Matrice des exigences de la certification

(version 1.0 du 07/10/2022)

Notice	
Point de contrôle	Point de contrôle noté « En ». Remarque : la numérotation du point de contrôle est propre à ce document.
Référence	Référence au document (Exigences Techniques et ses annexes, voire Loi et Décret) et de la partie renseignant le point de contrôle.
Libellé	Description du point de contrôle.
Niveau de criticité	Niveau de criticité du point de contrôle : - le niveau de criticité 1 correspond essentiellement aux exigences liées à l'existence d'une documentation ou d'une procédure (exemple : politique de sécurité, procédure de mise à jour, de durcissement d'un système, etc.) ; - le niveau de criticité 2 correspond essentiellement aux exigences pour lesquelles une non-conformité a un impact opérationnel : défaut d'application d'une procédure, défaut de respect des exigences opérationnelles de conformité et de sécurité définies par l'ANJ, ou encore défaut de suivi des règles de bonnes pratiques en sécurité des systèmes d'information ; - le niveau de criticité 3 correspond aux exigences dont le non-respect est jugé très critique, le plus souvent en termes de conformité règlementaire, ou en termes de sécurité (sur un composant exposé et/ou manipulant des données critiques).
Elément d'analyse de la certification à 6 mois	Éléments sur lesquels l'analyse s'appuie sur : 1) les documents remis par l'opérateur, par exemple : - le dossier de définition de la plateforme d'hébergement du SMA ; - la documentation fonctionnelle et technique du logiciel capteur ; - le rapport de certification CSPN réalisé à l'occasion de la certification du coffre-fort et la cible de sécurité de cette certification ; - les rapports d'audits de sécurité déjà réalisés par l'opérateur – en particulier si le capteur est intégré à la plateforme de jeu – ou encore les rapport d'analyse de la maturité SSI de l'opérateur ; 2) les audits réalisés par le certificateur, visant à comprendre et valider techniquement les points de contrôle, et apprécier les éléments déclaratifs décrits par l'opérateur dans sa documentation, en particulier : - l'audit fonctionnel, technique et de sécurité du composant logiciel capteur ; - l'audit de configuration de premier niveau de l'infrastructure d'hébergement du SMA. Le rapport associé est noté « audit de configuration des plateformes d'hébergement » dans la suite du document. Le niveau d'analyse demandé peut être précisé : « analyse de premier niveau » signifie qu'une analyse pragmatique et de bon sens est attendue. Au contraire, un « avis d'expert » sera plus technique et étayé (élément de configuration, extrait de code, etc.).
Elément d'analyse de la certification annuelle	Éléments sur lesquels l'analyse s'appuie sur : 1) les documents remis par l'opérateur, par exemple : - le dossier de définition, mis à jour, de la plateforme d'hébergement du SMA et de la plateforme de jeu ; - la documentation fonctionnelle et technique actualisée du logiciel capteur et de la plateforme de jeu ; - le rapport de certification initiale à 6 mois du composant SMA ; - les rapports d'homologation effectués sur les logiciels de jeu ; - les rapports d'audits de sécurité réalisés par l'opérateur indépendamment des certifications prévues par la réglementation ; - les attestations d'absence de modification d'un composant (exemple : capteur) ; - les plans de remédiation des non-conformités et des vulnérabilités identifiées lors des précédentes certifications. 2) les audits réalisés par le certificateur, visant à comprendre et valider techniquement les points de contrôle, et apprécier les éléments déclaratifs décrits par l'opérateur dans sa documentation, en particulier : - les audits d'architecture technique de la plateforme de jeu ; - les audits de configuration de premier niveau de l'infrastructure d'hébergement du SMA et de la plateforme de jeu. Ces rapports sont notés « audits de configuration des plateformes d'hébergement » dans la suite du document ; - les audits applicatifs intrusifs qui portent sur les composants logiciels de la plateforme de jeu qui ne font pas l'objet d'homologation. Le niveau d'analyse demandé peut être précisé : « analyse de premier niveau » signifie qu'une analyse pragmatique et de bon sens est attendue. Au contraire, un « avis d'expert » sera plus approfondi, technique et étayé (élément de configuration, extrait de code, etc.). La certification annuelle repose sur un socle d'analyses obligatoires, pouvant faire l'objet d'une actualisation. Les ET5 indiquent les analyses pour lesquelles cette actualisation peut être réalisée.
Commentaires ANJ	Précisions apportées par l'ANJ, afin d'aider à la compréhension du point de contrôle.
Rapports concernés	Références du ou des documents ainsi que des chapitres sur lesquels l'analyse a été effectuée, le cas échéant, par l'organisme certificateur.
Conformité	Constat de l'analyse menée par l'organisme certificateur.
Commentaires certificateur	Précisions apportées par l'organisme certificateur, afin d'aider à la compréhension des résultats l'analyse du point de contrôle.

Matrice des exigences de la certification

(version 1.0 du 07/10/2022)

Exigence de la certification à 6 mois ?	Exigence de la certification annuelle ?	Point de contrôle	Libellé	Niveau de criticité	Éléments d'analyse	Commentaires ANJ	Rapports concernés	Conformité	Commentaires certificateur
	OUI	**PARTIE 1 - Suivi des audits de sécurité, certifications et homologations**							
	OUI	E1	Dans le cadre de la mission générale de contrôle de l'ANJ, les organismes certificateurs réalisent des audits de sécurité afin de vérifier le niveau de maturité SSI des opérateurs ainsi que le niveau de sécurité atteint par les dispositifs SMA et les plateformes de jeux. Un accès au site ainsi qu'à l'ensemble des équipements et des données de la ou des plateformes de jeux devra être accordé à l'ANJ ou aux organismes certificateurs mandatés.	3	Documentation remise par l'opérateur. Audit de configuration des plateformes d'hébergement.	L'opérateur devra notamment donner à l'organisme certificateur mandaté l'ensemble des accès et éléments de configuration requis afin que ce dernier puisse procéder aux contrôles attendus dans le cadre de sa mission d'audit.		Conforme	
	OUI	E2	L'opérateur doit corriger les éventuelles vulnérabilités mineures, importantes, majeures ou critiques, constatées à l'issue des audits de sécurité. Si aucune mesure de sécurité ne permet de les corriger directement, l'opérateur devra proposer des mesures de contournement provisoire afin d'éviter l'exploitation de ces vulnérabilités. Le plan de remédiation associé et établi par l'opérateur devra être communiqué à l'ANJ et à l'organisme certificateur mandaté.	3	Documentation remise par l'opérateur, notamment : - rapports d'homologation des logiciels de jeu ; - rapports d'audit de configuration réalisés dans le cadre de la certification initiale à 6 mois du dispositif SMA ou dans le cadre des certifications annuelles antérieures, le cas échéant ; - rapports d'audits de sécurité effectués sur les systèmes d'information de l'opérateur, qu'ils soient réalisés par l'ANJ ou un organisme mandaté par l'ANJ ; - plans de remédiation associés aux différentes vulnérabilités constatées.	Il s'agira de s'assurer que toutes les vulnérabilités constatées à l'issue des audits de sécurité font l'objet d'une remédiation et que les recommandations les plus pertinentes sont bien appliquées.		Conforme avec réserve	
	OUI	E3	L'opérateur informe l'ANJ des évolutions substantielles opérées (ex : mise en place d'une nouvelle technologie) au sein de sa plateforme.	2	Documentation remise par l'opérateur.	L'opérateur devra notamment présenter au certificateur la liste des changements effectués au niveau de ses systèmes d'information (capteur + plates-formes de jeu, aussi bien au niveau des logiciels que des infrastructures) et les éléments communiqués à l'ANJ, depuis le dépôt de la demande d'agrément ou la dernière certification annuelle effectuée, le cas échéant.		Non conforme	
	OUI	E4	L'opérateur communique à l'ANJ les résultats des audits de sécurité réalisés sur ses plateformes de jeux par des organismes tiers.	1	Documentation remise par l'opérateur.				
