Commission de Surveillance du Secteur Financier

Annex 1

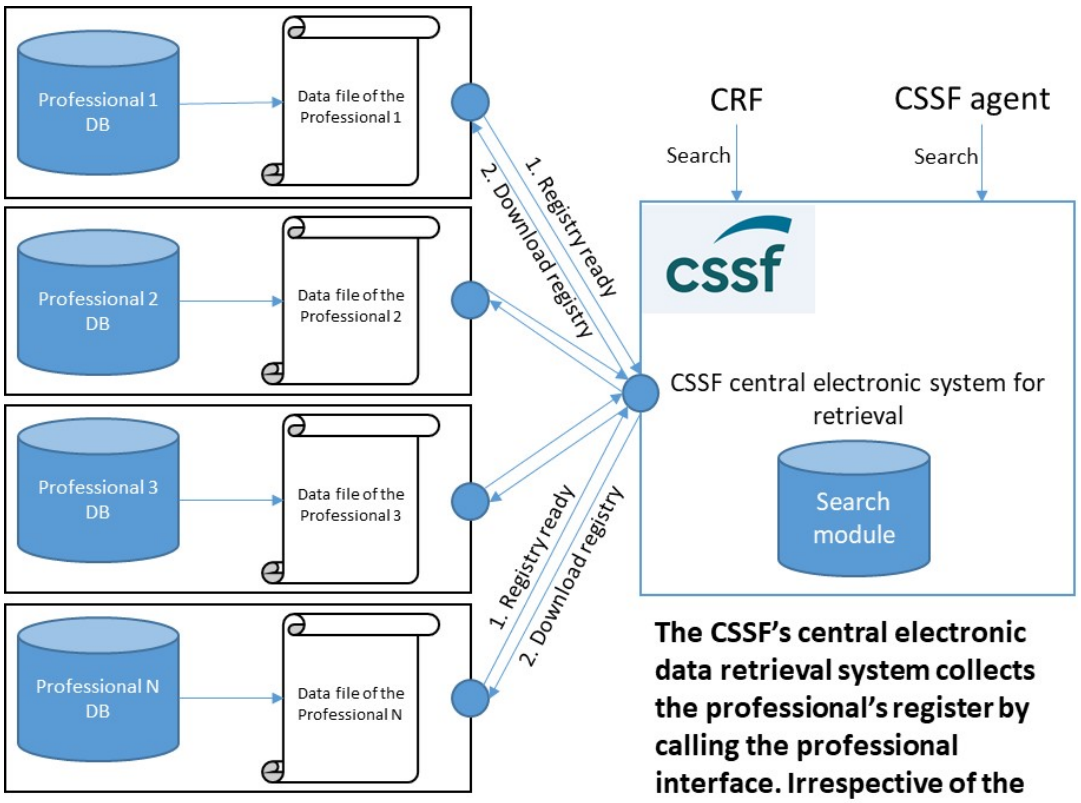
Version tracking

Version	Date	Comments
1.0	21/07/2020	Version 1 – Official publication
2.0	04/09/2020	Version 2 – Official publication - Modification of the enrolment procedure - Modification of CSSF's authentication to the professional interface - Additional information of file storage/clarification on the frequency of file sending - Additional information on the environment made available by the CSSF - Additional information to be provided for the MFT account creation request
2.1	24/06/2022	Version 2 – Official publication Update on file exchange frequency

CONTENTS

1. General architecture

For the purposes of setting up a central electronic data retrieval system, as defined in this circular, professionals shall make a data file available, in their IT system, which the CSSF will have access to.



The CSSF's central electronic data retrieval system collects the professional's register by calling the professional interface. Irrespective of the professional's interface availability, the search module will be made available to national authorities.

