AUTORITÉ NATIONALE DES JEUX

RÉPUBLIQUE FRANÇAISE

EXIGENCES TECHNIQUES RELATIVES AUX SYSTÈMES D'INFORMATION DES OPÉRATEURS DE JEU

Résumé

Conformément au VIII de l'article 34 de la loi du 12 à l'article 32 du décret n°2010-518 dans sa version applicable à compter du 1er octobre 2020, qui prévoit que le Collège de l'ANJ détermine les exigences techniques nécessaires à son application, ce document précise les exigences techniques relatives aux systèmes d'information des opérateurs de jeu.

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 L. 320-4 du code de la sécurité intérieure :

« Les opérateurs de jeux d'argent et de hasard définis à l'article L. 320-6 concourent aux objectifs mentionnés aux 1°, 2° et 3° de l'article L. 320-3. Leur offre de jeu contribue à canaliser la demande de jeux dans un circuit contrôlé par l'autorité publique et à prévenir le développement d'une offre illégale de jeux d'argent ».

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 :

« 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 évalue les contrôles internes mis en place par les opérateurs. À cette fin, elle peut procéder ou faire procéder à tout audit des systèmes d'information ou des processus. […] »

Arrêté du 27 mars 2015 portant approbation du cahier des charges applicable aux opérateurs de jeu en ligne (annexe, article 11).

I.2 Présentation du corpus des exigences techniques

Afin de favoriser la lisibilité et la mise en œuvre des différentes catégories d'exigences techniques, le choix a été fait, d'une part, de les réécrire intégralement afin d'adapter le corpus des règles et de les segmenter en cinq volumes afin d'en faciliter l'appropriation par les opérateurs de jeux.

1. Volume 1 : exigences techniques relatives à l'agrément et la sécurité des systèmes d'information

Ce volume regroupe les obligations architecturales et matérielles, mais également organisationnelles, informationnelles et procédurales attendues en matière de politique de sécurité des systèmes d'information.

L'objectif visé ici est d'évaluer les moyens techniques et humains mis en œuvre pour gérer les risques liés aux systèmes techniques et fonctionnels de collecte, gestion et conservation des données.

Ces exigences sont mises en œuvre par l'opérateur dès l'obtention de l'agrément et la présentation de leur réalisation sous-tend la partie technique de l'instruction de la demande de renouvellement de l'agrément. Sans qu'elle fasse formellement l'objet d'un agrément, la partie du système d'information des opérateurs titulaires de droits exclusifs couvrant les jeux relevant de ces droits exclusifs doit conceptuellement intégrer les mêmes exigences, dans la mesure où les exigences ici formulées portent sur l'intégralité du système d'information ou des composants transverses.

Abordant de façon globale le système d'information et lié à la maturité de l'organisation en matière de sécurité, ce volume ne prend son plein sens qu'avec les autres volumes.

2. Volume 2 : exigences techniques relatives à l'homologation des logiciels

Ce document fixe le cadre d'homologation des logiciels de jeux et de paris permettant de garantir l'intégrité et la sécurité des logiciels de jeux.

Il définit le champ d'application de l'homologation, son périmètre technique et précise le détail de la procédure, formalisant et structurant les pièces et informations attendues de la part des opérateurs.

3. Volume 3 : exigences techniques relatives à la mise à disposition des données en application des articles 31 et 38 de la loi n° 2010-476 du 12 mai 2010

Ce volume permet de définir les mécanismes à mettre en place afin de garantir l'intégrité et la consistance de l'enregistrement des données de jeux, les modalités de mise à disposition ainsi que le formalisme des enregistrements effectués via le support matériel d'archivage (SMA).

Il s'attache également à définir les informations que les opérateurs doivent fournir en permanence par le biais du SMA afin de permettre à l'Autorité d'exercer sa mission de contrôle permanent de l'activité des opérateurs de jeux (articles 31 et 38 de la loi n° 2010-476 du 12 mai 2010).

4. Volume 4 : exigences techniques relatives à l'interrogation du ficher des Interdits de jeux

Ce volume définit les procédures techniques (formation des clés d'interrogation, canaux et mécanismes de consultation des services DNS) à mettre en œuvre par les opérateurs afin de procéder à l'interrogation du fichier des Interdits de jeux en application de l'article 22 du décret n° 2010-518 du 19 mai 2010 modifié.

Ce volume n'envisage pas la gestion par l'Autorité du fichier.

5. Volume 5 : exigences techniques relatives à la certification

Cet volet regroupe l'ensemble des exigences techniques relatives à l'architecture et aux mesures de sécurité que doivent examiner les organismes certificateurs à l'occasion de la certification du SMA six mois après le lancement de l'activité, et de la certification annuelle prévues par les dispositions de l'article 23 de la loi n° 2010-476 du 12 mai 2010 modifiée afin de s'assurer du maintien d'un niveau adéquat de sécurité du système.

Les volumes 1 à 5 s'appliquent tout au long de l'activité d'un opérateur.

I.3 Présentation et objectifs du document

Conformément aux dispositions du VIII de l'Article 34 de 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, l'ANJ 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.

À cette fin, le présent document définit les exigences techniques relatives à la demande d'agrément qui jalonne l'entrée sur le marché d'un opérateur puis à échéance de 5 ans lors du renouvellement d'agrément. Mais les exigences posées doivent s'entendre comme des exigences techniques, de sécurité et organisationnelles qui doivent nécessairement s'inscrire dans le temps de façon pérenne, pour tous les opérateurs.

La procédure d'agrément des opérateurs de jeu d'argent et de hasard doit permettre à l'Autorité de s'assurer de :

- la conformité aux règles relatives au SMA. Dans le cas d'un nouvel opérateur pour lequel le SMA ne serait pas encore en place, l'enjeu est de s'assurer que la stratégie de mise en œuvre de celui-ci intègre bien les exigences relatives au SMA ;
- la sécurité et de la robustesse du système d'information, tant dans sa composante technique qu'organisationnelle, inscrites dans la durée, sur lequel les jeux et services connexes (services de comptes joueurs, paiements, opérations de jeu, etc.) sont mis en œuvre par l'opérateur.

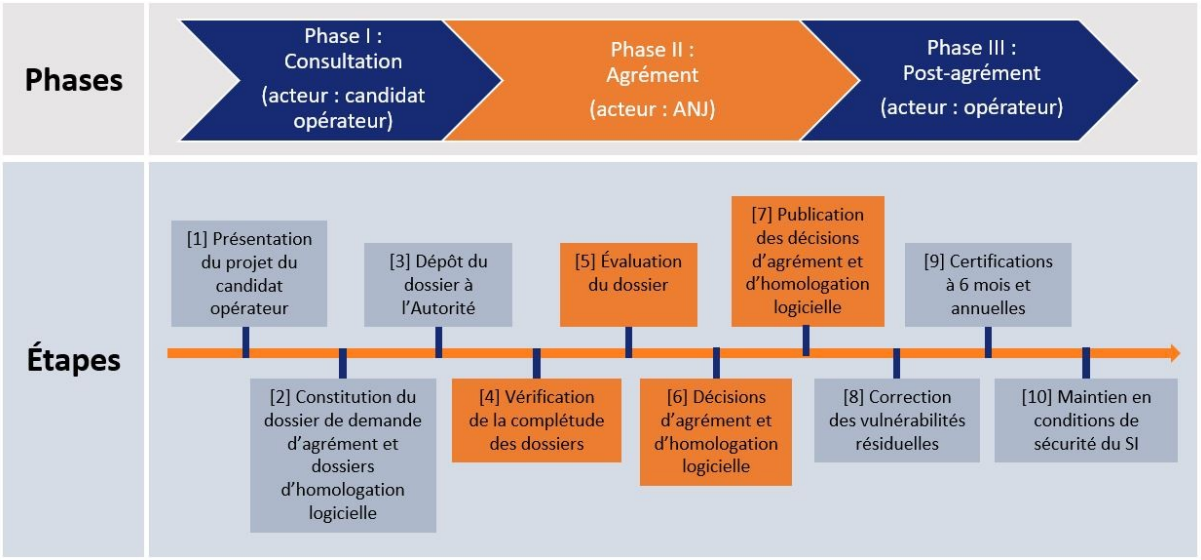
Les actions opérées par l'Autorité dans ce cadre font partie du dispositif de contrôle qu'elle a mis en place, visant à satisfaire aux objectifs définis à l'article L. 320-3 du code de la sécurité intérieure. S'il ressort de l'instruction d'une demande d'agrément que le moyens mis en œuvre ne permettent pas le respect de ces objectifs, l'ANJ rejettera la demande d'agrément. Plus particulièrement, il résulte du

premier alinéa du III de l'article 21 de la loi du 12 mai 2010 modifiée que l'Autorité peut refuser la délivrance ou le renouvellement d'un agrément « *pour un motif tiré de l'incapacité technique (…) du demandeur de faire face durablement aux obligations attachées à son activité ou de la sauvegarde de l'ordre public, de la lutte contre le blanchiment des capitaux et le financement du terrorisme, des nécessités de la sécurité publique et de la lutte contre le jeu excessif ou pathologique* ».

