RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

DIRECTORATE-GENERAL FOR PUBLIC FINANCE
IT SYSTEMS SERVICE

SHARING ECONOMY

Encryption guide for Linux and Windows operating systems

Table of contents

1 Presentation....4
2 Proceed encryption....5
2.1 Asymmetric encryption....5
3 Tool used for Linux operating system....6
3.1 XML file compression....6
3.2 Import the public key....6
3.3 List the imported public key....7
3.4 Encrypt the xml file....7
4 Tool used for a Windows operating system....9
4.1 Compression of file....9
4.2 Installation of encryption software for Windows....10
4.3 Public key....11
4.4 Integration of the public key into encryption software....13
4.5 Encryption of the file....14

Monitoring of amendments

Release	Date	Author	Check	Subject
1.8	04/11/2020	DGFiP — SI-1C		Initialisation of version management.

1 Presentation

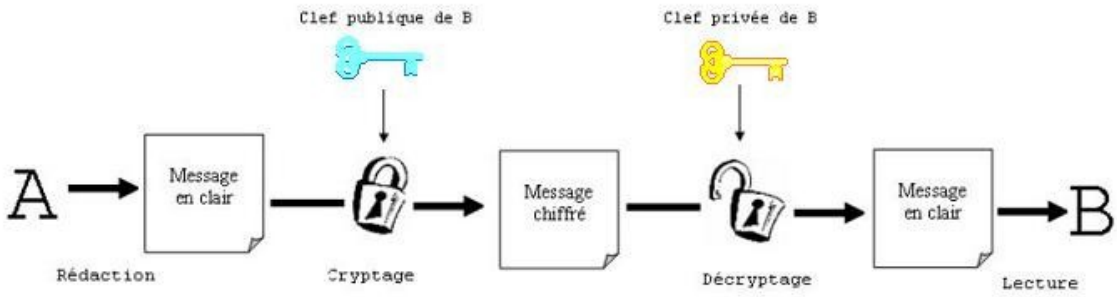
- This guide is intended for sharing economy platforms in order to help them encrypt the compressed Ecollab files.

- After presenting the asymmetric encryption process, the first part of this guidewill detail how to encrypt a file with GnuPG free software for Linux operating systems and the second part will detail the Gpg4win free software (Kleopatra component) for a Windows operating system.

2 Proceed encryption

2.1 Asymmetric encryption

- This process uses a two keys (bi-key) based on mathematical functions. Where one of these two keys has been used to encrypt a document, only the other key can be used to decipher it.
- Each user has a two-key set. One of these keys remains personal (the private key in yellow and known in French as « clé privée ») and the other key (the public key in blue and known in French as « clé publique ») is distributed to all his contacts. Encrypted documents with B's public key can only be quantified by him.
- The safe, which is closed by one key, can only be opened by the other key.



Cryptographie à clef publique : le message est chiffré avec la clef publique du destintaire et décrypté avec sa clef privée.

Schéma 2 : Chiffrement asymétrique

- In the following examples, the test key will be used.
- **files will be rejected if you fail to user the production key for files submitted on the production platform and the test key for files submitted on the pilot (i.e test) platform.**

3 Tool used for Linux operating system

- **Please note that the test protocol key is to be used in the examples given for the Linux part of the guide.**
- The GnuPG (GNU Privacy Guard) software, still known as GPG, is the GNU (formerly Unix's Free Competitive Project) for secure communications and data storage.
- It works in Linux, Unix, etc.
- This software is accessible in online command mode. A complementary tool is also available for more user-friendly use, with an easy-to-use user interface.
- To access a user interface, several software is available depending on the operating system you are using.
- Under Debian, the Nautilus and Seahorse tools are available.
- You can easily find the instructions for using these software via a search engine.

3.1 XML file compression

- Important: For this part of the process, the xml file has already been generated but is not compressed in gzip format. Otherwise, go directly to the encryption part.
- The file example is named as follows: *EcolLAB_2020_123456789_001_20200106102416.xml*
- Log in as a user with the rights to execute the following commands (e.g.: Root).
- To compress the xml file, execute the following command (replacing the name of the file): Gzip *EcolLAB_2020_123456789_001_20200106102416.xml*
- The file will be compressed in GZIP format.
- The result shall be: *EcolLAB_2020_123456789_001_20200106102416.**XML.GZ***

3.2 Import the public key

- As a first step, the public key made available on the professional portal by the DGFIP must be imported.
- In order to be able to import the public key, you must first submit the file containing it in the

folder of your choice.

