner lieu à un enregistrement temporaire, conservé au niveau du capteur dans une mémoire tampon ou un dispositif de stockage temporaire équivalent (ex: base de données, par exemple), avant toute transmission au niveau du coffre et dans l'attente d'un acquittement de la plate-forme de jeux validant la bonne et due forme de cet événement.	**3**	Le respect de mode de fonctionnement à état assure que les évènements transmis au coffre sont générés à l'initiative du joueur (action ou acquittement), mais sont validés, avant stockage au coffre, par la plate-forme.	Tout écart par rapport à ce mode de fonctionnement doit être techniquement justifié (ex : évènements POPARTIE générés par la plate-forme de jeu, et transmis pour acquittement au joueur avant stockage). Une analyse technique de la sécurité du processus de validation des évènements par le capteur est attendue, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur. Un mode de fonctionnement dans lequel les données transmises par le joueur seraient directement journalisées par le coffre est rédhibitoire pour la certification du frontal. Idem pour des données transmises directement de la plate-forme de jeu vers le coffre, sans acquittement préalable par le joueur.		
E130	ANN	3.1.1		- gérer un acquittement de la plate-forme de jeux, afin de limiter les risques d'attaques qui viseraient à saturer le coffre d'évènements aléatoires, ou à enregistrer des évènements falsifiés générés par un joueur malveillant.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E131	ANN	3.1.1		- en cas d'acquittement négatif de la part de la plate-forme de jeux, l'évènement préenregistré au niveau du capteur doit être détruit. Une erreur doit être générée et faire l'objet d'un message dans la journalisation technique du capteur.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E132	ANN	3.1.1		- en cas d'acquittement positif de la part de la plate-forme de jeux, l'évènement présent en mémoire tampon au niveau du capteur peut être transformé au format exigé par l'ARJEL, pour son stockage par le coffre.	**3**	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.			
E133	ANN	3.1.1		- gérer les cas d'acquittements négatifs de la part du coffre, en cas de défaillance d'enregistrement.	**2**		Des mécanismes de reprise sur erreur peuvent être implantés au niveau du capteur, par exemple par des tentatives de retransmission au coffre d'un l'évènement.		
E134	ANN	3.1.1		- garantir l'enregistrement d'un évènement de jeu au niveau du coffre, sous peine d'annulation de l'opération de jeu.	**2**	Cette exigence repose, dans le DET, sur un fonctionnement synchrone entre capteurs et coffres. Le capteur, dans ce modèle, doit attendre un acquittement positif du coffre avant de poursuivre la transaction.	Dans la pratique : - l'introduction d'un traitement par lots, le cas échéant, proscrit un fonctionnement synchrone au sens strict, - l'approbation de l'utilisation de mécanismes basés sur des files d'attente entre capteurs et coffres proscrit également ce mode de fonctionnement. Il est donc notamment attendu un avis d'expert technique sur : - le synchronisme entre le capteur et le mécanisme de dépôt au coffre, en décrivant files d'attente, mécanismes de détection et de reprise sur erreur (ex : retransmission par le capteur), - la redondance et la fiabilité du dispositif assurant le traitement des évènements entre leur émission par le capteur, et leur stockage *in fine* par le coffre (ex : analyse du mécanisme de file d'attente de type ActiveMQ, par exemple).		
			Le stockage des données consiste en les étapes suivantes :						
E135	DET	4.1.5		- l'établissement d'un canal sécurisé, suite à l'authentification mutuelle du déposant avec le coffre, via une session TLS mutuellement authentifiée par certificat X.509v3 ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E136	DET	4.1.5		- la vérification de l'habilitation du profil à déposer des traces ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.	- l'approbation de l'utilisation de mécanismes basés sur des files d'attente entre capteurs et coffres proscrit également ce mode de fonctionnement.		
E137	DET	4.1.5		- le chaînage avec la trace précédente, en liant l'empreinte des données à une empreinte de la signature de la trace précédente, et en incluant l'identifiant d'évènement unique à l'opérateur ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E138	DET	4.1.5		- le calcul de l'empreinte, à l'aide d'une fonction de hachage. L'empreinte ne doit pas être calculée au moment de l'ajout, mais être conservée en mémoire depuis l'opération précédente ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E139	DET	4.1.5		- le scellement des données, par signature horodatée incluant l'élément de chaînage pour en garantir l'intégrité, et les lier à une heure précise ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E140	ANN	1.1.5		- l'horodatage, qui doit être effectué sur l'évènement (ou le lot d'évènements) en clair.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
			Concernant les opérations de signature et de chiffrement :						
E141	DET	4.1.5		- le format de signature est XADES-T avec un jeton d'horodatage RFC 3161.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.	Un autre format de signature peut être implanté, à condition d'être justifié.		
E142	DET	4.1.5		- le chiffrement des données est réalisé au moyen de la clé publique de l'ARJEL pour en assurer la confidentialité.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.	La méthode de chiffrement pourra faire intervenir un algorithme de chiffrement symétrique, suivant des opérations qui seront précisément décrites.		
			Concernant le traitement par lots :						
E143	ANN	1.1.5		- le traitement par lot doit être paramétrable pour une durée ou un nombre maximal d'évènements.	**1**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E144	ANN	1.1.5		- la granularité du traitement par lot doit être l'évènement.	**1**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
			Frontal : fonctions d'accès aux traces						
			L'opérateur agréé doit fournir les éléments suivants pour chaque agrément :						
E145	DET	4.1.6		- un mécanisme d'accès aux données permettant la saisie des données sur site (copie de tout ou partie du coffre fort) ;	**3**	Documentation remise par l'opérateur.			
E146	DET	4.1.6		- un mécanisme d'accès aux données permettant l'interrogation des données à distance, par l'intermédiaire d'un outil de collecte ;	**3**	Documentation remise par l'opérateur.			
E147	DET	4.1.6		- un outil de validation des données du frontal et d'extraction des traces des opérations de jeu utilisable sur le site du frontal, et dans les laboratoires de l'ARJEL (mode hors-ligne).	**3**	Documentation remise par l'opérateur.			
			L'architecture de la partie coffre-fort du frontal doit distinguer :						

