

**DÉCISION N° 2020-059 DU 3 DÉCEMBRE 2020
PORTANT ADOPTION DES EXIGENCES TECHNIQUES RELATIVES
A L'INTERROGATION DU FICHIER DES INTERDITS DE JEUX**

Le collège de l'Autorité nationale des jeux,

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

Vu le code de la sécurité intérieure, notamment son article L.320-9 ;

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

Vu le décret n°2010-518 modifié relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux, notamment son article 22 ;

Vu la notification n° 2020/525/F adressée à la Commission européenne le 26 août 2020 ;

Après avoir entendu la commissaire du gouvernement, en ses observations, et en avoir délibéré le 3 décembre 2020,

DÉCIDE :

Article 1er : Les exigences techniques relatives aux modalités d'interrogation du fichier des interdits de jeux, prises en application de l'article L320-9 du code de la sécurité intérieure et annexées à la présente décision, sont adoptées.

Article 2 : Elles sont publiées sur le site Internet de l'Autorité.

Article 3 : Le directeur général de l'Autorité nationale des jeux est chargé de l'exécution de la présente décision.

Fait à Paris, le 3 décembre 2020.

La Présidente de l'Autorité nationale des jeux

I. FALQUE-PIERROTIN

EXIGENCES TECHNIQUES RELATIVES A L'INTERROGATION DU FICHIER DES INTERDITS DE JEUX EN APPLICATION DE L'ARTICLE L320-9 DU CODE DE LA SECURITE INTERIEURE

Le volume 4 des exigences techniques est relatif à l'interrogation du fichier des interdits de jeux. Il est pris sur le fondement de l'article 22 du décret n°2010-518 du 19 mai 2010 relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux. Il définit les procédures techniques à mettre en œuvre par les opérateurs afin de procéder à l'interrogation du fichier des Interdits de jeux en application dudit article.

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



SOMMAIRE

1	Rappel des dispositions légales et réglementaires.....	3
1.1	Code de la Sécurité intérieure.....	3
1.1.1	Article L. 320-9.....	3
1.1.2	Article L. 320-9-1.....	3
1.1.3	Article L. 320-10.....	3
1.2	Décret n°2010-518 modifié relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux.....	4
1.2.1	Article 7.....	4
1.2.2	Article 22.....	4
2	Portée de l'obligation.....	4
3	Modalités de vérification.....	5
3.1	Clef d'interrogation.....	5
3.2	Génération de la clef d'interrogation.....	6
4	Modalités techniques de connexion.....	8
4.1	Protocole d'interrogation.....	8
4.2	Format de la réponse DNS.....	9
4.3	Sécurisation du serveur DNS.....	10
4.4	Continuité de service et reprise sur erreur.....	10

1 Rappel des dispositions légales et réglementaires.

1.1 Code de la Sécurité intérieure.

1.1.1 Article L. 320-9.

« Les opérateurs de jeux d'argent et de hasard exploités en ligne ou sur des terminaux d'enregistrement physique sans intermédiation humaine au moyen d'un compte sont tenus de faire obstacle à la participation aux activités de jeu qu'ils proposent des personnes interdites de jeu en vertu des dispositions de l'article L. 320-9-1.

Les opérateurs de jeux d'argent et de hasard mentionnés aux 3°, 4° et 5° de l'article L. 320-6 s'assurent périodiquement que les personnes réalisant des opérations de jeux dans les postes d'enregistrement de jeux de loterie, de jeux de paris sportifs ou de paris hippiques au moyen d'un compte ne sont pas interdites de jeu en vertu de l'article L. 320-9-1. Tout compte joueur dont le titulaire est interdit de jeu est clôturé.

Les opérateurs mentionnés aux deux alinéas précédents clôturent tout compte joueur, dont le titulaire viendrait à faire l'objet d'une interdiction ou d'une exclusion selon les modalités fixées à l'article L. 320-10 ».

1.1.2 Article L. 320-9-1.

« I. Une interdiction de jeux peut être prononcée par l'autorité administrative compétente à l'égard des personnes dont le comportement est de nature à troubler l'ordre, la tranquillité ou le déroulement normal des jeux.

