Ministère de l'Action et des Comptes Publics

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES
SERVICE DES SYSTÈMES D'INFORMATION

ÉCONOMIE COLLABORATIVE

Guide de chiffrement pour les systèmes d'exploitation Linux et Windows

Table des matières

Suivi des modifications

Version	Date	Rédaction	Vérification	Objet
1.8	04/11/2020	DGFIP – Bureau SI-C		Initialisation de la gestion de version.
1.9	18/11/2021	DGFIP – Bureau BSI4		Modification du millesime (2020 devient 2021)

1 Présentation

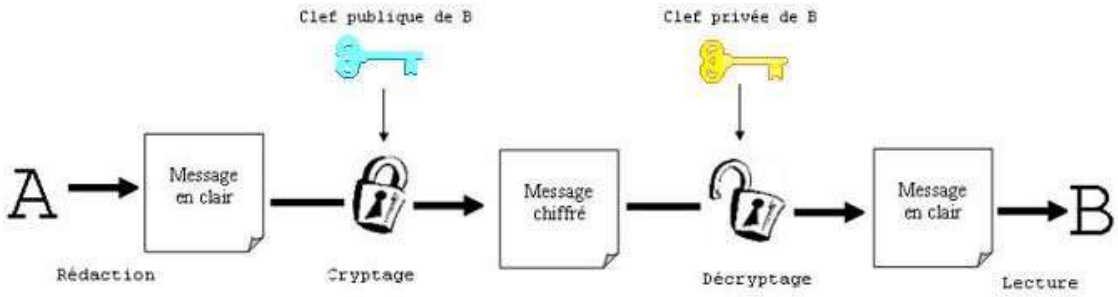
- Ce guide est destiné aux entreprises de l’économie collaborative afin de les aider à chiffrer les fichiers compressés des déclarations Ecollab.

- Après avoir présenté le procédé de chiffrement asymétrique, la première partie de ce guide vous indiquera comment chiffrer un fichier avec le logiciel libre GnuPg pour les systèmes d’exploitation Linux et la deuxième partie vous présentera le logiciel libre Gpg4win (composant Kleopatra) pour un système d’exploitation Windows.

2 Procédé de chiffrement

2.1 Le chiffrement asymétrique

- Ce procédé utilise un couple de clés (bi-clé) basé sur des fonctions mathématiques. Lorsqu'une de ces deux clés a servi à chiffrer un document, seule l'autre clé permet de le déchiffrer.
- Chaque utilisateur possède une bi-clé. Une de ces clés reste personnelle (la clé privée figurée en jaune) et l'autre clé (la clé publique figurée en bleu), est diffusée à tous ses contacts. Les documents chiffrés avec la clé publique de B ne peuvent être chiffrés que par lui.
- Le coffre-fort qui est fermé par une clé, ne peut être ouvert que par l'autre clé.



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

Schéma 2 : Chiffrement asymétrique

- Dans les exemples qui vont suivre, nous utiliserons la clé de test.
- **Sous peine de voir vos déclarations rejetées, vous devez utiliser la clé de production pour des déclarations à destination de la plateforme de production et la clé de test pour la plateforme pilote.**

3 Outil utilisé pour un système d'exploitation Linux

- **Attention, nous utiliserons, dans les exemples, pour cette partie Linux du guide : la clé de chiffrement du protocole de test.**
- Le logiciel GnuPG (GNU Privacy Guard), encore appelé GPG, est l'utilitaire GNU (ancien projet libre concurrent d'Unix) permettant des communications et le stockage de données sécurisées.
- Il fonctionne dans les environnements Linux, Unix...
- Ce logiciel est accessible en mode ligne de commande. Un outil complémentaire est également disponible pour une utilisation plus conviviale, avec une interface utilisateur facile d'emploi.
- Pour accéder à une interface utilisateur, plusieurs logiciels sont disponibles selon le système d'exploitation que vous utilisez.
- Sous Debian, les outils Nautilus et Seahorse sont disponibles.
- Vous trouverez facilement les modes d'emploi de ces logiciels via un moteur de recherche.

