

Matrice des exigences de la certification unique à 6 mois du composant frontal  
Version du 17 mars 2014

Notice	
Point de contrôle	Point de contrôle noté « E1 ». Remarque : la numérotation du point de contrôle est propre à ce document.
Référence	Référence au document (DET, Annexe au DET, voire Loi ou décret) et de la partie renseignant le point de contrôle. DET : dossier des exigences techniques <a href="http://www.arjel.fr/IMG/pdf/det.pdf">http://www.arjel.fr/IMG/pdf/det.pdf</a> ANN : annexe au dossier des exigences techniques <a href="http://www.arjel.fr/IMG/pdf/annexe.pdf">http://www.arjel.fr/IMG/pdf/annexe.pdf</a>
Libellé	Description du point de contrôle, selon les termes du document de référence.
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 (ex : 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'ARJEL, 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 réglementaire, ou en termes de sécurité (sur un composant exposé et/ou manipulant des données critiques).
Éléments d'analyse	Éléments sur lesquels l'analyse s'appuie : 1. documents remis par l'opérateur, par exemple : - dossier de définition de la plate-forme d'hébergement du frontal, - documentation fonctionnelle et technique du logiciel capteur, - rapport de certification CSPN réalisé à l'occasion de la certification du coffre-fort, et la cible de sécurité de cette certification, - rapports d'audits de sécurité déjà réalisés par l'opérateur – en particulier si le capteur est intégré à la plate-forme de jeu – ou encore d'analyse de la maturité SSI de l'opérateur ; 2. 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 applicatif intrusif du composant logiciel capteur. Ce rapport est noté « audit applicatif de type 'intrusif' de l'application capteur » dans la suite du document ; - l'audit de configuration de premier niveau de l'infrastructure d'hébergement du frontal. Ce rapport est noté « audit de configuration des plates-formes 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.).
Commentaires	Précisions apportées par l'ARJEL, 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.
Conformité	Constat de l'analyse

Point de Contrôle	Référence	Libellé	Niveau de criticité	Éléments d'analyse	Commentaires	Rapports concernés	Conformité
<b>Exigences organisationnelles</b>							
<b>Procédures d'administration et d'exploitation</b>							
		L'organisation mise en place pour gérer les systèmes d'information de l'opérateur doit s'appuyer sur une documentation et des procédures permettant de suivre ses évolutions. La documentation comporte :					
E1	DET	5.7.2.a 5.7.2.b		- la politique de sécurité, ou un document remplissant une fonction similaire ;	1	Documentation remise par l'opérateur + analyse de premier niveau.	
E2	DET	5.7.2.b		- une description fonctionnelle de l'infrastructure d'hébergement du composant frontal, précisant les différents composants, leurs fonctions et les flux transitant par ces derniers.	1	Documentation remise par l'opérateur + avis d'expert.	
E3	DET	5.7.3.a		La documentation des infrastructures d'hébergements du composant frontal et de la plate-forme de jeu 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.	
E4	DET	5.7.3.d		L'opérateur sera responsable, sur toute la durée de validité de l'agrément, de la tenue à jour et de la cohérence de ce dossier. Chaque modification de l'un de ces dossiers devra faire l'objet d'une nouvelle remise de document à l'ARJEL ; L'opérateur doit mettre à jour le « dossier » de définition avec la liste des correctifs de sécurité appliqués sur les serveurs, et doit communiquer à l'ARJEL la version actualisée du document.	1	Documentation remise par l'opérateur + analyse de premier niveau.	
		La documentation des infrastructures d'hébergement du composant frontal et de la plate-forme de jeu qui intègre un volet technique et procédural comporte :					
E5	DET	5.7.2.b		- 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.	
E6	DET	5.7.2.b		- les spécifications techniques du système, en particulier les configurations à jour des équipements qui le compose ;	2	Documentation remise par l'opérateur (dossier de définition) + avis d'expert.	
E7	DET	5.7.2.b		- la liste descriptive précise de tous les composants, avec le recensement d'éléments factuels, comme les versions des logiciels utilisés, 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.	