L'interdiction administrative de jeux s'applique à l'égard des jeux d'argent et de hasard proposés :

1° Dans les casinos ;

2° Sur les sites de jeux en ligne autorisés en vertu de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ;

3° Sur le site de jeux en ligne de la personne morale unique titulaire de droits exclusifs mentionnée à l'article 137 de la loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises ;

4° Sur les terminaux de jeux sans intermédiation humaine mentionnés au premier alinéa de l'article L. 320-9 ;

5° Sur les postes d'enregistrement mentionnés au deuxième alinéa de l'article L. 320-9.

Elle est prononcée pour une durée maximale de cinq ans.

II. Toute personne peut engager des démarches auprès de l'autorité administrative compétente afin d'empêcher sa participation à des jeux d'argent et de hasard.

L'interdiction volontaire de jeux s'applique à l'égard des jeux d'argent et de hasard visés aux 1° à 4° du I .

Elle est prononcée pour une durée de trois ans renouvelables tacitement ».

1.1.3 Article L. 320-10.

« Pour l'application de l'article L 320-9, le solde du compte est clôturé selon les modalités de l'article 17 de la loi n° 2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne ».

1.2 Décret n°2010-518 du 19 mai 2010 modifié¹ relatif à l'offre de jeux et de paris des opérateurs de jeux et à la mise à disposition de l'Autorité nationale des jeux des données de jeux.

1.2.1 Article 7.

« Sans préjudice des cas mentionnés aux articles 4 et 12, ainsi que des autres cas de clôture d'un compte pouvant être prévus dans le règlement portant conditions générales de l'offre de jeux et de paris, l'opérateur clôture sans délai un compte joueur lorsque son titulaire : /(...) 4° Vient à être interdit de jeu en application de l'article L. 320-9-1 du code de la sécurité intérieure ; (...) »

1.2.2 Article 22.

« Les opérateurs mentionnés au premier alinéa de l'article L. 320-9 du code de la sécurité intérieure s'assurent, par l'intermédiaire du système d'information de l'Autorité nationale des jeux, à l'ouverture du compte joueur puis à chaque connexion du joueur, que ce dernier n'est pas interdit de jeu en application de l'article L. 320-9-1 du même code.

Les opérateurs mentionnés au deuxième alinéa de l'article L. 320-9 de ce code s'assurent à l'ouverture du compte joueur puis au moins chaque jour où le joueur réalise des opérations de jeux dans les postes d'enregistrement de jeux de loterie, de jeux de paris sportifs ou de paris hippiques au moyen d'un compte que ce joueur n'est pas interdit de jeux en application de l'article L. 320-9-1 dudit code.

Les modalités de cette vérification ainsi que les modalités techniques de connexion au système d'information de l'Autorité nationale des jeux permettant à l'opérateur de procéder à ces vérifications sont déterminées par celle-ci ».

2 Portée de l'obligation.

En application des dispositions combinées des articles L320-9 du code de sécurité intérieure et 22 du décret n°2010-518 du 19 mai 2010 modifié, les opérateurs de jeux d'argent et de hasard sont tenus d'interroger le fichier des interdits :

- pour l'activité de jeux en ligne ou au moyen d'un compte joueur sur borne en réseau physique
 - o lors de l'ouverture d'un compte joueur ;
 - o à chaque connexion pour l'activité à partir du site de l'opérateur ou à partir d'une borne ;
 - o et, en tout état de cause, au moins à la première action journalière de mise ou de dépôt pour l'activité à partir d'une application mobile.
- pour l'activité au moyen d'un compte joueur dans les postes d'enregistrement (prise de paris téléphonique et SMS incluses, mais hors bornes)
 - o lors de l'ouverture d'un compte joueur ;
 - o puis au moins une fois par jour, le moment étant laissé au choix de l'opérateur.

Par ailleurs, les articles L. 320-10 du code de sécurité intérieure et l'article 7 du décret précité, quant à eux, prévoient que les opérateurs clôturent immédiatement le compte d'un joueur, dont l'interrogation du fichier révèle qu'il y est inscrit.

¹ Modifié par les dispositions du n° 2020-494 du 28 avril 2020 relatif aux modalités de mise à disposition de l'offre de jeux et des données de jeux

3 Modalités de mise en oeuvre

La mise en œuvre des dispositions de l'article 22 du décret n°2010-518 du 19 mai 2010 implique que:

- les services de l'Autorité mettent à jour le fichier de manière continue, à mesure que sont enregistrées des demandes d'inscription à celui-ci, une fois la procédure de vérification achevée ;
- les opérateurs consultent le fichier des interdits de jeux selon l'une des deux modalités mentionnées au point précédent pour déterminer le droit d'un joueur à utiliser ses services deux modalités (vérification à chaque connexion ou au moins une fois par jour, selon le canal par lequel le joueur accède à l'offre de jeu).

