Commission de Surveillance du Secteur Financier

Annexe 1

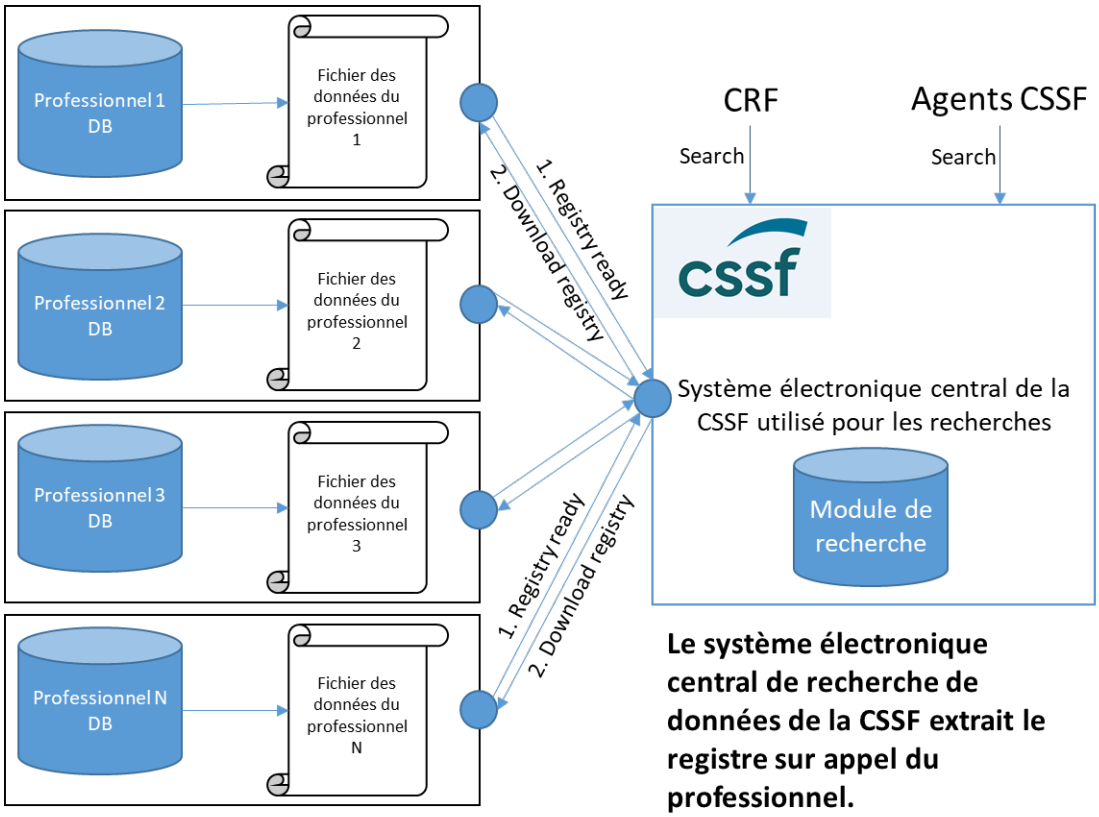
Suivi des versions

Version	Date	Commentaires
1.0	21/07/2020	Version 1 – publication officielle
2.0	04/09/2020	Version 2 – publication officielle - Modifications concernant la procédure d'enrôlement - Modifications concernant l'authentification de la CSSF auprès du professionnel - Ajout des spécifications concernant le stockage des fichiers / clarification sur la fréquence d'envoi - Ajout d'informations concernant les environnements mis à disposition par la CSSF - Informations supplémentaires à fournir pour la demande de création de compte MFT

TABLE DES MATIÈRES / TABLE OF CONTENTS

1. Architecture générale

Afin de mettre en place le système électronique central de recherche des données tel que défini dans la présente circulaire, le professionnel doit mettre à disposition dans son système informatique, un fichier de données auquel la CSSF accédera.



Le système électronique central de recherche de données de la CSSF extrait le registre sur appel du professionnel. Indépendamment de la disponibilité du professionnel, un module de recherche sera mis à disposition des autorités nationales.

