RÉPUBLIQUE FRANÇAISE

_____

Autorité nationale des jeux

_____

DÉCISION N° 2022-219 DU 20 OCTOBRE 2022 PORTANT ADOPTION DES EXIGENCES TECHNIQUES RELATIVES À LA CERTIFICATION DES OPÉRATEURS DE JEUX D'ARGENT ET DE HASARD AGRÉÉS OU TITULAIRES DE DROITS EXCLUSIFS

Le collège de l'Autorité nationale des jeux,

Vu la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information ;

Vu le code de la sécurité intérieure, notamment ses articles L. 320-3 et L. 320-4 ;

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

Vu la notification n° 2022/470/F adressée à la Commission européenne le 5 juillet 2022 ;

Après avoir entendu le commissaire du gouvernement, en ses observations, et en avoir délibéré le 20 octobre 2022,

DÉCIDE :

Article 1er : Les exigences techniques relatives à la certification des opérateurs de jeux d'argent et de hasard agréés ou titulaires de droits exclusifs annexées à la présente décision sont adoptées.

Article 2 : Les certifications obtenues avant l'entrée en vigueur de ces exigences techniques conservent leur validité annuelle.

Article 3 : Le directeur général de l'Autorité nationale de jeux est chargé de l'exécution de la présente décision qui sera publiée sur le site Internet de l'Autorité.

Fait à Paris, le 20 octobre 2022.

La Présidente de l'Autorité nationale des jeux

Isabelle FALQUE-PIERROTIN

Décision publiée sur le site de l'ANJ le 26 octobre 2022

AUTORITÉ NATIONALE DES JEUX

RÉPUBLIQUE FRANÇAISE

EXIGENCES TECHNIQUES RELATIVES A LA CERTIFICATION DES OPERATEURS DE JEUX AGREES OU TITULAIRES DE DROITS EXCLUSIFS

Résumé

Conformément à l'article 23 de la Loi n°2010-476 du 12 mai 2010, les opérateurs agréés ou titulaires de droits exclusifs sont soumis à une procédure de certification (à 6 mois et annuelle).

Un régulateur au service d'un jeu sûr, intègre et maîtrisé

Table des matières

I Présentation générale

I.1 Rappel des obligations légales et réglementaires

Article L.320-3 du code de la sécurité intérieure :

« La politique de l'État en matière de jeux d'argent et de hasard a pour objectif de limiter et d'encadrer l'offre et la consommation des jeux et d'en contrôler l'exploitation afin de :

1° Prévenir le jeu excessif ou pathologique et protéger les mineurs ;

2° Assurer l'intégrité, la fiabilité et la transparence des opérations de jeu ;

3° Prévenir les activités frauduleuses ou criminelles ainsi que le blanchiment de capitaux et le financement du terrorisme ;

4° Veiller à l'exploitation équilibrée des différents types de jeu afin d'éviter toute déstabilisation économique des filières concernées. »

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 :

« I. — Toute entreprise titulaire de l'agrément d'opérateur de jeux et paris en ligne prévu à l'article 21 respecte les obligations prévues aux articles 15 à 19.

II. — Dans un délai de six mois à compter de la date de mise en fonctionnement du support prévu à l'article 31, l'opérateur de jeux ou de paris en ligne transmet à l'Autorité nationale des jeux un document attestant de la certification qu'il a obtenue, laquelle porte sur le respect par ses soins des obligations relatives aux articles 31 et 38. Cette certification est réalisée par un organisme indépendant choisi par l'opérateur au sein d'une liste établie par l'Autorité nationale des jeux. Le coût de cette certification est à la charge de l'opérateur de jeux ou de paris en ligne.

III. — Dans un délai d'un an à compter de la date d'obtention de l'agrément prévu à l'article 21, l'opérateur de jeux ou de paris en ligne ou l'opérateur titulaire de droits exclusifs transmet à l'Autorité nationale des jeux un document attestant de la certification qu'il a obtenue. Cette certification porte sur le respect par ses soins de l'ensemble des exigences techniques déterminées par l'Autorité en matière d'intégrité des opérations de jeux et de sécurité des systèmes d'information. Elle est réalisée par un organisme indépendant choisi par l'opérateur au sein de la liste mentionnée au II. Le coût de cette certification est à sa charge.

La certification fait l'objet d'une actualisation annuelle.

Un décret détermine les conditions d'application du présent III. »

VIII de l'article 34 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 :

« VIII. — L'Autorité nationale des jeux fixe les caractéristiques techniques des plates-formes et des logiciels de jeux et de paris en ligne des opérateurs soumis à un régime d'agrément et des opérateurs titulaires de droits exclusifs. Elle en évalue périodiquement le niveau de sécurité. […]

Elle détermine les exigences techniques en matière d'intégrité des opérations de jeux et de sécurité des systèmes d'information auxquelles doivent se conformer les opérateurs. Elle détermine les

paramètres techniques des jeux en ligne pour l'application des décrets prévus aux articles 13 et 14 de la présente loi.

Elle s'assure de la qualité des certifications réalisées en application de l'article 23. Elle établit la liste des organismes certificateurs et peut procéder à sa modification. Elle est destinataire des rapports de certification prévus au même article.

Elle évalue les contrôles internes mis en place par les opérateurs. A cette fin, elle peut procéder ou faire procéder à tout audit des systèmes d'information ou des processus.

Dans des conditions fixées par décret, elle évalue les résultats des actions menées par les opérateurs en matière d'intégrité du jeu et de système d'information et peut leur adresser des prescriptions à ce sujet. […] »

Dispositions des articles 11 à 24 du décret n° 2020-1349 du 4 novembre 2020 relatif aux modalités de régulation de l'Autorité nationale des jeux :

« Chapitre 1er : Conditions d'inscription sur la liste des organismes certificateurs (Articles 11 à 15)[…]

Chapitre 2 : Obligations des organismes certificateurs (Articles 16 à 19) […]

Chapitre 3 : Travaux de certification (Articles 20 à 24)

Article 20 :

Conformément aux dispositions de l'article 23 de la loi du 12 mai 2010 susvisée, les travaux de certification portent sur le respect par l'opérateur de l'ensemble des obligations techniques applicables à son activité.

L'Autorité nationale des jeux détermine la méthode, la nature et l'étendue des contrôles menés par les organismes certificateurs.

Article 21 :

Les opérations d'analyse conduites par l'organisme certificateur ne sont pas itératives au cours d'une même certification : chaque exigence contrôlée fait l'objet d'un contrôle unique. Des échanges peuvent avoir lieu au moment du contrôle entre l'organisme certificateur et l'opérateur dont il assure la certification. Toutefois, une fois le contrôle effectué, ces échanges ne peuvent en aucun cas conduire l'organisme certificateur à effectuer une nouvelle analyse.

En particulier, les modifications, le cas échéant 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.

Article 22 :

A l'issue de ses travaux, l'organisme certificateur établit un rapport faisant état des constats réalisés. Ce rapport dresse la liste de l'ensemble des non-conformités constatées, quel que soit leur niveau de gravité.

Le rapport conclut soit à la certification sans réserve, soit à la certification avec réserves. La certification est faite avec réserves lorsqu'une ou plusieurs exigences techniques présentant un niveau critique défini par le référentiel technique ne sont pas atteintes.

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 du 12 mai 2010 précitée afin que celui-ci procède à la transmission prévue à cet article. Ce document indique si la certification est obtenue avec ou sans réserve et fait état, le cas échéant, de la ou des réserves concernées.

Article 23 :

A l'issue de la remise du rapport de certification, l'opérateur établit, s'il y a lieu, des fiches d'anomalies qu'il adresse à l'Autorité nationale des jeux 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 leur niveau de gravité. 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 nationale des jeux 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. L'opérateur pourra, le cas échéant, faire procéder à un nouveau contrôle et en produire le résultat avec la transmission à l'Autorité nationale des jeux des fiches d'anomalies.

Article 24 :

Les organismes inscrits sur la liste des organismes certificateurs en raison de leurs compétences techniques avant la date de publication du présent décret demeurent inscrits sur cette liste jusqu'au terme fixé par les dispositions en vigueur à la date de leur inscription.

Les organismes inscrits sur la liste des organismes certificateurs en raison de leurs compétences techniques en leur qualité de sous-traitants avant la date de publication du présent décret demeurent inscrits sur cette liste jusqu'au terme fixé par les dispositions en vigueur à la date de leur inscription. Ils peuvent proposer des missions de certification à titre principal dans le cadre des dispositions du présent décret à compter de sa publication. »

Article L.231-1 du code des relations entre le public et l'administration :

« Le silence gardé pendant deux mois par l'administration sur une demande vaut décision d'acceptation. »

Article 1er du décret n° 2015-397 du 7 avril 2015 relatif au régime des décisions d'inscription sur la liste des organismes certificateurs et d'homologation de logiciel de jeux ou de paris prises par l'Autorité de régulation des jeux en ligne :

« En application du 4° de l'article L.231-4 du code des relations entre le public et l'administration, vaut décision de rejet :

1° Le silence gardé pendant deux mois par l'Autorité nationale des jeux sur une demande d'inscription sur la liste mentionnée au II de l'article 23 de la loi du 12 mai 2010 susvisée ;

2° Le silence gardé pendant deux mois par l'Autorité nationale des jeux sur une demande d'homologation de logiciel de jeux ou de paris formée par un opérateur de jeux ou de paris en ligne en application du deuxième alinéa du III[1] de l'article 34 de la loi du 12 mai 2010 susvisée. »

I.2 Présentation du document et des objectifs de la certification

Les dispositions de 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, modifiée par l'ordonnance n° 2019-1015 du 2 octobre 2019 réformant la régulation des jeux d'argent et de hasard, soumettent les opérateurs agréés de jeux ou de paris en ligne et les opérateurs titulaires de droits exclusifs à une procédure de certification.

Celle-ci doit être réalisée par un organisme indépendant choisi par l'opérateur au sein d'une liste établie et mise à jour par l'ANJ, l'établissement et la mise à jour de cette liste constituant un des leviers permettant à l'Autorité de s'assurer de la qualité des certifications conformément aux dispositions du VIII de l'article 34 de cette loi.

Cette certification a pour objectif de s'assurer du respect, par les opérateurs, de l'ensemble des exigences techniques applicables à son activité, et plus particulièrement celles déterminées par l'Autorité en matière d'intégrité et de fiabilité des opérations de jeux et de sécurité des systèmes d'information qui déclinent l'objectif de la politique de l'Etat en matière de jeux d'argent et de hasard énoncé au 2° de l'article L.320-3 du code de la sécurité intérieure.

Les actions menées par l'Autorité dans ce cadre font partie, plus largement, du dispositif de contrôle qu'elle a mis en place visant à satisfaire à l'ensemble des objectifs définis à l'article L.320-3 de ce code.

Dans ce cadre, le présent document a pour objet d'exposer :

- les conditions de référencement et de déréférencement des organismes certificateurs telles qu'elles résultent des dispositions du chapitre 1er du Titre III du décret n° 2020-1349 du 4 novembre 2020 relatif aux modalités de régulation de l'Autorité nationale des jeux ;
- les obligations applicables aux organismes certificateurs inscrits sur la liste de l'ANJ, telles qu'elles résultent des dispositions du chapitre 2 du Titre III du décret n° 2020-1349 du 4 novembre 2020 susmentionné ;
- les modalités de mise en œuvre des travaux de certification, telles qu'elles résultent notamment des dispositions du chapitre 3 du Titre III du décret n° 2020-1349 du 4 novembre 2020 susmentionné et qui visent notamment à rappeler :
  - le champ d'application de la certification, c'est-à-dire les cas dans lesquels la certification doit être conduite ;
  - le périmètre de la certification, c'est-à-dire l'ensemble des éléments qui doivent être couverts par les différents audits de la certification ;
  - les livrables attendus.

[1] Il s'agit en pratique du deuxième alinéa du VIII suite à une renumérotation des articles, imparfaitement référencée ici.

I.3 Glossaire

ANJ : Autorité Nationale des Jeux.

Authenticité : caractère d'une information (document, données) dont on peut prouver qu'elle est bien ce qu'elle prétend être, qu'elle a été effectivement produite ou reçue par la personne qui prétend l'avoir produit ou reçu, et qu'elle a été produite ou reçue au moment où qu'elle prétend l'avoir été.

Capteur : élément constitutif du système de collecte et d'archivage (i.e. SMA), dont la fonction est la création de traces. La fonction de création de traces correspond au formatage des données circulant entre le joueur et la plateforme de jeu puis au transfert de ces données vers le module coffre-fort du système de collecte et d'archivage.

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

Coffre-fort : élément constitutif du système de collecte et d'archivage (i.e. SMA), dont la fonction est de chiffrer, signer, horodater et archiver les données tracées et collectées depuis le flux en provenance du joueur ou fournies par la plateforme de jeu. Ceci afin de garantir la confidentialité, l'authenticité et l'exhaustivité dans le temps.

Confidentialité : propriété selon laquelle l'information n'est pas rendue disponible ni divulguée à des personnes, des entités ou des processus non autorisés.

Intégrité : caractère complet et non altéré d'une information prouvant que celle-ci n'a subie aucun ajout, aucun retrait ni aucune modification accidentelle ou intentionnelle, depuis sa validation.

Plateforme de jeu : système informatique de l'opérateur, dédié à une activité de jeu. Il s'agit principalement des ressources matérielles et logicielles qui assurent particulièrement la gestion complète des opérations de jeux.

Système d'information (SI) : ensemble structuré de ressources techniques (matériel informatique, équipements réseaux, logiciels, processus métier et procédures) et sociales (structure organisationnelle et personnes liées au SI) au sein d'une organisation, destinées à élaborer, collecter, traiter, classifier, stocker, diffuser des informations.

