COLLEGE DE L'AUTORITE DE REGULATION DES JEUX EN LIGNE

DECISION N°2010-065 EN DATE DU 13 JUILLET 2010 PORTANT ADOPTION DU REGLEMENT DE PROCEDURE D'INSCRIPTION SUR LA LISTE DES ORGANISMES CERTIFICATEURS

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, 34 et 43 ;

Après en avoir délibéré le 13 juillet 2010 ;

DECIDE :

Article 1er :

Le règlement relatif à la procédure d'inscription sur la liste des organismes indépendants réalisant les certifications prévues par 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 rédigé comme suit :

"REGLEMENT RELATIF A LA PROCEDURE D'INSCRIPTION SUR LA LISTE DES ORGANISMES INDEPENDANTS REALISANT LES CERTIFICATIONS PREVUES PAR LA LOI N°2010-476 DU 12 MAI 2010 RELATIVE A L'OUVERTURE A LA CONCURRENCE ET A LA REGULATION DU SECTEUR DES JEUX D'ARGENT ET DE HASARD EN LIGNE

Article 1er : Définitions et règle retenue pour la computation des délais

Les termes "ARJEL" et "Autorité" désignent l'Autorité de régulation des jeux en ligne.

Les organismes indépendants mentionnés 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 sont désignés dans le présent règlement sous les termes de : "organisme(s) certificateur(s)" ou "certificateur(s)".

La computation des délais prévus par le présent règlement est opérée dans les conditions fixées par l'article 642 du code de procédure civile français.

Article 2 : Objet de la procédure

La procédure définie par le présent règlement décrit le processus d'inscription par l'ARJEL d'un organisme sur la liste des organismes indépendants mentionnés à l'article 23 de la loi n° 2010-476 du 12 mai 2010.

La procédure d'inscription sur la liste des organismes certificateurs permet de s'assurer que le demandeur à l'inscription sur cette liste :

a) est apte à certifier le respect par les opérateurs de jeux et de paris en ligne agréés par l'ARJEL des obligations définies aux articles 31 et 38 de la loi n°2010-476 du 12 mai 2010, conformément aux dispositions du II de l'article 23 de cette même loi ;

b) est apte à certifier le respect par ces mêmes opérateurs de l'ensemble de leurs obligations légales (législatives et réglementaires) conformément aux dispositions du III de l'article 23 de la loi n°2010-476 du 12 mai 2010 ;

c) est apte à certifier le respect des obligations légales (législatives et réglementaires) à la suite d'une mise en demeure de l'ARJEL ayant constaté un manquement d'un opérateur agréé conformément aux dispositions de l'article 43 de la loi n°2010-476 du 12 mai 2010 ;

d) est indépendant vis-à-vis des opérateurs de jeux et de paris en ligne ;

e) que sa structure juridique et son organisation sont compatibles avec l'exercice d'une activité d'évaluation et de certification.

Les éléments sur lesquels porte notamment la certification prévue au II de l'article 23 de la loi n°20 10-476 du 12 mai 2010 figurent en annexe I au présent règlement.

Les éléments sur lesquels porte notamment la certification prévue au III de l'article 23 de la loi n°2 010-476 du 12 mai 2010 figurent en annexe II au présent règlement.

Article 3 : Demande d'inscription

Article 3.1. Décision d'inscription

La décision d'inscription sur la liste des organismes certificateurs est prononcée par l'ARJEL.

Cette décision peut énoncer les obligations particulières auxquelles est soumis le certificateur.

La décision d'inscription sur la liste des organismes certificateurs est délivrée *intuitu personae*.

Un certificateur est inscrit sur la liste des organismes certificateurs pour accomplir les évaluations définies aux II et III de l'article 23 de la loi n° 2010-476 ainsi que celles prévues en au II de l'article 43 de la loi n°2010-476, quelles que soient les catégo ries de jeux ou de paris en ligne proposées par un opérateur demandeur de la certification.

