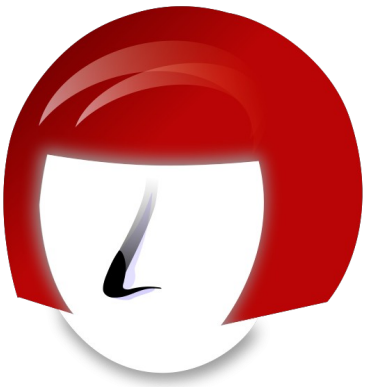
Guide d’utilisation de GPG avec Kleopatra



Kleopatra

Crypto Manager

Table des matières

Introduction

Ce guide détaille l'utilisation de GPG à l'aide de l'interface graphique Kleopatra.

GPG[1] est un logiciel permet la transmission de messages électroniques signés et chiffrés, garantissant ainsi leurs authenticité, intégrité et confidentialité.

Kleopatra[2] est un gestionnaire de certificats et une interface graphique pour GnuPG. Le logiciel stocke vos certificats et clés OpenPGP. Il est disponible pour Windows, Mac et Linux.

La première partie décrit la procédure d'installation de GPG et Kleopatra sous Windows, Mac et Linux. (TODO : ANDROID, IOS)

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

La troisième partie présente des concepts et définitions de la cryptographie qui sont couramment utilisées, notamment dans ce guide.

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

Installation

Windows

Gpg4win[3] (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

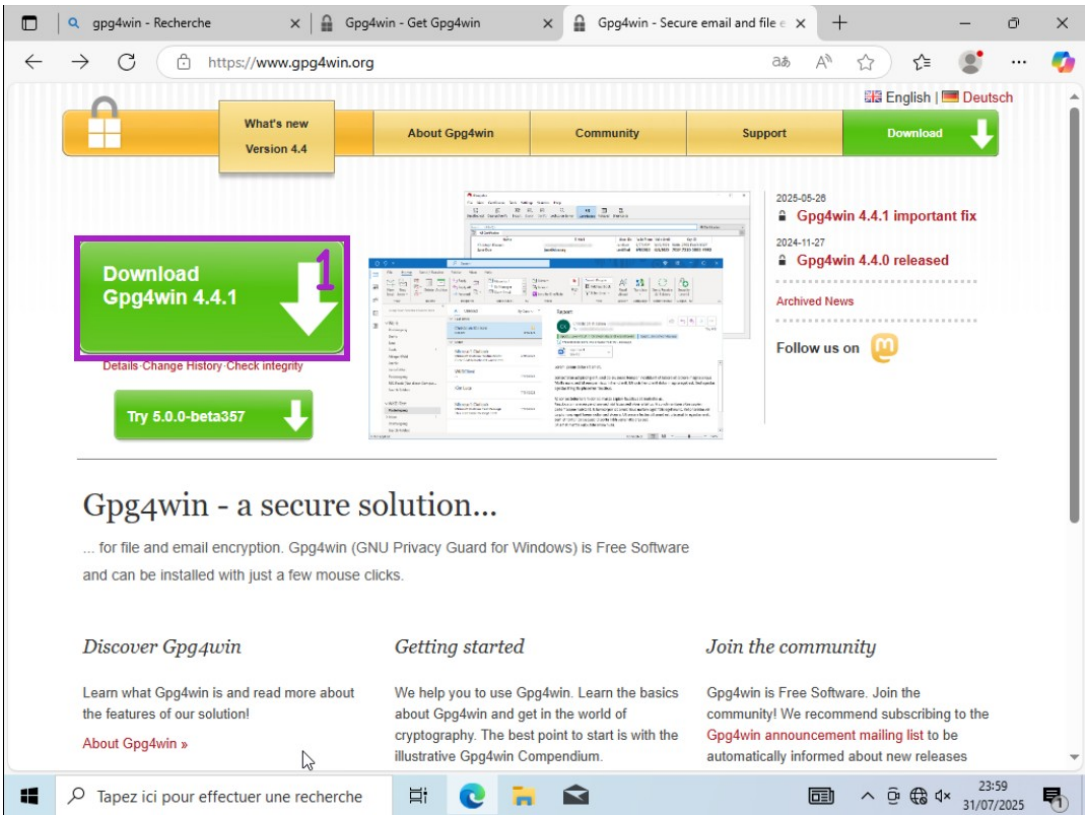


Figure 1: Site de Gpg4win

Une fois sur le site de Gpg4win (Figure 1) :

