



Liberté • Égalité • Fraternité

RÉPUBLIQUE FRANÇAISE

Ministère de l'Action et des Comptes Publics

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES
SERVICE DES SYSTÈMES D'INFORMATION

TELE-TD

Service Tiers-déclarants

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

Table des matières

1	Présentation.....	4
2	Procédé de chiffrement.....	5
2.1	Le chiffrement asymétrique.....	5
3	Outil utilisé pour un système d'exploitation Linux.....	6
3.1	Compression du fichier.....	6
3.2	Importer la clé publique.....	7
3.3	Lister la clé publique importée.....	8
3.4	Chiffrer le fichier xml.....	8
4	Outil utilisé pour un système d'exploitation Windows.....	10
4.1	Compression du fichier.....	10
4.2	Installation du logiciel de chiffrement pour Windows.....	11
4.3	Clé publique.....	12
4.4	Intégration de la clé publique au logiciel de chiffrement.....	13
4.5	Chiffrement de la déclaration.....	15
5	Outil utilisé pour un système d'exploitation MAC.....	19
5.1	Installation de GNUPG.....	19

Suivi des modifications

Version	Date	Rédaction	Vérification	Objet
1.0	03/06/2021	DGFIP – Bureau SI-C		Initialisation de la gestion de version.
1.1	13/10/2021	DGFIP – Bureau BSI4		Mise à jour avec exemple pour le projet TELETD
1.2	10/11/2021	DGFIP- Bureau GF1A		Mise à jour des liens vers la page tiers déclarant du site impots.gouv.fr
1.3	10/11/2023	DGFIP – Bureau BSI4		Ajout de la partie 5. Chiffement sur Mac Modification des références de la clé dans les copies d'écran

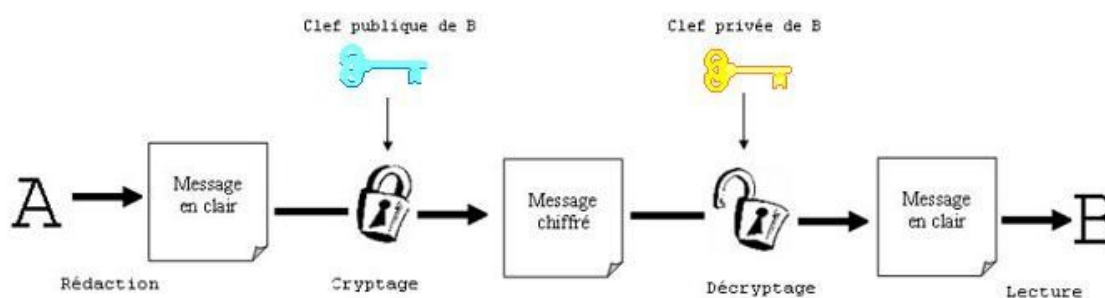
1 Présentation

- Ce guide est destiné aux partenaires de l'application TELE-TD afin de les aider à chiffrer les fichiers compressés des déclarations :
 - Auto-certification L102AG : fichier xml
 - FATCA, CRS/DAC2, DPI-DAC7 : fichier xml
 - TD/bilatéral : fichier txt
- 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, la deuxième partie vous présentera le logiciel libre Gpg4win (composant Kleopatra) pour un système d'exploitation Windows et la troisième partie détaillera les modalités de chiffrement sur Mac.

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 destinataire 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

- Point important : Pour cette étape du processus, le fichier 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 les fichiers suivants :
 - Auto-certification
`AUTO-CERTIFICATION_L.102AG_2019_345678912_999_20201212.xml`
 - FATCA et CRS/DAC2
`EAI_2020_123456789_001_20200106102416.xml`
 - TD/bilatéral
`DMET_2020_123456789_001_20200106102416.txt`
- 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 <nom_fichier>`
 - Auto-certification
`gzip AUTO-CERTIFICATION_L.102AG_2019_345678912_999_20201212.xml`
 - FATCA et CRS/DAC2

- gzip `EAI_2020_123456789_001_20200106102416.xml`
- TD/bilatéral
- gzip `DMET_2020_123456789_001_20200106102416.txt`

