AUTORITÉ NATIONALE DES JEUX

RÉPUBLIQUE FRANÇAISE

EXIGENCES TECHNIQUES RELATIVES A L'HOMOLOGATION DES LOGICIELS DE JEUX ET DE PARIS

Résumé

Conformément à l'article 34 de la Loi n°2010-476 du 12 mai 2010, l'ANJ homologue les logiciels de jeux et de paris utilisés par les opérateurs agréés ou titulaires de droits exclusifs.

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

Table des matières

I Présentation générale 4

I.1 Rappel des obligations légales et réglementaires 4

I.2 Présentation et objectifs du document 5

I.3 Glossaire 6

I.4 Identification des exigences et recommandations dans le document 9

II Champ d'application de l'homologation du logiciel de jeu 10

III Périmètre de l'homologation d'un logiciel de jeu 11

IV Travaux préalables au dépôt de la demande d'homologation 13

IV.1 Dispositions communes aux différents audits 13

IV.1.1 Réalisation des audits 13

IV.1.2 Non-conformités et anomalies de sécurité 14

IV.1.3 Plan de remédiation 15

IV.2 Dispositions relatives à l'audit de la sécurité du logiciel de jeu ou du composant visé par l'homologation 16

IV.3 Dispositions relatives à l'audit de la qualité et de la sécurité du générateur de nombres aléatoires 17

IV.4 Dispositions relatives à l'audit de la conformité de l'implémentation des fonctions métier 19

V Procédure d'homologation du logiciel de jeu 22

V.1 Contenu du dossier 22

V.1.1 Cas de l'homologation d'un jeu en ligne 22

V.1.2 Cas de l'homologation d'un dispositif GNA 23

V.1.3 Cas de l'homologation d'un moteur de jeu 23

V.1.4 Cas de l'homologation d'un totalisateur pour les jeux à caractère mutuel 24

V.1.5 Cas de l'homologation d'un logiciel de jeu en point de vente ou sur borne 24

V.1.6 Cas de l'homologation d'un logiciel d'impression de tickets de jeu de grattage 25

V.1.7 Dispositions communes 26

V.2 Modalités de transmission des livrables 26

V.3 Instruction de la demande 26

VI Exigences relatives au cycle de vie des logiciels de jeux homologués 27

VI.1 Cycle de vie 27

VI.2 Liens entre homologations logicielles et certification annuelle 27
VII ANNEXES..... 29
VII.1 Annexe n°1 – Exemples de scenarii relatifs à l'homologation d'un logiciel 29
VII.2 Annexe n°2 – Types de prestations d'audit attendues..... 39
VII.2.1 Test d'intrusion..... 39
VII.2.2 Test dynamique 39
VII.2.3 Audit de code source 39
VII.2.4 Audit intrusif..... 40
VII.2.5 Audit intrusif différentiel 40
VII.3 Annexe n°3 – Échelle de classification des vulnérabilités 41
VII.3.1 Échelle d'impact de l'exploitation de la vulnérabilité..... 41
VII.3.2 Échelle de facilité d'exploitation de la vulnérabilité..... 42
VII.3.3 Matrice de gravité de la vulnérabilité 42
VII.4 Annexe n°4 – Sécurité et recommandations d'usage..... 43

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. »

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 homologue, en vue notamment de s'assurer de leur conformité aux règlements de jeux et paris concernés, les logiciels de jeux et de paris utilisés par les opérateurs.

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. […] »

Article L231-1 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. »

Dispositions de l'article 11 de l'annexe à l'arrêté du 27 mars 2015 portant approbation du cahier des charges applicable aux opérateurs de jeu en ligne.

Dispositions du décret n° 2016-1326 du 6 octobre 2016 relatif aux catégories de jeux de cercle mentionnées au II de l'article 14 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.

I.2 Présentation et objectifs du document

Conformément aux dispositions du 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, modifiée par l'ordonnance n° 2019-1015 du 2 octobre 2019 réformant la régulation des jeux d'argent et de hasard, l'ANJ homologue les logiciels de jeux et de paris utilisés par les opérateurs de jeux agréés ou titulaires de droits exclusifs.

L'homologation du logiciel de jeu a pour objectifs de :

- S'assurer de la conformité du logiciel de jeu au règlement de jeu affiché par l'opérateur aux joueurs ;
- S'assurer de la sécurité et de la robustesse du dispositif technique mis en œuvre par l'opérateur ;
- Et de façon générale, s'assurer de la conformité du logiciel de jeu aux objectifs de l'État en matière de jeux d'argent et de hasard.

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'homologation que le logiciel de jeu contrevient à l'un de ces objectifs, l'ANJ rejettera la demande d'homologation.

À cette fin, le présent document définit les exigences techniques relatives à l'homologation du logiciel de jeu.

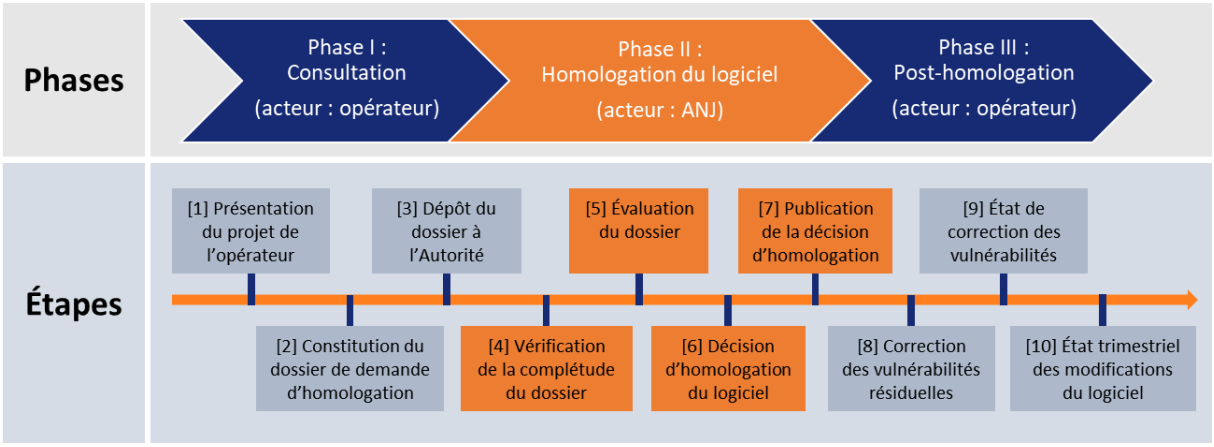
Il expose :

- Le champ d'application de la procédure d'homologation du logiciel de jeu, c'est-à-dire dans quels cas l'opérateur doit faire une demande d'homologation logicielle (section II) ;
- Le périmètre de l'homologation, c'est-à-dire l'ensemble des éléments qui doivent être couverts par les différents audits inclus dans le dossier d'homologation (section III) ;
- Les travaux et audits à effectuer préalablement au dépôt de la demande (section IV) ;

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

- La procédure d'homologation (section V) ;
- Le suivi des logiciels homologués (section VI).

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



I.3 Glossaire

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[2], 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).

[2] 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.

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 ;
- 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.4 Identification des exigences et recommandations dans le document

Le présent document comporte deux niveaux de préconisations :

- Les préconisations précédées de **[E_numero]** sont des exigences qui revêtent un caractère **obligatoire**, sous réserve des exceptions mentionnées au sein des présentes exigences techniques ;
- Les préconisations 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'homologation du logiciel de jeu

Les exigences ci-dessous définissent le cadre permettant d'évaluer la pertinence de l'homologation d'un logiciel de jeu. L'homologation logicielle est requise dans les cas suivants :

[E_HOM_CHA1] Un nouveau logiciel de jeu ou un nouveau composant d'un logiciel de jeu est systématiquement homologué avant sa mise en exploitation. Cette règle s'applique pour les homologations demandées (i) dans le cadre du dépôt d'un dossier de demande d'agrément, mais aussi (ii) lorsqu'un opérateur régulé par l'ANJ souhaite exploiter un nouveau jeu.

[E_HOM_CHA2] Un logiciel de jeu ou un composant du logiciel de jeu spécifique à un nouveau support (exemples : téléphone mobile, tablette, etc.) est considéré comme un nouveau logiciel de jeu.

[E_HOM_CHA3] Un logiciel de jeu ayant fait l'objet d'une évolution substantielle, depuis sa dernière homologation, est considéré comme un nouveau logiciel de jeu.

Qu'est-ce qu'une évolution substantielle ?

Une évolution est qualifiée de substantielle lorsque soit :

1. Elle modifie la mécanique de jeu ;
2. Elle modifie les règles de jeu ;
3. Elle remet en question l'analyse de la sécurité du logiciel de jeu.

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 du logiciel de jeu modifiant tout ou partie des mécanismes ou configurations impactant directement la sécurité du logiciel de jeu (exemples : authentification, gestion des sessions, chiffrement des communications client-serveur) ;
5. La modification de l'architecture interne du logiciel de jeu (i.e. ajout ou suppression d'un ou plusieurs composants) ;
6. Une évolution technique correspondant au remplacement d'une technologie par une autre dans le logiciel de jeu (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 logiciel de jeu (changement du site d'hébergement, de l'hébergeur, du fournisseur de plateforme de jeu) ;
8. L'ajout ou la modification d'une ou plusieurs interconnexions directes du logiciel de jeu avec d'autres systèmes d'information.

