COLLEGE DE L'AUTORITE DE REGULATION DES JEUX EN LIGNE

DECISION N° 2013-092 EN DATE DU 28 NOVEMBRE 2013

Le collège de l'Autorité de régulation des jeux en ligne ;

Vu l'article L. 131-16-1 du code du sport ;

Vu les articles R. 131-37 et suivants du code du sport, créés par le décret n° 2013-947 du 22 octobre 2013 pris pour l'application de l'article L. 131-16-1 du code du sport et relatif aux interdictions de paris sportifs ;

Vu 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 ;

Après en avoir délibéré le 28 novembre 2013 ;

MOTIFS DE LA DECISION :

Considérant que l'article L. 131-16-1 du code du sport dispose que :

> *« L'accès d'une fédération délégataire, en vue de la mise en œuvre d'une éventuelle procédure disciplinaire contre un acteur d'une compétition sportive qui aurait parié sur celle-ci, à des informations personnelles relatives à des opérations de jeu enregistrées par un opérateur de jeux ou de paris en ligne titulaire de l'agrément prévu à l'article 21 de la loi n° 2010-476 du 12 mai précitée s'effectue par demande adressée à l'Autorité de régulation des jeux en ligne.*
>
> *L'Autorité de régulation des jeux en ligne communique à des agents de la fédération délégataire spécialement habilités à cette fin, dans des conditions prévues par décret les éléments strictement nécessaires, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »*

Considérant que l'article R. 131-41 du code du sport prévoit que :

> *« L'Autorité de régulation des jeux en ligne définit :*
> *1° La nomenclature des compétitions qui doit être utilisée pour présenter les informations mentionnées dans le cadre de la demande prévue au 2° de l'article R. 131-42 ;*
> *2° Les modalités techniques de transmission et de traitement de la demande prévue à l'article R. 131-43 du code du sport. »*

Considérant que l'Autorité de régulation des jeux en ligne met à disposition des fédérations délégataires un dispositif informatique d'interrogation en application de l'article L. 131-16-1 du code du sport ;

Considérant que l'Autorité a défini la nomenclature des compétitions pour l'enregistrement des données par les opérateurs de paris sportifs agréés conformément au dossier des exigences techniques (DET) ; que cette nomenclature et ses évolutions successives sont utilisées pour présenter les informations mentionnées dans le cadre de la demande prévue au 2° de l'article R. 131-42 du code du sport et sont donc intégrées à ce titre dans le dispositif informatique permettant d'interroger l'ARJEL ;

Considérant que les modalités techniques de transmission et de traitement de la demande sont établies dans un document spécifique ;

DECIDE :

Article 1er – Les modalités techniques de transmission et de traitement de la demande prévue à l'article R. 131-43 du code du sport et relatif aux interdictions de paris sportifs sont adoptées et font corps avec la présente décision à laquelle elles sont jointes.

Article 2 – Le directeur général de l'Autorité est chargé de l'exécution de la présente décision qui sera publiée sur le site Internet de l'Autorité de régulation des jeux en ligne.

Fait à Paris, le 28 novembre 2013 ;

Le Président de l'Autorité de régulation des jeux en ligne

Jean-François VILOTTE

Décision mise en ligne sur le site officiel de l'ARJEL le 28 novembre 2013

Autorité de régulation des jeux en ligne
RÉPUBLIQUE FRANÇAISE

Modalités techniques de transmission et de traitement de la demande prévue à l'article R. 131-43 du code du sport

V1.0 du jeudi 28 novembre 2013

AVERTISSEMENT : Les fédérations délégataires qui interrogent l'ARJEL devront s'assurer, sous leur seule responsabilité, que les personnes visées dans leurs demandes étaient effectivement soumises à une interdiction de parier sur la compétition concernée (licenciées et interdiction prévue par le règlement) pendant la période pour laquelle elles présentent cette demande de vérification.

Le décret n°2013-947 du 22 octobre 2013 pris pour l'application de l'article L.131-16-1 du code du sport et relatif aux interdictions de paris sportifs, autorise les fédérations délégataires qui organisent ou autorisent des compétitions sportives faisant l'objet de paris sportifs à constituer un traitement informatisé de données à caractère personnel relatives aux acteurs de ces compétitions afin de pouvoir contrôler le respect de l'interdiction de parier faite à ces derniers.

L'article R.131-41 du code du sport prévoit que l'Autorité de régulation des jeux en ligne (ARJEL) définit les modalités techniques de transmission et de traitement de la demande prévue à l'article R.131-43.

La mise en œuvre de ce dispositif s'inscrit dans le respect des dispositions du référentiel général de sécurité (RGS) s'agissant des échanges électroniques entre l'ARJEL et les fédérations délégataires.

Pour ce traitement, l'ARJEL met en œuvre un service dématérialisé et sécurisé conçu autour de deux composants essentiels:

- ✓ **un dispositif « externe » de recueil des demandes** effectuées par les fédérations délégataires ;
- ✓ **un dispositif « interne » de rapprochement de ces demandes avec les opérations de jeu** collectées auprès des supports matériels de recueil et d'archivage sécurisé mis en œuvre par les opérateurs agréés.

Ce document est constitué d'une note principale synthétisant l'ensemble du processus ainsi que de différentes annexes permettant de revenir de façon détaillée sur les différents thèmes abordés dans le texte principal.

ANNEXE I : Informations préalables à fournir à l'ARJEL

ANNEXE II: Configuration technique des postes utilisés pour les requêtes

ANNEXE III : Installation du certificat électronique

ANNEXE IV : Mode d'emploi détaillé du dispositif de recueil des demandes

ANNEXE V : Règles de sécurité des postes utilisés pour les requêtes

I - Dispositif « externe » de recueil des demandes des fédérations délégataires

Le dispositif de recueil des demandes est exclusivement électronique et est mis à la disposition des seuls agents habilités par les fédérations délégataires. L'article R. 131-42 du code du sport prévoit que ces agents, habilités par le président d'une fédération afin de transmettre à l'ARJEL les demandes de rapprochement, doivent disposer des compétences techniques et juridiques adéquates.

Dès réception de la décision d'habilitation d'un agent, les services de l'ARJEL lui font parvenir **un certificat électronique personnel** nécessaire au bon fonctionnement du service (cf. Annexe III pour l'installation du certificat électronique). Selon son appréciation et notamment dans le but de faire progresser le niveau de sécurité du dispositif, l'ARJEL se réserve le droit de faire parvenir de nouveaux certificats aux agents habilités ou de remplacer l'usage des certificats par l'utilisation d'un support matériel de type « carte à puce » ou clé USB dédiée. Les services de l'ARJEL prendront alors en charge la génération et le déploiement des outils nécessaires, assurant un chiffrement à l'état de l'art.

L'accès au dispositif de recueil est réalisé au travers d'une interface sécurisée par protocole « https » en provenance d'une ou de plusieurs adresses IP fixes préalablement portées à la connaissance de l'ARJEL (cf. Annexe I pour la liste des **informations préalables** qui doivent être déclarées à l'ARJEL). L'ARJEL recommande aux fédérations concernées de dédier un poste informatique à cet usage, sécurisé selon l'état de l'art (cf. Annexe V). La configuration technique nécessaire du ou des postes de travail est précisée dans l'Annexe II.

Après fourniture à l'ARJEL des **informations préalables** puis installation du **certificat électronique** fourni, le dispositif de recueil des demandes est rendu accessible par Internet à travers :

- ✓ un navigateur internet pour une saisie manuelle des requêtes ou une saisie multiple par l'intermédiaire d'un fichier de données de type « CSV » ;
- ✓ une interface d'échange par « service web » permettant une saisie automatisée des requêtes et instrumentée par les fédérations délégataires.

I.1 Recueil des demandes par navigateur internet

L'Annexe IV correspond au mode d'emploi détaillé du site internet mis à disposition par l'ARJEL pour ce type de demande. Ce paragraphe I.1 synthétise les fonctionnalités principales du site.

L'usage de l'interface web via un navigateur internet permet de procéder à deux types de demande, la saisie manuelle ou l'envoi d'un fichier. Le choix entre ces deux méthodes est accessible depuis la page principale du site.

I.1.1 La saisie manuelle des requêtes

Cette méthode convient à des demandes ponctuelles, unitaires ou limitées à quelques interrogations.

Une requête unitaire sera constituée des éléments suivants :

- les données d'identification de l'acteur de la compétition visées par l'article R131-38 du code de sport, à savoir les nom, prénom(s), date et ville de naissance de la personne concernée. On indiquera le pays de naissance à la place de la ville de naissance pour les personnes nées à l'étranger ;
- les informations permettant de décrire la ou les compétition(s) faisant l'objet de l'interdiction ;
- la période de temps sur laquelle les vérifications doivent porter.

L'agent habilité indique la compétition pour laquelle une interdiction a été posée à un acteur de compétition par sa fédération. Cette saisie est assistée : selon le contexte, les possibilités de saisie sont suggérées au fil de la frappe ou présentées sous forme de menus déroulants. Si la vérification doit être effectuée au niveau de plusieurs compétitions, plusieurs requêtes doivent être réalisées.

La prise en compte de la demande est matérialisée par l'affichage d'un récapitulatif sans informations nominatives associées. Un identifiant de demande (**Ticket**) est associé à l'affichage. Cet identifiant prend la forme d'un code alphanumérique ; il est attribué par le dispositif de recueil des demandes qui en garantit l'unicité pendant la période de traitement (il est susceptible d'être réutilisé ensuite) et permet à la fédération délégataire d'assurer le suivi du traitement de sa demande.

En mode « saisie manuelle », lorsqu'un fichier regroupant plusieurs requêtes unitaires est adressé au dispositif de recueil des demandes, ce dernier retourne autant d'identifiants de demande que de requêtes.

I.1.2 L’envoi d’un fichier au format CSV

Cette méthode convient à des demandes plus nombreuses, par le dépôt d’un fichier multi-lignes.

La saisie des informations permettant de sélectionner la ou les compétition(s) faisant l’objet de l’interdiction est identique, seul l’écran de saisie manuelle de l’identité est remplacé par un écran de sélection de fichier multi-lignes. Le fichier multi-lignes (au format dit « CSV ») permet de regrouper plusieurs requêtes.

Le format qui doit être utilisé est le suivant :

`prénom;nom;AAAA-MM-JJ;ville` (si naissance en France)

`prénom;nom;AAAA-MM-JJ;pays` (si naissance à l’étranger)

Une attention toute particulière doit être apportée à la constitution du fichier, sous peine d’invalider les demandes malformées ou décalées.

Un identifiant de demande (ticket) sera associé à chaque requête unitaire incluse dans la demande globale. Il y aura donc autant de tickets que de lignes dans la demande.

I.2 Dispositif de recueil des demandes via une interface d'échange par service web

Un dispositif de recueil des demandes via un service web est également mis en place. Il permet une saisie automatisée des requêtes par les fédérations délégataires.

Le modèle d'architecture déployé est le modèle *REST* (Representational State Transfer) créé en 2000 par Roy Fielding.

L'ARJEL rend disponible sur son site www.arjel.fr les ressources techniques associées afin de permettre aux fédérations délégataires familières avec ce type de modèle de d'automatiser les requêtes nécessaires et d'interpréter les réponses de dépôt reçues.

II. Dispositif « interne » de rapprochement des demandes avec les opérations de jeu

Les données d'identification transmises par les fédérations ne sont pas conservées durablement par les systèmes informatiques de l'ARJEL. Les informations nominatives sont automatiquement condensées sous la forme d'une empreinte cryptographique, non réversible, sur la base de laquelle reposera le **dispositif « interne »** de rapprochement. A l'issue du traitement, ces informations sont effacées selon des procédés logiciels robustes aux techniques de récupération de données.

Le dispositif de rapprochement avec les opérations de jeu détenues par l'ARJEL fonctionne sur la base des éléments suivants :

- l'empreinte cryptographique, calculée à partir des informations nominatives communiquées par les fédérations délégataires. Cette empreinte figure dans chacun des enregistrements de pari que les opérateurs mettent à disposition de l'ARJEL (« empreinte-joueur ») ;
- les informations de description relatives aux compétitions pour lesquelles l'acteur de la compétition a interdiction de parier. Ces informations de description figurent, tout comme l'empreinte, dans tout enregistrement de pari, selon une codification qui respecte la nomenclature des compétitions supports de paris définie par l'ARJEL : la granularité supportée par le dispositif de rapprochement est donc celle de la compétition, et non de la rencontre.

III. Réponse à la fédération délégataire

A l'issue de l'opération de rapprochement, le numéro de demande ainsi que le résultat de la recherche portant sur les enregistrements de pari collectés rattachés à un compte joueur définitif sont communiqués à la fédération délégataire par l'ARJEL dans les cas où des opérations interdites auront été identifiées. Le secret de l'identité du détenteur du compte joueur sera levé dans ces seuls cas.

Si les vérifications mettent en évidence que des opérations de jeu ont été prises sur des compétitions interdites par l'intermédiaire d'un compte joueur provisoire, l'ARJEL informe la fédération délégataire si le compte joueur venait à être confirmé. En effet, un compte provisoire peut être créé sans communication de pièces d'identité et la transmission de ces dernières permet notamment de s'assurer que le compte est effectivement ouvert par le titulaire apparent.

Annexe I – Informations préalables à fournir à l'ARJEL

A. Adresse(s) IP de connexion.

L'accès à l'application de rapprochement de fichiers doit être réalisé depuis une adresse IP fixe.

La fédération délégataire doit donc préalablement communiquer à l'ARJEL la ou les adresses IPv4 fixes depuis lesquelles les connexions seront établies.

B. Information d'identification des agents habilités.

Les informations suivantes sont attendues afin d'identifier les agents habilités par les fédérations délégataires :

- informations personnelles : nom, prénom ;
- coordonnées professionnelles, dont : la fonction, l'adresse postale, le numéro de téléphone (standard et ligne directe), l'adresse de messagerie électronique.

Les moyens de contact professionnels seront utilisés afin de communiquer à l'agent ses identifiants de connexion ainsi que les secrets d'authentification (certificat, mot de passe d'exportation du certificat) au format électronique ou papier (pour le mot de passe) selon les moyens d'échange qui auront été convenus avec la fédération.

Toute modification (ajout ou suppression d'une adresse IPv4 d'accès au service, modification des coordonnées d'un agent habilité par la fédération délégataire) doit – sans délai - être portée à la connaissance de l'ARJEL, via l'adresse de contact communiquée.

Annexe II – Configuration des postes utilisés pour les requêtes

Les navigateurs Internet suivants sont supportés :

- Firefox 25 (et plus) ;
- Google Chrome 31 (et plus).

Plus généralement, les dernières versions de la branche stable des navigateurs Firefox et Google Chrome devraient être supportées.

Annexe III – Installation du certificat de sécurité.

Le dispositif de recueil des demandes requiert une authentification basée sur un certificat de sécurité généré et communiqué par l'ARJEL.

Un certificat de sécurité est une donnée personnelle : il ne doit pas être communiqué à un tiers.

Le certificat de sécurité est transmis sous le format d'un fichier électronique dont l'extension est « .p12 » (format PKCS#12). Il est protégé par un mot de passe, demandé à son importation. Ce mot de passe, dit « mot de passe d'importation » est communiqué par l'ARJEL : il est à usage unique et dédié à l'importation du certificat et du secret (clef privée) qui lui est associé.

La procédure d'installation du certificat d'authentification diffère selon le navigateur utilisé :

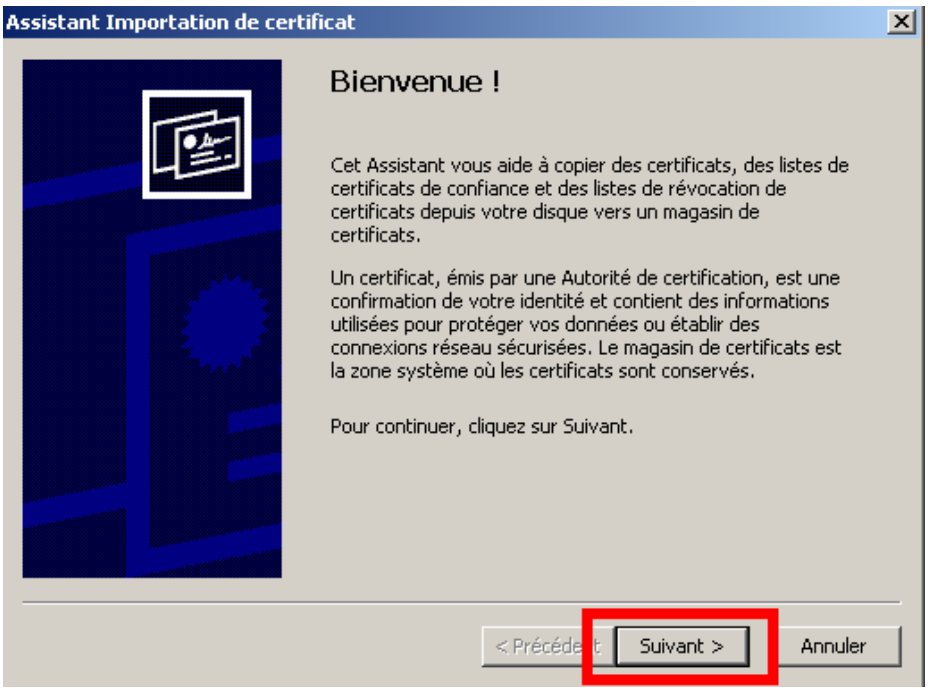
- si le navigateur est Chrome sous Windows, le certificat est conservé dans le catalogue de certificats du système d'exploitation. Son installation suit donc la procédure standard d'installation d'un certificat de sécurité sous Windows (partie A.) ;
- si le navigateur est Firefox, le certificat est conservé dans le catalogue de certificats interne du navigateur, qui diffère donc du catalogue du système d'exploitation. La procédure d'importation est donc spécifique à ce logiciel (partie B.).

