Ministère de l'Action et des Comptes Publics

DIRECTION GENERALE DES FINANCES PUBLIQUES
SERVICE DES SYSTEMES D'INFORMATION

Guide de chiffrement

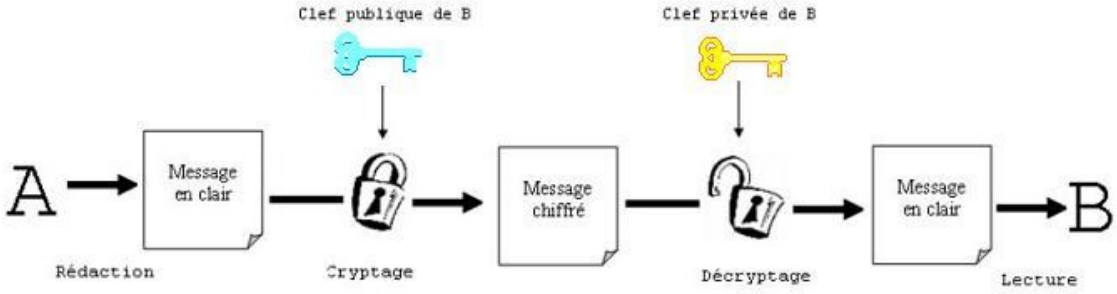
Présentation du procédé de chiffrement

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

Outil utilisé

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.
Ce logiciel fonctionne dans les environnements Linux, Unix, Macintosh et Windows 95/98/NT/2000/ME/XP/Vista/Windows 7.

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.
Sous macOS, GPG Suite est disponible.
Sous Windows, GPG4Win est disponible.

Vous trouverez facilement les modes d'emploi de ces logiciels via un moteur de recherche.

Nous ne développerons dans ce manuel que la solution en mode ligne de commande.

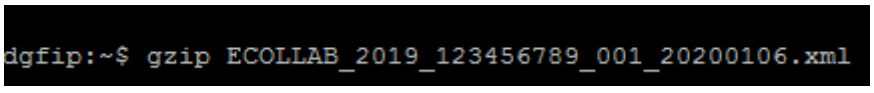
Compression du fichier XML

Points importants : Dans cette présentation, le fichier xml aura déjà été généré par la plate forme. Si votre fichier est déjà compressé au format gzip, passez directement à l'étape chiffrement.

Nous prendrons comme exemple le fichier suivant :
ECOLLAB_2019_12345678912345_001_20200106.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_2019_123456789_001_20200106.xml*



Le fichier sera compressé au format GZIP.
Le résultat sera : *ECOLLAB_2019_12345678912345_001_20200106.**xml.gz***

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 »)

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 ».

Chiffrer le fichier xml

Exécuter la commande suivante pour chiffrer le fichier xml compressé (remplacer le nom du fichier) :

gpg -e -r BE6BA1B4 *ECOLLAB_2019_12345678912345_001_20200106.xml.gz*

ECOLLAB_2019_12345678912345_001_20200106.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_2019_123456789_001_20200106.xml
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 ajouté à votre fichier xml compressé et chiffré (ex : *ECOLLAB_2019_12345678912345_001_20200106.xml.gz**.gpg***).

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