Dans un cas comme dans l'autre, le référentiel utilisé dans le cadre de cette vérification peut être :

- le service DNS mis à disposition par l'Autorité et selon des dispositions décrites dans la suite du présent document ;
- un référentiel local au SI de l'opérateur. Dans ce cas, l'opérateur réalisera la mise à jour quotidienne dudit référentiel dans les tranches horaires que lui attribuera l'Autorité.

Ces dispositions sont mises en place au titre d'une phase transitoire permettant à l'ensemble des acteurs de disposer d'un temps raisonnable afin de mettre leur système en conformité avec le nouveau cadre réglementaire rappelé précédemment.

Un bilan du fonctionnement du dispositif interviendra six mois après l'entrée en vigueur de période transitoire décrite précédemment. A l'issue de cette période, les opérateurs de jeux d'argent et de hasard exploités en ligne ou sur des terminaux d'enregistrement physique sans intermédiation humaine au moyen d'un compte seront tenus, quel que soit le cas de figure, de s'assurer par l'intermédiaire du système d'information de l'Autorité nationale des jeux, à l'ouverture du compte joueur puis à chaque connexion du joueur, que ce dernier n'est pas interdit de jeu en application de l'article L. 320-9-1 du code de sécurité intérieure.

4 Modalités de vérification.

4.1 Clef d'interrogation.

La consultation du fichier des interdits pour déterminer si tel ou tel compte est interdit se fait sur la base d'une interrogation construite à partir des paramètres suivants :

- premier prénom du joueur ;
- nom patronymique ou dit « de naissance » ;
- date de naissance.

Remarques :

L'attention est appelée sur le fait que l'article 2 du décret n°2010-518² prévoit la communication du nom de naissance. La prise en compte du seul nom d'usage constitue donc un manquement, d'une part, aux dispositions du décret et, d'autre part, aux présentes exigences.

Par ailleurs, pour pallier les éventuelles inversions de prénoms, il est recommandé de procéder à une interrogation pour chacun des prénoms des joueurs, le cas échéant.

² Aux termes de l'article 2 du décret susmentionné : « Lorsqu'une personne sollicite l'ouverture d'un compte joueur auprès d'un opérateur agréé de jeux ou de paris en ligne ou d'un opérateur titulaire de droits exclusifs, celui-ci, préalablement à l'ouverture de ce compte, lui demande : / 1° De lui communiquer nom de naissance, prénoms, date et lieu de naissance ainsi que son adresse postale. L'opérateur peut en outre demander à la personne sollicitant l'ouverture d'un compte de lui communiquer une adresse électronique. (...) »

Afin d'assurer la confidentialité de ces informations, la clef est le résultat d'une fonction de hachage indexée par un secret partagé entre l'opérateur de jeux et l'ANJ.

La fonction mise en œuvre est *hmac-sha1*. Le secret partagé est échangé de façon sécurisée entre l'opérateur et l'ANJ : le secret partagé *HMAC*, ainsi que la clef *TSIG* d'interrogation DNS sont remis à l'opérateur au format papier lors du dépôt de la demande d'agrément. Ces éléments peuvent ultérieurement faire l'objet d'un renouvellement.

Pour des raisons techniques, cette clef d'interrogation reste suffixée dans un premier temps par le domaine *interdits-ARJEL.fr*.

Elle le sera ensuite, dans un second temps, par le par le domaine *interdits-ANJ.fr*. Les opérateurs seront informés par une publication sur le site de l'ANJ, ainsi que par message électronique.

4.2 Génération de la clef d'interrogation.

Les paramètres précédents sont mis sous forme canonique³, en particulier :

- le nom patronymique ou dit « de naissance » et le prénom sur lequel porte l'interrogation sont concaténés, et font chacun l'objet d'une normalisation (mise sous forme canonique), avec :
 - o la suppression des diacritiques indépendamment de la casse (accents aigus, graves et circonflexes, trémas et cédilles),
 - o le passage à la casse supérieure,
 - o la suppression des caractères hors de la classe de caractères **[A-Z]** ;
- la date de naissance est normalisée au format "**AAAAMMJJ**" (chaîne de caractères).