Matrices des exigences de la certification unique à 6 mois du composant frontal

E8	DET	5.7.2.b		<ul style="list-style-type: none"> <li>- une liste de procédures d'exploitation, notamment :</li> <li>- procédures de gestion des journaux ;</li> <li>- procédures de gestion des alertes ;</li> <li>- procédures de mise à jour régulière de tous les composants (systèmes d'exploitation, applications, routeurs, etc.) ;</li> <li>- procédures de gestion des composants à mise à jour fréquente (anti-virus, systèmes de détection d'intrusion, le cas échéant) ;</li> <li>- procédures de mise à jour en cas d'édition d'un correctif de sécurité critique ;</li> <li>- procédures pour la mise en sécurité des systèmes en cas d'urgence ou de danger imminent ;</li> <li>- procédures d'exploitation des composants du SI (serveurs, routeurs) ;</li> <li>- procédures d'exploitation des comptes et mots de passe ;</li> <li>- procédures de gestion des composants infogérés ;</li> <li>- procédures relative à la sécurité physique (gardiennage, etc.) ;</li> <li>- procédures de gestion des sauvegardes et des restaurations ;</li> <li>- procédures de veille technologique ;</li> <li>- procédures pour la télé-administration ;</li> <li>- procédures de gestion des tableaux de bord SSI.</li> </ul>	1	Documentation remise par l'opérateur (dossier de définition) + analyse de premier niveau.			
<b>Gestion de la disponibilité et des mises à jour</b>									
E9	DET	5.7.3.c	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 plates-formes d'hébergement. Documentation remise par l'opérateur.			
E10	DET	5.7.3.f	- 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 ( <a href="http://www.certa.ssi.gouv.fr">http://www.certa.ssi.gouv.fr</a> ) par exemple. - L'opérateur applique les correctifs de sécurité qui sont proposés par les éditeurs, dans les documents du CERT ou demandés explicitement par l'ARJEL, le cas échéant.		2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E11	DET	5.7.3.f	L'opérateur devra au moins prohiber l'utilisation sur ses plates-formes des systèmes et logiciels obsolètes référencés par le CERTA.		2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
			Si aucun correctif de sécurité n'est disponible auprès de l'éditeur, l'opérateur suit :						
E12	DET	5.7.3.d		- les recommandations de ce dernier ou d'un CERT, dans le cadre d'un contournement provisoire ;	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E13	DET	5.7.3.d		- 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 plates-formes d'hébergement. Documentation remise par l'opérateur.			
E14	DET	5.7.3.d	L'opérateur devra mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer à l'ARJEL la version actualisée du document.		1				
E15	DET	5.7.3.c	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 plates-formes d'hébergement. Documentation remise par l'opérateur.			
<b>Authentification des accès d'administration</b>									
			Les accès d'administration aux équipements du frontal doivent être protégés à l'aide des mécanismes suivants :						
E16	DET	5.7.3.e.2		- 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 plates-formes d'hébergement. Documentation remise par l'opérateur.			
E17	DET	5.7.3.e.2		- <u>ou bien</u> une authentification par mot de passe, avec des règles de composition et de renouvellement conforme 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 plates-formes d'hébergement. Documentation remise par l'opérateur.	Les authentifications en clair seront prohibées, et en l'absence de mode défi/réponse un chiffrement des communications sera obligatoire. La mesure doit permettre de prouver la robustesse des mots de passe		
E18	DET	5.7.3.e.2		- un contrôle d'accès basé sur les adresses IP est réalisé, le cas échéant.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
<b>Gestion des configurations</b>									
E19	DET	5.7.3.f	À l'issue de la mise en œuvre d'un nouvel équipement ou de l'installation d'une nouvelle application, l'opérateur mettra à disposition de l'ARJEL 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 plates-formes d'hébergement. Documentation remise par l'opérateur.			
E20	DET	5.7.3.f	Les composants systèmes, réseau et applicatifs mis en œuvre par l'opérateur devront avoir fait l'objet d'une minimalisation de leur configuration et 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 dangereuses (interface d'administration de serveurs d'application), suppression des comptes et mots de passe constructeurs, etc.		2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
E21	DET	5.7.3.f	Afin de détecter d'éventuelles erreurs de manipulation mais aussi le résultat d'attaques, l'intégrité des fichiers de configuration des équipements devra être vérifiée régulièrement. Cette vérification devra pouvoir être faite sur demande de l'ARJEL, et un rapport de diagnostic devra pouvoir lui être transmis.		2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.			
<b>Gestion de la sécurité dans les cycles de développement</b>									
E22	DET	5.7.3.g	L'opérateur devra gérer 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 droit de l'opérateur de l'effectuer.		
E23	DET	5.7.3.g	L'opérateur devra contractualiser avec ses prestataires le respect d'un référentiel de développement sécurisé pour les projets dont il externaliserait la prise en charge.		1	Audit applicatif intrusif. Documentation remise par l'opérateur.			
			Le référentiel de développement sécurisé devra en particulier aborder le problème de la validation des paramètres, notamment :						
E24	DET	5.7.3.g		- 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.			
E25	DET	5.7.3.g		- vérifier les données en entrée et en sortie ;	2	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E26	DET	5.7.3.g		- utiliser une fonction de vérification des données identique et centralisée.	2	Audit applicatif intrusif. Documentation remise par l'opérateur.			
E27	DET	5.7.3.g	L'opérateur devra pouvoir transmettre à l'ARJEL l'ensemble de codes sources des logiciels de jeux utilisés sur ses plates-formes.		3	Documentation remise par l'opérateur.			
E28	DET	5.7.3.g	L'opérateur devra gérer 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 droit de l'opérateur de l'effectuer.		
<b>Gestion des sauvegardes des données</b>									

