Guide d’utilisation de GPG avec Kleopatra

Kleopatra

Crypto Manager

Table des matières

Introduction

Ce guide détaille l'utilisation du logiciel Kleopatra.

Kleopatra[1] est un gestionnaire de certificats et une interface graphique pour GnuPG (GPG). Le logiciel stocke vos certificats et clés OpenPGP. Il est disponible pour Windows, Mac et Linux.

GPG[2] est un logiciel qui permet la transmission de messages électroniques signés et chiffrés, garantissant ainsi leurs authenticité, intégrité et confidentialité.

La première partie présente les bases de la cryptographie asymétrique en expliquant le fonctionnement des paires de clés..

La deuxième partie décrit la procédure d'installation de GPG et Kleopatra sous Windows, Mac et Linux.

La troisième partie détaille l'utilisation de GPG avec Kleopatra pour organiser ses certificats, chiffrer/déchiffrer des messages, signer/vérifier des messages.

À l'issue de ce guide, vous serez capable de :

1. Créer et sauvegarder vos certificats personnels
2. Ajouter et certifier les clés publiques de vos contacts
3. Chiffrer et signer un message ou un fichier
4. Déchiffrer et vérifier un message ou un fichier

1 https://www.openpgp.org/software/kleopatra/
2 https://fr.wikipedia.org/wiki/GNU_Privacy_Guard

Le principe des paires de clés

Pour échanger des messages chiffrés, on utilise un système appelé « paires de clés ».
GPG est une alternative libre à PGP. C'est un logiciel de cryptographie asymétrique (ou par paires de clés)[3].

La cryptographie asymétrique utilise un système de paire de clés[4]. Chaque utilisateur possède une « clé privée », ainsi qu'une « clé publique ».

- La « clé privée » permet le déchiffrement et la signature des messages.
- La « clé publique », est dérivée d'une « clé privée ». Elle sert à chiffrer et vérifier les messages pour cette « clé privée » d'origine.

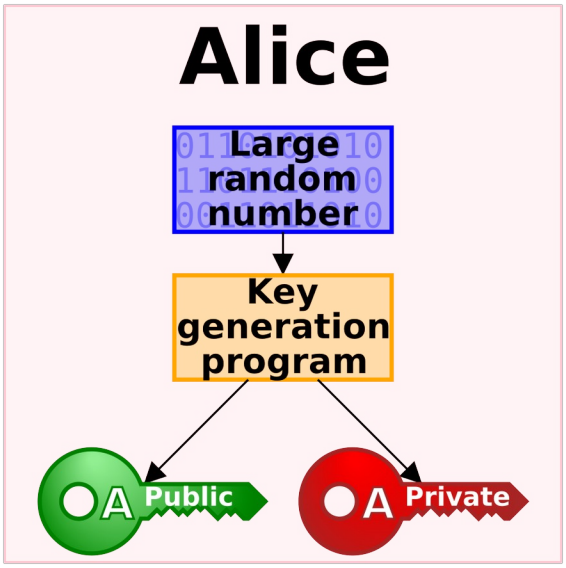

Figure 1: Paire de clés d'Alice

La figure 1 montre une paire de clés générée par une utilisatrice, Alice. Avec cette paire de clés, Alice peut recevoir des messages chiffrés et prouver son identité avec les deux opérations suivantes :

- Le chiffrement : "C'est comme mettre un message dans un cadenas dont seul Alice a la clé."
- La signature : "C'est comme signer une lettre à la main : tout le monde peut vérifier que c'est bien votre écriture."

3 https://fr.wikipedia.org/wiki/Cryptographie_asymétrique
4 https://fr.wikipedia.org/wiki/Clé_de_chiffrement

Le chiffrement

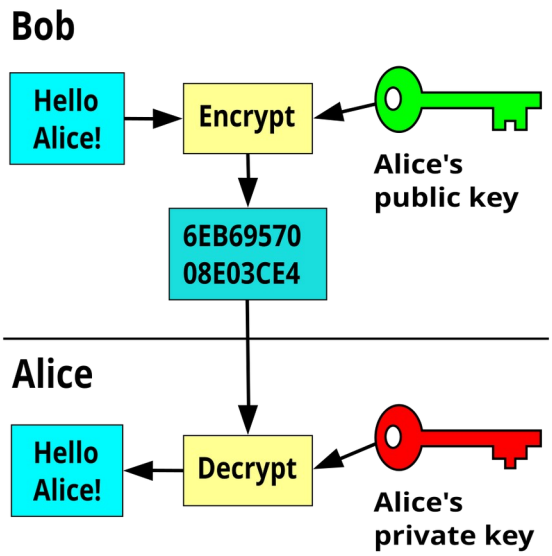

Figure 2: Exemple chiffrement

Dans l'exemple illustré par la figure 2, un autre utilisateur, Bob, cherche à envoyer un message chiffré à Alice. Alice lui envoie sa clé publique.

- Bob utilise la « clé publique » d'Alice pour chiffrer le message.
- Le message chiffré est envoyé à Alice.
- Alice déchiffre le message avec sa clé privée.

La signature

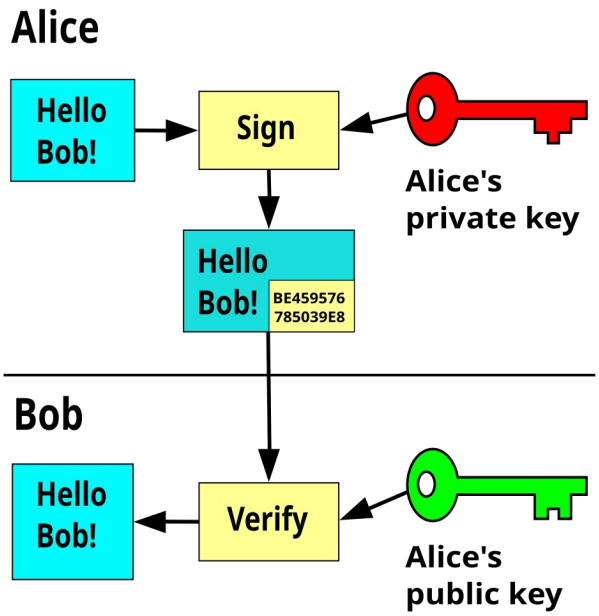

Figure 3: Exemple signature

Alice cherche maintenant à envoyer un message signé à Bob :

- Alice signe un message avec sa « clé privée ».
- Alice envoie le message à Bob.
- Bob vérifie la signature avec la « clé publique » d'Alice, la signature est valide, Bob sait que le message vient bien d'Alice.

En résumé, la clé publique sert à chiffrer et à vérifier, tandis que la clé privée sert à déchiffrer et à signer.

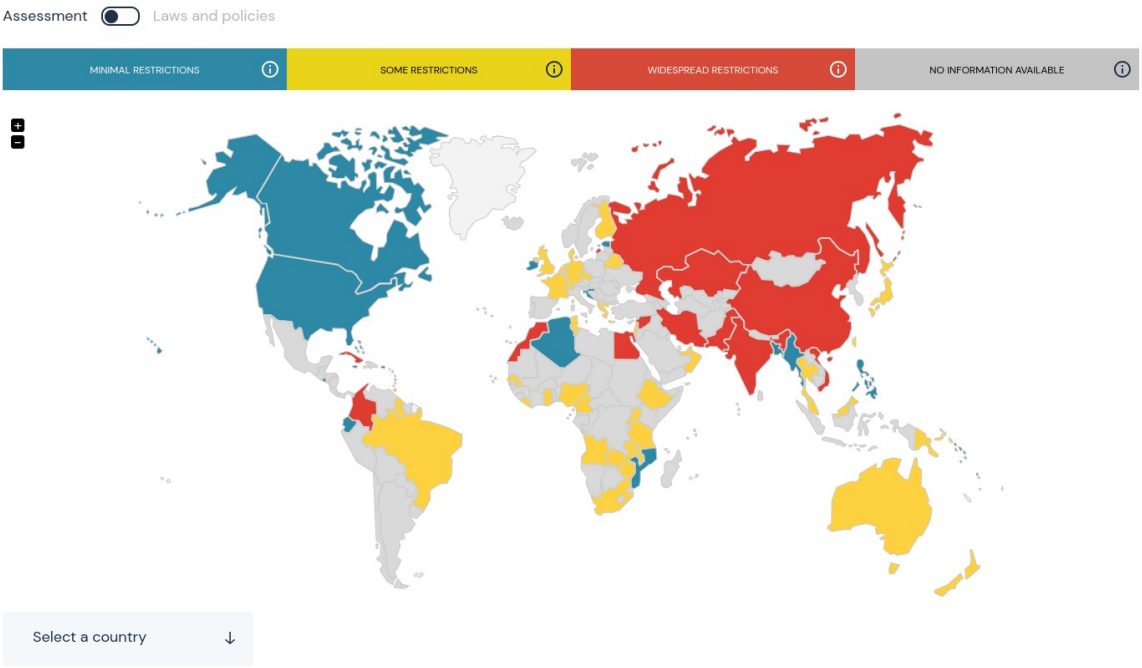

Figure 4: Carte mondiale des lois et politiques de chiffrement

Selon l'endroit où vous êtes dans le monde, le statut juridique du chiffrement varie considérablement. Dans certains pays, l'utilisation des technologies liées au cryptage n'est que peu entravée ; dans d'autres, les entreprises et les utilisateurs sont soumis à d'importantes restrictions.

En France, par exemple :

L'importation, l'exportation et la fourniture de services de cryptographie sont soumis à l'autorisation du Premier Ministre en France. Dans certaines circonstances, les entités privées ou les personnes qui fournissent des services de cryptologie doivent déchiffrer les données chiffrées par leurs services dans les 72 heures, sauf s'ils peuvent démontrer que cela ne serait pas possible. La loi prévoit également à un procureur, à un tribunal d'enquête ou à un fonctionnaire de la police judiciaire de désigner toute entité ou personne privée pour utiliser les moyens techniques nécessaires pour déchiffrer les données chiffrées au cours d'une enquête pénale.[5]

Cette carte n'est pas complètement à jour. Je vous invite à vous renseigner avant d'utiliser la cryptographie.

5 https://www.gp-digital.org/world-map-of-encryption/

Installation

Windows

Gpg4win[6] (GNU Privacy Guard for Windows) est un logiciel de chiffrement pour signer et chiffrer des fichiers et des courriels. La création de Gpg4win a été soutenue par l'Allemagne Office fédéral de la sécurité de l'information (BSI).