3.1 Compression du fichier XML

- Point important : Pour cette étape du processus, le fichier xml a déjà été généré mais n'est pas compressé au format gzip. Dans le cas contraire, passez directement à l'étape de chiffrement.
- Nous prendrons comme exemple le fichier suivant :
  ECOLLAB_2021_123456789_001_20210106102416.xml
- Se connecter avec un utilisateur ayant les droits permettant d'exécuter les commandes ci-dessous (ex : root).
- Pour compresser le fichier xml, exécuter la commande suivante (en remplaçant le nom du fichier):
  gzip *ECOLLAB_2021_123456789_001_20210106102416.xml*
- Le fichier sera compressé au format GZIP.
- Le résultat sera : *ECOLLAB_2021_123456789_001_20210106102416.**xml.gz***

3.2 Importer la clé publique

- Dans un premier temps, il faut importer la clé publique mise à disposition sur le portail professionnel par la DGFIP.
- Pour pouvoir importer la clé publique, vous devez au préalable déposer le fichier la contenant dans le répertoire de votre choix.
- **Il est important de placer le fichier xml à chiffrer ainsi que la clé de chiffrement dans le même répertoire.**
- La commande permettant d'importer la clé publique sur votre serveur est la suivante :
  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)
```

- Ne pas tenir compte du message d'erreur : « gpg: aucune clé de confiance ultime n'a été trouvée ».
  gpg : correspond à GnuPG
- import : permet d'importer une clé
  ECOLLAB_TEST.asc: nom du fichier contenant la clé publique pour la phase de test (téléchargeable à l'adresse suivante : https://www.impots.gouv.fr/portail/economie-collaborative-et-plateformes-numeriques dans la rubrique « Documentation utile »)

3.3 Lister la clé publique importée

- Vous pouvez lister la clé publique importée via la commande suivante :
  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]
```

- Il est important de noter le code qui permettra d'utiliser cette clé, ici « BE6BA1B4 ».

3.4 Chiffrer le fichier xml

- Exécuter la commande suivante pour chiffrer le fichier xml compressé (remplacer le nom du fichier) :
  gpg -e -r BE6BA1B4 *ECOLLAB_2021_123456789_001_20210106102416.xml.gz*

  ECOLLAB_2021_123456789_001_20210106102416.xml.gz : nom du fichier à chiffrer
  BE6BA1B4 : identifiant de la clé publique DGFIP pour la phase de test

dgfip:~$ gpg -e -r BE6BA1B4 ECOLLAB_2021_123456789_001_20210106102416.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
```

- Répondre « o » à la question posée par le système : « Utiliser cette clé quand même ? (o/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)
```

- L’extension « .gpg» a été ajoutée à votre fichier xml compressé et chiffré (ex : *ECOLLAB_2021_123456789_001_20210106102416.xml.gz****.gpg***).

- Vous pouvez le déposer sur votre espace professionnel dans la rubrique « Économie Collaborative ».

4 Outil utilisé pour un système d'exploitation Windows

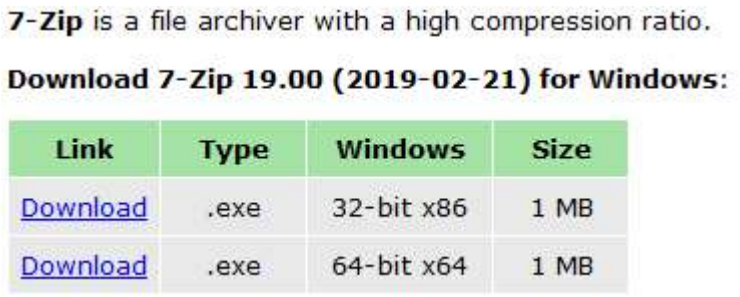
- **Attention, nous utiliserons, dans les exemples, pour cette partie Windows du guide : la clé de chiffrement de production.**
- Gpg4win (composant Kleopatra) est un logiciel de chiffrement de fichiers et de méls fonctionnant sous la plupart des versions de Microsoft Windows. Il utilise le système de chiffrement asymétrique de GNU Privacy Guard (GPG) pour chiffrer et signer.

- Pour information, vous avez besoin de la clé **publique** pour chiffrer vos données (une étape y est consacrée).

4.1 Compression du fichier

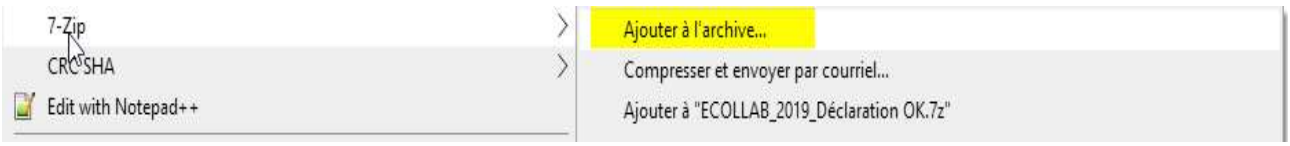
- Nous vous rappelons que les fichiers de déclarations doivent être **compressés** avant d'être **chiffrés** sous peine d'être rejetés. Le logiciel préconisé par la DGFIP est **7zip**, le format attendu est **GZIP**.