Matrices des exigences de la certification unique à 6 mois du composant frontal

E29	DET	5.7.3.h	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 coffre-fort du frontal.	3	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E30	DET	5.7.3.h	Ces sauvegardes sont mises à disposition de l'ARJEL par l'opérateur pour consultation et archivage.	2	Documentation remise par l'opérateur.		
E31	DET	5.7.3.h	Le type de support et le format de la sauvegarde sont indiqués pour permettre à l'ARJEL de vérifier l'exploitabilité de ces sauvegardes et de leurs contenus.	3	Documentation remise par l'opérateur.		
E32	DET	5.7.3.h	La durée de conservation des informations, définie par le code du commerce, doit être de 5 ans, suivant la fermeture du compte de jeu.	3	Documentation remise par l'opérateur.		
			Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, doivent :				
E33	DET	5.7.3.h		3	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E34	DET	5.7.3.h		3	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E35	DET	5.7.3.h		3	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E36	DET	5.7.3.h	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 sécurisés de protection des archives qu'il est capable de mettre en œuvre.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
			La précision de l'horloge par rapport à laquelle les systèmes d'information se synchronisent pour dater les événements journalisés ou archivés doit :				
E37	DET	5.7.3.h		2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.	L'auditeur devra démontrer le respect de l'exigence	
E38	DET	5.7.3.h	Une totale intégrité des données et des traitements est requise pour l'ensemble des données sur le frontal.	3	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
<b>Gestion de la journalisation technique et fonctionnelle</b>							
			L'opérateur doit maintenir, et pouvoir fournir à l'ARJEL, les journaux des traces techniques pour les événements clé. Une première liste des événements concernés :				
E39	DET	5.7.3.k		2	Documentation remise par l'opérateur.		
E40	DET	5.7.3.k	Si des personnes physiques sont à l'origine des événements 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 événements seront journalisés en s'appuyant sur une source de temps fiable.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E41	DET	5.7.3.k	Concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un package Linux, ...), toutes les traces disponibles au niveau des équipements seront activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E42	DET	5.7.3.k	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 plates-formes d'hébergement. Documentation remise par l'opérateur.		
E43	DET	5.7.3.k	Les traces de sécurité issues de la journalisation technique des plates-formes seront analysées périodiquement par l'opérateur afin d'identifier les anomalies éventuelles.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E44	DET	5.7.3.k	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 plates-formes d'hébergement. Documentation remise par l'opérateur.		
E45	DET	5.7.3.k	L'opérateur pourra mettre à disposition de l'ARJEL ces journaux bruts produits par les différents équipements ou logiciels.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E46	DET	5.7.3.k	Les incidents ou les comportements anormaux pouvant avoir un impact sur la sécurité du service devront être traités et systématiquement faire l'objet d'une alerte et d'un compte-rendu écrit qui pourra être communiqué à l'ARJEL.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
			L'opérateur doit maintenir, et pouvoir fournir à l'ARJEL, les journaux des traces techniques pour les événements clé. Une première liste des événements concernés :				
E47	DET	5.7.3.k		2	Documentation remise par l'opérateur.		
E48	DET	5.7.3.k	Si des personnes physiques sont à l'origine des événements 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 événements seront journalisés en s'appuyant sur une source de temps fiable.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E49	DET	5.7.3.k	Concernant l'administration (création d'un compte utilisateur Linux, modification d'une permission sur un répertoire Windows, ajout d'un package Linux, ...), toutes les traces disponibles au niveau des équipements seront activées pour permettre d'identifier l'administrateur ayant réalisé l'action en cas de problème détecté.	2	Audit de configuration des plates-formes d'hébergement. Documentation remise par l'opérateur.		
E50	DET	5.7.3.k	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 plates-formes d'hébergement. Documentation remise par l'opérateur.		
<b>Frontal</b>							
E51	DET	4	L'opérateur devra 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. sur l'ensemble des noms de domaine déclarés auprès de l'ARJEL)		
E52	DET	4	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 est en France devront être redirigées vers ce site.	3	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.		
			Le frontal est un dispositif de recueil et d'archivage des données échangées entre joueur et la plateforme de l'opérateur à l'occasion des opérations de jeux. Ce dispositif est :				
E53	DET	4.1.1		2	Documentation remise par l'opérateur (identification des prestataires : développeurs, exploitants, etc.).		
E54	DET	4.1.1		3	Description de l'infrastructure d'hébergement. Cette exigence s'applique au coffre et au capteur.		
E55	DET	4.1.2	Tous les échanges entre un joueur réputé français et la plate-forme de jeu devront transiter par le frontal.				
			Les connexions provenant de joueurs réputés français doivent être redirigées vers le frontal qui se trouve en coupure de flux applicatif. La plateforme de jeu doit refuser ou rediriger vers son frontal français les requêtes suivantes :				
E56	DET	4.1.2		3	Audit de configuration de la plate-forme d'hébergement, en particulier la description des dispositifs techniques mis en place par l'opérateur côté frontal/plate-forme 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-authentication).		
E57	DET	4.1.2		3			
E58	Décret N° 2010-509	Art.6	L'opérateur doit permettre à l'ARJEL de se rendre, à tout moment, sur le site d'hébergement du support matériel d'archivage pour saisir l'ensemble ou un sous-ensemble des données qui y sont conservées. À cette fin, l'ARJEL 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 frontal, le cas échéant, pour autoriser un tel accès.		
			Les échanges de données suivants devront être sécurisés afin d'en garantir l'authenticité ainsi que la confidentialité :				