Ne sont pas considérés par l'ANJ comme des évolutions substantielles les quatre points suivants, sous réserve que les modifications apportées n'impliquent pas les points n° 1 à 3 :

9. La montée de version du logiciel de jeu 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 de l'interface du logiciel de jeu accessible aux joueurs ;
12. La modification par paramétrage.

En cas de doute sur le respect des objectifs de la politique de l'État en matière de jeux d'argent et de hasard énoncés à l'article L. 320-3 du code de la sécurité intérieure, l'Autorité nationale des jeux se réserve la possibilité de réviser la qualification de l'évolution retenue par l'opérateur lors des suivis trimestriels (cf. section VI.1) et des certifications annuelles (cf. section VI.2). Aussi l'Autorité pourra exiger d'un opérateur qu'il procède à une demande d'homologation d'un logiciel s'il lui apparaît que l'évolution en cause est substantielle.

[E_HOM_CHA4] Un logiciel de jeu, ou l'un de ses composants, qui a été décommissionné (c'est-à-dire sorti d'exploitation) depuis plus de douze mois, est considéré par l'Autorité comme un nouveau logiciel de jeu si l'opérateur décide de le remettre en service.

[E_HOM_CHA5] Un logiciel de jeu homologué doit être mis en production dans un délai de douze mois à compter de la date d'homologation. Au-delà, l'exploitation du logiciel de jeu est conditionnée à l'obtention d'une nouvelle homologation, sauf avis explicite contraire de l'Autorité.

[E_HOM_CHA6] La mise en exploitation par un opérateur, pour sa propre activité de jeu ou de paris, d'un logiciel de jeu ou composant de jeu déjà homologué au bénéfice d'un autre opérateur est soumise à l'obtention d'une nouvelle homologation.

Néanmoins, sous réserve que le code source n'ait pas fait l'objet d'une évolution substantielle depuis le prononcé de l'homologation au bénéfice d'un autre opérateur, le périmètre du rapport d'audit de la sécurité peut se concentrer sur l'intégration par l'opérateur du logiciel jeu ou composant de jeu. Le rapport d'audit de la conformité de l'implémentation des fonctions métiers visera la conformité au règlement de jeu.

[E_HOM_CHA7] Un logiciel sur borne ou terminal en point de vente, permettant aux joueurs l'accès direct ou indirect (*via* par exemple un buraliste) à un jeu d'argent, est considéré comme un composant du logiciel de jeu. Son exploitation est conditionnée à l'obtention d'une homologation.

[E_HOM_CHA8] Un logiciel d'impression de tickets physiques de jeux de grattage sous droits exclusifs est considéré comme faisant partie du dispositif de jeu de l'opérateur. Ce logiciel est donc soumis à l'obtention d'une homologation.

III Périmètre de l'homologation d'un logiciel de jeu

[E_HOM_PER1] Le périmètre de l'homologation du logiciel de jeu n'inclut que le logiciel de jeu concerné. Toutefois, l'audit de sécurité prévu au IV.2 du présent document doit être en mesure de garantir que la sécurité du logiciel de jeu n'est pas impactée par les autres composants de la plateforme. Le périmètre de l'audit pourrait s'en trouver étendu.

[E_HOM_PER2] Le périmètre de l'audit de sécurité est défini en tenant compte :

- Des recommandations, réserves et plans de remédiation issus des homologations et audits précédents pour un logiciel de jeu déjà homologué ;
- Des interconnexions du logiciel de jeu avec d'autres systèmes d'information ;
- Des moyens et procédures mis en œuvre pour le maintien en condition de sécurité (MCS) du logiciel de jeu ;

- Des moyens et procédures mis en œuvre pour les opérations de maintenance, d'exploitation et de télégestion du système d'information, notamment lorsqu'elles sont réalisées par des prestataires externes (exemple : partenariat B2B entre un opérateur agréé et un fournisseur de plateforme de jeu pour les activités de jeu de poker en ligne).
- Le cas échéant, des plans d'assurance sécurité pour les services en mode *Software as a Service (SaaS*).

L'adoption d'une approche modulaire du logiciel de jeu peut être envisagée dans le cadre d'une homologation. Le périmètre de la demande d'homologation peut alors être restreint :

- Soit aux seuls nouveaux composants du logiciel de jeu non encore homologués ;
- Soit aux composants déjà homologués du logiciel de jeu ayant fait l'objet d'une évolution substantielle depuis la dernière homologation.

Par exemple, un nouveau client de jeu pourra faire l'objet d'une homologation seule, sans qu'il soit nécessaire d'homologuer à nouveau le moteur de jeu, déjà homologué, sur lequel le jeu s'appuie, sous réserve que ce dernier n'ait pas fait l'objet d'une évolution substantielle depuis sa dernière homologation.

[E_HOM_PER3] La limitation de la portée de la demande d'homologation d'un logiciel de jeu à seulement une partie de ses composants doit être expliquée et justifiée par l'opérateur dans le dossier de demande d'homologation.

Information importante :

L'opérateur ne peut exploiter un logiciel de jeu avant son homologation par l'Autorité nationale des jeux. L'opérateur qui méconnaît le caractère préalable de l'homologation commet un manquement susceptible de conduire à l'ouverture d'une procédure de sanction en application de l'article 43 de la loi n° 2010-476 du 12 mai 2010 modifiée. En outre, l'Autorité pourra demander à l'opérateur de cesser sans délai l'exploitation de ce logiciel, qui devrait être regardée comme ayant lieu aux risques et périls de l'opérateur.

Recommandation :

En cas de doute sur la nécessité d'une homologation, le périmètre de celle-ci ou toute autre interrogation, les opérateurs sont invités à se rapprocher de l'ANJ en amont du dépôt éventuel du dossier.

Cet échange peut également permettre d'évoquer la conformité juridique du projet.

IV Travaux préalables au dépôt de la demande d'homologation

Dans l'hypothèse où une homologation de logiciel de jeu est nécessaire, l'opérateur doit faire procéder à un certain nombre d'audits (cf. les sections IV.2, IV.3 et IV.4) et établir un plan de remédiation en fonction de leurs conclusions.

IV.1 Dispositions communes aux différents audits

IV.1.1 Réalisation des audits

[E_HOM_AUD1] Les différents audits demandés dans le cadre de l'homologation d'un logiciel de jeu sont réalisés par un ou plusieurs auditeurs tiers.

[E_HOM_AUD2] L'opérateur est tenu de joindre, au dossier de la demande d'homologation, une copie des contrats de prestation d'audit.

[E_HOM_AUD3] Ces différents audits sont opérés dans les douze mois précédant le dépôt de la demande d'homologation. La date de fin de prestation d'audit apparaissant dans chacun des différents rapports d'audit permet de s'assurer du respect de ce délai.

L'attention de l'opérateur est appelée sur le fait que le non-respect de cette obligation relative à l'ancienneté des audits est un motif d'incomplétude de la demande d'homologation.

[E_HOM_AUD4] Chaque rapport d'audit est signé électroniquement par l'auditeur qui en est l'auteur, selon le standard défini dans l'annexe n°4 du présent document. Les fichiers de signature électronique obtenus accompagnent alors les différents rapports d'audit joints au dossier de la demande d'homologation.

Afin de pouvoir vérifier l'authenticité des rapports d'audit, les auditeurs communiqueront à l'ANJ, préalablement au dépôt de la demande d'homologation, leur clef publique *via* l'adresse mail de contact : regulation-si@anj.fr.

[E_HOM_AUD5] Chaque ressource auditée ou utilisée pour appuyer un audit, (i) de type ressource documentaire, par exemple le règlement de jeu ou des annexes techniques, ou (ii) de type code source, remise à l'auditeur par l'opérateur dans le cadre d'un audit, est jointe au dossier de la demande d'homologation :

1. la ressource documentaire ;
2. le rapport d'audit liste chaque code source audité, avec son nom, version et date de réception par les auditeurs ainsi que le checksum du code source. Le code source ne sera transmis, chiffré avec la clé ANJ, que sur demande expresse de l'ANJ à l'opérateur. L'opérateur est tenu de conserver le code source tant que l'homologation logicielle correspondante est utilisée.

Les codes sources pourront être transmis directement par le fournisseur si l'opérateur n'y a pas accès.