- Vous pouvez télécharger le logiciel ici :
  https://www.7-zip.org/

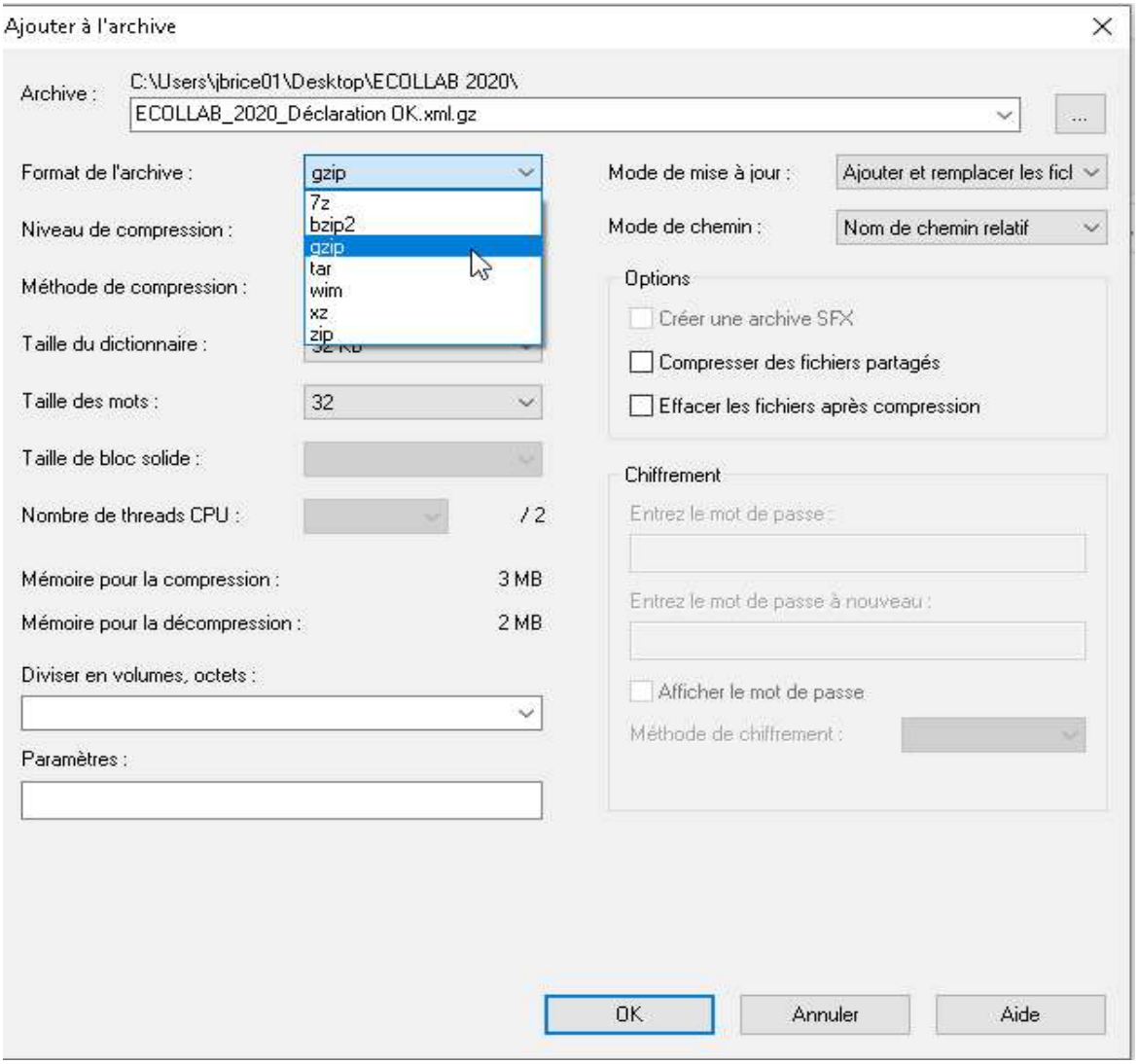


- Le logiciel 7-zip est téléchargé et installé sur votre ordinateur.

- Pour compresser votre déclaration, il suffit de faire un clic droit dessus, de dérouler le menu 7-Zip et cliquer sur « Ajouter à l'archive » :



- Vous devez ensuite spécifier le format de l’archive en GZIP comme ceci :



- En cliquant sur OK, votre déclaration sera compressée et se trouvera dans votre dossier courant.