A. Installation du certificat pour le navigateur Chrome.

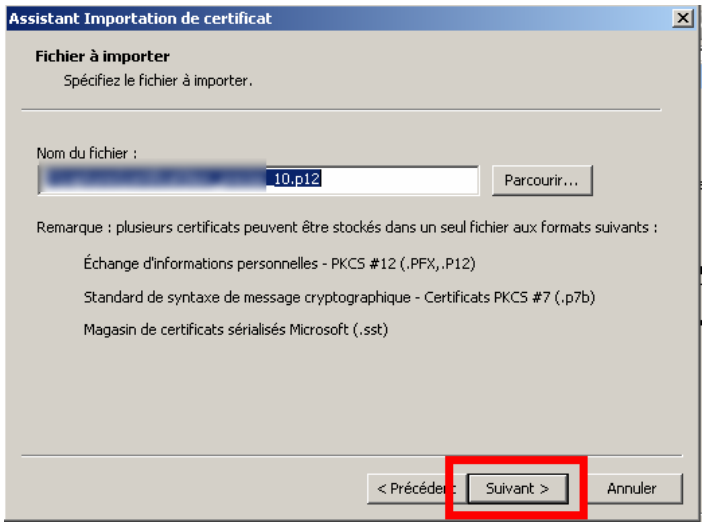
Une action d'importation est automatiquement associée, sous Windows, aux fichiers dont l'extension est « .p12 ».

La procédure d'importation est donc simplement déclenchée en double-cliquant sur le fichier électronique « .p12 » communiqué par l'ARJEL. Suite à cette action, le menu d'importation apparaît donc, et les fenêtres peuvent être successivement déroulées en cliquant sur le bouton « *Suivant* ».

Le détail des fenêtres présentées ainsi que les éventuelles actions spécifiques à entreprendre, sont décrits ci-dessous :

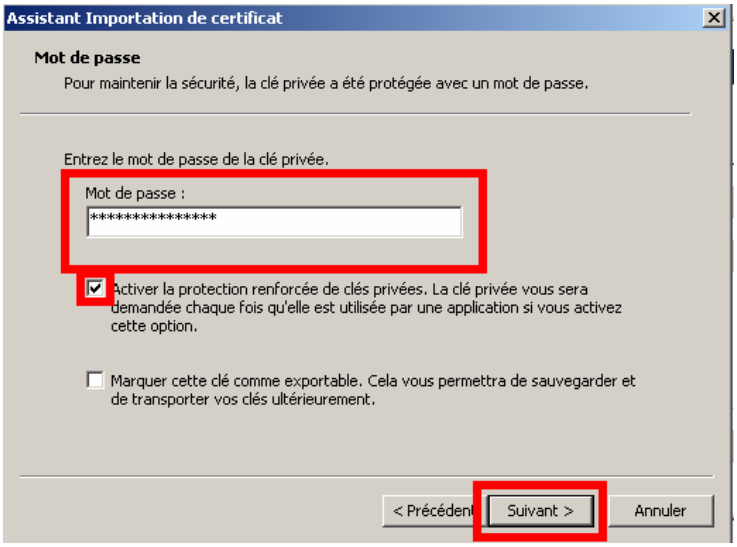


Le fichier à importer est donc le fichier « .p12 » communiqué par l'ARJEL, contenant le certificat de sécurité et la clef privée associée, le bouton « *Suivant* » peut être sélectionné sans autre action :

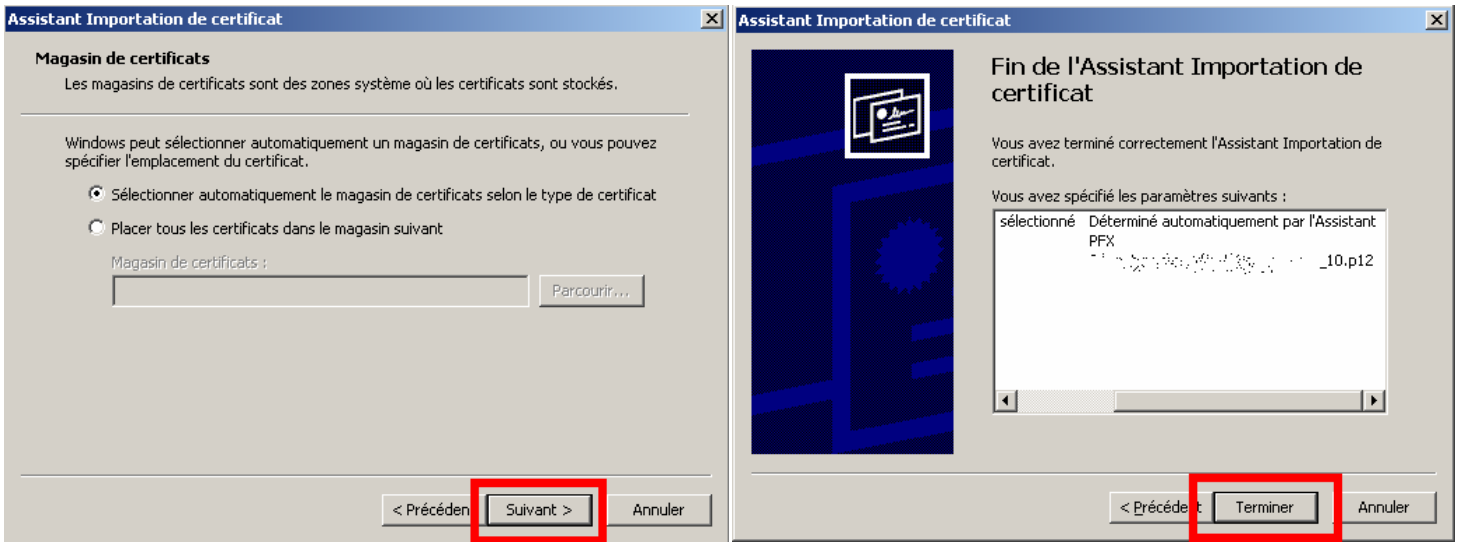


Le mot de passe d'importation du certificat de sécurité et de la clef privée associée doit être saisi (« *Entrez le mot de passe de la clé privée* »). Ce mot de passe est celui communiqué par l'ARJEL.

Par ailleurs, il est recommandé d'activer l'option « *protection renforcée des clés privées* » en la cochant :

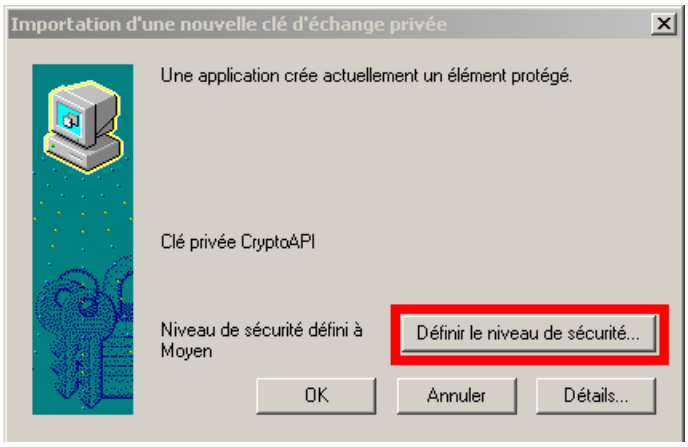


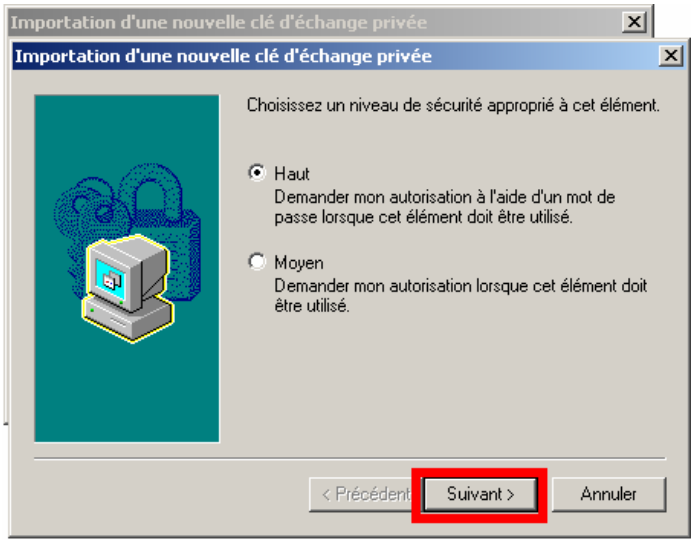
Dans la fenêtre suivante, le magasin de certificats est automatiquement sélectionné, et le bouton « *Suivant* » peut être donc cliqué sans action supplémentaire, idem avec le bouton « *Terminé* » :



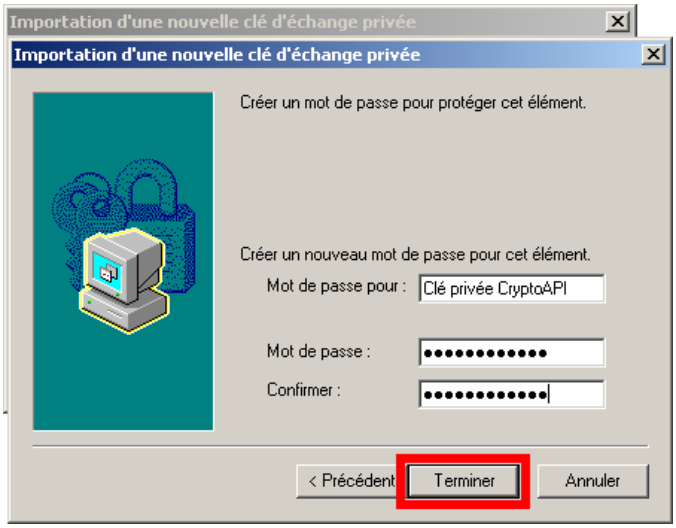
Le niveau de protection associé à la clef peut alors être configuré : le niveau de protection « *moyen* » doit être, *a minima*, sélectionné.

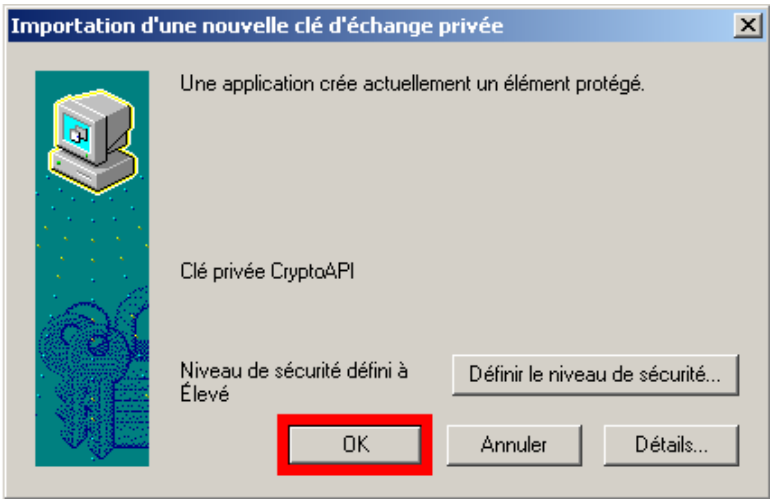
Le niveau de protection « haut » est recommandé : il permet de protéger l'utilisation du certificat d'authentification grâce à un mot de passe qui sera demandé, à chaque session, avant sa première utilisation.



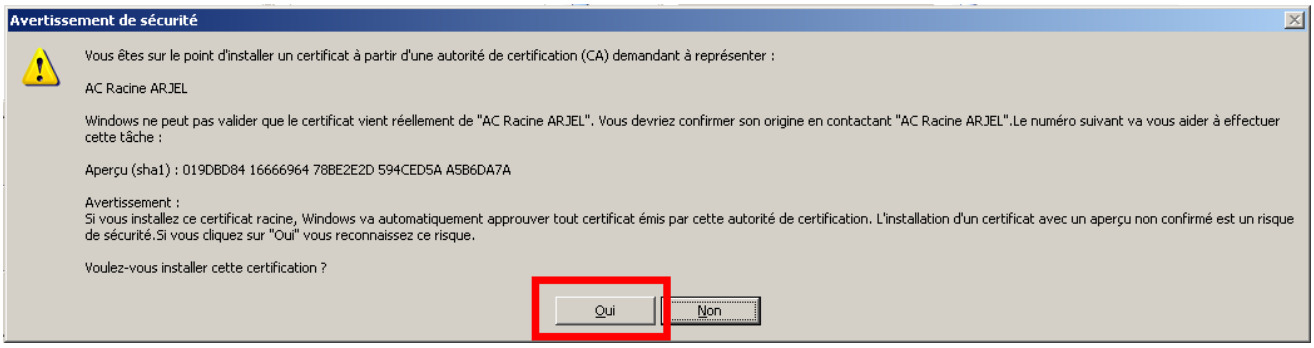


Le choix de ce mot de passe est discrétionnaire : il s'agit donc d'un mot de passe qui peut être différent du mot de passe d'importation. Il est recommandé à l'utilisateur de choisir un mot de passe fort, autrement dit que ses critères de complexité respectent les règles de bonnes pratiques (chiffres, lettres minuscules et majuscules, caractères spéciaux, longueur minimale de 10 caractères et utilisation dédiée à cet usage).

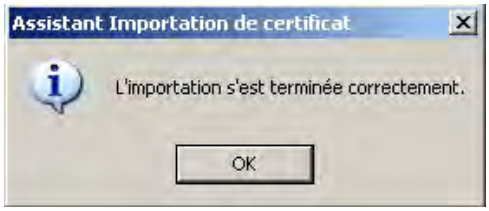




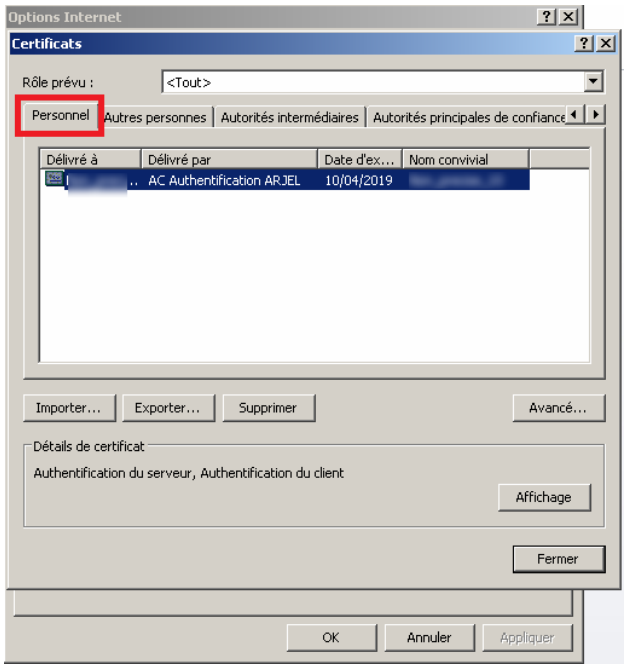
L'importation de la clef s'achève avec l'importation du certificat racine de l'ARJEL. Ce certificat racine sera également utilisé pour authentifier l'interface du croisement de fichier.

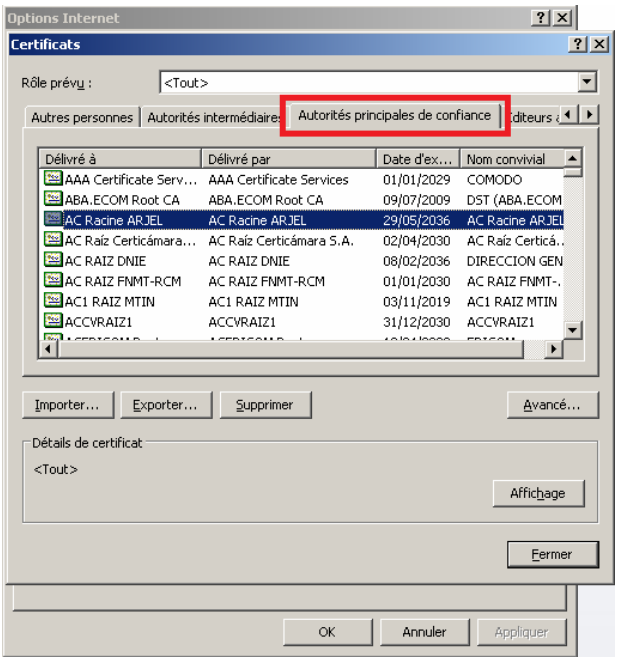


Si l'opération d'importation est concluante, la fenêtre suivante apparaît :

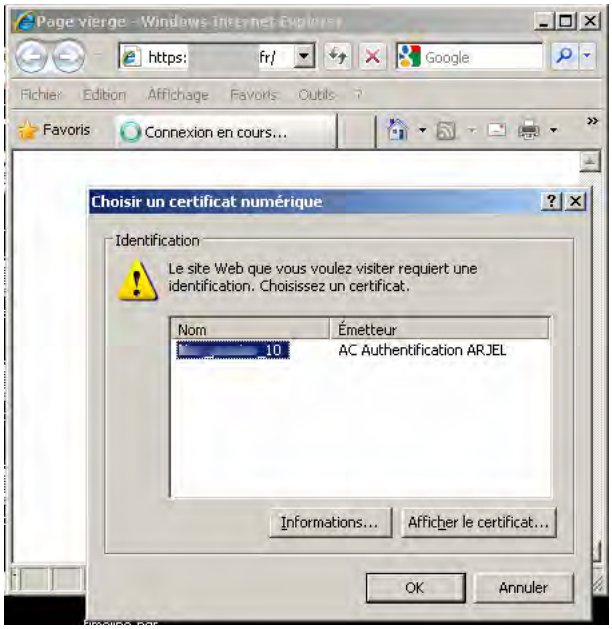


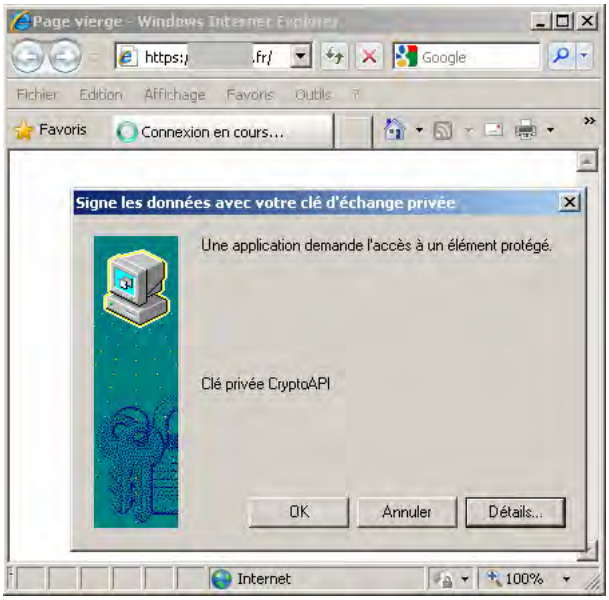
Le certificat d'authentification, ainsi que le certificat racine ARJEL, apparaissent alors dans le catalogue de certificats du système d'exploitation, consultable via le menu « *Options Internet* > *onglet 'Contenu'* > *Certificats* ». Le certificat est alors prêt à être utilisé :