Article 3.1.1. Durée de validité de l'inscription

La décision d'inscription est valable cinq ans à compter de la date de sa notification.

Article 3.1.2. Notification et publication de la décision d'inscription

A l'issue de l'examen du dossier de demande d'inscription par l'ARJEL, la décision d'inscription est, en même temps qu'elle est notifiée au bénéficiaire par courrier recommandé avec avis de réception et/ou courrier électronique recommandé, publiée sur le site internet de l'Autorité.

Toute décision de refus d'inscription est motivée et notifiée au demandeur.

Article 3.2. Demande d'inscription

La demande d'inscription sur la liste des organismes certificateurs peut être faite par toute entreprise, quelle que soit sa forme juridique, établie dans un Etat membre de l'Union européenne ou un Etat partie à l'accord sur l'espace économique européen.

La demande d'inscription comprend un dossier de candidature et un mémoire technique rédigés en langue française. Lorsque la demande d'inscription comporte des pièces qui ne sont pas rédigées en français, ces dernières sont traduites en français.

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

Autorité de régulation des jeux en ligne (ARJEL)
Direction des Agréments et de la Supervision
99-101, rue Leblanc
75015 PARIS

Dans l'hypothèse où l'ARJEL constate que la demande d'inscription est incomplète, l'Autorité invite le candidat à lui transmettre les pièces et/ou renseignements manquants dans un délai de 15 jours, par tout moyen permettant d'attester de la réception y compris par voie électronique.

Au terme de ce délai, toute demande demeurée incomplète entraîne le prononcé par l'ARJEL d'une décision de refus d'inscription.

Article 3.2.1. Phase préparatoire et durée de l'instruction

A la réception d'une demande d'inscription, l'ARJEL procède à son enregistrement et en accuse réception.

L'instruction d'une demande d'inscription est de 2 mois à compter de sa date de réception, durée au terme de laquelle, en l'absence de décision expresse, l'ARJEL est réputée avoir rejeté la demande, conformément aux dispositions de l'article 21 de la loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations.

Article 3.2.2. Objectif et composition du dossier de candidature.

Le dossier de candidature permet à l'ARJEL de vérifier qu'un demandeur dispose des capacités professionnelles, techniques, juridiques et financières suffisantes pour accomplir les évaluations nécessaires à la certification des opérateurs de jeux ou de paris en ligne et ainsi prétendre à son inscription sur la liste des organismes certificateurs.

Ce dossier comprend les documents et éléments suivants :

- Une photocopie d'un extrait Kbis de la société ou tout document équivalent pour les entreprises non françaises ;

- Si l'entreprise candidate n'est pas une personne morale, celle-ci doit justifier :

    - de l'identité de son ou de ses propriétaires, par la production d'une copie d'une pièce d'identité s'il s'agit de personnes physiques, d'un extrait K *bis* ou un équivalent s'il s'agit de personnes morales et, le cas échéant, du contrat de société en participation ;

    - de son numéro SIRET ou un équivalent, et de ceux de ses associés s'il est question d'une société en participation.

- Un sous-dossier constitué des éléments permettant d'apprécier les capacités professionnelles du candidat comprenant :

    - Une présentation générale de l'entreprise, avec notamment, le cas échéant, un ou des organigrammes présentant la place du candidat dans le groupe si celui-ci est accueilli dans un groupe de sociétés ;

- Les expériences et références nationales et internationales récentes de prestations similaires et les périodes de réalisation des prestations. Le candidat devra justifier notamment de ses compétences pour les activités d'évaluation et de certification de l'architecture et de la sécurité de systèmes d'information d'une part et de ses compétences notamment juridiques et financières permettant d'évaluer le respect par les opérateurs de jeux en ligne de leurs obligations légales (législatives et réglementaires) d'autre part ;