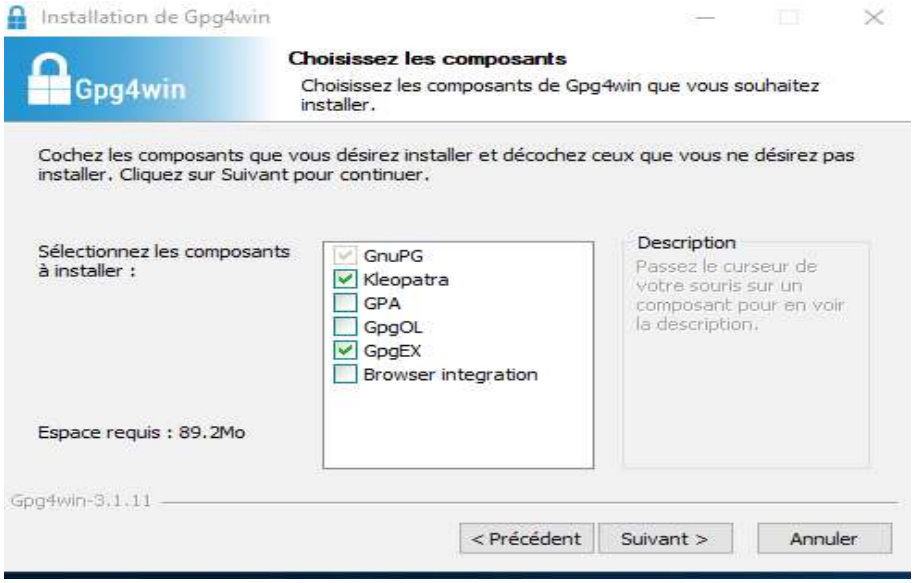
- Vous pouvez ensuite passer à l’étape de chiffrement de la déclaration.

- **Tout fichier de déclaration non compressé ou non chiffré entraîne automatiquement son rejet**.

4.2 Installation du logiciel de chiffrement pour Windows

- Télécharger le logiciel GPG4WIN sur le site officiel : https://www.gpg4win.org/download.html

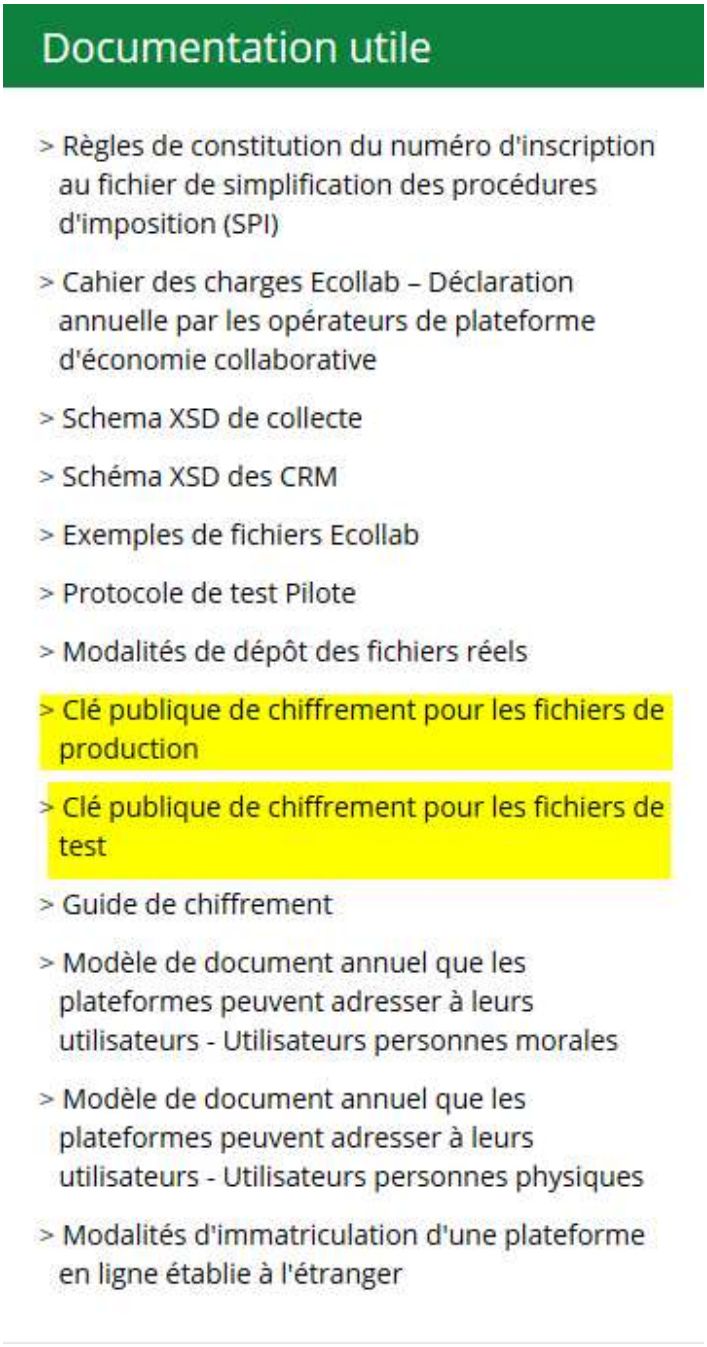
- Installer le logiciel sur votre ordinateur . Sélectionner ses composants à installer (Kleopatra et GpgEx) comme ci-dessous :