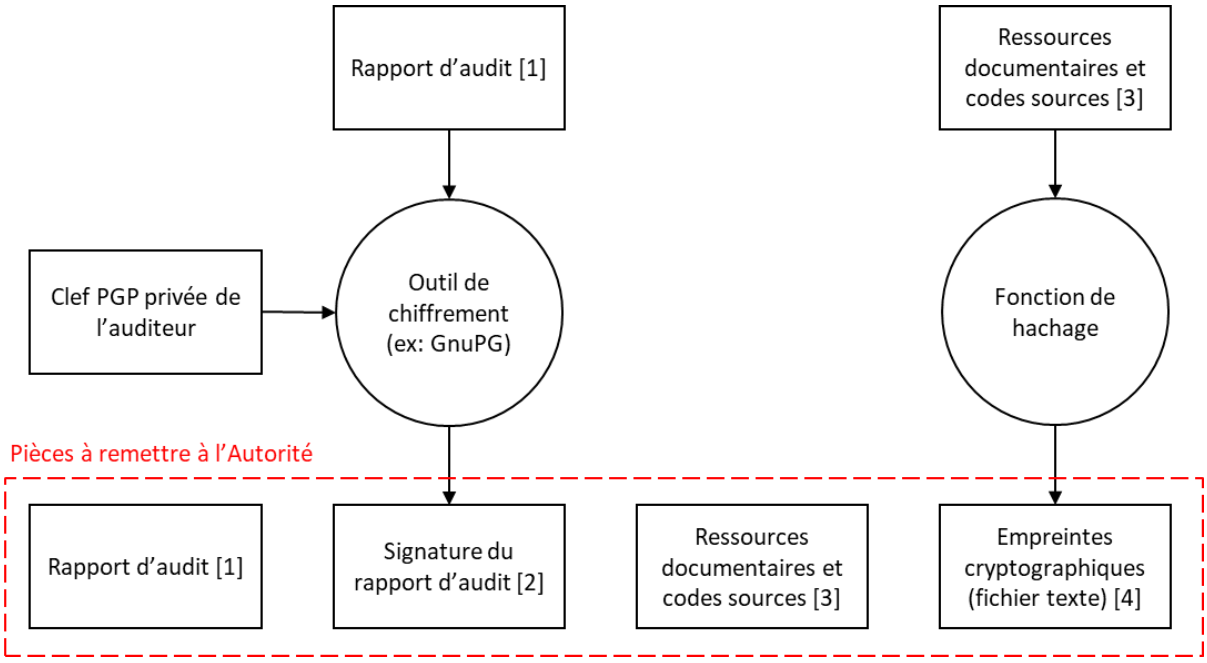
Le code source propre à l'infrastructure cloud (scripts de déploiement de type « Infrastructure as code ») n'a pas à être couvert dans le cadre de l'audit de code source, cet aspect de l'infrastructure étant validé dans le cadre d'un audit de configuration dans le cadre de la certification annuelle.

Dans le cas où ni l'opérateur, ni le fournisseur ne seraient en mesure de communiquer à l'ANJ les codes sources, les audits de sécurité et/ou fonctionnels desdits codes du fournisseur devront être fournis, accompagnés de la présentation des éventuelles clauses contractuelles relatives à la sécurité du logiciel de jeu.

[E_HOM_AUD6] Les ressources auditées ou utilisées pour appuyer un audit, doivent faire l'objet d'un calcul d'empreinte cryptographique. Ce calcul est réalisé par l'auditeur à l'aide de la fonction de hachage indiquée dans l'annexe n°4 du présent document. Les empreintes ainsi obtenues sont compilées dans un fichier texte accompagnant le rapport d'audit établi par ce même auditeur. L'empreinte cryptographique du fichier texte doit par ailleurs apparaître dans les rapports d'audit.

L'ensemble de ces empreintes cryptographiques doit permettre de s'assurer que les ressources présentées à l'Autorité dans le cadre d'une demande d'homologation d'un logiciel de jeu correspondent aux ressources auditées ou utilisées pour alimenter un audit.

Se référer au schéma de principe ci-dessous :



IV.1.2 Non-conformités et anomalies de sécurité

[E_HOM_CAN1] Préalablement au dépôt de la demande d'homologation, les éventuelles non-conformités, identifiées lors de l'audit de la conformité de l'implémentation des fonctions métier au sein du logiciel de jeu, ont fait l'objet (i) d'une remédiation, (ii) les corrections apportées ont été validées par l'auditeur et (iii) cette validation a été tracée dans le rapport d'audit joint au dossier de la demande d'homologation.

[E_HOM_CAN2] Préalablement au dépôt de la demande d'homologation, les éventuelles anomalies de sécurité qualifiées de majeures ou critiques[3], identifiées lors de l'audit de la sécurité du logiciel de jeu, ont fait l'objet (i) d'une remédiation, (ii) les corrections apportées ont été validées par l'auditeur et (iii) cette validation a été tracée dans le rapport d'audit joint au dossier de la demande d'homologation.

[E_HOM_CAN3] Les éventuelles anomalies de sécurité qualifiées de mineures ou importantes, identifiées lors de l'audit de la sécurité du logiciel de jeu, doivent faire l'objet (i) d'un plan de remédiation. Leur correction n'est pas exigée en amont de la décision d'homologation du logiciel de jeu, mais elle doit intervenir dans un délai qui ne peut excéder (ii) douze mois pour les anomalies mineures et (iii) six mois pour les anomalies importantes à compter de la décision d'homologation. Les corrections apportées devront être validées dans le cadre de la certification annuelle.

[E_HOM_CAN4] Si aucune mesure de sécurité ne permet de corriger directement les anomalies de sécurité, l'opérateur devra (i) proposer des mesures compensatoires afin d'éviter leur exploitation. Les mesures compensatoires ou de protection périmétrique proposées pour les anomalies de sécurité, majeures ou critiques devront (ii) être mises en place et (iii) faire l'objet d'une validation par l'auditeur, préalablement au dépôt de la demande d'homologation. (iv) Cette validation devra être tracée dans les rapports d'audit concernés joints au dossier de la demande d'homologation.

[E_HOM_CAN5] Lors du dépôt de la demande d'homologation, l'opérateur justifie auprès de l'ANJ tout refus de correction des anomalies et non-conformités identifiées au cours des différents audits 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.

Le cas échéant, sur demande de l'ANJ lors de l'instruction du dossier, l'opérateur prépare en amont avec l'auditeur et organise une réunion associant l'ANJ et l'auditeur dans les 15 jours calendaires suivant la demande pour un échange contradictoire sur les refus de corrections qu'il a exprimé.

IV.1.3 Plan de remédiation

[E_HOM_PRM1] L'opérateur établit un plan de remédiation, qui contient, pour chaque anomalie ou non-conformité recensée dans les rapports d'audit, une fiche comportant au minimum trois volets :

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

[E_HOM_PRM2] Pour les anomalies de sécurité mineures ou importantes, l'opérateur est tenu de rendre compte à l'ANJ de la réalisation du plan de remédiation aux dates indiquées.

[3] Se référer à l'échelle de gravité des vulnérabilités définie dans l'annexe n°3 du présent document.

IV.2 Dispositions relatives à l'audit de la sécurité du logiciel de jeu ou du composant visé par l'homologation

Cet audit permet de s'assurer que la sécurité mise en œuvre au niveau du logiciel de jeu ou du composant visé par l'homologation est « à l'état de l'art » ou s'en approche.

[E_HOM_SEC1] Le rapport d'audit intrusif suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire :

Conditions de réalisation :

1. Le nom et les coordonnées de l'organisme chargé de réaliser l'audit ;
2. Les informations sur les intervenants (nom, prénom, fonction, adresse de contact) ;
3. Les dates de début et de fin de la prestation d'audit ;
4. La charge (en JH) de la prestation d'audit ;
5. La liste des éléments mis à disposition des auditeurs ;

Périmètre de l'audit :

6. La description du périmètre de l'audit. Il s'agit également de présenter la liste des modules applicatifs audités et des versions associées ;
7. L'empreinte cryptographique des fichiers des codes sources audités afin de pouvoir garantir l'absence de modification du logiciel audité ;
8. L'empreinte cryptographique des ressources documentaires auditées ou utilisées pour appuyer l'audit ;
9. Lorsque l'homologation est concernée par l'application de [E_HOM_CHA6], c'est-à-dire la mise en exploitation par l'opérateur pour sa propre activité de jeu ou de paris, d'un logiciel de jeu ou composant de jeu déjà homologué au bénéfice d'un autre opérateur, ce point est explicité dans le périmètre, avec la référence à l'homologation (objet, numéro d'homologation, date) dont bénéficie le logiciel de jeu ou composant de jeu visé par l'homologation. Sous réserve que le code source n'ait pas fait l'objet d'une évolution substantielle depuis le prononcé de l'homologation au bénéfice d'un autre opérateur, le périmètre du rapport d'audit de la sécurité peut se concentrer sur l'intégration par l'opérateur.

Méthodologie :

10. La description explicite de la méthodologie employée lors de l'audit pour détecter les vulnérabilités et les exploiter le cas échéant (exemple : analyse en mode boîte blanche/grise, analyse manuelle/automatisée des codes sources, recherche des points sensibles du langage et des technologies utilisées, analyse des fichiers de configuration, recherche des points d'entrées potentiellement dangereux) ;

Synthèse managériale :

11. L'avis de l'auditeur concernant le niveau de sécurité du logiciel de jeu ou du composant visé par l'homologation ;

12. La synthèse des points positifs ;

13. La synthèse des vulnérabilités recensées et des risques associés ;

14. La synthèse des recommandations de l'auditeur pour corriger les vulnérabilités recensées ;

Validation des corrections :

15. L'avis de l'auditeur concernant les corrections et autres mesures compensatoires appliquées par l'opérateur aux vulnérabilités recensées, en particulier les vulnérabilités majeures ou critiques ;

Présentation du logiciel de jeu ou du composant visé par l'homologation :

16. Un rappel de la description fonctionnelle du logiciel, de l'architecture applicative et des interactions entre les différentes briques logicielles ;

Analyse détaillée :

17. L'identification des besoins de sécurité : cette partie présentera les fonctionnalités de sécurité requises (exemple : authentification, gestion de session, stockages des données sensibles, politique des mots de passe, prévention contre les attaques connues : XSS, CSRF, Injection SQL, déni de service…) ;

18. La validation des fonctionnalités de sécurité et de la bonne implémentation des mesures de sécurité répondant aux besoins cités dans le point précédent : cette partie décrira les différents mécanismes de sécurité et leur implémentation dans le code source du logiciel de jeu ou du composant visé par l'homologation (sécurisation des communications, utilisation de jeton anti-CSRF, validation des données échangées, robustesse des algorithmes de hachage et de chiffrement utilisés…) ;

19. La recherche de vulnérabilités hors périmètre des fonctionnalités de sécurité : cette partie doit préciser si l'application est vulnérable à d'autres types d'attaques, non traités dans le point précédent (exemple : défaut de configuration, utilisation d'une version obsolète d'une dépendance…) ;

20. Les recommandations de l'auditeur pour corriger les vulnérabilités recensées et pour améliorer la sécurité du logiciel (exemple : bonnes pratiques de développement).