L'approche générale :

1. **Sur base journalière,** le professionnel doit constituer dans son système informatique les fichiers de données concernant toute information relative aux comptes de paiements, aux comptes bancaires et/ou aux coffres-forts », selon le format défini dans l'annexe 2 (cf. §4.1.4 « Structure du fichier »)

2. Le professionnel met à disposition le fichier et prévient la CSSF de sa disponibilité [Etape 1 : « Registry ready » du schéma d'architecture] ;
3. La CSSF se connecte et télécharge le fichier [Etape 2 : « download registry » du schéma d'architecture] ;
4. La CSSF envoie aux professionnels un fichier de retour (feedback) incluant le statut du fichier téléchargé : accepté ou rejeté incluant les erreurs rencontrées. En cas de rejet, un fichier corrigé doit être mis à disposition de la CSSF. (cf. §4.2 « Retour/Réponse CSSF »).
5. Le professionnel est responsable de la sécurisation du fichier mis à disposition. Il pourra par exemple le supprimer une fois le fichier téléchargé par la CSSF.

Afin de s'identifier auprès de la CSSF et de mettre à disposition son fichier le professionnel doit implémenter une interface de communication spécifique, dite « Application Programming Interface », (« API »).

Commission de Surveillance du Secteur Financier

2. Enrôlement

2.1 Principe

Pour garantir le bon fonctionnement du nouveau canal de sécurité entre le professionnel et la CSSF, il est nécessaire de procéder à une phase d'initialisation, permettant d'échanger différents types d'informations de sécurité. La procédure d'enrôlement, l'API détaillée et les détails d'implémentation technique seront fournis aux professionnels moyennant une demande spécifique qui devra parvenir à la CSSF une fois la présente circulaire publiée (cf. 5.3 Demande d'accès par MFT).

Veuillez trouver ci-dessous les grandes étapes de la phase d'enrôlement :

1. Initialisation :

   La CSSF fournit les clés RSA privées et publiques du professionnel qui seront utilisées pour l'initialisation de la connexion sécurisée entre le professionnel et la CSSF. La clé privée envoyée est protégée par un mot de passe (passphrase) qui sera envoyé par la CSSF au professionnel via un autre canal sécurisé.

   Le professionnel récupère la clé publique RSA de la CSSF correspondant à son certificat client TLS ainsi que les clés publiques PGP nécessaires au chiffrement des fichiers ;

2. Toute communication entre la CSSF et le professionnel utilise au minimum une authentification « Mutual TLS » ;
3. Le professionnel fournit une API permettant à la CSSF d'envoyer les identifiants « HTTP » du professionnel utilisés pour s'authentifier auprès de la CSSF ;
4. Les clés publiques PGP des professionnels, utilisées pour signer les fichiers envoyés et déchiffrer les fichiers reçus, sont publiées par chaque professionnel dans l'API d'enrôlement de la CSSF.

2.2 Protection du canal sécurisé

L'échange des fichiers et l'accès à l'API se font par le biais d'une connexion Internet chiffrée en HTTPS et authentifiée à l'aide de certificats TLS mutuels. La présence d'une API du côté de la CSSF et d'une API coté professionnel implique l'utilisation de deux canaux HTTPS différents (l'un du professionnel vers la CSSF et l'autre de la CSSF vers le professionnel). Chacun de ces deux canaux est pourvu d'une authentification par certificat client (TLS mutuel). La CSSF met en œuvre une liste blanche des adresses IP pouvant accéder à ses API. Une liste blanche doit également être maintenue par le professionnel concernant les accès réalisés par la CSSF.

Les certificats utilisés pour l'authentification mutuelle sont signés par l'autorité de certification de la CSSF et sont fournis aux professionnels. Les spécifications techniques concernant cette authentification TLS sont les suivantes :

- La CSSF doit fournir la clé publique de son certificat client et la chaine de confiance complète (« Chain file ») au professionnel ;
- Les deux connexions HTTPS (du professionnel vers la CSSF, et vice versa) doivent utiliser des protocoles de chiffrements robustes et dépourvus de failles connues, tant pour le chiffrement de la connexion, l'échange de clé et le mécanisme de hachage ;
- Le protocole TLSv1.2 minimum doit être mis en œuvre.