Support matériel d'archivage (SMA) : dispositif de recueil et d'archivage des données échangées entre le joueur et la plateforme de jeu de l'opérateur à l'occasion des opérations de jeux. Ce dispositif est développé et exploité sous la responsabilité de l'opérateur. Il est constitué des composants « capteur » et « coffre-fort ».

Traçabilité : propriété qui permet la non-répudiation et d'assurer l'imputabilité. Cela signifie que cette propriété garantit l'origine de la source, de la destination, la véracité d'une action et l'identification de l'entité responsable.

I.4 Identification des exigences et recommandations dans le document

Le présent document comporte deux niveaux de mesures :

- Les mesures précédées de **[E_numero]** sont des exigences qui revêtent un caractère **obligatoire**, sous réserve des exceptions mentionnées au sein des présentes exigences techniques ;
- Les mesures précédées de **[R_numero]** sont des recommandations, que les opérateurs peuvent décider de ne pas suivre sous réserve d'en justifier auprès de l'Autorité et d'indiquer à cette dernière les mesures alternatives qu'ils entendent mettre en place.

II Partie « Certificateurs »

II.1 Procédures de référencement d'un organisme certificateur

Les organismes certificateurs sont soumis aux procédures suivantes :

a) De référencement initial par laquelle l'Autorité habilite, après examen du dossier de demande, l'organisme certificateur à réaliser des certifications pour le compte des opérateurs de jeux ;
b) De renouvellement du référencement à l'issue d'un délai de 5 ans, qui conduit à une nouvelle habilitation de l'Autorité réalisée après examen d'un nouveau dossier constitué des mêmes pièces, actualisées, que celles demandées dans le dossier de référencement initial ;
c) De sortie du référencement : la demande de sortie – avant l'expiration du délai de 5 ans de validité du référencement – doit être notifiée par l'organisme certificateur à l'Autorité, par courrier recommandé, afin de permettre le maintien à jour de la liste des organismes certificateurs référencés pour les opérateurs. A l'inverse, l'Autorité peut procéder, par une décision motivée, au retrait de la liste d'un organisme certificateur.

Les procédures et livrables correspondants sous détaillées ci-après.

II.1.1 Procédures de référencement initial et renouvellement à 5 ans

Le référencement correspond à l'inscription sur la liste des organismes certificateurs.

[E_CRT_REF1] Conformément aux dispositions de l'article 12 du décret n° 2020-1349, seuls peuvent être inscrits sur la liste des organismes certificateurs, les organismes :

- établis dans un Etat membre de l'Union européenne ou un Etat partie à l'accord sur l'Espace économique européen ;
- disposant des compétences suffisantes et du personnel qualifié approprié ;
- exerçant leurs missions de certification en toute indépendance et en toute impartialité.

[E_CRT_REF2] Le dossier de demande de référencement initial est déposé auprès de l'ANJ selon les modalités prévues à l'article 13 du décret n° 2020-1349 du 4 novembre 2020. Ce dossier, transmis dans un format dématérialisé, comprend les pièces suivantes :

1. Le formulaire de demande de référencement ;
2. Un document retraçant les références de prestations réalisées par le demandeur dans des domaines d'expertise similaires à ceux exigés pour délivrer la certification (cf. l'exigence [E_CRT_LRA1], section II.2) ;
3. La liste des personnes dédiées aux opérations de certification ainsi que leurs *curriculums vitae* détaillés (cf. l'exigence [E_CRT_LRA2], section II.2) ;
4. Des rapports d'analyse type mettant en avant les méthodologies utilisées et l'étendue des analyses conduites en matière d'audits applicatifs intrusifs et d'audits de configuration de plate-forme d'hébergement.

[E_CRT_REF3] Le dossier de demande de renouvellement de référencement déposé par un organisme certificateur habilité auprès de l'ANJ, dans un format dématérialisé, comprend les mêmes pièces, mises à jour, que celles transmises lors du référencement initial (cf. l'exigence [E_CRT_REF2]).

[E_CRT_REF4] Lorsque le dossier de demande 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, la ou les pièces 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'ANJ, d'une décision d'irrecevabilité de la demande d'inscription.

[E_CRT_REF5] Au cours de l'instruction, le demandeur est tenu de fournir, à la demande de l'ANJ, toute information de nature à l'éclairer sur les éléments contenus dans le dossier déposé. Le demandeur peut être auditionné par l'ANJ.

[E_CRT_REF6] La décision de l'Autorité est notifiée à l'organisme demandeur, dans les deux mois à compter de la réception de sa demande. L'organisme certificateur reçoit alors un numéro de référencement et est inscrit dans la liste des organismes certificateurs référencés.

II.1.2 Procédure de sortie

[E_CRT_PRS1] Un organisme certificateur référencé peut demander son retrait de la liste des organismes référencés par l'ANJ, avant l'expiration du délai de 5 ans de validité du référencement, en notifiant sa demande directement auprès de l'Autorité, par courrier recommandé.

A l'issue d'un délai maximal de 2 mois à compter de la réception de sa demande, l'organisme est retiré de la liste des organismes certificateurs référencés.

[E_CRT_PRS2] Conformément aux dispositions de l'article 19 du décret n° 2020-1349 du 4 novembre 2020, si un organisme certificateur ne présentait plus les qualités requises pour être inscrit sur la liste des organismes certificateurs, l'ANJ peut procéder, par décision motivée, à son retrait de la liste des organismes certificateurs. Dans ce cas, avant de procéder à un éventuel retrait, l'Autorité notifie par courrier son intention à l'organisme certificateur concerné, lequel dispose de 15 jours calendaires pour formuler ses observations.

II.2 Spécificités sur les livrables attendus

[E_CRT_LRA1] Le document retraçant les références de prestations réalisées par le demandeur dans des domaines d'expertise similaires à ceux exigés pour délivrer la certification précisera, pour chaque référence :

1. le périmètre précis de la prestation;
2. sa durée ;
3. le client ;
4. la ou les périodes de réalisation des audits ;
5. les noms et prénoms des auditeurs ayant mené la mission.

[E_CRT_LRA2] La liste des personnes dédiées aux opérations de certification ainsi que leurs *curriculums vitae* détaillés inclura :

1. les noms et prénoms des personnes concernées ;
2. une présentation synthétique des missions de certifications réalisées par ces personnes ;
3. leur ancienneté chez l'organisme certificateur et les fonctions occupées.

II.3 Obligations des organismes certificateurs

Les travaux de certification sont du ressort des certificateurs, conformément à l'exigence [E_CRT_AUD1]. Lors de ces travaux, les certificateurs sont astreints à un certain nombre d'obligations décrites ci-après.

[E_CRT_OOC1] L'organisme inscrit sur la liste des organismes certificateurs accomplit la mission de certification qui lui est confiée conformément à l'état de l'art.

[E_CRT_OOC2] Conformément aux dispositions de l'article 17 du décret n° 2020-1349 du 4 novembre 2020, l'organisme certificateur est indépendant de l'opérateur pour lequel il effectue la mission de certification.

En particulier, il ne peut mener aucune mission de certification pour un opérateur de jeux s'il a été son conseil ou son prestataire, ou celui de l'éventuelle société contrôlant[2] l'opérateur de jeux, dans les douze mois précédant la signature du contrat de certification avec l'opérateur.

[E_CRT_OOC3] L'organisme inscrit sur la liste des organismes certificateurs informe sans délai l'ANJ de la survenance d'une situation de conflit d'intérêt au regard de son activité de certification.

[E_CRT_OOC4] Une copie du contrat de certification conclu entre l'organisme certificateur et l'opérateur faisant l'objet de la certification est communiquée par l'opérateur à l'ANJ à l'issue de l'exécution de la prestation de certification.

[E_CRT_OOC5] L'organisme inscrit sur la liste des organismes certificateurs informe sans délai l'ANJ des changements affectant la liste des personnes chargées des opérations de certification. Le *curriculum vitae* des nouvelles personnes intégrant cette liste devra être remis à l'ANJ à cette occasion.

[2] au sens du code du commerce

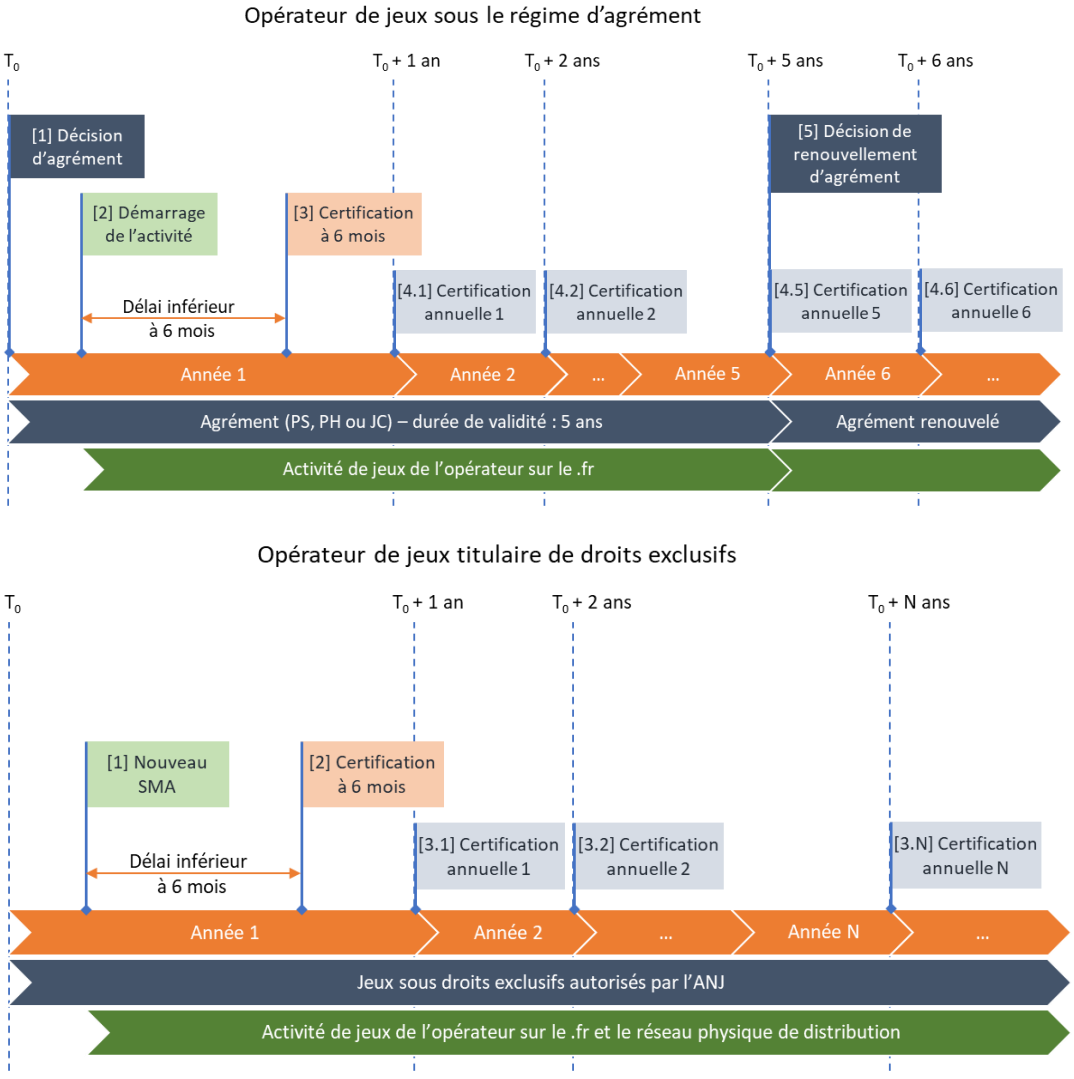
III Partie « Certification »

III.1 Champ d'application

[E_CRT_CHA1] La certification est une procédure qui s'applique d'une part, aux opérateurs agréés de jeux ou de paris détenteurs d'un ou plusieurs agréments délivrés par l'Autorité en application de l'article 21 de la loi n° 2010-476 du 12 mai 2010, désignés dans le présent document comme « opérateurs agréés » et, d'autre part aux opérateurs également titulaires de droits exclusifs.

Elle comporte deux sous-procédures :

a) Une certification à 6 mois, qui doit être conduite avant l'échéance des 6 mois suivant la mise en exploitation d'un nouveau SMA ;
b) Une certification annuelle, qui doit être réalisée annuellement (i) à la date anniversaire de l'obtention de l'agrément pour les opérateurs agréés ou (ii) à date fixée par l'ANJ conjointement avec l'opérateur, pour les opérateurs titulaires de droits exclusifs (cf. exigence [E_CRT_PER3]).



[E_CRT_CHA2] Si l'opérateur dispose de plusieurs agréments, une certification annuelle unique est réalisée.

[E_CRT_CHA3] Le rapport de l'organisme certificateur et sa conclusion relative à la certification à 6 mois ou annuelle obtenue – avec ou sans réserve – doivent être remis à l'ANJ selon les échéances prévues (cf. sections III.3.2 et III.3.3).

La certification ne donne pas lieu à la notification d'une décision de l'ANJ. Elle peut toutefois conduire, en cas de réserves significatives et selon la gravité de celles-ci, à l'ouverture d'une enquête par les services e l'ANJ sur le fondement de l'article 42 de la loi n° 2010-476 du 10 mai 2010 modifiée susceptible elle-même de déboucher sur la saisine de la commission des sanctions en application de l'article 43 de la même loi.

III.2 Périmètre de la certification

III.2.1 Certification à 6 mois

[E_CRT_PER1] 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 SMA et son infrastructure d'hébergement.