- **It is important to place the xml file to be encrypted and the encryption key in the same folder.**

- The command to import the public key to your server is as follows:
  GPG --import ***ECOLLAB_TEST.asc***

```
dgfip:~$ gpg --import ECOLLAB_TEST.asc
gpg: clé BE6BA1B4: clé publique "DGFIP ECOLLAB PILOTE <collecte-ecocollab@dgfip.finances.gouv.fr>" importée
gpg:           Quantité totale traitée: 1
gpg:                       importée: 1   (RSA: 1)
```

- Disregard the error message: ‘GPG: no ultimate trust key was found”.
  for GPG: corresponds to GnuPG

- import: — allows you to import a key
  ECOLLAB_TEST.asc: name of the file containing the public key for the test phase (downloadable from: Https://www.impots.gouv.fr/portail/economie-collaborative-et-plateformes-numeriques under “Useful documentation”)

3.3 List the imported public key

- You can list the imported public key via the following command:
  GPG --list-key

```
dgfip:~$ gpg --list-key
/root/.gnupg/pubring.gpg
------------------------
pub   2048R/BE6BA1B4 2019-07-11 [expire: 2024-07-10]
uid                  DGFIP ECOLLAB PILOTE <collecte-ecocollab@dgfip.finances.gouv.fr>
sub   2048R/DFAFD342 2019-07-11 [expire: 2024-07-10]
```

- It is important to note the code that will allow this key to be used here “BE6BA1B4”.

3.4 Encrypt the xml file

- Execute the following command to encrypt the compressed xml file (replace file name):
  GPG -e -r BE6BA1B4 *EcolLAB_ 2020_123456789_00120200106102416.xml.gz*

  EcolLAB_2020_123456789_00120200106102416.xml.gz: *name of file to be encrypted*
  BE6BA1B4: DGFIP public keyidentifier for the test phase

DGFiP: ~ $GPG -e -r BE6BA1B4 ECOLLAB_2020_123456789_001_20200106102416.xml.gz

```
pub  2048R:DFAFD342 2019-07-11 DGFIP ECOLLAB PILOTE <collecte-ecocollab@dgfip.finances.gouv.fr>
 Empreinte de la clé principale: 62E1 B7CA 4F56 B75B 74BD 393C 5911 6849 BE6B A1B4
       Empreinte de la sous-clé: 754A 5CA7 23B3 1584 6C81 01DA E0BA B5AF DFAF D342
```

- Answer « o » (in French) or « y » (in English) to the question asked by the system: “Using this key still? (y/N)’:

```
Il n'est PAS certain que la clé appartient à la personne nomée dans
le nom d'utilisateur. Si vous savez *vraiment* ce que vous faites,
vous pouvez répondre oui à la prochaine question.

Utiliser cette clé quand même ? (o/N)
```

- The extension “.gpg” has been added to your compressed and encrypted xml file (e.g.: *EcolLAB_2020_123456789_00120200106102416.XML.GZ**.GPG***).

- The file can be uploaded on your workspace (professional account on the impots.gouv.fr website), in the “Sharing Economy” section (known in French as « Économie collaborative »).

4 Tool used for a Windows operating system

- **Please note that the production protocol key is to be used in the examples given for the Windows part of the guide.**
- Gpg4win (Kleopatra component) is encryption software for files and e-mails operating under most versions of Microsoft Windows. It uses GNU Privacy Guard (GPG) asymmetric encryption system to encrypt and sign.

- For information, you need the**public** key to encrypt your data (a step is dedicated to it).

4.1 Compression of file

- It is reminded that files must be **compressed** before being encrypted. Failing to do so will result in the rejection of the file submitted. The software recommended by the DGFiP is 7zip, the expected format is **GZIP**.

- The software can be downloaded here:
  https://www.7-zip.org/

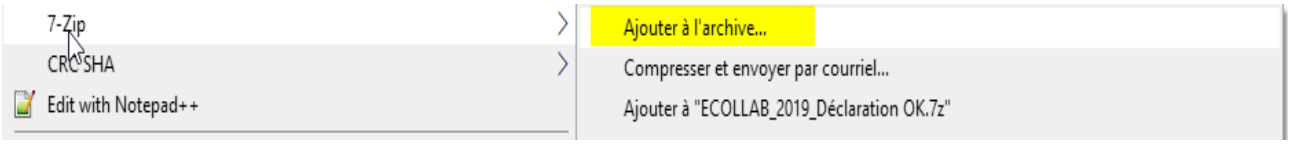
7-Zip is a file archiver with a high compression ratio.