General approach:

1. Professionals shall prepare **on day to day basis**, in their IT system, data files related to information on payment accounts, bank accounts identified by IBAN (hereinafter "bank accounts") and/or safe-deposit boxes. The files shall comply with the format defined in annex 2 (cf. §4.1.4 "Structure of the file");
2. Professionals shall make the file available and notify the CSSF of its availability [Step 1: "Registry ready" of the architectural pattern];

3. The CSSF connects to the professional interface and downloads the file [Step 2: "Download registry" of the architectural pattern];
4. The CSSF notifies the professionals with a feedback containing the status of the file processing: accepted or rejected and the list of errors encountered when relevant. In case of failure, , a corrected file shall be made available to the CSSF (cf. §4.2 CSSF Feedback/Answer");
5. Professionals are in charge of securing this file provided. Professionals should foresee, for example, to delete it once the file has been downloaded by the CSSF.

To identify themselves with the CSSF and to make their file available, professionals shall implement a specific communication interface, the so-called "Application Programming Interface", ("API").

2. Enrolment

2.1 Principle

In order to set up a secure channel between the CSSF and the professional, an initialisation phase called enrolment must be conducted. During this phase, the CSSF and the professional will exchange through a secure way, security and identification information. All the necessary information (the enrolment procedure, the detailed API and the technical implementation details) will be provided to professionals. The professional shall address a specific request to the CSSF once the circular has been published (cf. §5.3 "Access request via MFT").

Please find below the major steps of the enrolment phase:

1. Initialisation
   The CSSF provides the professionals' private and public RSA keys which will be used for the initialisation of the secure connection between professionals and the CSSF. This private key is protected by a password (passphrase) which will be sent by the CSSF to professionals via another secure channel.

   Professionals receive via an API the CSSF's RSA public key corresponding to their TLS client certificate as well as the PGP public keys used for the file encryption;

   2. Any communication between the CSSF and the professional uses at least "Mutual TLS" authentication.

   3. The professional exposes an API to the CSSF to send the professional "HTTP" identifiers used to identify itself to the CSSF.

4. Professionals' PGP public keys, which are used to sign the files sent and to decrypt files received, are made available by each professional through the CSSF's enrolment API.

2.2 Secure channel protection

The exchange of files and the access to the API are performed through HTTPS-encrypted Internet connections. The connection is authenticated via a mutual TLS certificate. Two APIs (one from CSSF's side and one from professionals' side) are made available. This requires to use two different HTTPS channels: one, from professionals to the CSSF, and the other, from the CSSF to professionals. Both channels include a customer certificate authentication (mutual TLS). The CSSF maintains a white list of IP addresses that are authorised to access its APIs. A white list shall also be maintained by professionals with respect to the access achieved by the CSSF.

The certificates used for the mutual authentication are signed by the CSSF's certification authority and will be provided to professionals. The technical specifications regarding this TLS authentication are as follows:

- The CSSF shall provide a public key of its client certificate and a complete trust chain file to the professional;
- Both HTTPS connections (from the professional to the CSSF, and vice-versa) shall include strong encryption protocols without known issue for the connection encryption, key exchange and hashing mechanism;
- The minimum TLSv1.2 protocol shall be implemented.

Some APIs used by the CSSF will also be authenticated at HTTP level (using a username and a password, that will generate a JWT token).

3. Exchange interfaces

3.1 API authentication

When calling the professional's API, the CSSF shall authenticate using HTTP. The aim of this authentication is to limit calls to the API in addition to the HTTPS client certificate. The professional then uses credentials provided by the CSSF

The life cycle of passwords is managed by the CSSF

3.2 API provided by professionals

Each professional shall make available an API to enable the file retrieval. Professionals may request to get more technical details on this API through the contact point defined by the CSSF (registre.compte@cssf.lu). These technical details will be provided in OpenAPI v3.0 (OpenAPI).

The API provided by the professional allows in a secure way, to exchange the following information:

- the daily file including all the information expected by the CSSF (cf. "Notification");
- the feedback provided by the CSSF that informs professionals of the file's status (cf. "CSSF feedback").
- identifiers used by the professional to connect to the CSSF interface.