III.2.2 Certification annuelle

[E_CRT_PER2] Prévue au III de l'article 23 de la loi n°2010-476 du 12 mai 2010, la certification annuelle porte sur le système d'information dédié aux activités de jeux et de paris proposées par l'opérateur, en ce compris la plateforme de jeu de fournisseurs tiers le cas échéant, ainsi que sur les modifications apportées aux logiciels homologués depuis leur dernière homologation. Ce périmètre inclut également le SMA pour le volet sécurité et le cas échéant son volet techno-fonctionnel s'il a fait l'objet d'une évolution substantielle.

Qu'est-ce qu'une évolution substantielle du SMA ?

Une évolution est qualifiée de substantielle lorsque :

1. elle remet en question le fonctionnement du SMA ;
2. Elle remet en question l'analyse de la sécurité de ce dernier.

Le fonctionnement du SMA est susceptible d'être remis en question lorsque l'évolution porte sur un ou plusieurs des points suivants :

1. Une évolution modifiant la stratégie employée pour la création et la collecte des traces ;
2. Une évolution modifiant la stratégie employée pour l'archivage des traces ;
3. Une évolution modifiant la stratégie employée pour l'accès aux traces et leur extraction.

L'analyse de sécurité est susceptible d'être remise en question lorsque l'évolution porte sur un ou plusieurs des points suivants :

4. Une évolution modifiant tout ou partie des mécanismes ou configurations impactant directement la sécurité du SMA (exemples : authentification, contrôle d'accès, chiffrement des communications) ;
5. Une évolution modifiant l'architecture interne du SMA ;

6. Une évolution technique correspondant au remplacement d'une technologie par une autre au sein du SMA (exemples : framework, bibliothèque logicielle, langage de programmation), hors montée de version ;
7. Une modification d'infrastructure modifiant la surface d'exposition en termes de sécurité du SMA (exemples : changement du site d'hébergement, de l'hébergeur, du fournisseur de plateforme de jeu ou de la plateforme du fournisseur de coffre) ;
8. L'ajout ou la modification d'une ou plusieurs interconnexions directes au SMA avec d'autres systèmes d'information.

Ne sont pas considérés par l'ANJ comme des évolutions substantielles, sous réserve que les modifications apportées ne tombent pas sous l'un des deux cas ci-dessus (i.e. points n° 1 et 2) :

9. La montée de version du SMA ou de l'un de ses composants ;
10. La correction de bogues et de vulnérabilités éventuelles ;
11. Les modifications se rapportant à l'ergonomie ou au graphisme des interfaces utilisateurs du SMA.

L'Autorité nationale des jeux se réserve la possibilité de réviser la qualification de l'évolution retenue par l'opérateur sur la base des conclusions des travaux de certification précédentes et des contrôles opérés par l'ANJ.

[E_CRT_PER3] Pour les opérateurs titulaires de droits exclusifs, sur la partie du SI qui porte les jeux sous droits exclusifs et sur celle-ci uniquement, la certification pourra être pluriannuelle par secteurs, assurant une couverture globale sur un cycle de 2, 3, 4 ou 5 ans, à l'exception (i) du volet relatif à la sécurité du SMA, (ii) des tests d'intrusion externes[3] de la plateforme de jeu et (iii) du contrôle des plans de remédiation qui font l'objet d'un contrôle annuel.

Un secteur s'entend comme un périmètre technico-fonctionnel cohérent du système d'information de l'opérateur, sur la partie sous droits exclusifs, en ce compris les services de fournisseurs tiers le cas échéant.

La durée du cycle, le programme et calendrier de certification sur chacune des années du cycle, qui doit couvrir la totalité du périmètre soumis à certification sur l'ensemble du cycle, fait l'objet d'une proposition écrite à l'Autorité par l'opérateur titulaire de droits exclusifs, remise au plus tard 6 mois avant l'entrée dans un nouveau cycle. Le programme de certification de chacune des années du cycle pourra s'appuyer sur les secteurs définis dans une annexe dédiée.

L'Autorité validera, sous deux mois à compter du dépôt de la proposition, le programme proposé, et pourra le cas échéant demander des modifications. En cas de désaccord, la décision établissant le programme de certification revient à l'Autorité.

En l'absence de proposition formalisée écrite par l'opérateur sous droits exclusifs au plus tard 6 mois avant l'entrée dans un nouveau cycle, la certification sera réputée suivre un rythme annuel, avec un périmètre couvrant tous les secteurs soumis à certification.

Concernant les logiciels homologués, dans le cadre d'une certification pluriannuelle, le périmètre de la certification sera restreint aux logiciels homologués des secteurs visés par la certification de l'année N,

[3] Les tests d'intrusion internes seront réalisés par secteur, selon le programme de certification retenu.

sauf demande contraire de l'Autorité exprimée dans le courrier de notification les décisions d'homologation délivrées au plus tard un mois avant la remise du dossier de certification.

III.3 Procédures de certification

III.3.1 Dispositions communes aux travaux de certification

III.3.1.1 Réalisation des audits de certification

[E_CRT_AUD1] La certification – à 6 mois ou annuelle – est réalisée par un organisme indépendant choisi par l'opérateur au sein de la liste des organismes certificateurs établie par l'ANJ. Le coût de cette certification est à la charge de l'opérateur.

[E_CRT_AUD2] Les opérations d'audit conduites par l'organisme certificateur sont réalisées sur la base du référentiel technique établi par les exigences techniques déclinées dans le présent document et ses annexes (en particulier, la matrice d'exigences de la certification à 6 mois et la matrice d'exigences de la certification annuelle).

Les exigences de conformité et de sécurité font l'objet de différents points de contrôle qui sont présentés dans ledit référentiel technique.

[E_CRT_AUD3] Pour chaque point de contrôle du référentiel technique, l'organisme certificateur complète la matrice des exigences concernée (cf. annexe n°2), en renseignant la conformité de l'exigence évaluée et son niveau de criticité (cf. annexe n°3) résultant de son analyse. Cette évaluation doit prendre en compte les éléments communiqués par l'opérateur (exemples : ressources documentaires, codes sources), les tests et les audits techniques effectués par l'organisme certificateur, ainsi que des attestations d'absence de modification produites, le cas échéant, par l'opérateur.

[E_CRT_AUD4] Les opérations d'analyse conduites par l'organisme certificateur ne sont pas itératives au cours d'une même certification : chaque exigence contrôlée fait l'objet d'un contrôle unique.

Des échanges peuvent avoir lieu au moment du contrôle entre l'organisme certificateur et l'opérateur dont il assure la certification. Toutefois, une fois le contrôle effectué, ces échanges ne peuvent en aucun cas conduire l'organisme certificateur à effectuer une nouvelle analyse. En particulier, les modifications apportées le cas échéant 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.

[E_CRT_AUD5] A l'issue des travaux de certification, l'organisme certificateur établit :

1. Le rapport de certification faisant état des constats réalisés (cf. III.4.1 et III.4.2) ;
2. L'attestation de certification.

Le rapport dresse la liste de l'ensemble des non-conformités constatées, quel que soit leur niveau de gravité. Le rapport conclut soit à une certification sans réserve, soit à une certification avec réserves, lesquelles doivent être explicitées.

La certification est faite avec réserves lorsqu'une ou plusieurs exigences techniques dont le niveau de criticité est supérieur ou égal à 2 ne sont pas atteintes ou lorsque des vulnérabilités de niveau de gravité importante, majeur ou critique ont été identifiées.

L'attestation de certification ne reprend que la nature de la certification avec ou sans réserve et, le cas échéant, fait état de la ou les réserves émises.

[E_CRT_AUD6] Le rapport de certification et l'attestation sont signés électroniquement par l'organisme certificateur qui en est l'auteur, selon le standard défini dans l'annexe n°5 du présent document. Les fichiers de signature électronique obtenus accompagnent le rapport de certification et l'attestation respectivement.

Afin de pouvoir vérifier l'authenticité des documents signés, l'organisme certificateur communique à l'ANJ, à l'exécution de la prestation de certification, sa clef publique *via* le moyen d'échange mis çà disposition par l'ANJ.

[E_CRT_AUD7] A l'issue des travaux de la certification, l'organisme certificateur transmet à l'opérateur concerné le rapport et l'attestation de certification signés électroniquement afin que l'opérateur procède à leur transmission à l'ANJ prévue pour la certification à 6 mois (cf. III.3.2) et la certification annuelle (cf. III.3.3).

III.3.1.2 Non-conformité et vulnérabilités

[E_CRT_CAN1] Les éventuelles non-conformités identifiées lors des travaux de certification, doivent faire l'objet d'un plan de remédiation. Leur correction doit intervenir dans un délai qui ne peut excéder douze mois à compter de la date de remise à l'ANJ du plan de remédiation ou, si celui-ci n'était pas remis par l'opérateur dans les délais prévus par les exigences **[E_CRT_ASM2]** et **[E_CRT_ANN2]**, à compter de la date butée de sa remise fixée par ces mêmes exigences. Les corrections apportées devront être validées par l'organisme certificateur dans le cadre de la certification annuelle suivante.

[E_CRT_CAN2] Les éventuelles vulnérabilités identifiées lors des travaux de certification, en particulier lors des tests d'intrusion, doivent faire l'objet d'un plan de remédiation. Leur correction doit intervenir dans un délai qui ne peut excéder trois mois pour les vulnérabilités majeures ou critiques[4], six mois pour les vulnérabilités importantes et douze mois pour les vulnérabilités mineures, à compter de la date de remise du plan de remédiation ou, si celui-ci n'était pas remis par l'opérateur dans les délais prévus par les exigences **[E_CRT_ASM2]** et **[E_CRT_ANN2]**, à compter de la date butée de sa remise fixée par ces mêmes exigences. Les corrections apportées devront être validées par l'organisme certificateur dans le cadre de la certification annuelle suivante.

[E_CRT_CAN3] Si aucune mesure de sécurité ne permet de corriger directement les vulnérabilités, l'opérateur devra proposer des mesures compensatoires afin d'éviter leur exploitation et les expliciter dans le plan de remédiation. Les mesures compensatoires ou de protection périmétrique devront être validées par l'organisme certificateur dans le cadre de la certification annuelle suivante.

[E_CRT_CAN4] L'opérateur justifie dans le plan de remédiation tout refus de correction des vulnérabilités et non-conformités identifiées au cours des travaux de certification et, le cas échéant, présente les mesures alternatives qu'il propose. L'appréciation du bien-fondé des justifications et, le cas échéant, des mesures alternatives présentées par l'opérateur revient à l'ANJ.

[4] Se référer à l'échelle de gravité des vulnérabilités définie dans l'annexe n°4 du présent document.

[R_CRT_CAN1] Afin de lever une réserve (notamment les vulnérabilités majeures ou critiques et les non-conformités de niveau 3), l'opérateur pourra, le cas échéant, faire procéder à un nouveau contrôle et en produire le résultat avec la transmission à l'ANJ des fiches d'anomalies.

III.3.1.3 Plan de remédiation

[E_CRT_PRM1] L'opérateur établit un plan de remédiation, qui contient, pour chaque vulnérabilité ou non-conformité recensée dans le rapport de certification, une fiche comportant au minimum trois volets :

1. La description synthétique de la vulnérabilité ou de la non-conformité. S'il s'agit d'une vulnérabilité, le niveau de risque associé (cf. annexe n°4) doit également apparaître sur la fiche ;
2. Les recommandations de l'organisme certificateur pour corriger la vulnérabilité ou la non-conformité ;
3. Le plan d'actions justifiant la prise en charge par l'opérateur de la vulnérabilité ou de la non-conformité. Ce plan détaille les actions prises ou envisagées par l'opérateur pour corriger la vulnérabilité ou la non-conformité (y compris les mesures compensatoires) et précise le calendrier de mise en œuvre de ces actions.

[E_CRT_PRM2] Pour les vulnérabilités critiques, majeures ou importantes ainsi que les non-conformités dont le niveau de criticité est supérieur ou égal à 2, l'opérateur est tenu de rendre compte à l'ANJ de la réalisation du plan de remédiation aux dates indiquées. Un regroupement trimestriel des rendus compte est possible.

III.3.2 Délai de dépôt des pièces relatives à la certification à 6 mois

[E_CRT_ASM1] Dans un délai de six mois à compter de la date de mise en fonctionnement du SMA, l'opérateur agréé ou titulaire de droits exclusifs transmet à l'ANJ :

1. Le rapport de certification signé électroniquement ;
2. L'attestation de certification signée électroniquement.

[E_CRT_ASM2] Le plan de remédiation est adressé par l'opérateur à l'ANJ et l'organisme certificateur dans un délai d'un mois suivant la remise du rapport de certification.

III.3.3 Délai de dépôt des pièces relatives à la certification annuelle

[E_CRT_ANN1] Dans un délai d'un an à compter de la date d'obtention de l'agrément, ou la date en tenant lieu pour les opérateurs sous droits exclusifs, l'opérateur de jeux ou de paris transmet à l'ANJ :

1. Le rapport de certification signé électroniquement ;
2. L'attestation de certification signée électroniquement.

[E_CRT_ANN2] Le plan de remédiation est adressé par l'opérateur à l'ANJ et à l'organisme certificateur dans le délai d'un mois suivant la remise du rapport de certification. Si l'opérateur change de certificateur l'année suivante, il devra également transmettre le plan de remédiation au nouveau certificateur en amont des travaux de ce dernier.

[E_CRT_ANN3] La certification fait l'objet d'une actualisation annuelle, au plus tard à la date d'anniversaire de la précédente certification.

III.4 Livrables

III.4.1 Livrables pour la certification à 6 mois

Les contrôles effectués lors de la certification à 6 mois, portant sur le SMA, reposent sur un socle d'analyses obligatoires, décrites ci-après.

III.4.1.1 Livrables attendus

[E_CRT_LCA1] Les livrables relatives à la certification à 6 mois sont à remettre à l'ANJ dans un format dématérialisé.