[R_HOM_SEC1] Dans le cadre de l'évolution d'un logiciel de jeu ou du composant visé par l'homologation, déjà homologué, le périmètre de l'audit pourra être restreint aux seules modifications qui auront été apportées depuis la dernière homologation. Il s'agira donc de réaliser un audit intrusif différentiel (cf. annexe n°2).

IV.3 Dispositions relatives à l'audit de la qualité et de la sécurité du générateur de nombres aléatoires

Cet audit permet de s'assurer que le niveau de qualité et de sécurité du dispositif GNA est suffisant pour satisfaire l'objectif d'intégrité des opérations de jeux prescrits au 2 de l'article L. 320-3 du code de la sécurité intérieure.

[E_HOM_GNA1] Le rapport d'audit du dispositif GNA suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire :

Conditions de réalisation :

1. Le nom et les coordonnées de l'organisme chargé de réaliser l'audit ;
2. Les informations sur les intervenants (nom, prénom, fonction, adresse de contact) ;
3. Les dates de début et de fin de la prestation d'audit ;
4. La charge (en JH) de la prestation d'audit ;
5. La liste des éléments mis à disposition des auditeurs ;

Périmètre de l'audit :

6. La description du périmètre de l'audit. Il s'agit également de présenter la liste des codes applicatifs audités, le générateur de valeurs aléatoires et les codes transformant ces valeurs aléatoires en aléa de jeu qui constituent le dispositif GNA ;
7. L'empreinte cryptographique des fichiers des codes sources audités afin de pouvoir garantir l'absence de modification des codes applicatifs audités ;
8. L'empreinte cryptographique des ressources documentaires auditées ou utilisées pour appuyer l'audit ;

Méthodologie :

9. La description de la procédure d'audit de la qualité et de la sécurité du GNA ;

Synthèse managériale :

10. L'avis de l'auditeur concernant la qualité et la sécurité du GNA ;
11. La synthèse des points positifs ;
12. La synthèse des vulnérabilités recensées et des risques associés ;
13. La synthèse des recommandations de l'auditeur pour corriger les vulnérabilités recensées ;

Validation des corrections :

14. L'avis de l'auditeur concernant les corrections et autres mesures compensatoires appliquées par l'opérateur aux vulnérabilités recensées, en particulier des vulnérabilités majeures ou critiques ;

Présentation du dispositif GNA :

15. La description du contexte d'utilisation du GNA (exemple : tirage de cartes au poker) ;

16. La description générale du GNA. Il s'agit notamment de présenter l'architecture du dispositif et les technologies employées ;

17. La description de la plateforme matérielle associée au dispositif GNA ;

Analyse détaillée :

18. L'analyse de la documentation de l'opérateur (notamment la description fonctionnelle et technique) relative au dispositif GNA. Il s'agit de vérifier si une telle documentation existe, si elle est à jour, ainsi que sa qualité rédactionnelle ;

19. La validation des choix technologiques (logiciels, matériels, architecture) au regard du contexte d'usage du dispositif GNA ;

20. L'analyse du processus d'initialisation et de rafraîchissement du GNA (type et qualité des sources d'aléa, entropie de la graine, fréquence de rafraîchissement du générateur) ;

21. L'analyse de l'algorithme du GNA ;

22. L'analyse de l'utilisation des nombres aléatoires dans la plateforme de jeu (exemple : analyse de l'algorithme de mélange des cartes mis en œuvre dans le cadre des jeux de poker) ;

23. La validation du mécanisme garantissant l'intégrité du générateur dans le temps (exemple : vérification régulière de la signature des binaires des codes applicatifs constituant le GNA) ;

24. La validation du processus de contrôle garantissant la stabilité dans le temps de la qualité du caractère aléatoire des nombres générés (exemple : tests statistiques réalisés de façon périodique, accompagnés d'une procédure de gestion des anomalies) ;

25. Les recommandations de l'auditeur pour corriger les vulnérabilités recensées et pour améliorer la sécurité et la qualité du GNA.

IV.4 Dispositions relatives à l'audit de la conformité de l'implémentation des fonctions métier

Cet audit permet de s'assurer que l'implémentation, au niveau du logiciel ou du composant visé par l'homologation, des fonctions métier relatives aux règles de jeu et à la mécanique de jeu (notamment les règles de calcul, les primitives de jeu et, de façon générale, le comportement du logiciel) est conforme au règlement de jeu tel que présenté, de façon littérale, aux joueurs et au déroulement du jeu tel que présenté sur le site ou l'application, support de l'offre de jeu.

Elle permet également de s'assurer raisonnablement de l'absence de moyen de contournement de ces règles.

[E_HOM_CFM1] Le rapport d'audit des fonctions métier suivra le plan détaillé ci-après. Il pourra contenir des sections supplémentaires si l'opérateur ou l'auditeur le juge nécessaire :

Conditions de réalisation :

1. Le nom et les coordonnées de l'organisme chargé de réaliser l'audit ;

2. Les informations sur les intervenants (nom, prénom, fonction, adresse de contact) ;
3. Les dates de début et de fin de la prestation d'audit ;
4. La charge (en JH) de la prestation d'audit ;
5. La liste des éléments mis à disposition des auditeurs ;

Périmètre de l'audit :

6. La description du périmètre de l'audit ;
7. L'empreinte cryptographique des fichiers des codes sources audités afin de pouvoir garantir l'absence de modification du logiciel audité ;
8. L'empreinte cryptographique des ressources documentaires auditées ou utilisées pour appuyer l'audit (exemples : règlement de jeu, annexes techniques, cahier des charges) ;

Méthodologie :

9. La description de la procédure d'audit des fonctions métier et de leur implémentation dans les codes sources du logiciel audité ;

Synthèse managériale :

10. L'avis de l'auditeur concernant le niveau de conformité d'implémentation des fonctions métier ;
11. La synthèse des non-conformités recensées ;
12. La synthèse des recommandations de l'auditeur pour corriger les non-conformités ;
13. L'avis de l'auditeur concernant les corrections apportées par l'opérateur aux non-conformités recensées ;

Validation des corrections :

14. L'avis de l'auditeur concernant les corrections et autres mesures compensatoires appliquées par l'opérateur aux non-conformités recensées ;

Analyse détaillée des fonctions métier et de leur implémentation :

15. Dans le cas des jeux de cercle :
    a) Les règles de jeu telles qu'affichées aux joueurs et leur analyse ;
    b) L'analyse des variantes de jeu de poker proposées ;
    c) L'analyse des offres de jeu : tournois, cash-games, sit&go et autres formats de jeu éventuels ;
    d) L'analyse de la gestion de l'inscription d'un joueur à un jeu (notamment les tournois) ;
    e) L'analyse des actions de jeu (placement des joueurs, augmentation des blindes, distribution des cartes, distribution des gains…) ;

f) L'analyse des informations affichées aux joueurs (historique de jeu, jeux en cours, résultats, mises engagées et gains) ;

16. Dans le cas des paris sportifs :

    a) Les règles de jeu telles qu'affichées aux joueurs et leur analyse ;

    b) L'analyse des actions de jeu (enregistrement de pari, débouclage, distribution des gains…) ;

    c) L'analyse des informations affichées aux joueurs (historique de jeu, paris et jeux en cours, résultats, mises engagées et gains) ;

17. Dans le cas des paris hippiques :

    a) Les règles de jeu telles qu'affichées aux joueurs et leur analyse ;

    b) L'analyse des actions de jeu (enregistrement de pari, débouclage, distribution des gains…) ;

    c) L'analyse des informations affichées aux joueurs (historique de jeu, paris et jeux en cours, résultats, mises engagées et gains) ;

18. Dans le cas des jeux de loterie :

    a) L'analyse des règles de jeu affichées aux joueurs ;

    b) L'analyse des actions de jeu (prise de jeu, débouclage, distribution des gains…) ;

    c) L'analyse des informations affichées aux joueurs (historique de jeu, jeux en cours, résultats, mises engagées et gains) ;

19. Dans le cas spécifique d'un moteur de jeu :

    a) L'analyse de toutes les primitives de jeu ;

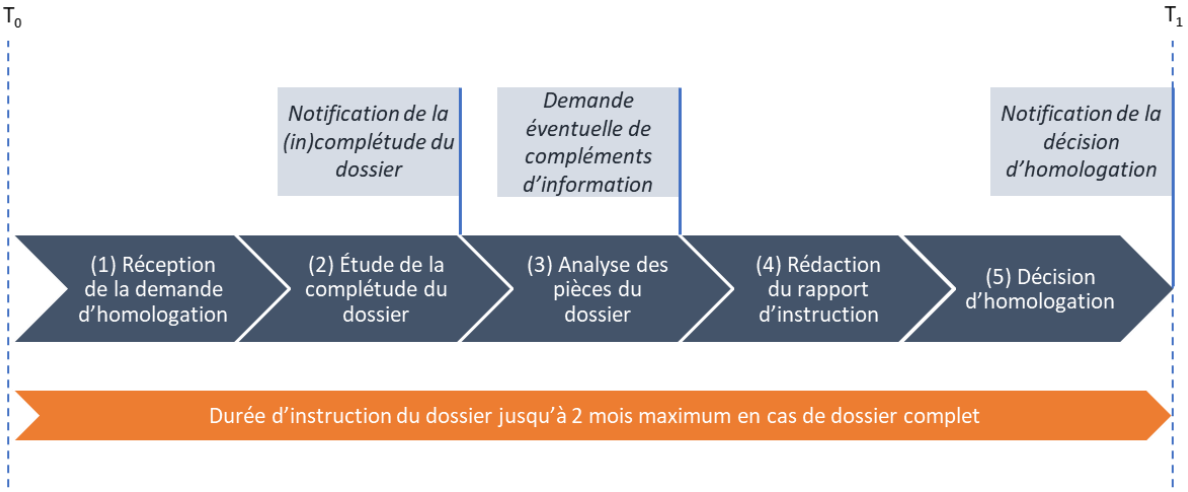
20. Dans le cas spécifique d'un totalisateur pour les jeux à caractère mutuel :

    a) L'analyse des règles de calcul portant en particulier sur les masses d'enjeux, les rapports et la distribution des gains ;

21. La recherche de moyens de contournement des règles de jeu, des règles de calcul et de la mécanique de jeu implémentées au niveau des codes sources du logiciel.