Le document expose :

- le champ d'application de la procédure d'agrément, c'est-à-dire dans quels cas l'opérateur doit faire une demande d'agrément (section II) ;
- le périmètre de l'agrément sur le volet SI dans ses principes (section III) ;
- le contenu du dossier d'agrément pour le volet SI, c'est-à-dire les documents qui le composent et les exigences relatives à chacun de ces documents en termes de contenu et d'organisation de l'information demandée (section IV)
- la procédure d'agrément (section V) ;
- les suites de l'agrément (section VI).

Les différentes phases de la procédure d'agrément sont présentées dans la figure ci-dessous :



I.4 Glossaire

Ce glossaire couvre l'intégralité des exigences techniques pour les volumes 1 à 5. Chacun des volumes reprend à l'identique les éléments du glossaire dans le seul objectif de faciliter le travail du lecteur en lui permettant de disposer d'un document auto-suffisant.

RGPD : règlement général sur la protection des données

Cloud : « service d'informatique en nuage », un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées.

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

Cyber-risque : les cyber-risques désignent toute atteinte aux systèmes informatiques et de communication, ainsi qu'aux données stockées ou en transfert. Ces sinistres, de nature à bloquer le fonctionnement de l'organisation, peuvent être le fait d'actes malveillants, d'erreurs humaines involontaires ou bien de dysfonctionnements techniques.

Disponibilité : propriété d'être accessible et utilisable à la demande par une entité autorisée.

Gestion d'incident : toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures et protocoles utiles à l'intervention en cas d'incident.

Incident : tout évènement ayant un impact négatif réel sur la sécurité des systèmes d'information et réseaux.

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.

Risque : combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque avec l'impact sur les éléments essentiels et sur l'organisme.

Risque résiduel : risque subsistant après la démarche de gestion des risques.

Système informatique : un système informatique représente l'ensemble des ressources matérielles et logicielles organisées pour collecter, stocker, traiter et communiquer les informations.

Sécurité des du système d'information (SSI) : la sécurité d'un système d'information consiste à réduire les risques pesant sur le système d'information, pour limiter leurs impacts sur le fonctionnement et les activités métiers des entreprises.

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.

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 archivage, 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.

Coffre-fort : élément constitutif du SMA, dont la fonction est de chiffrer, signer, horodater et archiver les données tracées et collectées depuis le flux en provenance du joueur ou fournis par la plateforme de jeux. Ceci afin de garantir la confidentialité, l'authenticité et l'exhaustivité dans le temps.

Support Matériel d'Archivage (SMA) : dispositif de recueil et d'archivage des données échangées entre le joueur et la plateforme de l'opérateur à l'occasion des opérations de jeux. Ce dispositif est développé et exploité sous la responsabilité de l'opérateur.

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

CNIL : Commission Nationale de l'Informatique et des Libertés.

Besoin de sécurité : propriété de sécurité à garantir pour une information, un processus, un service ou un bien matériel (exemples : disponibilité, intégrité, confidentialité).

Directive de sécurité : déclinaison de la PSSI sur une thématique spécifique.

Donnée sensible : au sens des présentes exigences, une donnée sensible est une information ou un support non classifié mais qui, si elle était révélée au public (via tout moyen de communication, vers le cercle professionnel ne disposant pas du besoin d'en connaître ou dans le cadre de l'environnement personnel) ou si un document était falsifié, pourrait nuire à l'image ou aux intérêts de l'ANJ, des opérateurs titulaires d'un agrément ou d'un droit exclusif, des organismes liés par contrat ou convention ou à leur personnel.

Ex : rapports d'audit (homologation, certification, agrément…), codes source, rapport d'homologation, rapports d'instruction, plan d'action, etc.

Document sensible : un document sensible est un document qui ne doit pas être porté à la connaissance de personnes (y compris en interne) qui n'ont pas le besoin de le connaitre.

Évènement redouté : incident qui affecte la disponibilité, l'intégrité et/ou la confidentialité d'une information, d'un processus, d'un service ou d'un bien matériel (exemple : indisponibilité du serveur de fichiers).

Gravité : estimation du niveau et de l'intensité des effets d'un risque. La gravité fournit une mesure des impacts préjudiciables perçus, qu'ils soient directs ou indirects.

Homologation de sécurité : validation par une autorité dite d'homologation, que le niveau de sécurité atteint par l'organisation est conforme aux attentes et que les risques résiduels sont acceptés dans le cadre de l'étude.

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 une ou plusieurs normes.

Incident de sécurité : évènement ou un ensemble d'évènements qui affecte la disponibilité, l'intégrité et/ou la confidentialité d'une information, d'un processus, d'un service ou d'un bien matériel.

Menace : terme générique pour désigner toute intention hostile de nuire.

Mesure de sécurité : moyen de traiter un risque prenant la forme de solutions ou d'exigences pouvant être inscrites dans un contrat. Une mesure peut être d'ordre fonctionnel, technique ou organisationnel. Elle peut agir sur une information, un processus, un service, un bien matériel, une partie prenante de l'écosystème.

Partie prenante : personne, groupe de personnes, organisation ou source de risque en interaction directe ou indirecte avec l'objet d'étude (exemples : un prestataire intervenant sur un système informatique du SI, un fournisseur).

Plan de continuité d'activité (PCA) : ensemble formalisé des procédures et mesures visant à poursuivre l'activité sans interruption de service et d'assurer la disponibilité des informations quels que soient les incidents rencontrés.

Plan de reprise d'activité (PRA) : ensemble formalisé des procédures à suivre pour la reconstruction et la remise en activité d'un système d'information en cas de sinistre ou d'incident majeur entraînant une interruption d'activité (exemples : incendie, panne, etc.).

Politique de sécurité des systèmes d'information (PSSI) : ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du ou des systèmes d'information.

Principe de sécurité : les principes de sécurité sont l'expression des orientations de sécurité nécessaires et des caractéristiques importantes de la SSI en vue de l'élaboration d'une PSSI.

Poste sensible : poste au sens des ressources humaines, susceptible d'avoir accès directement ou indirectement aux données à caractère personnel au sens du RGPD ou aux opérations de jeu ou à des données sensibles.

Règle de sécurité : les règles de sécurité définissent les moyens et les comportements définis dans le cadre de la PSSI. Elles sont construites par déclinaison des principes de sécurité dans un environnement et un contexte donné.

Risque : scénario décrivant un évènement redouté et toutes les menaces qui le rendent possibles. Son niveau est estimé en termes de gravité et vraisemblance.

Risque initial : scénario de risque évalué avant application de la stratégie de traitement du risque. Son niveau est estimé en termes de gravité et vraisemblance.

Risque résiduel : scénario de risque subsistant après application de la stratégie de traitement du risque. Son niveau est estimé en termes de gravité et vraisemblance.

Software as a service (SaaS) ou **logiciel en tant que service :** modèle d'exploitation commerciale des logiciels au sein duquel un fournisseur tiers héberge des applications logicielles et les rend disponibles à ses clients au travers de services en ligne.

Source de risque : élément, personne, groupe de personnes ou organisation susceptible d'engendrer un risque, de manière accidentelle ou délibérée.

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.

Le système d'information ne doit pas être confondu avec le système informatique qui n'est qu'un sous-ensemble du premier.

Système informatique : ensemble des moyens informatiques nécessaires au traitement de l'information (ordinateurs, programmes, réseau, les logiciels, etc.).

Vraisemblance : estimation de la probabilité qu'un risque se produise.

ANJ : Autorité Nationale des Jeux.

Jeu et pari en ligne : jeu et pari dont l'engagement passe par l'intermédiaire d'un service de communication au public en ligne.

Règles de jeu : ensemble des normes régissant les conditions de déroulement d'un jeu. Les règles de jeu décrivent notamment le matériel nécessaire au jeu, le nombre de joueurs autorisés, le but du jeu (ou conditions de victoire), la situation de début de partie et le déroulement du jeu.

Mécanique de jeu (ou logique de jeu) : dans le présent document, s'entend comme l'ensemble des calculs, traitements de l'information et comportements permettant la mise en œuvre des règles de jeu définissant le jeu.

Primitive (de jeu) : fonction élémentaire de traitement de l'information relative à un jeu. Le séquencement d'un ensemble cohérent de primitives de jeu vise à constituer une mécanique de jeu.