4.3 Clé publique

- La clé publique est disponible à l'adresse suivante : https://www.impots.gouv.fr/portail/economie-collaborative-et-plateformes-numeriques

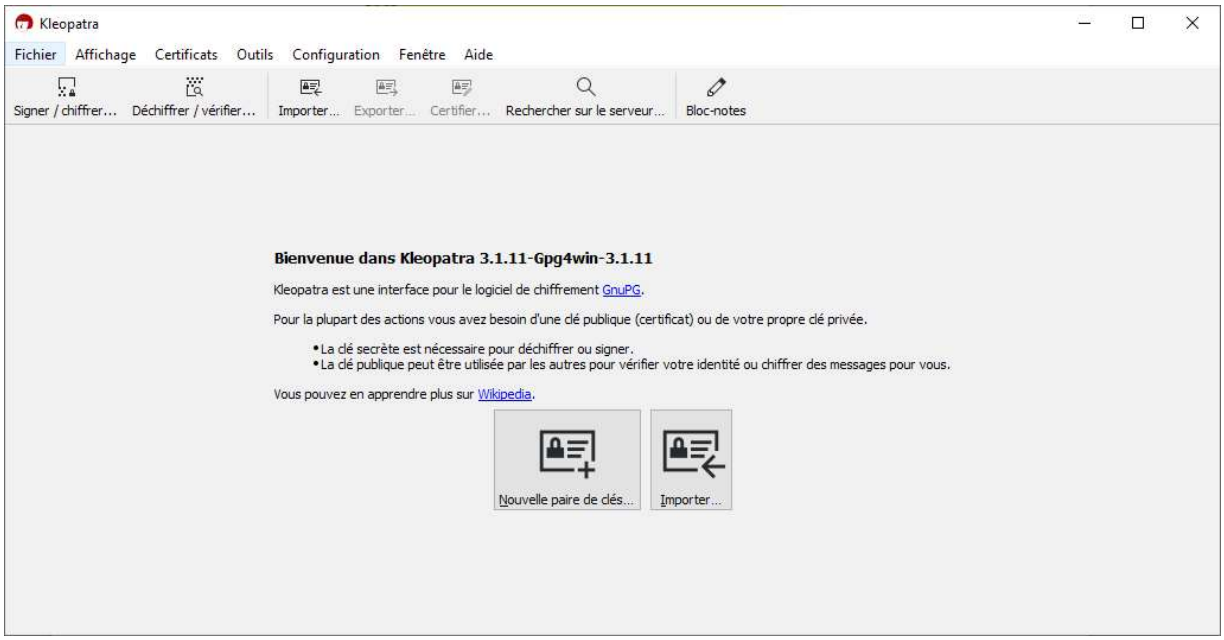
- Télécharger la clé publique disponible à droite de la page en fonction de votre besoin, pour les fichiers de production ou pour les fichiers de tests :



- Décompresser ensuite l’archive dans le répertoire de votre choix. La clé publique a pour extension « **.asc »** (ex. : pour la clé publique de chiffrement des fichiers de production: DGFIP_ECOLLAB_PROD.asc).

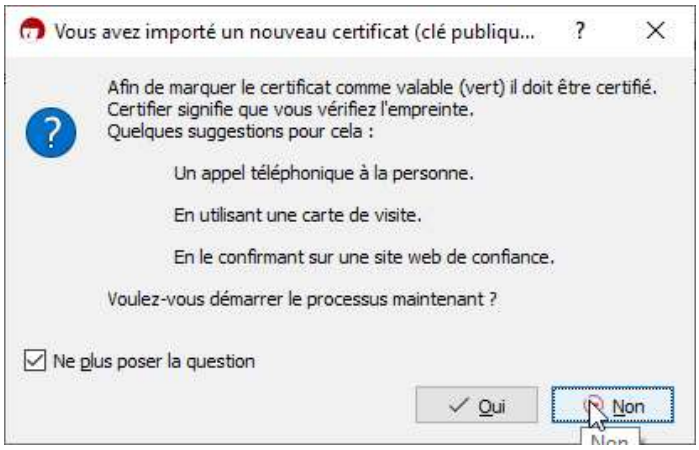
4.4 Intégration de la clé publique au logiciel de chiffrement

- Lancer l'application Kleopatra (par défaut l'icône se trouve sur votre bureau). Une fenêtre s'affiche :