Lien de téléchargement : https://www.gpg4win.org/download.html

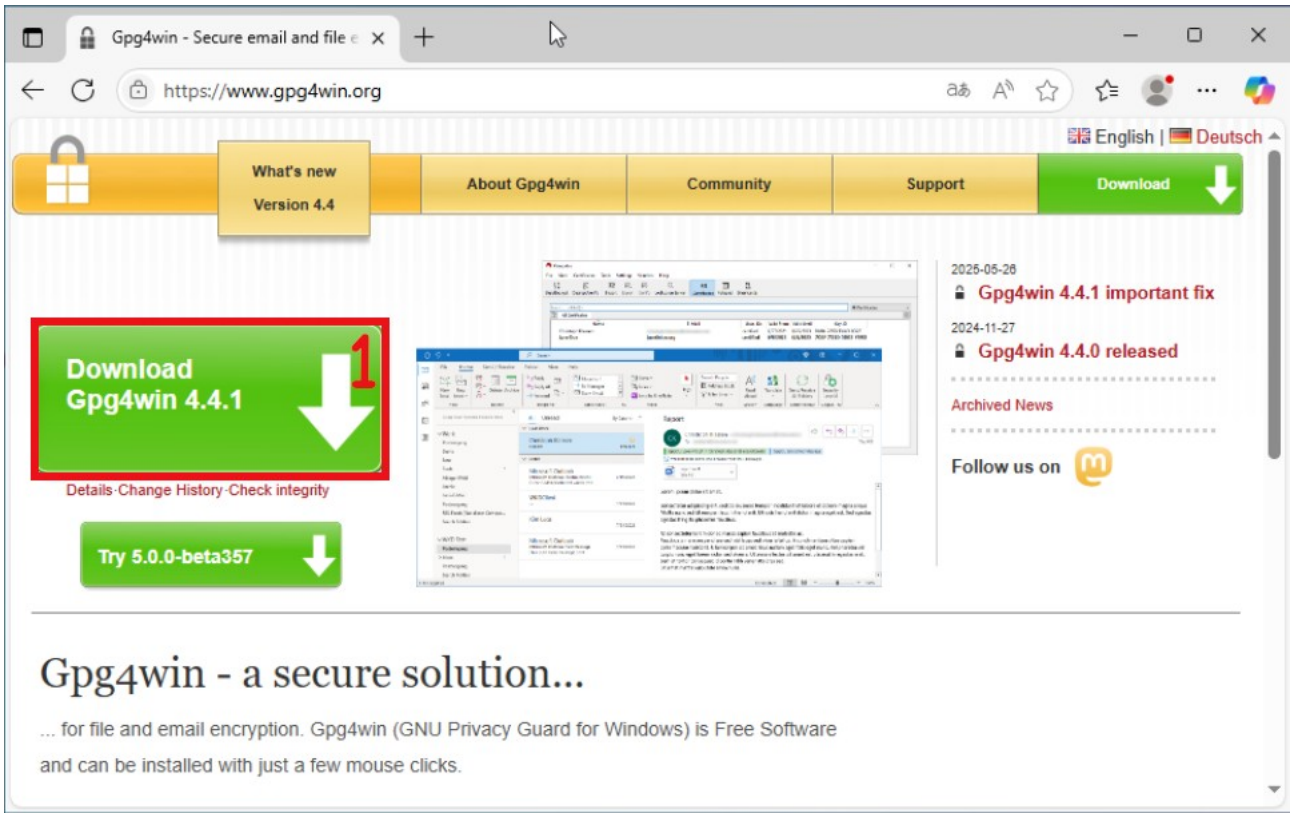

Figure 5: Site de Gpg4win

Une fois sur le site de Gpg4win (Figure 5) :

1. Cliquer sur le bouton « Download Gpg4win »

6 https://fr.wikipedia.org/wiki/Gpg4win

Figure 6: Page de téléchargement

Sur la page de téléchargement (Figure 6) :

2. Sélectionner le montant de la donation que vous souhaitez réaliser.
3. Cliquer sur « Download ».

Figure 7: Téléchargement en cours

4. Le téléchargement est en cours (figure 7)

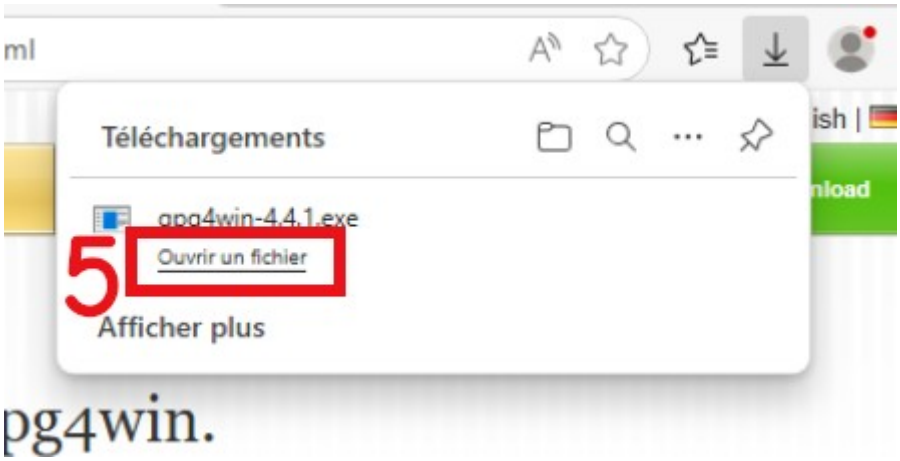

Figure 8: Téléchargement terminé

Une fois le téléchargement terminé (Figure 8) :

5. Cliquer sur « Ouvrir un fichier »

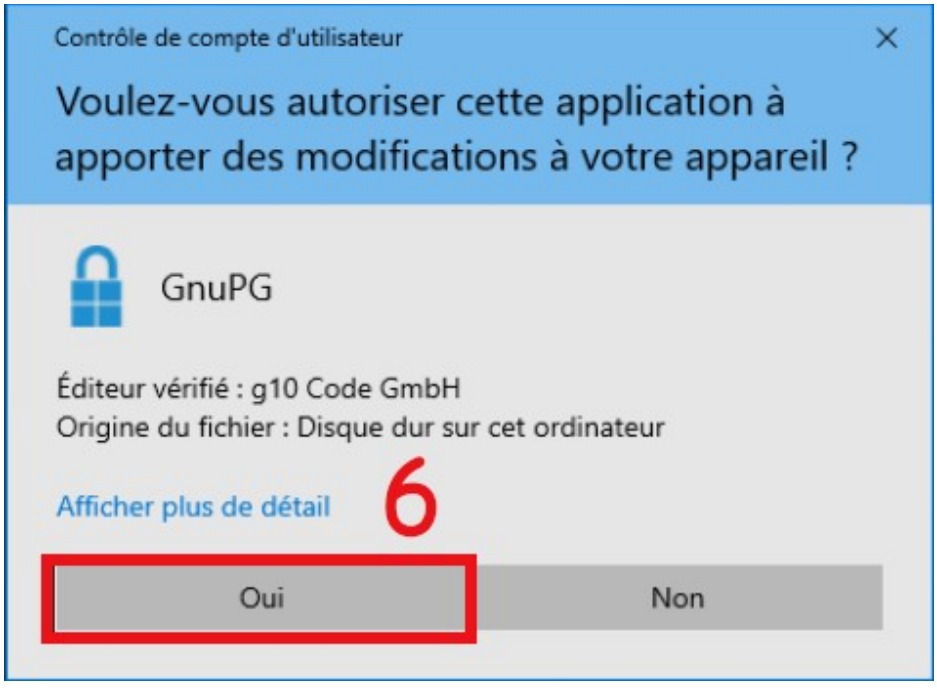

Figure 9: Autorisation windows

Autoriser Windows à lancer l'application (Figure 9) :

6. Cliquer sur Oui.

Figure 10: Installation de Gpg4win

Dans la fenêtre d'installation (Figure 10) :

7. Cliquer sur « Suivant > »

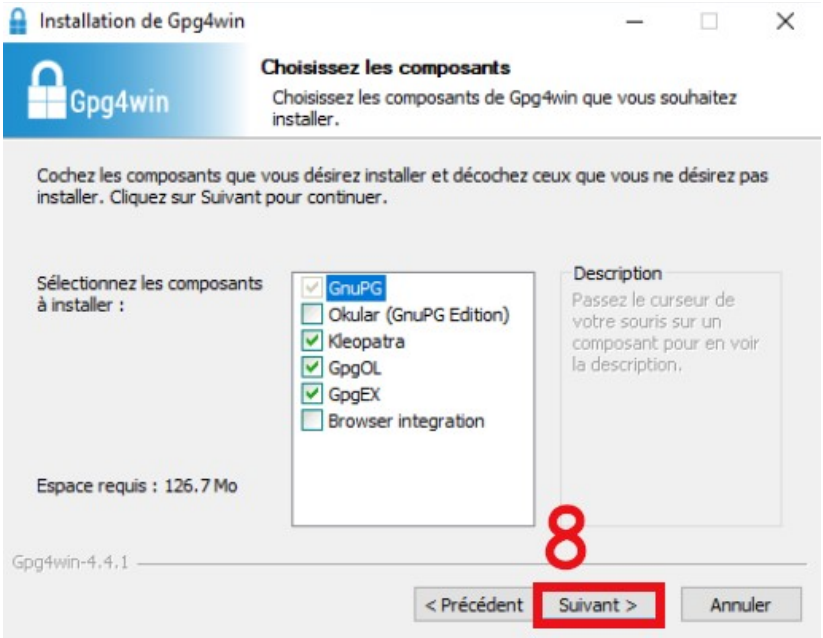

Figure 11: Choix composants

Dans la fenêtre de choix des composants (Figure 11), laisser les composants par défaut (GnuPG, Kleopatra, GpgOL, GpgEX).