[E_CRT_LCA2] Les livrables de la certification à 6 mois sont les suivants :

1. Le rapport de certification produit par l'organisme certificateur, signé électroniquement conformément à l'exigence [E_CRT_AUD6] (cf. section III.3.1.1) ;
2. L'attestation de certification produit par l'organisme certificateur, signé électroniquement conformément à l'exigence [E_CRT_AUD6] (cf. section III.3.1.1) ;
3. Le plan de remédiation des non-conformités et des vulnérabilités identifiées au cours des audits de la certification, produit par l'opérateur de jeux ou de paris.

III.4.1.2 Contenu du rapport de certification

[E_CRT_LCA3] Le rapport de la certification à 6 mois se compose, pour chaque agrément ou périmètre d'activité, des 6 pièces suivantes :

1. La synthèse des rapports susmentionnés aux points 3, 4 et 5, avec mention des éventuelles réserves ;
2. La matrice des exigences dûment renseignée ;
3. Le rapport d'audit fonctionnel, technique et de sécurité du capteur ;
4. Le rapport d'audit de configuration du SMA (i.e. capteur et coffre) et de son infrastructure d'hébergement ;
5. Le rapport de vérification du respect des exigences ;
6. Les annexes techniques.

[E_CRT_LCA4] La synthèse des rapports suivra le plan détaillé ci-après. Elle pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. La présentation du candidat opérateur ;
2. Un rappel du nom et des coordonnées de l'organisme certificateur chargé de réaliser la certification ;
3. Les dates des différentes prestations d'audit ;
4. Le charge (en jour homme) consacrés à chaque point de contrôle ;
5. La date de mise en œuvre opérationnelle du SMA ;
6. La synthèse stratégique des résultats obtenus par point de contrôle ;
7. La liste de l'ensemble des vulnérabilités et non-conformités constatées.
8. La liste exhaustive et détaillée des réserves.

[E_CRT_LCA5] Le rapport d'audit fonctionnel, technique et de sécurité du capteur suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. Synthèse de l'audit :
    a. Synthèse de l'audit fonctionnel et technique ;
    b. Synthèse de l'audit intrusif (audit de code et tests d'intrusion) ;
    c. Synthèse des non-conformités, classées par criticité et impact ;
    d. Synthèse des vulnérabilités, classées par criticité et impact ;
    e. Synthèse des recommandations, classées par criticité et coût de mise en œuvre ;
2. Audit fonctionnel et technique du capteur :
    a. Présentation de la solution et conformité de mise en œuvre :
        i. Mécanismes de création et d'enregistrement des traces ;
        ii. Mécanismes de vérification et de filtrage des données ;
        iii. Mécanismes de sécurité du capteur ;
    b. Audit du code source portant sur les fonctionnalités du capteur ;
3. Audit intrusif du capteur :
    a. Déroulement linéaire de l'audit intrusif du capteur, avec description explicite de la méthodologie employée pour détecter les vulnérabilités et les exploiter, le cas échéant ;
    b. Audit du code source portant sur la sécurité du capteur.

Dans le cadre de l'audit fonctionnel et technique du capteur, l'organisme certificateur n'effectue pas l'analyse syntaxique et sémantique des traces enregistrées au format XML mais s'assure que la mise en œuvre du capteur est conforme aux exigences techniques relatives aux données mises à disposition de l'ANJ (ET3) et que l'ensemble des enregistrements produits par le capteur sont correctement formés au sens de la norme XML et des schémas XSD publiés par l'ANJ.

Dans le cadre de l'audit intrusif du capteur, il est en particulier attendu de l'organisme certificateur que celui-ci tente, au travers des tests d'intrusion, *via* par exemple l'injection dans le coffre-fort de traces spécialement forgées afin d'en détourner les fonctions d'enregistrement et de sécurité (exemples : corruption des enregistrements, injection de faux évènements), (i) de prendre le contrôle à distance du capteur et du coffre-fort et (ii) de manipuler les enregistrements relatifs aux paris ou à la gestion de compte.

[E_CRT_LCA6] Le rapport d'audit de configuration du SMA et de son infrastructure d'hébergement suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. Synthèse de l'audit :
    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. Audit de configuration :
    a. Analyse de la stratégie de sécurité (politique de sécurité technique, procédures, etc.) ;
    b. Analyse de l'architecture technique (matrices de flux, règles de pare-feu, etc.) ;
    c. Analyse des configurations, aux niveaux système, réseau et applicatif.

[E_CRT_LCA7] Le rapport de vérification du respect des exigences réunit les différentes analyses (et leur résultats) qui n'ont pas été abordées dans les précédents livrables.

III.4.1.3 Contenu des annexes techniques

[E_CRT_LCA8] Les annexes techniques sont constituées de la documentation opérateur relative au SMA (capteur et coffre-fort), détaillant notamment la solution mise en œuvre.

III.4.2 Livrables pour la certification annuelle

III.4.2.1 Caractère actualisable des livrables de la certification annuelle

La certification annuelle repose sur un socle d'analyses susceptibles de faire, ou non, l'objet d'une actualisation, partielle ou totale, *via* des audits différentiels. On parle, le cas échéant, d'une analyse actualisable.

Par actualisation, il est entendu 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 et des commentaires assortis.

Une attestation d'absence de modification produite par l'opérateur peut par ailleurs conduire l'organisme certificateur à ne pas effectuer d'analyse sur le périmètre concerné, sous réserve que cette absence de modification soit compatible avec le maintien en condition de sécurité du système d'information visé par la certification.

[E_CRT_LCB1] Toutes les analyses ne sont pas actualisables et, à plus forte raison, ne peuvent pas être remplacées par une attestation d'absence de modification par l'opérateur. En particulier :

1. 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 ;
2. Les tests d'intrusion, internes[5] et externes, doivent être totalement réalisés chaque année.

Les analyses actualisables sont identifiées en couleur verte dans la présente section. L'exigence **[E_CRT_LCB13]** précise les conditions requises pour effectuer des audits différentiels.

III.4.2.2 Livrables attendus

[E_CRT_LCB2] Les livrables de la certification annuelle sont les suivants :

1. Le rapport de certification produit par l'organisme certificateur signé électroniquement conformément à l'exigence **[E_CRT_AUD6]** (cf. section III.3.1.1) ;
2. L'attestation de certification produit par l'organisme certificateur signé électroniquement conformément à l'exigence **[E_CRT_AUD6]** (cf. section III.3.1.1) ;
3. Le plan de remédiation des non-conformités et des vulnérabilités identifiées au cours des audits de la certification produit par l'opérateur de jeux ou de paris.

[5] Exception faite en application de l'exigence [E_CRT_PER3] où seuls les tests d'intrusion externes doivent être réalisés chaque année sur la totalité du périmètre soumis à la certification.

[E_CRT_LCB3] Les livrables relatives à la certification annuelle sont à remettre à l'ANJ dans un format dématérialisé.

III.4.2.3 Contenu du rapport de certification

[E_CRT_LCB4] Le rapport de la certification annuelle se compose, pour chaque agrément ou périmètre d'activité, des pièces suivantes :

1. La synthèse des rapports susmentionnés aux points 3 à 8 avec mention des éventuelles réserves ;
2. La matrice des exigences dûment renseignée ;
3. Le rapport des tests d'intrusion internes et externes de la plateforme de jeu, dont le composant capteur du SMA ;
4. Le rapport d'audit fonctionnel et technique du capteur ;
5. Le rapport d'audit de l'architecture technique de la plateforme de jeu ;
6. Le rapport d'audit de configuration des équipements de la plateforme de jeu ;
7. Le rapport d'audit des évolutions des logiciels de jeu ;
8. Le rapport de vérification du respect des exigences ;
9. Les annexes techniques.

[E_CRT_LCB5] La synthèse des rapports suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. La présentation du candidat opérateur ;
2. Un rappel du nom et des coordonnées de l'organisme certificateur chargé de réaliser la certification ;
3. Les dates des différentes prestations d'audit ;
4. Le charge (en jour homme) consacrés à chaque point de contrôle ;
5. La date de mise en œuvre opérationnelle des évolutions du SMA le cas échéant ;
6. La synthèse stratégique des résultats obtenus par point de contrôle ;
7. La liste de l'ensemble des vulnérabilités et non-conformités constatées.
8. La liste exhaustive et détaillée des réserves ;

[E_CRT_LCB6] Le rapport des tests d'intrusion internes et externes de la plateforme de jeu, dont le composant capteur du SMA, suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. Synthèse de l'audit :
    a. Synthèse des tests d'intrusion ;
    b. Synthèse des vulnérabilités, classées par criticité et impact ;
    c. Synthèse des recommandations, classées par criticité et coût de mise en œuvre ;
2. Tests d'intrusion :
    a. Analyse des risques synthétique ;
    b. Déroulement linéaire des tests d'intrusion internes et externes de la plateforme de jeu dont le capteur, avec description explicite de la méthodologie employée pour détecter les vulnérabilités et les exploiter, le cas échéant.

[E_CRT_LCB7] Le rapport d'audit fonctionnel et technique du capteur suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. Synthèse de l'audit :
    a. Synthèse de l'audit fonctionnel et technique ;
    b. Synthèse des non-conformités, classées par criticité et impact ;
    c. Synthèse des recommandations, classées par priorité et coût de mise en œuvre ;
2. Audit fonctionnel et technique du capteur :
    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. Audit du code source portant sur les fonctions les plus importantes du capteur.

[E_CRT_LCB8] Le rapport d'audit d'architecture technique de la plateforme de jeu suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. Synthèse de l'audit :
    a. Synthèse technique de l'audit d'architecture ;
    b. Synthèse des vulnérabilités, classées par criticité et impact ;
    c. Synthèse des recommandations, classées par criticité et coût de mise en œuvre ;
2. Audit d'architecture :
    a. Présentation de l'architecture technique ;
    b. Analyse de l'architecture technique (schéma réseau (niveau 3), matrices de flux, règles de filtrage, etc.) ;
    c. Analyse du cloisonnement ;
    d. Mécanismes d'administration.

[E_CRT_LCB9] Le rapport d'audit de configuration des équipements de la plateforme de jeu suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. Synthèse de l'audit :
    a. Synthèse technique de l'audit des équipements ;
    b. Synthèse des vulnérabilités, classées par criticité et impact ;
    c. Synthèse des recommandations, classées par priorité et complexité de mise en œuvre ;
2. Audit de configuration : analyse des configurations aux niveaux système, réseau et applicatif.

Dans le cadre de l'audit de configuration, l'organisme certificateur peut échantillonner les composants à auditer par rôle et/ou par criticité. Lors des 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 les composants qui n'auraient pas fait l'objet d'une analyse approfondie à l'occasion d'une précédente certification. Les contrôles relatifs à la sécurité des systèmes doivent cependant systématiquement être effectués (i.e. état des mises à jour, gestion des comptes des utilisateurs, gestion des droits, complexité des mots de passe, synchronisation horaire, etc.).

[E_CRT_LCB10] Le rapport d'audit des évolutions des différents logiciels de jeu suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'organisme certificateur le juge nécessaire :

1. Synthèse de l'audit ;
2. Audit des évolutions des logiciels de jeu :
    a. Liste des différents logiciels de jeu utilisés (clients et serveur) ;
    b. Analyse des changements apportés.
    c. Le contrôle de la mise en œuvre effective des plans de remédiation des jeux homologués conformément aux calendriers de ces plans. Le certificateur se réfèrera aux exigences techniques relatives aux homologations, sections IV.1.2 et IV.1.3, quant aux délais de correction maximaux convenus.

[E_CRT_LCB11] Le rapport de vérification du respect des exigences réunit les différentes analyses (et leur résultats) qui n'ont pas été abordées dans les précédents livrables.

III.4.2.4 Contenu des annexes techniques

[E_CRT_LCB12] Les annexes techniques sont constituées des pièces suivantes :

1. La documentation opérateur ;
2. Les attestations de l'opérateur d'absence de modification des éléments visés par les audits techniques et fonctionnels exigés ci-dessus, le cas échéant.

III.4.2.5 Dispositions particulières

[E_CRT_LCB13] Dans le cadre de la certification annuelle, les audits techniques et fonctionnels pourront être conduits de façon différentielle et ne porter que sur les composants ayant fait l'objet d'une évolution depuis la précédente certification, sans revenir aux composants inchangés. Le cas échéant, les composants inchangés devront faire l'objet d'une attestation spécifique d'absence de modification visée par le point 2 de l'exigence [E_CRT_LCB12]. La matrice d'exigences concernée pourra alors reprendre à l'identique les résultats obtenus lors de la précédente certification.

Cette possibilité d'audit différentiel des audits fonctionnels et techniques, visant à la simplification et l'allègement de la certification, ne s'applique pas aux audits de sécurité qui doivent obligatoirement être réalisés chaque année.

[E_CRT_LCB14] La possibilité est offerte à l'opérateur, aux fins d'allègement de la certification annuelle, d'utiliser les rapports d'audits réalisés dans le cadre de certifications ISO, de la World Lottery Association (WLA) ou équivalents, à condition de respecter les contraintes suivantes :

1. Les audits ISO, WLA, ou équivalents ne datent pas de plus de 9 mois à la date de remise du rapport de certification à l'ANJ ;
2. Les rapports des certifications ISO, WLA, ou équivalents ne se substituent pas au rapport de certification annuelle. Les livrables demandés par l'Autorité (i.e. rapports d'audit, matrice d'exigence renseigné, attestation de certification) sont toujours produits par l'organisme certificateur mais leurs sections relatives aux audits pourront afficher un renvoi précis à une ou plusieurs sections et pages du ou des rapports d'audits ISO, WLA ou équivalents couvrant le point de contrôle ou l'exigence idoine ;

3. L’organisme certificateur s’assure de la couverture des exigences de la certification annuelle.

Pour les opérateurs titulaires de droits exclusifs, l’utilisation de cette faculté d’utiliser ces rapports devra être déclinée dans le cadre de l’exigence **[E_CRT_PER3]** et figurera explicitement dans le programme pluriannuel présenté à l’Autorité.

