

Dans le cadre de ses missions, le CASD réceptionne des données provenant de divers organismes. Les échanges présentant un caractère sensible doivent faire l'objet d'un chiffrement permettant d'en assurer la confidentialité.

A cette fin, le CASD préconise l'utilisation de la cryptographie asymétrique basée sur PGP. Le CASD publie sur son site sa clef publique qui peut être utilisée pour chiffrer des données. Le CASD en revanche est le seul à disposer de la clef privée associée nécessaire au déchiffrement.

Il existe de nombreux outils permettant de réaliser ce chiffrement, la suite de ce document donne le détail d'un outil libre : [gpg4win](#). Il présente l'avantage de ne pas nécessiter de privilège administrateur pour être installé puis utilisé, et de disposer d'une interface graphique ergonomique, Kleopatra.

Voici le mode de fonctionnement :

1. Installer le programme en conservant les options par défaut, il n'est pas nécessaire de disposer de privilèges administrateur.
2. Lancer le programme Kleopatra
3. Télécharger la clef publique du CASD publiée sur son [site Internet](#) (clic droit sur l'icône fichier PGP > enregistrer sous...)

PGP

La clef PGP publique du CASD peut être utilisée pour sécuriser les transmissions vers le CASD. Nous vous invitons à nous contacter via service@casd.eu pour toute question à ce sujet.

TÉLÉCHARGER LA CLEF PGP PUBLIQUE DU CASD



DETAILS CONCERNANT LA CLEF :

ID: 2BBE1271

Type : RSA

Size : 4096/4096

Created : 2013-06-12

Expires : Never

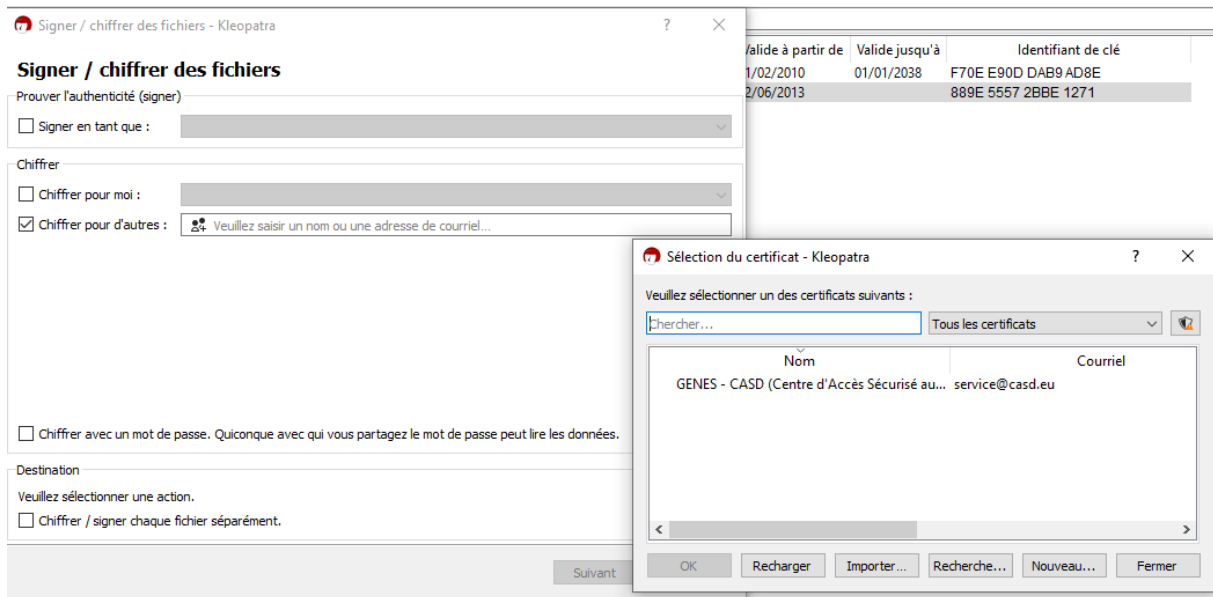
Cipher : AES-256

Fingerprint : 53B8 8ED6 A9F1 0E0B 62FD 5208 889E 5557 2BBE 1271

4. Importer la dans Kleopatra (menu Fichier > Importer, sélectionner le fichier GENES-CASD-53B88ED6A9F10E0B62FD5208889E55572BBE1271.asc téléchargé précédemment)
5. Double cliquer sur la clef et assurez-vous que son empreinte correspond effectivement à celle du site :

Empreinte : 53B8 8ED6 A9F1 0E0B 62FD 5208 889E 5557 2BBE 1271

6. Cliquer sur Signer/chiffrer, sélectionner le fichier à chiffrer puis indiquer le CASD comme unique destinataire.



7. Cliquer sur Chiffrer, et puis sur Continuer pour indiquer que vous êtes conscient que vous ne serez pas en mesure de déchiffrer le fichier résultant (les fichiers en clair ne seront pas supprimés)
8. Cliquer sur OK, le fichier chiffré sera généré au même emplacement, et portera le même nom suffixé par .pgp

Il est nécessaire de procéder à un chiffrement de test avec des données publiques (par exemple de data.gouv.fr) ou simulées avant tout envoi de données confidentielles.