- La liste et les *curriculum vitae* des experts techniques identifiés pour réaliser les prestations d'expertise. Ces documents devront notamment faire apparaître, le cas échéant, les contributions (publications, conférences, formations, certifications, *etc…*) de ces experts ; les experts réalisant les certifications devront impérativement être validés au préalable par l'ARJEL ;

- Des rapports d'analyse « type », mettant en avant les méthodologies et le niveau de profondeur des analyses conduites par l'organisme candidat dans des domaines d'expertise similaires à ceux abordés dans le cadre de la certification, et plus particulièrement dans les domaines :

    - 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 de démontrer les vulnérabilités du composant, et de déduire de cette analyse une liste de recommandations ;

    - des audits de configuration de plate-forme d'hébergement, dont l'objectif est d'évaluer, par rapport à l'état de l'art et à aux politiques de sécurité générale et technique de l'entité, 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)

    - des audits de conformité juridique et financière.

- Une déclaration, accompagnée de tout document utile, engageant le candidat, attestant de son indépendance vis-à-vis des opérateurs de jeux ou de paris en ligne et, de façon générale, à l'égard de toute personne pouvant compromettre cette indépendance ;

- Une déclaration concernant le chiffre d'affaires global et, le cas échéant, le chiffre d'affaires relatif 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 ;

- Tout autre document pouvant apporter des informations jugées utiles par le candidat.

Article 3.2.3. Mémoire technique et critères

En sus du dossier de candidature, le candidat produit un mémoire technique permettant à l'ARJEL d'évaluer s'il est en mesure de remplir les critères définis ci-après :

Critère n°1 : Indépendance et impartialité

Le certificateur doit apporter les éléments justificatifs et les engagements permettant à l'ARJEL de vérifier que les évaluations qu'il réalise sont faites :

- De façon impartiale : le certificateur ne subit pas de pressions visant à modifier les résultats des travaux d'évaluation et s'engage à déclarer à l'ARJEL toute pression, quelle qu'en soit l'origine ;

- De façon indépendante : le certificateur ne doit pas accepter de demande de certification qui le placerait en situation de conflit d'intérêts avec un opérateur de jeux en ligne ou un sous-traitant. Un conflit d'intérêts s'entend d'une situation dans laquelle une même personne poursuit deux ou plusieurs intérêts et lorsque ces intérêts sont contradictoires.

Critère n°2 : Confidentialité

Le certificateur doit prendre les dispositions permettant d'assurer la confidentialité des éléments portés à sa 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.

Critère n°3 : Sous-traitance

- Cas normal : sous-traitant accepté au stade de la demande d'inscription

La sous-traitance ne peut porter que sur une partie de l'évaluation et doit avoir été préalablement acceptée par l'ARJEL à qui l'organisme certificateur transmet, dès le stade de la demande d'inscription, les documents nécessaires attestant, d'une part, des capacités professionnelles, techniques, juridiques et financières du sous-traitant et d'autre part, du respect par le sous-traitant des critères énumérés au présent règlement.

Dans l'hypothèse où, le certificateur envisage de recourir à un autre sous-traitant que celui accepté par l'ARJEL lors de la demande d'inscription, le nouveau sous-traitant doit être accepté par l'Autorité, selon les mêmes modalités que lors de la demande d'inscription, préalablement à l'accomplissement de toute nouvelle opération concourant à l'activité de certification de l'organisme agréé.

- Cas dérogatoire : sous-traitant accepté en cours de validité d'agrément.

A titre exceptionnel, si des circonstances propres à la situation du certificateur ou à une ou plusieurs opérations de certification en cours ou à venir l'exigent, un organisme certificateur n'ayant pas déclaré au stade de la demande d'agrément son intention de recourir à un sous-traitant, peut recourir à un tel prestataire, sous réserve de son acception préalable par l'ARJEL. A cet effet, l'organisme certificateur transmet à l'Autorité les documents nécessaires attestant, d'une part, des capacités professionnelles, techniques, juridiques et financières du sous-traitant, et, d'autre part, du respect par le sous-traitant des critères définis au présent règlement et des obligations résultant de l'inscription conformément à l'article 4.