Fonctions métier (au sens du logiciel de jeu) : ensemble des primitives de jeu et des fonctions contribuant à l'implémentation de la mécanique de jeu et des règles de jeu définissant un jeu.

Architecture logicielle : organisation des différents éléments constitutifs d'un logiciel.

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.

Plateforme de jeu : ensemble des infrastructures techniques mises en œuvre aux fins de proposer des services de jeu aux joueurs ou parieurs.

Les éléments d'infrastructures ou de services peuvent être gérés en propre par l'opérateur ou l'être par des tiers (exemples : hébergement par un tiers, infrastructure tierce, solution logicielle de jeu mise à disposition par un tiers).

Logiciel de jeu : ensemble des applications ou programmes informatiques implémentant la mécanique de jeu.

Toute application ou programme informatique prenant en charge ou modifiant tout ou partie de la mécanique de jeu doit être considéré comme partie intégrante du logiciel de jeu.

Le logiciel de jeu est conceptuellement constitué des composants métiers suivants :

- D'un moteur de jeu intégré à la plateforme de jeu ;
- D'un totalisateur pour les jeux de paris à caractère mutuel ;
- D'un dispositif générateur de nombres aléatoires (GNA), pour les jeux de hasard ;
- D'un ou plusieurs clients de jeu mis à disposition des joueurs (exemples : application web, applications mobiles pour Android et iOS, logiciel sur borne, logiciel sur le terminal en point de vente, systèmes automatiques de prise de jeu à distance) ;
- De services API[1], intégrés à la plateforme de jeu, permettant aux différents composants applicatifs de la plateforme de jeux ou à toute autre application externe (dont les clients de jeu), d'interagir avec le moteur de jeu.

Si le logiciel de jeu a été développé selon une architecture modulaire respectant le découpage en composants métiers décrit ci-dessus, l'homologation logicielle peut être traitée de façon modulaire.

Moteur de jeu : composant du logiciel de jeu, généralement intégré à la plateforme de jeu, chargé de fournir des primitives de jeu au logiciel de jeu, voire d'assurer la gestion complète des opérations de jeu (exemples : prise de paris pour les paris sportifs et hippiques, tirage et distribution des cartes au poker, calcul et distribution des gains, …). L'intérêt d'un moteur de jeu développé comme un module distinct réside dans le caractère modulaire de la solution et la couche d'abstraction qu'il offre pour le développement des jeux qui s'appuient dessus. Les règles de jeu et la mécanique de jeu sont généralement portées par le moteur de jeu.

Totalisateur (pour les paris mutuels) : composant du logiciel de jeu à caractère mutuel, généralement intégré au moteur de jeu, réalisant un ensemble de calculs, dans le cadre d'un jeu, tels que le calcul des masses d'enjeux, des rapports payables des jeux gagnants et des gains associés aux coupons gagnants des joueurs.

Client de jeu : composant du logiciel de jeu, mis à disposition des joueurs ou parieurs, voire des détaillants en point de vente, permettant à ces derniers d'interagir, dans une relation « client-serveur », avec la plateforme de jeu, en particulier le moteur de jeu (exemples : consultation de l'offre de jeu affichée par l'opérateur, placement de paris, consultation des résultats des paris et des gains associés).

Le client de jeu peut implémenter tout ou partie de la mécanique de jeu et se présenter sous différentes formes :

- Application web, accessible depuis le site web de l'opérateur à l'aide d'un navigateur web ;
- Application pour ordinateur se présentant sous la forme d'un client lourd à installer sur le poste de l'utilisateur ;
- Application pour appareils mobiles ou tablettes ;

[1] API : Application Programming Interface. Solution qui permet à des applications de communiquer entre elles et de s'échanger mutuellement des services ou des données, *via* un langage de programmation.

- Application pour les bornes ou les terminaux en point de vente ;
- Système automatique de traitement des prises de jeu à distance (exemple : logiciel de prise de paris par SMS ou par messagerie instantanée).

Il convient de noter que le client de jeu est conceptuellement distinct du client applicatif utilisé. Par exemple, dans le cas d'une application pour téléphone mobile, le client applicatif contient le client de jeu mais peut également contenir des services de type gestion de compte, statistiques de jeu, actualités, etc. L'homologation du client de jeu n'a pas vocation à porter sur ces services annexes, mais il convient toutefois de s'assurer que le client de jeu est correctement isolé en termes de sécurité.

Borne (automatique) :également appelée terminal de jeu sans intermédiation humaine : dispositif matériel, positionné en réseau physique de distribution (exemples : hippodromes, détaillants, buralistes), intégrant une interface logicielle de type client de jeu, directement accessible aux joueurs ou parieurs. Ce dispositif autorise la prise de jeu et la consultation des résultats d'un jeu et des gains associés. Il autorise également les opérations de paiement (alimentation et retrait d'argent) selon les conditions préalablement portées à la connaissance des joueurs.

Terminal en point de vente, également appelé terminal de jeu avec intermédiation humaine : le terminal en point de vente occupe les mêmes fonctions que la borne en point de vente, l'accès à l'interface logicielle étant toutefois réservé aux personnels habilités par l'opérateur et responsables du point de vente (exemples : détaillants, buralistes). Le terminal peut disposer des fonctions de gestion dédiées aux détaillants (gestion de stocks, comptabilité, vente de tickets …).

Terminal Internet : moyen du joueur permettant à ce dernier d'accéder à Internet. En général, il s'agit d'un ordinateur, mais il peut également s'agir d'un téléphone ou d'une tablette, à la condition que le moyen permette un accès direct du joueur au site Internet.

Générateur de nombres aléatoires (GNA) : dispositif capable de générer une séquence de valeurs présentant des propriétés relevant du hasard (ou s'en approchant), pour laquelle il est difficile, voire impossible, de repérer des groupes de nombres qui suivent des règles de prédiction identifiables.

Ce dispositif est mis en œuvre lorsque le déroulement du jeu nécessite la génération d'un aléa, par exemple, au poker avec le tirage aléatoire des cartes ou encore les jeux de loterie en ligne sans tirage physique.

I.5 Identification des exigences et recommandations dans le document

Le présent document comporte deux niveaux de préconisations :

- 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 Champ d'application de l'agrément

Les exigences ci-dessous rappellent les cas dans lesquels un agrément est requis :

[E_AGR_CHA1] Un nouvel opérateur est systématiquement agréé préalablement à toute décision d'homologation logicielle, laquelle doit précéder toute ouverture d'offre de jeu.

[E_AGR_CHA2] Un opérateur bénéficiant d'un agrément doit le renouveler à l'échéance des 5 ans de validé de celui-ci. La procédure de renouvellement est strictement identique à la procédure initiale. Le dossier remis à l'autorité précisera quels éléments ont évolué par rapport à la situation 5 ans auparavant.

III Périmètre du volet SI de l'agrément

[E_AGR_PER1] Le périmètre du volet SI de l'agrément couvre l'ensemble des aspects organisationnels et techniques du SI de l'opérateur tels que mis en place (cas d'un renouvellement d'agrément) ou seront mis en place (cas d'un agrément nouveau), avec un accent particulier porté sur les composants spécifiques liés au jeu (compte joueur, capteur, SMA, …) et la sécurité du SI dans sa globalité.

IV Contenu du dossier d'agrément pour le volet SI

IV.1 Liste des documents exigés et dispositions communes

[E_AGR_DOS2] Le dossier de demande d'agrément d'un opérateur de jeu déposé auprès de l'ANJ, dans un format dématérialisé, comprend les pièces suivantes :

1. le schéma directeur du système d'information ;
2. la politique de sécurité des systèmes d'information ;
3. un document chapeau décrivant d'architecture globale et détaillée. Ledit document sera accompagné des documents annexes suivants:
    a. un document annexe présentant le SMA (capteur et coffre-fort) ;
    b. un document annexe présentant la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs ;
    c. un document annexe présentant les plateformes SI et briques fournisseurs ;
    d. un document annexe présentant les processus et niveau de service (SLA) ;

Les dispositions relatives à chacun des documents listés ci-dessus, et en particulier le contenu attendu sont détaillés dans les sections qui suivent.

[E_AGR_DOS2] Hors le cas d'un nouvel opérateur qui n'aurait pas encore intégralement mis en place l'infrastructure et les processus, les différents documents doivent refléter la situation présente au moment du dépôt, en particulier PSSI et schéma directeur doivent correspondre à la version en vigueur.

L'attention de l'opérateur est appelée sur le fait que le non-respect de cette obligation **[E_AGR_DOS2]** est un motif de refus de la demande d'agrément.