Matrices des exigences de la certification unique à 6 mois du composant frontal

E59	DET	4.1.1		- les échanges entre le joueur et le frontal ;	3	Audit de configuration de la plate-forme d'hébergement, en particulier la description technique des protocoles de sécurité mis en place (ex : algorithmes, certificats 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.				
E60	DET	4.1.1		- les échanges entre les différents modules du frontal ; - les échanges entre le frontal et la plate-forme de jeux de l'opérateur ; - les échanges entre le frontal et la plate-forme de l'ARJEL.	2	Audit de configuration de la plate-forme 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.				
			Le frontal doit comporter des fonctionnalités de sécurité visant à le protéger des attaques par saturation, qu'elles agissent :								
E61	ANN	3.1.1		- 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 (Naphtha, Sockstress, etc.) ;	2	Audit de configuration de la plate-forme 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.					
E62	ANN	3.1.1		- au niveau applicatif, avec l'envoi de multiples requêtes HTTP qui viseraient la saturation du frontal, qui constitue potentiellement un point de défaillance unique de l'architecture, afin de le protéger ; - d'un épuisement de ressources (saturation des enregistrements temporairement mis en tampon et en attente d'un acquittement) ; - d'une saturation du coffre avec des enregistrements mal formés.	2	Audit de configuration de la plate-forme d'hébergement, audit applicatif de type 'intrusif' de l'application capteur, notamment la description des dispositifs techniques mis en place par l'opérateur appuyée par des éléments de configuration.					
<b>Frontal : coffre-fort</b>											
E63	DET	4.1.1	Le coffre-fort doit détenir une certification de sécurité de premier niveau (CSPN) délivrée par l'ANSSI ( <a href="http://www.ssi.gouv.fr">http://www.ssi.gouv.fr</a> ).		3	L'absence de certification CSPN est rédhibitoire pour l'obtention de la certification du frontal.					
			La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des menaces :								
E64	DET	4.1.1		- le dépôt ou l'injection d'enregistrements non autorisés ;	3	Rapport et cible de la certification ANSSI/CSPN.					
E65	DET	4.1.1		- l'altération d'enregistrements ;	3	Rapport et cible de la certification ANSSI/CSPN.					
E66	DET	4.1.1		- le vol de données ;	3	Rapport et cible de la certification ANSSI/CSPN.					
E67	DET	4.1.1		- le déni de service.	3	Rapport et cible de la certification ANSSI/CSPN.					
			La certification de sécurité de premier niveau devra au minimum prendre en compte les éléments suivants, au niveau des fonctions de sécurité :								
E68	DET	4.1.1		- l'authentification forte des utilisateurs et administrateurs ;	3	Rapport et cible de la certification ANSSI/CSPN.					
E69	DET	4.1.1		- le chiffrement, la signature et l'horodatage des événements ;	3	Rapport et cible de la certification ANSSI/CSPN.					
E70	DET	4.1.1		- le chaînage des événements.	3	Rapport et cible de la certification ANSSI/CSPN.					
E71	DET	4.1.3	Toute suppression ou altération des données archivées, de manière malveillante ou non, doit pouvoir être identifiée par l'ARJEL.		3	Audit de configuration de la plate-forme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.					