E148	DET	4.1.6		- un espace de stockage des données situé dans une zone réseau sécurisée ;	**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.			
E149	DET	4.1.6		- une couche d'accès à l'espace de stockage accessible.	**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.			
E150	DET	4.1.6.a	Les données stockées dans le coffre doivent être en permanence accessibles à distance, depuis les locaux de l'ARJEL, *i.e.* depuis une ou plusieurs adresses IP identifiées.		**3**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E151	DET	4.1.6.a	L'extraction du coffre doit pouvoir se faire sur une tranche de données, correspondant à une période d'activité ou une tranche d'identifiants d'évènements avec l'outil de collecte à distance mis à disposition par l'opérateur.		**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E152	DET	4.1.6	La couche d'accès à l'espace de stockage doit elle-même être sécurisée, aux niveaux applicatif et réseau, vis-à-vis de l'extérieur, notamment contre les attaques de déni de service, et les accès autres que ceux initiés par l'ARJEL.		**2**	Audit de configuration de la plate-forme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur + avis d'expert.			
			La couche d'accès expose un service web doté des deux principales interfaces suivantes :						
E153	DET	4.1.6		- une interface de consultation : elle permet l'extraction d'une trace ou d'un ensemble de traces à partir d'une date ou d'une tranche caractérisée par une date de début et une date de fin. À une même date peuvent correspondre aucun, un ou plusieurs évènements ;	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E154	DET	4.1.6		- une interface de synchronisation : elle permet l'extraction d'une trace et ou d'un ensemble des traces à partir de l'identifiant d'un évènement ou d'une tranche d'évènements.	**3**	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E155	DET	4.1.6	Les données doivent rester accessibles sur site sur toute la durée de conservation exigée par la loi (article 10 du Décret n° 2010-509 du 18 mai 2010).		**3**	Documentation remise par l'opérateur.			
E156	DET	4.1.6	Les données accessibles à distance doivent couvrir au moins les 12 derniers mois d'opération (période glissante).		**3**	Documentation remise par l'opérateur.			
			L'outil réalisé par l'opérateur doit permettre :						
E157	ANN	3.1.3		- d'interroger à distance le coffre de l'opérateur pour télécharger les traces demandées (outil de collecte) ;	**3**	Documentation remise par l'opérateur.			
E158	ANN	3.1.3		- d'extraire les traces ainsi téléchargées pour ensuite les déchiffrer et vérifier l'intégrité des données (outil d'extraction et de validation). Cette extraction doit pouvoir être réalisée hors-ligne.	**3**	Documentation remise par l'opérateur.			
			L'outil doit implanter :						
E159	ANN	3.1.3.c		- l'interface WSDL définie par l'ARJEL, ou proposer une interface d'interrogation équivalente notamment basée sur l'identifiant d'opérateur, de coffre, sur l'agrément, et une tranche d'évènements ou de dates ;	**1**	Documentation remise par l'opérateur.			
E160	ANN	3.1.3		- les options en ligne de commande décrites dans la partie 3.1.3 de l'annexe au DET (fonctionnalités d'interrogation à distance) ;	**1**	Documentation remise par l'opérateur.			
E161	ANN	3.1.3		- le protocole TLS v1.1 au niveau du protocole de transport, et si possible, le triple d'algorithmes DHE-RSA-AES256-SHA ;	**2**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.			
E162	ANN	3.1.3		- des algorithmes cryptographiques manipulant des clefs dont la taille doivent être conformes aux règles énoncées dans le Référentiel général de sécurité disponible sur le site de l'ANSSI.	**3**	Documentation remise par l'opérateur.			
			L'accès réseau de l'accès à distance doit :						
E163	ANN	3.1.3		- faire l'objet d'un filtrage implanté sous la forme d'une liste blanche au niveau d'un équipement de sécurité périmétrique de type pare-feu ;	**2**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.			
E164	ANN	3.1.3		- faire l'objet d'une journalisation, et l'objet de procédures de traitement d'incident, le cas échéant.	**2**	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.			
E165	ANN	3.1.3.a	L'outil d'extraction et de validation des traces doit implanter les options décrites dans la partie 3.1.3.a de l'annexe au DET (fonctionnalités d'extraction des traces et de vérification).		**1**	Documentation remise par l'opérateur.			
			Évènements XML : généralités						
			Les enregistrements XML sont :						
E166	ANN	1.1.1		- encodés au format UTF-8. On veillera en particulier au respect des caractères accentués (é, è, à) ;	**3**	Audit de code	L'analyse devra démontrer l'usage de filtres dans le code source		
E167	ANN	1.1.1		- conformes à la norme XML (en particulier en termes d'encodage des entités XML) ;	**3**				
E168	ANN	1.1.1		- conformes au schéma XSD publié par l'ARJEL ;	**3**				
E169	ANN	1.3		- filtrés, en termes de contenu, conformément aux expressions régulières (facette *pattern*) décrites dans le schéma XSD ;	**3**				
E170	ANN	1.3		- filtrés, en termes de contenu, afin de prévenir des attaques web classiques par injection (injections SQL, XPath, voire XSS, en complément d'un encodage des sorties par entités HTML, par exemple, etc.) ;	**3**				

Autorité de régulation des jeux en ligne
RÉPUBLIQUE FRANÇAISE

RÉFÉRENTIEL JURIDIQUE ET FINANCIER

ANNEXE II du Règlement relatif à la certification prévue à l'article 23 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne adopté par la décision n° 2014-018 du collège de l'Autorité de régulation des jeux en ligne en date du 17 mars 2014.