[E_AGR_DOS3] Dans le cas où certaines sections de documents ne présenteraient que le prévisionnel, sans que les travaux soient finalisés, par un nouvel opérateur n'ayant pas encore mis en place toute son infrastructure et processus, il devra :

1. remettre dans le dossier de demande d'agrément le calendrier de finalisation de ceux-ci ;
2. communiquer à l'Autorité les éléments complémentaires conformément au calendrier communiqué ;
3. et soumettre ces éléments à l'analyse du certificateur à la certification suivante.

Ceci, sous réserve que les absences en question ne constituent pas une incomplétude du dossier obérant son instruction, ce qu'il revient à l'Autorité d'apprécier.

IV.2 Dispositions relatives au schéma directeur du système d'information

[E_AGR_DIR1] Le schéma directeur du système d'information suivra le plan détaillé ci-après :

1. stratégie d'entreprise à 3-5 ans ;
2. stratégie du système d'information ;
3. organisation de la fonction système d'information ;
4. ressources humaines de la fonction système d'information ;
5. ressources budgétaires ;
6. gouvernance SI.

Le document pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire.

Dans le cas où des documents en application correspondent au contenu demandé pour les chapitres mentionnés ci-dessus alors une matrice de correspondance entre le plan décrit ci-dessus et les sections précises et pagination du ou des documents est fourni par le candidat à l'agrément.

[E_AGR_DIR2] Le chapitre « stratégie d'entreprise » décrit les éléments suivants :

1. La date d'établissement du schéma directeur, la période couverte et les dates de mises à jour prévisionnelles sont précisées.
2. la stratégie de l'entreprise sur un horizon temporel de 3 à 5 ans en présentant contexte, ambition et positionnement ;
3. les enjeux métiers déclinant cette cible.

[E_AGR_DIR3] Le chapitre « stratégie du système d'information » décrit les éléments suivants :

1. Les principes directeurs IT couvrant tout le périmètre porté par le SI ;
2. les projets SI structurants répondant aux enjeux métiers, leur objectif détaillé, phasage éventuel et leur calendrier. La composante SSI dans chaque projet devra être explicitée.
3. Pour les projets lancés, une synthèse de l'avancement à date est jointe.

[E_AGR_DIR4] Le chapitre « organisation de la fonction système d'information » contient, a minima, les éléments suivants :

1. les différentes structures qui la composent, avec leurs missions précises ;
2. les éventuelles entités qui lui sont rattachées, avec leurs fonctions respectives et leurs implantations géographiques ;

[E_AGR_DIR5] Le chapitre « ressources humaines de la fonction système d'information » contient, a minima, les éléments suivants :

1. les effectifs internes et équivalent temps plein (ETP) correspondants par structures et missions de la fonction système d'information sont précisés, en distinguant a minima les fonctions exploitation, sécurité du système d'information, projets infrastructure, projets applicatifs & MCO, pilotage & stratégie ;
2. le cas échéant, les évolutions des effectifs prévues sur l'horizon temporel du schéma directeur ;
3. la politique d'externalisation applicable à la fonction système d'information ;
4. elle précise les métiers ou fonctions faisant appel à la sous-traitance ou à l'externalisation (notamment hébergement web, infogérance, sécurité, …) et les volumes (ETP) correspondants.

[E_AGR_DIR6] Le chapitre « Ressources budgétaires » contient, a minima, les éléments suivants :

1. le budget global SI prévisionnel annuel sur l'horizon temporel du schéma directeur ;
2. sa répartition prévisionnelle par grands domaines (fonction exploitation, sécurité du système d'information, projets infrastructure, projets applicatifs & MCO), par année sur la période couverte par le schéma directeur ;
3. sa répartition prévisionnelle annuelle sur l'horizon temporel du schéma directeur par projets SI structurants déclinant la stratégie SI.

[E_AGR_DIR7] Le chapitre « gouvernance SI » décrit les éléments suivants :

1. Les acteurs de la gouvernance SI, leurs rôles et responsabilités respectives.
2. La comitologie mise en place pour le pilotage du portefeuille des projets SI, incluant en particulier les projets structurants mentionnés au chapitre « stratégie du système d'information ».

IV.3 Dispositions relatives au document décrivant la politique de sécurité des systèmes d'information

[E_AGR_SSI1] La politique de sécurité des systèmes d'information (PSSI) suit le plan détaillé ci-après :

1. Politique, organisation, gouvernance ;
2. Ressources humaines ;
3. Gestion des biens ;
4. Intégration de la sécurité des systèmes d'information dans le cycle de vie des projets ;
5. Sécurité physique ;
6. Sécurité des réseaux ;
7. Architecture des systèmes d'information ;
8. Exploitation des systèmes d'information ;
9. Sécurité du poste de travail ;
10. Sécurité du développement des systèmes ;

11. Traitements des incidents ;
12. Continuité d'activité ;
13. Conformité, audit, contrôle

Le document pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire.

Dans le cas où des documents en application correspondent au contenu demandé pour les chapitres mentionnés ci-dessus alors une matrice de correspondance entre le plan décrit ci-dessus et les sections précises et pagination du ou des documents est fourni par le candidat à l'agrément.

[E_AGR_SSI2] Les déclinaisons techniques détaillées des éléments exigés par sa politique de sécurité sont fournies avec leur lien avec la PSSI y compris avec les procédures liées aux systèmes d'information ainsi que les moyens (organisationnels et techniques) de sécurisation et leur suivi dans le temps.

[E_AGR_SSI3] Le chapitre « Politique, organisation, gouvernance » décrit :

- La date de début d'application de la politique de sécurité des systèmes d'information ;
- La périodicité de mise à jour de la politique de sécurité des systèmes d'information ;
- Les orientations stratégiques ainsi que le niveau de réalisation des actions en découlant ;
- Le périmètre d'application de la politique de sécurité des systèmes d'information ;
- Les aspects légaux et réglementaires liés au périmètre d'application de la politique de sécurité ;
- L'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 ;
- La description des besoins de sécurité des domaines d'activité de l'opérateur, selon l'échelle de besoins présentée dans la partie précédente ;
- L'analyse des menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications ;
- Une description de l'organisation mise en place pour assurer la sécurité des systèmes d'information, ainsi que la sécurité physique des locaux ;
  L'existence des fonctions suivantes est indiquée ainsi que les informations demandées :
  - Responsable sécurité du système d'information : définition précise des responsabilités, degré de formalisation, nombre d'adjoints et rattachement hiérarchique ;
  - Autorité d'exploitation du système d'information (SI) (ou fonction équivalente) : définition précise des responsabilités, degré de formalisation et, le cas échéant, nature des responsabilités en matière de sécurité des systèmes d'information (SSI) ;
  - Juriste spécialisé en SSI : nombre et rattachement hiérarchique ;
  - Auditeurs internes en SSI : nombre et rattachement hiérarchique ;
  - Fonction de contrôle interne en SSI : nombre et rattachement hiérarchique ;
  - Fonction support en SSI : nombre et rattachement hiérarchique ;
  - Fonction opérationnelle en SSI : nombre et rattachement hiérarchique) ;
  - Fonction de conception en SSI : nombre et rattachement hiérarchique ;
- Les modèles de tableaux de bord SSI ;

[E_AGR_SSI4] Le chapitre « Ressources Humaines » décrit la proportion du personnel de l'opérateur ayant été sensibilisé ou formé à la SSI dans les chaînes SI et SSI et parmi les utilisateurs. Il précise également s'il existe une gestion et un suivi régulier de la compétence de chacun.

[E_AGR_SSI5] Le chapitre « Gestion des biens » décrit les procédures et mécanismes mis en place afin de protéger les données traitées par l'opérateur, notamment :

- Les données nominatives et personnelles de ses clients ;
- Les données et statistiques de jeu ou de certains joueurs dont la connaissance pourrait avantager un joueur ;
- Les données de jeu " secrètes " (par exemple les cartes des autres joueurs, ou celles qui n'ont pas été retournées lors d'une partie de poker).
- Les modalités d'identification et de classification des composants sensibles (y compris les données) et la méthodologie y afférente ;

[E_AGR_SSI6] Le chapitre « Intégration de la SSI dans le cycle de vie des projets » décrit :

- La gestion de la sécurité mis en œuvre par l'opérateur à chaque étape du cycle de développement des systèmes, dans les phases de définition, de développement, d'exploitation et d'utilisation, puis de maintenance et d'évolution. L'opérateur expose sa politique en cas de vulnérabilité identifiée et d'absence de correctifs ;
- La procédure de recette SSI relative aux projets de systèmes d'information avant leur mise en service et précise la proportion des systèmes d'information ayant effectivement fait l'objet d'une telle recette ;
- Les modalités de mise en œuvre de tout examen formalisé d'impact sur la sécurité d'un SI ou sur la mise en exploitation d'un nouveau composant (modèle de serveur, système d'exploitation, application, données, etc.) ;
- Les études de risques réalisées. La méthodologie est précisée ;
- Les contrôles exercés auprès des sous-traitants afin d'assurer un maintien du niveau de sécurité de ses plates-formes et systèmes d'information.