	OUI	E5	Les nouveaux logiciels de jeu doivent être systématiquement homologués avant mise en exploitation.	3	Documentation remise par l'opérateur.	L'opérateur devra lister les versions des logiciels de jeu qu'il emploie (côté client comme côté serveur) et les rapports et décisions d'homologation correspondants. Cette exigence inclut notamment les éventuels logiciels clients déployés sur smartphones ou les interfaces correspondantes côté serveur. Un avis d'expert est attendu de la part du certificateur sur les homologations réalisées au regard de l'historique des modifications apportées aux logiciels, côté client comme côté serveur.			
	OUI	**PARTIE 2 - PSSI : Politique et schéma directeur en sécurité des systèmes d'information de l'opérateur**							
	OUI	E6	L'opérateur possède un schéma directeur en sécurité des systèmes d'information, ou un document équivalent. Il en précisera la date de son début d'application et la périodicité de mise à jour. Il précisera également s'il est intégré dans le schéma directeur informatique et en fournira la dernière version et, si possible, la version précédente.	1	Documentation remise par l'opérateur + analyse de premier niveau.	L'analyse devra plus généralement porter sur la plateforme d'hébergement du SMA et la plateforme de jeu.			
	OUI	E7	L'opérateur possède une politique de sécurité des systèmes d'information. Si un tel document n'existe pas, il indiquera, si un ou des documents remplissent une fonction similaire. Cette politique de sécurité doit aborder les sujets suivants :	1					
	OUI		- Eléments stratégiques :						
	OUI	E8	- le périmètre d'application de la politique de sécurité, par exemple en termes de domaines d'activités ou de systèmes d'information ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E9	- les enjeux et orientations stratégiques, à travers la formalisation des enjeux liés au périmètre précédemment défini ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E10	- les aspects légaux et réglementaires liés au périmètre d'application de la politique de sécurité ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E11	- une échelle de besoins qui comportera une pondération et des valeurs de référence selon les critères de sécurité choisis, ainsi qu'une liste d'impacts enrichis d'exemples ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E12	- une description des besoins de sécurité des domaines d'activité de l'opérateur, selon l'échelle de besoins présentée dans la partie précédente ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E13	- une analyse des menaces retenues et non retenues pour le périmètre de l'étude, avec des justifications.	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI		- Règles de sécurité, classées par thème :						
	OUI	E14	- organisation : organisation de la SSI, gestion des risques, sécurité et cycle de vie, assurance et certification, évolution de la PSSI ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E15	- mise en oeuvre : aspects humains, plan de secours, gestion des incidents, sensibilisation et formation, exploitation, sécurité physique ;	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E16	- technique : identification / authentification, contrôle d'accès logique, journalisation, chiffrement.	1	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E17	L'opérateur décline les éléments exigés par sa politique de sécurité. Cette déclinaison technique et détaillée fait le lien entre la politique de sécurité et toutes les procédures liées aux systèmes d'information, en établissant des moyens de sécurisation, aussi bien organisationnels que techniques, des systèmes d'information et en assurant le suivi de ces moyens dans le temps.	2	Documentation remise par l'opérateur + analyse de premier niveau.				
	OUI	E18	L'opérateur doit imposer des exigences de sécurité aux divers sous-traitants avec lesquels des relations contractuelles sont établies, il les fournira si possible.	1	Documentation remise par l'opérateur + analyse de premier niveau.				
OUI	OUI	**PARTIE 3 - Architecture globale et procédures d'administration et d'exploitation**							
OUI	OUI		L'organisation mise en place pour gérer le système d'information de l'opérateur doit s'appuyer sur une documentation et des procédures permettant de suivre ses évolutions. La documentation comporte :						

OUI	OUI	E19		- la déclinaison sous forme de procédures de la politique de sécurité ;	1	Documentation remise par l'opérateur + analyse de premier niveau.					
OUI	OUI	E20		- une description fonctionnelle de l'infrastructure d'hébergement du SMA, précisant les différents composants, leurs fonctions et les flux transitant par ces derniers.	1	Documentation remise par l'opérateur + avis d'expert.					
OUI	OUI	E21	La documentation des infrastructures d'hébergement du SMA et de la plateforme de jeu de l'opérateur qui intègre un volet technique et procédural fait l'objet d'un dossier appelé « dossier de définition ».		1	Documentation remise par l'opérateur + analyse de premier niveau.					
OUI	OUI	E22	L'opérateur est responsable, sur toute la durée de validité de l'agrément ou de l'autorisation d'exploitation sous droits exclusifs, de la tenue à jour et de la cohérence du « dossier de définition ». Chaque modification du dossier fait l'objet d'une nouvelle remise de document à l'ANJ.		1	Documentation remise par l'opérateur + analyse de premier niveau.	Les modifications du « dossier de définition » intervenues dans l'année sont compilées et présentées à l'organisme certificateur. Cette soumission via la certification annuelle tient lieu de remise à l'ANJ.				
OUI	OUI		La documentation des infrastructures d'hébergement du SMA et de la plateforme de jeu qui intègre un volet technique et procédural rassemble les informations suivantes :								
OUI	OUI	E23		- une description de l'architecture, en termes de composants techniques, plan d'adressage et de nommage, de flux, en mentionnant les protocoles associés, sens d'établissement des connexions, règles de filtrage, etc. ;	2	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.					
OUI	OUI	E24		- les spécifications techniques du système d'information, en particulier les configurations à jour des équipements qui le composent ;	2	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.					
OUI	OUI	E25		- la liste descriptive précise de tous les composants, avec le recensement d'éléments factuels, comme les versions des logiciels utilisées, les contrats de maintenance, les configurations et l'état des modifications effectuées, etc. ;	2	Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.					