Download 7-Zip 19.00 (2019-02-21) for Windows:

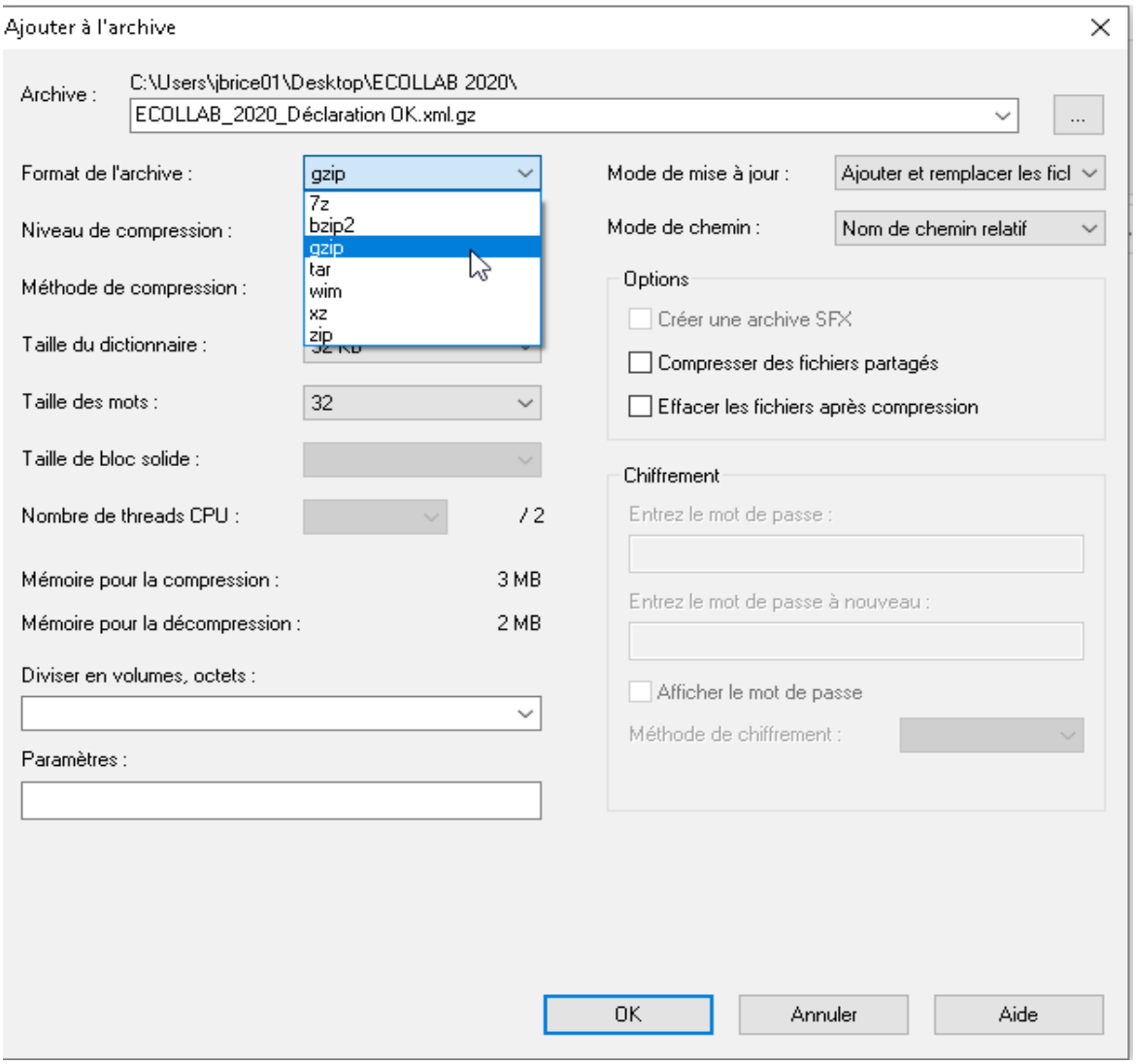
Link	Type	Windows	Size
Download	.exe	32-bit x86	1 MB
Download	.exe	64-bit x64	1 MB

- The 7-zip software is downloadedand installed on ther computer.