[E_AGR_SSI7] Le chapitre « Sécurité physique » décrit :

- Les procédures de vérification des candidats postulant à un poste sensible ;
- Les procédures de gestion des conflits d'intérêt ;
- Les procédures de mises en sécurité de l'information lors du départ de salariés de la société ;
- Les mesures de sécurité concernant son personnel ;
- Les moyens mis en œuvre aux fins de protection des locaux techniques ;
- Les moyens mis en œuvre de protection incendie ;
- La politique de redondance en alimentation électrique ;
- La politique de surveillance H24 de ses sites en exploitation ;
- La politique de gestion des accès physiques ;

[E_AGR_SSI8] Le chapitre « Sécurité des réseaux » décrit :

1. Les centres d'exploitation et de supervision informatiques et réseau : leur localisation, les applications hébergés et le personnel affecté ;
2. Les centres d'hébergement : leur localisation et le type d'hébergement ;

3. Les centres d'interconnexion : les types d'interconnexion utilisés ;
4. Les centres opérationnels ;
    a. Pour les plates-formes de jeux, le frontal, et l'ensemble des systèmes d'information afférents à ceux-ci, le candidat à l'agrément précise :
    b. La ou les fonctions assurées ;
    c. Le type de données traitées ;
    d. L'entreprise ou l'autorité responsable de son exploitation ;
    e. Le fournisseur d'accès ;
    f. L'hébergeur.
5. Le cloisonnement du réseau appliqué
6. La politique de filtrage réseau et la description les règles de filtrage en termes de liste blanche.
7. Les typologies de cloisonnement réseau employés (filtrage IP, filtrage applicatif, VLAN, 802. 1X, NAP/ NAC, etc.).
8. Les mécanismes de sécurité mis en œuvre 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 ;
9. Les mesures techniques et organisationnelles prises en termes de résilience réseau de ses systèmes d'information, notamment au regard de la lutte contre les attaques en déni de service (distribuées ou non, par épuisement de bande passante, ou encore de ressources système) au niveau des plates-formes de jeux et du frontal : L'opérateur décrit notamment les procédés techniques mis en œuvre (équilibrage de charge, ajustement des TTL DNS, ré-adressage IP dynamique des plates-formes, et du frontal) et les mesures organisationnelles associées (remontée d'alerte en cas d'attaque, protocole d'accord avec les FAI pour la lutte contre les DDOS, etc.).

[E_AGR_SSI9] Le chapitre « Architecture des SI » décrit l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux au sein de ses plates-formes de jeux et du frontal : ces flux concernent les administrateurs faisant partie du personnel de l'opérateur tels les exploitants par exemple, les administrateurs externes tels ceux qui assurent la télémaintenance des matériels, etc.

[E_AGR_SSI10] Le chapitre « Exploitation des SI » décrit :

1. Les mécanismes d'identification et d'authentification des joueurs ;
2. Les mécanismes de contrôle d'accès des joueurs : détails des éventuels profils de joueurs et mécanismes de cloisonnement des droits ;
3. Les procédés cryptographiques permettant de garantir l'authentification des composants, la confidentialité et l'authenticité des communications suivantes :
    a. Les communications entre l'opérateur et l'ANJ ;
    b. Les communications réseaux entre joueurs et l'opérateur ;
    c. Les communications réseaux entre les modules au sein du frontal ;
4. La description de l'ensemble des mécanismes et mesures mis en œuvre pour garantir la confidentialité et l'intégrité des flux au sein de ses plates-formes de jeux et du frontal : ces flux concernent les administrateurs faisant partie du personnel de l'opérateur tels les exploitants par exemple, les administrateurs externes tels ceux qui assurent la télémaintenance des matériels, etc ;

5. La description des mécanismes d'accès aux fonctions d'administration de la plateforme de jeu et du frontal y compris ;
6. Les mesures mises en œuvre lui permettant de garantir un haut niveau de sécurité dans la gestion des secrets d'authentification (notamment, robustesse des mots de passe, changement périodique, authentification forte) pour les personnels exploitant de l'opérateur ;
7. Le processus d'application des correctifs, et notamment en cas de régression constatée ;
8. Les procédures techniques permettant un retour en arrière dans le cas où un correctif provoquerait une éventuelle régression ;
9. La description de la journalisation des alertes ainsi que leur durée de conservation.

[E_AGR_SSI11] Le chapitre « Sécurité du poste de travail » décrit :

1. La procédure de fourniture et la politique de gestion des postes de travail ;
2. La procédure formalisée de configuration des postes de travail ;
3. Les mécanismes de protection physique contre le vol ;
4. La gestion des privilèges sur les postes de travail ;
5. La gestion des accès en nomadisme tel que le télétravail ;
6. La gestion des supports de stockage amovibles.

[E_AGR_SSI12] Le chapitre « Sécurité du développement des systèmes » décrit :

1. Les moyens que l'opérateur met en œuvre pour protéger les données à caractère personnel et la vie privée des joueurs ;
2. Les mesures de contrôle et méthodes d'évaluation de ses développements à chaque étape d'un projet de développement ;
3. Le référentiel de développement sécurisé pour les projets dont l'opérateur assure le développement ;

L'opérateur communiquera les contrats conclus avec ses prestataires relatifs à la mise en place d'un référentiel de développement sécurisé pour les projets dont il externalise la prise en charge.

[E_AGR_SSI13] Le chapitre « Traitement des incidents » décrit :

1. Le mode de fonctionnement du centre opérationnel chargé de la SSI de l'opérateur. Il précise notamment le rattachement hiérarchique, le régime de veille et l'effectif de permanence. A défaut, il précise les modalités de veille et de déclenchement des alertes ;
2. Les procédures mises en place en vue de traiter les cas d'incident et de détection de fraude. Elle précise le niveau de diffusion de ces documents ainsi que les modalités d'alerte prévues.
3. L'état des incidents de SSI ou des fraudes que l'opérateur aurait pu constater. Il en précise les occurrences (notamment l'identification des sources d'entrée et du niveau) et la gestion qui en a été faite ;
4. Les solutions mises en œuvre pour éviter ou détecter, le cas échéant, les attaques et intrusions sur ses systèmes d'information.

[E_AGR_SSI14] Le chapitre « Continuité d'activité » décrit :

1. Le service d'archivage en vue d'assurer la conservation de l'ensemble de ses données de traitement, et en particulier celles stockées dans le coffre-fort du frontal. L'opérateur précise le type de support et le format de la sauvegarde,

2. Les mécanismes d'archivage ainsi que les moyens sécurisés de protection des archives que l'opérateur est capable de mettre en œuvre ;
3. Les modalités de son plan de sauvegarde. L'opérateur précise en particulier les modalités et les délais de restauration d'une sauvegarde à la suite d'un incident ainsi que le ou les lieux de stockage des sauvegardes et les mesures de sécurité appliquées à ce(s) lieu(x).
4. Les plans de continuité d'activité et plans de reprise d'activité que l'opérateur a pu élaborer dans le cadre de son activité et les modalités qu'elle prévoit pour les adapter au contexte du frontal.

[E_AGR_SSI15] Le chapitre « Conformité, audit, inspection, contrôle » décrit la nature, la périodicité, les acteurs et la méthodologie des audits SSI réalisés sur les systèmes d'information et les applications. L'opérateur en communique les comptes rendus et les principales recommandations. Il précise les modalités de décision des mesures correctrices, et celles de leur mise en œuvre et du contrôle de leur bonne exécution. Il indique la proportion des mesures réellement appliquées.

IV.4 Dispositions relatives au document chapeau décrivant l'architecture globale et détaillée

[E_AGR_ARC1] le document décrivant l'architecture globale et détaillée du SI suivra le plan détaillé ci-après :

1. La description générale de la plateforme du système d'information :
   a. L'ensemble des composants mis en œuvre dans le SI et, pour chacun, la ou les fonctions qu'il assure ;
   b. Le type d'hébergement de chaque composant ;
   c. L'ensemble des interconnexions entre composants et, pour chacune, en décrire la finalité de telle sorte que soit défini comment les composants collaborent pour assurer le fonctionnement global du système ;
   d. L'entreprise ou l'autorité responsable de l'exploitation de chaque composant.
   e. Les centres d'exploitation et de supervision informatiques et réseau en précisant la ou leurs localisations, les modes de fonctionnement ainsi qu'une estimation du volume d'ETP mis en œuvre ;
   f. Les centres d'hébergement (localisation, type d'hébergement) ;
   g. Les centres d'interconnexion (types, fournisseurs) ;
   h. Les centres opérationnels (notamment centre de sécurité, centre service client, centre de service pour le développement, …) ;
   i. Les fournisseurs d'accès réseau pour chaque liaison sortant/entrant dans le SI ;
   j. Il sera précisé également la liste des principaux logiciels mis en œuvre dans le cadre des activités liées aux agréments ou activités visées.
2. La présentation globale de l'architecture avec schémas réseau logique et physique, schémas applicatifs, la cartographie du réseau ;
3. Les dispositions relatives au document annexe présentant le SMA (voir chapitre ci-dessous) ;
4. Les dispositions relatives au document annexe présentant la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs (voir chapitre ci-dessous) ;

5. Les dispositions relatives au document annexe présentant les plateformes SI et briques fournisseurs (voir chapitre ci-dessous).