Le résultat de sortie obtenu doit être identique pour tout encodage de caractères considéré en entrée (qu'en entrée la chaîne soit en ISO8859-1[5] en UTF-8, ou autres.).

Pour la mise sous forme canonique des nom et prénom, les caractères accentués sont traduits vers les caractères ASCII équivalents, par exemple, de la façon suivante :

Caractère	Caractère ASCII	code(s) ASCII (hexa)
à	A	0x41
â	A	0x41
ä	A	0x41
ç	C	0x43
é	E	0x45
è	E	0x45
ê	E	0x45
ë	E	0x45
î	I	0x49
ï	I	0x49
ô	O	0x4F
ö	O	0x4F

Caractère	Caractère ASCII	code(s) ASCII (hexa)
À	A	0x41
Â	A	0x41
Ä	A	0x41
Ç	C	0x43
É	E	0x45
È	E	0x45
Ê	E	0x45
Ë	E	0x45
Î	I	0x49
Ï	I	0x49
Ô	O	0x4F
Ö	O	0x4F

³ La mise en forme canonique est le procédé par lequel on convertit des données qui ont plusieurs représentations possibles vers un format standard. On en éprouve généralement le besoin lorsque l'on veut pouvoir faire des comparaisons logiques, pour améliorer l'efficacité de certains algorithmes en éliminant les évaluations superflues, ou pour permettre d'ordonner des éléments en fonction de leur sens.

ù	U	0x45
û	U	0x45
ü	U	0x45
ÿ	Y	0x45
æ	Æ	0x41 0x45
œ	Œ	0x4F 0x45

Û	U	0x45
Ū	U	0x45
Ů	U	0x45
Ÿ	Y	0x45
Æ	Æ	0x41 0x45
Œ	Œ	0x4F 0x45

Exemple de mise sous forme canonique :

Soit l'utilisateur Grégory Dupont, né le 1er janvier 1970 à Paris.

La forme canonique formée par le prénom et le nom est la chaîne **GREGORYDUPONT** (expression régulière **[A-Z]+**). La forme canonique de la date est **19700101**. Leur concaténation est **GREGORYDUPONT19700101** (expression régulière **[A-Z]+[0-9]{8}**).

Ce texte et la clef partagée sont passés en entrée de la fonction hmac-sha1. L'empreinte hmac-sha1 doit être générée au format hexadécimal, soit une chaîne de 40 caractères imprimables (expression régulière **[a-z0-9]{40}**).

```

graph TD
    Input["Grégory Dupont 01/01/1970"] -- "Mise sous forme canonique" --> Canonical["GREGORYDUPONT19700101"]
    Canonical --> HMAC((HMAC SHA1))
    Secret["Secret partagé"] --> HMAC
    HMAC --> Output["9deec2[...]51d62f"]
    Output --- Identifier["Identifiant"]
  
```

Autres exemples :

Nom	Prénom	Date de naissance	Forme canonique	Secret	Empreinte
Dupont	Jean	30/02/1970	JEANDUPONT19700230	Secret!	56a48a5d07a0f82108f9032fc01af423d45085f8
LÆN	Lætitia	30/02/1970	LAETITALAEN19700230	123456	61f74c57b5e7eb1b9ca944d1d258a4cddb23a7cd
Raphaël Œne	Éléonore	30/02/1970	ELEONORERAPHAELOENE19700230	Bonjour1	f3b9d28ce7ee70d3125d1d5f26f6fc311b1f2539

5 Modalités techniques de connexion.

L'opérateur doit interroger une infrastructure mise à disposition des opérateurs par l'ANJ. Les interrogations menées par les opérateurs obtiennent une réponse binaire : absence ou présence dans la liste.

Le protocole d'interrogation est un mécanisme d'interrogation de liste noire DNS (DNSBL) avec, pour clef d'interrogation, une empreinte cryptographique *hmac-sha1* calculée sur la base des champs nom, prénom et date de naissance du joueur.

Les échanges DNS sont authentifiés à l'aide de l'extension DNS *TSIG*. L'opérateur doit impérativement utiliser la clef *TSIG* qui lui est dédiée et lui a été affectée lors de sa demande d'agrément.

En cas de réponse positive du système d'interrogation DNSBL, i.e. lorsque le joueur est présent dans la liste des interdits de jeux, un enregistrement de ressources de type A est défini, ainsi qu'un enregistrement TXT référençant le lieu de naissance du joueur.