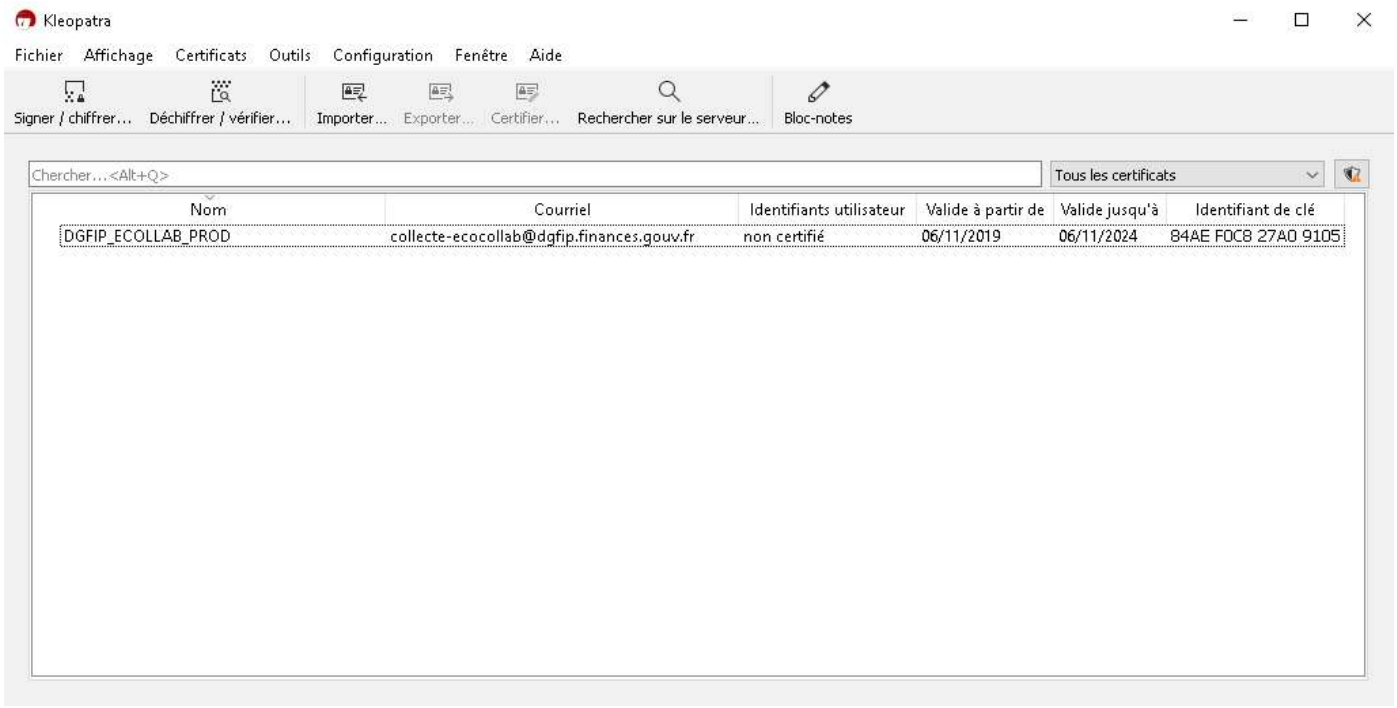


- Pour importer la clé publique, cliquer sur « **Importer »**. Une fenêtre « Sélectionner un fichier de certificat » s'affiche. Se positionner à l'emplacement de votre clé puis ouvrir le fichier.

- Une fenêtre concernant la certification de la clé s'affiche. Ce processus n'étant pas nécessaire, cocher la case « Ne plus poser la question » et cliquer sur non :