			Quatre profils d'autorisation doivent pouvoir être définis :								
E72	DET	4.1.3		- profil « déposant » : profil attribué au module « capteur » du frontal de l'opérateur. Il permet uniquement d'écrire des traces dans le journal. Le module capteur du frontal 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 plate-forme d'hébergement. Documentation remise par l'opérateur.					
E73	DET	4.1.3		- profil « lecteur » : profil attribué aux agents de l'ARJEL 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 plate-forme d'hébergement. Documentation remise par l'opérateur.					
E74	DET	4.1.3		- 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 plate-forme d'hébergement. Documentation remise par l'opérateur.					
E75	DET	4.1.3		- profil « administrateur fonctionnel » : profil attribué aux personnes physiques de l'ARJEL ou désignées par l'ARJEL, 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 plate-forme d'hébergement. Documentation remise par l'opérateur.					
			Les certificats associés au profil « lecteur » sont utilisés :								
E76	DET	4.1.3		- 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 plate-forme d'hébergement. Documentation remise par l'opérateur.					
E77	DET	4.1.3		- 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 plate-forme d'hébergement. Documentation remise par l'opérateur.					
			En termes de gestion des clefs de chiffrement, de signature, et d'horodatage :								
E78	DET	4.1.3		- les tailles de clefs doivent être conformes aux règles énoncées dans le référentiel général de sécurité de l'ANSSI ( <a href="http://www.ssi.gouv.fr/">http://www.ssi.gouv.fr/</a> ) ;	3	Rapport et cible de la certification ANSSI/CSPN.					
E79	DET	4.1.5		- la cryptographie mise en œuvre en termes de générateurs de nombres pseudo-aléatoires, fonctions de hachage, algorithmes symétriques et asymétriques doit respecter les règles de bonnes pratiques spécifiées dans le référentiel général de sécurité de l'ANSSI ( <a href="http://www.ssi.gouv.fr/">http://www.ssi.gouv.fr/</a> ) ;	3	Rapport et cible de la certification ANSSI/CSPN.					
E80	DET	4.1.3		- un HSM est utilisé pour les opérations de signature ; le biclef de signature peut être soit injecté 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.				
E81	DET	4.1.3		- les données chiffrées le sont au moyen de la clef publique du certificat transmis par l'ARJEL : seule l'ARJEL 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 plate-forme d'hébergement. Documentation remise par l'opérateur.					
E82	DET	4.1.5	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 : en effet, dans le cadre d'un coffre mutualisé entre plusieurs agréments, chaque agrément doit faire l'objet d'un espace de stockage spécifique. Cette ségrégation des espaces de stockage doit, a fortiori, être implantée dans le cadre d'une mutualisation inter-opérateurs, le cas échéant.		3	Rapport et cible de la certification ANSSI/CSPN.					
			La sécurité physique des accès au coffre sera assurée par :								
E83	DET	4.1.3		- l'hébergement dans un emplacement protégé ;	2						
E84	DET	4.1.3		- la mise en place d'un contrôle d'accès ;	2	Audit de configuration de la plate-forme d'hébergement : une analyse de premier niveau de la sécurité physique de					