A la connexion au site dédié, une fenêtre (« *Choisir un certificat numérique* ») indique que le certificat de sécurité est prêt à être utilisé pour l'authentification. Selon le niveau de protection (« moyen » ou « haut ») sélectionné, une confirmation ou encore la saisie du mot de passe protégeant le secret peut être demandée :

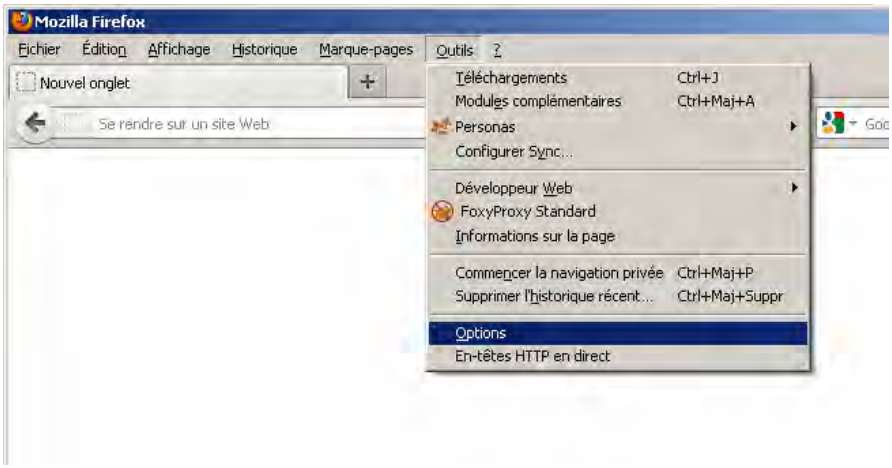




B. Installation du certificat pour le navigateur Firefox.

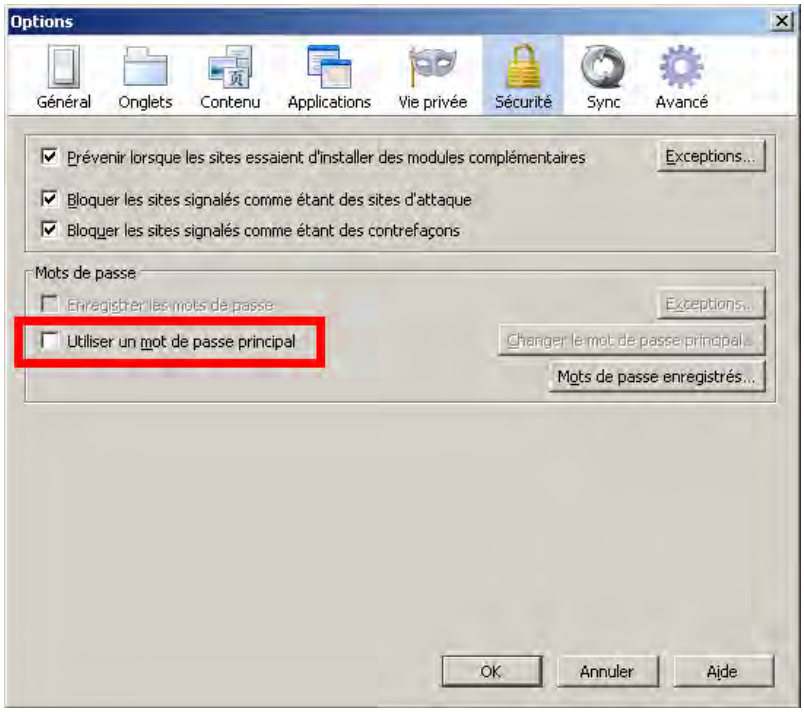
La procédure d'importation repose sur le module d'importation du navigateur Firefox.

Ce module d'importation est accessible via le menu « *Outils* » du navigateur, puis le sous-menu « *Options* » :



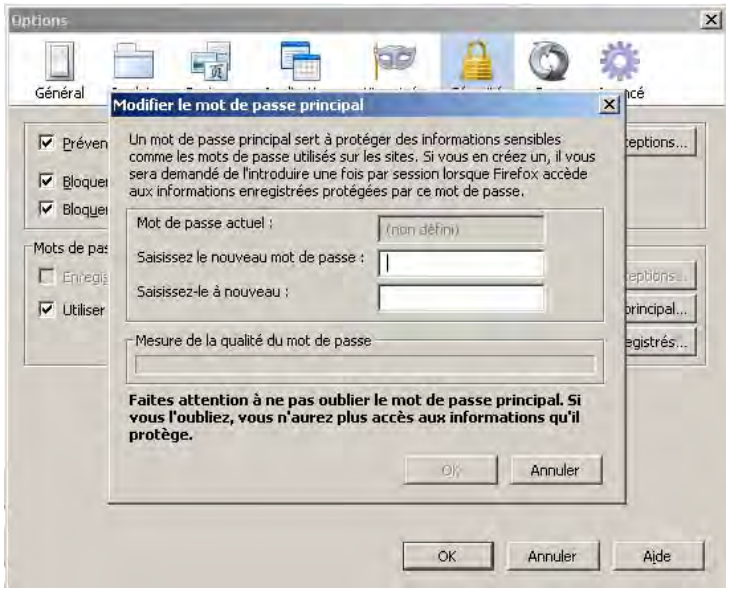
Une étape préliminaire consiste*, si cela n'a pas déjà été effectué par l'utilisateur*, à configurer un mot de passe qui permettra de protéger les secrets enregistrés par le navigateur. Le certificat d'authentification et la clef privée associée font partie de ces secrets : cette étape préliminaire est donc vivement recommandée.

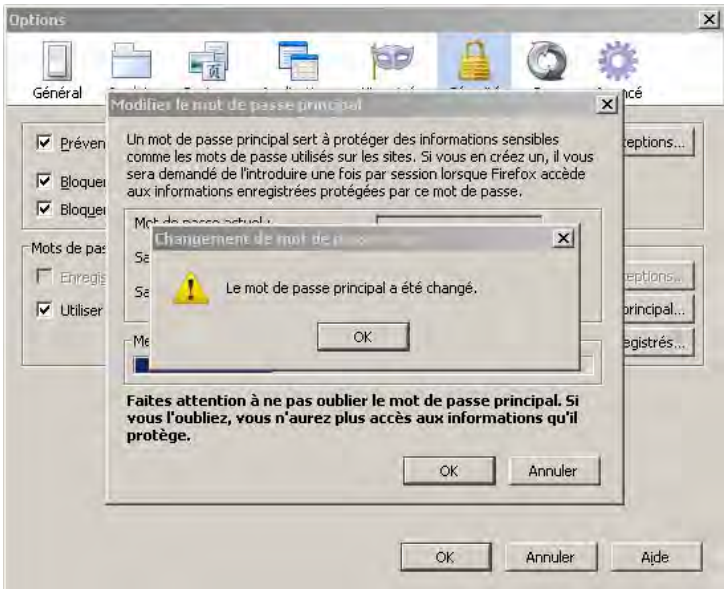
Cette étape consiste à se rendre dans l'onglet « *Sécurité* » du menu précédemment sélectionné, puis à sélectionner l'option « *Utiliser un mot de passe principal* » :

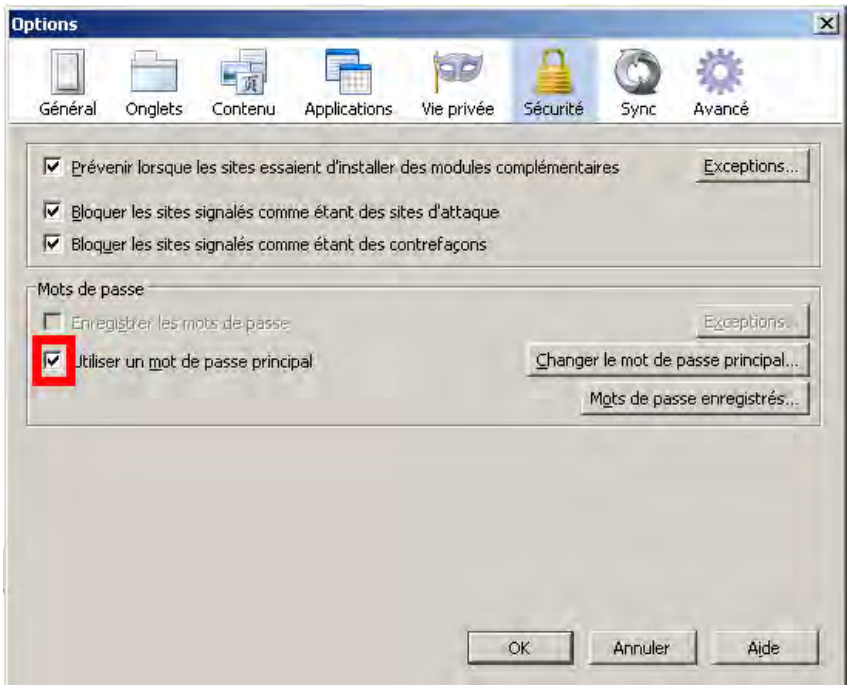


Le mot de passe principal permet de protéger l'utilisation du certificat d'authentification : il sera demandé à chaque nouvelle session du navigateur, à la première utilisation du certificat.

Le choix de ce mot de passe est discrétionnaire : il s'agit donc d'un mot de passe qui peut être différent du mot de passe d'importation fourni par l'ARJEL afin de protéger le certificat. Il est recommandé à l'utilisateur de choisir un mot de passe fort, autrement dit que ses critères de complexité respectent les règles de bonnes pratique (chiffres, lettres minuscules et majuscules, caractères spéciaux, longueur minimale de 10 caractères et utilisation dédiée à cet usage) :



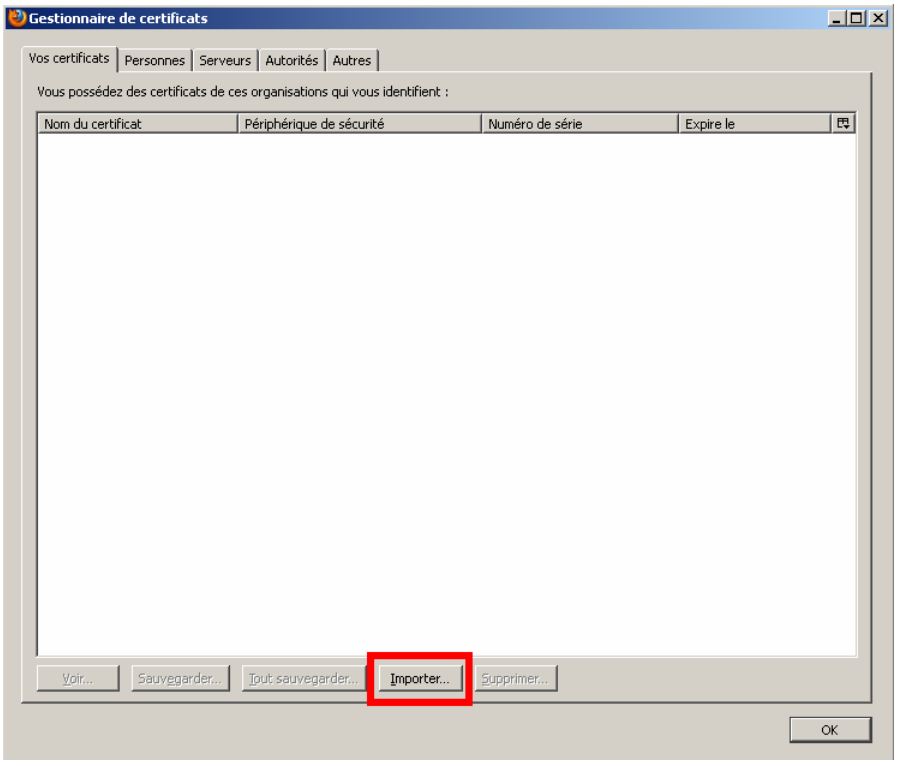




Suite à cette opération, l'option « *Utiliser un mot de passe principal* » est sélectionnée.

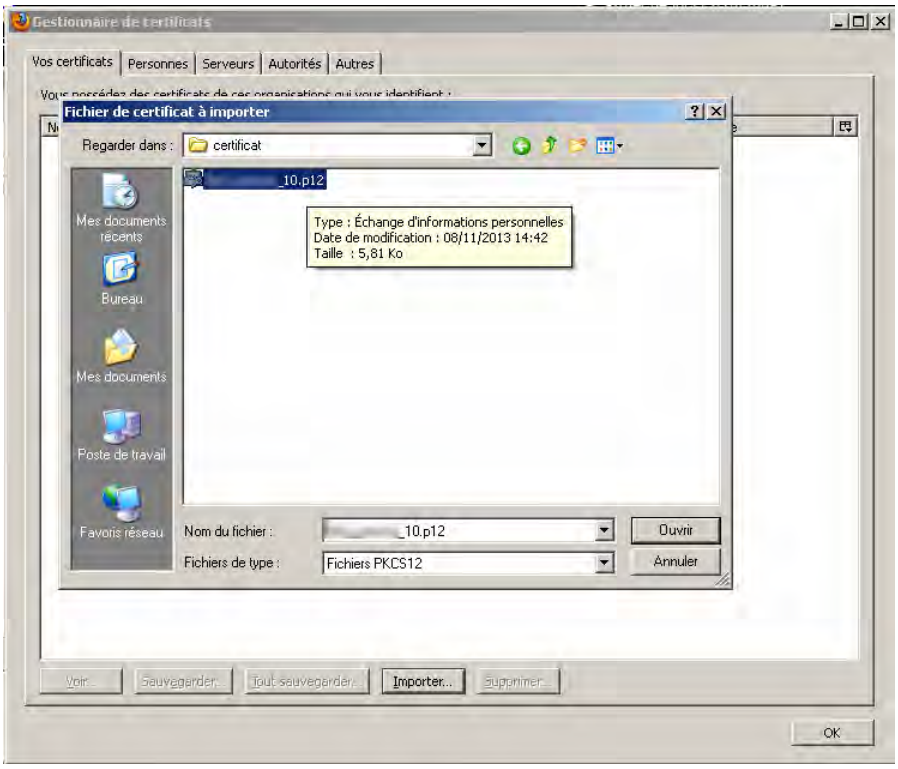
Une fois le mot de passe principal configuré, le certificat d'authentification communiqué par l'ARJEL peut être importé dans le navigateur, via le menu « *Outils* » du navigateur, sous-menu « *Options* » et l'onglet « *Avancé* » :

Le bouton « *Afficher les certificats* » doit être sélectionné :

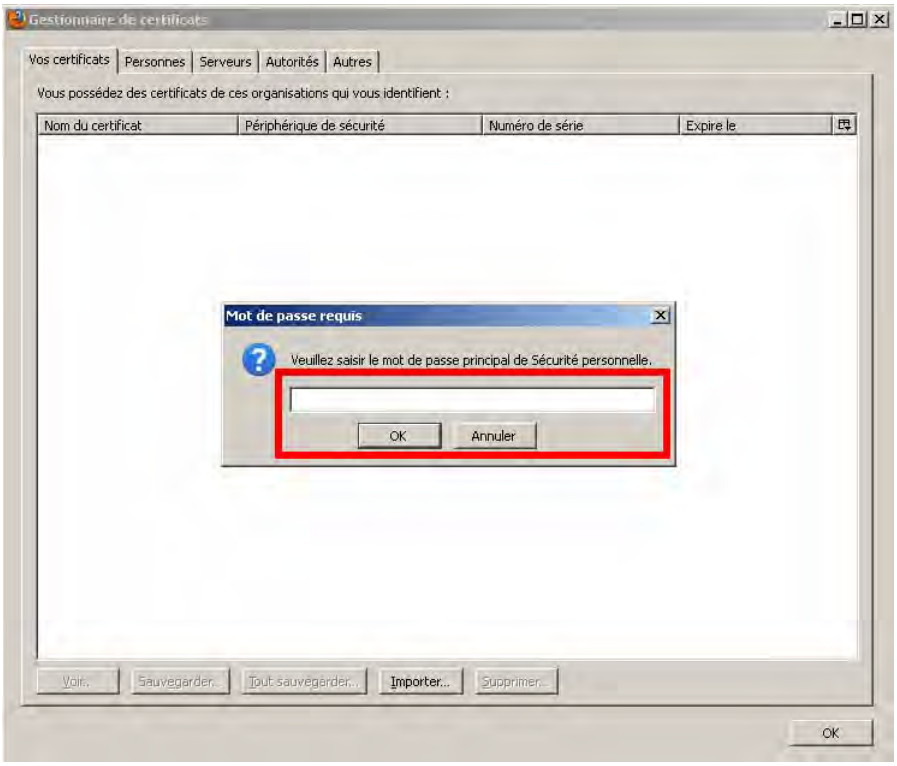


Le bouton « *Importer* » doit être sélectionné : il permet de choisir le fichier à partir duquel importer le certificat d'authentification. Ce fichier est le fichier d'extension « .p12 » communiqué par l'ARJEL.