OUI	OUI	E26		- une liste des procédures d'exploitation, notamment : - procédures de gestion des journaux ; - procédures de gestion des alertes ; - procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.) ; - procédures de gestion des composants à mise à jour fréquente (anti-virus, systèmes de détection d'intrusion, le cas échéant) ; - procédures de mise à jour en cas d'édition d'un correctif de sécurité critique ; - procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent ; - procédures d'exploitation des composants du SI (serveurs, routeurs) ; - procédures d'exploitation des comptes et mots de passe ; - procédures de gestion des composants infogérés ; - procédures relative à la sécurité physique (gardiennage, etc.) ; - procédures de gestion des sauvegardes et des restaurations ; - procédures de veille technologique ; - procédures pour la télé-administration ; - procédures de gestion des tableaux de bord SSI.	1	Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.					
	OUI	**PARTIE 4 - Architecture réseau**									
	OUI	E27	Les systèmes d'information de l'opérateur doivent faire l'objet d'une segmentation et d'un filtrage réseau en accord avec le principe de défense en profondeur, notamment au niveau des réseaux de services, d'administration et de supervision des plateformes.		2	Documentation remise par l'opérateur + avis d'expert.	Un schéma de niveau 3 doit impérativement être réalisé par le certificateur. Ce schéma devra faire apparaitre les adresses IP des machines les plus importantes.				
	OUI		L'opérateur met en œuvre un cloisonnement du réseau à l'aide de mécanismes de filtrage de niveau 3 (modèle OSI) au minimum, au moins entre les zones suivantes :								
	OUI	E28		- les zones dédiées aux serveurs, avec un cloisonnement supplémentaire en fonction du niveau de sensibilité identifié pour chacun par la politique de sécurité : - les serveurs métiers (serveurs d'applications, systèmes de gestion de base de données), - les serveurs d'infrastructure (serveurs d'authentification, serveurs de messagerie, serveurs de fichiers, serveurs de distribution de logiciels), - les équipements d'infrastructure réseau (routeurs, commutateurs), - les serveurs de tests, de développement et de préproduction ;	2	Documentation remise par l'opérateur, en particulier : a) les rapports d'audits de configuration des plateformes d'hébergement réalisés dans le cadre de la vérification initiale de la plateforme de jeu ; b) les rapports d'audits de configuration de la certification à 6 mois du dispositif SMA ; c) les rapports d'audit de configuration des certifications annuelles antérieures, le cas échéant. Audit de configuration des plateformes d'hébergement. Audit d'architecture technique de la plateforme de jeu.				
	OUI	E29		- la zone des équipements dédiés à l'administration, l'exploitation et la supervision du système d'information. Cette zone qui héberge notamment les postes de travail des administrateurs et les serveurs de supervision devra faire l'objet d'une attention particulière compte tenu des accès privilégiés qu'ils sont susceptibles d'accorder sur les ressources les plus critiques du SI ;	2		Le filtrage des interfaces d'administration doit s'effectuer au niveau 3 (IP) et non pas seulement au niveau 7 (applicatif).				
	OUI	E30		- la ou les zones dédiées aux postes de travail des utilisateurs, le cas échéant, avec un découpage supplémentaire dont la granularité pourra varier selon les missions des différents services métiers et la criticité de l'information dont ils ont la responsabilité.	2						
	OUI	E31	La politique de filtrage réseau adoptée respecte le principe du moindre privilège : les règles de filtrage sont élaborées suivant un principe de liste blanche.		2	Audit de configuration des plateformes d'hébergement. Audit d'architecture technique de la plateforme de jeu.	L'analyse devra prendre en compte le filtrage en entrée et en sortie.				
OUI	OUI	E32	L'opérateur met en œuvre des mécanismes de sécurité afin d'assurer une défense contre les attaques classiques sur IP et les protocoles associés, en particulier par rapport aux attaques en déni de service réseau.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.					
OUI	OUI	**PARTIE 5 - Maintien en conditions de sécurité**									
OUI	OUI	E33	Au titre de la maintenance et du maintien en conditions de sécurité, l'opérateur suit les évolutions logicielles des éditeurs de façon à être en mesure de se procurer les correctifs de sécurité mis à disposition régulièrement. L'opérateur surveille au moins les avis et les alertes d'un CERT, comme le CERTA (https://www.certa.ssi.gouv.fr). L'opérateur applique les correctifs de sécurité qui sont proposés par les éditeurs, dans les documents du CERT ou demandés explicitement par l'ANJ, le cas échéant.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.					
OUI	OUI	E34	L'opérateur doit a minima prohiber l'utilisation, sur ses plateformes, des systèmes et logiciels obsolètes, c'est-à-dire qui ne sont plus maintenus par leur éditeurs et ne bénéficient plus de support correctif.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.					
OUI	OUI		Si aucun correctif de sécurité n'est disponible auprès de l'éditeur :								
OUI	OUI	E35		- l'opérateur suit les recommandations de ce dernier ou d'un CERT, dans le cadre d'un contournement provisoire ;	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.					
OUI	OUI	E36		- si le contournement nécessite la désactivation d'une fonctionnalité indispensable au système, l'opérateur s'engage à proposer des mesures permettant d'éviter l'exploitation de la vulnérabilité.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.					

OUI	OUI	E37	L'opérateur tient à jour le « dossier de définition » avec la liste des correctifs de sécurité appliqués sur les serveurs et communique à l'ANJ la version actualisée du document.		1	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.				
OUI	OUI	**PARTIE 6 - Sécurisation des communications et contrôle des accès d'administration**								
	OUI	E38	L'intégralité des échanges de données doit être sécurisée à l'aide de procédés cryptographiques permettant de garantir l'authentification des composants, la confidentialité et l'authenticité des communications. Tous les échanges de fichiers (données d'administration, mise à jour de contenu, etc.) doivent se faire en utilisant des mécanismes reposant sur des algorithmes de chiffrement reconnus et des protocoles normalisés par l'IETF (IPsec, TLS, SSH, etc.). Ces échanges comprennent principalement les communications suivantes : - les communications entre opérateur et l'ANJ ; - les communications réseaux entre joueurs et opérateur ; - les communications réseaux entre les modules au sein du SMA.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI		Les accès d'administration aux équipements, dont les équipements du SMA, doivent être protégés à l'aide des mécanismes suivants :							
OUI	OUI	E39		- en priorité, une authentification par certificat X.509v3, par clef publique RSA ou par système à deux facteurs (dont un mot de passe à usage unique), si les applications et les systèmes le supportent ;	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E40		- ou bien une authentification par mot de passe, avec des règles de composition et de renouvellement conformes aux bonnes pratiques recommandées par le CERTA, que l'opérateur détaillera. Ces mots de passe devront être employés dans le cas de protocoles d'authentification par défi/réponse ;	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.	Les authentifications en clair sont prohibées, un chiffrement des communications est obligatoire. La mesure doit permettre de prouver la robustesse des mots de passe.			