Certaines des API exposées par la CSSF seront également authentifiées au niveau HTTP (à l'aide d'un identifiant et d'un mot de passe, générant un token JWT).

3. Interfaces d'échanges

3.1 Authentification des APIs

Le professionnel doit s'authentifier en HTTP lors de certains appels API vers la CSSF. Le but de cette authentification est de limiter les appels à l'API en plus de la partie certificat client HTTPS. Le professionnel utilise alors un compte de service fourni par la CSSF.

Le cycle de vie des mots de passe est géré par la CSSF.

3.2 API fournie par les professionnels

Chaque professionnel doit mettre à disposition une API liée à la récupération du fichier pour la construction du registre central de recherche. Le professionnel peut obtenir les détails techniques de cette API par l'intermédiaire du point de contact défini par la CSSF (registre.compte@cssf.lu). Ces détails techniques sont fournis au format OpenAPI v3.0 (OpenAPI).

L'API à fournir par le professionnel propose, de manière sécurisée, les services suivants :

- Mise à disposition d'un fichier contenant l'ensemble des informations attendues par la CSSF (cf. Notification)
- Réception du feedback CSSF informant les professionnels sur le statut du fichier (cf. Retour de la CSSF)
- Réception des identifiants utilisés par le professionnel pour se connecter auprès de la CSSF.

3.3 API fournie par la CSSF

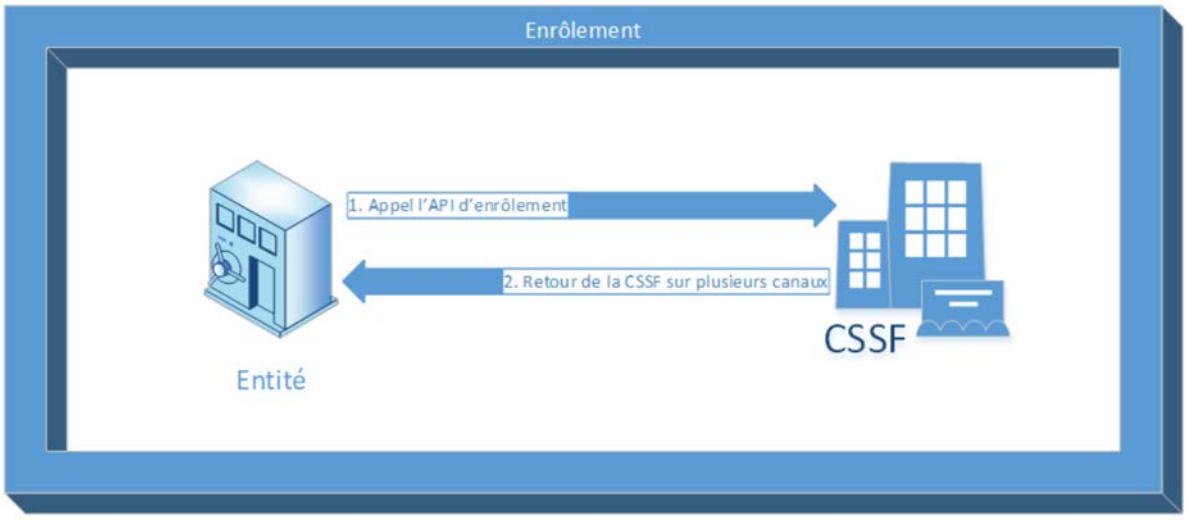
La CSSF expose plusieurs API :

- L'API d'authentification http ;
- L'API enrôlement ;
- L'API de réinitialisation ;
- L'API de notification ;
- L'API de récupération des clés PGP publiques.

3.3.1 API d'authentification HTTP

Cette API permet au professionnel d'obtenir un token JWT utilisable sur le reste des API. Pour ce faire, le professionnel doit fournir les identifiants HTTP préalablement fournis par la CSSF. Cette API n'est disponible que sur présentation d'un certificat client TLS valide.

3.3.2 API d'enrôlement



L'API d'enrôlement permet l'enregistrement des professionnels dans le système. Elle permet au professionnel de transmettre les informations suivantes :

- Adresse web de l'API du professionnel, où les fichiers vont être récupérés
- Adresses IP utilisées par le professionnel pour appeler les API de la CSSF
- Clé PGP publique pour la signature des fichiers envoyés à la CSSF
- Clé PGP publique pour le déchiffrement des fichiers reçus par le professionnel

Les clés PGP seront fournies au format ASCII Armor.