- Le fichier sera compressé au format GZIP.
- Le résultat sera :
 - Auto-certification
`AUTO-CERTIFICATION_L.102AG_2019_345678912_999_20201212.xml.gz`
 - FATCA et CRS/DAC2
`EAI_2020_123456789_001_20200106102416.xml.gz`
 - TD/bilatéral
`DMET_2020_123456789_001_20200106102416.txt.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 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 `DGFIP_TIERSDECLARANTS_TEST.asc`

```
[root] # gpg --import /home/DGFIP_TIERSDECLARANTS_TEST.asc
gpg: clef B2FCE419 : clef publique « DGFIP_TIERSDECLARANTS_TEST <bureau.si-part-
teletd@dgfip.finances.gouv.fr> » importée
gpg:      Quantité totale traitée : 1
gpg:      importées : 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
`DGFIP_TIERSDECLARANTS_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/tiers-declarants](https://www.impots.gouv.fr/portail/tiers-declarants) 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

```
[root] # gpg --list-key
/root/.gnupg/pubring.gpg
-----
```

```
pub 2048R/B2FCE419 2023-08-30 [expire : 2028-08-28]
uid DGFIP_TIERSDECLARANTS_TEST <bureau.si-part-teletd@dgfip.finances.gouv.fr>
sub 2048R/150E98B5 2023-08-30 [expire : 2028-08-28]
```

- Il est important de noter le code qui permettra d'utiliser cette clé, ici « B2FCE419 ».

3.4 Chiffrer le fichier xml

- Exécuter la commande suivante pour chiffrer le fichier xml compressé (remplacer le nom du fichier) :
gpg -e -r B2FCE419 <nom_fichier>

<nom_fichier> : nom du fichier à chiffrer

B2FCE419: identifiant de la clé publique DGFIP pour la phase de test

```
dgfip:~$ gpg -e -r B2FCE419 AUTO-CERTIFICATION_L.102AG_2019_456789123_000_20200309.xml.gz
```

```
[root] # gpg -e -r B2FCE419 AUTO-CERTIFICATION_L.102AG_2019_456789123_000_20200309.xml.gz
gpg: 150E98B5 : aucune assurance que la clef appartienne vraiment à l'utilisateur nommé.

pub 2048R/150E98B5 2023-08-30 DGFIP_TIERSDECLARANTS_TEST <bureau.si-part-teletd@dgfip.finances.gouv.fr>
Empreinte clef princip. : E712 5CD4 04D1 60E6 C1C7 7329 9182 BFA4 B2FC E419
Empreinte de sous-clef : E504 79B7 1CE9 6F94 4D8C 8BFC A4C4 5EF6 150E 98B5
```

- Répondre « o » à la question posée par le système : « Utiliser cette clé quand même ? (o/N) » :
- L'extension « .gpg » a été ajoutée à votre fichier compressé et chiffré

```
dans l'identité. Si vous savez *vraiment* ce que vous
faites, vous pouvez répondre oui à la prochaine question.
```