Critère n°4 : Prescriptions relatives au personnel

Critère n° 4-1 : Les personnes autorisées à signer les rapports d'évaluation doivent être indiquées à l'ARJEL.

Critère n° 4-2 : Le personnel de l'organisme certificateur ou de son éventuel sous-traitant doit être compétent en technologies de l'information, qualifié et expérimenté en évaluation de l'architecture de systèmes d'information et de leur sécurité ainsi qu'en audit de conformité légale. L'estimation de cette expérience est du ressort de l'ARJEL. Notamment, la compétence du personnel du certificateur et le cas échéant de son sous-traitant doit être conforme à la nature des certifications exigées par les dispositions des articles 23 et 43 de la loi n°201 0-476 du 12 mai 2010.

Critère n° 4-3 : A l'occasion de la demande d'inscription, les *curriculum vitae* des personnels du certificateur et, le cas échéant, du sous-traitant, chargés de réaliser les évaluations doivent être transmis à l'ARJEL pour validation. L'ARJEL se réserve le droit de refuser qu'un personnel indiqué par l'organisme certificateur participe à certaines certifications.

Les compétences du personnel qui réalise les certifications doivent être suivies.

Critère n° 5 : Relations commerciales entre l'organisme certificateur et l'opérateur de jeux ou de paris en ligne demandeur de la certification

Conformément à l'article 23 de la loi n° 2010-476, le coût des certifications est à la charge de l'opérateur de jeux ou de paris en ligne.

Les conditions de la prise en charge des opérations de certification sont fixées par contrat entre l'organisme certificateur et l'opérateur de jeux ou de paris en ligne.

L'ARJEL doit être mentionnée 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 doit prévoir que l'opérateur agréé remet au certificateur un exemplaire du dossier de demande d'agrément qu'il a remis à l'ARJEL.

Une copie du contrat conclu entre l'opérateur et l'organisme certificateur doit être transmise à l'ARJEL.

Critère n° 6 : Compétences techniques, juridiques et financières

A la demande de l'ARJEL, l'organisme certificateur doit être en mesure de démontrer qu'il dispose des compétences nécessaires pour mener à bien les opérations de certification pour lesquelles il est inscrit sur la liste des organismes certificateurs. Cette démonstration se fait dans un délai fixé par l'ARJEL.

Critère n° 7 : Méthodes et procédures de travail concernant la réalisation des rapports d'évaluation

Dans son activité de certification et la réalisation des rapports, l'organisme certificateur doit travailler selon une méthodologie compatible avec les exigences de l'évaluation notamment en termes de contrôle et d'assurance qualité.

Tous les rapports de certification sont rédigés ou traduits en langue française et sont transmis à l'ARJEL qui procède à la vérification de tout ou partie d'entre eux afin de s'assurer de la cohérence du travail réalisé et de mettre à jour la liste des organismes certificateurs.

Article 3.2.4. Audition de l'organisme certificateur

Dans le délai d'un mois à compter de la réception de la demande d'inscription, l'ARJEL peut, si elle l'estime nécessaire, inviter le candidat, par courrier recommandé avec avis de réception et/ou courrier électronique recommandé, à un entretien pendant lequel il est auditionné afin de vérifier sa capacité à répondre aux critères définis à l'article 3.2.3.

Le cas échéant, si l'ARJEL l'estime nécessaire, un ou plusieurs entretiens complémentaires sont organisés.