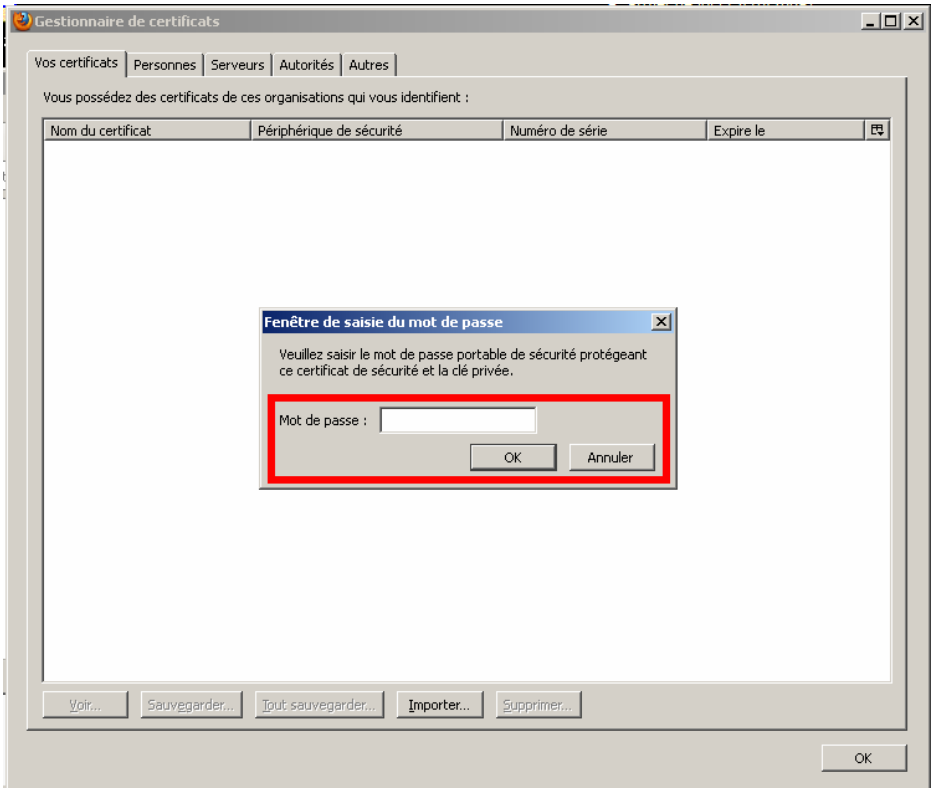
Le fichier d'extension « .p12 » doit donc être sélectionné et ouvert (bouton « Ouvrir ») via cette interface :



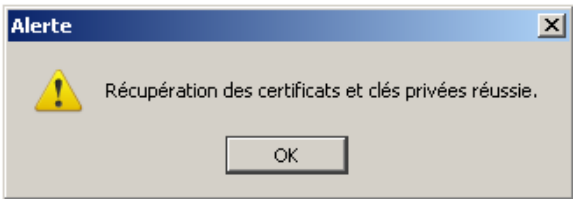
Tout d'abord, le mot de passe principal doit être saisi. Remarque : il ne s'agit pas du mot de passe d'importation communiqué par l'ARJEL, mais du mot de passe choisi précédemment et configuré afin de protéger les secrets conservés par le navigateur Firefox :

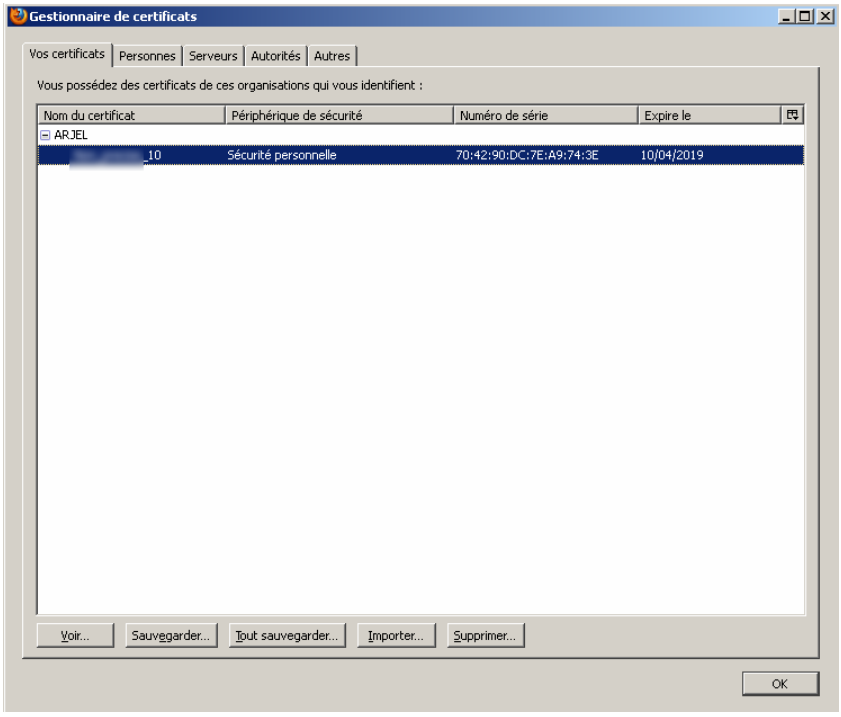


Une fois le mot de passe principal saisi, le mot de passe d'importation du certificat et de la clef privée associée peut être entré. Ce mot de passe est celui communiqué par l'ARJEL.



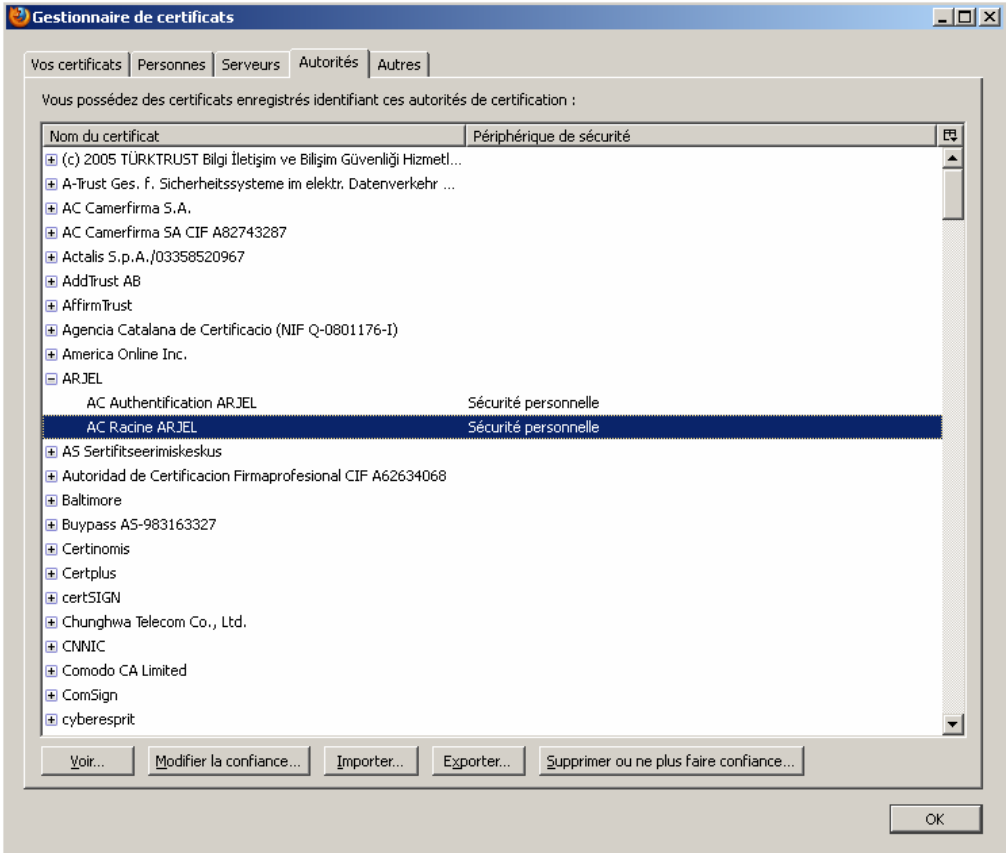
A l'issue de ces deux saisies de mot de passe (mot de passe principal, puis mot de passe d'importation), le certificat de sécurité et la clef privée sont correctement importés dans le navigateur :



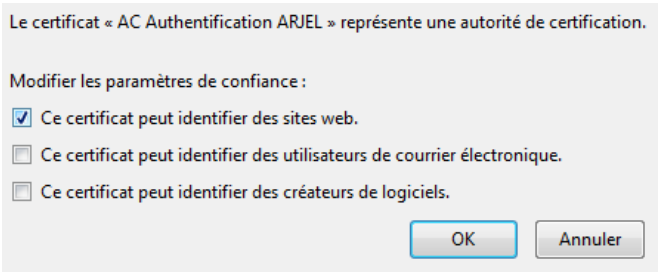


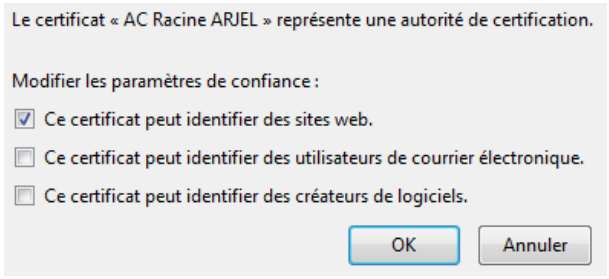
Le certificat apparaît alors dans le catalogue de certificats du navigateur.

La dernière étape consiste, via l'onglet « *Autorités* » de l'interface de gestion des certificats, à sélectionner les certificats ARJEL « *AC Racine ARJEL* » et « *AC Authentification ARJEL* » et à modifier, pour chacun, l'option « *Modifier la confiance* » :



Les paramètres de confiance des certificats doivent être modifiés de façon à permettre l'authentification des sites web (option « *Ce certificat peut identifier des sites web* »), i.e. de la façon suivante :





Annexe IV : Mode d'emploi détaillé du dispositif de recueil des demandes

Introduction

Ce document est destiné à être le manuel utilisateur de référence pour toute personne habilitée à utiliser le service Fidji de l'ARJEL.

Les termes en *italique* sont expliqués dans le lexique à la fin de ce manuel.

Les termes en chasse fixe sont des mots clés, paramètres ou retours de fonction informatique.

L'ensemble des captures d'écran de l'application dans ce document ont été réalisées avec la version 25.0.1 de *Firefox*, certains aspects visuels et procédures peuvent légèrement varier d'un navigateur à un autre. En cas de doute, référez-vous au paragraphe "Compatibilité" de ce document pour savoir si votre navigateur est supporté ou contactez l'ARJEL par messagerie à l'adresse communiquée.

Fidji constitue le **dispositif externe de recueil des données** permettant aux fédérations délégataires de pouvoir contrôler le respect de l'interdiction de parier faite aux acteurs de compétitions. Ce service est accessible par Internet à travers une application et un service web dont l'accès n'est possible qu'à l'aide d'un *certificat SSL* personnel remis par l'ARJEL après l'habilitation d'une personne. (Conformément au décret n° 2013-947 du 22 octobre 2013).

L'application web est une solution clé en main vous permettant d'utiliser dès maintenant ce service. Cependant, si vous disposez des ressources techniques nécessaires, le **service web** vous permettra d'automatiser l'échange de données entre votre système d'information et celui de l'ARJEL.

Demande de rapprochement et procédure associée

Une « demande de rapprochement » est constituée de trois informations indispensables :

- un périmètre sportif ;
- une période de temps ;
- l'identité du ou des acteurs de la/des compétition(s).

Lorsque l'ARJEL enregistre votre demande, l'identité de la personne est anonymisée à l'aide d'une fonction cryptographique complexe permettant de la masquer tout au long du traitement. Pour cette raison, chaque demande dispose de son propre identifiant nommé "**ticket**". C'est ce numéro de ticket qui vous permettra de suivre la progression d'une demande.

Une demande prend successivement les statuts suivants :

- `En attente` : la demande de rapprochement a bien été prise en compte et est enregistrée sur l'interface de dépôt de Fidji. Celle-ci est en attente de sa transmission au service de rapprochement de l'ARJEL.
- `En cours` : la demande de rapprochement est en cours de traitement.
- `Traitée` : La demande a été traitée, la réponse définitive est en cours d'acheminement auprès de vos services.

La réponse définitive contenant la synthèse d'activité d'un acteur de compétition sportive n'est pas transmise par le dispositif de recueil des demandes de l'ARJEL. Celle-ci est envoyée par un courrier reprenant le numéro de ticket de la demande comme référence.

Application Web

Cette première partie concerne l'application web. Vous y trouverez les informations pour y accéder et effectuer les opérations de demande et de suivi.

Accès à l'application

Une fois votre certificat SSL installé dans votre navigateur internet, il vous suffit de vous connecter à l'adresse du site dédié. Il est important de noter la présence du "s" à la suite du "*http*" ainsi que l'absence des "www". Il' s'agit d'un service sécurisé où l'ensemble des communications entre votre navigateur web et les serveurs de l'ARJEL est chiffré.

Lors de la connexion, une fenêtre *pop-up* vous invitant à sélectionner le certificat pour vous connecter au service apparait. (fig. 1)

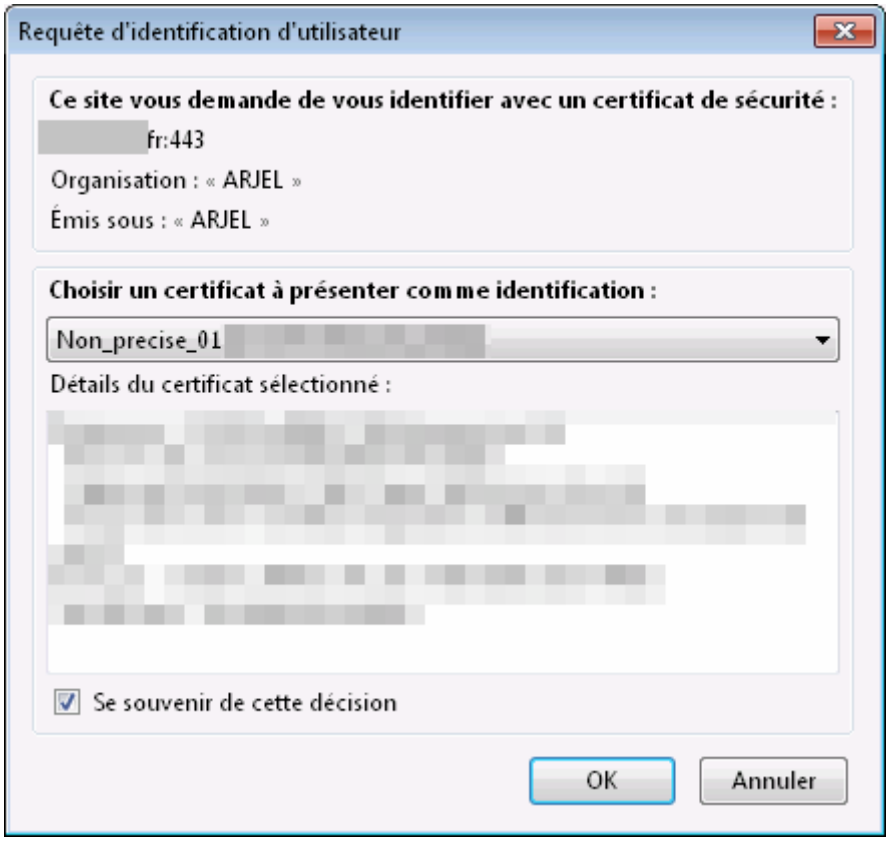


fig. 1 : Sélection du certificat SSL client

S'il s'agit de la première connexion et que vous utilisez Firefox, ce dernier vous informe que "Cette connexion n'est pas certifiée" (fig. 2). Cela vient du fait que l'ARJEL n'est pas enregistrée par défaut comme un site de confiance dans votre navigateur. Pour enregistrer l'ARJEL dans les sites de confiance, cliquez sur "Je comprends les risques" puis le bouton "Ajouter une exception". (fig. 3)

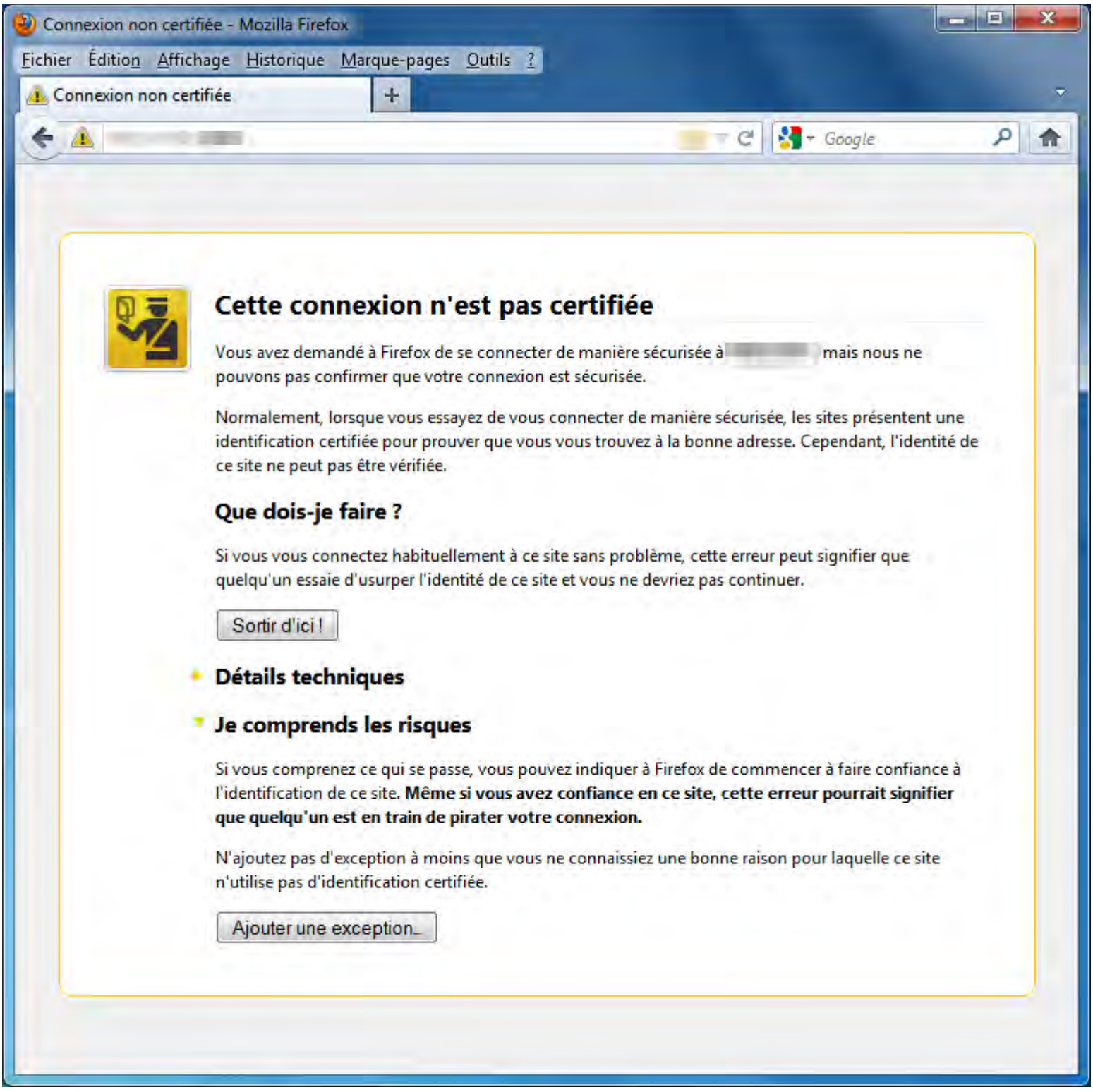


fig. 2 & fig. 3 : Enregistrement du site dédié comme site de confiance.