```
Faut-il quand même utiliser cette clef ? (o/N) █
```

- Auto-certification
AUTO-CERTIFICATION_L.102AG_2019_345678912_999_20201212.xml.gz.gpg
- FATCA et CRS/DAC2
EAI_2020_123456789_001_20200106102416.xml.gz.gpg

- TD/bilatéral
- **DMET_2020_123456789_001_20200106102416.txt.gz.gpg**
-
- Vous pouvez le déposer sur votre espace professionnel dans la rubrique « **Service Tiers-Déclarant** ».

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

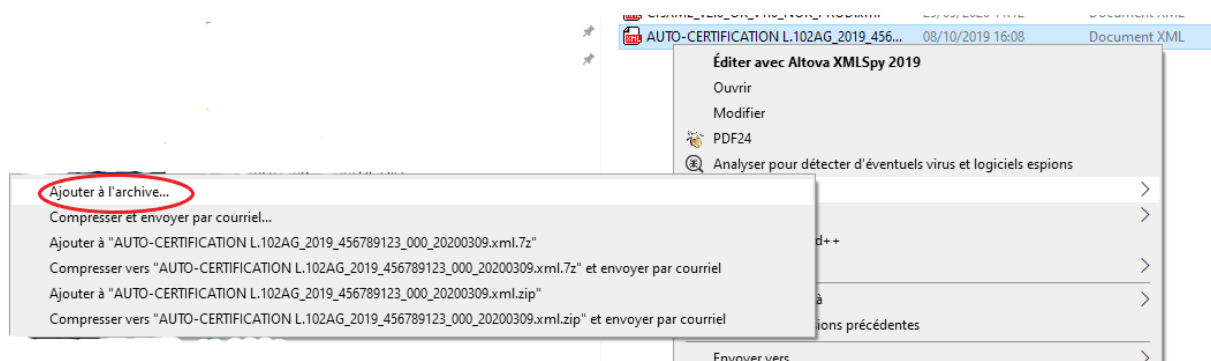
- Nous vous rappelons que les fichiers de déclarations doivent être **compressés** avant d'être **chiffrés** sous peine d'être rejetés. Le logiciel préconisé par la DGFIP est **7zip**, le format attendu est **GZIP**.
- Vous pouvez télécharger le logiciel ici : <https://www.7-zip.org/>

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

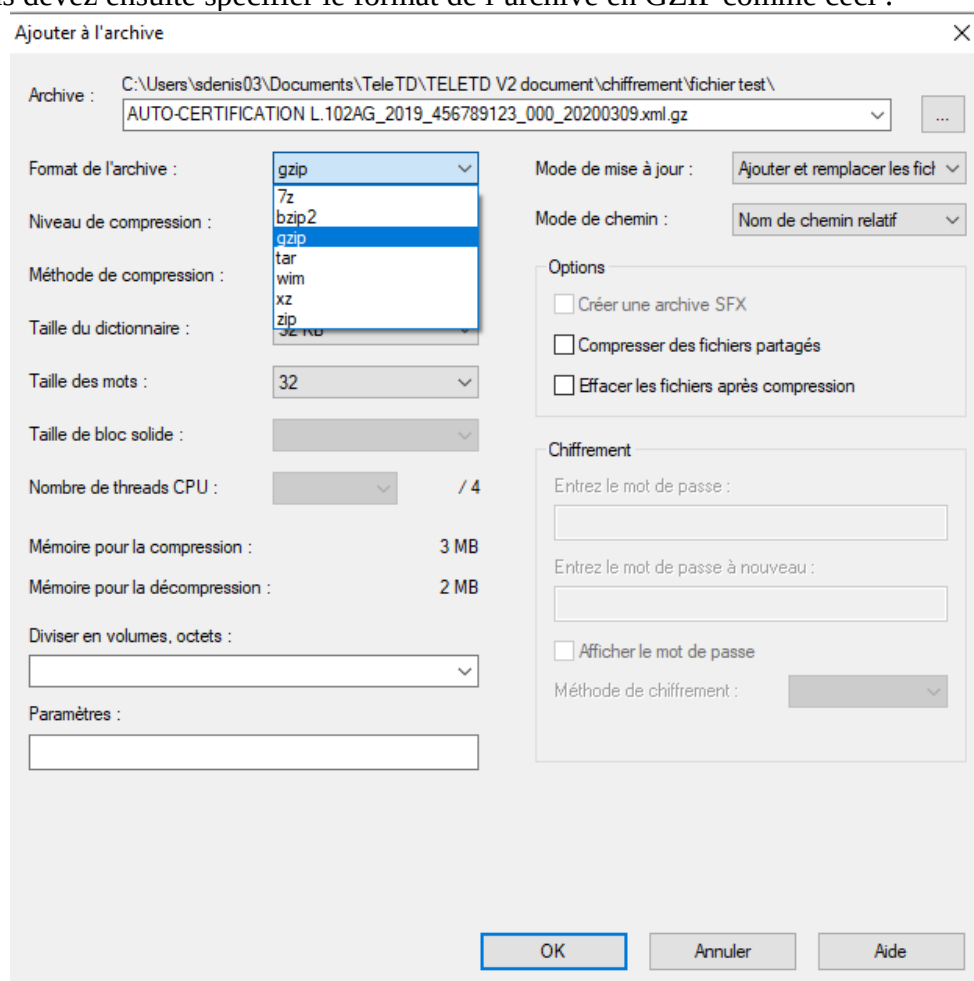