IV Annexes

IV.1 Annexe n°1 – Types de prestations d'audit attendues

IV.1.1 Test d'intrusion

Une prestation de test d'intrusion a pour objectif de rechercher et d'exploiter les vulnérabilités découvertes sur un système. Il ne s'agit pas uniquement d'un test de vulnérabilités automatisé. Des tests manuels détaillés doivent également apparaître dans le rapport.

L'analyse doit faire apparaître les différentes étapes classiques du test d'intrusion (prise d'empreinte, recherche de vulnérabilité, tests manuels…). Celui-ci doit également comporter des détails techniques précis (outils utilisés, condition des tests, résultats obtenus) afin que les tests soient reproductibles et vérifiables sans ambiguïté.

IV.1.2 Test dynamique

Une prestation de test dynamique a pour objectif de vérifier la présence de vulnérabilités et/ou d'anomalies fonctionnelles au niveau du logiciel en réalisant une analyse du comportement du logiciel à partir d'hypothèses exprimées en fonction des données d'entrée, de l'état du logiciel et des résultats ou observations attendus.

Le test dynamique consiste à exécuter tout ou partie du logiciel, dans des conditions contrôlées et reproductibles aux fins d'observation du comportement de ce dernier et de mise en évidence de défaut de fonctionnement.

Le test dynamique s'apparente à un test fonctionnel.

IV.1.3 Audit de code source

Une prestation d'audit de code source a pour objectif de vérifier la présence de vulnérabilités et/ou d'anomalies fonctionnelles au niveau du logiciel en réalisant une analyse du code source du logiciel. L'auditeur devra se concentrer sur les problématiques liées à la sécurité et la sûreté de fonctionnement du logiciel vis-à-vis des attaques potentielles.

L'analyse est réalisée en considération des deux axes de recherche suivants :

- Sur le plan technique, l'analyse consiste à valider le respect des bonnes pratiques de développement. L'auditeur devra alors adapter ses analyses aux particularités du langage (fonctions sensibles, gestion de la mémoire, appel de composants externes…) ;
- Sur le plan fonctionnel, l'analyse consiste à valider la bonne implémentation des fonctions de sécurité et des fonctions métiers, et à rechercher la présence de moyens de contournement illicites de ces fonctions.

L'audit de code source est une prestation qui pourra éventuellement être assistée par des outils automatisés. Néanmoins une analyse manuelle reste nécessaire.

L'audit de code source devra porter *a minima* sur :

1. Le mécanisme de communication client/serveur ;
2. Le mécanisme d'authentification et de suivi de session ;
3. Le mécanisme d'autorisation et/ou de contrôle d'accès ;
4. Les vulnérabilités d'interception ;
5. Les vulnérabilités d'injection ;
6. Le traitement des entrées/sorties ;
7. La protection des données sensibles.

L'analyse doit clairement faire apparaître des extraits pertinents de code source dans le corps du rapport d'audit.

Afin de pouvoir garantir l'absence de modification des logiciels audités, une empreinte cryptographique des différents fichiers devra être fournie dans le rapport. En présence de code source imposant, des mécanismes d'empreinte « de répertoires » pourront être fournis. Le mécanisme d'empreinte devra être clairement détaillé et reproductible.

IV.1.4 Audit intrusif

L'audit intrusif du logiciel combine un audit de code source à un test d'intrusion.

Cette analyse s'apparente à un test d'intrusion en boîte blanche, il a pour objectif d'apporter les avantages de l'audit de code source couplé à un test d'intrusion. Les résultats de l'audit de code source et du test d'intrusion doivent être croisés afin de s'alimenter mutuellement.

L'analyse du code source doit clairement faire apparaître des extraits pertinents de code source dans le corps du rapport d'audit.

IV.1.5 Audit intrusif différentiel

L'audit intrusif différentiel associe l'audit du code source modifié du logiciel à un test d'intrusion.

L'auditeur concentre son analyse sur les changements apportés dans le logiciel depuis sa dernière homologation, afin de s'assurer qu'aucun problème de sécurité n'a été introduit. La méthodologie doit s'appuyer sur celle décrite dans les audits intrusifs.

IV.1.6 Audit d'architecture technique

Une prestation d'audit d'architecture technique a pour objectif de présenter la plateforme de jeu dans son ensemble, de décrire la ou les infrastructures de l'opérateur.

Cette analyse doit clairement faire apparaître des schémas réseau de niveau 3 complétés des observations de l'auditeur dans le rapport. Les schémas doivent présenter le cloisonnement, le nom des serveurs, leurs rôles et, si nécessaire, leurs adresses IP. Une attention particulière doit être apportée aux interactions des systèmes de l'opérateur avec les réseaux ou systèmes externes, mais également sur les mécanismes d'administration.

Le rapport doit mettre en évidence les éléments ayant fait l'objet d'un audit.

L'analyse de l'environnement physique doit s'effectuer d'après les observations effectuées sur site.

IV.1.7 Audit de configuration

Une prestation d'audit de configuration a pour objectif de vérifier la conformité des éléments d'une infrastructure par rapport aux bonnes pratiques en matière de sécurité du système d'information et aux exigences techniques définies au sein d'un référentiel telles que les matrices d'exigences de certification.

L'audit de configuration se veut être non invasive. Elle doit s'appuyer sur des extractions observées par l'auditeur et effectuées sur site.

Cette analyse doit être réalisée sur tous les équipements pouvant influer sur la sécurité de la plateforme de jeu, et en particulier sur les éléments suivants :

1. Equipements filtrants ;
2. Equipements de commutation ou de routage ;
3. Base de données ;
4. Services réseaux classiques (SSH, HTTP, DNS, etc.) ;
5. Serveurs de relais ;
6. Serveurs d'applications (Apache, Tomcat, etc.).

Toutefois, si le périmètre le nécessite, un échantillonnage des équipements pourra être effectué. Celui-ci pourra être effectué en se basant sur le niveau de criticité et le niveau d'exposition des éléments de l'infrastructure auditée.

Cette analyse doit prendre en compte le rôle des équipements, leur environnement, ainsi que le fonctionnement des applications présentes afin de s'assurer de la cohérence des configurations appliquées.

Cette analyse doit clairement faire apparaître des extraits pertinents de configuration dans le corps du rapport d'audit.

IV.1.8 Analyse des risques synthétique

Une analyse de risques synthétique a pour but de présenter une vision globale des risques pesant sur la plateforme de jeu. L'objectif de cette partie est de présenter la vision globale « expert technique » de l'auditeur sur les vulnérabilités résiduelles de l'infrastructure.

Cette analyse ne doit en aucun cas se baser sur un formalisme ou référentiel tel qu'EBIOS ou MEHARI. Elle se veut synthétique.

IV.1.9 Vérification du respect des exigences

La vérification des exigences est un livrable permettant de couvrir l'ensemble des exigences définies dans le référentiel d'exigence technique relatif à la certification. Cette partie regroupe l'analyse des exigences qui ne sont pas abordés au sein des autres livrables de la certification.

Pour chaque exigence, l'auditeur devra justifier la raison de la conclusion en se basant, lorsque c'est possible, sur les analyses effectuées dans les rapports précédents.

IV.2 Annexe n°2 – Matrices d'exigences techniques de la certification

La certification à 6 mois du SMA et la certification annuelle font l'objet de matrices d'exigences techniques distinctes : (i) la matrice d'exigences de la certification à 6 mois et (ii) la matrice d'exigences de la certification annuelle.

Chaque matrice regroupe des exigences de conformité et de sécurité, numérotées et classées par thème. Les matrices d'exigences doivent être complétées par l'organisme certificateur à l'issue de ses analyses lors des travaux de certification. Elles synthétisent les résultats obtenus à travers :

- Les différentes opérations d'analyse technique conduites par l'organisme certificateur (audits applicatifs, d'architecture, de configuration ou encore tests d'intrusion) ;
- L'analyse de la documentation remise par l'opérateur ;
- L'intégration des attestations d'absence de modification produites, le cas échéant, par l'opérateur. Remarque : cette absence de modification ne doit pas être incompatible avec un maintien en condition de sécurité (ex : gestion des mises à jour de sécurité, adaptation aux nouvelles attaques par des mesures de durcissement conformes à l'état de l'art, etc.).

Les matrices sont disponibles dans le document intitulé « Matrices d'exigences techniques de la certification » accompagnant le présent document.

IV.3 Annexe n°3 – Échelle de classification des exigences

Un niveau de criticité, sur une échelle de 1 à 3 (criticité la plus élevée), est affectée à chaque exigence des matrices d'exigences de la certification :

Niveau de criticité	Description
Niveau 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).
Niveau 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'ANJ ou encore défaut de suivi des règles de bonnes pratiques en sécurité des systèmes d'information.
Niveau 1	➢ Correspond essentiellement aux exigences liées à l'existence d'une documentation ou d'une procédure (exemple : politique de sécurité, procédure de mise à jour, de durcissement d'un système, etc.)

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. 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.

IV.4 Annexe n°4 – Échelle de classification des vulnérabilités

Les vulnérabilités sont classées en fonction du risque qu'elles font peser sur le système d'information. Ce risque est évalué en fonction de l'impact de la vulnérabilité sur le système d'information et de sa difficulté d'exploitation.

Sont présentées ci-après les différentes échelles que l'ANJ propose d'utiliser dans le cadre des audits de sécurité du logiciel de jeu afin de classifier les éventuelles vulnérabilités identifiées.

IV.4.1 Échelle d'impact de l'exploitation de la vulnérabilité

L'impact correspond aux conséquences que l'exploitation de la vulnérabilité peut entrainer sur le système d'information audité. Il est apprécié selon l'échelle suivante :

Niveau d'impact	Description
Critique	➢ Conséquences généralisées sur l'ensemble du système d'information. ➢ Atteinte en intégrité et en confidentialité à des données sensibles. ➢ L'exploitation de la vulnérabilité peut menacer la pérennité du système et plus généralement les intérêts vitaux de l'organisation.
Majeur	➢ Conséquences restreintes sur une partie du système d'information. ➢ Atteinte en confidentialité à des informations sensibles. ➢ L'exploitation de la vulnérabilité permet à un attaquant de compromettre la sécurité de la cible et de son environnement, et constituera de fait une nuisance conséquente et étendue pour l'organisation.
Important	➢ Conséquences isolées sur des points précis du système d'information. ➢ Atteinte en confidentialité à des informations techniques sur la cible. ➢ L'exploitation de la vulnérabilité permet à un attaquant de compromettre partiellement la sécurité de la cible et constituera une nuisance conséquente pour l'organisation.
Mineur	➢ Pas ou peu de conséquence directe sur la sécurité du système d'information en cas d'exploitation de la vulnérabilité. ➢ Atteinte en confidentialité à des informations non sensibles.

IV.4.2 Échelle de facilité d'exploitation de la vulnérabilité

La facilité d'exploitation d'une vulnérabilité correspond au niveau d'expertise et aux moyens nécessaires à la réalisation d'une attaque. Elle est appréciée selon l'échelle suivante :

Facilité d'exploitation	Description
Facile	L'exploitation de la vulnérabilité est triviale : elle ne nécessite ni compétence technique spécifique, ni outil particulier.
Modérée	L'exploitation de la vulnérabilité nécessite la mise en œuvre de techniques simples et/ou d'outils disponibles publiquement.
Élevée	L'exploitation de la vulnérabilité nécessite des compétences en sécurité des systèmes d'information et le développement d'outils simples.
Difficile	L'exploitation de la vulnérabilité nécessite une expertise en sécurité des systèmes d'information et un coût de mise en œuvre élevée notamment en raison du développement d'outils spécifiques et ciblés.

IV.4.3 Matrice de gravité de la vulnérabilité

Le niveau du risque lié à chaque vulnérabilité est apprécié selon l'échelle de valeur suivante :

Niveau de gravité	Description
Critique	Risque critique sur le système d'information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.
Majeur	Risque majeur sur le système d'information et nécessitant une correction à court terme.
Important	Risque modéré sur le système d'information et nécessitant une correction à moyen terme.
Mineur	Faible risque sur le système d'information pouvant nécessiter une correction.