Une nouvelle fenêtre pop-up apparait (fig. 4), dans celle-ci cochez la case "Conserver cette exception de manière permanente" puis le bouton "Confirmer l'exception de sécurité". Dorénavant, chaque connexion à l'adresse en https du site dédié vous conduit directement à la page d'accueil du service (fig. 5).

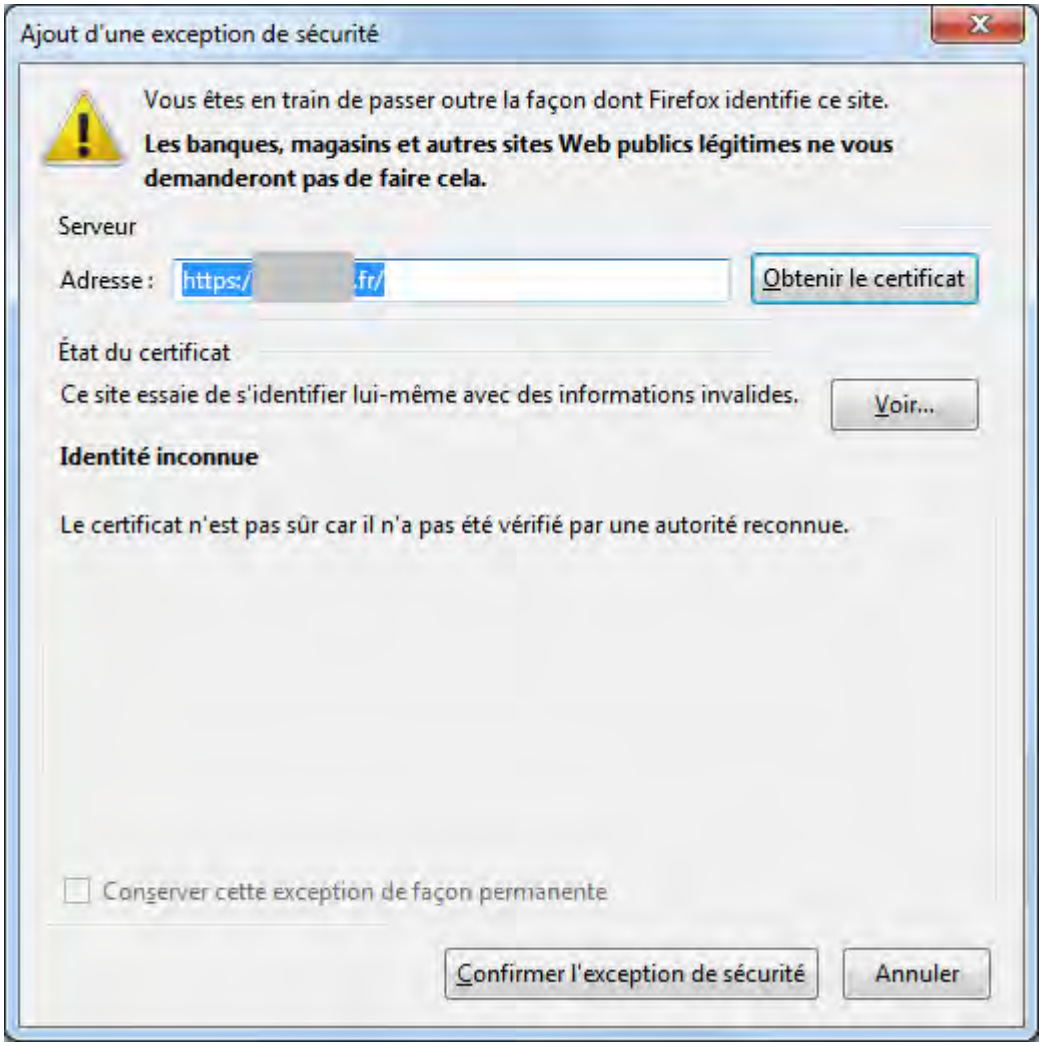


fig. 4 : Enregistrement du site dédié comme site de confiance (suite et fin)

Organisation de l'application

Une fois la connexion établie avec le site internet, l'application se sépare en deux parties[1] distinctes et détaillées ci-dessous :

Accueil

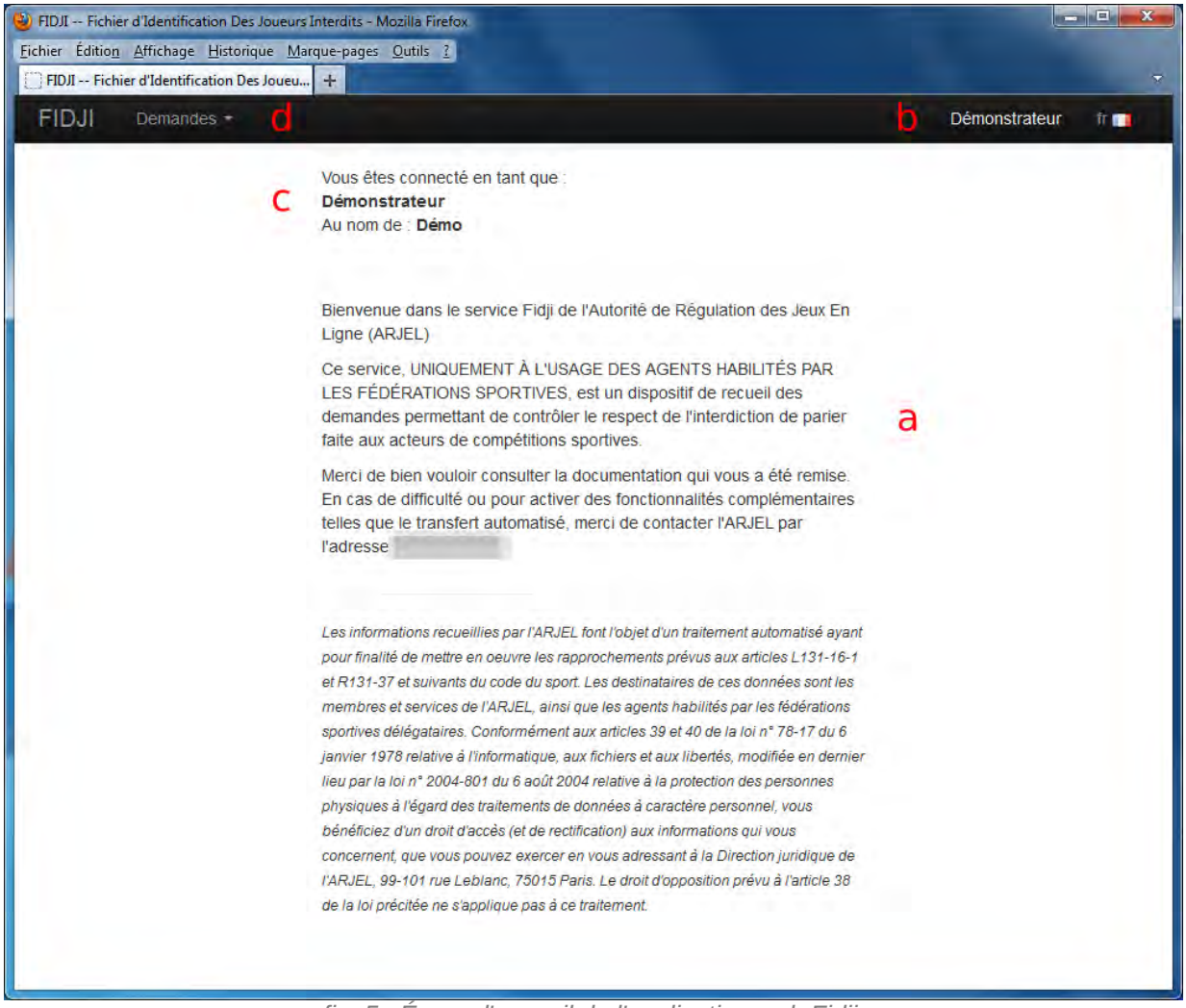


fig. 5 : Écran d'accueil de l'application web Fidji.

L'accueil est votre premier contact avec Fidji. Vous y trouverez des informations rappelant le rôle de ce service (a), votre identité (b) ainsi que l'organisme délégataire au nom du quel vous opérez (c). Enfin, vous pouvez accéder aux autres fonctionnalités de l'application grâce au menu (d).

Cette page peut être utilisée pour vous transmettre des informations sur l'évolution du service, aussi restez attentif à son évolution.

[1] Cela peut être amené à évoluer dans les prochaines versions afin d'offrir de nouvelles fonctionnalités.

Suivi des demandes

Cet écran est le cœur de Fidji. Pour y accéder, cliquez sur le menu "Demandes" puis "Suivi et nouvelles demandes". À partir de cette page il vous est possible de suivre et effectuer de nouvelles demandes de rapprochement. (fig. 6)

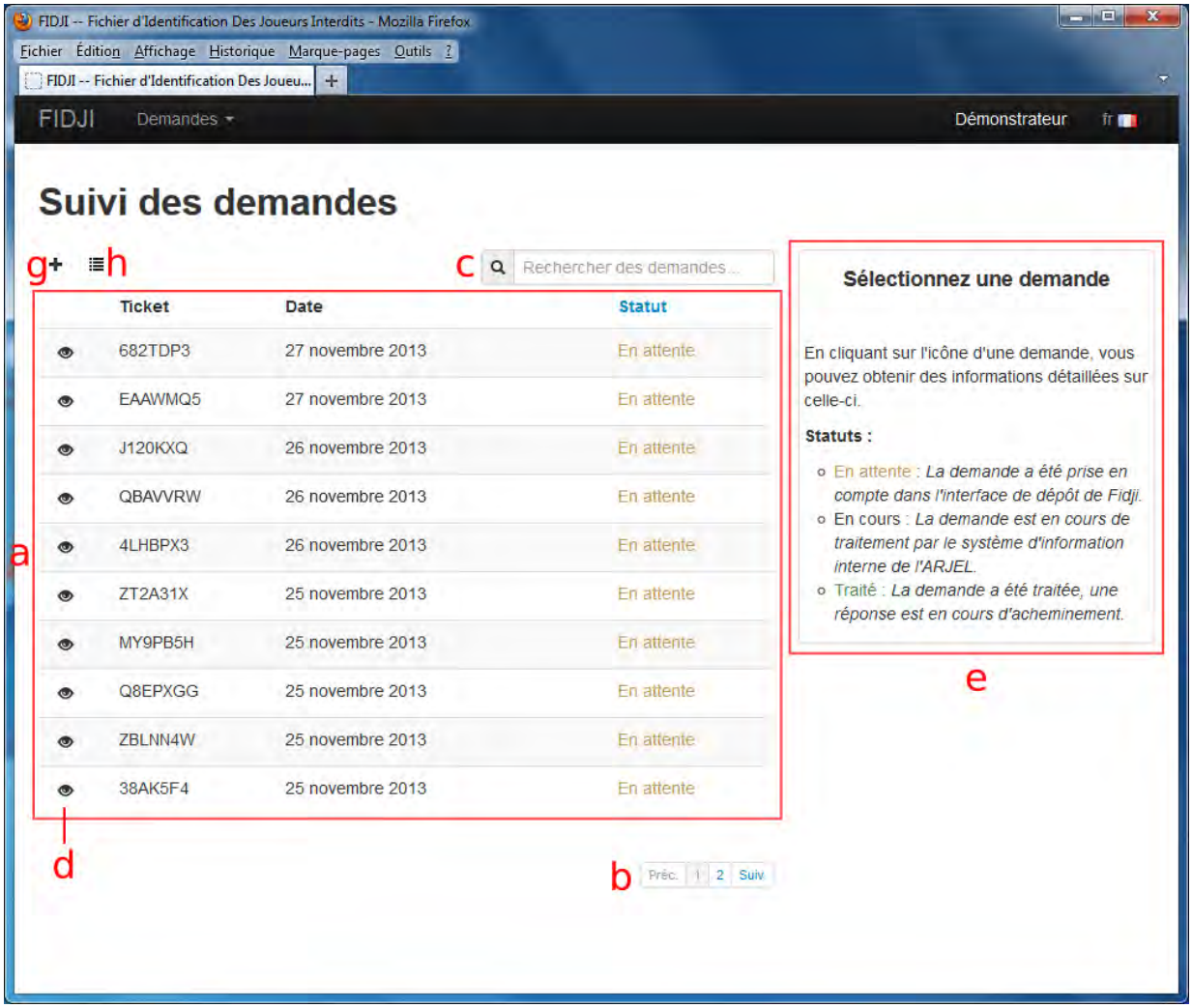


fig. 6a : Écran de suivi des demandes

Les demandes sont réunies dans un tableau contenant pour chacune son numéro de ticket, sa date et son statut (a). Le tableau est paginé à raison de 10 demandes par page, accessibles grâce aux boutons de navigation en bas à droite de celui-ci (b). Un champ de saisie est disponible pour filtrer les demandes (c). Pour afficher les détails d'une demande (périmètre et période, la demande étant anonymisée l'identité ne peut pas être affichée) il suffit de cliquer sur l'icône (d) pour les afficher dans la colonne à droite de l'écran (e). (fig. 6b)

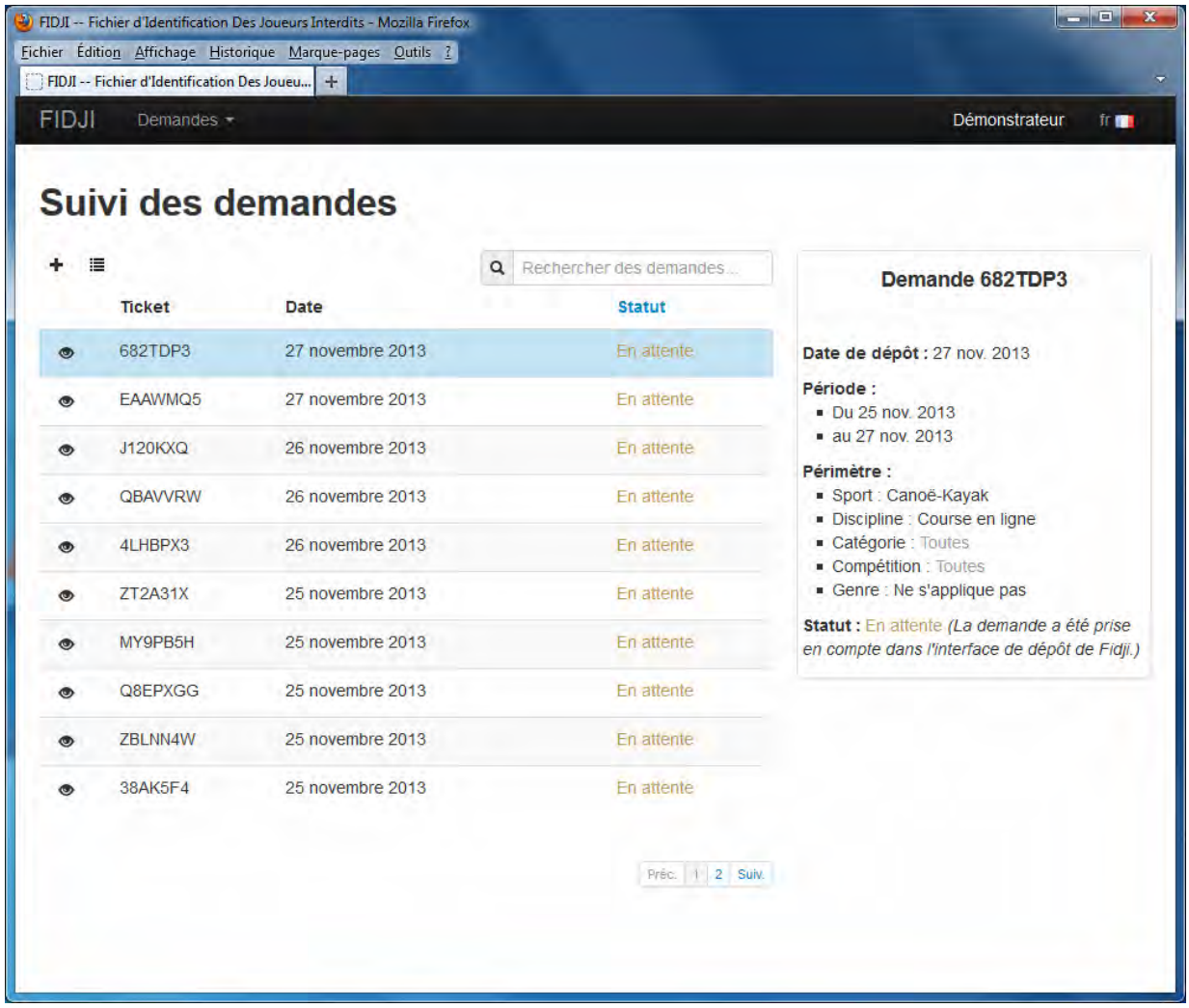


fig. 6b : Écran de suivi des demandes (demande sélectionnée)