- To compress the file, make a right-click on it, scroll down menu 7-Zip and click on “Add to the archive”:



- The format of the GZIP archive must then be specified as follows:

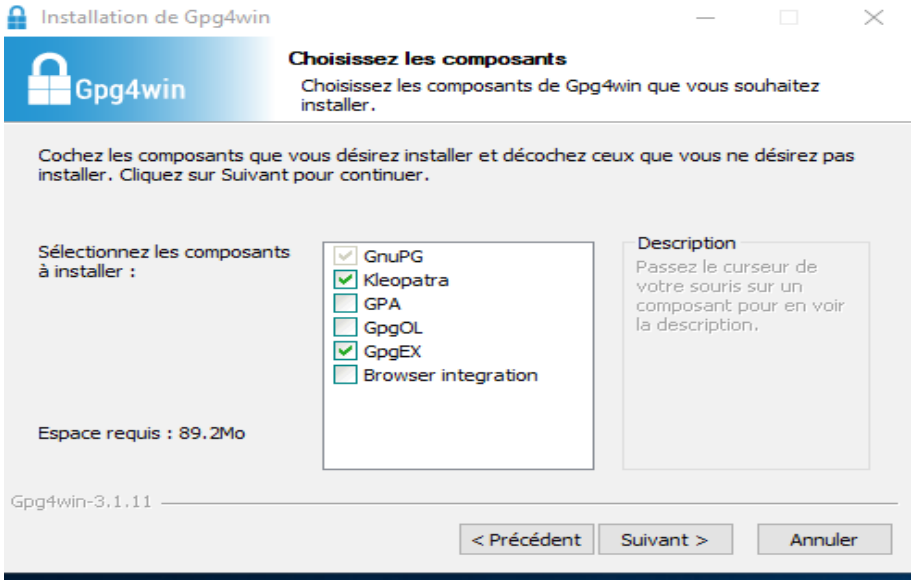


- By clicking on OK, your file will be compressed and will be in your current file.
- You can then go to the encryption step of the file.
- **Any uncompressed or unencrypted declaration file automatically leads to its rejection**.

4.2 Installation of encryption software for Windows

- Download the GPG4WIN software from the officiel site: https://www.gpg4win.org/download.html

- Install the software on your computer. Select components to be installed (Kleopatra and GpgEx) as follows:

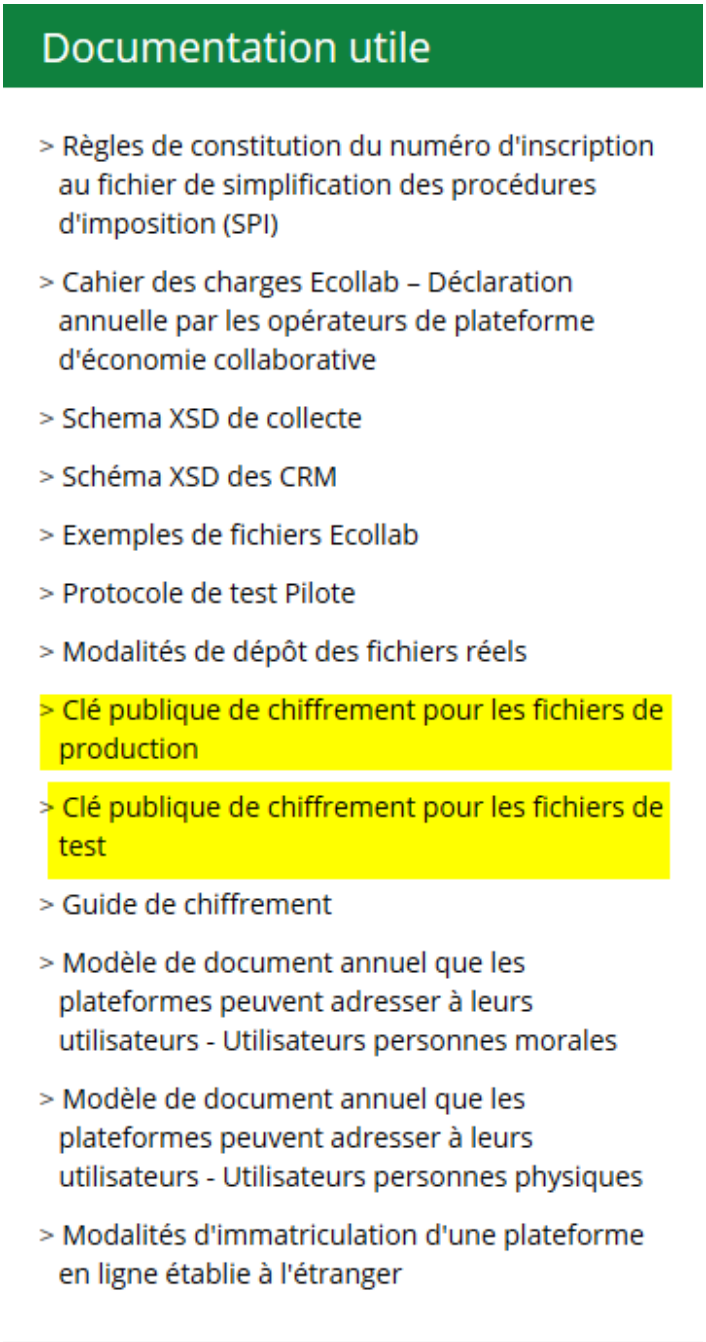


4.3 Public key

- The public key is available at: https://www.impots.gouv.fr/portail/economie-collaborative-et-plateformes-numeriques