Sommaire

Préambule – Guide méthodologique

Le présent référentiel est applicable à la certification prévue au premier alinéa du III de l'article 23 de la loi n° 2010-476 du 12 mai 2010 (certification annuelle initiale) ainsi qu'à celle prévue au deuxième alinéa du III de cet article (actualisation de la certification annuelle initiale).

Les travaux de certification juridique et financière réalisés en application du III de l'article 23 de la loi n° 2010-476 du 12 mai 2010 sont exécutés conformément au présent référentiel, dans le respect des dispositions du règlement relatif à la certification adopté par la décision n° 2014-018 du collège de l'Autorité de régulation des jeux en ligne en date du 17 mars 2014.

Nature des travaux attendus

Le présent référentiel se compose d'une liste de 41 exigences juridiques et financières (ci-après : « *EJF* »).

La nature des travaux attendus varie en fonction de l'EJF considérée. Elle est précisée pour chaque EJF.

Différentes types de travaux peuvent être demandés :

- Recherche et/ou analyse documentaire ;
- Constatations sur le site Internet de l'opérateur ;
- Entretiens avec l'opérateur ;
- Analyse d'extraits du « *back office* » ;
- Tests de cheminement ;
- Tests d'échantillonnage.

L'organisme certificateur est naturellement libre de compléter ces travaux par toute analyse complémentaire qu'il estime utile à la vérification des EJF.

Dans les cas où le référentiel précise que des **tests de cheminements** doivent être réalisés, il est attendu de l'organisme certificateur qu'il vérifie lui-même que les différentes étapes de la procédure ou du point de contrôle considéré sont conformes aux exigences légales et réglementaires. Il procède à ces vérifications à l'aide d'un ou plusieurs compte(s) joueur(s) créé(s) pour réaliser ces tests en vue de retracer un parcours client type.

L'organisme certificateur est en outre tenu de décrire les procédures mises en place par l'opérateur, en s'appuyant notamment sur de l'analyse documentaire, des constatations sur le site Internet de l'opérateur ou encore des entretiens menés avec les opérationnels en charge du processus.

Les tests de cheminement ne peuvent se fonder sur la seule analyse des conditions générales d'utilisation.

Dans les cas où le référentiel précise que des **tests d'échantillonnage** doivent être réalisés, il est attendu de l'organisme certificateur qu'il fonde ses conclusions sur l'analyse d'un échantillon représentatif de comptes joueurs extraits du « *back office* » de l'opérateur. L'analyse peut porter, le cas échéant, sur un échantillon d'opérations bancaires ou de salariés.

Périmètre de la certification

Certification annuelle initiale

Lorsqu'il procède à une certification annuelle initiale, l'organisme certificateur est tenu de contrôler l'ensemble des EJF du référentiel.

Actualisation de la certification annuelle

Lorsqu'il procède à l'actualisation d'une certification annuelle :

- (a) L'organisme certificateur est tenu, en tout état de cause, de contrôler les EJF suivantes[1] :
    - EJF 1 à 10
    - EJF 12
    - EJF 40 et 41
- (b) L'organisme certificateur est tenu, en outre, de contrôler les EJF ayant fait l'objet de réserves lors de la précédente certification annuelle[2] ;
- (c) En l'absence de modifications intervenues depuis la dernière certification, l'organisme certificateur n'est pas tenu de contrôler les EJF suivantes :
    - EJF 11
    - EJF 13 à 39

  L'absence de modifications est attestée par une déclaration de l'opérateur annexée au rapport de certification. Cette déclaration vise explicitement chacune des EJF concernées pour lesquelles l'opérateur atteste qu'aucune modification n'est intervenue depuis la dernière certification.

[1] Ces EJF sont identifiées sur le référentiel par le symbole *****.
[2] Lorsque la précédente certification annuelle a été réalisée avant l'entrée en vigueur du règlement relatif à la certification adopté par la décision du collège de l'Autorité de régulation des jeux en ligne n° 2014-018 du 17 mars 2014, l'ensemble des EJF ayant alors fait l'objet de non-conformités doit être mesuré à nouveau lors de l'actualisation de ladite certification, à l'exception des EJF supprimées dans le présent référentiel.

Décision sur la certification

Les EJF que l'organisme certificateur considère comme n'ayant pas été atteintes constituent des non-conformités. Elles doivent être mentionnées comme telles dans le rapport de certification.

Lorsque une ou plusieurs EJF du référentiel n'est/ne sont pas atteinte(s), la certification est délivrée avec réserve(s).

Il est précisé que, en matière juridique et financière, aucun niveau de criticité n'est attaché *a priori* au non respect d'une exigence.

Référentiel

#	Textes de référence		Nature des travaux attendus
I. Informations personnelles			
A. Eléments juridiques			
EJF1 *	Loi n° 2010-476 du 12 mai 2010 - Art. 15	Vérifier l'identité et le lieu d'établissement du titulaire de l'agrément (personne morale ou personne physique) et de ses dirigeants. Produire toute pièce justificative à jour et notamment, le cas échéant, le KBIS de la société ou tout document équivalent pour les sociétés établies à l'étranger.	Recherche et analyse documentaire
EJF2 *	Loi n° 2010-476 du 12 mai 2010 - Art. 15	Vérifier que l'entreprise titulaire de l'agrément, son propriétaire ou, s'il s'agit d'une personne morale, un de ses dirigeants ou mandataires sociaux n'a fait l'objet, depuis la délivrance de l'agrément ou la dernière certification annuelle, d'aucune condamnation pénale devenue définitive relevant des catégories énumérées à l'article 12 du décret n° 2010-482 du 12 mai 2010.	Recherche et analyse documentaire
B. Moyens humains			
EJF3 *	Loi n° 2010-476 du 12 mai 2010 - Art. 15	Vérifier (et, le cas échéant, mentionner) les éventuelles évolutions des moyens humains du titulaire de l'agrément par rapport au dossier de demande d'agrément ou à la dernière certification annuelle. Annexer l'organigramme présentant la répartition des effectifs ainsi que les fonctions du personnel interne et externe nécessaire au fonctionnement de la société, ainsi que, le cas échéant, toute pièce justificative des évolutions mentionnées.	Recherche et analyse documentaire
C. Moyens matériels			
EJF4 *	Loi n° 2010-476 du 12 mai 2010 - Art. 15	Vérifier (et, le cas échéant, déclarer) les éventuelles modifications des moyens matériels du titulaire de l'agrément par rapport au dossier de demande d'agrément ou à la dernière certification annuelle. Annexer, le cas échéant, toute pièce justificative de ces modifications. Vérifier que la localisation des équipements utilisés n'a pas changé depuis la délivrance de l'agrément ou la dernière certification annuelle. En cas de changement, vérifier que l'équipement concerné n'est pas localisé dans un Etat ou territoire non coopératif au sens de l'article 238-0 A du code général des impôts et annexer toute pièce justificative en attestant.	Recherche et analyse documentaire