V Procédure d'homologation du logiciel de jeu

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



V.1 Contenu du dossier

[E_HOM_PDH1] Le dossier de demande d'homologation d'un logiciel de jeu déposé auprès de l'ANJ, dans un format dématérialisé, comprend les pièces suivantes :

V.1.1 Cas de l'homologation d'un jeu en ligne

De façon générale, le dossier de demande d'homologation d'un logiciel de jeu associé à un jeu en ligne inclut :

1. Le formulaire de demande d'homologation du logiciel de jeu, dûment renseigné. Ce formulaire est mis à disposition sur le site[4] de l'ANJ ;
2. La description fonctionnelle et technique du logiciel de jeu et, le cas échéant, de ses évolutions ;
3. Le rapport d'audit de la sécurité du logiciel de jeu (cf. section IV.2) ;
4. Le rapport d'audit certifiant que les règles du jeu et la mécanique de jeu implémentées dans le logiciel de jeu sont bien conformes au jeu tel qu'il est présenté au joueur (cf. section IV.4) ;
5. Le règlement de jeu, décrivant les règles de jeu et accompagné des éventuelles conditions générales d'utilisation ;
6. Le plan de remédiation des anomalies et non-conformités constatés au cours de l'audit du logiciel de jeu (cf. section IV.1.3) ;

[4] Lien : https://anj.fr/regulation/documentation-destination-des-operateurs

Si le jeu s'appuie sur un dispositif GNA qui n'est pas déjà homologué, celui-ci devra faire l'objet d'une homologation spécifique (cf. section IV.3).

Si le jeu s'appuie sur un moteur de jeu qui a déjà fait l'objet d'une homologation indépendante, le périmètre de l'homologation pourra être restreint aux autres composants du logiciel de jeu non encore homologués ou ayant fait l'objet d'une évolution substantielle depuis la dernière homologation.

V.1.2 Cas de l'homologation d'un dispositif GNA

Le générateur de nombres aléatoires (GNA) sur lequel s'appuie un jeu fait l'objet d'une homologation indépendante du logiciel de jeu. Cette modularité permet la réutilisation du GNA pour un autre jeu sans qu'il soit nécessaire de procéder à la ré-homologation du composant GNA, sous réserve que celui-ci n'ait pas fait l'objet d'une évolution substantielle depuis sa dernière homologation.

L'attention de l'opérateur est appelée sur le fait que l'homologation du dispositif GNA ne se vaut pas homologation du logiciel de jeu et de ses composants.

Le dossier de demande d'homologation inclut :

1. Le formulaire de demande d'homologation du logiciel de jeu, dûment renseigné. Ce formulaire est mis à disposition sur le site[5] de l'ANJ ;
2. La description fonctionnelle et technique du dispositif GNA et, le cas échéant, de ses évolutions ;
3. La justification des choix technologiques (logiciels et matériels, architecture) mis en œuvre ;
4. Le rapport d'audit de la qualité et de la sécurité du dispositif GNA (cf. section IV.3) ;
5. Le plan de remédiation des anomalies constatées au cours de l'audit du dispositif GNA (cf. section IV.1.3) ;

V.1.3 Cas de l'homologation d'un moteur de jeu

Le moteur de jeu sur lequel s'appuie un jeu peut faire l'objet d'une homologation indépendante du logiciel de jeu. Cette modularité permet la réutilisation du même moteur de jeu pour un autre jeu, en allégeant l'homologation du logiciel associé au second jeu.

L'attention de l'opérateur est appelée sur le fait que l'homologation du moteur de jeu ne vaut pas homologation du logiciel de jeu et de ses composants.

Le dossier de demande d'homologation inclut :

1. Le formulaire de demande d'homologation du logiciel de jeu, dûment renseigné. Ce formulaire est mis à disposition sur le site[6] de l'ANJ ;
2. La description fonctionnelle et technique du moteur de jeu et, le cas échéant, de ses évolutions. Cette documentation doit également détailler les primitives de jeu disponibles ;

[5] Lien : https://anj.fr/regulation/documentation-destination-des-operateurs
[6] Lien : https://anj.fr/regulation/documentation-destination-des-operateurs

3. Le rapport d'audit de la sécurité du moteur de jeu (cf. section IV.2) ;
4. Le rapport d'audit de la bonne implémentation des primitives de jeu (cf. section IV.4) ;
5. Le plan de remédiation des anomalies et non-conformités constatées au cours des audits (cf. section IV.1.3) ;

Si le moteur de jeu s'appuie sur un dispositif GNA qui n'est pas déjà homologué, celui-ci devra faire l'objet d'une homologation spécifique (cf. section IV.3).

V.1.4 Cas de l'homologation d'un totalisateur pour les jeux à caractère mutuel

Le totalisateur utilisé pour les paris mutuels et sur lequel s'appuie un jeu peut faire l'objet d'une homologation indépendante du logiciel de jeu. Cette modularité permet la réutilisation du même totalisateur pour un autre jeu, en allégeant l'homologation du logiciel associé au second jeu.

L'attention de l'opérateur est appelée sur le fait que l'homologation du totalisateur ne vaut pas homologation du logiciel de jeu et de ses composants.

Le dossier de demande d'homologation inclut :

1. Le formulaire de demande d'homologation du logiciel de jeu, dûment renseigné. Ce formulaire est mis à disposition sur le site[7] de l'ANJ ;
2. La description fonctionnelle et technique du totalisateur et, le cas échéant, de ses évolutions. Cette documentation doit notamment détailler les calculs pouvant être opérés par le totalisateur ;
3. Le rapport d'audit de la sécurité du totalisateur (cf. section IV.2) ;
4. Le rapport d'audit de la bonne implémentation des règles de calcul portant en particulier sur les masses d'enjeux, les rapports et la distribution des gains (cf. section IV.4) ;
5. Le plan de remédiation des anomalies et non-conformités constatées au cours des audits (cf. section IV.1.3) ;

V.1.5 Cas de l'homologation d'un logiciel de jeu en point de vente ou sur borne

Le logiciel de jeu sur les bornes en libre accès ou sur les terminaux en point de vente, fait l'objet d'une homologation indépendante et spécifique.

L'attention de l'opérateur est appelée sur le fait que l'homologation du logiciel de jeu sur borne ou terminal en point de vente n'est pas réduite aux éléments logiciels physiquement installés dans le point de vente mais inclut également dans son périmètre les composants sur la ou les plateformes centrales de l'opérateur avec lesquels le terminal ou la borne échange, en particulier les composants d'interconnexion, les composants participants à la mécanique de jeu et aux éventuels mécanismes de gestion des mises à jour des logiciels sur borne ou terminal. S'il est considéré que les composants

[7] Lien : https://anj.fr/regulation/documentation-destination-des-operateurs

participants à la mécanique de jeu sont assimilables à un moteur de jeu, ces composants pourront faire l'objet d'une homologation indépendante (cf. section V.1.3).

Le dossier de demande d'homologation inclut :

1. Le formulaire de demande d'homologation du logiciel de jeu, dûment renseigné. Ce formulaire est mis à disposition sur le site[8] de l'ANJ ;
2. La description technique et fonctionnelle du logiciel de jeu et, le cas échéant, de ses évolutions. Cette documentation doit également présenter le dispositif matériel (borne ou terminal) sur lequel est installé le logiciel de jeu et détailler les moyens de sécurisation, aussi bien matériels que logiciels, mis en œuvre au niveau de la borne ou du terminal en point de vente ;
3. Le rapport d'audit de la sécurité du logiciel de jeu en point de vente (cf. section IV.2) ;
4. Le rapport d'audit certifiant que les règles du jeu et la mécanique de jeu implémentées dans le logiciel de jeu en point de vente sont bien conformes au jeu tel qu'il est présenté au joueur (cf. section IV.4) ;
5. Le règlement de jeu, à l'état de projet ou en version définitive, décrivant les règles de jeu et accompagné des éventuelles conditions générales d'utilisation ;
6. Le plan de remédiation des anomalies et non-conformités constatées au cours de l'audit du logiciel de jeu (cf. section IV.1.3) ;

V.1.6 Cas de l'homologation d'un logiciel d'impression de tickets de jeu de grattage

Le logiciel d'impression de tickets physiques de jeux de grattage est soumis à une homologation indépendante et spécifique car il est porteur des règles de jeu et de la mécanique de jeu lors de l'impression des tickets.