Par défaut, seules les demandes en attente ou en cours de traitement sont affichées. Pour modifier ce paramétrage par défaut, il vous suffit de cliquer sur le titre de la colonne "Statut" (f) pour faire apparaitre un menu vous permettant de (dé)filtrer certaines demandes. (fig. 7)

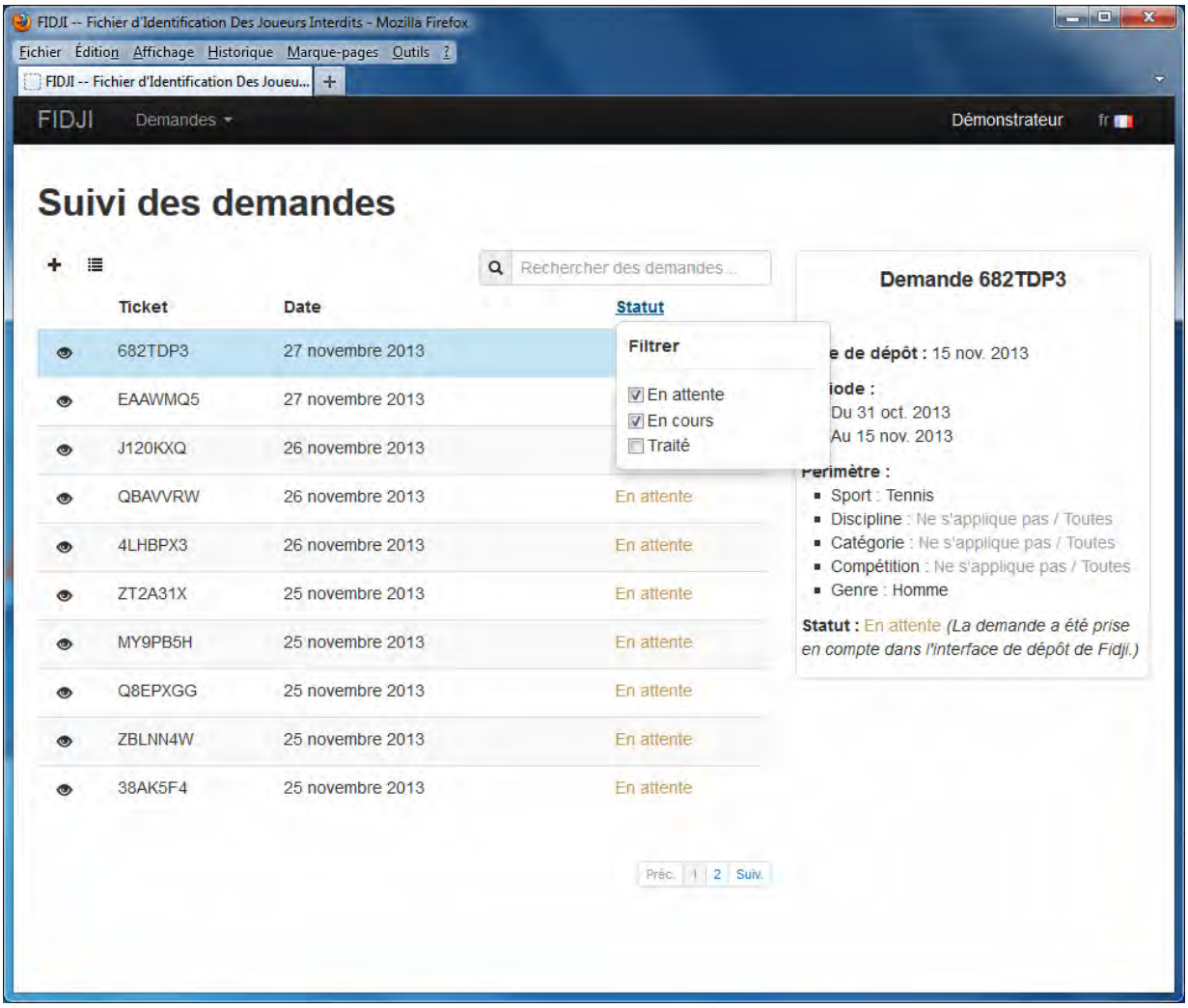


fig. 7 : Filtrage des demandes affichées sur le statut.

Pour effectuer une nouvelle demande, il suffit de cliquer sur l'icône (g). Il est aussi possible d'effectuer une demande groupée en cliquant sur l'icône (h).

Effectuer une demande simple

Une demande simple est une demande de rapprochement qui ne porte que sur une seule personne. Pour l'effectuer, deux moyens s'offrent à vous :

Par le menu principal, en faisant "Demandes" puis "Nouvelle demande simple".

Depuis le suivi des demandes (fig. 6) en cliquant sur l'icône.

L'opération se déroule en 4 étapes :

Définition du périmètre sportif de la demande

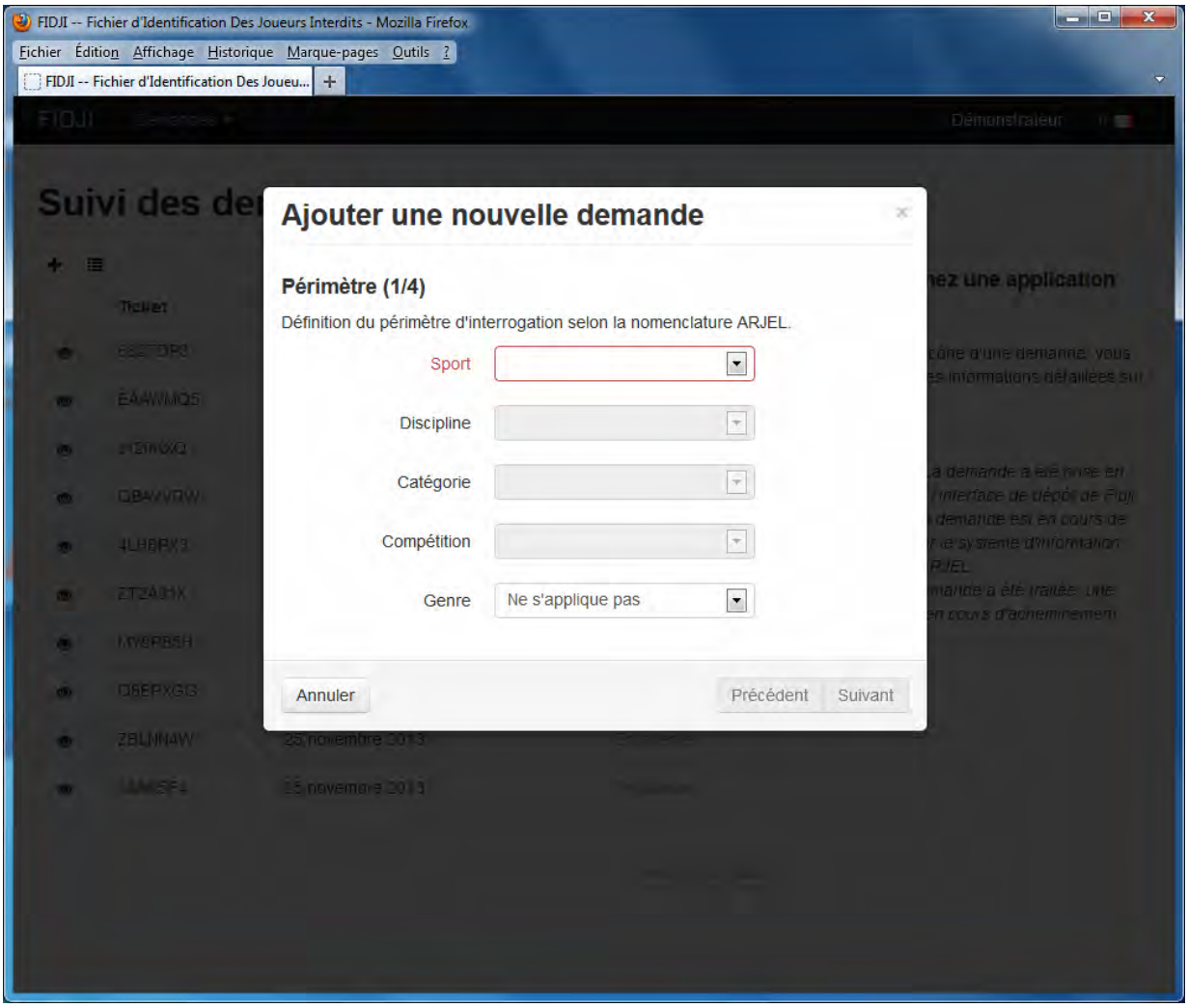


fig. 8 : Sélection du périmètre sportif.

Le périmètre se définit en suivant la nomenclature hiérarchisée de l'ARJEL. Lorsque vous sélectionnez la valeur d'un champ, les choix du suivant sont automatiquement mis à jour. S'il n'y a qu'un choix, ce choix est automatiquement sélectionné. L'absence de valeur dans un champ indique que le périmètre concerne l'ensemble des compétitions sportives respectant le périmètre "partiel".

Par exemple :

Sport : Football, Discipline : Ne s'applique pas, Catégorie : Ligue 1, Compétition : Championnat national (France)

Va précisément définir une compétition de football.

Sport : Athlétisme, Discipline : Saut, Catégorie : Toutes, Compétition : Toutes

Va englober à la fois le saut à la perche, en longueur, en hauteur et le triple-saut sur l'ensemble des compétitions ouvertes aux paris.

Tous les champs, à l'exception du genre et du sport, sont optionnels.

Les compétitions qui peuvent être sélectionnées sont uniquement les compétitions organisées en France où celles dont certaines rencontres se déroulent en France.

Définition de la période

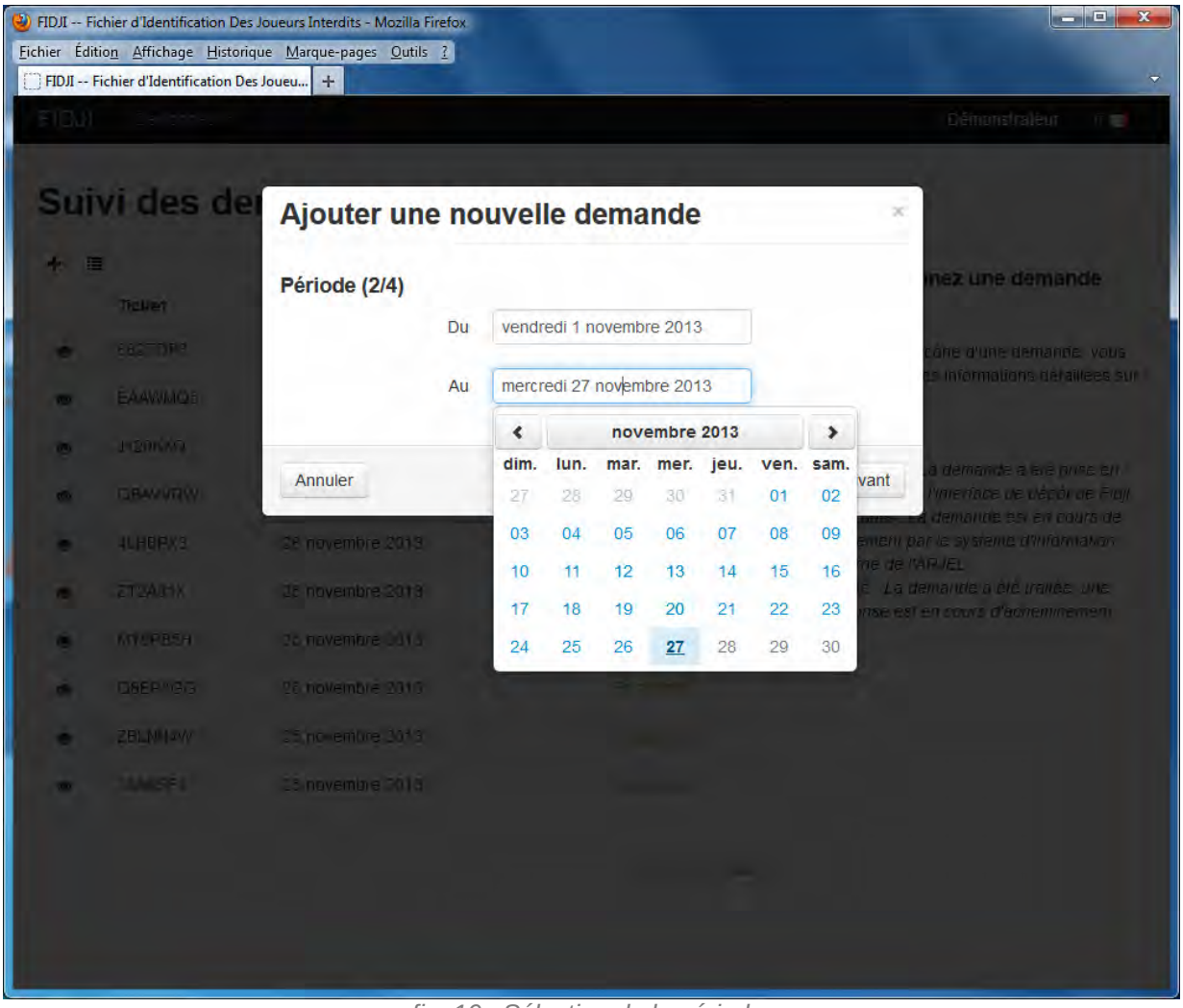


fig. 10 : Sélection de la période.

La période d'interrogation correspond à la période de vérification de la présence d'éventuelles prises de paris ; il ne s'agit donc aucunement de la période liée à la compétition choisie. Cette période d'interrogation est délimitée par deux dates. La date de fin ne peut être postérieure à la date du jour de la demande.

Le menu de sélection de date permet une navigation facilitée en permettant une sélection rapide du mois et de l'année en plus des fonctionnalités habituelles de ce type de composant. (fig. 10)

L'identité

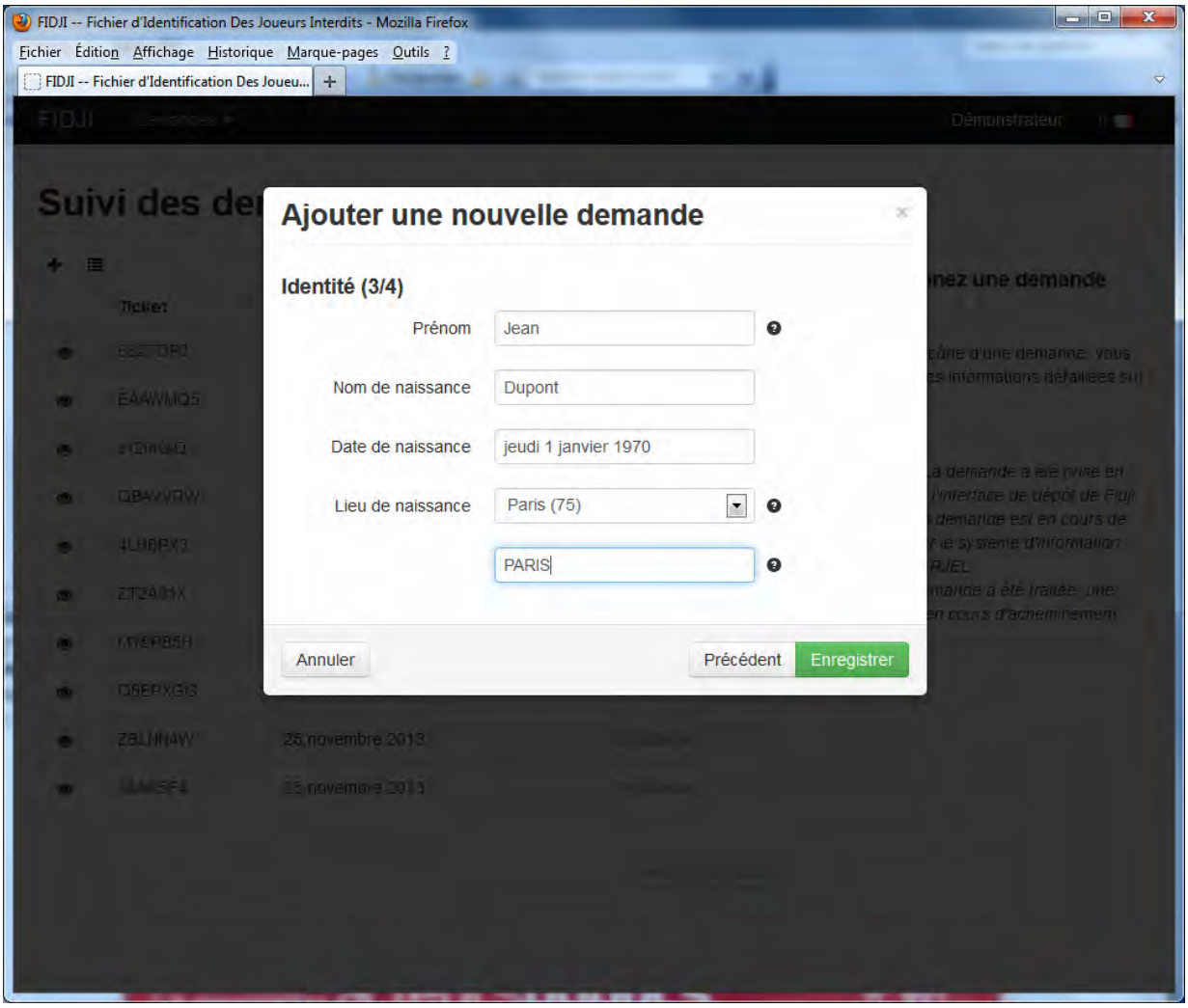


fig. 11 : Sélection de l'identité

L'identité est une étape critique. L'anonymisation ne permet pas de détecter la moindre erreur de saisie, aussi une simple faute de frappe ne permettra pas d'effectuer le rapprochement tout en ne provoquant aucune erreur.