1. Cliquer sur le bouton « Download Gpg4win »

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

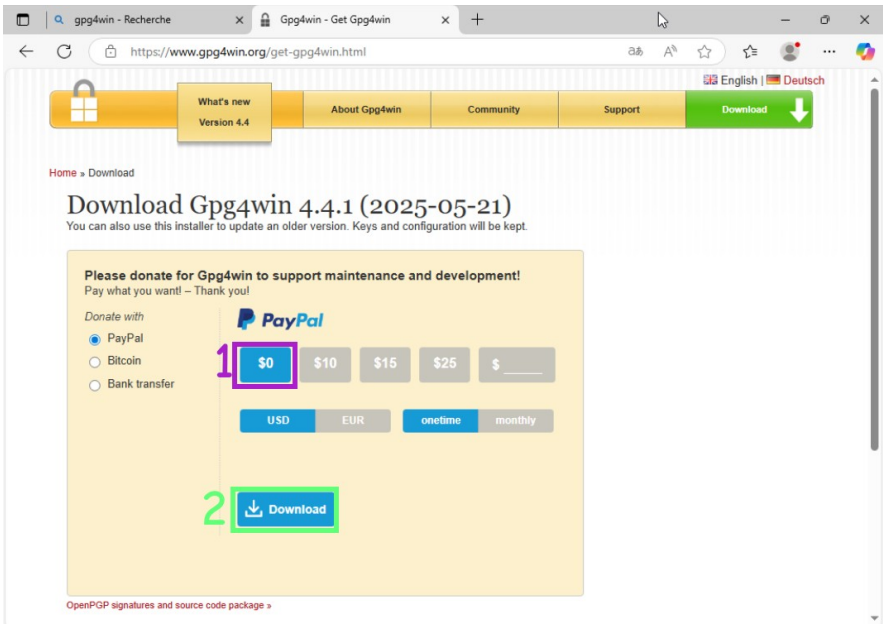


Figure 2: Page de téléchargement

Sur la page de téléchargement (Figure 2) :

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

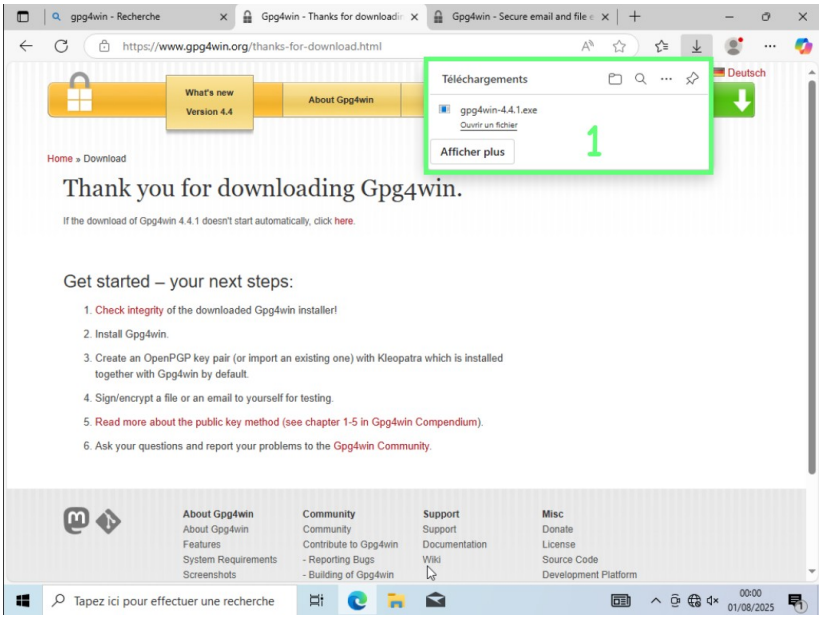


Figure 3: Téléchargement terminé

Une fois le téléchargement terminé (Figure 3) :