8. Cliquer sur « Suivant > »

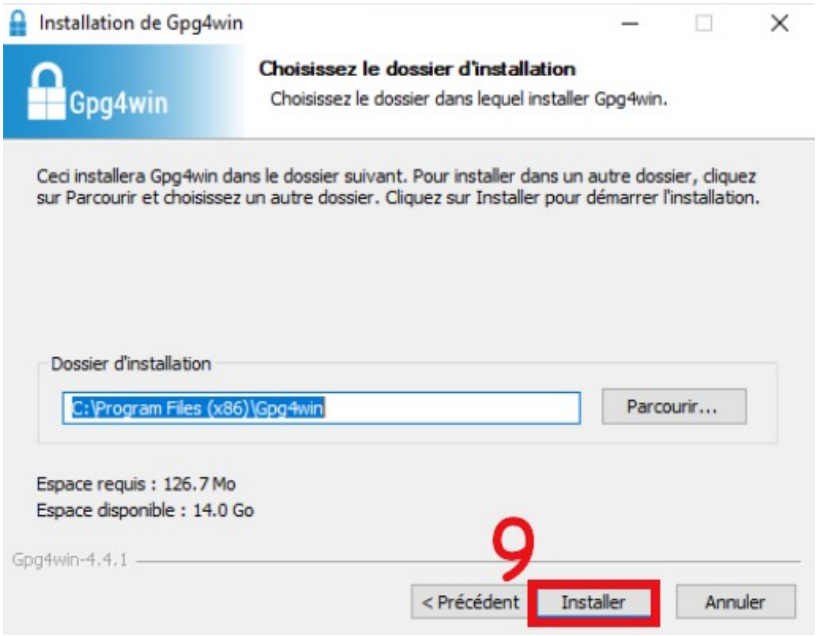

Figure 12: Dossier d'installation

Dans la fenêtre de sélection du dossier d'installation (Figure 12), choisir l'emplacement du dossier d'installation.

9. Cliquer sur « Installer »

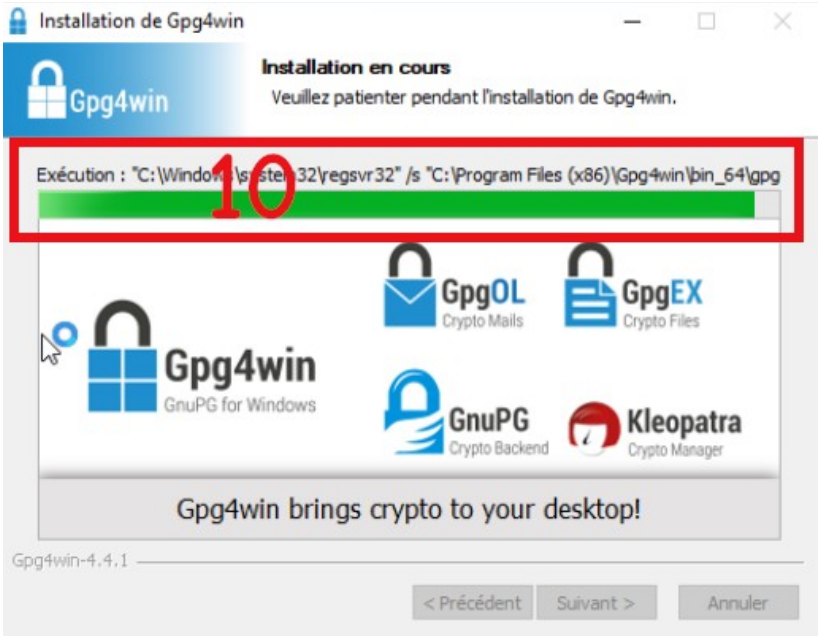

Figure 13: Installation en cours

10. L'installation est en cours (figure 13)

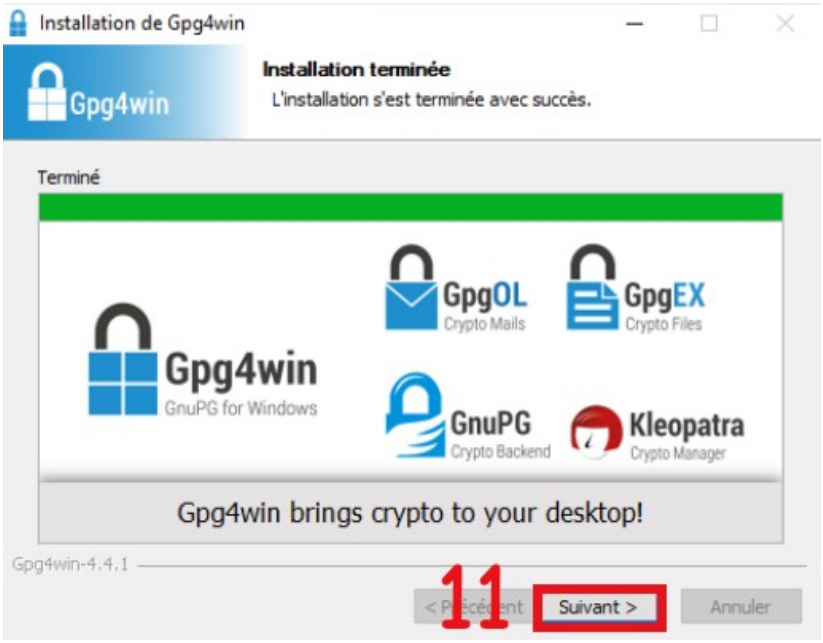

Figure 14: Installation terminée

L'installation est terminée (figure 14)

11. Cliquer sur « Suivant > » pour continuer

Figure 15: Fin installation

L'installation est terminée (Figure 15) :

12. Cliquer sur « Fermer »

Linux

Kleopatra est disponible dans les dépôts de toutes les distributions majeures.

MacOS

Kleopatra4Mac est un port tout-en-un pré-construit de l'utilitaire GPG de KDE pour une utilisation sur MacOS.
https://github.com/algertc/homebrew-kleopatra4mac

Utilisation de Kleopatra

Ce guide d'utilisation explique comment utiliser Kleopatra. L'ensemble est illustré par des captures d'écrans commentées, faisant figurer quatre utilisateurs « Odaabeq », « Yajawn », « Nisgr » et « Baintotor » dans une configuration d'exemple.

Découverte de l'interface

Au lancement, Kleopatra affiche le contrôle automatique (Figure 16).

1. Cliquer sur « Afficher tous » pour avoir le détail (Les détails pourraient avoir l'air différent sur votre machine)
   - Certains tests sont en Échec. « scdaemon » sert pour les lecteurs de cartes. Il n'est pas nécessaire pour la suite
2. Cliquer sur « ✓ Continuer » pour passer à la suite

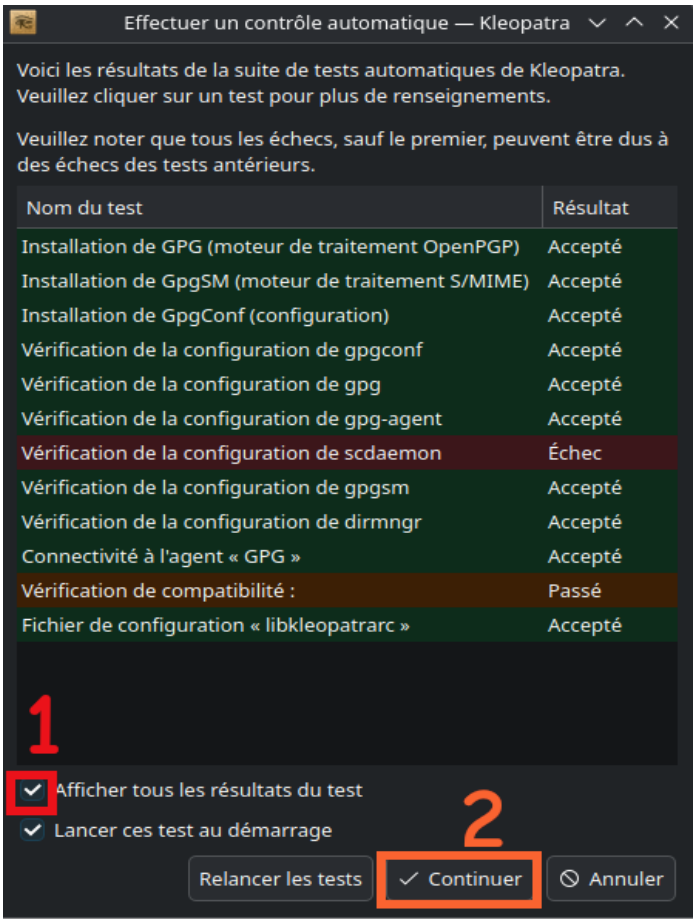

Figure 16: Contrôle automatique

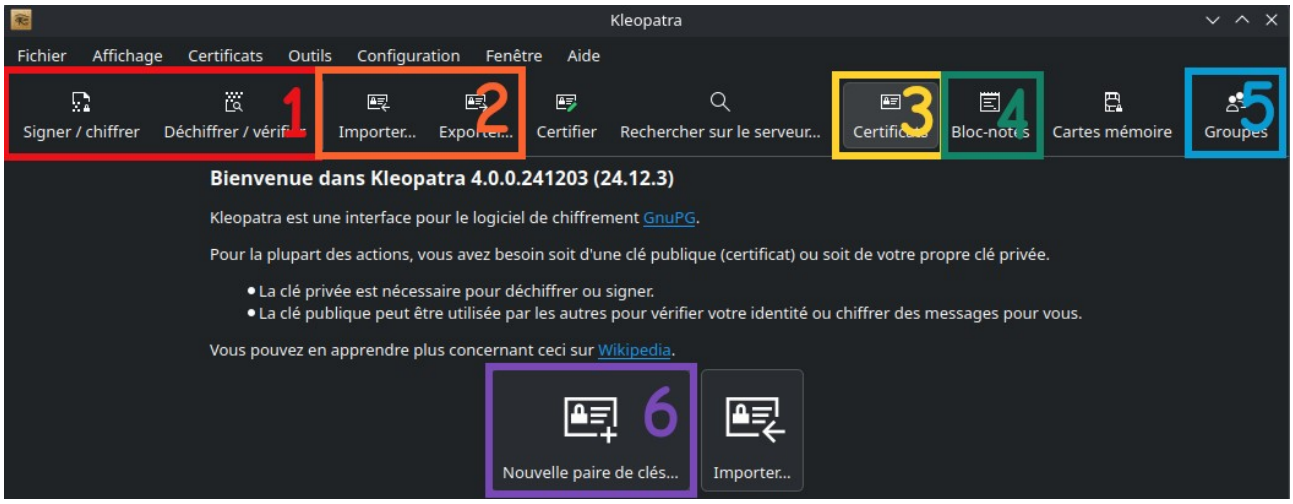

Figure 17: Interface de Kleopatra

Présentation de l'interface (Figure 17) :

1. Chiffrer/Déchiffrer et Signer/Vérifier des fichiers
2. Importer/Exporter des certificats
3. Certificats personnels de l'utilisateur et des contacts
4. Espace de texte pour opérations rapides
5. Permet d'organiser ses contacts sous forme de groupes
6. Cliquer sur « Nouvelle paire de clés... » pour passer à la suite

Créer un certificat

Dans cette partie, l'utilisateur « Odaabeq » créer son premier « certificat »[7]. Tout est automatique. Le logiciel s'occupera tout seul de générer la « clé privée », ainsi que la « clé publique » correspondante. Celle-ci est englobée dans ce qu'on appelle un « certificat ».