Les informations suivantes sont demandées : le prénom, le nom, la date de naissance ainsi que le lieu de naissance.

Le prénom : Il s'agit du premier prénom de la personne. Si le prénom est composé, chaque partie du prénom doit être séparé par un tiret simple (ex: "jean-michel"). Les lettres de l'alphabet, le tiret et l'apostrophe sont les seuls caractères acceptés. Les accents et la casse sont ignorés (ex: "Élodie" et "elodie" sont équivalents).

Le nom : Il s'agit du nom patronymique (nom apparaissant sur la carte d'identité). Les noms d'usages sont à proscrire. À la différence du prénom, l'espace est pris en compte. Un nom composé doit être retranscrit dans son intégralité.

La date de naissance : Elle ne peut être postérieure à la date du jour moins dix-huit ans, les mineurs n'étant pas autorisés à parier en ligne : ils ne sont pas concernés par le rapprochement de fichiers.

Le lieu de naissance : Il s'agit de la commune de naissance (commune au format INSEE) pour les personnes nées en France et de nationalité française ou le pays de naissance (pays au format INSEE) pour les autres.

Résumé

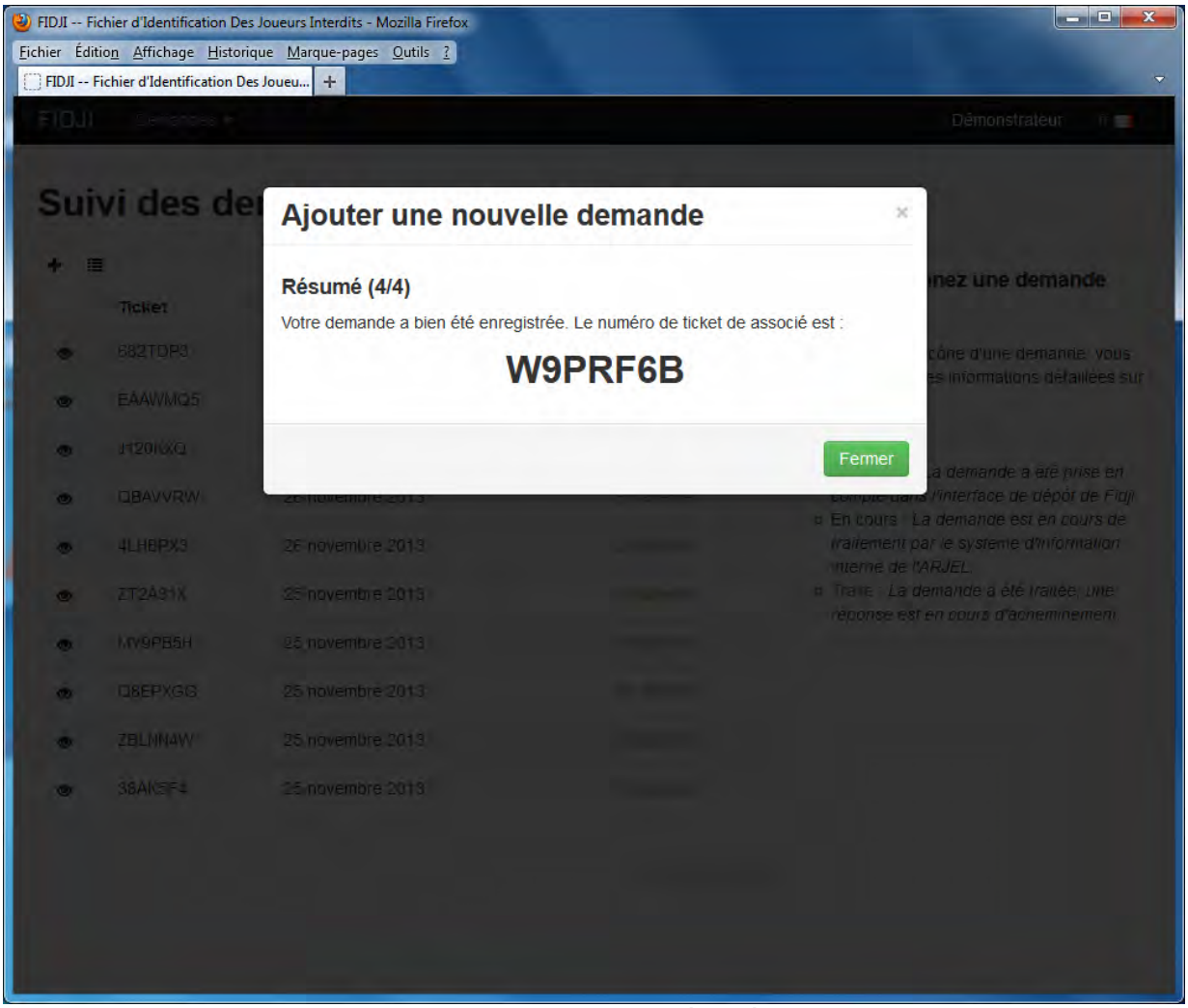


fig. 11 : Affichage du résumé

Si l'enregistrement de la demande s'est bien passé, alors son numéro de ticket est affiché dans le résumé de la demande. Après fermeture du formulaire de demande, vous retrouverez celle-ci dans la liste des demandes en attente dans le suivi des demandes.

Effectuer une demande groupée

Une demande groupée est une demande de rapprochement portant sur plusieurs personnes pour un même périmètre et une même période. Elle repose sur l'utilisation d'un fichier « CSV » dont le format est le suivant :

caractère séparateur : **;** (point-virgule)

pas de ligne d'en-tête

première colonne : premier prénom

deuxième colonne : nom patronymique

troisième colonne : date de naissance au format ISO-8601 (année, mois, jour séparés par des tirets, ex : 1981-11-23 pour le 23 novembre 1981.)

quatrième colonne : lieu de naissance

Les mêmes restrictions de format que l'étape 3 de la demande simple s'appliquent aux différents champs du fichier CSV. Ci-dessous, un exemple de fichier valide.

```
John;Doe;1985-01-01;PARIS
Jane;Doe;1990-02-12;PARIS
```

Pour effectuer une demande groupée, deux moyens s'offrent à vous :

Par le menu principal, en faisant "Demandes" puis "Nouvelle demande groupée".

Depuis le suivi des demandes (fig. 6) en cliquant sur l'icône .

L'opération se déroule en 4 étapes. Les deux premières étapes sont identiques à la demande simple :

Envoi du fichier CSV des identités

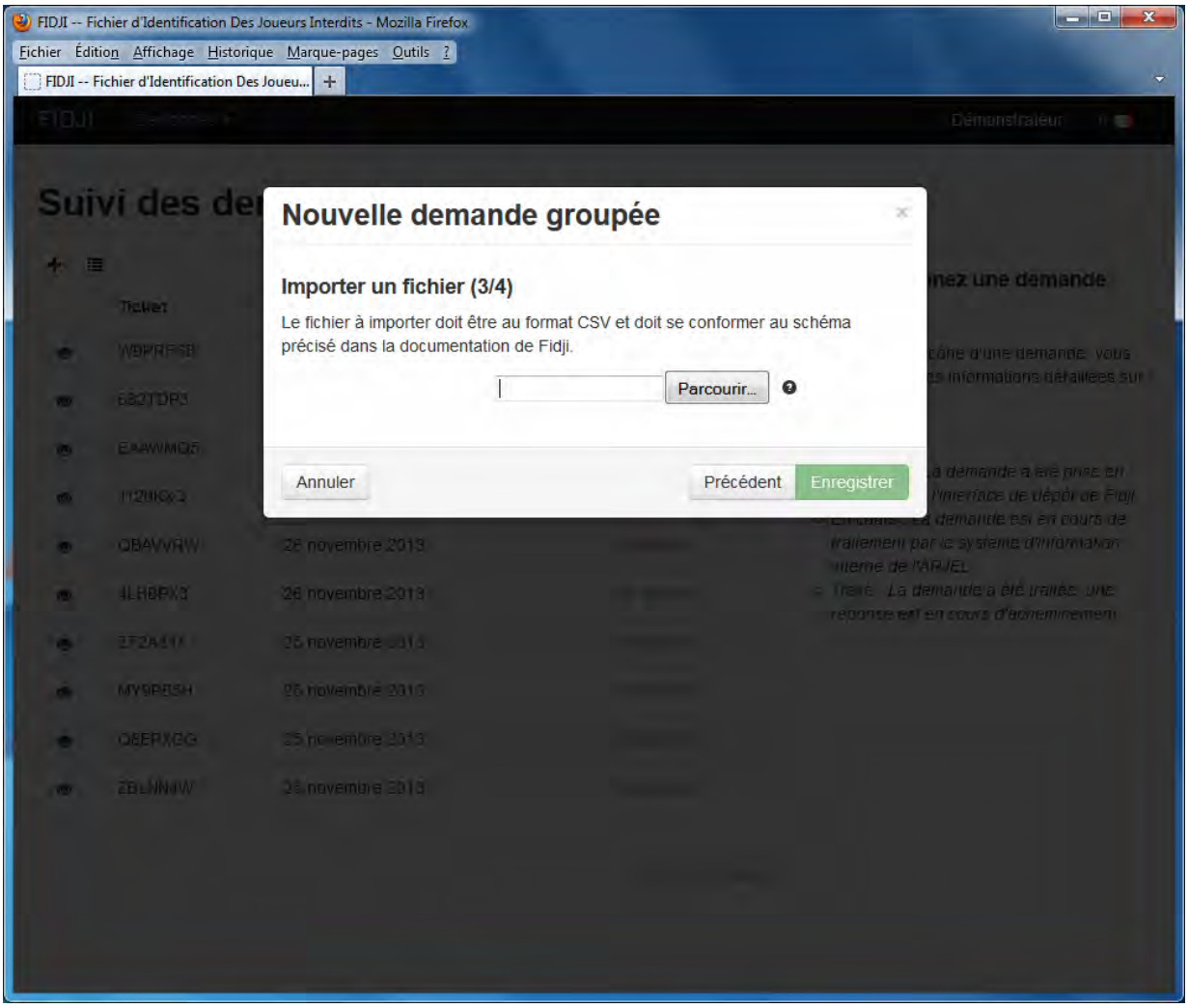


fig. 14 : Envoi du fichier CSV

Un certain nombre de contrôles sont effectués sur le format du fichier CSV, ainsi tant que celui-ci n'est pas valide, un message d'erreur vous avertissant de la nature de cette dernière apparaitra et bloquera l'enregistrement. Une fois le fichier valide envoyé, la demande groupée peut être enregistrée.

Résumé

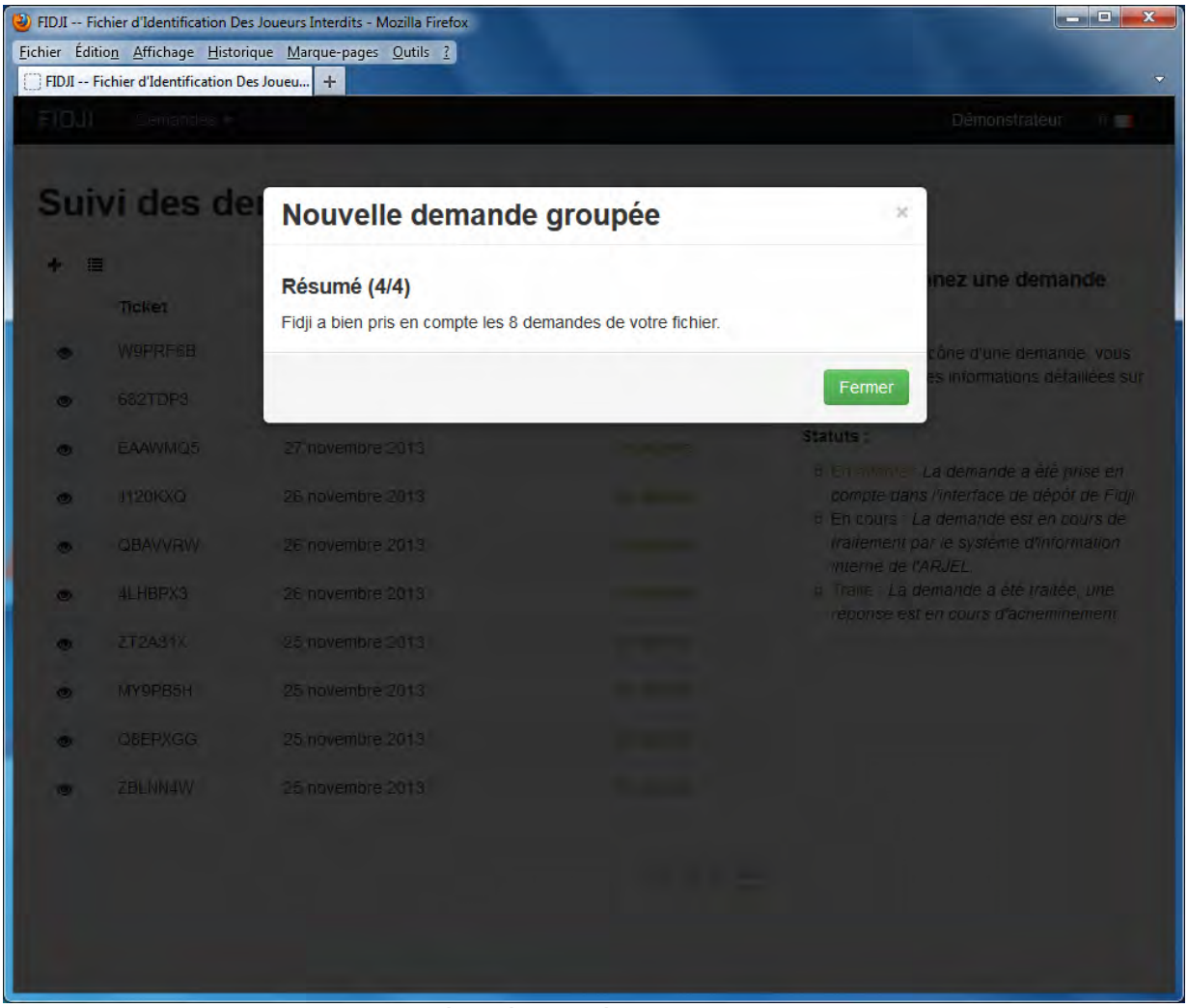


fig. 15 : Résumé de l'intégration du fichier CSV

Si l'enregistrement de la demande s'est bien passé, alors un résumé indiquant le nombre de demandes individuelles contenues dans la demande groupé est affiché. Chaque demande rejoint la liste des demandes en attente dans l'outil de suivi.

Service Web

Le service web est une interface de programmation (API) dite *RESTful*. Architecturée par-dessus le protocole HTTP, elle permet à une application de déposer automatiquement et simplement de nouvelles demandes en effectuant une requête HTTP spécifique.

Au même titre qu'un utilisateur physique, l'accès au service web de Fidji nécessite l'utilisation d'un certificat SSL client.

https://[site dédié]/api/applications/[?status=<arg>]	**GET**
Récupérer la liste des demandes en cours pour la fédération délégataire identifiée par le certificat. **Arguments** : ***arg*** : une ou plusieurs valeurs séparées par des virgules (,) parmi `pending`, `active` et `processed`. Ces trois valeurs correspondent aux différents statuts pris par une demande. **Réponse** : (200) Success Le format de la réponse est de type `application/json`	

https:// [site dédié]/api/applications/	**POST**
Effectuer une nouvelle demande simple pour la fédération délégataire identifiée par le certificat. En cas de succès, la demande anonymisée et accompagnée de son numéro de ticket est retournée. **Payload :** Le *payload* doit être de type `application/json` **Réponse** : (201) Created Le format de la réponse est de type `application/json`	

https:// [site dédié]/api/applications/?_bulk=true	**POST**

Effectuer une nouvelle demande multiple pour la fédération délégataire identifiée par le certificat.

Les demandes sont envoyées dans une liste, en cas de succès de l'enregistrement de l'ensemble des demandes, une liste de demandes enregistrées est retournée avec une correspondance par index entre la demande et la réponse.

Payload :

Le *payload* doit être de type `application/json`

Réponse : (201) Created

Le format de la réponse est de type `application/json`

Lexique

ARJEL

Autorité de Régulation des Jeux En Ligne

Certificat SSL

Certificat électronique utilisé pour identifier une entité physique et chiffrer ses échanges.

Chrome

Navigateur web disponible sur plusieurs plateformes, supporté pour l'accès au service FIDJI

CSV

Comma-Separated Values. Format de fichier informatique simple et ouvert permettant de représenter des données tabulaires sous forme de valeurs séparées par un caractère spécifique. Généralement une virgule ou un point-virgule.

Fidji

Fichier d'Identification des Joueurs Interdits. Service mis à disposition des fédérations sportives par l'ARJEL pour contrôler le respect de l'interdiction de parier faite à des acteurs de compétition.

Firefox

Navigateur web libre et open-source disponible sur plusieurs plateformes, supporté pour l'accès au service FIDJI

HTTP

HyperText Transfer Protocol. Protocole de communication utilisé sur le web.

Nomenclature hiérarchisée ARJEL

Méthode de classification utilisée par l'ARJEL pour organiser l'offre agréée de pari.

Payload

Données adossées à la requête HTTP. Généralement le payload ne concerne que les requêtes POST et PUT.

Périmètre

Basé sur la nomenclature hiérarchisée ARJEL, il s'agit d'une définition du périmètre sportif sur lequel des paris peuvent être pris.

Pop-up

Fenêtre jaillissante.

REST (RESTful)

Caractéristique architecturale et comportementale d'une interface de programmation singeant le fonctionnement du web. Chaque requête s'exécute dans son propre contexte, étant de fait sans état. Une requête concerne une ressource sur laquelle une action est effectuée. Ces actions sont celles du protocole HTTP.

WWW

World Wide Web. Partie d'Internet accessible à travers un navigateur web.