La zone DNS interrogée demeure *interdits-ANJ.fr*.

Pour des raisons techniques, cette clef d'interrogation reste suffixée dans un premier temps par le domaine *interdits-ARJEL.fr*.

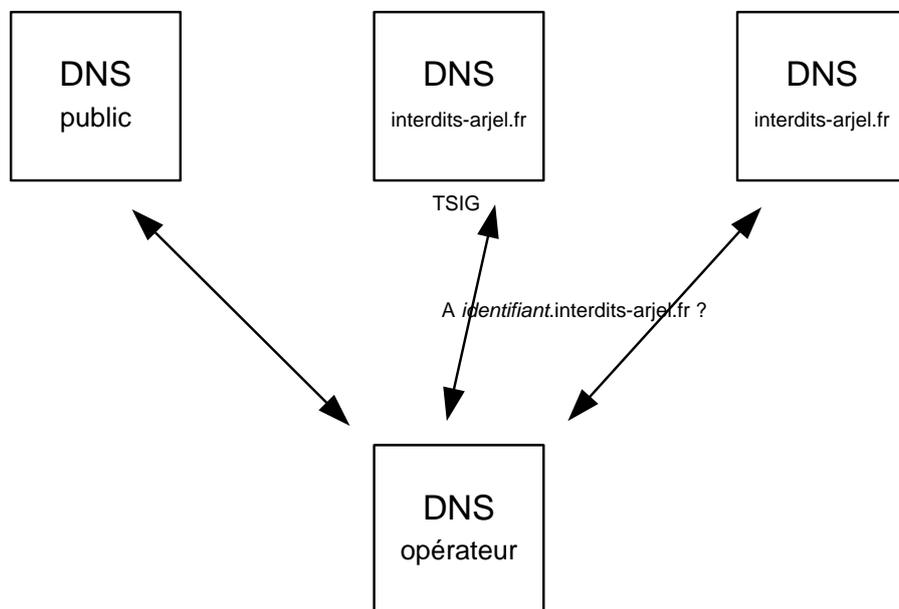
Elle le sera ensuite, dans un second temps, par le par le domaine *interdits-ANJ.fr*. Les opérateurs seront notifiés par information publiée sur le site de l'ANJ, ainsi que par message électronique.

L'architecture DNS mise en place par l'ANJ est redondante : l'opérateur doit donc ordonnancer ses interrogations en respectant le principe du **round-robin DNS**, afin de répartir la charge de ses interrogations entre les différents serveurs autoritaires pour cette zone. **Il est en particulier proscrit que les interrogations effectuées par un opérateur soient effectuées à destination d'un seul et même serveur.**

5.1 Protocole d'interrogation.

Afin que le dispositif concilie haute-disponibilité, extensibilité et sécurité des transactions, les interrogations s'appuient sur le protocole DNS, avec la mise en œuvre de l'extension de sécurité *TSIG*.

Le schéma de principe est le suivant :



- l'application génère, à partir des identifiants du joueur, la clef d'interrogation grâce à la fonction *hmac-sha1* et du secret partagé avec l'ANJ. Cet identifiant correspond au suffixe du nom de domaine pleinement qualifié qui fera l'objet d'une interrogation ;

- l'application effectue une résolution sur le nom *identifiant.interdits-ANJ.fr*. La demande de résolution peut porter sur :
 - o l'enregistrement de ressources A associé au nom de domaine pleinement qualifié ;
 - o l'enregistrement de ressources TXT.

Remarques :

- si l'enregistrement de ressources A est absent, le joueur ayant fait l'objet de l'interrogation ne figure pas dans le fichier des interdits de jeux et peut poursuivre son inscription ou son accès au site. Dans le cas contraire, l'accès lui est interdit après vérification de la concordance du lieu de naissance ;
- il est fortement recommandé que la résolution soit effectuée par le biais d'un serveur DNS configuré pour répondre récursivement aux demandes de la plateforme et que l'implantation au niveau logiciel de jeu consiste en de simples appels au résolveur natif du système. En particulier, l'implantation du protocole DNS et de l'extension TSIG au cœur de l'application n'est absolument pas recommandée ;
- le serveur DNS doit être géré par l'opérateur et dédié à l'interrogation du fichier des interdits. Le protocole DNS entre le résolveur de l'opérateur et les DNS de l'ANJ doit impérativement être sécurisé avec l'extension de sécurité TSIG assurant l'authenticité des transactions, avec le secret TSIG partagé avec les serveurs DNS de l'ANJ.
- la mise en cache des réponses en provenance du système de DNS des interdits n'est pas souhaitable, cependant elle pourra être admise si le TTL associé n'excède pas 3sec

5.2 Format de la réponse DNS.

En cas d'absence du joueur dans la liste des interdits de jeux, une erreur de type *NXDOMAIN* est transmise.