Matrices des exigences de la certification unique à 6 mois du composant frontal

E85	DET	4.1.3		- 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	l'infrastructure d'hébergement est attendue.			
E86	DET	4.1.6.a		- la mise en oeuvre de protections physiques	2	La méthode de scellement du coffre 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.			
<b>Frontal : capteur</b>									
E87	ANN	3.1.1	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. Le module capteur doit :		2	Audit applicatif de type 'intrusif' de l'application capteur. Documentation remise par l'opérateur.			
E88	ANN	3.1.1		- être authentifié par certificat auprès du coffre, 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 de type 'intrusif' de l'application capteur.	L'analyse doit être étayée par des extraits de code du capteur		
E89	ANN	3.1.1		- 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 de type 'intrusif' de l'application capteur. Voir les exigences dédiées aux fonctions de création et de stockage des traces.			
E90	DET	4.1.5		L'ensemble des composants doivent être synchronisés en temps, auprès d'une source de temps fiable.	3	Audit de configuration de la plate-forme d'hébergement.			
<b>Frontal : fonctions de création et de stockage des traces</b>									
La fonction de création de traces du capteur doit respecter les principes suivants :									
E91	DET	4.1.4		- la fonction de création de traces correspond à l'écriture de données liées à un événement de jeu ou à un compte joueur dans le module coffre-fort du frontal intercepte voire relaie le flux applicatif entre le joueur et l'opérateur. Elle doit donc être réalisée au niveau applicatif : - soit par interception protocolaire du flux HTTP ; - soit par insertion dans la logique de présentation de l'application.	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 de type 'intrusif' de l'application capteur.			
E92	DET	4.1.4		- la fonction de création de traces est implantée en amont de la logique de jeu : elle s'insère en coupure dans la chaîne de traitement des requêtes émises par le joueur vers la plateforme de jeux.	3				
E93	DET	4.1.4		- le frontal doit offrir une architecture dotée d'une très haute disponibilité avec redondance de mécanismes afin de strictement limiter les incidents potentiels de stockage.	3				
E94	DET	4.1.4		- le principe d'une annulation d'un jeu concerné par un incident de stockage d'un des événements doit être retenu.	2				
La fonction de création de traces d'un événement doit :									
E95	ANN	3.1.1		- être invoquée suite à une requête émise par le joueur (si celle-ci requiert un enregistrement). Cette requête peut résulter : - d'une action du joueur, à son initiative, comme une prise de pari ; - d'un acquittement par le joueur, suite à message transmis à l'initiative de la plate-forme, 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 de type 'intrusif' de l'application capteur.			
E96	ANN	3.1.1		- reposer sur un module applicatif à état qui respecte la cinématique de création décrite dans le schéma 3.1.1 de l'annexe du DET, et en particulier donner lieu à un enregistrement temporaire, conservé au niveau du capteur dans une mémoire tampon ou un dispositif de stockage temporaire équivalent (ex: base de données, par exemple), avant toute transmission au niveau du coffre et dans l'attente d'un acquittement de la plate-forme de jeux validant la bonne et due forme de cet événement.	3	Le respect de mode de fonctionnement à état assure que les événements transmis au coffre sont <u>générés à l'initiative du joueur</u> (action ou acquittement), mais sont <u>validés, avant stockage au coffre, par la plate-forme</u> .	Tout écart par rapport à ce mode de fonctionnement doit être techniquement justifié (ex : événements POPARTIE générés par la plate-forme de jeu, et transmis pour acquittement au joueur avant stockage).  Une analyse technique de la sécurité du processus de validation des événements par le capteur est attendue, appuyée par des éléments de configuration et par des éléments issus de l'analyse de l'audit applicatif de type 'intrusif' de l'application capteur.  Un mode de fonctionnement dans lequel les données transmises par le joueur seraient <u>directement</u> journalisées par le coffre est <u>réhibitoire</u> pour la certification du frontal. Idem pour des données transmises <u>directement</u> de la plate-forme de jeu vers le coffre, sans acquittement préalable par le joueur.		
E97	ANN	3.1.1		- gérer un acquittement de la plate-forme de jeux, afin de limiter les risques d'attaques qui viseraient à saturer le coffre d'événements aléatoires, ou à enregistrer des événements 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 de type 'intrusif' de l'application capteur.			
E98	ANN	3.1.1		- en cas d'acquiescement négatif de la part de la plate-forme 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 de type 'intrusif' de l'application capteur.			
E99	ANN	3.1.1		- en cas d'acquiescement positif de la part de la plate-forme de jeux, l'évènement présent en mémoire tampon au niveau du capteur peut être transformé au format exigé par l'ARJEL, pour son stockage par le coffre.	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 de type 'intrusif' de l'application capteur.			
E100	ANN	3.1.1		- gérer les cas d'acquiescements négatifs de la part du coffre, en cas de défaillance d'enregistrement.	2		Des mécanismes de reprise sur erreur peuvent être implantés au niveau du capteur, par exemple par des tentatives de retransmission au coffre d'un l'évènement.		