1. Cliquer sur « Ouvrir un fichier »

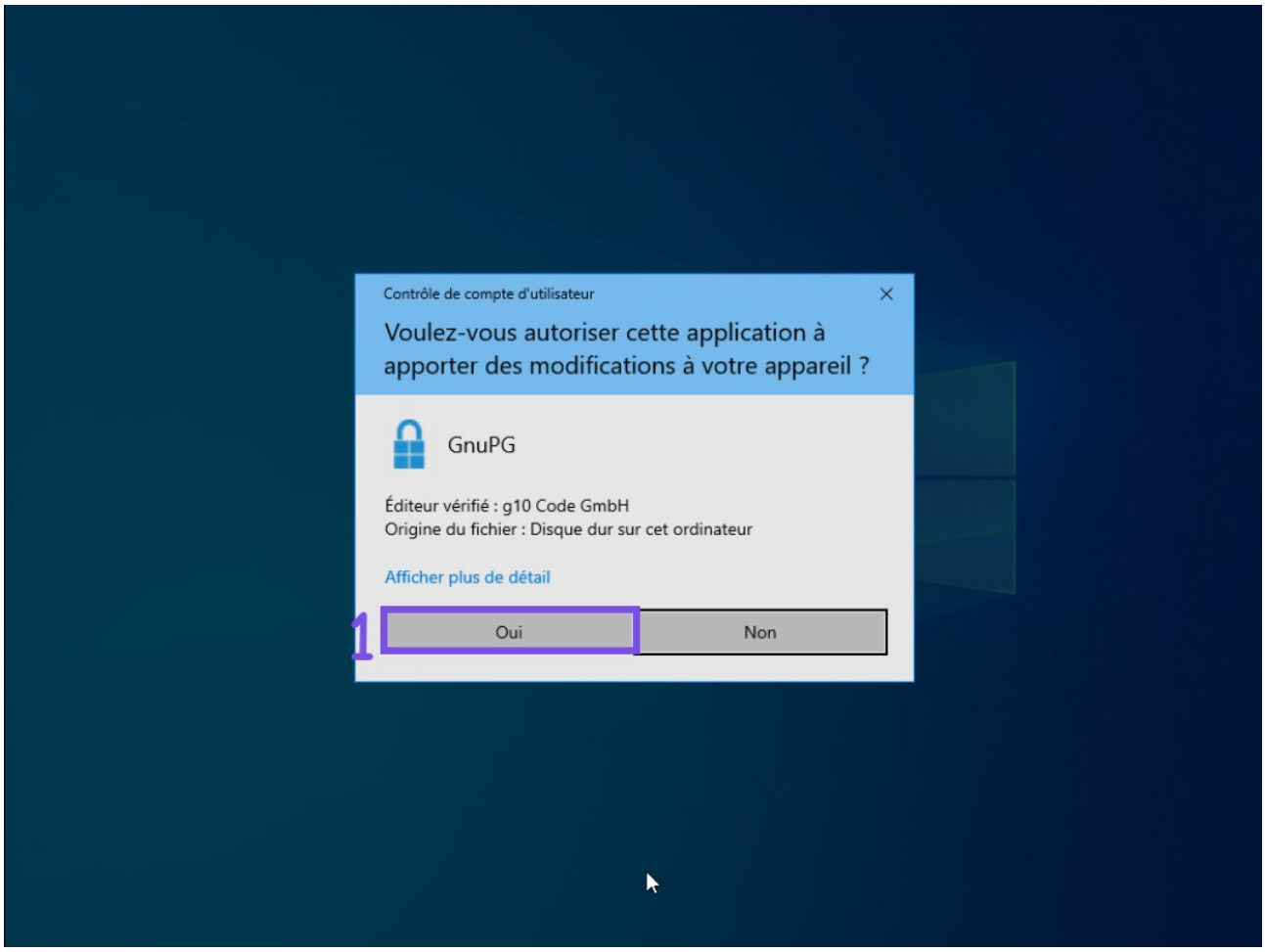


Figure 4: Autorisation windows

Autoriser Windows à lancer l'application (Figure 4) :

1. Cliquer sur Oui.

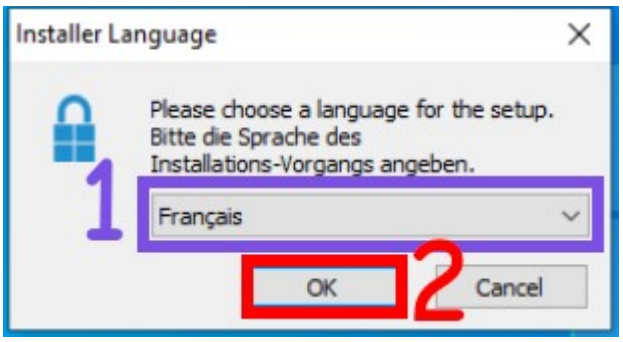


Figure 5: Choix langue

Sélectionner la langue (Figure 5) :