Un « certificat », englobe la « clé publique » avec l'identité de l'utilisateur (Ici, son pseudo « Odaabeq »).

C'est ce « certificat » qui est partagé avec ses contacts, plutôt que la « clé publique » seule. Cette mesure permet de vérifier l'origine et la validité du certificat.

7 https://fr.wikipedia.org/wiki/Certificat_électronique

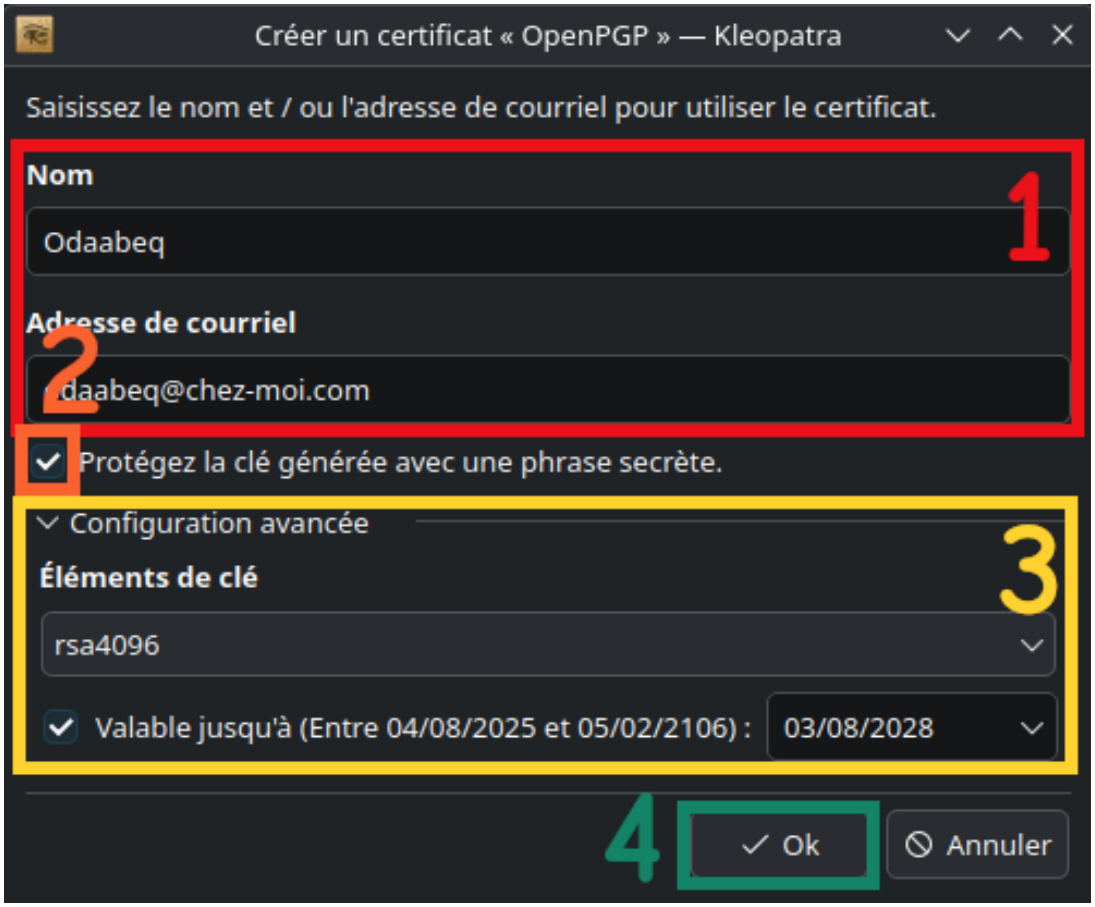

Figure 18: Créer un certificat

« Odaabeq » créer un nouveau certificat (Figure 18) :

1. Saisie du nom et d'un e-mail (facultatif)
2. **Important : La clé doit être protégée avec un mot de passe afin de se prémunir contre les vols. Cette case DOIT être cochée. Le mot de passe de votre clé privée est précieux, conservez-le soigneusement**
3. Dans configuration avancée, choisir rsa4096, plus lent, mais plus robuste. Il est aussi possible de changer la date d'expiration du certificat
4. Cliquer sur « ✓ Ok » pour passer à la suite

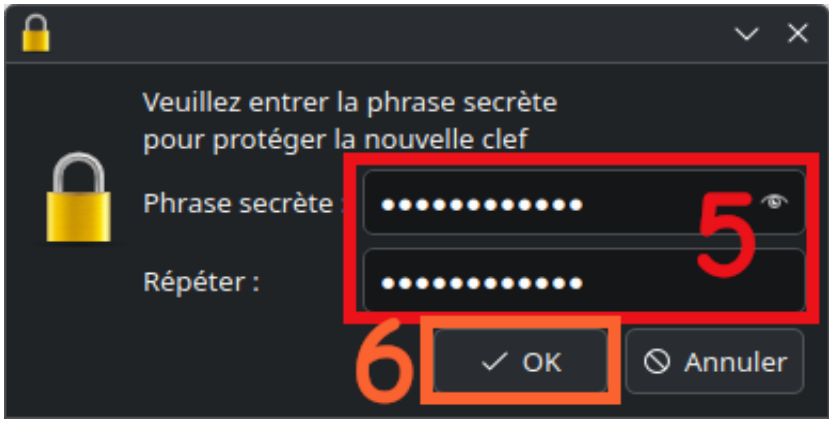

Figure 19: Saisie de mot de passe

5. Saisir un mot de passe (Figure 19)
6. Cliquer sur « ✓ Ok » pour passer à la suite

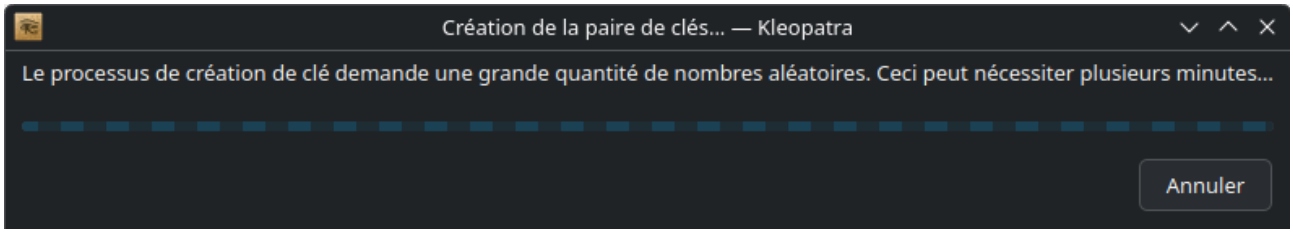

Figure 20: Création en cours

7. Attendre la fin de la création (Figure 20)

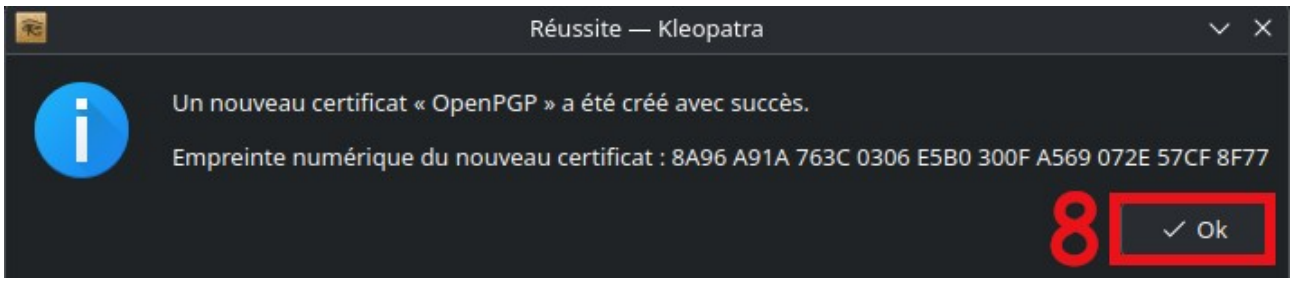

Figure 21: Création réussie

8. Cliquer sur « ✓ Ok » pour passer à la suite (Figure 21)
9. Si besoin, pour créer une nouvelle paire, faire : Fichier → Nouvelle paire de clés « OpenPGP »…

Sauvegarder sa clé privée

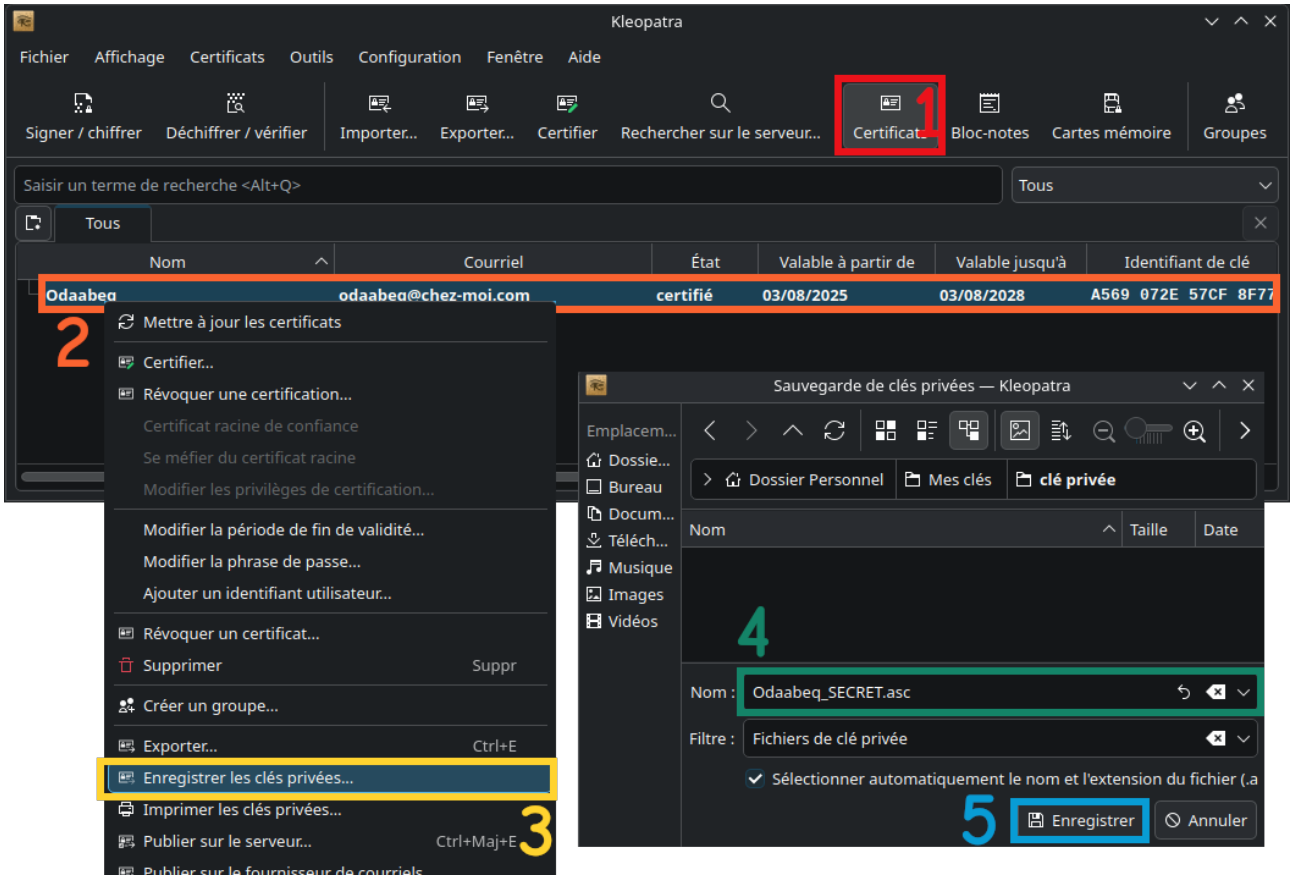

Figure 22: Enregistrer clé privée

« Odaabeq » réalise une copie de secours de sa clé privée (Figure 22) :