OUI	OUI	E41		- un contrôle d'accès basé sur les adresses IP est réalisé.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	**PARTIE 7 - Gestion des configurations**								
OUI	OUI	E42	À l'issue de la mise en œuvre d'un nouvel équipement ou de l'installation d'une nouvelle application, l'opérateur met à disposition de l'ANJ la version à jour du « dossier de définition » incluant toutes les informations relatives à la configuration de ce nouvel élément.		1	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.				
OUI	OUI	E43	Les composants systèmes, réseau et applicatifs mis en œuvre par l'opérateur doivent avoir fait l'objet d'un durcissement en termes de sécurité : restriction des applications exécutées au démarrage, limitation du nombre d'applications en écoute sur le réseau, désactivation des fonctionnalités inutiles voire dangereuse (interface d'administration de serveurs d'application), suppression des comptes et mots de passe constructeurs, etc.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E44	Afin de détecter d'éventuelles erreurs de manipulation mais aussi le résultat d'attaques, l'intégrité des fichiers de configuration des équipements doit être vérifiée régulièrement. Cette vérification doit pouvoir être faite sur demande de l'ANJ et un rapport de diagnostic doit pouvoir lui être transmis.		2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	**PARTIE 8 - Gestion de la sécurité dans les cycles de développement**								
OUI	OUI	E45	L'opérateur gère la sécurité à chaque étape du cycle de développement de ses systèmes, dans les phases de définition, de développement, d'exploitation et d'utilisation, puis de maintenance et d'évolution.		2	Documentation remise par l'opérateur.	Cette exigence couvre, outre la vérification de la procédure technique liée à cette transmission, le devoir de l'opérateur de l'effectuer.			
OUI	OUI	E46	L'opérateur contractualise avec ses prestataires le respect d'un référentiel de développement sécurisé pour les projets dont il externalise la prise en charge.		1	Audit applicatif intrusif. Documentation remise par l'opérateur.				
OUI	OUI		Le référentiel de développement sécurisé doit en particulier aborder le problème de la validation des paramètres, notamment :							
OUI	OUI	E47		- vérifier toutes les données transmises par l'utilisateur selon des critères de taille, type et caractères autorisés, et selon un mécanisme de liste blanche ;	2	Audit applicatif intrusif. Documentation remise par l'opérateur.				
OUI	OUI	E48		- vérifier les données en entrée et en sortie ;	2	Audit applicatif intrusif. Documentation remise par l'opérateur.				
OUI	OUI	E49		- utiliser une fonction de vérification des données identique et centralisée.	2	Audit applicatif intrusif. Documentation remise par l'opérateur.				
OUI	OUI	E50	L'opérateur doit pouvoir transmettre à l'ANJ l'ensemble de codes sources des composants de logiciels de jeux au sens du volume des exigences techniques (ET2) utilisés sur ses plateformes, si cette dernière le lui demande.		3	Documentation remise par l'opérateur.				
OUI	OUI	**PARTIE 9 - Gestion des sauvegardes des données**								
OUI	OUI	E51	L'opérateur fournit les moyens de mettre en œuvre un service d'archivage afin d'assurer la conservation de l'ensemble de ses données de traitement, et en particulier celles stockées dans le composant coffre-fort du SMA.		3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E52	Ces sauvegardes sont mises à disposition de l'ANJ par l'opérateur pour consultation et archivage.		2	Documentation remise par l'opérateur.				
OUI	OUI	E53	Le type de support et le format de la sauvegarde sont indiqués par l'opérateur pour permettre à l'ANJ de vérifier l'exploitabilité de ces sauvegardes et de leurs contenus.		3	Documentation remise par l'opérateur.				
OUI	OUI	E54	Les données que l'opérateur est tenu de mettre à la disposition de l'ANJ (cf. articles 30 et 31 du décret n° 2010-518) doivent être conservées pour une durée de 6 ans. Pour les données personnelles concernant chaque joueur, ce délai de 6 ans court à compter de la clôture du compte joueur correspondant.		3	Documentation remise par l'opérateur.				
OUI	OUI		Pendant tout le temps de leur conservation, les archives et leurs sauvegardes, doivent :							
OUI	OUI	E55		- être protégées en intégrité ;	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E56		- être accessibles aux personnes autorisées seulement ;	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E57		- pouvoir être relues et exploitées.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				

OUI	OUI	E58	Le niveau de protection des sauvegardes des archives doit être au moins équivalent au niveau de protection des archives : l'opérateur présentera dans sa réponse les mécanismes d'archivage ainsi que les moyens de protection des archives qu'il est capable de mettre en œuvre.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E59	La précision de l'horloge par rapport à laquelle les systèmes d'information se synchronisent pour dater les événements journalisés ou archivés, doit être inférieure à une seconde par rapport au temps UTC. La source de temps doit être fiable.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.	L'auditeur devra démontrer le respect de l'exigence.			
OUI	OUI	**PARTIE 10 - Gestion de la journalisation technique et fonctionnelle**							
OUI	OUI	E60	L'opérateur doit maintenir et pouvoir fournir à l'ANJ, les journaux des traces techniques pour les évènements clé. Une première liste des événements concernés : - accès aux modules du SMA ; - opérations de maintenance effectuées ; - ouverture et fermeture de la prise de paris, mises poker, etc.	2	Documentation remise par l'opérateur.				
OUI	OUI	E61	Si des personnes physiques sont à l'origine des évènements tracés : - la journalisation doit permettre d'établir un lien entre l'identifiant technique utilisé dans la trace et la personne physique responsable des actions ; - les évènements sont journalisés en s'appuyant sur une source de temps fiable.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E62	Concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un package Linux, etc.), toutes les traces disponibles au niveau des équipements sont activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E63	L'opérateur consolidera l'ensemble des traces issues de la journalisation technique des différents équipements (réseau, système, applicatifs et sécurité), par exemple via l'application et le protocole syslog.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E64	Les traces de sécurité issues de la journalisation technique des plateformes sont analysées périodiquement par l'opérateur afin d'identifier les anomalies éventuelles.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E65	Les journaux techniques produits par les différents équipements doivent être conservés au minimum pendant trois mois en tant qu'archive.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E66	L'opérateur pourra mettre à disposition de l'ANJ ces journaux bruts produits par les différents équipements ou logiciels.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E67	Les incidents ou les comportements anormaux pouvant avoir un impact sur la sécurité du service doivent être traités et systématiquement faire l'objet d'une alerte et d'un compte-rendu écrit qui pourra être communiqué à l'ANJ.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	**PARTIE 11 - Gestion des accès physiques**							
OUI	OUI	E68	Les locaux techniques doivent être accessibles aux seules personnes habilitées par l'opérateur.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI		L'opérateur doit :						
	OUI	E69	- être en mesure d'identifier parfaitement les personnes ayant à intervenir dans ses locaux et sur ses équipements ;	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E70	- maintenir à jour les fonctions et les autorisations d'accès de ces personnes.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E71	Les personnes ayant à intervenir sur les équipements des plateformes de jeux doivent avoir été sensibilisées à la sécurité des systèmes d'information (ex: confidentialité des mots de passe et des données hébergées, etc.).	1	Documentation remise par l'opérateur.				