1. Choisir la langue d'installation
2. Cliquer sur « OK »

Figure 6: Installation de Gpg4win

Dans la fenêtre d'installation (Figure 6) :

1. Cliquer sur « suivant > »

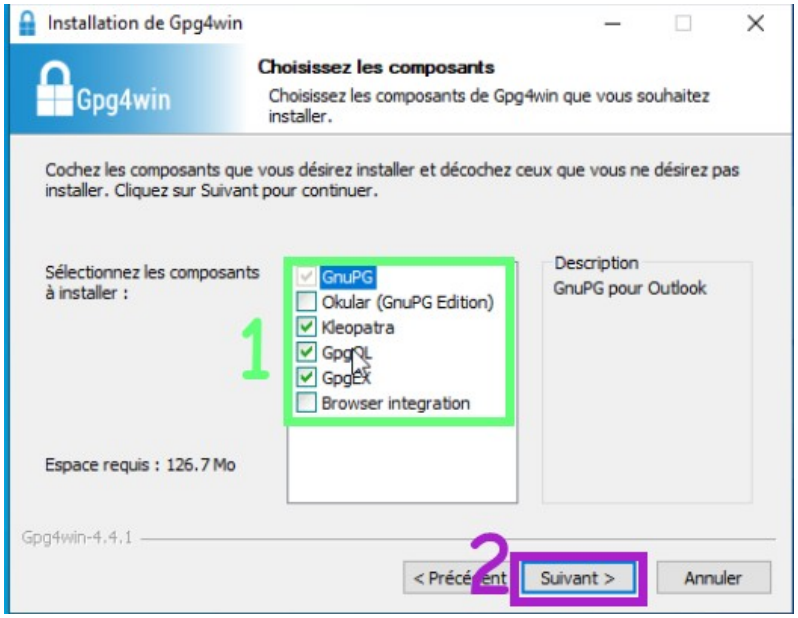


Figure 7: Choix des composants

Dans la fenêtre de choix des composants (Figure 7) :

1. Laisser par défaut (GnuPG, Kleopatra, GpgOL, GpgEX).
2. Cliquer sur « suivant ».

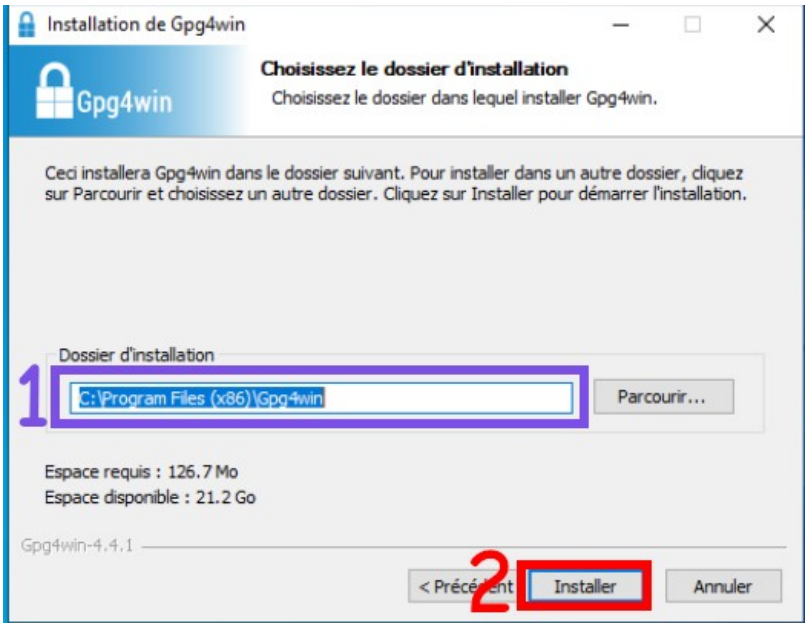


Figure 8: Dossier d'installation

Dans la fenêtre de sélection du dossier d'installation (Figure 8) :