La détermination du niveau de gravité (ou criticité) des vulnérabilités identifiées se dérive selon l'impact et la facilité d'exploitation de la vulnérabilité considérée et s'appuie sur la matrice suivante :

Facilité d'exploitation / Impact	Difficile	Élevée	Modérée	Facile
Critique	Important	Majeur	Critique	Critique
Majeur	Important	Majeur	Majeur	Critique
Important	Mineur	Important	Important	Majeur
Mineur	Mineur	Mineur	Important	Majeur

IV.5 Annexe n°5 – Sécurité et recommandations d'usage

Conformément aux règles et recommandations définies dans le Référentiel Général de Sécurité (RGS) établi par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), l'ANJ recommande l'emploi des standards et outils selon les usages suivants :

Cas d'usage	Standards / fonctions / algorithmes préconisés	Outils recommandés
Chiffrement d'un fichier	Standard OpenPGP (RFC 4880) – chiffrement asymétrique – système RSA (taille des clefs d'au moins 2048 bits)	GNU Privacy Guard (GnuPG)
Signature électronique d'un fichier	Standard OpenPGP (RFC 4880) – signature asymétrique – système RSA (taille des clefs d'au moins 2048 bits)	GNU Privacy Guard (GnuPG)
Calcul de l'empreinte cryptographique d'un fichier	SHA-256	sha256sum

Matrice des exigences de la certification

(version 1.0 du 07/10/2022)

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 (Exigences Techniques et ses annexes, voire Loi et Décret) et de la partie renseignant le point de contrôle.
Libellé	Description du point de contrôle.
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 (exemple : 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'ANJ, 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).
Elément d'analyse de la certification à 6 mois	Éléments sur lesquels l'analyse s'appuie sur : 1) les documents remis par l'opérateur, par exemple : - le dossier de définition de la plateforme d'hébergement du SMA ; - la documentation fonctionnelle et technique du logiciel capteur ; - le rapport de certification CSPN réalisé à l'occasion de la certification du coffre-fort et la cible de sécurité de cette certification ; - les rapports d'audits de sécurité déjà réalisés par l'opérateur – en particulier si le capteur est intégré à la plateforme de jeu – ou encore les rapport d'analyse de la maturité SSI de l'opérateur ; 2) les 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 fonctionnel, technique et de sécurité du composant logiciel capteur ; - l'audit de configuration de premier niveau de l'infrastructure d'hébergement du SMA. Le rapport associé est noté « audit de configuration des plateformes 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.).
Elément d'analyse de la certification annuelle	Éléments sur lesquels l'analyse s'appuie sur : 1) les documents remis par l'opérateur, par exemple : - le dossier de définition, mis à jour, de la plateforme d'hébergement du SMA et de la plateforme de jeu ; - la documentation fonctionnelle et technique actualisée du logiciel capteur et de la plateforme de jeu ; - le rapport de certification initiale à 6 mois du composant SMA ; - les rapports d'homologation effectués sur les logiciels de jeu ; - les rapports d'audits de sécurité réalisés par l'opérateur indépendamment des certifications prévues par la réglementation ; - les attestations d'absence de modification d'un composant (exemple : capteur) ; - les plans de remédiation des non-conformités et des vulnérabilités identifiées lors des précédentes certifications. 2) les 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 : - les audits d'architecture technique de la plateforme de jeu ; - les audits de configuration de premier niveau de l'infrastructure d'hébergement du SMA et de la plateforme de jeu. Ces rapports sont notés « audits de configuration des plateformes d'hébergement » dans la suite du document ; - les audits applicatifs intrusifs qui portent sur les composants logiciels de la plateforme de jeu qui ne font pas l'objet d'homologation. 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 et étayé (élément de configuration, extrait de code, etc.). La certification annuelle repose sur un socle d'analyses obligatoires, pouvant faire l'objet d'une actualisation. Les ET5 indiquent les analyses pour lesquelles cette actualisation peut être réalisée.
Commentaires ANJ	Précisions apportées par l'ANJ, 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, par l'organisme certificateur.
Conformité	Constat de l'analyse menée par l'organisme certificateur.
Commentaires certificateur	Précisions apportées par l'organisme certificateur, afin d'aider à la compréhension des résultats l'analyse du point de contrôle.

Matrice des exigences de la certification

(version 1.0 du 07/10/2022)

Exigence de la certification à 6 mois ?	Exigence de la certification annuelle ?	Point de contrôle	Libellé	Niveau de criticité	Éléments d'analyse	Commentaires ANJ	Rapports concernés	Conformité	Commentaires certificateur
	OUI	**PARTIE 1 - Suivi des audits de sécurité, certifications et homologations**							
	OUI	**E1**	Dans le cadre de la mission générale de contrôle de l'ANJ, les organismes certificateurs réalisent des audits de sécurité afin de vérifier le niveau de maturité SSI des opérateurs ainsi que le niveau de sécurité atteint par les dispositifs SMA et les plateformes de jeux. Un accès au site ainsi qu'à l'ensemble des équipements et des données de la ou des plateformes de jeux devra être accordé à l'ANJ ou aux organismes certificateurs mandatés.	3	Documentation remise par l'opérateur. Audit de configuration des plateformes d'hébergement.	L'opérateur devra notamment donner à l'organisme certificateur mandaté l'ensemble des accès et éléments de configuration requis afin que ce dernier puisse procéder aux contrôles attendus dans le cadre de sa mission d'audit.		Conforme	
	OUI	**E2**	L'opérateur doit corriger les éventuelles vulnérabilités mineures, importantes, majeures ou critiques, 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. Le plan de remédiation associé et établi par l'opérateur devra être communiqué à l'ANJ et à l'organisme certificateur mandaté.	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 dispositif SMA 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'ANJ ou un organisme mandaté par l'ANJ ; - plans de remédiation associés aux différentes vulnérabilités constatées.	Il s'agira de s'assurer que toutes les vulnérabilités constatées à l'issue des audits de sécurité font l'objet d'une remédiation et que les recommandations les plus pertinentes sont bien appliquées.		Conforme avec réserve	
	OUI	**E3**	L'opérateur informe l'ANJ des évolutions substantielles opérées (ex : mise en place d'une nouvelle technologie) au sein de sa plateforme.	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'ANJ, depuis le dépôt de la demande d'agrément ou la dernière certification annuelle effectuée, le cas échéant.		Non conforme	
	OUI	**E4**	L'opérateur communique à l'ANJ les résultats des audits de sécurité réalisés sur ses plateformes de jeux par des organismes tiers.	1	Documentation remise par l'opérateur.				
	OUI	**E5**	Les nouveaux logiciels de jeu doivent être 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 et décisions d'homologation 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.			
	OUI	**PARTIE 2 - PSSI : Politique et schéma directeur en sécurité des systèmes d'information de l'opérateur**							
	OUI	**E6**	L'opérateur possède 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 mise 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 plateforme d'hébergement du SMA et la plateforme de jeu.			
	OUI	**E7**	L'opérateur possède 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 doit aborder les sujets suivants :	1					
	OUI		- Eléments stratégiques :						
	OUI	**E8**	- 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.				
	OUI	**E9**	- 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.				
	OUI	**E10**	- 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.				
	OUI	**E11**	- 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.				
	OUI	**E12**	- 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.				
	OUI	**E13**	- 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.				
	OUI		- Règles de sécurité, classées par thème :						
	OUI	**E14**	- 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.				
	OUI	**E15**	- 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.				
	OUI	**E16**	- technique : identification / authentification, contrôle d'accès logique, journalisation, chiffrement.	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	**E17**	L'opérateur décline les éléments exigés par sa politique de sécurité. Cette déclinaison technique et détaillée fait le lien entre la politique de sécurité et toutes les procédures liées aux systèmes d'information, en établissant des moyens de sécurisation, aussi bien organisationnels que techniques, des systèmes d'information et en assurant le suivi de ces moyens dans le temps.	2	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	**E18**	L'opérateur doit 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.				
OUI	**OUI**	**PARTIE 3 - Architecture globale et procédures d'administration et d'exploitation**							
OUI	**OUI**		L'organisation mise en place pour gérer le système d'information de l'opérateur doit s'appuyer sur une documentation et des procédures permettant de suivre ses évolutions. La documentation comporte :						

OUI	**OUI**	**E19**		- la déclinaison sous forme de procédures de la politique de sécurité ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
OUI	**OUI**	**E20**		- une description fonctionnelle de l'infrastructure d'hébergement du SMA, précisant les différents composants, leurs fonctions et les flux transitant par ces derniers.	1	Documentation remise par l'opérateur + avis d'expert.				
OUI	**OUI**	**E21**	La documentation des infrastructures d'hébergement du SMA et de la plateforme de jeu de l'opérateur 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.				
OUI	**OUI**	**E22**	L'opérateur est responsable, sur toute la durée de validité de l'agrément ou de l'autorisation d'exploitation sous droits exclusifs, de la tenue à jour et de la cohérence du « dossier de définition ». Chaque modification du dossier fait l'objet d'une nouvelle remise de document à l'ANJ.		1	Documentation remise par l'opérateur + analyse de premier niveau.	Les modifications du « dossier de définition » intervenues dans l'année sont compilées et présentées à l'organisme certificateur. Cette soumission via la certification annuelle tient lieu de remise à l'ANJ.			
OUI	**OUI**		La documentation des infrastructures d'hébergement du SMA et de la plateforme de jeu qui intègre un volet technique et procédural rassemble les informations suivantes :							
OUI	**OUI**	**E23**		- 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.				
OUI	**OUI**	**E24**		- les spécifications techniques du système d'information, en particulier les configurations à jour des équipements qui le composent ;	2	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.				
OUI	**OUI**	**E25**		- la liste descriptive précise de tous les composants, avec le recensement d'éléments factuels, comme les versions des logiciels utilisées, 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.				
OUI	**OUI**	**E26**		- une liste des 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.				
	OUI	**PARTIE 4 - Architecture réseau**								
	OUI	**E27**	Les systèmes d'information de l'opérateur doivent 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 plateformes.		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.			
	OUI		L'opérateur met en œuvre un cloisonnement du réseau à l'aide de mécanismes de filtrage de niveau 3 (modèle OSI) au minimum, au moins entre les zones suivantes :							
	OUI	**E28**		- 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 : a) les rapports d'audits de configuration des plateformes d'hébergement réalisés dans le cadre de la vérification initiale de la plateforme de jeu ; b) les rapports d'audits de configuration de la certification à 6 mois du dispositif SMA ; c) les rapports d'audit de configuration des certifications annuelles antérieures, le cas échéant. Audit de configuration des plateformes d'hébergement. Audit d'architecture technique de la plateforme de jeu.				
	OUI	**E29**		- la zone des équipements dédiés à 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 des interfaces d'administration doit s'effectuer au niveau 3 (IP) et non pas seulement au niveau 7 (applicatif).			
	OUI	**E30**		- 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					
	OUI	**E31**	La politique de filtrage réseau adoptée respecte le principe du moindre privilège : les règles de filtrage sont élaborées suivant un principe de liste blanche.		2	Audit de configuration des plateformes d'hébergement. Audit d'architecture technique de la plateforme de jeu.	L'analyse devra prendre en compte le filtrage en entrée et en sortie.			
OUI	**OUI**	**E32**	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 plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**PARTIE 5 - Maintien en conditions de sécurité**								
OUI	**OUI**	**E33**	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 (https://www.certa.ssi.gouv.fr). L'opérateur applique les correctifs de sécurité qui sont proposés par les éditeurs, dans les documents du CERT ou demandés explicitement par l'ANJ, le cas échéant.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E34**	L'opérateur doit a minima prohiber l'utilisation, sur ses plateformes, des systèmes et logiciels obsolètes, c'est-à-dire qui ne sont plus maintenus par leur éditeurs et ne bénéficient plus de support correctif.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**		Si aucun correctif de sécurité n'est disponible auprès de l'éditeur :							
OUI	**OUI**	**E35**		- l'opérateur suit les recommandations de ce dernier ou d'un CERT, dans le cadre d'un contournement provisoire ;	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E36**		- 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 plateformes d'hébergement. Documentation remise par l'opérateur.				

OUI	**OUI**	**E37**	L'opérateur tient à jour le « dossier de définition » avec la liste des correctifs de sécurité appliqués sur les serveurs et communique à l'ANJ la version actualisée du document.		1	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.				
OUI	**OUI**	**PARTIE 6 - Sécurisation des communications et contrôle des accès d'administration**								
	OUI	**E38**	L'intégralité des échanges de données doit 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, mise à jour de contenu, etc.) doivent 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'ANJ ; - les communications réseaux entre joueurs et opérateur ; - les communications réseaux entre les modules au sein du SMA.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**		Les accès d'administration aux équipements, dont les équipements du SMA, doivent être protégés à l'aide des mécanismes suivants :							
OUI	**OUI**	**E39**		- 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 plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E40**		- ou bien une authentification par mot de passe, avec des règles de composition et de renouvellement conformes 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 plateformes d'hébergement. Documentation remise par l'opérateur.	Les authentifications en clair sont prohibées, un chiffrement des communications est obligatoire. La mesure doit permettre de prouver la robustesse des mots de passe.			
OUI	**OUI**	**E41**		- un contrôle d'accès basé sur les adresses IP est réalisé.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**PARTIE 7 - Gestion des configurations**								
OUI	**OUI**	**E42**	À l'issue de la mise en œuvre d'un nouvel équipement ou de l'installation d'une nouvelle application, l'opérateur met à disposition de l'ANJ 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 plateformes d'hébergement. Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.				
OUI	**OUI**	**E43**	Les composants systèmes, réseau et applicatifs mis en œuvre par l'opérateur doivent avoir fait l'objet 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 plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E44**	Afin de détecter d'éventuelles erreurs de manipulation mais aussi le résultat d'attaques, l'intégrité des fichiers de configuration des équipements doit être vérifiée régulièrement. Cette vérification doit pouvoir être faîte sur demande de l'ANJ et un rapport de diagnostic doit pouvoir lui être transmis.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**PARTIE 8 - Gestion de la sécurité dans les cycles de développement**								
OUI	**OUI**	**E45**	L'opérateur gère 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 devoir de l'opérateur de l'effectuer.			
OUI	**OUI**	**E46**	L'opérateur contractualise avec ses prestataires le respect d'un référentiel de développement sécurisé pour les projets dont il externalise la prise en charge.		1	Audit applicatif intrusif. Documentation remise par l'opérateur.				
OUI	**OUI**		Le référentiel de développement sécurisé doit en particulier aborder le problème de la validation des paramètres, notamment :							
OUI	**OUI**	**E47**		- 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.				
OUI	**OUI**	**E48**		- vérifier les données en entrée et en sortie ;	2	Audit applicatif intrusif. Documentation remise par l'opérateur.				
OUI	**OUI**	**E49**		- utiliser une fonction de vérification des données identique et centralisée.	2	Audit applicatif intrusif. Documentation remise par l'opérateur.				
OUI	**OUI**	**E50**	L'opérateur doit pouvoir transmettre à l'ANJ l'ensemble de codes sources des composants de logiciels de jeux au sens du volume des exigences techniques (ET2) utilisés sur ses plateformes, si cette dernière le lui demande.		3	Documentation remise par l'opérateur.				
OUI	**OUI**	**PARTIE 9 - Gestion des sauvegardes des données**								
OUI	**OUI**	**E51**	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 composant coffre-fort du SMA.		3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E52**	Ces sauvegardes sont mises à disposition de l'ANJ par l'opérateur pour consultation et archivage.		2	Documentation remise par l'opérateur.				
OUI	**OUI**	**E53**	Le type de support et le format de la sauvegarde sont indiqués par l'opérateur pour permettre à l'ANJ de vérifier l'exploitabilité de ces sauvegardes et de leurs contenus.		3	Documentation remise par l'opérateur.				
OUI	**OUI**	**E54**	Les données que l'opérateur est tenu de mettre à la disposition de l'ANJ (cf. articles 30 et 31 du décret n° 2010-518) doivent être conservées pour une durée de 6 ans. Pour les données personnelles concernant chaque joueur, ce délai de 6 ans court à compter de la clôture du compte joueur correspondant.		3	Documentation remise par l'opérateur.				
OUI	**OUI**		Pendant tout le temps de leur conservation, les archives et leurs sauvegardes, doivent :							
OUI	**OUI**	**E55**		- être protégées en intégrité ;	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E56**		- être accessibles aux personnes autorisées seulement ;	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E57**		- pouvoir être relues et exploitées.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				