	OUI	E72	L'opérateur doit formaliser et appliquer des procédures organisationnelles nécessaires vis-à-vis des intervenants, notamment la vérification de l'absence de conflits d'intérêts, des candidats postulant pour un poste sensible, ainsi que les modalités de mise en sécurité de l'information lors de leur départ de la société (récupération des badges, gestion des mots de passe, etc.).	1	Documentation remise par l'opérateur.				
	OUI	E73	Les locaux abritant les équipements doivent être sécurisés : serrure haute sécurité, alarme d'ouverture, enregistrement des accès, video-surveillance, etc.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E74	L'accès physique aux locaux abritant les équipements doivent être limité : filtrage des personnes, contrôle des accès physiques, etc.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	**PARTIE 12 - Gestion de l'environnement physique**							
	OUI	E75	Les matériels et supports informatiques (support de sauvegarde, etc.) doivent être placés dans des zones de sécurité physiques, conçues pour lutter contre les tentatives d'intrusion et lutter contre les sinistres et accidents liées à l'environnement.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E76	La structure d'hébergement dispose de mesure de protection incendie.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E77	Le centre d'hébergement dispose, pour sa sécurité électronique, d'une double alimentation, d'onduleurs et d'un système de groupe électrogène principal et secondaire.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E78	Un système de climatisations redondantes et indépendantes par salle assure la stabilité des températures et du taux d'humidité.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E79	Tous les matériels (climatiseurs, panneaux électriques, etc.) utilisés par l'opérateur font l'objet d'un contrat de maintenance.	1	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	E80	Les sites d'exploitation doivent être surveillés 24h/24 et 7j/7.	2	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
	OUI	**PARTIE 13 - Équipe sécurité**							
	OUI	E81	L'opérateur doit justifier d'une « équipe sécurité » chargée de surveiller tous les équipements réseau, systèmes et les applications. La sécurité logique des équipements sera réalisée sous le contrôle de cette équipe.	1	Documentation remise par l'opérateur.				
	OUI	**PARTIE 14 - Interdits de jeu**							

	OUI	E82	Le serveur DNS doit faire l'objet d'une sécurisation conforme à l'état de l'art, plus particulièrement en termes de : - mise à jour, - durcissement du système d'exploitation sous-jacent, - durcissement de la configuration (en particulier avec la limitation de la récursivité aux seuls hôtes autorisés de la plateforme de jeu, par le biais d'une liste de contrôle d'accès). Les adresses IP des serveurs DNS de l'opérateur sont communiquées à l'ANJ, afin de mettre en œuvre des règles de filtrage réseau et listes de contrôle d'accès au niveau applicatif.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.	L'exigence relative à la synchronisation horaire s'applique en particulier aux serveurs DNS effectuant les interrogations, afin d'assurer le bon fonctionnement de l'extension de sécurité TSIG.			
	OUI	**PARTIE 15 - Données à la demande**								
	OUI	E83	Au délà des données tracées dans le SMA ou mises à disposition systématiquement, l'ANJ peut ponctuellement exiger des rapports ou données plus détaillés ou établis avec des critères de recherche précis, qui notamment peuvent être nominatifs. Ainsi, l'opérateur doit pouvoir exécuter des requêtes sur ses systèmes métier afin d'en extraire des données, dans des délais raisonnables. Ces rapports compléteront les informations qui peuvent être obtenues via le SMA et les informations remontées systématiquement et automatiquement vers le système d'information de l'ANJ. On peut citer : - la fourniture à l'ANJ de toutes les données techniques et non techniques liées à un évènement particulier ; - des demandes d'enquête de la part de l'ANJ concernant des évènements détectés et considérés comme anormaux ; - le détail de l'identité d'un joueur ; - le détail des coordonnées du compte de paiement d'un joueur ; - le détail d'une partie de poker, incluant une visibilité complète sur tous les joueurs ayant participé (toutes cartes, quelque soit l'opérateur de rattachement des joueurs dans le cas de réseaux d'opérateurs de mise en commun de joueurs) ; - certaines statistiques non prévues dans les données de supervision ; - le détail d'un pari particulier ; - la fourniture de données techniques (journaux) concernant certains éléments de l'architecture de jeu (SMA, plateforme, etc.).	3	Documentation remise par l'opérateur.	Pour chacun des éléments cités en exemple, l'opérateur devra spécifier la nature des données conservées, la période de rétention correspondante et les procédures mises en place pour la mise à disposition de ces informations à l'ANJ.			
OUI	OUI	**PARTIE 16 - SMA : généralités**								
OUI	OUI	E84	L'opérateur doit mettre en place un site Internet dédié, exclusivement accessible par un nom de domaine de premier niveau comportant la terminaison .fr.	3	Documentation remise par l'opérateur (informations techniques sur le nom de domaine pleinement qualifié : Whois, résolutions DNS, etc., et sur l'ensemble des noms de domaine déclarés auprès de l'ANJ)				
OUI	OUI	E85	Toutes les connexions à destination d'un site de l'opérateur ou d'une de ses filiales et issues d'une IP française ou d'un compte joueur dont l'adresse de domiciliation est en France doivent être redirigées vers ce site.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E86	Dans le cadre de ses activités de jeux, l'opérateur met en œuvre un dispositif technique appelé « SMA » à des fins de contrôle. Le SMA est un dispositif de recueil et d'archivage de données liées à un évènement de jeu ou à un compte joueur. Ce dispositif est :	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E87	- développé et exploité sous la responsabilité de l'opérateur ;	2	Documentation remise par l'opérateur (identification des prestataires : développeurs, exploitants, etc.).				
OUI	OUI	E88	- installé sur un support situé en France métropolitaine.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E89	Tous les échanges de données liées à un évènement de jeu ou à un compte joueur, entre un joueur réputé français et la plateforme de jeu, doivent transiter par le SMA.	3	Audit de configuration des plateformes d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI		En particulier, les connexions provenant de joueurs réputés français doivent être redirigées vers le SMA. La plateforme de jeu doit rediriger vers le SMA les requêtes suivantes :						
OUI	OUI	E90	- avant authentification du joueur, si l'origine de la connexion est une adresse IP réputée française (pays d'attribution de l'adresse IP du terminal Internet depuis lequel il se connecte est la France dans la base RIPE NCC) ;	3	Audit de configuration des plateformes d'hébergement, en particulier la description des dispositifs techniques mis en place par l'opérateur côté SMA/plateforme de jeu (ex : description du module de géolocalisation mis en place au niveau HTTP, ou encore au niveau DNS), étayée par des extraits de configuration (ex : module Apache de géolocalisation) et portion de code (redirection en post-authentification).				