1. Dans le menu Certificats
2. Clic droit sur « mon certificat »
3. Enregistrer les clés privées… (Le mot de passe de la clé peut être demandé)

Important : Sans backup, si la clé privée est perdue, il n'y a plus aucun moyen de récupérer les données chiffrées.

4. Nommer sa clé privée
5. Cliquer sur Enregistrer

Exporter son certificat

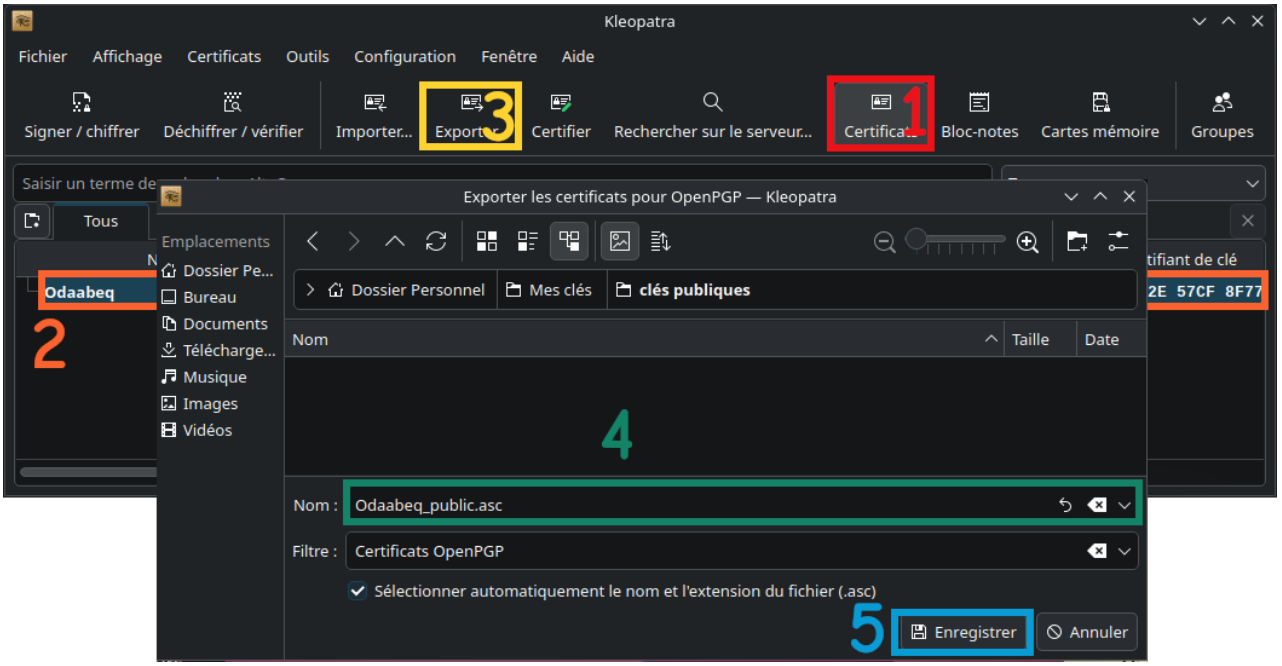

Figure 23: Exporter certificat

« Odaabeq » exporte son certificat (Figure 23) :

1. Dans le menu Certificats
2. Sélectionner « mon certificat »
3. Cliquer sur « Exporter »
4. Choisir un nom et un emplacement pour ce fichier
5. Cliquer sur « Enregistrer »
6. Envoyer ce fichier à tous les contacts. « Odaabeq » envoie son certificat à « Yajawn », « Nisgr » et « Baintotor »

Importer des certificats

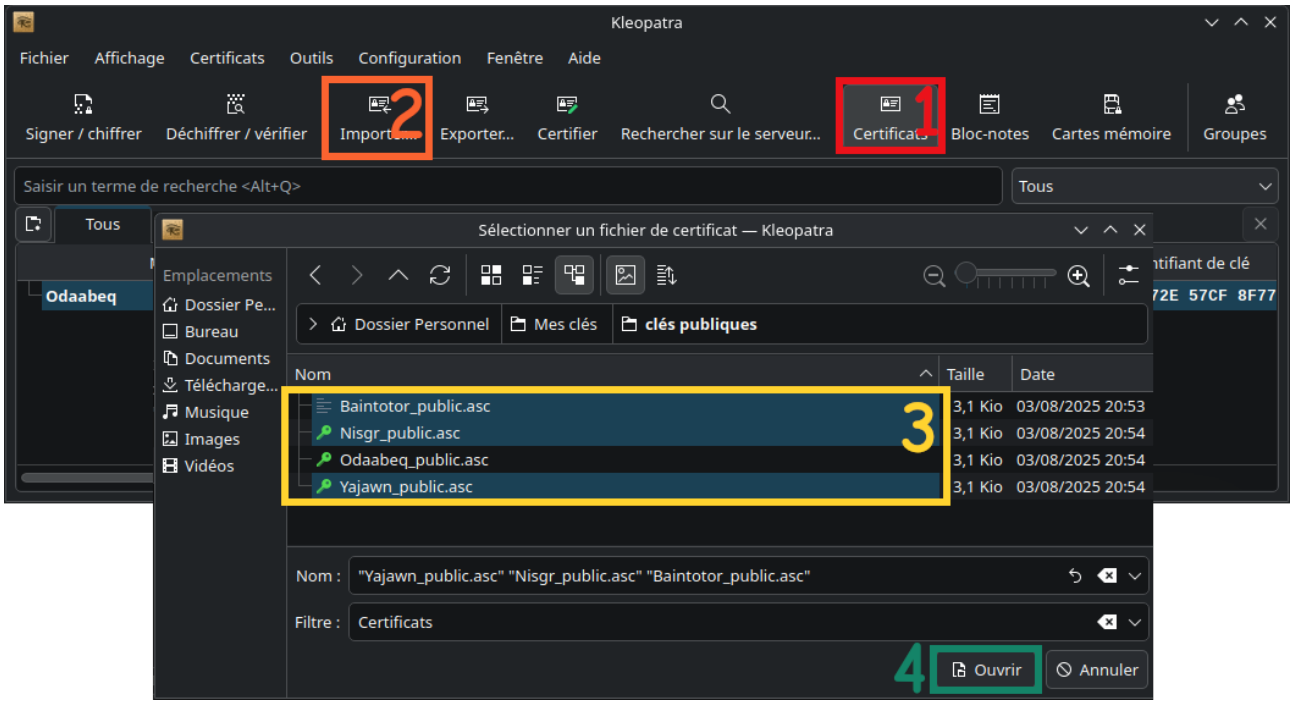

Figure 24: Importer des certificats

Une fois que tous les utilisateurs ont créés leurs paire de clés et partager leurs certificats, il faut les importer pour pouvoir s'échanger des messages chiffrés.

« Odaabeq » importe les certificats de ses contacts (Figure 24) :

1. Dans le menu « Certificats »
2. Cliquer sur Importer
3. Sélectionner les certificats des contacts. « Odaabeq » importe les certificats de « Yajawn », « Nisgr » et « Baintotor »
4. Cliquer sur Ouvrir

Si une seule clé est sélectionnée, vous serez invité à démarrer le processus de certification. Celui-ci est expliqué dans les parties suivantes « Récupérer mon empreinte » et « Certifier un contact ».

Récupérer son empreinte

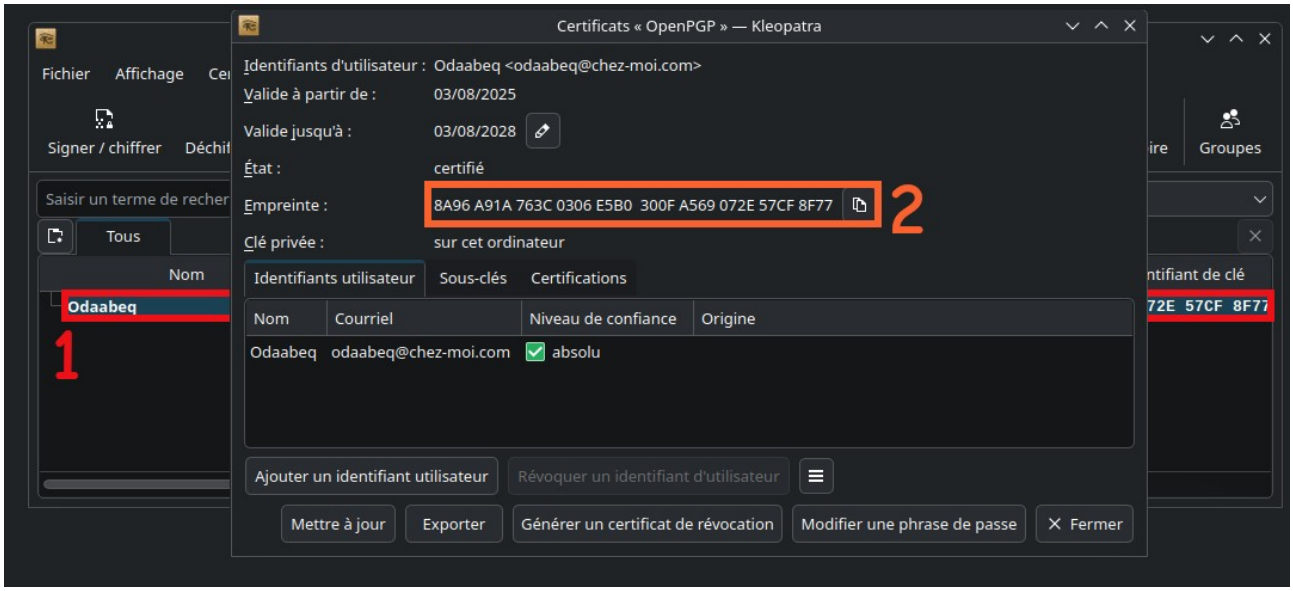

Figure 25: Récupérer empreinte

« Odaabeq » récupère son empreinte (Figure 25) :