Article 4 : Obligations résultant de l'inscription sur la liste des organismes certificateurs

L'organisme certificateur inscrit sur la liste établie par l'ARJEL s'engage à respecter les critères définis au présent règlement. En particulier, l'organisme certificateur :

- s'engage à refuser toute demande d'évaluation qui le mettrait dans une situation de conflit d'intérêts au regard de son activité d'évaluation et à avertir l'ARJEL dès la survenance de tout conflit ;

- rend compte immédiatement à l'ARJEL de tout changement dans la structure de son entreprise, de son organisation ou de son personnel, et fournit les pièces justificatives de ces modifications ;

- autorise les membres de l'ARJEL à contrôler à tout moment le déroulement d'une évaluation, à assister à des travaux d'évaluation et à contrôler que les critères définis au présent règlement sont respectés ;

- se conforme aux obligations légales de protection de l'information ;

- s'engage à assurer la non-divulgation aux tiers des informations relatives à ses outils et à ses méthodes d'évaluation.

Article 5 : Suivi de l'inscription sur la liste des organismes certificateurs

L'ARJEL suit de façon continue les activités de l'organisme certificateur.

L'ARJEL peut s'assurer à tout moment que le certificateur continue à satisfaire aux critères et aux obligations résultant de l'inscription sur la liste des organismes certificateurs par un audit.

Article 6 : Renouvellement de l'inscription

Au plus tard 6 mois avant l'échéance de la période de validité de l'inscription, l'organisme certificateur doit demander à l'ARJEL, s'il le souhaite, le renouvellement de cette inscription.

L'instruction de cette demande se déroule selon les mêmes modalités que la demande initiale, telles que décrites aux articles 3 à 3.2.4. Elle doit permettre :

- de vérifier que les critères et obligations définis au présent règlement sont toujours respectés ;

- de faire le point sur les écarts constatés et formalisés pendant la période d'inscription ainsi que sur les actions correctives mises en œuvre.

Si les conditions sont satisfaites, une nouvelle décision d'inscription est prononcée par l'ARJEL.

L'absence de demande de renouvellement, dans les conditions prévues ci-dessus, vaut renoncement à l'inscription au-delà de sa durée de validité. Lorsque ce terme est atteint l'ARJEL lui adresse une lettre de notification par courrier recommandé avec avis de réception et/ou par courrier électronique recommandé et le retire de la liste des organismes certificateurs.

Article 7 : Suspension de l'inscription sur la liste des organismes certificateurs

L'inscription sur la liste des organismes certificateurs peut être suspendue par l'ARJEL lorsque l'organisme certificateur ne répond pas aux critères de l'article 3.2.3 et aux obligations fixées par la décision d'inscription en application de l'article 4 ;

Lorsqu'une suspension de l'inscription est envisagée par l'ARJEL, l'Autorité en informe l'organisme certificateur par courrier recommandé avec avis de réception et/ou courrier électronique recommandé et l'invite, dans un délai qu'elle détermine et qui ne peut être inférieur à 8 jours à compter de la réception de la notification, à présenter ses observations écrites ou orales et à mettre en place les mesures correctives nécessaires afin d'être à nouveau en conformité avec les critères de l'inscription et les obligations qui en résultent.

Si au terme du délai susmentionné, le certificateur n'a pas, par ses observations ou par la mise en œuvre des mesures correctives appropriées, démontré qu'il répondait à nouveau aux critères et obligations définies au présent règlement, l'ARJEL suspend l'inscription par une décision notifiée à l'organisme certificateur par courrier recommandé avec avis de réception et/ou courrier électronique recommandé.

La décision de l'ARJEL fixe la durée de la suspension et propose des mesures correctives.

Pendant la durée de la suspension, le certificateur en cause est retiré de la liste des organismes certificateurs agréés par l'ARJEL.

L'organisme certificateur est tenu de notifier sa suspension aux opérateurs avec lesquels il est en contrat et doit en justifier auprès de l'ARJEL.

Durant la période de suspension, l'ARJEL décide au cas par cas :

- de l'acceptation ou du refus de nouveaux dossiers de certifications soumis par le certificateur ;

- de la prise en compte ou non des résultats des projets d'évaluation en cours menés par le certificateur.