D. Actionnariat			
EJF5 *	Loi n° 2010-476 du 12 mai 2010 - Art. 15	Vérifier les éventuelles modifications de l'actionnariat du titulaire de l'agrément s'il s'agit d'une entreprise constituée en société par actions ainsi que, le cas échéant, celui des personnes qui le contrôlent directement ou indirectement au sens de l'article L. 233-16 du Code de commerce. Annexer le schéma actionnarial détaillé de la société et, le cas échéant, toute pièce justificative des modifications constatées.	Recherche et analyse documentaire

II. Informations économiques, financières et comptables			
A. Capacité financière de l'opérateur			
EJF6 *	Loi n° 2010-476 du 12 mai 2010 - Art. 15	Vérifier que l'opérateur est à jour du paiement de ses cotisations fiscales et sociales. Annexer une attestation fiscale ou tout document équivalent permettant d'en justifier.	Recherche et analyse documentaire
B. Compte de paiement de l'opérateur			
EJF7 *	Loi n° 2010-476 du 12 mai 2010 - Art. 18	Vérifier que le compte dédié de l'opérateur est ouvert auprès d'un établissement de crédit établi au sein de l'Union européenne ou dans un Etat 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. Annexer le(s) relevé(s) d'identité bancaire du(des) compte(s) de l'opérateur dédié(s) aux opérations d'encaissement et de paiement liées aux jeux et paris qu'il propose légalement en France.	Recherche documentaire
EJF8 *	Loi n° 2010-476 du 12 mai 2010 - Art. 18	Vérifier que, depuis la délivrance de l'agrément ou la dernière certification annuelle, ont été exclusivement réalisées sur ce(s) compte(s) des opérations d'encaissement et de paiement liées aux jeux et paris que l'opérateur propose légalement en France. Le test d'échantillonnage pour cette EJF se réalise en deux temps. Dans un premier temps, sélectionner un échantillon de mouvements débiteurs passés au cours de l'année écoulée et vérifier la nature desdits mouvements (retraits joueurs, commissions bancaires ou PBJ de l'opérateur uniquement). Dans un second temps, obtenir un extrait du « *back office* » de l'opérateur permettant de sélectionner des mouvements de retraits de joueurs. Sélectionner certains de ces mouvements et vérifier leur passage sur le compte bancaire dédié de l'opérateur. Si les retraits des joueurs sont traités par lots (« *batch* »), récupérer le fichier correspondant communiqué par l'opérateur à sa banque et vérifier l'existence du mouvement au débit sur le compte dédié de l'opérateur. Pour les opérateurs ayant mis en place une garantie des avoirs des joueurs, décrire la procédure contractuelle permettant de couvrir le solde des comptes joueurs à tout moment.	Tests d'échantillonnage

III. Informations relatives au site de jeu en ligne			
A. Contrats de sous-traitance			
EJF9 *	Loi n° 2010-476 du 12 mai 2010 - Art. 16	Lister les contrats de fourniture ou de sous-traitance d'opérations de jeux ou de paris en ligne signés par l'opérateur, en précisant les éléments suivants : - Dénomination des parties ; - Objet et prix du contrat ; - Dates d'entrée en vigueur et d'extinction du contrat. Le cas échéant, annexer l'ensemble des contrats de mutualisation des masses conclus par l'opérateur.	Recherche documentaire
B. Sites affiliés, marque blanche, « *co-branding* »			
EJF10 *	Loi n° 2010-476 du 12 mai 2010 - Art. 16 Décision n°2010-107 du 24 septembre 2010	Annexer la liste actualisée des contrats de partenariat conclus par l'opérateur concernant : - Les sites internet affiliés à l'opérateur ; - Les sites en marques blanches ; - Les sites en « *co-branding* ». Accompagner cette liste d'une note synthétique d'analyse de ces contrats.	Recherche et analyse documentaire

IV. Informations relatives aux opérations de jeux ou de paris en ligne proposés			
A. Procédure de réclamation gratuite			
EJF11	Loi n° 2010-476 du 12 mai 2010 - Art. 19	Décrire la procédure de réclamation gratuite mise à la disposition des joueurs et vérifier l'application de cette procédure.	Tests de cheminement Constatations sur le site Internet de l'opérateur
B. Conditions générales d'utilisation			
EJF12 *	Décret n° 2010-518 du 19 mai 2010 - Art. 1	Lister les différentes versions des Conditions générales d'utilisation intervenues depuis la délivrance de l'agrément ou depuis la dernière certification annuelle en précisant, pour chaque version modifiée, la date de la modification. Vérifier que les Conditions générales d'utilisation de l'opérateur sont mises à disposition des joueurs de manière aisément accessible.	Recherche documentaire Constatations sur le site Internet de l'opérateur