3.3 API provided by the CSSF

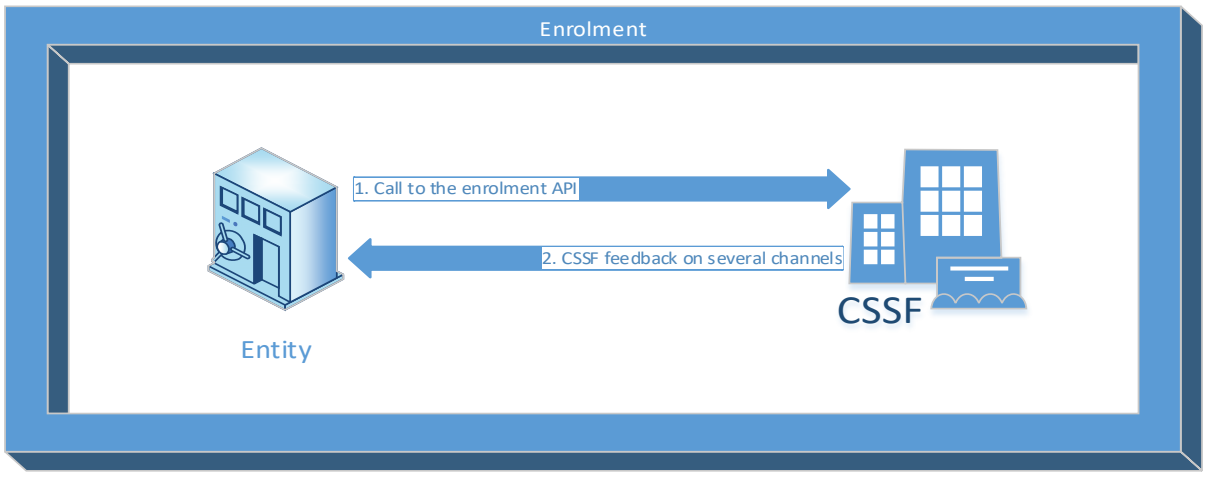
The CSSF provides several APIs:

- HTTP authentication API;
- Enrolment API;
- Reset API;
- Notification API;
- The Public PGP Keys Recovery API.

3.3.1 HTTP authentication API

This API allows the professional to retrieve a JWT token which will be used on the other the APIs. To do so, the professional must provide HTTP user identifications previously provided by the CSSF. This API is only available on presentation of a valid TLS client certificate.

3.3.2 Enrolment API



The enrolment API allows professionals registration into the system. It allows professionals to share the following information:

- Web address of the professional's API where the files will be retrieved;
- IP addresses used by the professional to call the CSSF's APIs;
- Public PGP key for the files signature sent to the CSSF
- Public PGP key for files decryption received by the professional.

PGP keys will be provided into the Armor ASCII format.