1. Double clic sur mon certificat
2. Copier l'empreinte pour l'envoyer aux contacts lors de la procédure de certification. Cette mesure empêche l'usurpation d'identité lors de l'import des certificats

Certifier un contact

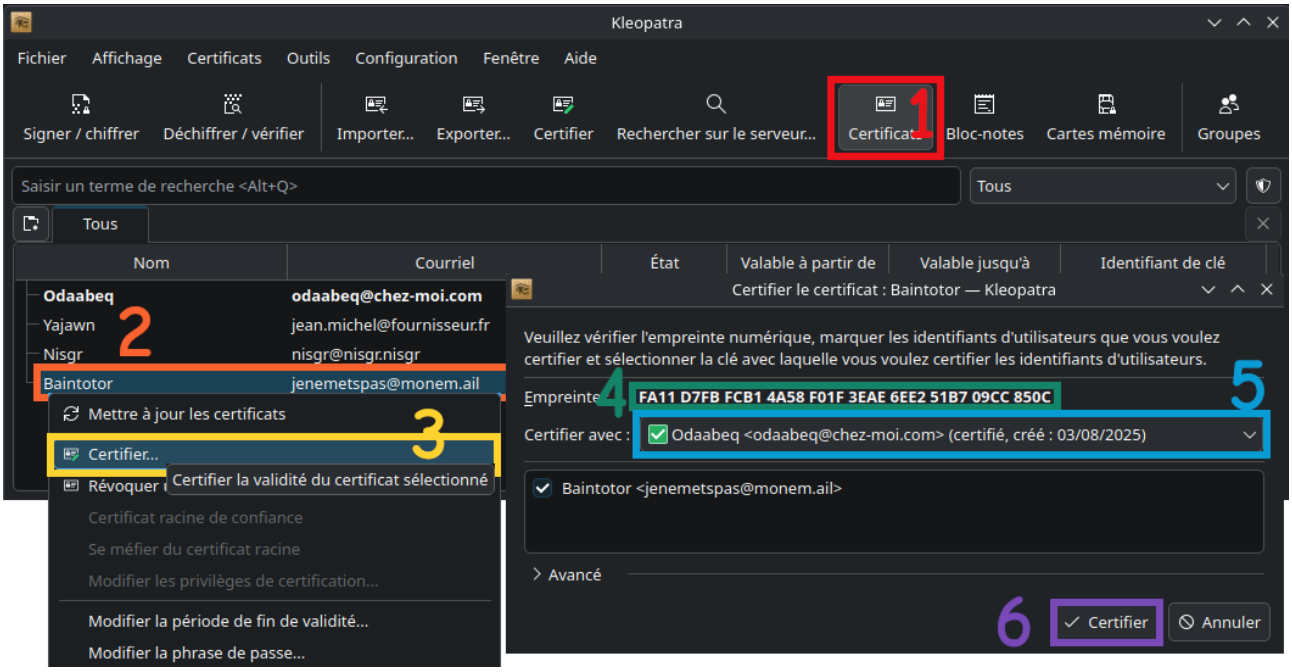

Figure 26: Certification d'un contact

« Odaabeq » certifie le certificat de « Baintotor » (Figure 26) :

1. Dans le menu certificats
2. Clic droit sur le contact à certifier
3. Dans le menu déroulant, choisir « Certifier... »
4. Vérifier que l'empreinte correspond bien à celle transmise par le contact
5. Choisir l'identité avec laquelle valider la certification. « Odaabeq » importe le certificat de « Baintotor ». Il certifie avec son identité que l'empreinte du certificat de « Baintotor » est valide
6. Cliquer sur « ✓ Certifier ». Le mot de passe du certificat qui valide peut être demandé
7. Le message « Le certificat a été créé avec succès. » devrait apparaître. Cliquer sur « ✓ Ok »

Créer un groupe

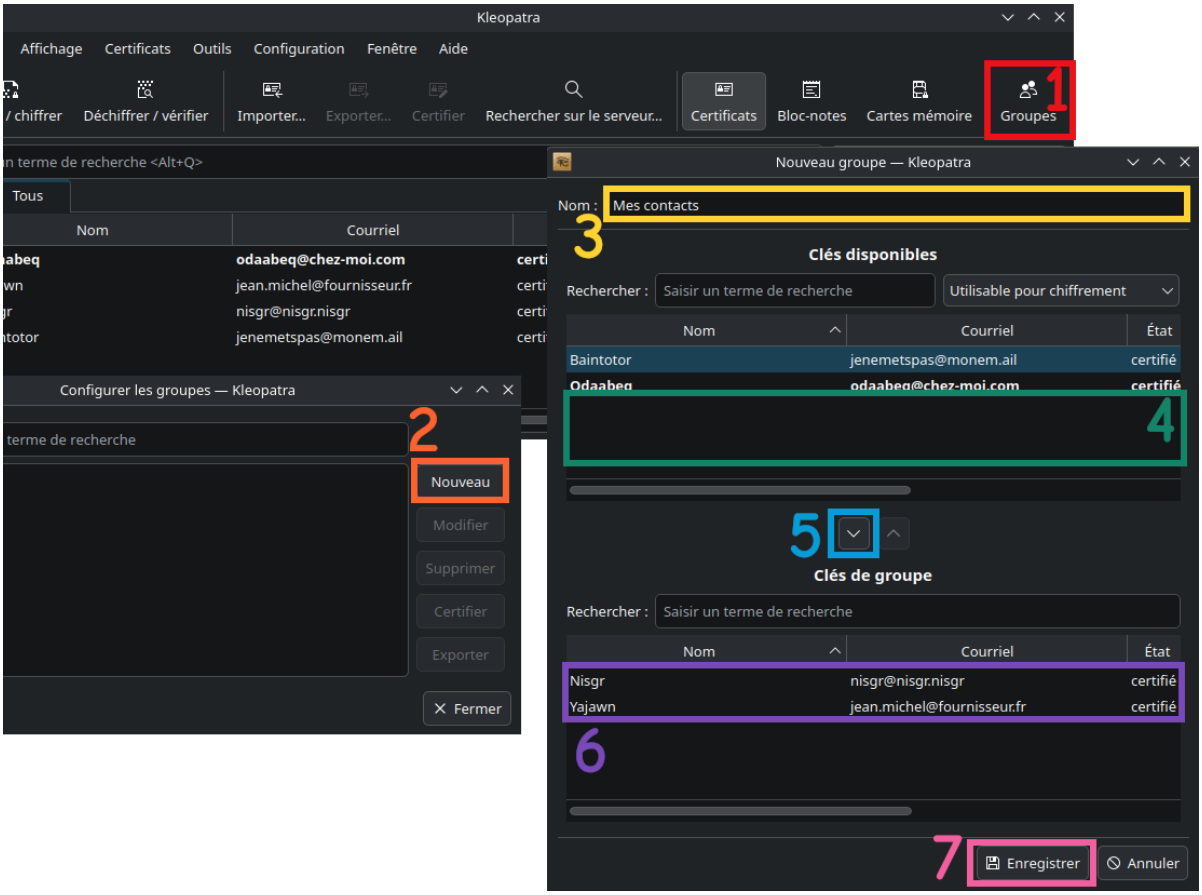

Figure 27: Création de groupe

« Odaabeq » créé un groupe contenant « Nisgr » et « Yajawn » (Figure 27) :

1. Cliquer sur « Groupes »
2. Dans la nouvelle fenêtre, cliquer sur « Nouveau »
3. Dans la nouvelle fenêtre, Choisir un nom de groupe
4. Dans la liste des contacts, sélectionner les contacts à ajouter au groupe
5. Cliquer sur la flèche du bas pour ajouter la sélection au groupe
6. Les contacts ajoutés devraient figurer dans cette partie du bas. Le groupe « Mes contacts » contient « Nisgr » et « Yajawn »
7. Cliquer sur « Enregistrer »

Chiffrer et signer un message

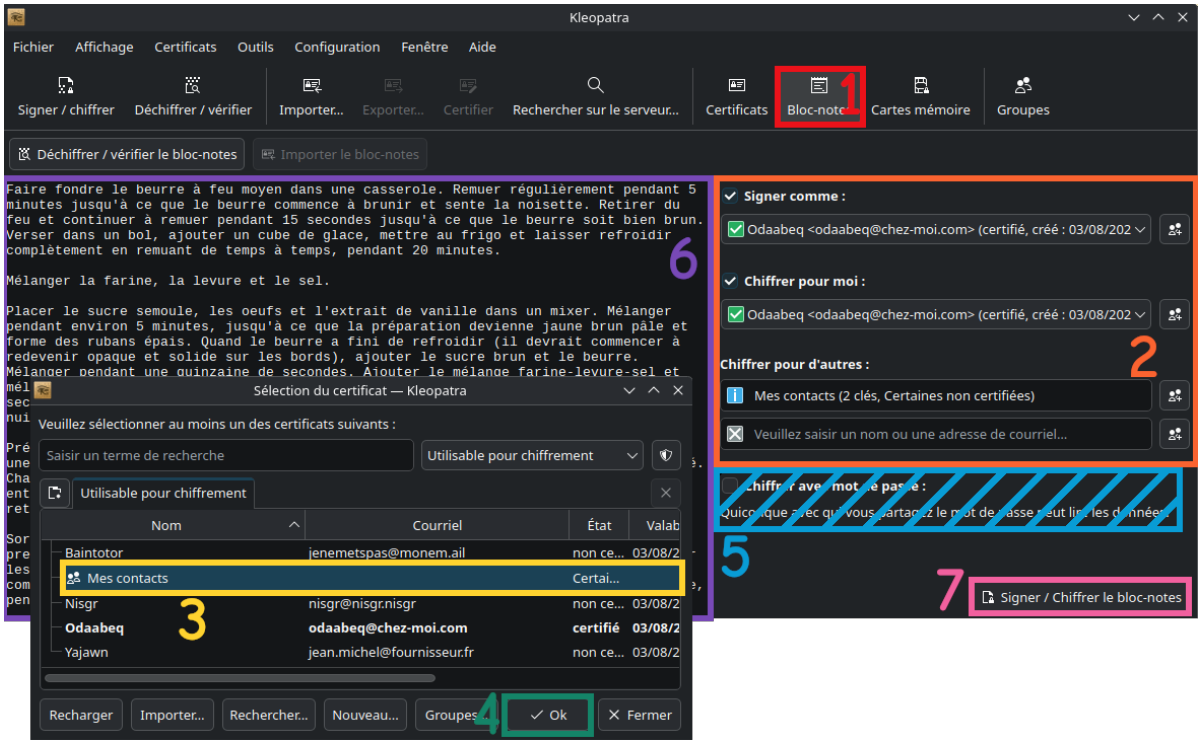

Figure 28: Chiffrer un message

« Odaabeq » chiffre un message pour « Nisgr » et « Yajawn » (Figure 28) :