Si à l'issue de cette période de suspension, l'ARJEL estime que les causes ayant entraîné la suspension ne sont pas corrigées ou en voie de l'être, une procédure de retrait définitif de la liste des organismes certificateurs est engagée.

Dans le cas contraire, l'organisme certificateur est averti de la fin de sa suspension et qu'il est réintégré dans liste susmentionnée.

Article 8 : Retrait définitif de la liste des organismes certificateurs en cas de manquements aux critères et obligations

Article 8.1. Causes du retrait définitif de la liste des organismes certificateurs

L'organisme certificateur peut être retiré définitivement de la liste des organismes certificateurs par l'ARJEL.

La décision de retrait définitif est notifiée à l'organisme certificateur concerné par courrier recommandé avec avis de réception et/ou courrier électronique recommandé.

Une liste non limitative des causes de retrait définitif en cas de manquements aux critères et obligations d'inscription est donnée ci-dessous à titre d'exemples :

- les causes ayant entraîné une suspension d'inscription n'ont pas été corrigées ;

- la méconnaissance des critères d'inscription et des obligations fixées par la décision d'inscription est d'une gravité telle qu'elle justifie un retrait non précédé d'une mesure de suspension.

Le bénéficiaire de l'inscription doit être mis en mesure de présenter sa défense par des observations écrites ou orales dans un délai fixé par l'ARJEL et qui ne peut être inférieur à 15 jours à compter de la notification, par courrier recommandé avec avis de réception et/ou courrier électronique recommandé, de l'ouverture d'une procédure de retrait par l'Autorité.

Au terme du délai susmentionné, l'ARJEL prononce ou non le retrait au vu des pièces du dossier et des observations produites par l'organisme certificateur.

Article 8.2. Conséquences du retrait définitif de la liste des organismes certificateurs

Le certificateur concerné est retiré de la liste des organismes certificateurs agréés.

Aucune nouvelle évaluation ne peut être engagée et l'organisme certificateur met fin immédiatement à toute opération d'évaluation en cours.

L'organisme certificateur doit remettre à l'ARJEL l'ensemble des dossiers relatifs aux évaluations menées.

L'organisme est tenu de notifier son retrait de la liste des organismes certificateurs aux opérateurs avec lesquels il est en contrat et doit en justifier auprès de l'ARJEL. En cas de défaillance de l'organisme, l'Autorité se réserve le droit de prévenir les opérateurs agréés et autres acteurs concernés par les évaluations en cours, du retrait de l'inscription sur la liste des organismes certificateurs de l'organisme.

Article 9 : Cessation d'activité de l'organisme certificateur

La demande de cessation d'activité est transmise à l'ARJEL par courrier recommandé avec avis de réception.

La demande de cessation d'activité entraîne le retrait de l'inscription sur la liste des organismes certificateurs établie par l'ARJEL.

Une notification de l'arrêt de l'inscription sur la liste des organismes certificateurs est transmise à l'organisme par courrier recommandé avec avis de réception et/ou par courrier électronique recommandé.

* * *
*

Annexe I : Eléments sur lesquels porte notamment la certification prévue au II de l'article 23 de la loi n°2010-476 du 12 mai 2010.

Dans le cadre de la certification unique à 6 mois du composant frontal et de son infrastructure d'hébergement, l'analyse s'assurera en premier lieu du respect :
- des fonctionnalités spécifiées dans la partie 4 du Dossier des Exigences Techniques (DET) et dans les parties 1 et 3.1 de l'Annexe au DET ;
- des exigences techniques jugées impérativement opérationnelles lors de l'ouverture de l'activité de jeu, et marquées d'un astérisque dans la partie 5.7 du DET ([E*]).