Le document pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire.

Dans le cas où des documents en application correspondent au contenu demandé pour les chapitres mentionnés ci-dessus alors une matrice de correspondance entre le plan décrit ci-dessus et les sections précises et pagination du ou des documents est fourni par le candidat à l'agrément.

IV.5 Dispositions relatives au document annexe présentant le SMA

[E_AGR_SMA1] Au moment du dépôt du dossier de demande d'agrément, le SMA n'est pas nécessairement en fonctionnement. L'entreprise doit néanmoins être en mesure de présenter sa stratégie détaillée de mise en œuvre prévue pour celui-ci dans le cadre de la collecte et la sauvegarde de la totalité des données qu'il sert à recueillir.

[E_AGR_SMA2] Pour se faire, l'entreprise fournit un document décrivant le SMA. Ce document suivra le plan détaillé ci-après et pourra contenir des sections supplémentaires si l'entreprise le juge nécessaire :

1. Description générale du SMA ;
2. Description détaillée du capteur pour la génération des traces ;
3. Description détaillée du coffre-fort pour le stockage sécurisé des traces ;
4. Description des fonctions d'accès aux traces recueillies par le SMA ;
5. Dispositions particulières relatives au frontal de la plateforme de jeu ;
6. Annexes techniques.

Le document pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire.

Dans le cas où des documents en application correspondent au contenu demandé pour les chapitres mentionnés ci-dessus alors une matrice de correspondance entre le plan décrit ci-dessus et les sections précises et pagination du ou des documents est fourni par le candidat à l'agrément.

[E_AGR_SMA3] Le chapitre « Description générale du SMA (coffre-fort et capteur) » contient les sections suivantes :

1. La stratégie globale employée : il s'agit de présenter le fonctionnement général mis en œuvre ou envisagé, s'agissant de la collecte et le stockage sécurisé des traces ;

2. L'architecture générale, présentant les différents composants du SMA, leur rôle, leur positionnement par rapport à la plateforme de jeu ainsi que leurs interactions avec la plateforme de jeu, les joueurs et tout autre éventuel SI ;

[E_AGR_SMA4] Le chapitre « Description détaillée du **capteur** » contient les sections suivantes :

<u>Cadrage global :</u>

1. La stratégie détaillée employée pour le capteur, relative à la génération des traces. Il s'agit de présenter la solution de capteur retenue et le fonctionnement associé vis-à-vis des données échangées dont les traces sont exigées (exemple : choix d'un capteur fonctionnant en coupure du flux applicatif entre le joueur et la plateforme de jeu concernant les requêtes émises par le joueur) ;
2. La stratégie employée vis-à-vis de la très haute disponibilité demandée, précisant les mesures mises en œuvre en cas d'indisponibilité ou dysfonctionnement du capteur ;
3. L'analyse de risques conduite concernant le capteur ;
4. La politique de sécurité applicable dont la description détaillée des mesures de sécurisation du capteur ;
5. Le capteur au sens logique peut être constitué de plusieurs capteurs physiques, potentiellement de types différents. La description demandée devra être déclinée pour chaque type de capteurs physiques mis en œuvre.

Réalisation :

6. L'identité et les coordonnées du (ou des) prestataire(s) réalisant le développement, la maintenance du capteur ou du fournisseur de la solution de capteur retenue ;
7. Les spécifications détaillées du capteur dont :
    a) L'architecture fonctionnelle et technique (applicative et réseau) détaillée du capteur ;
    b) Les spécifications des interfaces et le cas échéant des fonctions de « proxy » (du flux applicatif) implémentées par le du capteur ;
    c) La description des différents flux (i.e. type de données, protocoles) transitant par le capteur ;
    d) La description détaillée des mécanismes mis en œuvre relatifs à l'acquittement (positif ou négatif) des traces par la plateforme de jeux et par le coffre-fort ;
    e) La description détaillée des mécanismes mis en œuvre relatifs au traitement par lot des traces, s'agissant de la communication des traces au coffre-fort ;
    f) La description détaillée des mécanismes d'authentification et de confidentialité mis en place dans le cadre des échanges de données :
        - Entre le joueur et le capteur ;
        - Entre le capteur et la plateforme de jeu ;
8. Lorsque le SMA est d'ores et déjà mis en œuvre, la liste et les résultats des tests d'audits effectués ;

Hébergement :

9. La localisation physique du capteur ;
10. Les modalités d'hébergement du capteur ;

11. L'identité et les coordonnées du prestataire réalisant l'hébergement du capteur ;
12. La production du ou des contrats d'hébergement ;
13. Les documents d'administration et d'exploitation du capteur ;
14. Les procédures mises en place notamment en termes de protection contre les accès non autorisés ;

[E_AGR_SMA5] Le chapitre « Description détaillée du **coffre-fort** » contient les sections suivantes :

Cadrage global :

1. La stratégie détaillée employée pour le stockage sécurisé des traces. Il s'agit de présenter la solution de coffre-fort retenue et le fonctionnement associé ;
2. La stratégie employée vis-à-vis de la très haute disponibilité demandée, précisant les mesures mises en œuvre en cas d'indisponibilité du coffre-fort ;
3. L'analyse de risques conduite concernant le coffre-fort ;
4. La politique de sécurité applicable dont la description détaillée des mesures de sécurisation du coffre-fort ;

Réalisation :

5. L'identité et les coordonnées du (ou des) prestataire(s) réalisant le développement, la maintenance du coffre-fort ou du fournisseur de la solution de coffre-fort retenue ;
6. Les spécifications détaillées du coffre-fort dont :
    a) L'architecture fonctionnelle et technique détaillée du coffre-fort ;
    b) La description détaillée des mécanismes d'authentification et de confidentialité mis en place concernant l'échange de données :
        - Entre le capteur et le coffre-fort ;
        - Entre le coffre-fort et le système d'information de l'ANJ ;
    c) La description des différents algorithmes employés pour le stockage sécurisé des traces (exemple : chaînage des traces) ;
7. Lorsque le SMA est d'ores et déjà mis en œuvre, la liste et les résultats des rapports de tests effectués ;

Hébergement :

8. La localisation physique du coffre-fort (celui-ci devant être hébergé en France métropolitaine conformément à l'article 31 de la loi n°2010-476 du 12 mai 2010) ;
9. Les modalités d'hébergement du coffre-fort ;
10. L'identité et les coordonnées du prestataire réalisant l'hébergement du coffre-fort ;
11. La production du ou des contrats d'hébergement ;

12. Les documents d'administration et d'exploitation du coffre-fort dont en particulier :
    a) La spécification précise du déroulement de la cérémonie envisagée d'initialisation du coffre et de remise des clés nécessaire ;
    b) La spécification et rôle des bi-clés utilisées ;
    c) La description détaillée des mécanismes d'authentification des personnes physiques au coffre ;
    d) La description détaillée des fonctions d'administration et de gestion des utilisateurs du coffre-fort ;
13. Les procédures mises en place notamment en termes de protection contre les accès non autorisés ;

[E_AGR_SMA6] Le chapitre « Description des fonctions d'accès aux traces recueillies par le SMA » contient les sections suivantes :

1. La description détaillée de l'outil de consultation et de collecte à distance des fichiers de traces, dont :
    a) Les spécifications détaillées fonctionnelles et techniques ;
    b) Lorsque le SMA est d'ores et déjà mis en œuvre, les rapports des tests effectués ;
2. La description détaillée de l'outil de validation et d'extraction des fichiers de traces, dont :
    a) Les spécifications détaillées fonctionnelles et techniques ;
    b) Lorsque le SMA est d'ores et déjà mis en œuvre, les rapports des tests effectués ;

[E_AGR_SMA7] Le chapitre « Annexes techniques » contient :

1. Lorsque le SMA est d'ores et déjà mis en œuvre:
    a) Le code source du capteur ;

    L'Autorité se réserve le droit de demander en outre, lors de l'instruction de l'agrément ou ultérieurement :

    b) Le code source du coffre-fort ;
    c) Le code source de l'outil de consultation et de collecte à distance des fichiers de traces ;
    d) Le code source de l'outil de validation et d'extraction des fichiers de traces ;
2. Une copie du certificat de sécurité a minima de premier niveau (CSPN) du coffre-fort du SMA (ou du calendrier d'obtention accompagné d'une note du centre d'évaluation ou du centre de certification attestant que la procédure de certification a été engagée) ;
    a) La CSPN devra à minimum prendre en compte les éléments suivants, au niveau des menaces :
        1. Le dépôt ou l'injection d'enregistrements non autorisés ;

2. L'altération d'enregistrements ;
3. Le vol de données ;
4. Le déni de service ;

b) La CSPN devra à minimum prendre en compte les éléments suivants, au niveau des fonctions de sécurité :

1. L'authentification forte des utilisateurs et administrateurs ;
2. Le chiffrement, la signature et l'horodatage des évènements ;
3. Le chaînage des évènements.