Download 7-Zip 19.00 (2019-02-21) for Windows:

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

- 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>

Gpg4win 3.1.11 (Released: 2019-12-17)

You can download the full version (including the Gpg4win compendium) of Gpg4win 3.1.11 here:

Gpg4win 3.1.11

Size: 27.6 MByte



[OpenPGP signature](#) (for gpg4win-3.1.11.exe)

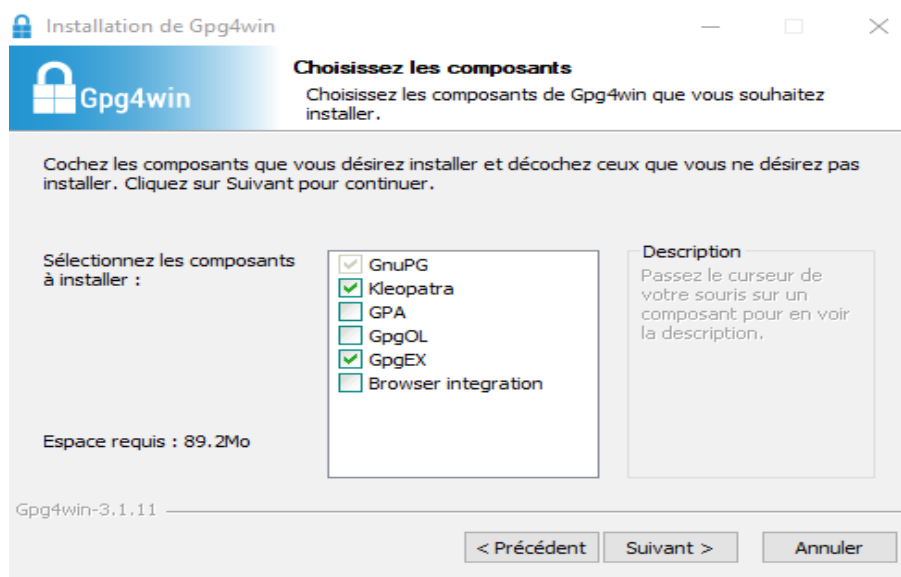
SHA256: 156de9f3f50bb5a42b207af67ae4ebcb2d10a7aaf732149e9c468eaf74ce7ffc

[Changelog](#)

Gpg4win 3.1.11 contains:

GnuPG 2.2.17
Kleopatra 3.1.8
GPA 0.10.0
GpgOL 2.4.2
GpgEX 1.0.6
Kompendium (de) 4.0.1
Kompendium (en) 3.0.0

- 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/tiers-declarants> dans la rubrique « Documentation utile »)
- 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 :

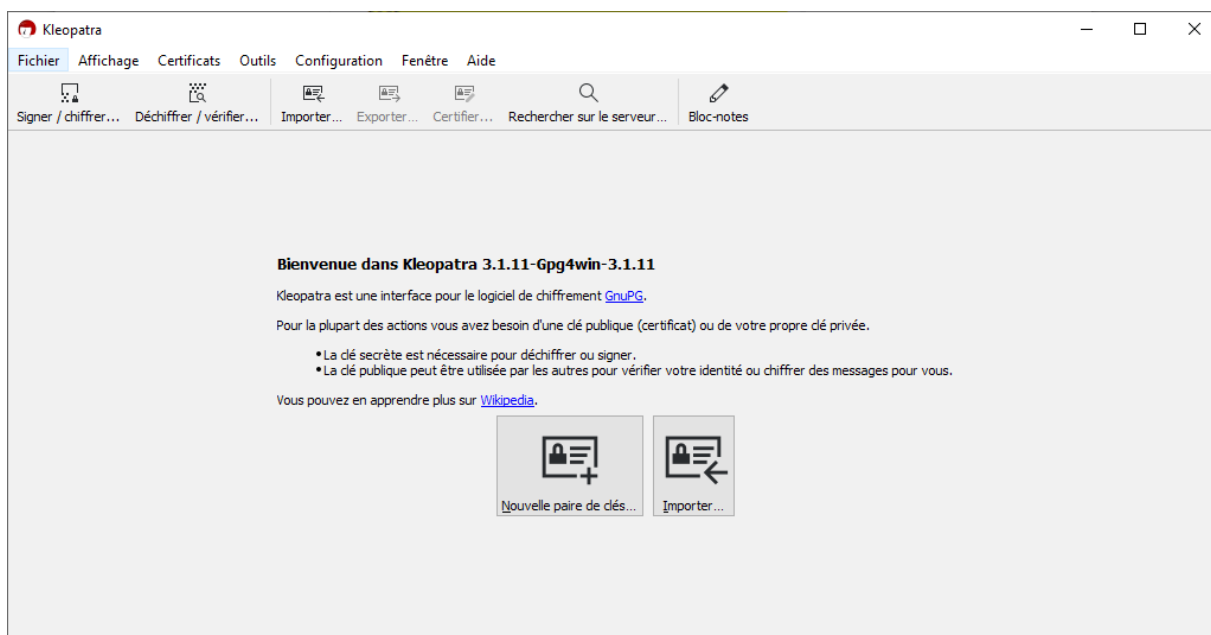
Documentation utile