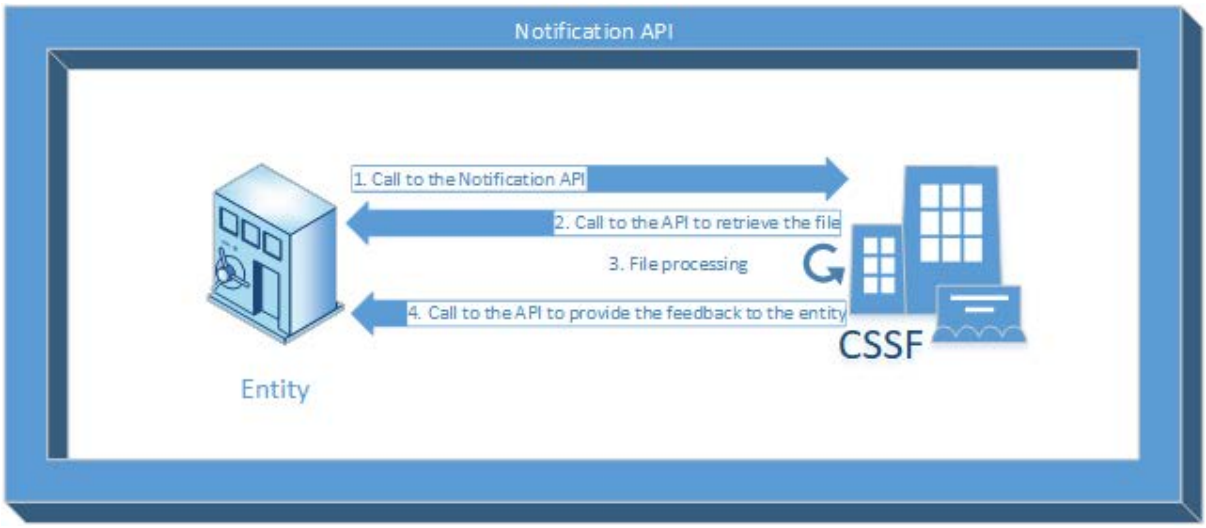
3.3.3 Reset API

Professionals receive a confirmation security code (reset token) that will be used in case of a new enrolment phase. The new enrolment shall occur in the following cases:

- Change of one or several professional's PGP keys;
- Change of the professional's API website;
- Change of IP contact addresses used by the professional for calling the CSSF's APIs.
- Revocation of the professional's HTTPS client certificate
- Change of the professional's password.

3.3.4 Notification API

Notification API informs the CSSF about a file to download.



3.3.5 Public PGP key retrieval API

This API is published by the CSSF. It allows the professional to receive two PGP keys:

- The public PGP key allowing to verify the CSSF's signature
- The public PGP key allowing to encrypt files to send to the CSSF.

Commission de Surveillance du Secteur Financier

4. Exchange of files

4.1 File established by professionals

4.1.1 Frequency of transmission

Professionals shall provide the CSSF with a new valid and full file ("FULL"), that contains all the data referred to in annex 2 of this circular, relating to payment accounts, bank accounts and/or safe-deposit boxes. The professionals must provide with the most recent information available on D - day. A file shall be made available to the CSSF from Monday to Friday, at least once a day (excluding weekends and Luxembourg public and bank holidays).

Unless there is a special situation that, where possible, will have to be communicated to the CSSF in advance, the notification to the CSSF of the file availability on the day D by the professional is expected between the day D 6 p.m. and the day D+1 6 a.m (Luxembourg time). If there is no change or modification in the information to be provided, the CSSF expects to receive the same data as the previous day.

Each new entry or modification of the information previously reported shall be made available within no more than 24 hours later.

4.1.2 Single download

The file made available to the CSSF by professionals will be downloaded via a single-use URL. This URL includes a single token transmitted when the professional notifies the CSSF that the file is available for download. Several calls that URL should generate an alert in the professionals' IT system.

In the case of a download failure (for example, if an error occurs while downloading the file by the CSSF), the professional will have to notify again the CSSF with a new token and to invalidate the older one.

4.1.3 File Security

The file sent by the professional must be encrypted and compressed using PGP with a public key provided by the CSSF and signed with a private PGP key of the professional.

The file sent by the CSSF to the professional notifying the daily file processing status, must be encrypted and compressed in PGP with a PGP key provided by the professional and signed with a CSSF's PGP private key.

The technical specifications regarding the PGP encryption of the files are as follows:

- PGP public keys are kept by the CSSF during 20 years even after a key renewal in order to guarantee non-repudiation;
- The PGP private keys shall support at least 4096 bits (RSA) or 256 in elliptical curves;
- The PGP keys of the professional shall have a validity of at least 2 years. After these two years, the CSSF may request renewal of the keys.
- Files sent shall be in PGP binary format; PGP keys are in the ASCII Armor format.

4.1.4 File structure

The Annexe 2 presents the description of the data expected and outlines the structure of the file in the expected JSON format, the optional or mandatory information, as well as their format, and an example file of possible values.

The information shall be encrypted in UTF8 format.

Note: The CSSF recommends professionals to check the validity of their data file either against the JSON validator that will be made available to them or against their own validator. This should allow to identify and notify possible encoding errors prior to the exchange. The JSON validator made available to the professional will be the same as the one used by the CSSF to validate files received daily.

4.1.5 Data recovery

In the case the professionals would like to correct or update information already provided into the file of the day, they shall provide a new data file including new information.