Annexe V : Règles de sécurité pour les postes utilisés pour les requêtes

Le décret n°2013-947 du 22 octobre 2013 pris pour l'application de l'article L.131-16-1 du code du sport et relatif aux interdictions de paris sportifs, autorise les fédérations délégataires qui organisent ou autorisent des compétitions sportives faisant l'objet de paris sportifs à constituer un traitement informatisé de données à caractère personnel relatives aux acteurs de ces compétitions afin de pouvoir contrôler le respect de l'interdiction de parier faite à ces derniers.

La mise en œuvre de ce dispositif s'inscrit dans le respect des dispositions du référentiel général de sécurité (RGS) s'agissant des échanges électroniques de l'ARJEL avec les fédérations délégataires Pour ce traitement, l'ARJEL met notamment en œuvre un service dématérialisé comprenant un dispositif de recueil des demandes permettant d'identifier les acteurs concernés.

L'accès à ce composant est réalisé au travers d'une interface sécurisée par protocole « https » en provenance d'adresses IP fixes préalablement portées à la connaissance de l'ARJEL. Par ailleurs, l'ARJEL recommande aux fédérations concernées de dédier un poste informatique à cet usage, sécurisé selon l'état de l'art.

Vous trouverez, ci-dessous, un ensemble de recommandations destinées aux **gestionnaires techniques** et aux **agents habilités** des fédérations. Ces dernières devront, dans la mesure du possible, faire également respecter les bonnes pratiques et recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), disponibles à titre principal depuis le site http://www.ssi.gouv.fr.

Présentation générale

Les utilisateurs d'ordinateurs sont de plus en plus nombreux et ces ordinateurs sont généralement connectés à des réseaux, en particulier à l'internet. Si les utilisateurs ne prennent pas un minimum de précautions, leurs ordinateurs peuvent être facilement attaqués, et les informations les plus sensibles ne sont alors plus protégées.

Ces attaques peuvent être « massives » (visant un grand nombre d'ordinateurs et compromettant ceux qui ne sont pas correctement protégés, ou à jour), elles peuvent aussi être ciblées (virus spécifiquement créé pour rentre silencieusement sur votre ordinateur, par un document piégé ou un lien malveillant). Et quand l'attaque ne vise pas l'ordinateur, elle vise directement l'utilisateur, par ingénierie sociale, pour qu'il donne de lui-même des informations (mots de passe, identifiants).

Compte-tenu de la nature de l'activité et des données qui sont traitées par les fédérations, il est important de tout faire pour faire échec aux tentatives d'intrusions, de consultations illicites, de récupérations ou de falsifications de données qui pourraient avoir lieu.

L'attention des agents habilités est particulièrement attirée sur la sensibilité des informations qu'ils vont être appelés à manipuler et à exploiter : il s'agit d'informations directement nominatives et confidentielles dont le traitement permet de contrôler le respect d'une interdiction de parier et dont le défaut peut notamment conduire à des sanctions disciplinaires. La sécurité informatique est l'ensemble des techniques et des bonnes pratiques pour protéger les ordinateurs et les données qui y sont stockées. Les plus simples doivent impérativement être connues et mises en œuvre par les utilisateurs qui auront été habilités par les fédérations pour réaliser ce traitement.

Le présent document présente les mesures les plus importantes que vous devez mettre en œuvre

Pour aller plus loin, vous pourrez utilement consulter :

- le portail gouvernemental de la sécurité informatique (http://www.securite-informatique.gouv.fr) qui propose des fiches pratiques, des conseils, des modules d'auto-formation, etc.

- L'ensemble des guides thématiques proposés par l'ANSSI (http://www.ssi.gouv.fr), particulièrement le guide d'hygiène informatique

- Le référentiel général de sécurité : http://references.modernisation.gouv.fr/rgs-securite

- les guides de la CNIL sur http://www.cnil.fr, et particulièrement le guide sur « La sécurité des données personnelles »

RECOMMANDATIONS

AU RESPONSABLE DE LA SECURITE INFORMATIQUE AU SEIN DE LA FEDERATION

A / Sécurité de l'environnement du poste de travail

*** Sécuriser l'accès au lieu où se trouve le poste destiné à formaliser les demandes transmises à l'ARJEL**

La sécurité du système de contrôle d'accès aux locaux est bien souvent critique pour la sécurité. En effet, dès lors qu'un attaquant parvient à obtenir un accès au réseau interne de la fédération, les mesures de sécurité périmétriques mises en place deviennent inefficaces. Il faut donc protéger rigoureusement les clés permettant l'accès aux locaux et aux codes d'alarme. Les règles suivantes doivent être appliquées :

- récupérer systématiquement les clés ou les badges d'un agent habilité à son départ définitif de la fédération – ou lorsque l'habilitation lui a été retirée ;

- changer fréquemment les codes de l'alarme de la fédération ;

- ne jamais donner de clé ou de code d'alarme à des prestataires extérieurs sauf s'il est possible de tracer ces accès et de les restreindre techniquement à des plages horaires données.

*** Rédiger et appliquer une procédure d'arrivée/départ des agents habilités**

Cette procédure est destinée à vérifier que les droits octroyés sur le système d'information sont appliqués au plus juste. Notamment, il est important que l'ensemble des droits affectés à un agent habilité soient révoqués lorsqu'il n'est plus autorisé par la fédération. La procédure doit décrire a minima la gestion du contrôle des habilitations du personnel - et la gestion (création / destruction) des comptes informatiques permettant l'accès aux postes informatiques dédiés et aux certificats délivrés par l'ARJEL.

B / Sécurité du poste de travail

* Imposer des mots de passe robustes pour l'authentification des agents habilités

Les mots de passe constituent souvent le talon d'Achille des systèmes d'information. Il est important que le mot de passe choisi pour l'accès au navigateur qui exploite le certificat de l'ARJEL soit robuste (difficile à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne) et respecte idéalement les règles préconisées par l'ANSSI :

- utilisez un mot de passe unique pour chaque personne ;
- choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc.) ;
- ne demandez jamais à un tiers de générer pour vous un mot de passe ;
- modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent ;
- renouvelez les mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles ;
- ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible ;
- configurez les logiciels, y compris le navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

La robustesse d'un mot de passe dépend en général d'abord de sa complexité. Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux). Deux méthodes pour choisir vos mots de passe : la méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ; la méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

* Ne pas conserver les mots de passe en clair dans des fichiers sur les systèmes informatiques

Par souci de simplicité, les administrateurs et surtout les utilisateurs écrivent fréquemment leurs mots de passe en clair dans des fichiers stockés sur leurs postes informatiques ou se les envoient par messagerie. Ces pratiques sont à proscrire. Les mots de passe ou les éléments secrets stockés sur les machines des agents habilités sont des éléments recherchés et exploités en priorité par les attaquants, qui permettraient d'accéder à des fichiers nominatifs sensibles.

* Ne donnez pas aux agents habilités des privilèges d'administration

Ne faites aucune exception. De nombreux utilisateurs sont tentés de demander à leur service informatique de pouvoir disposer de privilèges plus importants sur leurs machines (pouvoir installer des logiciels, pouvoir connecter des équipements personnels, etc.). De tels usages sont cependant excessivement dangereux et sont susceptibles de mettre en danger le réseau dans son ensemble, les données du traitement en particulier.

*** Sécurisez le poste de travail**

Il est impératif, au minimum, de désactiver les services inutiles au traitement et de restreindre les privilèges des comptes utilisateurs. L'utilisation d'un pare-feu individuel configuré au minimum pour bloquer les connexions entrantes non sollicitées sur chaque poste dédié au traitement est généralement indispensable. Par ailleurs, le BIOS des machines doit être verrouillé avec un mot de passe non trivial et le démarrage sur supports amovibles ou via le réseau (« *Wake On LAN* ») désactivé.

*** Mettez à niveau les logiciels**

Chaque jour, des vulnérabilités sont mises en évidence dans de très nombreux logiciels largement utilisés. Quelques heures suffisent parfois pour que des codes malveillants exploitant ces vulnérabilités commencent à circuler sur Internet. Il est donc très important d'utiliser en priorité des technologies pérennes, de connaître les modalités de mises à jour de l'ensemble des logiciels utilisés et de se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.

Les mises à jour (comme les logiciels) ne doivent être téléchargées que depuis des sites de confiance (le site de leur éditeur généralement).

Il est recommandé de **traiter en priorité les composants de base** (système d'exploitation, navigateur et outils nécessaires au traitement) puis de compléter l'inventaire avec l'ensemble des autres composants logiciels et d'intégrer ces éléments à la cartographie.

Il est par ailleurs nécessaire d'inventorier et de suivre les sources d'information susceptibles de remonter des vulnérabilités sur les composants identifiés et de diffuser des mises à jour (site des éditeurs des logiciels considérés, sites des CERT).

Enfin, il est vivement recommandé de **désinstaller tous les logiciels qui ne sont pas nécessaires au traitement** réalisé sur cet ordinateur dédié. Sauf cas très particulier, les suites bureautiques, la machine virtuelle Java ou le lecteur Flash ne sont pas nécessaires au traitement.

*** Interdire la connexion d'équipements personnels à l'ordinateur dédié**

La connexion des équipements personnels ne peut être envisagée que sur des réseaux ne contenant strictement aucune information sensible. Les équipements personnels (assistants personnels, tablettes, smartphones, lecteurs MP3, clés USB) sont en effet difficilement maîtrisables par la fédération.

Il est donc important d'empêcher leur connexion à l'ordinateur dédié. Cette interdiction est d'abord organisationnelle : même si aucune règle technique n'empêche leur connexion, il convient d'inciter les utilisateurs à ne pas recourir à de telles pratiques par exemple au moyen de la charte d'utilisation des moyens informatiques. Cette interdiction doit dans la mesure du possible être complétée par des mesures techniques, dont la mise en œuvre peut toutefois s'avérer plus complexe (contrôle systématique d'accès au réseau, désactivation des ports USB).

*** Interdire techniquement la connexion des supports amovibles**

Les supports amovibles sont un moyen privilégié de propagation des codes malveillants et d'exfiltration de données. Il convient donc d'essayer d'en limiter au maximum l'usage (sauf si cela est strictement nécessaire, auquel cas il faut désactiver l'exécution des autoruns depuis de tels supports).

*** Interdire autant que possible les connexions à distance sur les postes clients**

En cas d'impossibilité d'interdire, la fédération devra respecter strictement les principes décrits dans le document technique *Recommandations de sécurité relatives à la téléassistance* proposé par l'ANSSI : http://www.ssi.gouv.fr/IMG/pdf/NP_Teleassistance_NoteTech.pdf.

*** Chiffrer les données sensibles**

La perte ou le vol de l'ordinateur dédié peut-être lourd de conséquence pour la fédération : en l'absence de chiffrement, les données stockées sur le terminal seront en effet compromises, et ce même si le terminal est éteint ou si la session utilisateur est fermée. Il est donc important de chiffrer les données sensibles, notamment les fichiers nominatifs utilisés pour le traitement : fichier général, fichiers constitués ponctuellement.

A noter que plusieurs produits ont été qualifiés ou certifiés par l'ANSSI. Le chiffrement peut être réalisé sur l'ensemble du système (on parle de chiffrement intégral), sur un sous-ensemble du système (chiffrement de partitions) ou uniquement sur les fichiers les plus sensibles.

*** Éviter l'usage d'infrastructures sans fil (wifi notamment)**

L'ordinateur dédié devrait idéalement être isolé et relié à l'internet par un réseau filaire. Si l'usage de ces technologies sans fil ne peut être évité, il convient de cloisonner le réseau d'accès wifi du reste du système d'information, et d'avoir prioritairement recours à un chiffrement des réseaux wifi reposant sur WPA Entreprise (EAP-TLS avec chiffrement WPA2 CCMP) qui permet l'authentification des machines par certificats clients des machines accédant au réseau.

*** Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires**

Chaque agent habilité devrait en permanence (au minimum chaque année) se voir rappeler :

- que les informations traitées doivent être considérées comme sensibles ;
- que la sécurité de ces informations repose, entre autres, sur l'exemplarité de leur comportement et le respect des règles élémentaires d'hygiène informatique (non-contournement de la politique de sécurité, verrouillage systématique de la session lorsque l'utilisateur quitte sa position informatique, non-connexion d'équipements personnels au réseau de la fédération, non-divulgation de mots de passe à un tiers, non réutilisation de mots de passe professionnels dans la sphère privée, signalement des événements suspects, accompagnement des visiteurs et des intervenants extérieurs, etc.).

Le respect des règles d'hygiène qui concernent les utilisateurs devraient figurer dans une charte d'usage des moyens informatiques visée par chaque utilisateur.

*** Faire auditer la sécurité**

Faire réaliser des audits de sécurité périodiques (au minimum tous les ans). Chaque audit doit être associé à un plan d'action dont la mise en œuvre est suivie au plus haut niveau. La réalisation d'audits techniques sur un système d'information est essentielle. En effet, l'audit est le seul moyen efficace de constater concrètement l'efficacité des mesures mises en œuvre sur le terrain. Chaque audit permettra de définir un plan d'actions correctives à mettre en œuvre. Des réunions de suivi de ce plan d'action doivent être organisées fréquemment. Pour une plus grande efficacité, l'avancement du plan d'action devra être synthétisé dans un indicateur du tableau de bord à destination des responsables de la fédération.

RECOMMANDATIONS

AUX AGENTS HABILITES PAR LA FEDERATION

*** Utilisez un compte non administrateur pour utiliser le service**

L'usage de l'interface ARJEL se fera systématiquement depuis un compte utilisateur, jamais depuis un compte administrateur.

*** Verrouillez votre écran**

Lorsque vous vous absentez - même pour quelques minutes - de votre bureau, vous devez verrouiller votre ordinateur pour que personne ne puisse accéder à vos données. Il est inutile de fermer la session ou d'éteindre votre ordinateur ! Une simple combinaison de touches suffit à garantir la confidentialité de votre travail, de votre messagerie, de vos documents personnels ou confidentiels.

Vous n'êtes jamais à l'abri d'un visiteur indélicat ou d'un prestataire de service curieux qui profiterait de votre absence momentanée pour "jeter un coup d'œil", ou pour voir s'il ne pourrait pas trouver des informations intéressantes pour lui ou pour son employeur.

Verrouillez votre poste de travail est donc nécessaire, vous verrez : on s'y habitue très vite ! Pour verrouiller rapidement votre ordinateur, **appuyez sur la touche Windows de votre clavier, puis, tout en la maintenant enfoncée, pressez la touche L.**

Vous ne trouvez pas la touche Windows sur votre clavier ? Elle est en bas, à gauche de la barre d'espacement : généralement coincée entre la touche ctrl et la touche Alt, on y voit la représentation du drapeau flottant « Windows ». Cette manipulation est valable autant pour les ordinateurs sous XP que sous Windows Seven.

Vous devrez ensuite simplement saisir votre mot de passe (après avoir tapé simultanément sur les touches ctrl-alt-suppr) pour déverrouiller votre ordinateur et retrouver votre session exactement comme vous l'aviez laissée.

*** Documents imprimés**

Dotez l'ordinateur dédié d'une imprimante locale. En effet, lorsque l'imprimante est éloignée du poste de travail, et parfois même située à un autre étage, on oublie facilement de récupérer le document dont on vient de lancer l'impression. Tous les efforts de sécurisation du poste de travail sont alors vains : vous aurez laissé à la portée de tous, collaborateurs, visiteurs ou intervenants extérieurs, le document confidentiel que personne ne devait voir. Si d'autres collaborateurs ont également tardé à rechercher leurs documents, le risque est accru de ne pas pouvoir récupérer les siens car ils auront été emportés par un autre.

Lorsque vous imprimez un document, allez le chercher avant qu'un autre le fasse : évitez de laisser toute une série d'impressions abandonnée sur l'imprimante. Si nécessaire, retardez-en l'impression jusqu'au moment où vous serez certain de pouvoir aller le récupérer.

*** Ne cliquez pas trop vite sur un lien ; n'ouvrez pas trop vite la pièce jointe à un message**

Idéalement, votre messagerie ne devra pas se trouver sur le poste dédié au traitement. De même que votre navigateur à des fins autres que le traitement ARJEL.

Mais pour le cas où il serait impossible de procéder autrement, soyez très vigilant.

Une attaque très classique visant à tromper votre attention consiste à vous inciter à cliquer sur un lien placé dans un message, ou à ouvrir une pièce jointe, comme un document Word ou un fichier PDF. Généralement, vous recevrez par messagerie un message, semblant provenir d'un organisme de confiance ou d'un collaborateur, vous transmettant un document cohérent avec votre activité ou vos attentes. Le contenu du message est vraisemblable, il utilise le logo de l'organisme (par exemple le logo de l'ARJEL ou du ministère des sports).

Mais ce document peut-être trompeur et malveillant. Plutôt que de cliquer sur le lien, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. S'il s'agit d'un document joint et que vous avez le moindre doute, ne l'ouvrez pas et prévenez la personne en charge de la sécurité informatique au sein de la fédération. Ces courriers frauduleux peuvent être ciblés (créés spécialement pour vous compromettre) ou envoyés à des milliers d'adresses.

Comment s'en protéger ?

Vos correspondants – et particulièrement les services techniques de l'ARJEL - ne demandent pas (ou ne devraient pas vous demander) de saisir des informations personnelles dans un courrier électronique. Pour se connecter au site d'un correspondant, il vaut mieux entrer manuellement l'adresse du site dans votre navigateur.

Préférez saisir des informations personnelles (coordonnées bancaires, identifiants…) sur des sites internet sécurisés : un cadenas apparaît dans le navigateur et l'adresse du site commence par HTTPS au lieu de HTTP.

Soyez vigilant lorsqu'un courriel demande des actions urgentes.

Utilisez le filtre contre le filoutage du navigateur internet : la plupart des navigateurs (Microsoft Internet Explorer, Mozilla Firefox …) proposent une fonctionnalité d'avertissement contre le filoutage. Leurs principes peuvent être différents (liste noire, liste blanche, mot clé…) et sans être parfaites, ces fonctions aident à maintenir la vigilance.

Ne répondez jamais – et ne transférez jamais ces courriels.