- > Règles de constitution du numéro d'inscription au fichier de simplification des procédures d'imposition (SPI)
- > Cahier des charges Ecollab – Déclaration annuelle par les opérateurs de plateforme d'économie collaborative
- > Schema XSD de collecte
- > Schéma XSD des CRM
- > Exemples de fichiers Ecollab
- > Protocole de test Pilote
- > Modalités de dépôt des fichiers réels
- > Clé publique de chiffrement pour les fichiers de production
- > Clé publique de chiffrement pour les fichiers de test
- > Guide de chiffrement
- > Modèle de document annuel que les plateformes peuvent adresser à leurs utilisateurs - Utilisateurs personnes morales
- > Modèle de document annuel que les plateformes peuvent adresser à leurs utilisateurs - Utilisateurs personnes physiques
- > Modalités d'immatriculation d'une plateforme en ligne établie à l'étranger

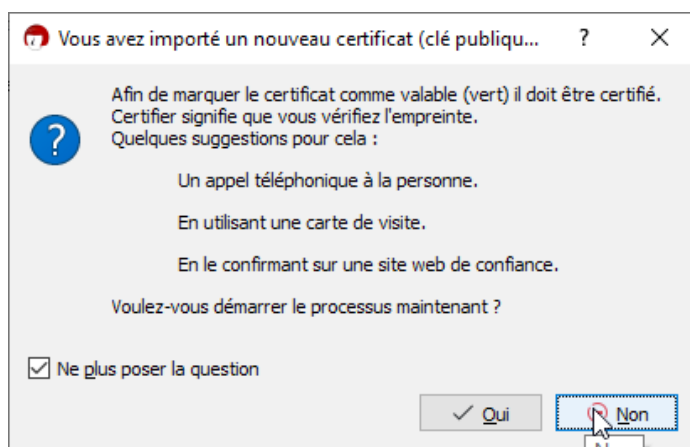
- Décompresser ensuite l'archive dans le répertoire de votre choix. La clé publique a pour extension « .asc » (ex. : pour la clé publique de chiffrement des fichiers de production: DGFIP_TIERSDECLARANTS_PROD.asc).

4.4 Intégration de la clé publique au logiciel de chiffrement

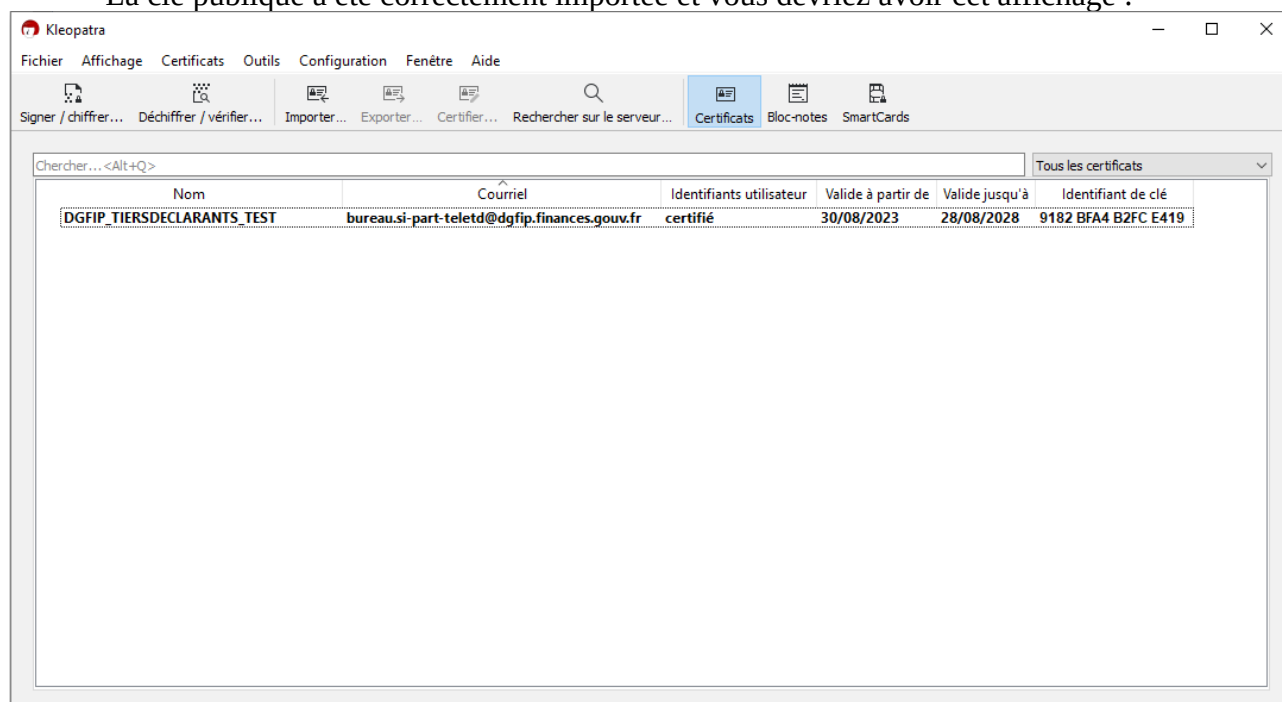
- Lancer l'application Kleopatra (par défaut l'icône se trouve sur votre bureau). Une fenêtre s'affiche :



- 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 :

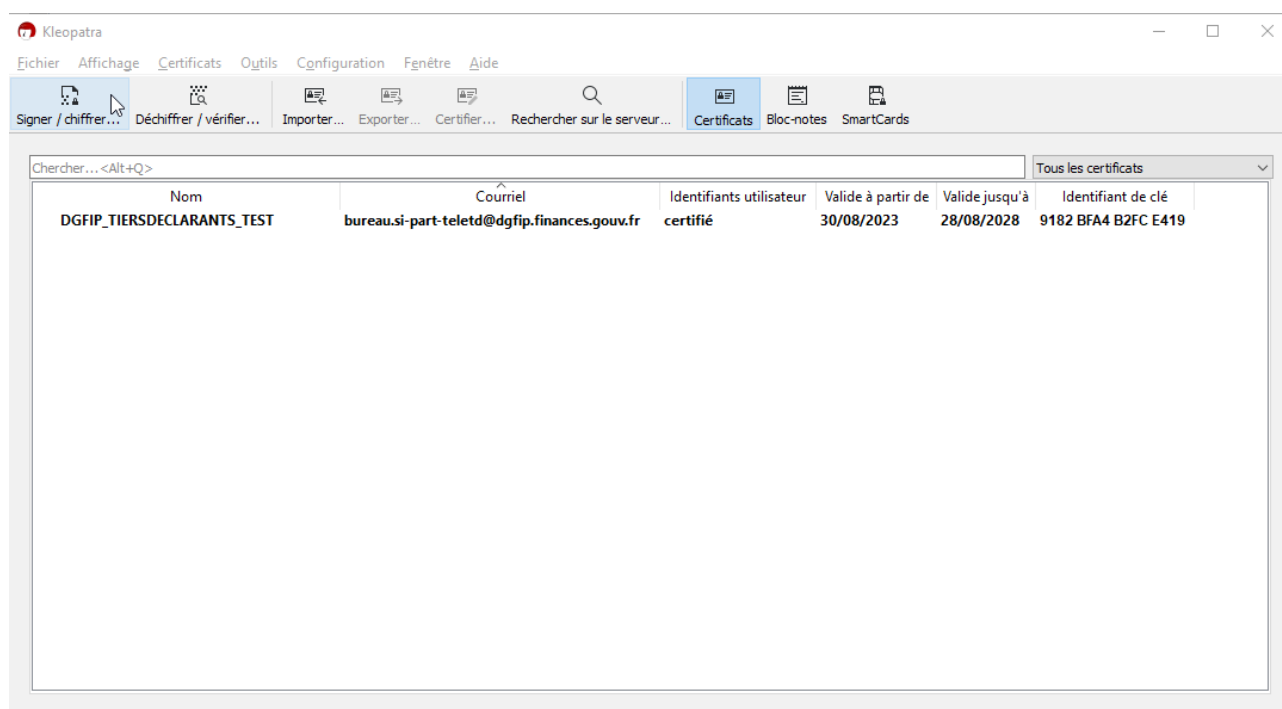


- La clé publique a été correctement importée et vous devriez avoir cet affichage :

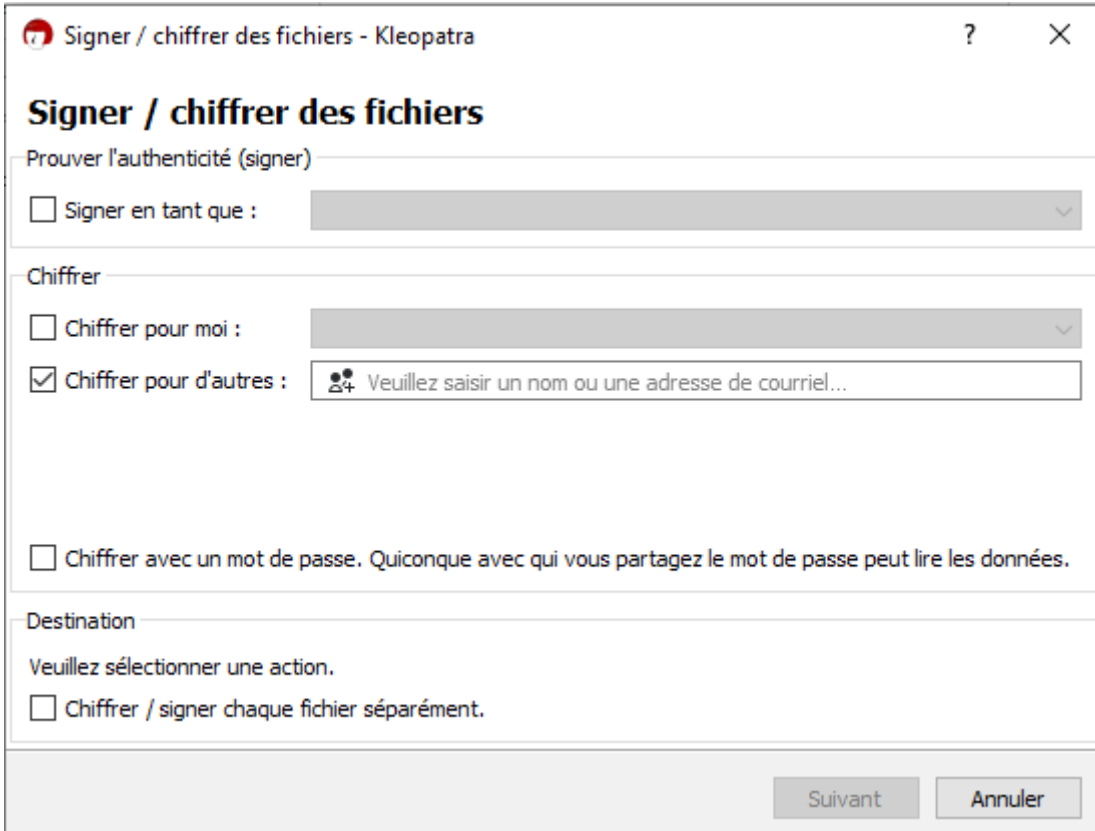


4.5 Chiffrement de la déclaration

- 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 :



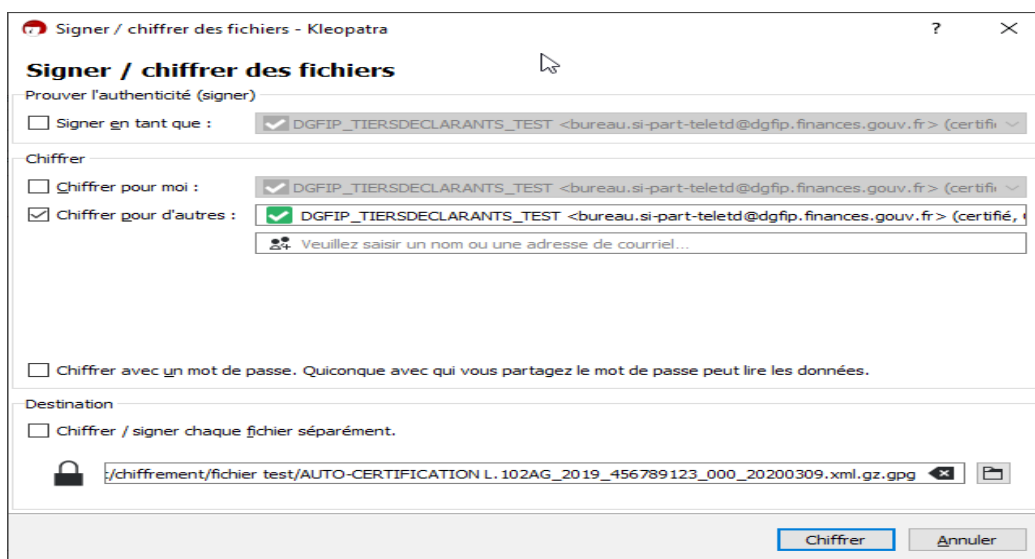
- Une fenêtre « Signer / chiffrer des fichiers » s’affiche :