[E_AGR_SMA8] Avant de débuter son activité, l'opérateur agréé déclare à l'ANJ que son SMA est en mode fonctionnement.

IV.6 Dispositions relatives au document annexe présentant la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs

[E_AGR_GCC1] le document décrit la brique de gestion des comptes joueurs et des canaux d'accès offerts aux joueurs suivra le plan détaillé ci-après :

1. Modalités techniques d'accès et d'inscription au site de tout joueur ;
2. Moyens techniques permettant de s'assurer de l'identité de chaque nouveau joueur, de son âge, de son adresse et de l'identification du compte de paiement sur lequel sont reversés ses avoirs ;
3. Modalités techniques d'encaissement et de paiement, à partir de son site, des mises et des gains ;

Le document pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire.

Dans le cas où des documents en application correspondent au contenu demandé pour les chapitres mentionnés ci-dessus alors une matrice de correspondance entre le plan décrit ci-dessus et les sections précises et pagination du ou des documents est fourni par le candidat à l'agrément.

[E_AGR_GCC2] Le candidat justifie de l'obtention au moins d'un nom de domaine de premier niveau comportant la terminaison ". fr " par la production d'un certificat d'enregistrement. Elle déclare, le cas échéant, tous les autres noms de domaine de premier niveau comportant la terminaison ". fr " qu'elle entend exploiter pour l'accès à son site de jeux en ligne et fournit les pièces justifiant des enregistrements correspondants.

[E_AGR_GCC3] Le candidat précise les caractéristiques de son site suivantes :

1. Plan du site ;
2. Marques ;
3. Caractéristiques techniques du site, nom de domaine ;

Le chapitre « Dispositions particulières relatives au frontal de la plateforme de jeu » contient les sections suivantes :

1. La description détaillée du site « .fr » mis en place :
    a. Hébergeur ;
    b. Localisation ;
    c. Code source ;
    d. Politique de sécurité ;
    e. Analyse de risques ;
    f. Procédures d'administration, d'exploitation et de sécurisation mises en place ;
2. La description détaillée des fonctions de redirection des connexions de joueurs ;

[E_AGR_GCC4] Le candidat précise les canaux de jeux prévus, qui permettront aux clients de jouer : clients lourds, applications natives sur smartphone complètes ou redirigeant vers un site web. Le candidat précisera si le site web offre des fonctionnalités de jeu. Il précisera le calendrier prévisionnel d'ouverture de ces différents canaux.

IV.7 Dispositions relatives au document annexe présentant les plateformes SI et briques fournisseurs

[E_AGR_PLA1] le document annexe décrivant la plateforme SI de l'Entreprise suivra, pour chacun des composants identifiés dans le cadre de l'exigence **[E_AGR_ARC1]** décrite au paragraphe IV.4 ***Dispositions relatives au document chapeau décrivant l'architecture globale et détaillée***, le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire :

1. Un descriptif d'architecture détaillé de chacun des composants du SI listés dans le document chapeau conformément à l'exigence **[E_AGR_ARC1]** ;
2. Un descriptif détaillé de l'architecture réseau et des flux associés.

Le document pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire.

Dans le cas où des documents en application correspondent au contenu demandé pour les chapitres mentionnés ci-dessus, une matrice de correspondance entre le plan décrit ci-dessus et les sections précises et pagination du ou des documents est fourni par le candidat à l'agrément.

[E_AGR_PLA2] Pour chacune des sections, le descriptif précisera :

1. les composants ou parties de composants qui sont sous-traités à des fournisseurs externes (ceci vaut également dans le cas où l'ensemble de la plateforme est sous-traitée) ;
2. Il sera précisé systématiquement les raisons de cette sous-traitance ;
3. seront décrits les accords contractuels encadrant ces sous-traitances et en particulier les engagements en matière de niveau de service, de responsabilités et de sécurité.

[E_AGR_PLA3] Pour chacune des sections, il sera pris en compte au même titre que les composants déjà en production, les briques logicielles ou éléments d'infrastructures qui seraient en chantier ou

non encore opérationnels, comme s'ils étaient déjà en production pour le périmètre mis en œuvre concernant les agréments ou les activités visées.

[E_AGR_PLA4] Les chapitres « descriptif d'architecture détaillé », rédigés pour chacun des composants listés décrivent :

1. La description détaillée du composant, mettant en évidence chacune de ses constituantes physique et logique avec pour chaque :
    a. la ou les fonctions assurées ;
    b. le type de données traitées ;
    c. l'entreprise ou l'autorité d'exploitation désignée ;
    d. le cas échéant, les moyens de chiffrement mis en œuvre ;
    e. l'importance de sa fonction (de " outil facilitant le travail " à " outil indispensable ") ;
    f. l'importance de sa disponibilité (de " aucun effet " à " effet bloquant " en cas d'arrêt total ou partiel du système) ;
    g. l'importance de l'intégrité des données (de " aucun effet " à " effet bloquant " en cas de modification de données) ;
    h. l'importance de la confidentialité des données (de " aucun effet " à " effet bloquant " en cas de divulgation de données) ;
    i. la durée de vie prévue.
2. une description technique détaillée du réseaux , dans la description duquel seront précisés les éléments relatifs à la segmentation et aux filtrages. Figureront les descriptions des réseaux opérationnels, mais également celles des réseaux supportant l'administration et la supervision.
    a. un schéma technique du réseau ;
    b. la liste des différents flux associés ;
    c. la liste des zones de sensibilités différentes
        i. Typologie (Internet ou réseau dédié…)
        ii. Sensibilité ;
    d. la liste descriptive des interconnexions de ces zones (rôle et finalité) ;
    e. il sera listé l'ensemble des technologies mises en œuvre.
    f. la liste des liens vers l'extérieur (lignes dédiées, interconnexions de réseaux …) et les accès distants possibles depuis l'extérieur avec pour chacun un descriptif précis des technologies protocoles et mesures de sécurité mis en œuvre ;

IV.8 Dispositions relatives au document annexe présentant les processus et niveaux de service (SLA)

[E_AGR_PRO1] Le document annexe présentant les processus et niveaux de service suivra le plan en deux chapitres suivants :

1. Procédures d'administration et d'exploitation
2. Niveaux de service (SLA)

Le document pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire.

Dans le cas où des documents en application correspondent au contenu demandé pour les chapitres mentionnés ci-dessus alors une matrice de correspondance entre le plan décrit ci-dessus et les sections précises et pagination du ou des documents est fourni par le candidat à l'agrément.

[E_AGR_PRO2] Le chapitre « procédures d'administration et d'exploitation » décrit les éléments suivants :

3. la liste des procédures d'exploitation utilisées, qui sera structurée par thématique. La thématique sécurité devra être explicitée. Elle devra couvrir notamment :
    a. Procédures de gestion des journaux ;
    b. Procédures de gestion des alertes ;
    c. Procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.) ;
    d. Procédures de gestion des composants à mise à jour fréquente (anti-virus, systèmes de détection d'intrusion le cas échéant) ;
    e. Procédures de mise à jour en cas d'édition d'un correctif de sécurité critique ;
    f. Procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent ;
    g. Procédures d'exploitation des composants du SI (serveurs, routeurs) ;
    h. Procédures d'exploitation des comptes et mots de passe ;
    i. Procédures de gestion des composants infogérés ;
    j. Procédures relatives à la sécurité physique (gardiennage, etc.) ;
    k. Procédures de gestion des sauvegardes et des restaurations ;
    l. Procédures en cas d'incident de sécurité ;
    m. Procédures pour la télé-administration ;
    n. Procédures de reprise et continuité d'activité (PRA et PCA).
4. la documentation décrivant les procédures listées supra sera communiquée. Afin de faciliter l'analyse, la liste supra inclura la référence précise (document, section, page) de chaque procédure dans la documentation.