Cette vérification de premier niveau consistera à :
- analyser la documentation existante et donner un avis sur sa lisibilité et sa complétude. On s'appuiera sur les référentiels suivants :
  - DET,
  - le dossier de demande d'agrément remis par l'opérateur,
  - la documentation d'installation, d'administration et d'exploitation des composants qui constituent le frontal,
  - les documents techniques portant sur les fonctions et mécanismes de sécurité implantés,
- reprendre les fonctionnalités spécifiées dans le DET (parties 4 et 5.7) et l'Annexe au DET (parties 1 et 3.1), et les tester ;
- indiquer les tests fonctionnels en précisant :
  - la fonctionnalité testée en cohérence avec les fonctionnalités répertoriées dans le DET,
  - les conditions du test (par exemple :
    - requête HTTP en entrée, taille, type,

        - fichier ou flux de sortie, taille type, analyse éventuelle du cryptogramme, le cas échéant, etc.),

    - les limites de la fonctionnalité s'il y en a,
    - si la fonctionnalité est conforme ou pas,
    - des éléments d'appréciation (avis d'expert).

Cette vérification de premier niveau sera complétée d'un audit applicatif à caractère intrusif portant sur le capteur. L'audit consistera à effectuer une recherche de vulnérabilités en s'appuyant sur :

- l'analyse succincte du code source de la partie capteur, essentiellement au niveau des fonctions de sécurité et des fonctions de manipulation des entrées utilisateur ; analyser le code source disponible, et donner un avis sur sa lisibilité et sa structuration dans la mesure du temps disponible, et selon la pertinence de cette analyse. Il ne s'agit pas de réaliser une analyse exhaustive du code source (ou audit de code) mais d'effectuer des tests de sécurité pratiques en s'appuyant sur le code source afin d'en faciliter et d'en approfondir l'analyse ;
- la réalisation de tests d'intrusion sur la partie capteur (envoi de requêtes HTTP mal ou spécifiquement formées, tentatives d'injection, d'exploitation de vulnérabilités dues à des défauts d'implantation, etc.), et l'analyse de son comportement lors du traitement de ces données inattendues.

Plan synthétique du rapport

- Synthèse du rapport :
    - présentation du candidat opérateur et de l'architecture technique
    - nombres de jour/homme consacrés à chaque point
    - synthèse stratégique des résultats obtenus par point
    - décision sur la certification
- vérification du respect des exigences fonctionnelles de la partie 4 du DET et de la partie 3.1 de l'Annexe au DET :
    - caractérisation des éventuelles différences et des impacts associés
- vérification du respect du format des données stockées dans le coffre-fort (partie 1 de l'Annexe au DET) :
    - caractérisation des éventuelles différences et des impacts associés
- vérification du respect des exigences [E*] du DET (partie 5.7) concernant le seul frontal :
    - caractérisation des éventuelles différences et des impacts associés
- analyse de sécurité :
    - synthèse technique de l'analyse du capteur, et du frontal
    - synthèse des vulnérabilités, classées par criticité et coût
    - synthèse des recommandations, classées criticité et coût
    - rapport d'analyse de la sécurité logicielle du capteur :
        - présentation fonctionnelle du code
        - présentation des fonctions de sécurité
        - analyse de la sécurité de l'implantation logicielle
    - rapport d'analyse de la sécurité du frontal
        - analyse de la stratégie de sécurité : politique de sécurité technique, procédures, etc.
        - analyse de l'architecture technique ;
        - analyse des configurations des principaux éléments du frontal, au niveau système, réseau et applicatif,
- tableau synthétique des résultats par point

Annexe II : Eléments sur lesquels porte notamment la certification prévue au III de l'article 23 de la loi n°2010-476 du 12 mai 2010.

Certification annuelle.

Partie 1 : Obligations techniques

Les opérations de vérification portent sur l'infrastructure globale d'hébergement du service de jeu en ligne.