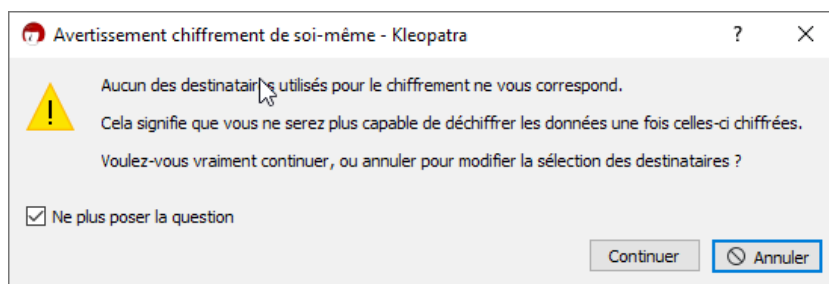
The screenshot shows a dialog box titled "Signer / chiffrer des fichiers - Kleopatra". The dialog is divided into several sections:

- Prouver l'authenticité (signer)**: Contains a checkbox "Signer en tant que :" followed by a dropdown menu.
- Chiffrer**: Contains two checkboxes: "Chiffrer pour moi :" (unchecked) and "Chiffrer pour d'autres :" (checked). The "Chiffrer pour d'autres" checkbox is followed by a text input field containing the placeholder text "Veillez saisir un nom ou une adresse de courriel...".
- Below the "Chiffrer" section, there is a checkbox "Chiffrer avec un mot de passe. Quiconque avec qui vous partagez le mot de passe peut lire les données." which is unchecked.
- Destination**: Contains the text "Veillez sélectionner une action." and a checkbox "Chiffrer / signer chaque fichier séparément." which is unchecked.