L'attention de l'opérateur est toutefois appelée sur le fait qu'il n'est pas nécessaire d'homologuer le logiciel d'impression à chaque nouveau jeu de grattage, sauf si le nouveau jeu de grattage implique une évolution substantielle du logiciel d'impression.

Le dossier de demande d'homologation inclut :

1. Le formulaire de demande d'homologation du logiciel de jeu, dûment renseigné. Ce formulaire est mis à disposition sur le site[9] de l'ANJ ;
2. La description de la procédure de génération de tickets et du dispositif d'impression de tickets ;
3. La description du processus de qualification de l'imprimeur ;
4. La présentation des éléments relatifs à la sécurité présentés dans le dossier de qualification qui ont conduit à retenir l'imprimeur ;
5. La présentation des clauses contractuelles dont dispose l'opérateur de jeu à l'égard de ses imprimeurs, relatives à la sécurité du dispositif d'impression et de son auditabilité ;

[8] Lien : https://anj.fr/regulation/documentation-destination-des-operateurs
[9] Lien : https://anj.fr/regulation/documentation-destination-des-operateurs

6. Les rapports d'audits réalisés auprès des imprimeurs portant (i) sur le logiciel d'impression et ses fonctionnalités, (ii) sur la qualité du GNA sur lequel s'appuie le logiciel d'impression pour produire les tickets et (iii) sur les moyens de sécurisation du dispositif d'impression ;

7. Le plan de remédiation des anomalies constatées au cours des audits.

V.1.7 Dispositions communes

[E_HOM_PDH1] 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_HOM_PDH2] L'absence de pièce exigée dans un dossier de demande d'homologation du logiciel de jeu devra être dûment justifiée. Dans le cas contraire, le dossier sera considéré comme incomplet.

[E_HOM_PDH3] Le cas échéant, sur demande expresse de l'ANJ pouvant intervenir lors de l'instruction ou ultérieurement tant que l'homologation logicielle correspondante est utilisée, l'opérateur transmet le code source du logiciel de jeu ou composant de jeu visé par l'homologation, à défaut, les substituts prévus dans l'exigence [E_HOM_AUD5].

[R_HOM_PDH4] En cas de doute, il est recommandé de consulter l'ANJ préalablement au dépôt de toute demande d'homologation du logiciel de jeu 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_HOM_TRF1] Le dossier de demande d'homologation est à remettre à l'ANJ par le biais du canal d'échange sécurisé mis à disposition des opérateurs.

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'homologation.

Lorsque la demande d'homologation de logiciel de jeu est formée par un opérateur de jeux ou de paris en ligne, le silence gardé pendant deux mois par l'ANJ sur cette demande vaut décision de rejet en application des dispositions du 2° de l'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.

Dans les autres cas, il est fait application des dispositions de l'article L. 231-1 du code des relations entre le public et l'administration.

Lorsque le dossier de demande est incomplet, un courrier est adressé à l'opérateur lui demandant d'y remédier dans un délai qui ne peut être inférieur à 10 jours calendaires. L'instruction est suspendue jusqu'à la date de réception des compléments demandés. Le délai de deux mois au terme duquel, à

défaut de décision expresse, la demande est réputée acceptée ou refusée ne court qu'à compter de la réception des pièces et informations requises.

Au cours de l'instruction, le demandeur est tenu de fournir, à la requête de l'ANJ, toute information légalement justifiée et de nature à éclairer cette dernière sur des éléments contenus dans le dossier déposé.

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

Lorsque la demande d'homologation est formulée dans le cadre d'une demande d'agrément en application de l'article 11.3 de l'arrêté du 27 mars 2015 portant approbation du cahier des charges applicable aux opérateurs de jeux en ligne, l'ANJ rend une décision sur la demande d'homologation des logiciels de jeux distincte de celle relative à la demande d'agrément.

VI Exigences relatives au cycle de vie des logiciels de jeux homologués

VI.1 Cycle de vie

[E_HOM_LOH1] L'opérateur de jeu agréé ou sous droits exclusifs adressera à la fin de chaque trimestre, par le biais du canal d'échange sécurisé mis à disposition par l'ANJ, la liste des modifications apportées au cours des trois derniers mois écoulés aux différents logiciels homologués dont il dispose.

Un formulaire d'état trimestriel des modifications apportées aux logiciels homologués est mis à disposition sur le site[10] de l'ANJ et précise l'ensemble des informations demandées.

[E_HOM_LOH2] L'opérateur est tenu d'assurer la sécurité et la robustesse de son logiciel de jeu dès lors que celui-ci est mis en exploitation. Il est donc attendu de l'opérateur que celui-ci mette en œuvre l'ensemble des mesures permettant de répondre à cet objectif (exemples : audits de sécurité réguliers, maintien en condition de sécurité (MCS) du logiciel, gestion du déploiement des correctifs, principe de défense en profondeur, …).

[E_HOM_LOH3] Si l'opérateur prévoit de décommissionner (c'est-à-dire sortir d'exploitation) un logiciel de jeu homologué ou l'un de ses composants, il est tenu d'en informer les services de l'ANJ à la première des deux dates dans l'année, 1er juillet ou 1er février, qui suit l'arrêt d'exploitation du logiciel.

VI.2 Liens entre homologations logicielles et certification annuelle

[E_HOM_CERT1] L'ensemble des modifications apportées sur l'année écoulée aux différents logiciels homologués dont dispose un opérateur est audité dans le cadre des certifications annuelles.

[E_HOM_CERT2] Les vulnérabilités identifiées au niveau des logiciels de jeu lors des audits de certification annuelle devront impérativement être corrigées ou leur exploitation rendue impossible,

[10] Lien : https://anj.fr/regulation/documentation-destination-des-operateurs

dans un délai ne pouvant excéder douze mois à compter de la remise à l'ANJ des rapports d'audit de certification.

VII ANNEXES

VII.1 Annexe n°1 – Exemples de scenarii relatifs à l'homologation d'un logiciel

Sont présentés, ci-après, quelques scenarii relatifs à l'homologation du logiciel de jeu.

Scénario n°1 : nouvel agrément

Situation initiale :	➢ Le candidat opérateur vient de déposer à l'ANJ une demande d'agrément pour l'activité de poker.
Obligations de l'opérateur :	➢ Le logiciel de jeu, support de l'offre de poker du candidat opérateur est considéré, par défaut, par l'Autorité, comme non homologué pour ce candidat. Ce dernier est tenu de faire homologuer le logiciel de poker et le dispositif GNA, avant leur mise en exploitation ; ➢ Les auditeurs concentreront leur attention sur la sécurité du logiciel de jeu et du dispositif GNA, et sur la conformité d'implémentation des règles de jeu et de la mécanique de jeu.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA1]** ➢ Logiciel de poker : **[E_HOM_SEC1], [E_HOM_CFM1]** ➢ Composant GNA : **[E_HOM_GNA1]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☑ La description fonctionnelle du logiciel de jeu et de ses évolutions ; ☑ La description technique du logiciel de jeu et de ses évolutions ; ☑ La description fonctionnelle du GNA et de ses évolutions ; ☑ La description technique du GNA et de ses évolutions ; ☑ La justification des choix technologiques mis en œuvre pour le GNA ; ☑ Le rapport d'audit de la sécurité du logiciel de jeu ; ☑ Le rapport d'audit de la qualité et de la sécurité du GNA ; ☑ Le rapport d'audit de la conformité d'implémentation des règles métier ; ☑ Le règlement de jeu affichant les règles de jeu ; ☑ Le plan de remédiation ; ☑ Les codes sources du logiciel de jeu ; ☑ Les codes sources du dispositif GNA.

Scénario n°2 : nouveau jeu ajouté à un logiciel de jeu déjà homologué

Situation initiale :	➢ L'opérateur de jeu dispose d'un logiciel de paris hippiques, déjà homologué, composé : ◦ D'un moteur de jeu pour la gestion des paris, intégrant un totalisateur pour le calcul des masses d'enjeux et des rapports ; ◦ D'une application web de prise de paris (sites desktop et mobile) ; ◦ Des services API relayant les requêtes des joueurs, *via* l'application web de prise de paris, vers le moteur de jeu.
Description de l'évolution :	➢ L'opérateur de jeu a fait évoluer son logiciel de jeu afin d'étoffer son offre de paris hippiques en ajoutant un nouveau jeu de paris mutuel. ➢ Le moteur de jeu, le totalisateur et l'application web de prise de paris ont été modifiés pour intégrer le nouveau jeu à l'offre de jeu existante. ➢ Le règlement de jeu a été mis à jour pour afficher les nouvelles règles de jeu associées à ce nouveau jeu de paris.
Obligations de l'opérateur :	➢ S'agissant d'un nouveau jeu de paris impliquant de nouvelles règles de jeu et une nouvelle implémentation au niveau des codes sources du moteur de jeu, du totalisateur et de l'application web de prise de paris, l'évolution du logiciel de jeu est considérée par l'Autorité comme une évolution substantielle du logiciel de paris hippiques. ➢ Le périmètre des audits devra inclure *a minima* les composants modifiés du logiciel de jeu (i.e. le moteur de jeu, le totalisateur et l'application web de prise de paris). ➢ Les auditeurs concentreront leur attention sur la sécurité du logiciel de jeu et la conformité d'implémentation des nouvelles règles de jeu et de la mécanique de jeu associée. Ils vérifieront également la bonne implémentation des règles de calcul inhérentes au totalisateur.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA1], [E_HOM_CHA3]** ➢ Logiciel de paris hippiques : **[E_HOM_SEC1], [E_HOM_CFM1]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☑ La description fonctionnelle du logiciel de jeu et de ses évolutions ; ☑ La description technique du logiciel de jeu et de ses évolutions ; ☐ La description fonctionnelle du GNA et de ses évolutions ; ☐ La description technique du GNA et de ses évolutions ; ☐ La justification des choix technologiques mis en œuvre pour le GNA ; ☑ Le rapport d'audit de la sécurité du logiciel de jeu ; ☐ Le rapport d'audit de la qualité et de la sécurité du GNA ; ☑ Le rapport d'audit de la conformité d'implémentation des règles métier ; ☑ Le règlement de jeu affichant les règles de jeu ; ☑ Le plan de remédiation ; ☑ Les codes sources du logiciel de jeu ; ☐ Les codes sources du dispositif GNA.