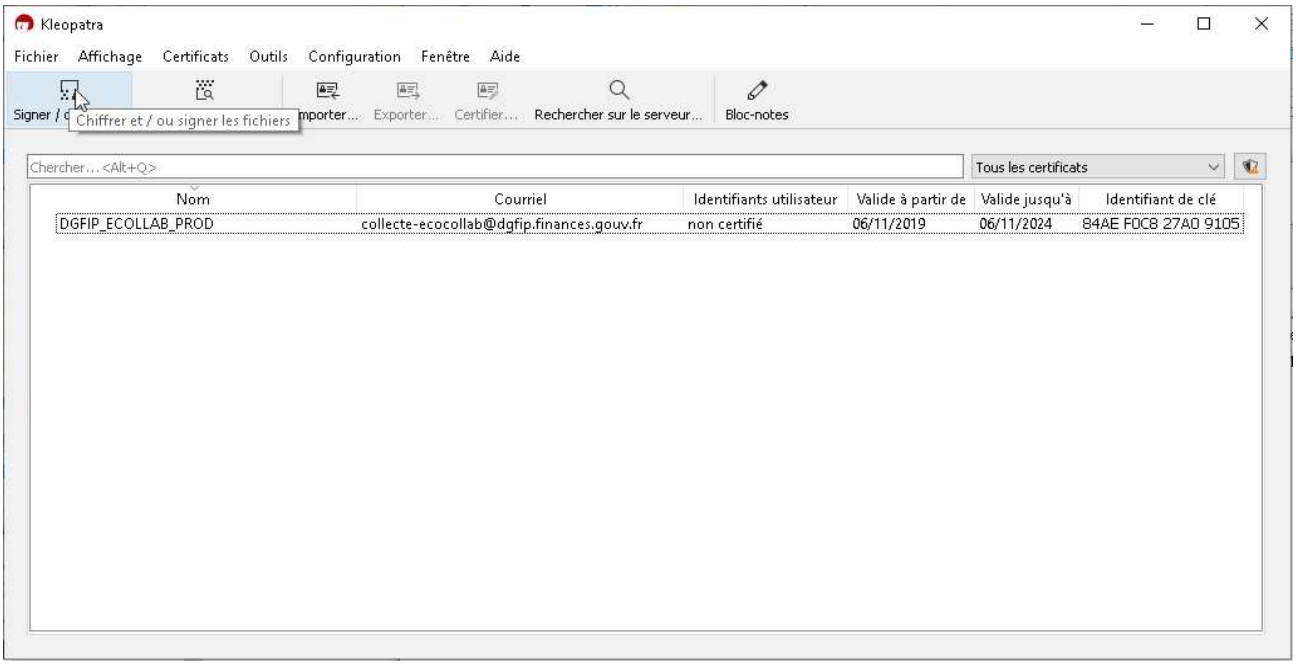


- La clé publique a été correctement importée et vous devriez avoir cet affichage :

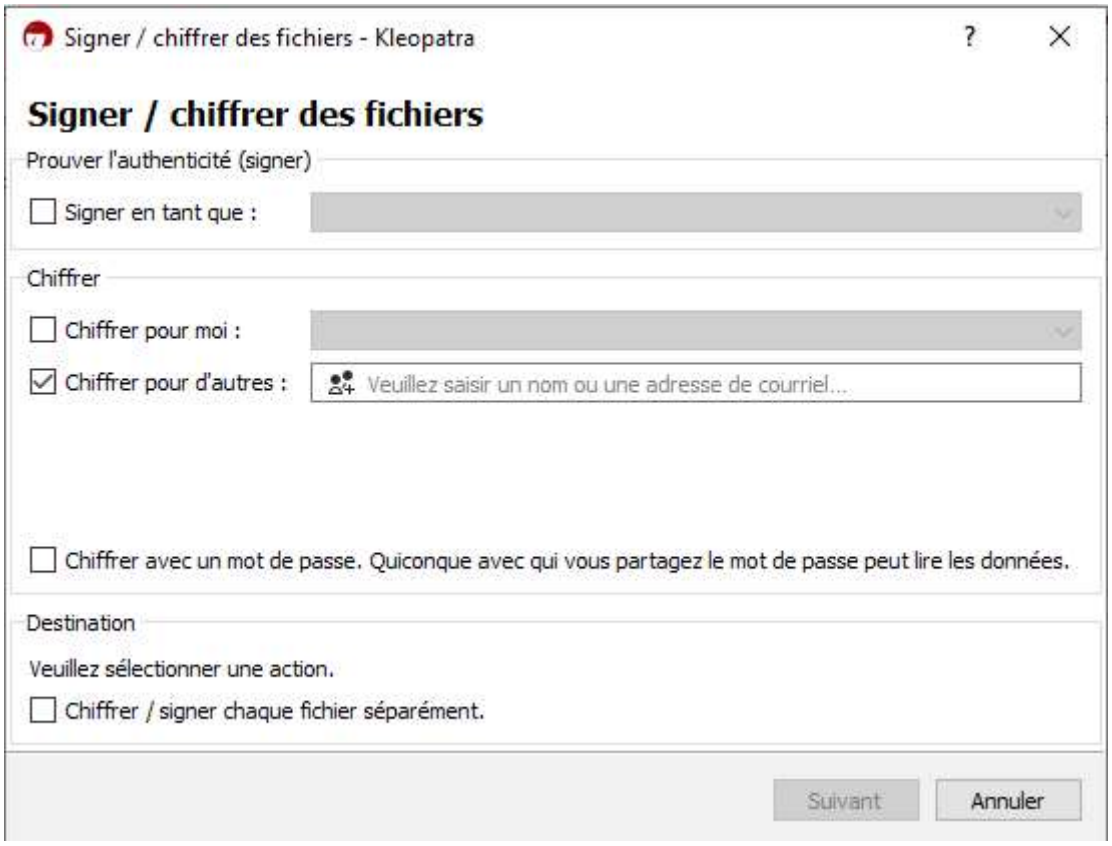


4.5 Chiffrement de la déclaration

- Pour chiffrer le fichier de votre déclaration, vous pouvez soit simplement glisser-déposer le fichier sur l'application, soit cliquer sur « Signer / chiffrer » et sélectionner votre fichier :