V. Informations relatives aux comptes joueurs			
A. Ouverture et fermeture du compte joueur			
1. Modalités d'ouverture du compte joueur			
EJF13	Loi n° 2010-476 du 12 mai 2010 - Art. 17	Vérifier que l'opérateur s'assure, lors de l'ouverture initiale du compte joueur et lors de toute session de jeu, que le joueur est une personne physique en requérant l'entrée d'un code permettant d'empêcher les inscriptions et l'accès de robots informatiques.	Constations sur le site Internet de l'opérateur
EJF14	Loi n° 2010-476 du 12 mai 2010 - Art. 17 Décret n°2010-518 du 19 mai 2010 - Art. 2	Vérifier que, préalablement à l'ouverture d'un compte joueur auprès de l'opérateur, celui-ci demande à la personne sollicitant l'ouverture de ce compte : - De lui communiquer ses noms, prénoms, date et lieu de naissance, l'adresse postale de son domicile ainsi que les références du compte de paiement mentionné au dernier alinéa de l'article 17 de la loi n° 2010-476 du 12 mai 2010 sur lequel l'opérateur reversera, le cas échéant, les avoirs du joueur ; - De certifier qu'elle a pris connaissance du règlement portant conditions générales de l'offre de jeux et paris et de manifester explicitement son acceptation des clauses de ce règlement ; cette acceptation doit être renouvelée à chaque modification du règlement ; - Si elle consent à ce que les données personnelles qu'elle confie à l'opérateur fassent l'objet d'utilisations à des fins de prospection commerciale. Vérifier que la demande prévue au 3° est distincte de celle mentionnée au 2° et que le consentement de la personne résulte d'une manifestation expresse de sa volonté. Vérifier que l'opérateur refuse l'ouverture d'un compte à toute personne ne lui ayant pas communiqué l'intégralité de ces réponses.	Analyse documentaire et entretiens Tests de cheminement
EJF15	Décret n°2010-518 du 19 mai 2010 - Art. 2	Vérifier que l'opérateur informe la personne sollicitant l'ouverture d'un compte de ce que : - La demande d'ouverture d'un compte joueur emporte renonciation à l'exercice du droit prévu au premier alinéa de l'article 38 de la loi du 6 janvier 1978 ; - Cette personne dispose, pour les données personnelles qu'elle a confiées à l'opérateur, d'un droit d'accès et de rectification, conformément aux dispositions des articles 39 et 40 de la même loi ; - L'Autorité de régulation des jeux en ligne peut être destinataire des données personnelles qu'elle lui a confiées, ainsi que de celles relatives à son activité de jeux ou de paris.	Analyse documentaire et entretiens Tests de cheminement

EJF16	Décret n° 2010-518 du 19 mai 2010 - Art. 3	Vérifier que, préalablement au contrôle par l'opérateur des documents exigés à l'article 4 du décret n° 2010-518, seul peut être ouvert un compte joueur provisoire ne permettant pas à son titulaire d'ordonner le reversement, même partiel, du solde créditeur de ce compte sur son compte de paiement.	Analyse documentaire et entretiens Tests de cheminement
EJF17	Décret n° 2010-518 du 19 mai 2010 - Art. 3	Vérifier que l'opérateur informe le joueur sollicitant l'ouverture d'un compte provisoire des conditions de fonctionnement de ce compte et lui demande d'accepter explicitement ces dernières.	Analyse documentaire et entretiens Tests de cheminement
EJF18	Décret n° 2010-518 du 19 mai 2010 - Art. 4	Vérifier que toute personne sollicitant l'ouverture d'un compte joueur auprès de l'opérateur est tenue de lui communiquer, dans le délai maximum d'un mois suivant sa demande d'ouverture de compte : - La copie d'une carte nationale d'identité, d'un passeport ou d'un permis de conduire en cours de validité justifiant de son identité et de sa date de naissance ; - Un document portant références du compte de paiement mentionné au dernier alinéa de l'article 17 de la loi n° 2010-476 du 12 mai 2010 et attestant que ce compte est ouvert à son nom.	Analyse documentaire et entretiens Tests de cheminement
EJF19	Décret n° 2010-518 du 19 mai 2010 - Art. 5	Vérifier que, lorsque les pièces exigées à l'article 4 du décret n° 2010-518 ont été transmises à l'opérateur et que celui-ci a procédé aux vérifications nécessaires, il communique au joueur, par courrier envoyé à l'adresse postale déclarée par ce dernier, un code secret, distinct du mot de passe permettant au joueur d'accéder, le cas échéant, à son compte provisoire. Vérifier que lorsqu'un compte provisoire a été ouvert, seule la saisie par le joueur du code secret permet de mettre fin au statut provisoire du compte.	Analyse documentaire et entretiens Tests de cheminement
EJF20	Décret n° 2010-518 du 19 mai 2010 - Art. 5	Vérifier que si, à l'expiration du délai d'un mois suivant la demande d'ouverture du compte joueur, l'une des pièces exigées par l'article 4 du décret n° 2010-518 ne lui a pas été communiquée, l'opérateur désactive le compte provisoire. Vérifier que cette désactivation est systématiquement prévue par la procédure d'inscription. En vous basant sur une extraction récente du « *back office* » de l'opérateur, sélectionner un échantillon de comptes joueurs provisoires pour lesquels l'ensemble des pièces exigées n'a pas été communiqué et vérifier que ces comptes ont bien été désactivés dans le délai d'un mois.	Analyse documentaire et entretiens Tests d'échantillonnage