Scénario n°3 : nouvelle application mobile.

Situation initiale :	➢ L'opérateur de jeu dispose d'un logiciel de paris hippiques, déjà homologué, comprenant : ◦ Un moteur de jeu pour la gestion des paris, intégrant un totalisateur pour le calcul des masses d'enjeux et des rapports ; ◦ Une application web de prise de paris (site desktop et mobile) ; ◦ Une application mobile pour iOS ; ◦ Des services API relayant les requêtes des joueurs, *via* les applications web et mobiles de prise de paris, vers le moteur de jeu.
Description de l'évolution :	➢ L'opérateur de jeu souhaite étendre l'accès à son offre de paris hippiques aux joueurs disposant d'un appareil mobile pour Android. Une nouvelle application mobile pour Android a donc été développée. ➢ Les applications mobiles pour Android et iOS se partagent la même base de code source. ➢ Les règles et la mécanique de jeu ne sont pas modifiées. ➢ La plateforme de jeu intégrant le moteur de jeu, le totalisateur, l'application web et les services API reste inchangée.
Obligations de l'opérateur :	➢ S'agissant d'un nouveau support de jeu, l'application mobile pour Android devra faire l'objet d'une homologation logicielle. ➢ Le périmètre des audits devra inclure *a minima* la nouvelle application mobile pour Android. ➢ Les auditeurs concentreront leur attention sur la sécurité de l'application mobile pour Android et des canaux de communication reliant cette application à la plateforme de jeu. ➢ Les auditeurs analyseront également la conformité d'implémentation des règles de jeu et de la mécanique de jeu, notamment au travers de la réalisation de tests dynamiques depuis la nouvelle application mobile.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA1], [E_HOM_CHA2]** ➢ Périmètre de l'audit : **[E_HOM_PER3]** ➢ Logiciel de paris hippiques : **[E_HOM_SEC1], [E_HOM_CFM1]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☑ La description fonctionnelle du logiciel de jeu et de ses évolutions ; ☑ La description technique du logiciel de jeu et de ses évolutions ; ☐ La description fonctionnelle du GNA et de ses évolutions ; ☐ La description technique du GNA et de ses évolutions ; ☐ La justification des choix technologiques mis en œuvre pour le GNA ; ☑ Le rapport d'audit de la sécurité du logiciel de jeu ; ☐ Le rapport d'audit de la qualité et de la sécurité du GNA ; ☑ Le rapport d'audit de la conformité d'implémentation des règles métier ; ☑ Le règlement de jeu affichant les règles de jeu ; ☑ Le plan de remédiation ; ☑ Les codes sources du logiciel de jeu ; ☐ Les codes sources du dispositif GNA.

Scénario n°4 : refonte applicative

Situation initiale :	➢ L'opérateur de jeu dispose d'un logiciel de jeu de poker, déjà homologué, comprenant : ◦ Un moteur de jeu de poker ; ◦ Une application web de jeu de poker (site desktop et mobile) ; ◦ Une application mobile pour iOS ; ◦ Une application mobile pour Android ; ◦ Des services API relayant les requêtes des joueurs, *via* les applications web et mobile, vers le moteur de jeu.
Description de l'évolution :	➢ L'opérateur a opéré une refonte de son moteur de jeu de poker. Il envisage de remplacer son moteur de jeu, déjà homologué mais vieillissant, par un nouveau moteur de jeu, entièrement redéveloppé. La refonte applicative est effectuée à iso-fonctionnalité de l'ancien moteur de jeu. ➢ Les règles et la mécanique de jeu ne sont pas modifiées. ➢ À l'exception du moteur de jeu, les autres composants du logiciel de jeu restent inchangés. ➢ Le dispositif GNA, déjà homologué, n'est pas concerné par cette refonte.
Obligations de l'opérateur :	➢ La nouvelle version du moteur de jeu de poker s'assimile à un nouveau composant du logiciel de jeu. Elle est donc soumise à l'obtention d'une homologation préalablement à sa mise en exploitation. ➢ Le périmètre des audits devra inclure *a minima* la nouvelle version du moteur de jeu, une attention particulière devant être portée à la conformité de l'implémentation des règles de jeu et des primitives de jeu.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA1], [E_HOM_CHA3]** ➢ Périmètre de l'audit : **[E_HOM_PER3]** ➢ Logiciel de poker : **[E_HOM_SEC1], [E_HOM_CFM1]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☑ La description fonctionnelle du logiciel de jeu et de ses évolutions ; ☑ La description technique du logiciel de jeu et de ses évolutions ; ☐ La description fonctionnelle du GNA et de ses évolutions ; ☐ La description technique du GNA et de ses évolutions ; ☐ La justification des choix technologiques mis en œuvre pour le GNA ; ☑ Le rapport d'audit de la sécurité du logiciel de jeu ; ☐ Le rapport d'audit de la qualité et de la sécurité du GNA ; ☑ Le rapport d'audit de la conformité d'implémentation des règles métier ; ☑ Le règlement de jeu affichant les règles de jeu ; ☑ Le plan de remédiation ; ☑ Les codes sources du logiciel de jeu ; ☐ Les codes sources du dispositif GNA.

Scénario n°5 : correction de bogues

Situation initiale :	➢ L'opérateur de jeu dispose d'un logiciel de paris hippiques, déjà homologué, composé : ◦ D'un moteur de jeu pour la gestion des paris, intégrant un totalisateur pour le calcul des masses d'enjeux et des rapports ; ◦ D'une application web de prise de paris (sites desktop et mobile) ; ◦ Des services API relayant les requêtes des joueurs, *via* l'application web de prise de paris, vers le moteur de jeu.
Description de l'évolution :	➢ L'opérateur de jeu a réalisé quelques corrections de bogues au niveau de son site mobile.
Obligations de l'opérateur :	➢ Les corrections apportées au logiciel de jeu, sous réserve qu'elles ne modifient pas la mécanique de jeu, les règles de jeu et leur implémentation, ainsi que les mécanismes de sécurité déjà en place, sont considérées comme des modifications mineures. Elles ne donnent donc pas lieu à une nouvelle homologation du logiciel de jeu. ➢ En cas de doute sur le caractère substantiel des modifications apportées au logiciel de jeu, la consultation de l'ANJ est vivement recommandée.
Exigences :	➢ Champ d'application : **[E_HOM_CHA3]**
Nécessité d'une homologation ?	➢ NON

Scénario n°6 : modifications mineures

Situation initiale :	➢ L'opérateur de jeu dispose d'un logiciel de jeu en ligne, homologué, composé : ◦ D'un moteur de jeu ; ◦ D'une application web accessible aux joueurs (client de jeu) ; ◦ Des services API relayant les requêtes des joueurs, *issues de* l'application web, vers le moteur de jeu.
Description de l'évolution :	➢ L'opérateur de jeu a mis à jour l'apparence de son site de jeu en ligne. Seul l'aspect visuel du site est modifié (*i.e.* les couleurs, images, positionnement et la taille des éléments de l'interface, ajout d'une nouvelle rubrique d'information). ➢ Les fonctionnalités du logiciel de jeu n'ont pas été modifiées.
Obligations de l'opérateur :	➢ La mécanique de jeu, les règles de jeu, l'implémentation associée et les mécanismes de sécurité du logiciel de jeu restant inchangés, les modifications opérées peuvent être assimilées à des modifications mineures. Elles ne donnent pas lieu à une nouvelle homologation du logiciel de jeu.
Exigences :	➢ Champ d'application : **[E_HOM_CHA3]**
Nécessité d'une homologation ?	➢ NON