Matrices des exigences de la certification unique à 6 mois du composant frontal

E101	ANN	3.1.1		- garantir l'enregistrement d'un évènement de jeu au niveau du coffre, sous peine d'annulation de l'opération de jeu.	2	Cette exigence repose, dans le DET, sur un fonctionnement synchrone entre capteurs et coffres. Le capteur, dans ce modèle, doit attendre un acquiescement 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 files d'attente, 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 <i>in fine</i> par le coffre (ex : analyse du mécanisme de file d'attente de type ActiveMQ, par exemple).		
			Le stockage des données consiste en les étapes suivantes :						
E102	DET	4.1.5		- l'établissement d'un canal sécurisé, suite à l'authentification mutuelle du déposant avec le coffre, via une session TLS mutuellement authentifiée par certificat X.509v3 ;	3	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
E103	DET	4.1.5		- 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.		
E104	DET	4.1.5		- 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.			
E105	DET	4.1.5		- 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.			
E106	DET	4.1.5		- 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.			
E107	ANN	1.1.5		- 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.			
			Concernant les opérations de signature et de chiffrement :						
E108	DET	4.1.5		- le format de signature est XADES-T avec un jeton d'horodatage 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.		
E109	DET	4.1.5		- le chiffrement des données est réalisé au moyen de la clé publique de l'ARJEL 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.		
			Concernant le traitement par lots :						
E110	ANN	1.1.5		- 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.			
E111	ANN	1.1.5		- la granularité du traitement par lot doit être l'évènement.	1	Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur.			
			<b>Frontal : fonctions d'accès aux traces</b>						
			L'opérateur agréé doit fournir les éléments suivants pour chaque agrément :						
E112	DET	4.1.6		- 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.			
E113	DET	4.1.6		- 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.			
E114	DET	4.1.6		- un outil de validation des données du frontal et d'extraction des traces des opérations de jeu utilisable sur le site du frontal, et dans les laboratoires de l'ARJEL (mode hors-ligne).	3	Documentation remise par l'opérateur.			
			L'architecture de la partie coffre-fort du frontal doit distinguer :						
E115	DET	4.1.6		- un espace de stockage des données situé dans une zone réseau sécurisée ;	3	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.			
E116	DET	4.1.6		- une couche d'accès à l'espace de stockage accessible.	3	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur. Rapport et cible de la certification ANSSI/CSPN.			
E117	DET	4.1.6.a		Les données stockées dans le coffre doivent être en permanence accessibles à distance, depuis les locaux de l'ARJEL, i.e. depuis une ou plusieurs adresses IP identifiées.	3	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur.			
E118	DET	4.1.6.a		L'extraction du coffre 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.			
E119	DET	4.1.6		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'ARJEL.	2	Audit de configuration de la plate-forme d'hébergement. Rapport et cible de la certification ANSSI/CSPN. Documentation remise par l'opérateur + avis d'expert.			
			La couche d'accès expose un service web doté des deux principales interfaces suivantes :						
E120	DET	4.1.6		- 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.			
E121	DET	4.1.6		- 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.			
E122	DET	4.1.6		Les données doivent rester accessibles sur site sur toute la durée de conservation exigée par la loi (article 10 du Décret n° 2010-509 du 18 mai 2010).	3	Documentation remise par l'opérateur.			
E123	DET	4.1.6		Les données accessibles à distance doivent couvrir au moins les 12 derniers mois d'opération (période glissante).	3	Documentation remise par l'opérateur.			
			L'outil réalisé par l'opérateur doit permettre :						
E124	ANN	3.1.3		- d'interroger à distance le coffre de l'opérateur pour télécharger les traces demandées (outil de collecte) ;	3	Documentation remise par l'opérateur.			
E125	ANN	3.1.3		- 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.			
			L'outil doit implanter :						
E126	ANN	3.1.3.c		- l'interface WSDL définie par l'ARJEL, ou proposer une interface d'interrogation équivalente notamment basée sur l'identifiant d'opérateur, de coffre, sur l'agrément, et une tranche d'évènements ou de dates ;	1	Documentation remise par l'opérateur.			
E127	ANN	3.1.3		- les options en ligne de commande décrites dans la partie 3.1.3 de l'annexe au DET (fonctionnalités d'interrogation à distance) ;	1	Documentation remise par l'opérateur.			
E128	ANN	3.1.3		- le protocole TLS v1.1 au niveau du protocole de transport, et si possible, le triple d'algorithmes DHE-RSA-AES256-SHA ;	2	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.			