OUI	OUI	E91	- ou, après authentification du joueur, si le joueur a indiqué un domicile en France lors de l'ouverture de son compte de jeu.	3					
OUI	OUI	E92	L'opérateur doit permettre à l'ANJ de se rendre, à tout moment, sur le site d'hébergement du SMA pour saisir l'ensemble ou un sous-ensemble des données qui y sont conservées. À cette fin, l'ANJ informe au moins deux heures à l'avance le représentant de l'opérateur de son intention d'accéder à ce site et de l'heure à laquelle cet accès devra leur être donné.	3	Procédures mises en place par l'opérateur et l'hébergeur du SMA, le cas échéant, pour autoriser un tel accès.	Il est en particulier question de l'accès au site d'hébergement du composant coffre-fort du SMA.			
OUI	OUI		Les échanges de données suivants doivent être sécurisés afin d'en garantir l'authenticité, l'intégrité ainsi que la confidentialité :						
OUI	OUI	E93	- les échanges entre le joueur et le SMA ;	3	Audit de configuration de la plateforme d'hébergement, en particulier la description technique des protocoles de sécurité mis en place (ex : algorithmes, certficats X.509, le cas échéant, etc.).	Avis d'expert sur les interactions HTTP/HTTPS pour les applications Web, notamment pour l'accès au formulaire d'authentification, et la gestion des identifiants de session, etc.			
OUI	OUI	E94	- les échanges entre les différents modules du SMA ; - les échanges entre le SMA et la plateforme de jeux de l'opérateur ; - les échanges entre le SMA et la plateforme de l'ANJ.	2	Audit de configuration de la plateforme d'hébergement, notamment le schéma d'architecture.	Description technique des flux et protocoles impliqués, en mentionnant les moyens de chiffrement/authenticité des flux (transport IPsec, SSL/TLS, ou colocation des équipements, par exemple) et d'authentification des parties mis en place.			
OUI	OUI		Le SMA doit comporter des fonctionnalités de sécurité visant à le protéger des attaques par saturation, agissant :						
OUI	OUI	E95	- au niveau transport, si ce composant termine les connexions TCP initiées par les clients : protection contre les dénis de service réseau, qui visent un épuisement de ressources TCP par des attaques de type SYN Flood, ou des attaques qui s'appuient sur un établissement complet de connexion TCP (Naphta, Sockstress, etc.) ;	2	Audit de configuration de la plateforme d'hébergement, notamment la description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration, ou encore des procédures de gestion d'incident mises en place avec le fournisseur d'accès en amont, le cas échéant, par exemple.				

OUI	OUI	E96		- au niveau applicatif, avec l'envoi de multiples requêtes HTTP qui viseraient la saturation du SMA qui constitue potentiellement un point de défaillance unique de l'architecture, afin de le protéger (i) d'un épuisement de ressources (saturation des enregistrements temporairement mis en tampon et en attente d'un acquittement) et (ii) d'une saturation du coffre avec des enregistrements mal formés.	2	Audit de configuration de la plateforme d'hébergement, audit applicatif intrusif de l'application capteur, notamment la description des dispositifs techniques mis en place par l'opérateur appuyée par des éléments de configuration.				
OUI	OUI	**PARTIE 17 - SMA : module « coffre-fort »**								
OUI	OUI	E97	Le coffre-fort doit détenir une certification de sécurité de premier niveau (CSPN) délivrée par l'ANSSI (https://www.ssi.gouv.fr).		3	L'absence de certification CSPN est rédhibitoire pour l'obtention de la certification du SMA.				
OUI	OUI		La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des menaces :							
OUI	OUI	E98		- le dépôt ou l'injection d'enregistrements non autorisés ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E99		- l'altération d'enregistrements ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E100		- le vol de données ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E101		- le déni de service.	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI		La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des fonctions de sécurité :							
OUI	OUI	E102		- l'authentification forte des utilisateurs et administrateurs ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E103		- le chiffrement, la signature et l'horodatage des évènements ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E104		- le chaînage des évènements.	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E105	Toute suppression ou altération des données archivées, de manière malveillante ou non, doit pouvoir être identifiée par l'ANJ.		3	Audit de configuration de la plateforme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.				
OUI	OUI		Quatre profils d'autorisation doivent pouvoir être définis :							
OUI	OUI	E106		- profil « déposant » : profil attribué au module « capteur » du SMA. Il permet uniquement d'écrire des traces dans le journal. Le module capteur du SMA s'authentifie à l'aide d'un certificat X.509v3 auprès de la partie coffre-fort avec une identité associée à ce profil ;	1	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E107		- profil « lecteur » : profil attribué aux agents de l'ANJ dotés des pouvoirs de contrôle et d'audit, qui permet l'extraction des données enregistrées, soit sur support amovible, soit via un dépôt de fichiers accessible à travers un service web ;	1	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E108		- profil « administrateur technique et opérationnel » : profil attribué au personnel technique de l'opérateur, responsable de l'administration et de la supervision technique du coffre-fort ;	1	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E109		- profil « administrateur fonctionnel » : profil attribué aux personnes physiques de l'ANJ ou désignées par l'ANJ, qui peuvent définir des rôles et leur associer un certificat d'authentification. Cette opération est nécessaire à l'initialisation des coffres, puis lors des renouvellements ou des révocations des certificats.	1	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI		Les certificats associés au profil « lecteur » sont utilisés :							
OUI	OUI	E110		- soit par des personnes physiques, pour les contrôles réalisés sur site, avec des biclefs RSA et un certificat X.509v3 d'authentification, par exemple conservé sur un support matériel (ex : carte à puce) fourni par l'opérateur ;	1	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E111		- soit par des agents de collecte, pour les consultations réalisées à distance, avec une authentification fondée sur un certificat X.509v3 client SSL/TLS, dans le cadre de la négociation d'un tunnel SSL/TLS mutuellement authentifié.	1	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI		En termes de gestion des clefs de chiffrement, de signature, et d'horodatage :							
OUI	OUI	E112		- les tailles de clefs doivent être conformes aux règles énoncées dans le référentiel général de sécurité de l'ANSSI (https://www.ssi.gouv.fr/) ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E113		- la cryptographie mise en œuvre en termes de générateurs de nombres pseudoaléatoires, fonctions de hachage, algorithmes symétriques et asymétriques doit respecter les règles de bonnes pratiques spécifiées dans le référentiel général de sécurité de l'ANSSI (https://www.ssi.gouv.fr/) ;	3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E114		- un HSM est utilisé pour les opérations de signature ; le biclef de signature peut être soit généré dans le HSM, soit injecté dans ce dernier ;	3	Rapport et cible de la certification ANSSI/CSPN.	Dans l'hypothèse où le biclef ferait l'objet d'une injection, un avis d'expert est attendu sur la sécurité de la méthode de génération du biclef hors HSM.			