EJF21	Décret n° 2010-518 du 19 mai 2010 - Art. 5	Vérifier que si, au terme du délai de deux mois suivant la demande d'ouverture du compte joueur, l'une des pièces exigées par l'article 4 du décret n° 2010-518 ne lui a pas été communiquée, l'opérateur clôture ledit compte. Vérifier que cette clôture est systématiquement prévue par la procédure d'inscription. En vous basant sur une extraction récente du « *back office* » de l'opérateur, sélectionner un échantillon de comptes joueurs provisoires pour lesquels l'ensemble des pièces exigées n'a pas été communiqué et vérifier que ces comptes ont bien été clôturés dans le délai de deux mois.	Analyse documentaire et entretiens Tests d'échantillonnage
EJF22	Décret n° 2010-518 du 19 mai 2010 - Art. 5	Vérifier que si, au terme d'un délai de six semaines à compter de l'envoi par l'opérateur du code secret prévu à l'article 5 du décret n° 2010-518, le joueur n'a pas saisi ce code, l'opérateur clôture le compte. Vérifier que cette clôture est systématiquement prévue par la procédure d'inscription. En vous basant sur une extraction récente du « *back office* » de l'opérateur, sélectionner un échantillon de comptes joueurs provisoires pour lesquels le code secret n'a pas été saisi et vérifier que ces comptes ont bien été clôturés dans le délai de six semaines.	Analyse documentaire et entretiens Tests d'échantillonnage
EJF23	Décret n° 2010-518 du 19 mai 2010 - Art. 6	Vérifier que la désactivation d'un compte joueur empêche son titulaire d'engager des mises et d'ordonner le reversement, même partiel, du solde créditeur de ce compte sur son compte de paiement.	Analyse documentaire et entretiens Tests de cheminement
EJF24	Décret n° 2010-518 du 19 mai 2010 - Art. 6	Vérifier que si le compte désactivé n'a pas été clôturé, l'opérateur le réactive lorsque son titulaire lui a communiqué l'ensemble des pièces mentionnées à l'article 4 du décret n° 2010-518.	Analyse documentaire et entretiens Tests de cheminement

2. Modalités de clôture du compte joueur			
EJF25	Décret n° 2010-518 du 19 mai 2010 - Art. 7	Vérifier que l'opérateur clôture sans délai un compte joueur lorsque son titulaire : - En fait la demande ; - Lui communique, après l'ouverture d'un compte joueur, des pièces comportant des informations ne correspondant pas à celles qu'il a saisies lors de l'ouverture du compte ; - Lui communique, aux fins de modification des informations associées à son compte joueur, des pièces dont les informations ne correspondent pas à celles qu'il a saisies ;	Analyse documentaire et entretiens Tests de cheminement
EJF26	Décret n° 2010-518 du 19 mai 2010 - Art. 7	Vérifier que l'opérateur clôture sans délai un compte joueur lorsque son titulaire n'a pas réalisé, dans les douze derniers mois, d'opération de jeux ou de paris. En vous basant sur une extraction récente du « *back office* » de l'opérateur, sélectionner un échantillon de comptes joueurs n'ayant donné lieu à aucune opération de jeux ou de paris depuis les douze derniers mois et vérifier que ces comptes ont bien été clôturés.	Test d'échantillonnage
EJF27	Décret n° 2010-518 du 19 mai 2010 - Art. 8	Vérifier que l'opérateur clôturant un compte joueur provisoire informe le joueur du motif de cette clôture. Vérifier que, lorsque le compte provisoire clôturé est créditeur, l'opérateur met en réserve sans délai la somme correspondante, pour une durée de cinq ans à compter de la clôture du compte. Vérifier que, durant cette période, et sans préjudice de l'application de l'article L. 561-16 du code monétaire et financier, le titulaire du compte peut obtenir le versement du montant du solde créditeur en communiquant à l'opérateur les pièces exigées à l'article 4 du décret n° 2010-518, sauf si ces pièces permettent d'établir qu'il n'était pas autorisé à jouer au moment où le compte provisoire était actif.	Analyse documentaire et entretiens Tests de cheminement
EJF28	Décret n° 2010-518 du 19 mai 2010 - Art. 9	Vérifier que l'opérateur clôturant un compte joueur non provisoire : - Le cas échéant, reverse immédiatement son solde créditeur sur le compte de paiement du joueur (sauf si l'opérateur soupçonne que cette opération est liée au blanchiment de capitaux ou au financement du terrorisme, en application de l'article L. 561-16 du code monétaire et financier) ; - Informe le joueur de la clôture de son compte et du motif de cette clôture, par tout moyen à sa disposition et dans un délai de trois jours ouvrés et précise, le cas échéant, le montant des sommes qu'il a reversées sur son compte de paiement.	Analyse documentaire et entretiens Tests de cheminement

B. Moyens et instruments de paiement et modalités d'encaissement et de paiement			
EJF29	Loi n° 2010-476 du 12 mai 2010 - Art. 17	Vérifier que l'opérateur ne reverse les avoirs du joueur que sur un seul compte de paiement du joueur.	Analyse documentaire et entretiens Tests de cheminement
EJF30	Loi n° 2010-476 du 12 mai 2010 - Art. 17	Lister les instruments de paiements utilisés et proposés au joueur pour approvisionner son compte joueur. Vérifier que les prestataires de paiement dont les instruments sont proposés par l'opérateur ont bien été agréés par l'Autorité de contrôle prudentiel et de résolution.	Constatations sur le site Internet de l'opérateur