Matrices des exigences de la certification unique à 6 mois du composant frontal

<b>E129</b>	ANN	3.1.3		- 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.	<b>3</b>	Documentation remise par l'opérateur.		
			L'accès réseau de l'accès à distance doit :					
<b>E130</b>	ANN	3.1.3		- faire l'objet d'un filtrage implanté sous la forme d'une liste blanche au niveau d'un équipement de sécurité périmétrique de type pare-feu ;	<b>2</b>	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.	Un autre format de signature peut être implanté, à condition d'être justifié.	
<b>E131</b>	ANN	3.1.3		- faire l'objet d'une journalisation, et l'objet de procédures de traitement d'incident, le cas échéant.	<b>2</b>	Audit de configuration de la plate-forme d'hébergement. Documentation remise par l'opérateur + avis d'expert.		
<b>E132</b>	ANN	3.1.3.a	L'outil d'extraction et de validation des traces doit implanter les options décrites dans la partie 3.1.3.a de l'annexe au DET (fonctionnalités d'extraction des traces et de vérification).		<b>1</b>	Documentation remise par l'opérateur.		
<b>Évènements XML : généralités</b>								
			Les enregistrements XML sont :					
<b>E133</b>	ANN	1.1.1		- encodés au format UTF-8. On veillera en particulier au respect des caractères accentués (é, è, à) ;	<b>3</b>	Audit de code	L'analyse devra démontrer l'usage de filtres dans le code source	
<b>E134</b>	ANN	1.1.1		- conformes à la norme XML (en particulier en termes d'encodage des entités XML) ;	<b>3</b>			
<b>E135</b>	ANN	1.1.1		- conformes au schéma XSD publié par l'ARJEL ;	<b>3</b>			
<b>E136</b>	ANN	1.3		- filtrés, en termes de contenu, conformément aux expressions régulières (facette <i>pattern</i> ) décrites dans le schéma XSD ;	<b>3</b>			
<b>E137</b>	ANN	1.3		- 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.) ;	<b>3</b>			