OUI	OUI	E58	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 de protection des archives qu'il est capable de mettre en œuvre.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E59	La précision de l'horloge par rapport à laquelle les systèmes d'information se synchronisent pour dater les événements journalisés ou archivés, doit être inférieure à une seconde par rapport au temps UTC. La source de temps doit être fiable.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.	L'auditeur devra démontrer le respect de l'exigence.			
OUI	OUI	**PARTIE 10 - Gestion de la journalisation technique et fonctionnelle**							
OUI	OUI	E60	L'opérateur doit maintenir et pouvoir fournir à l'ANJ, les journaux des traces techniques pour les évènements clé. Une première liste des événements concernés : - accès aux modules du SMA ; - opérations de maintenance effectuées ; - ouverture et fermeture de la prise de paris, mises poker, etc.	2	Documentation remise par l'opérateur.				
OUI	OUI	E61	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 sont journalisés en s'appuyant sur une source de temps fiable.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E62	Concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un package Linux, etc.), toutes les traces disponibles au niveau des équipements sont activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E63	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 plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E64	Les traces de sécurité issues de la journalisation technique des plateformes sont analysées périodiquement par l'opérateur afin d'identifier les anomalies éventuelles.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E65	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 plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E66	L'opérateur pourra mettre à disposition de l'ANJ ces journaux bruts produits par les différents équipements ou logiciels.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E67	Les incidents ou les comportements anormaux pouvant avoir un impact sur la sécurité du service doivent être traités et systématiquement faire l'objet d'une alerte et d'un compte-rendu écrit qui pourra être communiqué à l'ANJ.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	**PARTIE 11 - Gestion des accès physiques**							
OUI	OUI	E68	Les locaux techniques doivent être accessibles aux seules personnes habilitées par l'opérateur.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI		L'opérateur doit :						
	OUI	E69	- être en mesure d'identifier parfaitement les personnes ayant à intervenir dans ses locaux et sur ses équipements ;	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E70	- maintenir à jour les fonctions et les autorisations d'accès de ces personnes.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E71	Les personnes ayant à intervenir sur les équipements des plateformes de jeux doivent avoir été sensibilisées à la sécurité des systèmes d'information (ex: confidentialité des mots de passe et des données hébergées, etc.).	1	Documentation remise par l'opérateur.				
	OUI	E72	L'opérateur doit formaliser et appliquer des procédures organisationnelles nécessaires vis-à-vis des intervenants, 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	Documentation remise par l'opérateur.				
	OUI	E73	Les locaux abritant les équipements doivent être sécurisés : serrure haute sécurité, alarme d'ouverture, enregistrement des accès, video-surveillance, etc.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E74	L'accès physique aux locaux abritant les équipements doivent être limité : filtrage des personnes, contrôle des accès physiques, etc.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	**PARTIE 12 - Gestion de l'environnement physique**							
	OUI	E75	Les matériels et supports informatiques (support de sauvegarde, etc.) doivent être placés dans des zones de sécurité physiques, conçues pour lutter contre les tentatives d'intrusion et lutter contre les sinistres et accidents liées à l'environnement.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E76	La structure d'hébergement dispose de mesure de protection incendie.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E77	Le centre d'hébergement dispose, 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 plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E78	Un système de climatisations redondantes et indépendantes par salle assure la stabilité des températures et du taux d'humidité.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E79	Tous les matériels (climatiseurs, panneaux électriques, etc.) utilisés par l'opérateur font l'objet d'un contrat de maintenance.	1	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E80	Les sites d'exploitation doivent être surveillés 24h/24 et 7j/7.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	**PARTIE 13 - Équipe sécurité**							
	OUI	E81	L'opérateur doit 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.				
	OUI	**PARTIE 14 - Interdits de jeu**							

	OUI	**E82**	Le serveur DNS doit faire l'objet d'une sécurisation conforme à l'état de l'art, 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 plateforme 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'ANJ, afin de mettre en œuvre des règles de filtrage réseau et listes de contrôle d'accès au niveau applicatif.	3	Audit de configuration des plateformes 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.			
	OUI	**PARTIE 15 - Données à la demande**							
	OUI	**E83**	Au délà des données tracées dans le SMA ou mises à disposition systématiquement, l'ANJ peut ponctuellement exiger des rapports ou données plus détaillés ou établis avec des critères de recherche précis, qui notamment peuvent être nominatifs. Ainsi, l'opérateur doit pouvoir exécuter des requêtes sur ses systèmes métier afin d'en extraire des données, dans des délais raisonnables. Ces rapports complèteront les informations qui peuvent être obtenues via le SMA et les informations remontées systématiquement et automatiquement vers le système d'information de l'ANJ. On peut citer : - la fourniture à l'ANJ de toutes les données techniques et non techniques liées à un évènement particulier ; - des demandes d'enquête de la part de l'ANJ 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 (SMA, plateforme, etc.).	3	Documentation remise par l'opérateur.	Pour chacun des éléments cités en exemple, l'opérateur devra spécifier la nature des données conservées, la période de rétention correspondante et les procédures mises en place pour la mise à disposition de ces informations à l'ANJ.			
OUI	**OUI**	**PARTIE 16 - SMA : généralités**							
OUI	**OUI**	**E84**	L'opérateur doit 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., et sur l'ensemble des noms de domaine déclarés auprès de l'ANJ)				
OUI	**OUI**	**E85**	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 de domiciliation est en France doivent être redirigées vers ce site.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E86**	Dans le cadre de ses activités de jeux, l'opérateur met en œuvre un dispositif technique appelé « SMA » à des fins de contrôle. Le SMA est un dispositif de recueil et d'archivage de données liées à un évènement de jeu ou à un compte joueur. Ce dispositif est :	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E87**	- développé et exploité sous la responsabilité de l'opérateur ;	2	Documentation remise par l'opérateur (identification des prestataires : développeurs, exploitants, etc.).				
OUI	**OUI**	**E88**	- installé sur un support situé en France métropolitaine.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E89**	Tous les échanges de données liées à un évènement de jeu ou à un compte joueur, entre un joueur réputé français et la plateforme de jeu, doivent transiter par le SMA.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**		En particulier, les connexions provenant de joueurs réputés français doivent être redirigées vers le SMA. La plateforme de jeu doit rediriger vers le SMA les requêtes suivantes :						
OUI	**OUI**	**E90**	- 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 des plateformes d'hébergement, en particulier la description des dispositifs techniques mis en place par l'opérateur côté SMA/plateforme 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).				
OUI	**OUI**	**E91**	- ou, après authentification du joueur, si le joueur a indiqué un domicile en France lors de l'ouverture de son compte de jeu.	3					
OUI	**OUI**	**E92**	L'opérateur doit permettre à l'ANJ de se rendre, à tout moment, sur le site d'hébergement du SMA pour saisir l'ensemble ou un sous-ensemble des données qui y sont conservées. À cette fin, l'ANJ 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 SMA, le cas échéant, pour autoriser un tel accès.	Il est en particulier question de l'accès au site d'hébergement du composant coffre-fort du SMA.			
OUI	**OUI**		Les échanges de données suivants doivent être sécurisés afin d'en garantir l'authenticité, l'intégrité ainsi que la confidentialité :						
OUI	**OUI**	**E93**	- les échanges entre le joueur et le SMA ;	3	Audit de configuration de la plateforme 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.			
OUI	**OUI**	**E94**	- les échanges entre les différents modules du SMA ; - les échanges entre le SMA et la plateforme de jeux de l'opérateur ; - les échanges entre le SMA et la plateforme de l'ANJ.	2	Audit de configuration de la plateforme 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.			
OUI	**OUI**		Le SMA doit comporter des fonctionnalités de sécurité visant à le protéger des attaques par saturation, agissant :						
OUI	**OUI**	**E95**	- 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 plateforme 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.				

OUI	**OUI**	**E96**		- au niveau applicatif, avec l'envoi de multiples requêtes HTTP qui viseraient la saturation du SMA qui constitue potentiellement un point de défaillance unique de l'architecture, afin de le protéger (i) d'un épuisement de ressources (saturation des enregistrements temporairement mis en tampon et en attente d'un acquittement) et (ii) d'une saturation du coffre avec des enregistrements mal formés.	2	Audit de configuration de la plateforme d'hébergement, audit applicatif intrusif de l'application capteur, notamment la description des dispositifs techniques mis en place par l'opérateur appuyée par des éléments de configuration.				
OUI	**OUI**	**PARTIE 17 - SMA : module « coffre-fort »**								
OUI	**OUI**	**E97**	Le coffre-fort doit détenir une certification de sécurité de premier niveau (CSPN) délivrée par l'ANSSI (https://www.ssi.gouv.fr).		3	L'absence de certification CSPN est <u>rédhibitoire</u> pour l'obtention de la certification du SMA.				
OUI	**OUI**		La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des menaces :							
OUI	**OUI**	**E98**		- le dépôt ou l'injection d'enregistrements non autorisés ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E99**		- l'altération d'enregistrements ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E100**		- le vol de données ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E101**		- le déni de service.	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**		La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des fonctions de sécurité :							
OUI	**OUI**	**E102**		- l'authentification forte des utilisateurs et administrateurs ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E103**		- le chiffrement, la signature et l'horodatage des évènements ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E104**		- le chaînage des évènements.	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E105**	Toute suppression ou altération des données archivées, de manière malveillante ou non, doit pouvoir être identifiée par l'ANJ.		3	Audit de configuration de la plateforme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.				
OUI	**OUI**		Quatre profils d'autorisation doivent pouvoir être définis :							
OUI	**OUI**	**E106**		- profil « déposant » : profil attribué au module « capteur » du SMA. Il permet uniquement d'écrire des traces dans le journal. Le module capteur du SMA 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 plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E107**		- profil « lecteur » : profil attribué aux agents de l'ANJ 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 plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E108**		- 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 plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E109**		- profil « administrateur fonctionnel » : profil attribué aux personnes physiques de l'ANJ ou désignées par l'ANJ, 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 plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**		Les certificats associés au profil « lecteur » sont utilisés :							
OUI	**OUI**	**E110**		- 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 plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E111**		- 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 plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**		En termes de gestion des clefs de chiffrement, de signature, et d'horodatage :							
OUI	**OUI**	**E112**		- les tailles de clefs doivent être conformes aux règles énoncées dans le référentiel général de sécurité de l'ANSSI (https://www.ssi.gouv.fr/) ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E113**		- la cryptographie mise en œuvre en termes de générateurs de nombres pseudoaléatoires, fonctions de hachage, algorithmes symétriques et asymétriques doit respecter les règles de bonnes pratiques spécifiées dans le référentiel général de sécurité de l'ANSSI (https://www.ssi.gouv.fr/) ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E114**		- un HSM est utilisé pour les opérations de signature ; le biclef de signature peut être soit généré 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.			
OUI	**OUI**	**E115**		- les données chiffrées le sont au moyen de la clef publique du certificat transmis par l'ANJ : seule l'ANJ 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 plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	**OUI**	**E116**	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. Dans le cadre d'un coffre mutualisé entre plusieurs agréments, chaque agrément doit faire l'objet d'un espace de stockage spécifique. La ségrégation des espaces de stockage doit, *a fortiori*, être mise en oeuvre dans le cadre d'une mutualisation interopérateurs, le cas échéant.			3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**		La sécurité physique des accès au coffre-fort est assurée par :							
OUI	**OUI**	**E117**		- l'hébergement dans un emplacement protégé ;	2	Audit de configuration de la plateforme d'hébergement : une analyse de premier niveau de la sécurité physique de l'infrastructure d'hébergement est attendue.				