En cas de présence du joueur :

- l'enregistrement de ressources de type A associé est toujours *127.0.0.42* ;
- l'enregistrement de ressources de type TXT contient une chaîne de caractères formatée de la façon suivante :
 - o si le pays de naissance de la personne interdite est la France, le format de la réponse est "*COMMUNE; DEPARTEMENT; PAYS*", (PAYS au sens des COG INSEE), par exemple : "*TROUVILLE; SEINE-MARITIME; FRANCE*" et "*POINTE-A-PITRE; GUADELOUPE; GUADELOUPE*" ;
 - o si le pays de naissance de la personne interdite est un pays ou territoire étranger, le format de la réponse est "*COMMUNE; PAYS*", par exemple "*MADRID; ESPAGNE*".

En termes de format, les pays, départements et communes français respectent exactement (i.e. au caractère près) le code officiel géographique de l'INSEE. En particulier, les nomenclatures suivantes sont prises comme références :

- noms de communes : "Liste des communes", colonne NCC ;
- noms de départements : "Liste des départements", colonne NCC ;
- noms de pays: "Liste des pays et territoires étrangers", colonne LIBCOG.

Ces listes sont, au moment de la rédaction de ce dossier des exigences techniques, téléchargeables sur le site de l'INSEE, à l'adresse suivante : <https://www.insee.fr/fr/information/2560452>.

Les termes NCC et LIBCOG sont définis à l'adresse suivante : <https://www.insee.fr/fr/information/4316058>.

Seules les communes situées en pays et territoires étrangers ne sont pas soumises à cette normalisation. En pratique dans ces cas de figure, la convention d'écriture suivante est appliquée à ces communes (convention identique à celle appliquée aux communes françaises) :

- suppression des diacritiques ;
- passage à la casse supérieure ;
- suppression des déterminants ;
- remplacement des espaces (simples) par des tirets.

Exemples de réponses valides :

- "CLERMONT-FERRAND; PUY-DE-DOME; FRANCE"
- "TOULON; VAR; FRANCE"
- "BAGNOLET; SEINE-SAINT-DENIS; FRANCE"
- "LAUSANNE; SUISSE"

Enregistrements d'exemples :

Les enregistrements d'exemples suivants sont présents dans le système des interdits de jeux. Ces enregistrements peuvent être interrogés aussi bien par les opérateurs agréés, que par les opérateurs, dont la demande d'agrément est en cours d'instruction : ils sont définis dans la vue DNS dédiée aux opérateurs agréés, ainsi que dans celle dédiée aux opérateurs disposant d'une clef TSIG ayant déposé une demande. Une clef TSIG valide, ainsi que le secret indexant le calcul de l'empreinte hmac-sha1 sont nécessaires. Pour rappel, ces deux éléments sont remis à l'opérateur lors du dépôt de la demande d'agrément.

1	<i>abcdef</i> (nom)	<i>ghijkl</i> (prénom)	17/10/1929 (date)
	<i>SOCCIA; HAUTE-CORSE; FRANCE</i> (réponse)		
2	<i>Abcdef</i>	<i>Ghijkl</i>	01/11/1953
	<i>PARIS; PARIS; France</i>		
3	<i>Abc Def</i>	<i>Ghi jkl</i>	12/12/1972
	<i>HAGUENAU; BAS-RHIN; France</i>		
4	<i>Àbc D É f</i>	<i>Ghĭ j k l</i>	28/04/1989
	<i>LYON; RHONE; France</i>		
5	<i>ABC () *+ . / : DEF</i>	<i>=?ghi!@_ -jkl</i>	02/09/1941
	<i>MARSEILLE; BOUCHES-DU-RHONE; France</i>		
6	<i>ÀÄÅÇÈÉÊËÏÎÏÏÛÜÛÿ&ç</i>	<i>àääçéèèëïïôöùüÿæ&</i>	30/10/1938
	<i>SAINT-GERMAIN-EN-LAYE; YVELINES; France</i>		
7	<i>ÀÄÅÇÈÉÊËÏÎÏ 123</i>	<i>àääçéèèëïïô 456</i>	07/02/1947
	<i>POINTE-A-PITRE; GUADELOUPE; GUADELOUPE</i>		

5.3 Sécurisation du serveur DNS.

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 jeux, 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, en complément des mesures de sécurisation TSIG fondées sur un secret partagé qui seront associés à ces adresses.