- Download the public key available on the right of the page depending on your need, for production files (« Clé public de chiffrement pour les fichiers de production ») or for test

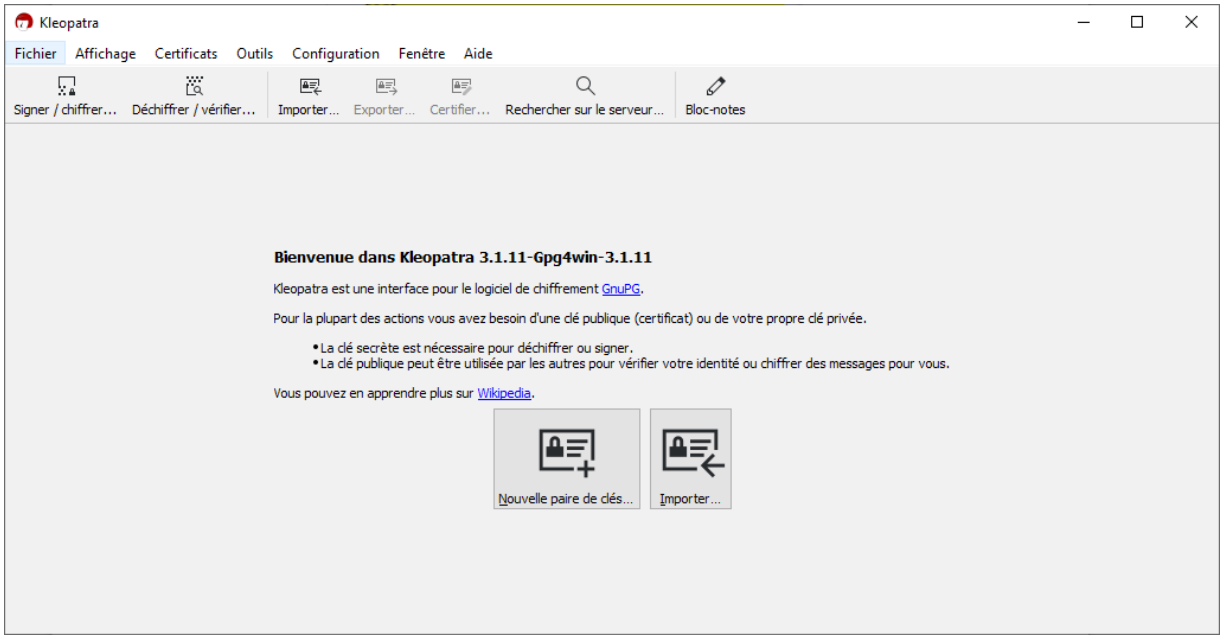
files (« Clé publique de chiffrement pour les fichiers de test ») :



- Then uncompressed the archive in the folder of your choice. The public key has the extension “.**ASC”** (e.g.: For the public key for encryption of production files: DGFIP_ECOLLAB_PROD.ASC).

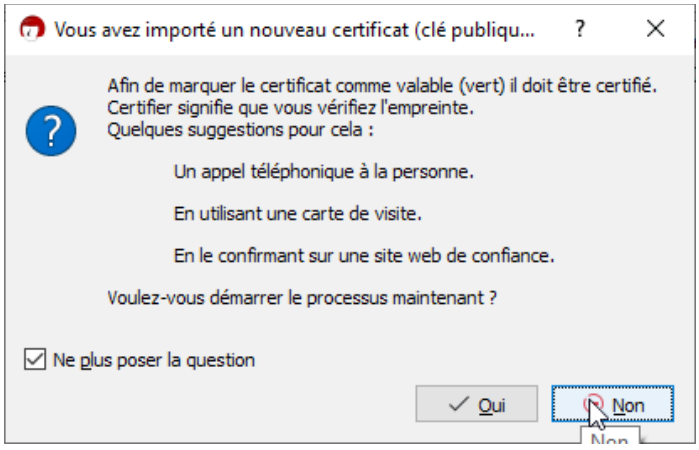
4.4 Integration of the public key into encryption software

- Launch the Kleopatra application (by default the icon is on your office). A window is displayed:

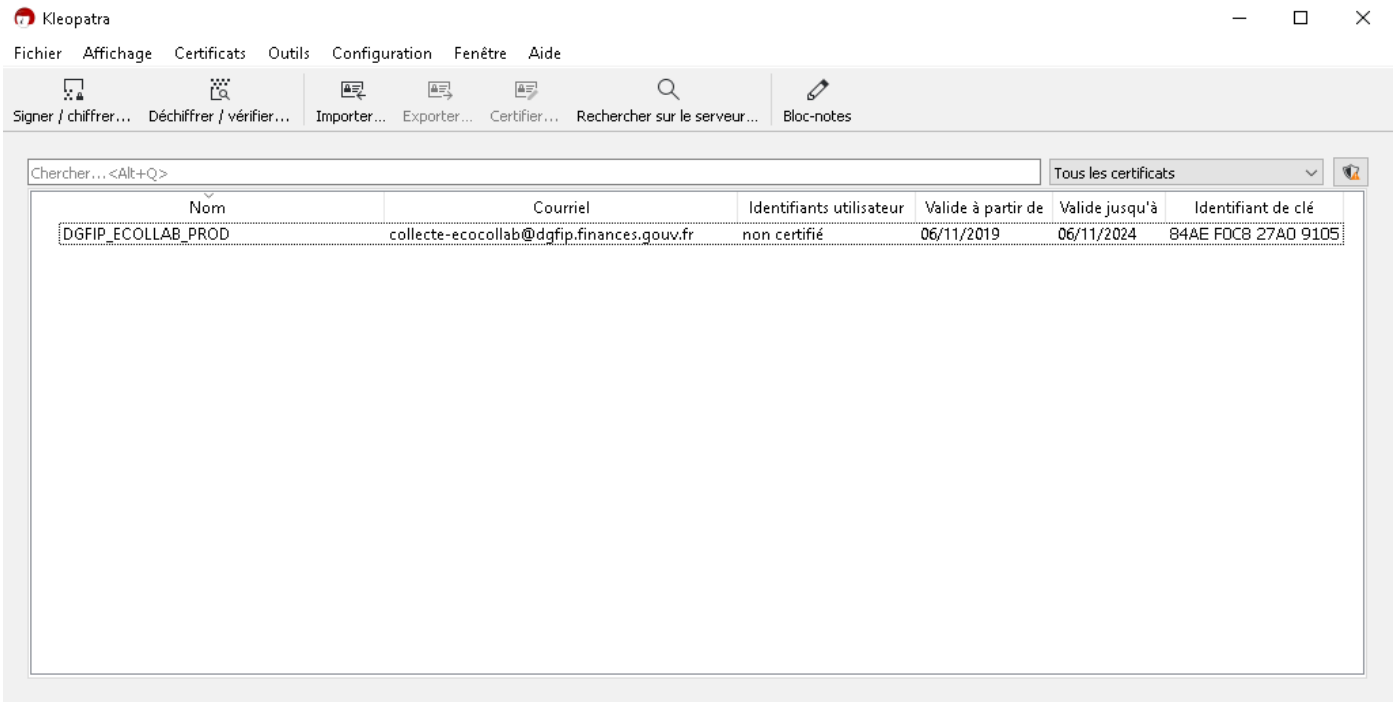


- To import the public key, click on " **Importer"**. A "Select Certificate File"window is displayed. Position yourself at the location of your key and then open the file.

- A window on the certification of the key is displayed. As this process is not necessary, tick the box "Don't ask me again" and click on no:

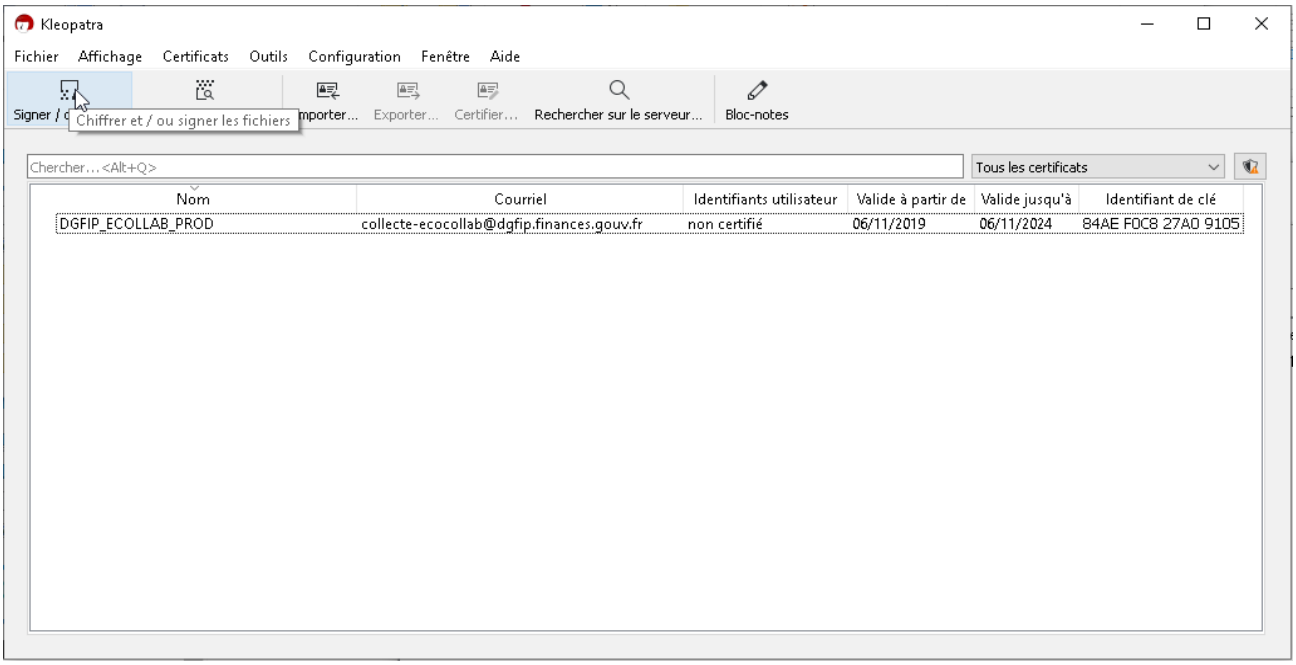


- The public key has been correctly imported the following screen should be displayed :

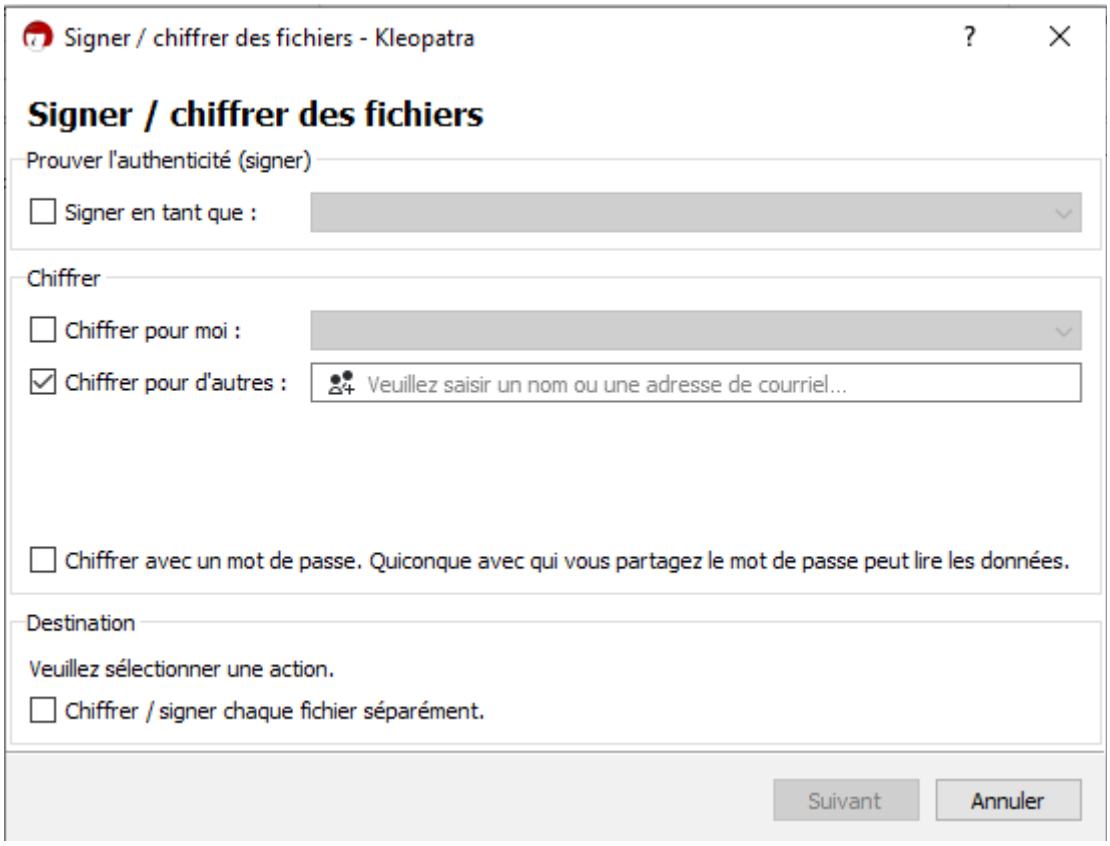


4.5 Encryption of the file

- To encrypt the file, either simply move the file to the application or click on “ Sign/encrypt”and select the file:

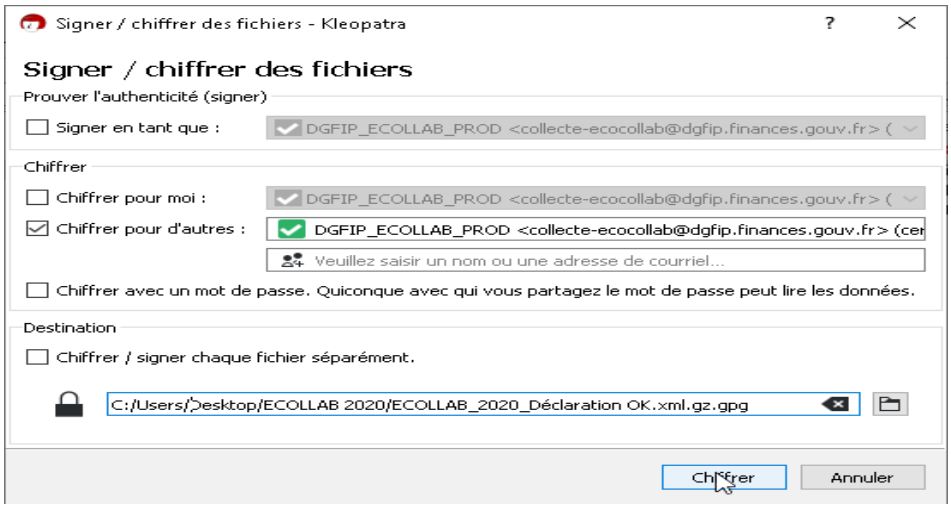


- A window “Signing/Number of files” is displayed:

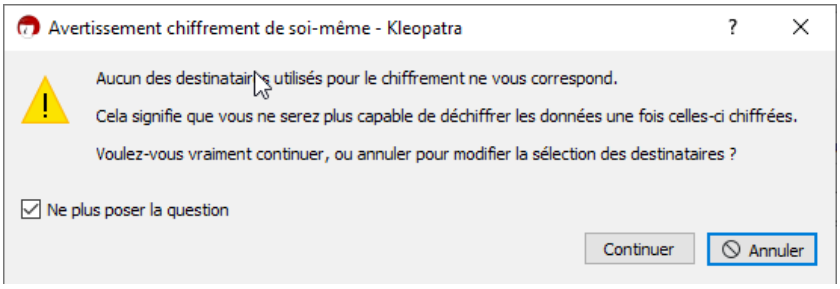


- Tick **only** the option “Figures for others”. The other boxes must be unticked.

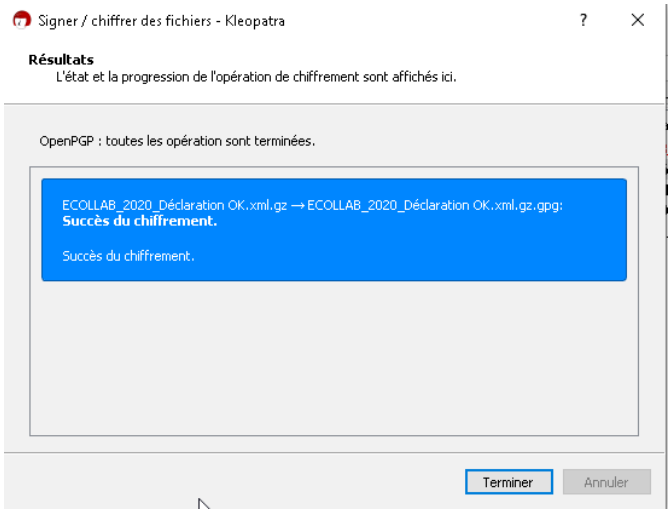
- Select the public key “DGFIP ECOLLAB PROD”. To do so, type ‘ d’ in the ‘Encrypt for others’ box. The drop-down menu displays the DGFIP public key to be selected.



- Click on the ‘Figurate’ button. A warning window is displayed:



- Tick « Don't ask me again » and click on « Continue »
- Your file is encrypted. A confirmation window displays the result:



- Click on the “Finish” button.
- The file is now encrypted in the same folder as the original file, with the same name but with the extension “.gpg”. It can be uploaded on your workspace in the “Collaborative Economy” section.