[E_AGR_PRO3] Le chapitre « niveaux de service et SLA» décrit les éléments suivants :

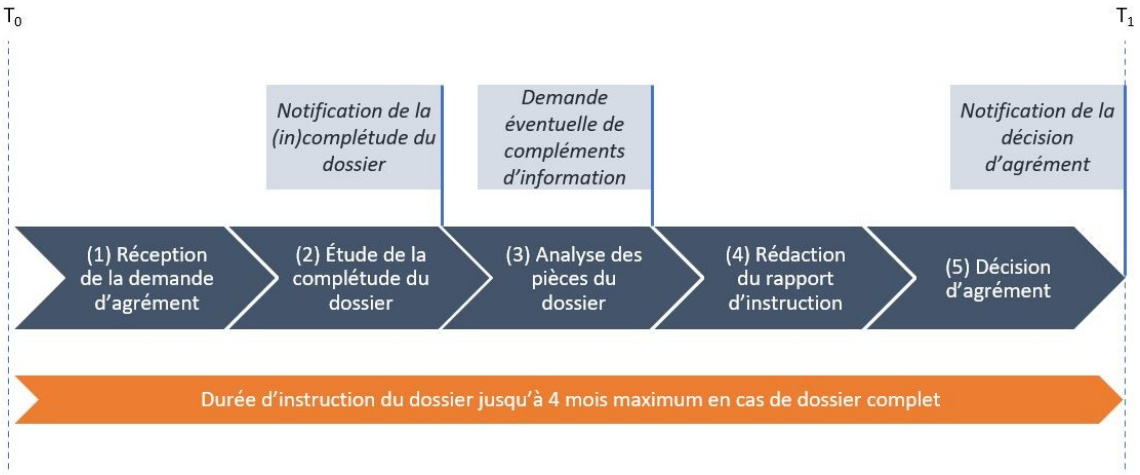
1. La liste des niveaux de service (SLA) mis en place tant en interne qu'en externe vis-à-vis des fournisseurs, classés par typologie (réseau, sécurité, disponibilité applicative, …).

2. Pour chaque SLA, la liste précisera la description de l'indicateur, la méthode de calcul, son ou ses seuils, son caractère interne ou externe, le délai maximum d'intervention en cas de non-respect.

IV.9 Dispositions relatives au formulaire du volet SI de l'agrément rempli

V Procédure d'agrément d'un opérateur de jeux

Le schéma ci-dessous présente les différentes étapes de l'instruction d'une demande d'agrément.



V.1 Contenu du dossier

Le dossier de demande d'agrément d'un opérateur de jeu déposé auprès de l'ANJ, dans un format dématérialisé, comprend les pièces définies dans l'exigence **[E_AGR_PER2]** (cf IV).

[E_AGR_PDA1] Il appartient à l'opérateur de jeux de s'assurer, le cas échéant, que l'entreprise qui met à sa disposition une plateforme ou un logiciel communique à l'ANJ l'ensemble des éléments nécessaires à l'instruction de la demande.

[E_AGR_PDA2] L'absence de pièce exigée dans un dossier de demande d'agrément devra être dûment justifiée. Dans le cas contraire, le dossier sera considéré comme incomplet.

[R_AGR_PDA3] En cas de doute, il est recommandé de consulter l'ANJ préalablement au dépôt de toute demande d'agrément afin d'éviter la suspension de l'instruction du dossier, pour des raisons d'incomplétude du dossier notamment.

V.2 Modalités de transmission des livrables

[E_AGR_TRF1] Le dossier de demande d'agrément est à remettre à l'ANJ par le biais du canal d'échange sécurisé mis à disposition des candidats à l'agrément. Un échange préalable est requis

pour ce faire où le candidat précisera les noms, prénoms et emails de ses agents habilités à déposer tout ou partie du dossier.

S'agissant du SMA, lorsqu'il est déjà mis en place, l'envoi des codes sources sur support physique de type clé USB reste toutefois envisageable exceptionnellement, auquel cas, les codes sources devront être chiffrés et transmis selon la procédure que l'ANJ aura indiquée à l'opérateur.

V.3 Instruction de la demande

L'ANJ dispose d'un délai de deux mois pour instruire la demande d'agrément.

Lorsque la demande d'agrément est formée par un opérateur de jeux ou de paris en ligne, le silence gardé pendant quatre mois par l'ANJ sur cette demande vaut décision de rejet (art. 8 du décret n° 2010-482 du 12 mai 2010 modifié)

Lorsque le dossier de demande n'est pas complet, l' Autorité nationale des jeux adresse à l'entreprise candidate un courrier lui demandant d'y remédier dans un délai qui ne peut être inférieur à quinze jours. L'instruction est suspendue pendant ce délai. Si, à l'expiration du délai imparti, les informations ou pièces demandées ne sont pas parvenues à l'Autorité, la demande d'agrément est rejetée. Au cours de l'instruction, l'entreprise candidate est tenue de fournir, à la requête de l'Autorité nationale des jeux, toute information légalement justifiée et de nature à éclairer cette dernière sur des éléments contenus dans le dossier déposé.

Les décisions relatives à l'agrément sont notifiées à l'opérateur et publiées sur le site de l'ANJ.

VI Régime de l'agrément

VI.1 Cycle de vie

[E_AGR_SUA1] L'opérateur de jeu nouvellement agréé devra déposer un dossier de certification à 6 mois du SMA lors de sa mise en œuvre initiale, conformément aux exigences techniques volumes 3 et 5.

[E_AGR_SUA2] L'opérateur agréé devra, pour tout jeu qu'il souhaite offrir, déposer un dossier d'homologation logicielle, conformément aux exigences techniques volume 2 et obtenir une décision favorable avant la fourniture du service aux joueurs.

[E_AGR_SUA3] L'opérateur agréé devra ouvrir un service de jeu au plus tard un an après l'obtention de l'agrément, sauf accord explicite contraire formalisé avec l'Autorité.

[E_AGR_SUA4] l'opérateur agréé est tenu d'assurer et maintenir la sécurité et la robustesse de son système d'information dans l'ensemble de ses composantes, conformément aux exigences techniques dans leur ensemble. Il est donc attendu de l'opérateur qu'il mette en œuvre l'ensemble des mesures permettant de répondre à cet objectif, en termes de mises à jour techniques, de structures et processus organisationnels et de mécanismes de contrôle adaptés.

[E_AGR_SUA5] L'opérateur agréé devra chaque année, à la date anniversaire d'obtention de son agrément, déposer auprès de l'autorité un dossier de certification conformément aux exigences techniques volume 5.

VII ANNEXES

VII.1 Article 12 renouvellement d'agrément

12.2.2. Informations relatives à l'architecture du système d'information.

Le demandeur fournit à l'ARJEL les éléments suivants :

a) Une description actualisée des éléments relatifs à la présentation générale de l'entreprise et de ses systèmes d'information, tels que prévus à l'article 11.4 du présent cahier des charges, en termes de :

-politique et organisation des systèmes d'information (11.4.1) ;

-description des systèmes d'information (11.4.2) ;

-ressources humaines dédiées à la sécurité informatique (11.4.3) ;

-pilotage des systèmes d'information (11.4.4) ;

b) Le dossier de définitions prévu à l'article 11.5.2.1. du présent cahier des charges ainsi qu'à l'article 5.7.3. a du dossier des exigences techniques (DET) ;

c) Une attestation de l'ANSSI indiquant que le coffre-fort a fait l'objet d'un rapport de maintenance, dans le cadre de la procédure de continuité d'assurance de la certification de sécurité de premier niveau (CSPN), ou bien d'une réévaluation CSPN ;

d) Le rapport d'analyse des vulnérabilités de la plate-forme prévu à l'article 11.3.2. du présent cahier des charges, constitué d'un rapport de type " audit intrusif ", dont l'objectif est de rechercher ainsi qu'exploiter les vulnérabilités d'une plate-forme, et les fiches d'anomalies associées, récapitulant les vulnérabilités identifiées ;

e) La liste des logiciels de jeu déployés sur la plate-forme, ainsi que les numéros des homologations associées et prévues à l'article 11.3.1 du présent cahier des charges.

12.3. Pièces exigées uniquement en cas de modification non portée à la connaissance de l'ARJEL

Les pièces énumérées aux articles 12.3.1 à 12.3.6 sont produites par le demandeur si une modification les concernant est intervenue et n'a pas été portée à la connaissance de l'ARJEL soit depuis la délivrance de l'agrément, soit depuis la dernière certification, soit depuis la dernière information faite aux services de l'ARJEL.

L'absence de modification est attestée par une déclaration de l'opérateur.