VI. Informations relatives à la lutte contre le jeu excessif ou pathologique			
A. Affichage			
EJF31	Loi n° 2010-476 du 12 mai 2010 - Art. 26 Décret n° 2010-518 du 19 mai 2010 - Art. 19	Vérifier que l'opérateur informe les joueurs des risques liés au jeu excessif ou pathologique par le biais d'un message de mise en garde.	Constatations sur le site Internet de l'opérateur
EJF32	Loi n° 2010-476 du 12 mai 2010 - Art. 26	Vérifier que l'opérateur communique en permanence à l'ensemble des joueurs fréquentant son site le solde instantané de leurs comptes.	Constatations sur le site Internet de l'opérateur
B. Les modérateurs de jeu			
1. Dispositifs d'autolimitation des dépôts et des mises			
EJF33	Loi n° 2010-476 du 12 mai 2010 - Art. 26 Décret n° 2010-518 du 19 mai 2010 - Art. 16 et 17	Vérifier que, dès l'ouverture du compte joueur, l'opérateur demande au joueur d'encadrer sa capacité de jeu par la fixation de limites d'approvisionnement de son compte et d'engagement des mises et qu'aucune opération de jeu ne peut être réalisée tant que le joueur n'a pas fixé ces limites. Vérifier que les limites précitées s'appliquent, d'une part, au montant cumulé des approvisionnements réalisés par le joueur par périodes de sept jours et, d'autre part, au montant cumulé des mises engagées par le joueur par périodes de sept jours.	Analyse documentaire et entretiens Tests de cheminement
EJF34	Décret n° 2010-518 du 19 mai 2010 - Art. 16	Vérifier que le joueur peut modifier les limites précitées à tout moment. Vérifier que lorsqu'il augmente l'une ou l'autre, la modification prend effet au plus tôt dans un délai de deux jours francs à compter de sa saisie par le joueur. Vérifier que lorsqu'il diminue l'une ou l'autre, la modification est d'effet immédiat. Vérifier que des mouvements successifs de hausse puis de baisse d'un plafond de modération n'entraînent pas une hausse du plafond initial avec effet immédiat.	Analyse documentaire et entretiens Tests de cheminement

EJF35	Décret n° 2010-518 du 19 mai 2010 - Art. 17	Vérifier que lors de la saisie du code secret visé à l'article 5 du décret n°2010-518, l'opérateur demande au joueur de déterminer un montant au-delà duquel les crédits disponibles inscrits sur son compte joueur sont automatiquement reversés sur son compte de paiement et qu'aucune opération de jeu ne peut être réalisée tant que le joueur n'a pas déterminé ce montant.	Analyse documentaire et entretiens Tests de cheminement
2. Mécanismes d'auto-exclusion			
EJF36	Loi n° 2010-476 du 12 mai 2010 - Art. 26 Décret n° 2010-518 du 19 mai 2010 - Art. 18	Vérifier la mise en place d'un dispositif permettant au joueur de demander en permanence son exclusion du jeu de manière temporaire ou définitive. Vérifier que le joueur détermine la durée de son exclusion temporaire et que celle-ci ne peut être inférieure à sept jours. Vérifier que l'exclusion définitive du joueur entraîne la clôture de son compte par l'opérateur et que le joueur ne peut solliciter à nouveau l'ouverture d'un compte avant l'expiration d'un délai de trois ans à compter de cette clôture.	Analyse documentaire et entretiens Tests de cheminement
EJF37	Décret n° 2010-518 du 19 mai 2010 - Art. 7, 10 et 18	Vérifier que la procédure de demande de clôture d'un compte à l'initiative du joueur est clairement distincte de la procédure de demande d'auto-exclusion sur le site Internet de l'opérateur.	Constatations sur le site Internet de l'opérateur
C. Interdits de jeu			
EJF38	Loi n° 2010-476 du 12 mai 2010 - Art. 26 Décret n°2010-518 du 19 mai 2010 - Art. 20 Arrêté du 8 juin 2010 NOR : BCRB1015075A	Vérifier que l'opérateur informe les joueurs des procédures d'inscription sur les fichiers des interdits de jeu tenus par les services du ministère de l'intérieur. Vérifier que l'opérateur fait figurer ce message sur les pages d'accueil de son site. Le message doit être présenté de manière accessible et aisément lisible. Vérifier que lorsque le joueur active ce message, il est renvoyé vers le service de communication en ligne de la procédure d'interdiction de jeu mis en place par le ministère de l'intérieur.	Constatations sur le site Internet de l'opérateur

VII. Prévention des conflits d'intérêts			
EJF39	Loi n° 2010-476 du 12 mai 2010 - Art. 32 et 33	Décrire la procédure mise en place par l'opérateur pour la prévention et la détection des conflits d'intérêts. Le cas échéant, procéder à l'analyse d'un contrat type de la société et de son règlement intérieur. Réaliser un test sur l'ensemble des dirigeants et mandataires sociaux de la société ainsi que sur un échantillon de salariés du groupe, afin de vérifier qu'ils ne détiennent pas de comptes joueurs.	Analyse documentaire Tests d'échantillonnage
EJF40 *	Loi n° 2012 - 476 du 12 mai 2010 - Art. 32	Annexer la liste actualisée des contrats de partenariat conclus par l'opérateur avec des personnes physiques ou morales organisant des courses hippiques, compétitions ou manifestations sportives ou y prenant part. Accompagner cette liste d'une note synthétique d'analyse de ces contrats.	Recherche documentaire
EJF41 *	Décret n° 2010-1289 du 27 octobre 2010	Pour les opérateurs de paris sportifs, vérifier que l'opérateur faisant l'objet de la certification respecte ses obligations légales relatives à la détention indirecte du contrôle au sens de l'article L.233-16 du code de commerce d'un organisateur de compétition ou manifestation sportives, d'une partie prenante à une compétition ou manifestation sportive ou d'un opérateur de jeux ou de paris en ligne.	Analyse documentaire

arjeL
Autorité de régulation des jeux en ligne
RÉPUBLIQUE FRANÇAISE

AVIS DU HAUT CONSEIL DU COMMISSARIAT AUX COMPTES

N° 2012-03 RENDU LE 22 MARS 2012 EN APPLICATION DE L'ARTICLE R.821-6 DU CODE DE COMMERCE RELATIF A LA POSSIBILITE, POUR UN COMMISSAIRE AUX COMPTES OU UN MEMBRE DE SON RESEAU D'INTERVENIR EN QUALITE DE « CERTIFICATEUR » AU SENS DE LA LOI N° 2010-476 DU 12 MAI 2010

ANNEXE III du Règlement relatif à la certification prévue à l'article 23 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne adopté par la décision n° 2014-018 du collège de l'Autorité de régulation des jeux en ligne en date du 17 mars 2014

Introduction

Le Haut Conseil a été saisi par l'Autorité de régulation des jeux en ligne (ARJEL) sur la compatibilité du statut de commissaire aux comptes avec celui de « *certificateur* » au sens de la loi n° 2010-476 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.