Cette vérification comprendra :

- d'une part, l'ensemble des exigences du DET (soit les exigences [E] et [E*] de la partie 5.7 du DET ainsi que les exigences de la partie 4) ;
- d'autre part, la réalisation d'un audit de configuration de premier niveau et d'un test d'intrusion en boîte blanche, dans la continuité des audits qui auront été réalisés au préalable dans le cadre de la demande d'agrément. Il ne s'agira pas d'un simple test de vulnérabilités automatiques, mais d'une recherche manuelle ou assistée de vulnérabilités applicatives, conduite par un expert technique et expérimenté.

Plan synthétique du rapport

- Synthèse du rapport :
    - présentation du candidat opérateur et de l'architecture technique,
    - nombres de jour/homme consacrés à chaque point,
    - synthèse stratégique des résultats obtenus par point,
    - décision sur la certification ;
- vérification du respect des exigences fonctionnelles de la partie 4 (DET) :
    - caractérisation des éventuelles différences et des impacts associés ;
- vérification du respect des exigences [E*] du DET (partie 5.7) pour tout le SI :
    - caractérisation des éventuelles différences et des impacts associés ;
- vérification du respect des exigences [E] du DET (partie 5.7) pour tout le SI :
    - caractérisation des éventuelles différences et des impacts associés ;
- analyse de sécurité :
    - synthèse technique de l'audit de premier niveau et du test d'intrusion ;
    - synthèse des vulnérabilités, classées par criticité et coût ;
    - synthèse des recommandations, classées criticité et coût ;
    - rapport du test d'intrusion :
        - déroulement linéaire du test d'intrusion, avec description explicite de la méthodologie employée pour détecter les vulnérabilités et les exploiter, le cas échéant ;
    - rapport d'audit de premier niveau, suivant les grands thèmes suivants :
        - analyse de la stratégie de sécurité : politique de sécurité technique, procédures, etc.
        - analyse de l'architecture technique ;
        - analyse des configurations des principaux éléments de la plate-forme, au niveau système, réseau et applicatif,
- tableau synthétique des résultats par point.

Partie 2 : Obligations générales

L'organisme certificateur devra notamment analyser la conformité des éléments listés aux points I à VIII suivants :

I. Informations personnelles
1) Moyens humains
2) Moyens matériels
3) Evolution de l'actionnariat

II. Informations économiques, financières et comptables
1) Tenue d'une comptabilité séparée par type d'agrément
2) Compte de paiement de l'opérateur

III. Informations relatives au site de jeu en ligne
1) Contrats de sous-traitance
2) Activités et prestations proposées sur le site
3) Nom(s) de domaine utilisé(s)
4) Espaces publicitaires sur le site
5) Liste des sites affiliés

IV. Informations relatives aux opérations de jeux ou de paris en ligne proposés
1) Procédure de réclamation gratuite
2) Respect de la typologie des jeux
3) Conformité des jeux au droit applicable

V. Informations relatives aux comptes joueurs
1) Ouverture du compte joueur
2) Moyens et instruments de paiement
3) Modalités d'encaissement et de paiement des mises et des gains

VI. Informations relatives à la lutte contre les activités frauduleuses ou criminelles, en particulier le blanchiment de capitaux et le financement du terrorisme

VII. Informations relatives à la lutte contre le jeu excessif ou pathologique
1) Moyens mis en place
2) Les modérateurs de jeu
3) Interdits de jeu

VIII. Prévention des conflits d'intérêts. "

Article 2 :

Le directeur général de l'Autorité est chargé de l'exécution de la présente décision qui sera publiée sur le site Internet de l'Autorité de régulation des jeux en ligne.

Le directeur général est chargé d'assurer la publicité de l'appel à candidature pour l'inscription sur la liste établie par l'ARJEL des organismes certificateurs par une annonce publiée au *Journal Officiel* de l'Union Européenne et sur le site de l'Autorité.

Fait à Paris, le 13 juillet 2010 ;

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

Jean-François VILOTTE