When the professional receives a feedback file from the CSSF including errors (See §4.2), he has to correct them, and send a new valid file respecting the legal deadlines.

4.2 CSSF Feedback / Answer

4.2.1 Feedback structure

At the end of the processing of the professional' data file, the CSSF sends a feedback about the file processing. This call shall be initiated by the CSSF using the API provided by professionals (cf. §3.2).

This feedback file is JSON-structured as described in the following OpenAPI v3.0 schema (OpenAPI):

```yaml
openapi: 3.0.0
info:
  version: 1.0.0
initial file key: borrow from the initial file SHA-512 type
components:
    feedback:
        title: File processing status
          type: object
          properties:
            status:
              type: string
              enum: [ACPT, RJCT]
              description: Status of the file received by the CSSF. If the file status is RJCT, the entity must correct the file and re-notify the CSSF of its availability.
            fileid:
              type: string
              pattern: '^[A-Z]\d{8}-\d+$'
              description: Unique identifier of the downloaded file. ID which shall be included in a notification sent to the CSSF. It shall start with the entities identifier «-» value sequence of the file.
            errors:
              type: array
              items:
                type: object
                properties:
                  id:
                    type: string
                    pattern: '^CSSF-\d{3}$'
                    description: Identification code of the error
                  message:
                    type: string
                    description: Details on the error message
      required:
        - status
        - fileid
```

4.2.2 Feedback examples

The following JSON is an example of an accepted feedback:

```
{
    "status": "ACPT"
    "initial_file_key": "B99999999-1"
}
```

The following JSON is an example of rejected feedback

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

          }
    ]
}
```

4.2.3 Procedure in case of rejection

If the CSSF feedback contains an “RJCT” rejected status, professionals shall provide the CSSF with a new data file until the file is accepted (the feedback status is accepted “ACPT”).

5. File storage

The professional has to store on daily basis the last file accepted by the CSSF for the current day as well as the acceptance proof (feedback provided by the CSSF)

The CSSF will keep and store the feedback sent to the professional. In order to check the daily file integrity, the CSSF will generate and store several Hash for each of the stored files.

The mandatory retention period is 5 years according with the provisions of the Article 3 § 6 of the Law of the 12 November 2004 (coordinated version as of March 25, 2020) on the fight against money laundering and terrorism financing.

6. Various information

6.1 Environments

In addition to the production environment, the CSSF will set up a test environment. The CSSF requests to the professionals to perform tests during which they make the data file available on this environment, prior to before any transition to the production environment.

The files made available by the professional in the test environment must contain anonymized data.

6.2 Data file availability

Professionals shall ensure a sufficient level of availability in order to make available, to the CSSF, the file through its interface, at least once every 24 hours.

The file shall be available for download once the notification has been sent to the CSSF and until the end of the file download. The professional's platform can be unavailable the remaining time.

In the absence of a response by the CSSF, professionals must continue to notify the CSSF every 10 minutes as long as the file has not been downloaded by the CSSF.

6.3 Access request via MFT

The documents relating to technical details are transmitted to the professional by the CSSF in a secure way through its online Managed File Transfer ("MFT") system.

In order to obtain an identifier for connection to the online system, professionals shall send an email to the CSSF at registre.compte@cssf.lu with the following information:

- The identification number allocated by the CSSF ("Bxxx");
- Name of the entity;
- Surname and first name of the person responsible for email sending;

- Main contact email address[1];
- Secondary contact email address to which part of the identification information will be sent. [2]
- Contact phone number.
- If the professional delegates one or several obligations laid down in the Law of 25 March 2020, the name(s) of the provider(s) chosen to fulfil each obligation

6.4 Contact information at the CSSF

Any technical question should be submitted to: registre.compte@cssf.lu.

[1] *It is recommended to use a generic and lasting email address instead of the name address of an employee who might perform other duties over time, or even to leave the firm*

[2] *It is recommended to use a generic and lasting email address instead of the name address of an employee who might perform other duties over time, or even to leave the firm*