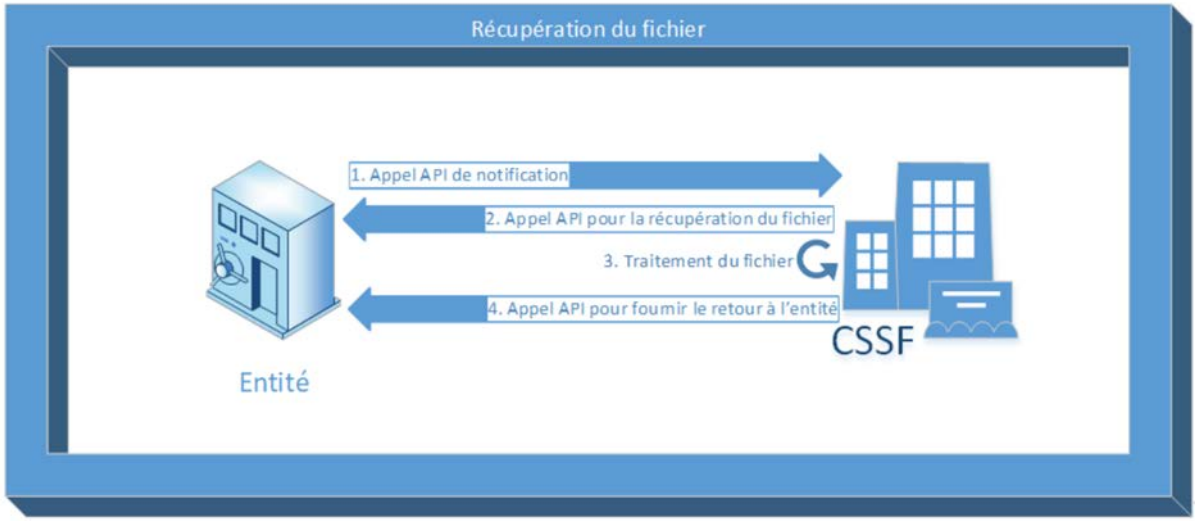
3.3.3 API de réinitialisation

Suite à un enrôlement réussi, le professionnel reçoit en confirmation un code de sécurité (reset token) qui lui servira à initier une nouvelle phase d'enrôlement dans un des cas suivants :

- Changement d'une ou plusieurs clés PGP du professionnel ;
- Changement de l'adresse web de l'API du professionnel ;
- Changement d'adresses IP utilisées par le professionnel pour appeler les API de la CSSF ;
- Révocation du certificat client HTTPS du professionnel ;
- Changement de mot de passe du professionnel.

3.3.4 API de notification

L'API de notification instruit la CSSF de la présence d'un fichier à télécharger.



3.3.5 API de récupération des clés PGP publiques

Cette API est publiée par la CSSF. Elle permet au professionnel de récupérer 2 clés PGP :

- la clé PGP publique permettant de vérifier la signature de la CSSF
- la clé PGP publique permettant de chiffrer les fichiers à envoyer à la CSSF.

4. Echange de fichiers

4.1 Le fichier mis en place par le professionnel

4.1.1 Fréquence d'envoi

Le professionnel doit fournir à la CSSF un nouveau fichier complet (« FULL ») et valide, contenant toutes les données visées à l'annexe 2 de la présente circulaire, relatives aux comptes de paiements, aux comptes bancaires et/ou aux coffres-forts, reflétant l'état des informations des professionnels au jour J. Un fichier doit être disponible pour la CSSF au moins une fois par jour, tous les jours (weekend et jours fériés compris).

Sauf situation exceptionnelle qui devra, dans la mesure du possible, être communiquée à la CSSF à l'avance, la notification à la CSSF de la mise à disposition du fichier du jour J par le professionnel est attendue entre le jour J à 18h et le jour J+1 à 6h (heures de Luxembourg). Dans le cas où aucune modification ou ajout n'ont eu lieu, la CSSF s'attend à recevoir les mêmes données que la veille.