1. Cliquer sur « Bloc-notes »
2. Renseigner les informations du message
   - **Signer comme** : Signature, attestant de la provenance du message
   - **Chiffrer pour moi** : Pour pouvoir déchiffrer son propre message
   - **Chiffrer pour d'autres** : Ils peuvent déchiffrer le message
3. Choisir les destinataires du message. Le groupe « Mes contacts » qui contient « Yajawn » et « Nisgr »
4. Cliquer sur « ✓ Ok »
5. **NE PAS UTILISER**, Remplace le système de certificats
6. Écrire un message
7. Cliquer sur « Signer / Chiffrer le bloc-notes ». Le mot de passe du signataire peut être demandé

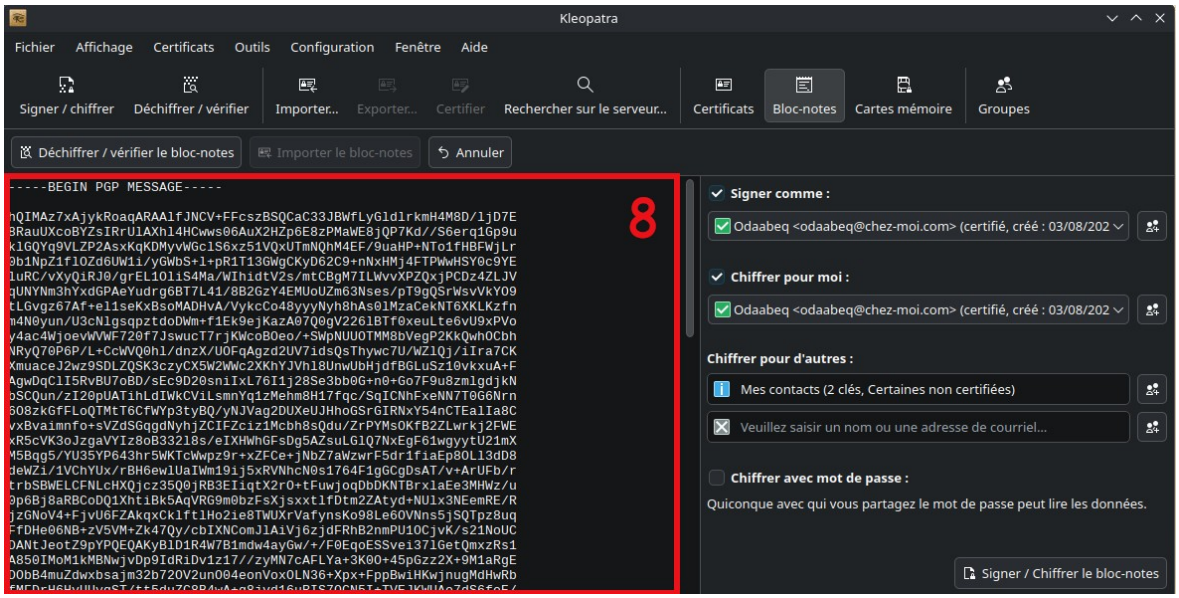

Figure 29: Le message est chiffré

8. Le message chiffré est dans la zone de texte (Figure 29). Il ne reste plus qu'à l'envoyer aux destinataires « Yajawn » et « Nisgr » qui sont les deux seuls à pouvoir déchiffrer ce message.

Déchiffrer et vérifier un message

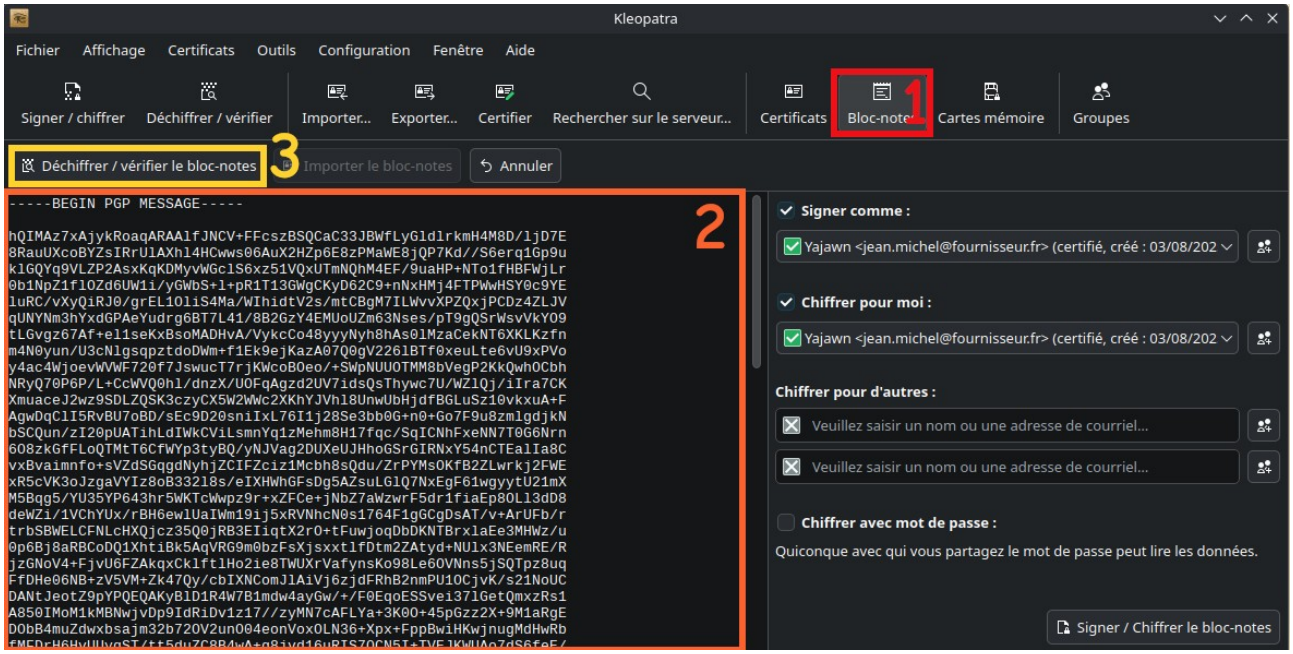

Figure 30: « Yajawn » déchiffre le message

« Yajawn » déchiffre le message envoyé par « Odaabeq » (Figure 30) :

1. Cliquer sur « Bloc-notes »
2. Copier le message chiffré
3. Cliquer sur « Déchiffrer / vérifier le bloc-notes ». « Yajawn » déchiffre le message envoyé par « Odaabeq ». « Nisgr » pourrait faire de même, il fait partie des destinataires du message

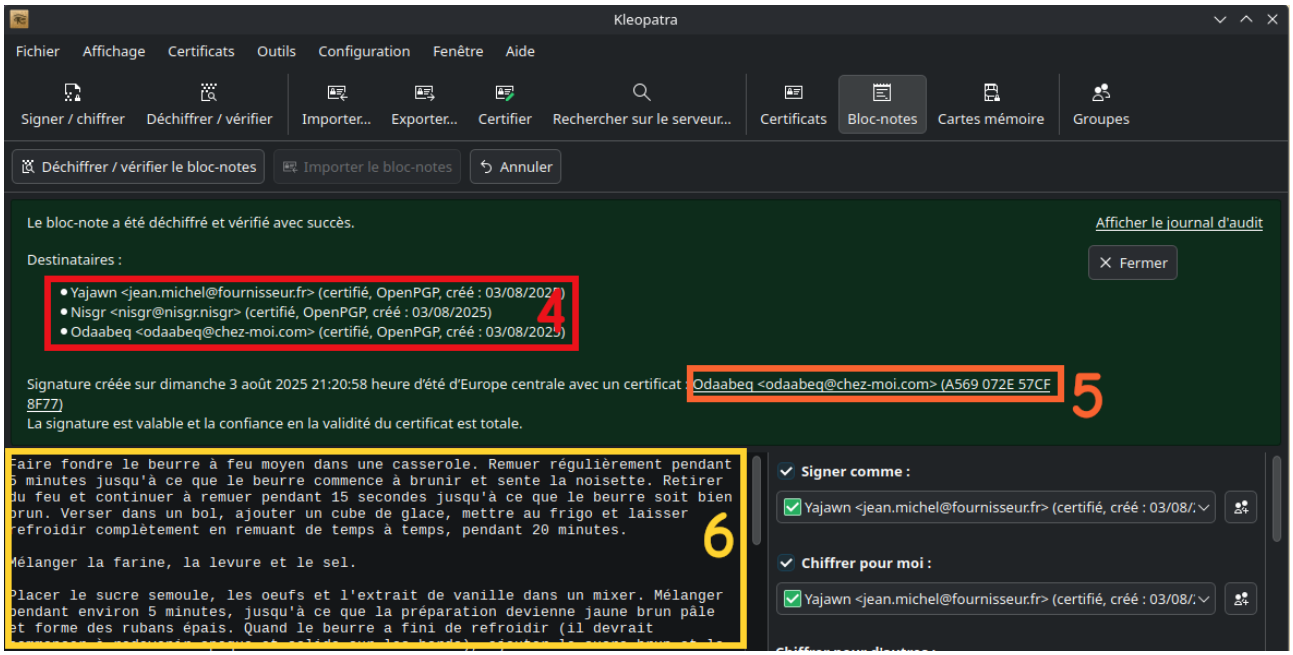

Figure 31: Message déchiffré

Le message est déchiffré (Figure 31) :