Depuis le 12 mai 2010, date de publication de la loi, les opérateurs agréés sont autorisés à proposer des paris hippiques, des paris sportifs et des jeux de cercle en ligne aux joueurs français.

Le dispositif mis en place prévoit notamment pour les opérateurs de faire contrôler certaines informations par un *« organisme indépendant »*, le *« certificateur »*. La loi ne prévoit pas de statut particulier pour le certificateur mais dispose en revanche que ce dernier doit être choisi dans une liste de certificateurs agréés établie par l'ARJEL.

La saisine de l'ARJEL s'inscrit dans le cadre de l'établissement de cette liste et en particulier de l'octroi de l'agrément de certificateur aux commissaires aux comptes qui le solliciteraient.

Le Haut Conseil a examiné cette saisine au cours de sa séance du 2 février 2012 et rend l'avis qui suit.

Avis du Haut Conseil

Le Haut Conseil a recueilli la position du Ministère de la Justice et des Libertés sur la question posée par l'ARJEL.

Le Ministère de la Justice et des Libertés a mentionné que *« (…) sous réserve de l'interprétation souveraine des cours et tribunaux, aucune incompatibilité absolue entre les fonctions de commissaire aux comptes et de certificateur au sens de la loi n° 2010-476 du 12 mai 2010 ne semble pouvoir être relevée »*.

Il a ajouté qu'il *« appartiendra toutefois au professionnel, avant d'accepter de telles fonctions, de s'assurer au préalable qu'elles ne risqueraient pas de le placer dans l'une ou l'autre des situations d'incompatibilités ou d'interdictions prévues par les textes »*.

Le Haut Conseil prend acte de la position du Ministère de la Justice et des Libertés.

Il relève en outre qu'en application des dispositions du II de l'article L. 822-11 du code de commerce *« il est interdit au commissaire aux comptes de fournir à la personne ou à l'entité qui l'a chargé de certifier ses comptes, ou aux personnes ou entités qui la contrôlent ou qui sont contrôlées par celle-ci au sens des I et II du même article, tout conseil ou toute autre prestation de services n'entrant pas dans les diligences directement liées à la mission de commissaire aux comptes, telles qu'elles sont définies par les normes d'exercice professionnel mentionnées au sixième alinéa de l'article L. 821-1 »*.

Le dernier alinéa du même article dispose que *« lorsqu'un commissaire aux comptes est affilié à un réseau national ou international, dont les membres ont un intérêt économique commun et qui n'a pas pour activité exclusive le contrôle légal des comptes, il ne peut certifier les comptes d'une personne ou d'une entité qui, en vertu d'un contrat conclu avec ce réseau ou un membre de ce réseau, bénéficie d'une prestation de services, qui n'est pas directement liée à la mission du commissaire aux comptes selon l'appréciation faite par le Haut Conseil du commissariat aux comptes en application du troisième alinéa de l'article L. 821-1 »*.

Aussi, le Haut Conseil a estimé qu'il lui incombait, sans préjudice des décisions que l'ARJEL pourrait prendre sous la législation qui lui est propre, d'examiner si les missions de « *certificateur* » peuvent être considérées, ou non, comme des prestations directement liées à la mission de commissaire aux comptes, condition nécessaire pour que ces missions puissent être réalisées par le commissaire aux comptes de l'opérateur auprès de cet opérateur, d'un opérateur qui le contrôle ou qui est contrôlé par lui, ou par un membre du réseau de ce commissaire aux comptes auprès de l'opérateur[1].

[1] Pour ce qui concerne les missions de « certificateur » qui pourraient être fournies par un membre du réseau du commissaire aux comptes de l'opérateur à cet opérateur, un opérateur qui le contrôle ou qui est contrôlé par lui, au sens des I et II de l'article

Le Haut Conseil a échangé avec des représentants de l'ARJEL et auditionné des certificateurs agréés aux fins d'apprécier la nature des travaux du certificateur et les relations qu'entretient ce dernier avec l'opérateur et avec l'ARJEL.

Les missions assignées au « *certificateur* » sont définies par la loi du 12 mai 2010[2] complétée par une décision du collège de l'ARJEL[3]. Elles portent sur le contrôle du respect, par l'opérateur, de l'ensemble de ses obligations légales et réglementaires.

Elles se décomposent en un volet dit « *technique* » portant sur les obligations relatives au dispositif de traitement informatique des opérations de jeux et en un volet dit « *général* » portant sur les obligations d'ordre juridique et financier.

Le Haut Conseil estime qu'il n'existe pas, à la date du présent avis, de norme d'exercice professionnel applicable à ces interventions. En conséquence celles-ci ne peuvent pas être réalisées par le commissaire aux comptes de l'opérateur ou par un membre du réseau du commissaire aux comptes, auprès de cet opérateur.

Le Haut Conseil souligne enfin que l'intervention d'un membre du réseau en qualité de « *certificateur* » au sein de la société qui contrôle ou qui est contrôlée par l'entité dont les comptes sont certifiés par le commissaire aux comptes reste subordonnée au respect des dispositions de l'article 24 du code de déontologie et d'éventuelles décisions intéressant les «*certificateurs*» que l'ARJEL pourrait estimer utile de prendre, en particulier celles visant à préciser les critères d'indépendance et d'impartialité prévus par son règlement traitant de la procédure d'inscription sur la liste des organismes certificateurs.

Christine THIN
Présidente

L. 233-3 du code de commerce, l'article 24 du code de déontologie prévoit que le commissaire aux comptes doit s'assurer que son indépendance ne se trouve pas affectée par cette prestation de services. Il n'existe pas en revanche de disposition prévoyant qu'une norme doit définir cette prestation.

[2] Article 23, II et III.

[3] Décision n° 2010-065 du 23 juillet 2010.