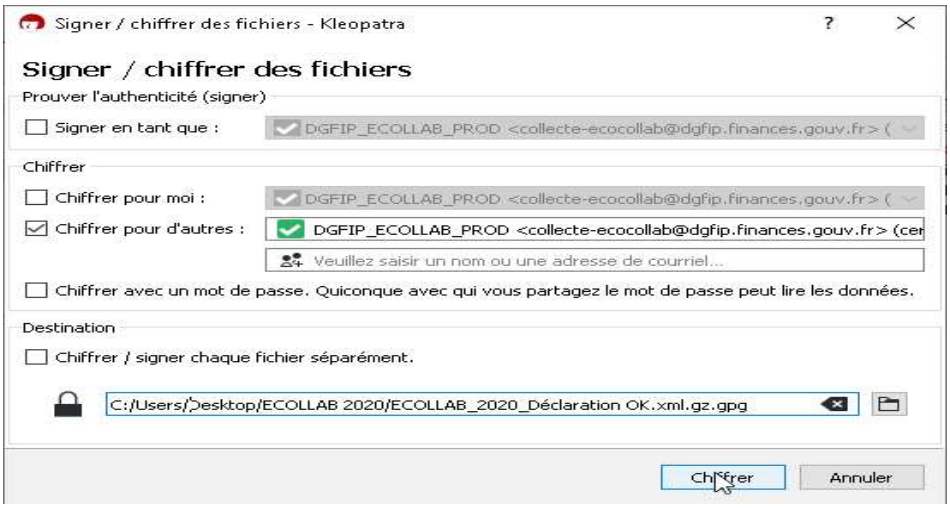


- Une fenêtre « Signer / chiffrer des fichiers » s'affiche :

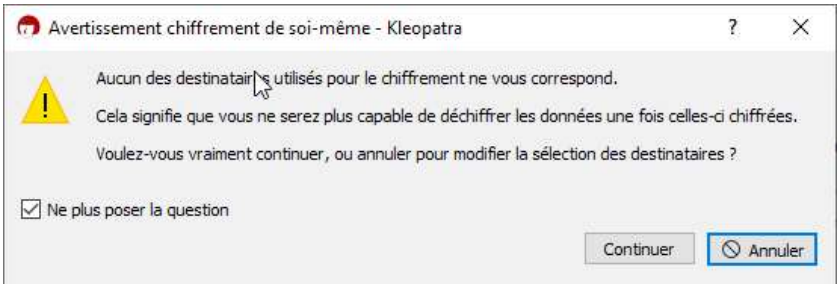


- Cocher **uniquement** l'option « Chiffrer pour d'autres ». Les autres cases doivent être décochées.

- Indiquer la clé publique « DGFIP ECOLLAB PROD». Pour cela, taper « d » dans le cadre « Chiffrer pour d'autres ». Le menu déroulant affiche la clé publique DGFIP et vous devez la sélectionner.

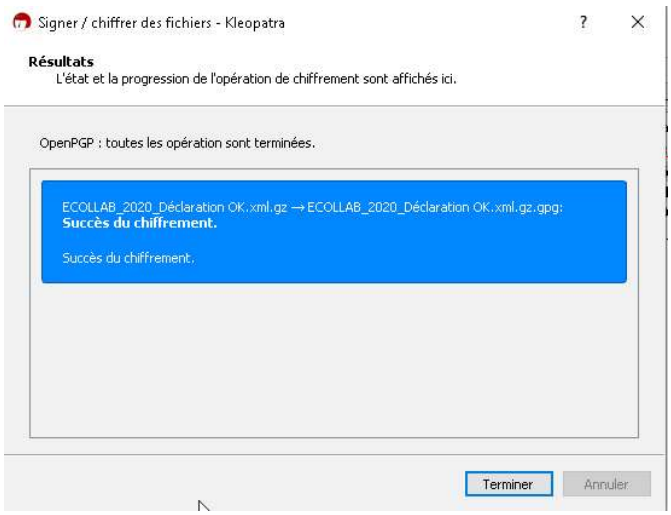


- Cliquer sur le bouton « Chiffrer ». Une fenêtre d'avertissement s'affiche :



- Cocher « Ne plus poser la question » et cliquer sur « Continuer »

- Votre fichier est chiffré. Une fenêtre de confirmation affiche le résultat :



- Cliquer sur le bouton « Terminer ».

- Votre fichier est à présent chiffré dans le même répertoire que le fichier d'origine, avec le même nom mais avec l'extension « .gpg ». Vous pouvez le déposer sur votre espace professionnel dans la rubrique « Économie Collaborative ».