La clef TSIG est fournie à l'opérateur par l'ANJ. Cette clef, ainsi que le secret partagé *hmac-sha1*, font l'objet d'un renouvellement périodique. Pendant les phases de transition entre deux clefs hmac-sha1, deux empreintes seront calculées pour chaque enregistrement.

5.4 Continuité de service et reprise sur erreur.

Bien que le dispositif soit conçu pour offrir un très haut niveau de disponibilité, il ne peut être exclu qu'en certaines circonstances exceptionnelles une réponse ne puisse être obtenue ou ne soit pas conforme au format attendu.

Cette situation est naturellement délicate car un joueur potentiellement interdit aurait eu ainsi la possibilité de jouer.

Cette éventualité a été prise en compte afin de définir un processus de réaction adapté, qui permette de restaurer rapidement la continuité du service.

Aussi, afin de permettre aux opérateurs de poursuivre leur activité et alors que les conditions techniques ne permettraient pas la vérification immédiate du statut d'interdiction de leurs joueurs, **les opérateurs seront autorisés à laisser les actions du joueur se dérouler, à la condition expresse qu'il n'y ait pas d'exécution du pari ou de l'opération jeu tant que la réponse à l'interrogation du fichier des interdits n'a pas été obtenue.**

Afin de permettre la continuité de service coté plateforme de jeux, tout en conservant la possibilité de recevoir une réponse nominale du système DNS des Interdits de jeux, un mécanisme de reprise d'interrogation en cas d'échec doit être implémenté selon les modalités précisées ci-après.

Ce n'est que lorsque l'appel est en échec sur l'ensemble des serveurs du dispositif que cette procédure de reprise doit être mise en œuvre, le principe de base restant l'interrogation selon le principe du **round-robin DNS**.

L'opérateur mettra donc en place le mécanisme de reprise d'interrogation suivant :

- Un nouveau cycle d'interrogation est initialisé à intervalle régulier tant qu'une réponse nominale (***NXDOMAIN*** ou détails demandeur tels que décrits plus haut) n'est pas reçue ;
- La durée des intervalles n'est pas linéaire :
 - o Chaque durée correspond au double de la précédente ;
 - o Au-delà d'une heure, la durée de l'intervalle est constante : chaque tentative est espacée d'une heure.

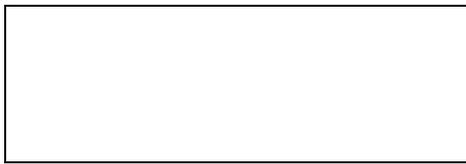
Enfin, en cas d'indisponibilité longue du service, qui ne peut être théoriquement écartée, l'Autorité mettra en place, dans les meilleurs délais possibles, un dispositif alternatif permettant de procéder à la vérification des statuts des joueurs.

Il reste que cette situation restera très délicate puisqu'un joueur « interdit » aura eu la possibilité de jouer. Et que s'il a enregistré des gains, il sera difficile de les annuler.

Exemple de durée d'intervalle entre deux tentatives :

	Temps en seconde après le dernier échec
essai 1	1
essai 2	2
essai 3	4
essai 4	8
essai 5	16
essai 6	32
essai 7	64
essai 8	128
essai 9	256
essai 10	512
essai 11	1024
essai 12	2048

	Temps en seconde après le dernier échec
essai 1	0,1
essai 2	0,2
essai 3	0,4
essai 4	0,8
essai 5	1,6
essai 6	3,2
essai 7	6,4
essai 8	12,8
essai 9	25,6
essai 10	51,2
essai 11	102,4
essai 12	204,8
essai 13	409,6



essai 14	819,2
essai 15	1638,4
essai 16	3276,8

En tout état de cause, toute anomalie dans l'interrogation du fichier, sous réserve de l'application du principe de round-robin DNS, doit être immédiatement signalée à l'ANJ.