Chaque ajout ou modification des informations que la CSSF s'attend à recevoir doit être mis à disposition dans les 24h au plus tard.

4.1.2 Unicité du téléchargement

Le fichier mis à disposition à la CSSF par le professionnel ne sera téléchargé que via une URL à usage unique. Cette URL comporte un « token » unique transmis lorsque le professionnel prévient la CSSF de la disponibilité du fichier pour téléchargement. De multiples appels sur une URL unique devrait générer une alerte dans le système d'information du professionnel.

Dans le cas d'un échec de téléchargement (par exemple, si une erreur survient durant le téléchargement du fichier par la CSSF), le professionnel devra renotifier le CSSF avec un nouveau token et invalider l'ancien.

4.1.3 Sécurité des fichiers

Le fichier envoyé par le professionnel doit être chiffré et compressé en PGP avec une clé publique fournie par la CSSF et signée avec une clé privée PGP du professionnel.

Le fichier envoyé par la CSSF au professionnel lui notifiant le statut de l'envoi doit être chiffré et compressé en PGP avec une clé publique PGP fournie par le professionnel et signée avec une clé privée PGP de la CSSF.

Les spécifications techniques concernant le chiffrement PGP des fichiers sont les suivantes :

- Les clés publiques PGP sont conservées par la CSSF pendant 20 ans, même après un renouvellement de clé afin de garantir la non répudiation ;
- Les clés privées PGP doivent avoir au minimum 4096 bits (RSA) ou 256 bits en courbes elliptiques ;
- Les clés PGP du professionnel doivent avoir une durée de validité d'au moins 2 ans. A l'issue de ces deux années, la CSSF se réserve le droit de demander un renouvellement des clés ;
- Les fichiers envoyés doivent être au format PGP binaire ; les clés PGP sont elles au format ASCII Armor.

4.1.4 Structure du fichier

L'annexe 2 présente la structure du fichier au format JSON attendu, les informations obligatoires ou optionnelles, ainsi que leur format, et un fichier exemple de valeurs possibles.

Les informations doivent être encodées au format UTF8.

Note : La CSSF conseille aux professionnels d'utiliser le validateur JSON qui sera mis à leur disposition ou d'implémenter leur propre validateur. Celui-ci doit permettre de vérifier la validité de leur fichier de données, de relever et de notifier les éventuelles erreurs d'encodage avant l'échange. Le validateur JSON mis à disposition du professionnel sera identique à celui utilisé par la CSSF pour valider les fichiers reçus quotidiennement.

4.1.5 Reprise des données

Dans le cas où le professionnel souhaite corriger ou mettre à jour des informations dans le fichier du jour, il garde la possibilité de fournir à la CSSF un nouveau fichier de données comportant les nouvelles informations.

De même, si le professionnel reçoit un fichier de retour de la CSSF comportant des erreurs (voir §4.2), il doit corriger les erreurs associées et envoyer un nouveau fichier valide en respectant les délais prévus par la loi.

4.2 Le fichier de retour / réponse de la CSSF

4.2.1 Structure du retour

La CSSF envoie à la fin du traitement de chaque fichier de données des professionnels, un fichier de retour (« feedback ») concernant le traitement du fichier. Cet appel est initié par la CSSF et utilise l'API fournie par les professionnels (cf. §1.1).

Ce fichier de retour est structuré en JSON comme décrit par le schéma OpenAPI v3.0 (OpenAPI) suivant :

```
openapi: 3.0.0
info:
version: 1.0.0
initial_file_key: emprunte du fichier initial de type SHA-512
components:
    feedback:
        title: Statut de traitement du fichier
          type: object
          properties:
            status:
              type: string
              enum: [ACPT, RJCT]
              description: Statut du fichier reçu par la CSSF. Si le fichier est au statut RJCT, l'entité doit corriger le fichier et notifier à nouveau la CSSF de sa disponibilité.
            fileid:
              type: string
              pattern: '^[A-Z]\d{8}-\d+$'
              description: Identifiant unique du fichier téléchargé. ID qui doit provenir d'une notification envoyée à la CSSF. Il doit commencer par l'identificateur d'entités «-» valeur de séquence du fichier.
            errors:
              type: array
              items:
                type: object
                properties:
                  id:
                    type: string
                    pattern: '^CSSF-\d{3}$'
```

```
                description: Code d'identification de l'erreur
              message:
                type: string
                description: Details du message d'erreur
      required:
        - status
        - fileid
```