OUI	OUI	E115		- les données chiffrées le sont au moyen de la clef publique du certificat transmis par l'ANJ : seule l'ANJ peut déchiffrer le contenu des données archivées. Remarque : les opérations de chiffrement des données peuvent indifféremment être réalisées par des moyens matériels ou logiciels.	3	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.				
OUI	OUI	E116	En termes de stockage des traces du coffre-fort, le coffre-fort met en œuvre une ségrégation entre l'espace de stockage destiné aux données de son administration et celui ou ceux destinés aux données de jeu tracées. Dans le cadre d'un coffre mutualisé entre plusieurs agréments, chaque agrément doit faire l'objet d'un espace de stockage spécifique. La ségrégation des espaces de stockage doit, *a fortiori* , être mise en oeuvre dans le cadre d'une mutualisation interopérateurs, le cas échéant.		3	Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI		La sécurité physique des accès au coffre-fort est assurée par :							
OUI	OUI	E117		- l'hébergement dans un emplacement protégé ;	2	Audit de configuration de la plateforme d'hébergement : une analyse de premier niveau de la sécurité physique de l'infrastructure d'hébergement est attendue.				

OUI	OUI	E118		- la mise en place d'un contrôle d'accès ;	2	Audit de configuration de la plateforme d'hébergement : une analyse de premier niveau de la sécurité physique de l'infrastructure d'hébergement est attendue.				
OUI	OUI	E119		- la mise en place de procédures de suivi des interventions (toutes les opérations de configuration du coffre-fort doivent notamment faire l'objet d'un suivi) ;	2	Audit de configuration de la plateforme d'hébergement : une analyse de premier niveau de la sécurité physique de l'infrastructure d'hébergement est attendue.				
OUI	OUI	E120		- la mise en oeuvre de protections physiques.	2	La méthode de scellement du coffre-fort doit faire l'objet d'une procédure qui, quelle que soit la méthode, doit être probante et garantir l'inocuité d'une intervention qui aurait pour conséquence de rompre ledit dispositif.				
OUI	OUI	**PARTIE 18 - SMA : module « capteur »**								
OUI	OUI	E121	Le capteur doit implanter des mécanismes de défense afin de protéger sa mémoire tampon et éviter toute saturation à destination de cette dernière ou du coffre lui-même.		2	Audit applicatif intrusif de l'application capteur. Documentation remise par l'opérateur.				
OUI	OUI		Le module « capteur » doit :							
OUI	OUI	E122		- être authentifié par certificat auprès du coffre-fort, au niveau duquel une session avec le profil « déposant » est ouverte ;	2	Documentation remise par l'opérateur, appuyée par des éléments issus de l'audit applicatif intrusif de l'application capteur.	L'analyse doit être étayée par des extraits de code source du capteur.			
OUI	OUI	E123		- attendre du coffre un acquittement, sous la forme d'une preuve du dépôt.	2	Documentation remise par l'opérateur, appuyée par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur. Voir les exigences dédiées aux fonctions de création et de stockage des traces.				
OUI	OUI	E124	L'ensemble des composants du SMA doivent être synchronisés en temps, auprès d'une source de temps fiable.		3	Audit de configuration de la plateforme d'hébergement.				
OUI	OUI	**PARTIE 19 - SMA : fonctions de création et de stockage des traces**								
OUI	OUI		La fonction de création de traces du capteur doit respecter les principes suivants :							
OUI	OUI	E125		- La fonction de création de traces correspond à l'écriture de données liées à un évènement de jeu ou à un compte joueur dans le module coffre-fort du SMA. Cette fonction doit être appelée systématiquement à chaque évènement ou échange de données dont les traces sont exigées ;	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI	E126		- la fonction de création de traces est implémentée en amont de la logique de jeu. Elle intercepte voire relaie le flux applicatif entre le joueur et l'opérateur (exemple : fonctionnement de type proxy) ;	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.	L'implémentation en amont de la logique de jeu concerne en particulier les évènements à tracer au coffre où l'acquittement du joueur est attendu ou sont une conséquence directe d'une action du joueur. Par opposition, lorsque l'évènement a pour origine l'opérateur et ne nécessite pas un acquittement de la part du joueur, la fonction de création de traces est directement appelée par la plateforme de jeu.			
OUI	OUI	E127		- le SMA doit offrir une architecture dotée d'une très haute disponibilité avec redondance de mécanismes afin de strictement limiter les incidents potentiels de stockage ;	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI	E128		- le principe d'une annulation d'un jeu concerné par un incident de stockage d'un des évènements doit être retenu.	2	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI		La fonction de création de traces d'un événement doit :							
OUI	OUI	E129		- être invoquée suite à une requête émise par le joueur (si celle-ci requiert un enregistrement). Cette requête peut résulter : (i) d'une action du joueur, à son initiative, comme une prise de pari, (ii) d'un acquittement par le joueur, suite à un message transmis à l'initiative de la plateforme, comme l'annonce d'un gain sur un pari.	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI	E130		- être invoquée suite à une action à l'initiative de l'opérateur, sans acquittement par le joueur, dont la trace est exigée (ex : rectification des informations du compte joueur).	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI	E131		- reposer sur un module applicatif à état : les traces d'évènement générés doivent être temporairement conservées au niveau du capteur dans une mémoire tampon ou un dispositif de stockage temporaire équivalent (ex: base de données), avant toute transmission au niveau du coffre-fort, dans l'attente d'un acquittement de la plateforme de jeux validant la bonne et due forme de cet évènement.	3	Le respect de mode de fonctionnement à état assure que les évènements transmis au coffre et générés à l'initiative du joueur (action ou acquittement) sont validés, avant stockage au coffre-fort, par la plateforme.	Tout écart par rapport à ce mode de fonctionnement doit être techniquement justifié (exemple : évènements POPARTIE générés par la plateforme de jeu, et transmis pour acquittement au joueur avant stockage). Une analyse technique de la sécurité du processus de validation des évènements par le capteur est attendue, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur. Un mode de fonctionnement dans lequel les données transmises par le joueur seraient directement journalisées par le coffre est rédhibitoire pour la certification du SMA.			
OUI	OUI	E132		- gérer un acquittement de la plateforme de jeux, afin de limiter les risques d'attaques qui viseraient à saturer le coffre-fort d'évènements aléatoires, ou à enregistrer des évènements falsifiés générés par un joueur malveillant.	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI	E133		- en cas d'acquittement négatif de la part de la plateforme de jeux, l'évènement pré-enregistré au niveau du capteur doit être détruit. Une erreur doit être générée et faire l'objet d'un message dans la journalisation technique du capteur.	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI	E134		- en cas d'acquittement positif de la part de la plateforme de jeux, l'évènement présent en mémoire tampon au niveau du capteur peut être transformé au format exigé par l'ANJ, pour son stockage par le coffre-fort.	3	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.				