- At the bottom right, there are two buttons: "Suivant" and "Annuler".

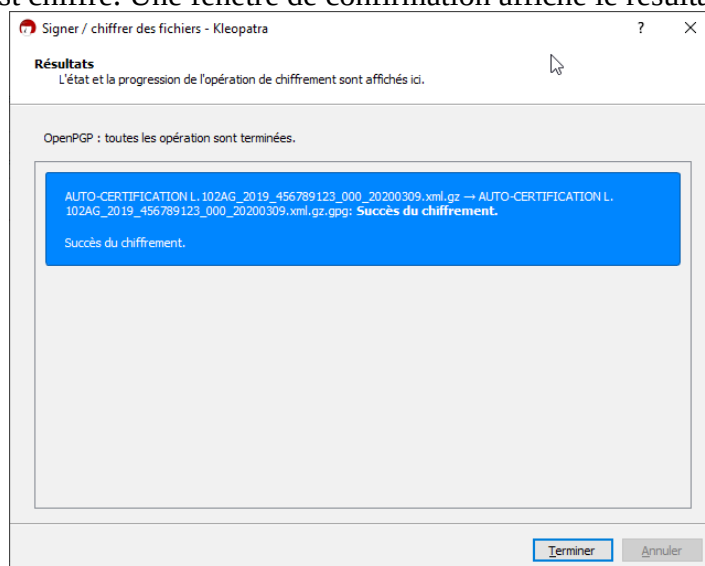
- Cocher **uniquement** l’option « Chiffrer pour d’autres ». Les autres cases doivent être décochées.
- Indiquer la clé publique « DGFIP TIERSEDECLARANTS_TEST ». Pour cela, taper « d » dans le cadre « Chiffrer pour d’autres ». Le menu déroulant affiche la clé publique DGFIP et vous devez la sélectionner.



- 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 « **Service Tiers Déclarant** ».

5 Outil utilisé pour un système d'exploitation MAC

5.1 Installation de GNUPG

- Ouvrir le **Terminal** qui permet la saisie en ligne de commande
- Lancer cette commande pour installer GNUPG : **brew install gnupg**
- Les étapes suivantes sont identiques à celles décrites dans la partie **3. Outil utilisé pour un système d'exploitation Linux**