4.2.2 Exemples de retours

Le JSON suivant est un exemple de retour en cas d'acceptation par la CSSF :

```
{
"status":"ACPT"
"initial_file_key":"c672b8d1ef56ed28ab87c3622c5114069bdd3ad7b8f9737498d0c01ecef0967a"
}
```

Le JSON suivant est un exemple de refus par la CSSF :

```
{
    "status": "RJCT"
      "initial_file_key":"c672b8d1ef56ed28ab87c3622c5114069bdd3ad7b8f9737498d0c01ecef0967a"
    "errors": [
          {
                "uuid": "QQOIUZHGF3GH45IK"
                "id": "CSSF-999"
                "message": "Wrong IBAN format"

          }
    ]
}
```

4.2.3 Modalités en cas de rejet

Si le retour de la CSSF contient un statut rejeté « RJCT », le professionnel doit fournir à la CSSF un nouveau fichier de données jusqu'à ce qu'il obtient un statut accepté « ACPT ».

5. Stockage des fichiers

Le professionnel a pour obligation de stocker quotidiennement le dernier fichier accepté par la CSSF pour le jour courant ainsi que la preuve d'acceptation (fichier de retour fourni par la CSSF).

La CSSF gardera également une copie du fichier de retour ; afin de vérifier l'intégrité de ces fichiers, elle générera et stockera plusieurs empreintes de type Hash pour chacun des fichiers stockés.

Le délai de conservation obligatoire est de 5 ans conformément aux dispositions prévues par l'article 3, paragraphe 6, de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme.

6. Informations diverses

6.1 Environnements

En plus de l'environnement de production, la CSSF mettra à disposition un environnement de test. Il est demandé au professionnel d'effectuer des tests de mise à disposition du fichier de données sur cet environnement avant passage à l'environnement de production.

Les fichiers mis à disposition par le professionnel dans l'environnement de test devront contenir des données anonymisées.

6.2 Disponibilité du fichier de données

Le professionnel s'engage à garantir un niveau de disponibilité de service suffisant pour transmettre les informations contenues au sein de leur fichier, au moins une fois toutes les 24h à la CSSF.

Le fichier doit être disponible au téléchargement une fois la notification envoyée à la CSSF et jusqu'à la fin du téléchargement du fichier. La plateforme du professionnel peut être indisponible le reste du temps.

En cas de non réponse de la CSSF, le professionnel continuera à notifier la CSSF toutes les 10 minutes tant que le fichier n'a pas été récupéré par celle-ci.

6.3 Demande d'accès par MFT

Les documents relatifs aux détails techniques sont transmis de manière sécurisée au professionnel par la CSSF au moyen de son système dit Managed File Transfer (« MFT »).

Afin d'obtenir un identifiant permettant la connexion au système en ligne, le professionnel renseignera à la CSSF par envoi à l'adresse de courriel électronique registre.compte@cssf.lu les informations suivantes :

- Numéro signalétique attribué par la CSSF (de type « Bxxx »)

- Nom de l'organisation

- Nom et prénom de la personne responsable en matière d'envoi

- Adresse de courriel principale de contact[1]

- Seconde adresse de courriel de contact à laquelle une partie des informations d'identification sera envoyée[1]

- Téléphone de contact

- Si le professionnel délègue une ou plusieurs des obligations prévues par la loi du 25 mars 2020, préciser quel(s) sera (respectivement seront) le(s) prestataire(s) choisi pour remplir chacune d'elles.

6.4 Informations de contact auprès de la CSSF

Toute question technique est à adresser à l'adresse électronique registre.compte@cssf.lu

[1] Il est requis que les adresses de contacts principale et secondaire fournies soient différentes et génériques, c'est-à-dire qu'elles ne soient pas nominativement attribuées à une personne physique. Il est requis que ces adresses ne soient pas accessibles par les mêmes personnes.