4. La liste des destinataires, « Yajawn », « Nisgr » et aussi « Odaabeq » qui a chiffré le message pour lui-même
5. La signature qui permet d'attester que seul « Odaabeq » aurait pu écrire ce message
6. Le contenu du message déchiffré

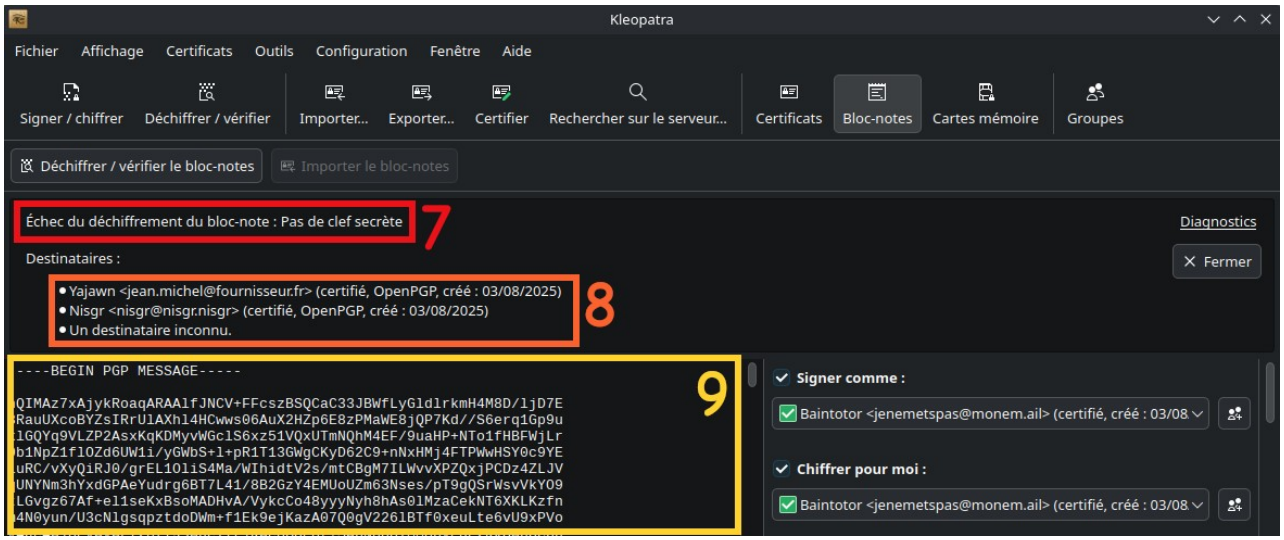

Figure 32: « Baintotor » tente de déchiffrer le message

« Baintotor » a intercepté le message et tente de le déchiffrer (Figure 32) :

7. Le déchiffrement n'a pas fonctionné. La clé secrète de « Baintotor » ne fonctionne pas sur ce message qui a été chiffré avec les certificats de « Yajawn », « Nisgr » et « Odaabeq ». Une clé secrète n'ouvre que les messages qui ont été chiffrés avec le certificat correspondant
8. « Baintotor » a ajouté les certificats de « Yajawn » et « Nisgr », il peut voir qu'ils font partie des destinataires. Il n'a pas ajouté le certificat d'« Odaabeq » qui apparaît comme « Un destinataire inconnu. »
9. Le contenu du message reste chiffré

Chiffrer et signer un fichier

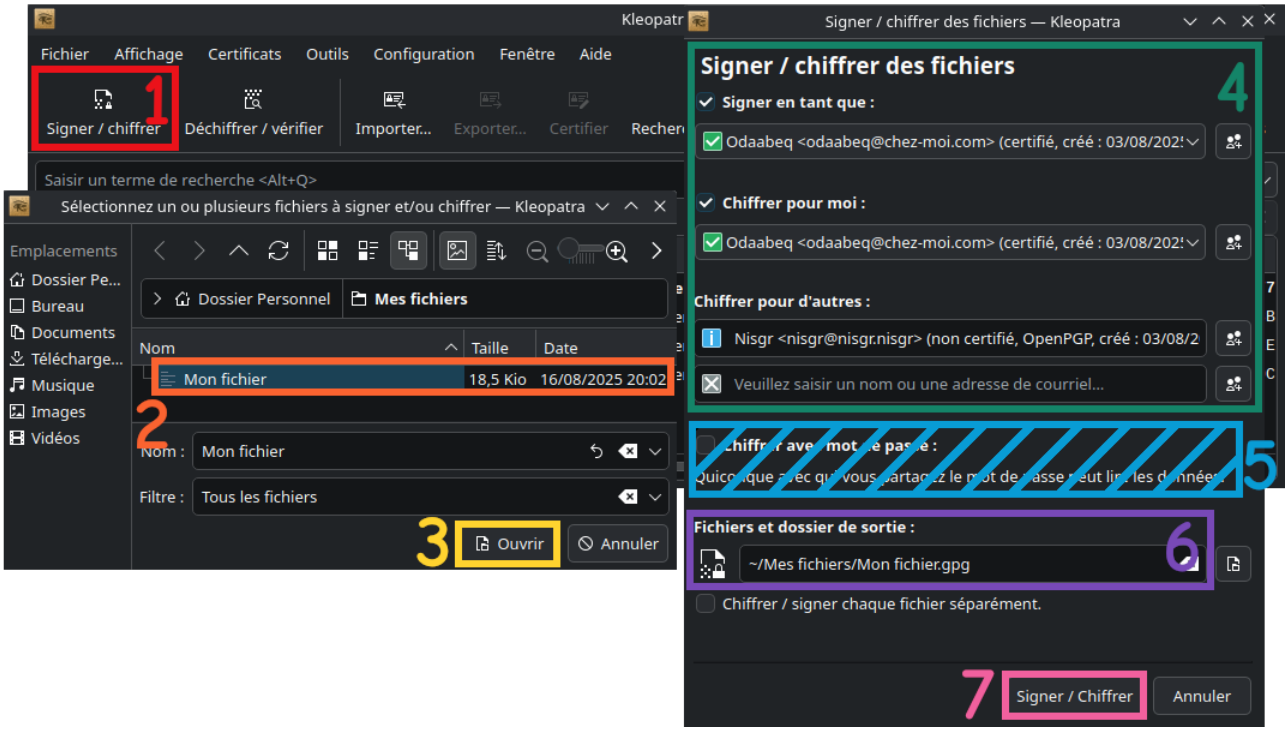

Figure 33: Chiffrer et signer un fichier

« Odaabeq » chiffre un fichier pour « Nisgr » (Figure 33) :

1. Cliquer sur « Signer / Chiffrer »
2. Sélectionner un fichier
3. Cliquer sur « Ouvrir »
4. Renseigner les informations, le fichier est chiffré pour « Nisgr » :
   - **Signer en tant que** : Atteste la provenance du fichier
   - **Chiffrer pour moi** : Pour pouvoir déchiffrer son propre fichier
   - **Chiffrer pour d'autres** : Ils peuvent déchiffrer le fichier
5. **NE PAS UTILISER**, Remplace le système de certificats
6. Choisir un emplacement pour enregistrer le fichier chiffré
7. Cliquer sur « Signer / Chiffrer ». Le mot de passe du signataire peut être demandé

Déchiffrer et vérifier un fichier

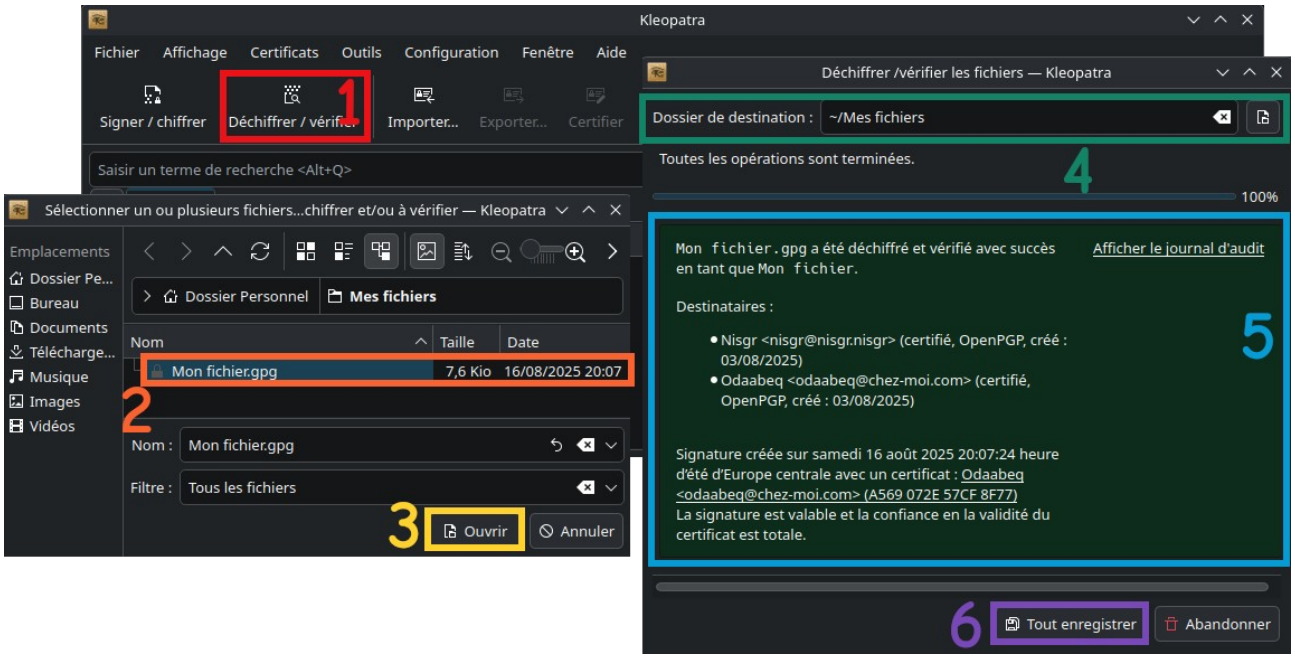

Figure 34: Déchiffrer et vérifier un fichier

« Nisgr » déchiffre et vérifie le fichier envoyé par « Odaabeq » (Figure 34) :

1. Cliquer sur « Déchiffrer / vérifier »
2. Sélectionner le fichier à déchiffrer
3. Cliquer sur « Ouvrir »
4. Choisir ou enregistrer le fichier
5. Comme pour les messages, les informations des destinataires ainsi que la signature du fichier apparaissent lors de l'opération de déchiffrement. Dans cet exemple, « Nisgr » déchiffre le fichier envoyé par « Odaabeq »
6. Cliquer sur « Tout enregistrer »

Le fichier est désormais déchiffré et accessible à l'emplacement choisi.