OUI	**OUI**	**E118**		- la mise en place d'un contrôle d'accès ;	2	Audit de configuration de la plateforme d'hébergement : une analyse de premier niveau de la sécurité physique de l'infrastructure d'hébergement est attendue.				
OUI	**OUI**	**E119**		- 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	Audit de configuration de la plateforme d'hébergement : une analyse de premier niveau de la sécurité physique de l'infrastructure d'hébergement est attendue.				
OUI	**OUI**	**E120**		- la mise en oeuvre de protections physiques.	2	La méthode de scellement du coffre-fort 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.				
OUI	**OUI**	**PARTIE 18 - SMA : module « capteur »**								
OUI	**OUI**	**E121**	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 intrusif de l'application capteur. Documentation remise par l'opérateur.				
OUI	**OUI**		Le module « capteur » doit :							
OUI	**OUI**	**E122**		- être authentifié par certificat auprès du coffre-fort, 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 intrusif de l'application capteur.	L'analyse doit être étayée par des extraits de code source du capteur.			
OUI	**OUI**	**E123**		- 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 intrusif de l'application capteur. Voir les exigences dédiées aux fonctions de création et de stockage des traces.				
OUI	**OUI**	**E124**	L'ensemble des composants du SMA doivent être synchronisés en temps, auprès d'une source de temps fiable.		3	Audit de configuration de la plateforme d'hébergement.				
OUI	**OUI**	**PARTIE 19 - SMA : fonctions de création et de stockage des traces**								
OUI	**OUI**		La fonction de création de traces du capteur doit respecter les principes suivants :							
OUI	**OUI**	**E125**		- 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 SMA. Cette fonction doit être appelée systématiquement à chaque évènement ou échange de données dont les traces sont exigées ;	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 intrusif de l'application capteur.				
OUI	**OUI**	**E126**		- la fonction de création de traces est implémentée en amont de la logique de jeu. Elle intercepte voire relaie le flux applicatif entre le joueur et l'opérateur (exemple : fonctionnement de type proxy) ;	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 intrusif de l'application capteur.	L'implémentation en amont de la logique de jeu concerne en particulier les évènements à tracer au coffre où l'acquittement du joueur est attendu ou sont une conséquence directe d'une action du joueur. Par opposition, lorsque l'évènement a pour origine l'opérateur et ne nécessite pas un acquittement de la part du joueur, la fonction de création de traces est directement appelée par la plateforme de jeu.			
OUI	**OUI**	**E127**		- le SMA doit offrir une architecture dotée d'une très haute disponibilité avec redondance de mécanismes afin de strictement limiter les incidents potentiels de stockage ;	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 intrusif de l'application capteur.				
OUI	**OUI**	**E128**		- le principe d'une annulation d'un jeu concerné par un incident de stockage d'un des évènements doit être retenu.	2	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 intrusif de l'application capteur.				
OUI	**OUI**		La fonction de création de traces d'un événement doit :							
OUI	**OUI**	**E129**		- être invoquée suite à une requête émise par le joueur (si celle-ci requiert un enregistrement). Cette requête peut résulter : (i) d'une action du joueur, à son initiative, comme une prise de pari, (ii) d'un acquittement par le joueur, suite à un message transmis à l'initiative de la plateforme, 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 intrusif de l'application capteur.				
OUI	**OUI**	**E130**		- être invoquée suite à une action à l'initiative de l'opérateur, sans acquittement par le joueur, dont la trace est exigée (ex : rectification des informations du compte joueur).	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 intrusif de l'application capteur.				
OUI	**OUI**	**E131**		- reposer sur un module applicatif à état : les traces d'évènement générés doivent être temporairement conservées au niveau du capteur dans une mémoire tampon ou un dispositif de stockage temporaire équivalent (ex: base de données), avant toute transmission au niveau du coffre-fort, dans l'attente d'un acquittement de la plateforme 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 et générés à l'initiative du joueur (action ou acquittement) sont validés, avant stockage au coffre-fort, par la plateforme.	Tout écart par rapport à ce mode de fonctionnement doit être techniquement justifié (exemple : évènements POPARTIE générés par la plateforme 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 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 SMA.			
OUI	**OUI**	**E132**		- gérer un acquittement de la plateforme de jeux, afin de limiter les risques d'attaques qui viseraient à saturer le coffre-fort 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 intrusif de l'application capteur.				
OUI	**OUI**	**E133**		- en cas d'acquittement négatif de la part de la plateforme 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 intrusif de l'application capteur.				
OUI	**OUI**	**E134**		- en cas d'acquittement positif de la part de la plateforme de jeux, l'évènement présent en mémoire tampon au niveau du capteur peut être transformé au format exigé par l'ANJ, pour son stockage par le coffre-fort.	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 intrusif de l'application capteur.				
OUI	**OUI**	**E135**		- gérer les cas d'acquittements négatifs de la part du coffre-fort, en cas de défaillance d'enregistrement.	2	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 intrusif de l'application capteur.	Des mécanismes de reprise sur erreur peuvent être implémentés au niveau du capteur, par exemple par des tentatives de retransmission au coffre d'un l'évènement.			

OUI	**OUI**	**E136**		- garantir l'enregistrement d'un évènement de jeu au niveau du coffre-fort, sous peine d'annulation de l'opération de jeu.	2	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 intrusif de l'application capteur.	Cette exigence repose sur un mode de 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 les files d'attente, les 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-fort (ex : analyse du mécanisme de file d'attente de type *message broker*).			
OUI	**OUI**		La fonction de stockage correspond à l'archivage des données tracées dans un coffre-fort numérique afin d'en garantir l'intégrité et l'exhaustivité dans le temps. Le stockage des données consiste en les étapes suivantes :							
OUI	**OUI**	**E137**		- l'établissement d'un canal sécurisé, suite à l'authentification mutuelle du déposant (i.e. le capteur) avec le coffre-fort, via une session TLS mutuellement authentifiée par certificat X.509v3 ;	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	**OUI**	**E138**		- 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.			
OUI	**OUI**	**E139**		- 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				
OUI	**OUI**	**E140**		- 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				
OUI	**OUI**	**E141**		- 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				
OUI	**OUI**	**E142**		- 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				
OUI	**OUI**		Concernant les opérations de signature et de chiffrement :							
OUI	**OUI**	**E143**		- le format de signature est XADES-T avec un jeton d'horodatage conforme à la 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.			
OUI	**OUI**	**E144**		- le chiffrement des données est réalisé au moyen de la clé publique de l'ANJ 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.			
OUI	**OUI**		Concernant le traitement par lots :							
OUI	**OUI**	**E145**		- 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				
OUI	**OUI**	**E146**		- la granularité du traitement par lot doit être l'évènement.	1	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	**OUI**	**PARTIE 20 - SMA : fonction d'accès aux traces**								
OUI	**OUI**		L'opérateur agréé ou titulaire de droits exclusifs doit fournir les éléments suivants, pour chaque agrément ou périmètre d'activité sous droits exclusifs :							
OUI	**OUI**	**E147**		- 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.				
OUI	**OUI**	**E148**		- 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.				
OUI	**OUI**	**E149**		- un outil de validation des données du SMA et d'extraction des traces des opérations de jeu utilisable sur le site du SMA, et dans les laboratoires de l'ANJ (mode hors-ligne).	3	Documentation remise par l'opérateur.				
OUI	**OUI**		L'architecture de la partie coffre-fort du SMA doit distinguer :							
OUI	**OUI**	**E150**		- un espace de stockage des données situé dans une zone réseau sécurisée ;	3	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E151**		- une couche d'accès à l'espace de stockage accessible.	3	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.				
OUI	**OUI**	**E152**	Les données stockées dans le coffre-fort doivent être en accès permanent à distance, depuis les locaux de l'ANJ (i.e. depuis une ou plusieurs adresses IP identifiées).		3	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.	Il s'agit de s'assurer que des mesures sont mises en œuvre pour garantir la haute-disponibilité des données stockées dans le coffre-fort.			
OUI	**OUI**	**E153**	Les données accessibles à distance doivent couvrir au moins les 12 derniers mois d'activité de l'opérateur (période glissante).		3	Documentation remise par l'opérateur.	Il s'agit de pouvoir accéder aux données en temps réel sur une période de 12 mois glissants. L'accès à des données plus anciennes peuvent quant à elles faire l'objet de demandes spécifiques.			
OUI	**OUI**	**E154**	Les données doivent rester accessibles sur le site d'hébergement du SMA sur toute la durée de conservation exigée par la loi (article 31 du Décret n° 2010-518 du 19 mai 2010).		3	Documentation remise par l'opérateur.				
OUI	**OUI**	**E155**	L'extraction du coffre-fort 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.				
OUI	**OUI**	**E156**	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'ANJ.		2	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.				

OUI	**OUI**		La couche d'accès expose un service web doté des deux principales interfaces suivantes :							
OUI	**OUI**	**E157**		- 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.				
OUI	**OUI**	**E158**		- 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.				
OUI	**OUI**		L'outil réalisé par l'opérateur doit permettre :							
OUI	**OUI**	**E159**		- d'interroger à distance le coffre de l'opérateur pour télécharger les traces demandées (outil de collecte) ;	3	Documentation remise par l'opérateur.				
OUI	**OUI**	**E160**		- 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.				
OUI	**OUI**		L'outil doit implémenter :							
OUI	**OUI**	**E161**		- l'interface WSDL définie par l'ANJ, ou proposer une interface d'interrogation équivalente notamment basée sur l'identifiant d'opérateur, de coffre, sur l'agrément ou périmètre d'activité sous droits exclusifs, et une tranche d'évènements ou de dates descendant à l'heure ;	1	Documentation remise par l'opérateur.				
OUI	**OUI**	**E162**		- les options en ligne de commande suivantes : - la configuration d'une URL, comportant un nom de domaine pleinement qualifié identifiant le service Web ; - la configuration d'un identifiant de coffre, dans le cas où l'architecture mise en place par l'opérateur compterait plusieurs coffres à des fins de haute-disponibilité ; - la configuration d'une plage horaire, permettant le téléchargement du fichier de traces correspondant aux évènements de jeux horodatée enregistrés dans cette plage ; - la configuration d'une plage d'évènements, permettant le téléchargement du fichier de traces correspondant aux évènements de jeux dont les identifiants sont présents dans la tranche ; - la configuration d'un certificat X509v3 client, au format PEM et de la biclef RSA au format PEM PKCS#8 associée, à utiliser dans le cadre de l'authentification mutuelle avec le Web Service ; - la configuration d'une passphrase, pouvant être prise en compte en ligne de commande, dans un fichier, sur l'entrée standard ou par l'intermédiaire de l'environnement et permettant le déchiffrement éventuel de la biclef RSA au format PEM PKCS#8 ; - la configuration d'une autorité de certification, sous la forme d'un certificat X509v3 au format PEM, afin de valider le certificat X.509v3 serveur présenté par le Web Service ; - la configuration d'une liste de noms de domaine pleinement qualifiés pouvant être utilisés comme dépôt de téléchargement de fichiers de traces (présents dans les URI des rapports générés) ; - la configuration d'un chemin sur le système de fichiers pointant vers le fichier dans lequel enregistrer les données téléchargées ; - la configuration d'un chemin sur le système de fichiers pointant vers le fichier de configuration de l'outil ; - la configuration d'un curseur de verbosité, permettant de régler le niveau d'affichage d'informations de débogage.	1	Documentation remise par l'opérateur.				
OUI	**OUI**	**E163**		- le protocole de transport TLS 1.3. Privilégier l'usage de suites crytographiques conformes aux recommandations énoncées par l'ANSSI.	2	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur + avis d'expert.	La version TLS v1.2 est tolérée. Les versions obsolètes SSLv2, SSLv3, TLS 1.0 et TLS 1.1 sont à proscrire.			
OUI	**OUI**	**E164**		- 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.				
OUI	**OUI**		L'accès réseau de l'accès à distance doit :							
OUI	**OUI**	**E165**		- faire l'objet d'un filtrage implémenté 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 plateforme d'hébergement. Documentation remise par l'opérateur + avis d'expert.				
OUI	**OUI**	**E166**		- faire l'objet d'une journalisation et l'objet de procédures de traitement d'incident, le cas échéant.	2	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur + avis d'expert.				
OUI	**OUI**	**E167**	L'outil d'extraction et de validation des traces doit implémenter les options suivantes : - la configuration d'un certificat X509v3 de déchiffrement, au format PEM et de la biclef RSA au format PEM PKCS#8 associée, à utiliser dans le cadre du déchiffrement des traces (chiffrées à l'aide de la clef publique de l'ANJ transmise à l'opérateur) ; - la configuration d'une passphrase, pouvant être prise en compte en ligne de commande, dans un fichier, sur l'entrée standard ou par l'intermédiaire de l'environnement et permettant le déchiffrement éventuel de la biclef RSA au format PEM PKCS#8 ; - la configuration d'un certificat X509v3 de signature, au format PEM, permettant la validation des signatures horodatées ; - la configuration d'une autorité de certification, sous la forme d'un certificat au format PEM une nouvelle fois, afin de valider le certificat X.509v3 de signature ; - la configuration de chemins sur le système de fichiers pointant vers les fichiers respectivement source des données chiffrées, et destination des données déchiffrées ; - la configuration d'un chemin sur le système de fichiers pointant vers le fichier de configuration de l'outil ; - la configuration d'un curseur de verbosité, permettant de régler le niveau d'affichage d'information de débogage.		1	Documentation remise par l'opérateur.				
OUI	**OUI**	**PARTIE 21 - SMA : évènements XML : généralités**								
OUI	**OUI**		Les enregistrements XML sont :							
OUI	**OUI**	**E168**		- encodés au format UTF-8. On veillera en particulier au respect des caractères accentués (é, è, à) ;	3	Audit de code				
OUI	**OUI**	**E169**		- conformes à la norme XML (en particulier en termes d'encodage des entités XML) ;	3	Audit de code				
OUI	**OUI**	**E170**		- conformes au schéma XSD publié par l'ANJ ;	3	Audit de code				

OUI	**OUI**	**E171**		- filtrés, en termes de contenu, conformément aux expressions régulières (facette pattern) décrites dans le schéma XSD ;	3	Audit de code	L'analyse devra démontrer l'usage de filtres dans le code source.			
OUI	**OUI**	**E172**		- 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	Audit de code	L'analyse devra démontrer l'usage de filtres dans le code source.			