OUI	OUI	E135		- gérer les cas d'acquittements négatifs de la part du coffre-fort, en cas de défaillance d'enregistrement.	2	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.	Des mécanismes de reprise sur erreur peuvent être implémentés au niveau du capteur, par exemple par des tentatives de retransmission au coffre d'un l'évènement.			

OUI	OUI	E136		- garantir l'enregistrement d'un évènement de jeu au niveau du coffre-fort, sous peine d'annulation de l'opération de jeu.	2	Description des dispositifs techniques mis en place par l'opérateur, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif intrusif de l'application capteur.	Cette exigence repose sur un mode de fonctionnement synchrone entre capteurs et coffres. Le capteur, dans ce modèle, doit attendre un acquittement positif du coffre avant de poursuivre la transaction. Dans la pratique : - l'introduction d'un traitement par lots, le cas échéant, proscrit un fonctionnement synchrone au sens strict, - l'approbation de l'utilisation de mécanismes basés sur des files d'attente entre capteurs et coffres proscrit également ce mode de fonctionnement. Il est donc notamment attendu un avis d'expert technique sur : - le synchronisme entre le capteur et le mécanisme de dépôt au coffre, en décrivant les files d'attente, les mécanismes de détection et de reprise sur erreur (ex : retransmission par le capteur) ; - la redondance et la fiabilité du dispositif assurant le traitement des évènements entre leur émission par le capteur, et leur stockage *in fine* par le coffre-fort (ex : analyse du mécanisme de file d'attente de type *message broker*).			
OUI	OUI		La fonction de stockage correspond à l'archivage des données tracées dans un coffre-fort numérique afin d'en garantir l'intégrité et l'exhaustivité dans le temps. Le stockage des données consiste en les étapes suivantes :							
OUI	OUI	E137		- l'établissement d'un canal sécurisé, suite à l'authentification mutuelle du déposant (i.e. le capteur) avec le coffre-fort, via une session TLS mutuellement authentifiée par certificat X.509v3 ;	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	OUI	E138		- la vérification de l'habilitation du profil à déposer des traces ;	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur	L'approbation de l'utilisation de mécanismes basés sur des files d'attente entre capteurs et coffres proscrit également ce mode de fonctionnement.			
OUI	OUI	E139		- le chaînage avec la trace précédente, en liant l'empreinte des données à une empreinte de la signature de la trace précédente, et en incluant l'identifiant d'évènement unique à l'opérateur ;	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	OUI	E140		- le calcul de l'empreinte, à l'aide d'une fonction de hachage. L'empreinte ne doit pas être calculée au moment de l'ajout, mais être conservée en mémoire depuis l'opération précédente ;	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	OUI	E141		- le scellement des données, par signature horodatée incluant l'élément de chaînage pour en garantir l'intégrité, et les lier à une heure précise ;	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	OUI	E142		- l'horodatage, qui doit être effectué sur l'évènement (ou le lot d'évènements) en clair.	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	OUI		Concernant les opérations de signature et de chiffrement :							
OUI	OUI	E143		- le format de signature est XADES-T avec un jeton d'horodatage conforme à la RFC 3161.	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur	Un autre format de signature peut être implanté, à condition d'être justifié.			
OUI	OUI	E144		- le chiffrement des données est réalisé au moyen de la clé publique de l'ANJ pour en assurer la confidentialité.	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur	La méthode de chiffrement pourra faire intervenir un algorithme de chiffrement symétrique, suivant des opérations qui seront précisément décrites.			
OUI	OUI		Concernant le traitement par lots :							
OUI	OUI	E145		- le traitement par lot doit être paramétrable pour une durée ou un nombre maximal d'évènements.	1	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	OUI	E146		- la granularité du traitement par lot doit être l'évènement.	1	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur				
OUI	OUI	**PARTIE 20 - SMA : fonction d'accès aux traces**								
OUI	OUI		L'opérateur agréé ou titulaire de droits exclusifs doit fournir les éléments suivants, pour chaque agrément ou périmètre d'activité sous droits exclusifs :							
OUI	OUI	E147		- un mécanisme d'accès aux données permettant la saisie des données sur site (copie de tout ou partie du coffre-fort) ;	3	Documentation remise par l'opérateur.				
OUI	OUI	E148		- un mécanisme d'accès aux données permettant l'interrogation des données à distance, par l'intermédiaire d'un outil de collecte ;	3	Documentation remise par l'opérateur.				
OUI	OUI	E149		- un outil de validation des données du SMA et d'extraction des traces des opérations de jeu utilisable sur le site du SMA, et dans les laboratoires de l'ANJ (mode hors-ligne).	3	Documentation remise par l'opérateur.				
OUI	OUI		L'architecture de la partie coffre-fort du SMA doit distinguer :							
OUI	OUI	E150		- un espace de stockage des données situé dans une zone réseau sécurisée ;	3	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E151		- une couche d'accès à l'espace de stockage accessible.	3	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.				
OUI	OUI	E152	Les données stockées dans le coffre-fort doivent être en accès permanent à distance, depuis les locaux de l'ANJ (i.e. depuis une ou plusieurs adresses IP identifiées).		3	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur.	Il s'agit de s'assurer que des mesures sont mises en œuvre pour garantir la haute-disponibilité des données stockées dans le coffre-fort.			
OUI	OUI	E153	Les données accessibles à distance doivent couvrir au moins les 12 derniers mois d'activité de l'opérateur (période glissante).		3	Documentation remise par l'opérateur.	Il s'agit de pouvoir accéder aux données en temps réel sur une période de 12 mois glissants. L'accès à des données plus anciennes peuvent quant à elles faire l'objet de demandes spécifiques.			
OUI	OUI	E154	Les données doivent rester accessibles sur le site d'hébergement du SMA sur toute la durée de conservation exigée par la loi (article 31 du Décret n° 2010-518 du 19 mai 2010).		3	Documentation remise par l'opérateur.				
OUI	OUI	E155	L'extraction du coffre-fort doit pouvoir se faire sur une tranche de données, correspondant à une période d'activité ou une tranche d'identifiants d'évènements avec l'outil de collecte à distance mis à disposition par l'opérateur.		3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.				
OUI	OUI	E156	La couche d'accès à l'espace de stockage doit elle-même être sécurisée, aux niveaux applicatif et réseau, vis-à-vis de l'extérieur, notamment contre les attaques de déni de service, et les accès autres que ceux initiés par l'ANJ.		2	Audit de configuration de la plateforme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.				

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

OUI	**OUI**	**E171**		- filtrés, en termes de contenu, conformément aux expressions régulières (facette pattern) décrites dans le schéma XSD ;	3	Audit de code	L'analyse devra démontrer l'usage de filtres dans le code source.			
OUI	**OUI**	**E172**		- filtrés, en termes de contenu, afin de prévenir des attaques web classiques par injection (injections SQL, XPath, voire XSS, en complément d'un encodage des sorties par entités HTML, par exemple, etc.).	3	Audit de code	L'analyse devra démontrer l'usage de filtres dans le code source.			