Scénario n°7 : changement de fournisseur de solution de jeu

Situation initiale :	➢ L'offre de poker de l'opérateur de jeu est hébergée sur la plateforme de jeu fournie par un prestataire A.
Description de l'évolution :	➢ L'opérateur de jeu migre son offre de poker sur la plateforme de jeu d'un nouveau prestataire B. ➢ À l'issue de la migration de l'offre, le logiciel de poker du prestataire A, homologué, sera délaissé au profit du logiciel de poker du prestataire B (dont les clients lourds, les applications mobiles et le dispositif GNA). ➢ Le prestataire B fournit déjà son logiciel de poker à d'autres opérateurs de jeu agréés. Ce logiciel de poker est déjà homologué pour ces opérateurs et n'a fait l'objet d'aucune évolution substantielle depuis la dernière homologation.
Obligations de l'opérateur :	➢ L'homologation d'un logiciel de jeu n'est valable que pour l'opérateur de jeu qui en a fait la demande expresse auprès des services de l'ANJ. ➢ En conséquence, le logiciel de poker du prestataire B (dispositif GNA y compris) n'est pas homologué pour l'opérateur qui opère la migration de son offre de poker et sera considéré, par l'Autorité, comme un nouveau logiciel non encore homologué. L'opérateur devra donc soumettre, en son nom, à l'ANJ, une demande d'homologation du logiciel de poker du prestataire B qu'il envisage d'exploiter dans le cadre de son activité de poker. ➢ Les auditeurs concentreront leur attention sur la sécurité du logiciel de jeu, des clients de jeu et du dispositif GNA. ➢ La conformité d'implémentation des fonctions métier (règles de jeu, mécanique de jeu) a déjà été vérifiée dans le cadre des précédentes homologations réalisées auprès des autres opérateurs exploitant ce logiciel de jeu. Sous réserve de n'avoir fait l'objet d'aucune évolution substantielle, l'audit de conformité d'implémentation des fonctions métier n'est donc pas nécessaire.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA1], [E_HOM_CHA6]** ➢ Périmètre de l'audit : **[E_HOM_PER1], [E_HOM_PER2]** ➢ Logiciel de poker : **[E_HOM_SEC1], [E_HOM_GNA1], [E_HOM_CFM1]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☑ La description fonctionnelle du logiciel de jeu et de ses évolutions ; ☑ La description technique du logiciel de jeu et de ses évolutions ; ☑ La description fonctionnelle du GNA et de ses évolutions ; ☑ La description technique du GNA et de ses évolutions ; ☑ La justification des choix technologiques mis en œuvre pour le GNA ; ☑ Le rapport d'audit de la sécurité du logiciel de jeu ; ☑ Le rapport d'audit de la qualité et de la sécurité du GNA ; ☐ Le rapport d'audit de la conformité d'implémentation des règles métier ; ☑ Le règlement de jeu affichant les règles de jeu ; ☑ Le plan de remédiation ;

	☑ Les codes sources du logiciel de jeu ; ☑ Les codes sources du dispositif GNA.

Scénario n°8 : mise à jour du dispositif GNA

Situation initiale :	➢ L'opérateur de jeu, pour son activité de poker, dispose d'un dispositif GNA, déjà homologué.
Description de l'évolution :	➢ L'opérateur de jeu a mis à jour son dispositif GNA associé à son logiciel de jeu de poker, en vue d'améliorer sa sécurité. Pour ce faire, l'ancien algorithme du GNA a été remplacé par un algorithme présentant des caractéristiques censées rendre le dispositif GNA robuste face à certaines nouvelles attaques permettant d'en prédire la séquence de valeurs produites.
Obligations de l'opérateur :	➢ Les modifications opérées impactent directement la sécurité du dispositif GNA, rendant caduques, les précédentes analyses menées lors de la dernière homologation du dispositif. Cette évolution du dispositif GNA sera donc considérée par l'Autorité comme une évolution substantielle du logiciel de jeu. La nouvelle version du dispositif GNA devra donc faire l'objet d'une nouvelle homologation avant sa mise en production. ➢ Les auditeurs concentreront leur attention sur la qualité et la sécurité du dispositif GNA.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA3]** ➢ Périmètre de l'audit : **[E_HOM_PER3]** ➢ Logiciel de poker : **[E_HOM_GNA1]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☐ La description fonctionnelle du logiciel de jeu et de ses évolutions ; ☐ La description technique du logiciel de jeu et de ses évolutions ; ☑ La description fonctionnelle du GNA et de ses évolutions ; ☑ La description technique du GNA et de ses évolutions ; ☑ La justification des choix technologiques mis en œuvre pour le GNA ; ☐ Le rapport d'audit de la sécurité du logiciel de jeu ; ☑ Le rapport d'audit de la qualité et de la sécurité du GNA ; ☐ Le rapport d'audit de la conformité d'implémentation des règles métier ; ☐ Le règlement de jeu affichant les règles de jeu ; ☑ Le plan de remédiation ; ☐ Les codes sources du logiciel de jeu ; ☑ Les codes sources du dispositif GNA.

Scénario n°9 : refonte du logiciel de paris hippiques disponible sur les bornes automatiques en point de vente.

Situation initiale :	➢ L'opérateur de jeu dispose d'un logiciel de paris hippiques pour son offre de paris sous droits exclusifs, déjà homologué, comprenant : ◦ Un moteur de jeu pour la gestion des paris, intégrant un totalisateur pour le calcul des masses d'enjeux et des rapports ; ◦ D'un logiciel, installé sur les bornes automatiques, en point de vente, destiné à la prise de paris et aux paiements ; ◦ Des services API relayant les requêtes des joueurs issues des bornes automatiques, vers le moteur de jeu.
Description de l'évolution :	➢ Dans le cadre de son projet de modernisation des bornes automatiques disponibles en point de vente, l'opérateur envisage de remplacer les bornes par de nouvelles bornes reposant sur un matériel plus récent. Sur ce nouveau matériel sera également déployé un nouveau logiciel de jeu destiné à la prise de paris et aux paiements. ➢ Les règles, la mécanique de jeu et l'offre de jeu restent inchangées. ➢ La plateforme de jeu intégrant le moteur de jeu, le totalisateur et les services API, reste inchangée.
Obligations de l'opérateur :	➢ S'agissant d'un nouveau support de jeu et d'un nouveau logiciel de jeu, le nouveau logiciel de jeu est soumis à l'obtention d'une homologation. ➢ Les auditeurs concentreront leur attention sur la sécurité du nouveau logiciel, du nouveau matériel et des canaux de communication reliant le logiciel sur borne à la plateforme de jeu. ➢ Les auditeurs analyseront également la conformité d'implémentation des règles de jeu et de la mécanique de jeu au niveau du nouveau logiciel qui sera déployé sur les nouvelles bornes.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA1], [E_HOM_CHA7]** ➢ Périmètre de l'audit : **[E_HOM_PER3]** ➢ Logiciel de paris hippiques : **[E_HOM_SEC1], [E_HOM_CFM1]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☑ La description fonctionnelle du logiciel de jeu et de ses évolutions ; ☑ La description technique du logiciel de jeu et de ses évolutions ; ☐ La description fonctionnelle du GNA et de ses évolutions ; ☐ La description technique du GNA et de ses évolutions ; ☐ La justification des choix technologiques mis en œuvre pour le GNA ; ☑ Le rapport d'audit de la sécurité du logiciel de jeu ; ☐ Le rapport d'audit de la qualité et de la sécurité du GNA ; ☑ Le rapport d'audit de la conformité d'implémentation des règles métier ; ☑ Le règlement de jeu affichant les règles de jeu ; ☑ Le plan de remédiation ; ☑ Les codes sources du logiciel de jeu ; ☐ Les codes sources du dispositif GNA.

Scénario n°10 : nouveau logiciel d'impression de tickets physiques de jeu de grattage.

Situation initiale :	➢ L'opérateur s'est rapproché d'un imprimeur spécialisé et a contractualisé avec ce dernier pour l'impression d'un nombre défini de tickets physiques de jeu de grattage.
Obligations de l'opérateur :	➢ Le logiciel d'impression de tickets est soumis à l'obtention de l'homologation logicielle car il est porteur d'une partie de la mécanique de jeu en introduisant de l'aléa lors de l'impression des tickets.
Exigences principales :	➢ Champ d'application : **[E_HOM_CHA1], [E_HOM_CHA8]**
Nécessité d'une homologation du logiciel de jeu ?	➢ OUI
Contenu du dossier de demande d'homologation	☑ Le formulaire de demande d'homologation du logiciel de jeu, renseigné ; ☑ La description de la procédure de génération de tickets et du dispositif d'impression de tickets ; ☑ La description du processus de qualification de l'imprimeur ; ☑ La présentation des éléments relatifs à la sécurité présentés dans le dossier de qualification qui ont conduit à retenir l'imprimeur ; ☑ La présentation des clauses contractuelles dont disposent l'opérateur de jeu à l'égard de ses imprimeurs, relatives à la sécurité du dispositif d'impression et de son auditabilité ; ☑ Les rapports d'audits réalisés auprès des imprimeurs portant sur le logiciel d'impression, sur la qualité du GNA sur lequel s'appuie le logiciel pour produire les tickets et sur les moyens de sécurisation du dispositif d'impression.

VII.2 Annexe n°2 – Types de prestations d'audit attendues

VII.2.1 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.

VII.2.2 Test dynamique

Une prestation de test dynamique a pour objectif de vérifier la présence d'anomalies au niveau du logiciel de jeu 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.

VII.2.3 Audit de code source

Une prestation d'audit de code source a pour objectif de vérifier la présence d'anomalies au niveau du logiciel de jeu 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 externe …) ;
- Sur le plan fonctionnel, l'analyse consiste à valider la bonne implémentation des fonctions de sécurité et des fonctions métiers relatives à la mécanique de jeu et aux règles de jeu affichées aux utilisateurs 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.

Afin de pouvoir garantir l'absence de modification des logiciels audités, une empreinte cryptographique des différents fichiers devra être fournie dans le rapport. Dans le cas de code source imposant, des mécanismes d'empreinte « de répertoires » pourront être fournis. Le mécanisme d'empreinte devra être clairement détaillé et reproductible (cf. [E_HOM_AUD6]).

VII.2.4 Audit intrusif

L'audit intrusif du logiciel de jeu 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.

VII.2.5 Audit intrusif différentiel

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

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

VII.3 Annexe n°3 – 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.

VII.3.1 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 intrinsèquement 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.

VII.3.2 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 élevé notamment en raison du développement d'outils spécifiques et ciblés.

VII.3.3 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 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

VII.4 Annexe n°4 – 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