1. Choisir l'emplacement du dossier d'installation.
2. Cliquer sur « Installer ».

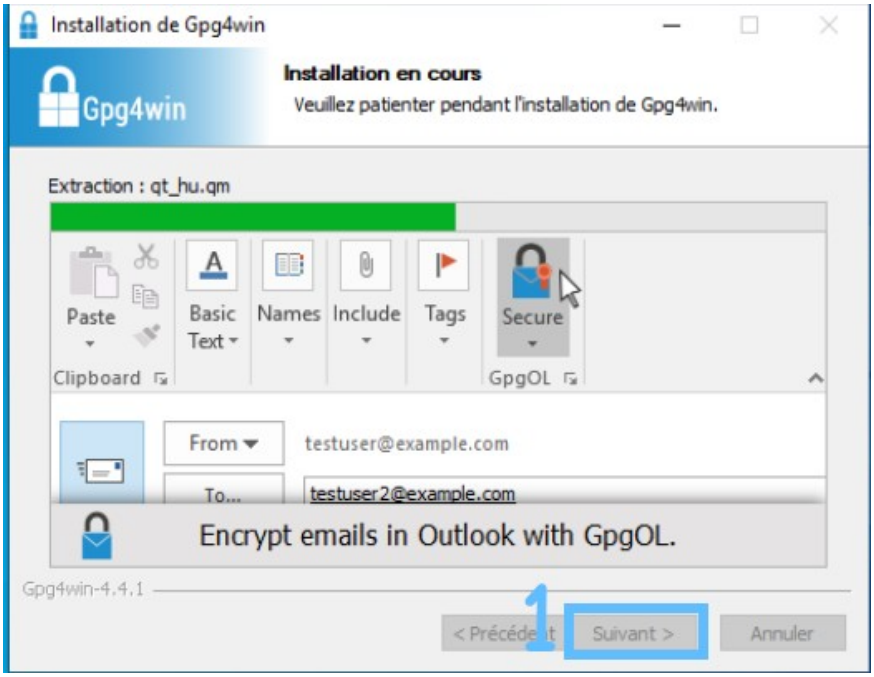


Figure 9: Installation en cours

L'installation est en cours (Figure 9) :

1. Une fois terminé, cliquer sur « Suivant > ».

Figure 10: Installation terminée

L'installation est terminée (Figure 10) :

1. Laisser sélectionner pour lancer Kleopatra à la fermeture.
2. 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 GPG avec Kleopatra

La suite du guide explique comment utiliser Kleopatra à l'aide de captures d'écran commentées. On y suivra un exemple de configuration pour l'utilisateur « je mets mon nom ici », qui souhaite envoyer un message à ses contacts « titi », « tata » et « toto ».

À l'issue de ce guide, vous devriez pouvoir :

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

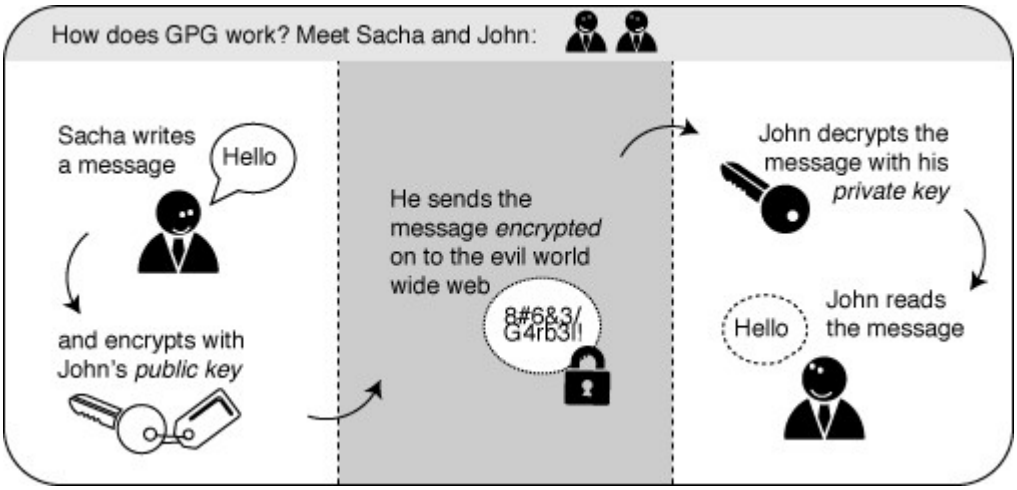


Figure 11: Open PGP encryption and decryption example

Le fonctionnement :

1. Chaque utilisateur possède sa clé privée (son certificat, son identité en quelque sorte), la clé privée est la seule qui permette de déchiffrer un message qui lui est destiné.
2. Chaque utilisateur possède une clé publique, qui est dérivée de cette clé privée. Elle permet de chiffrer un message. C'est celle qu'on envoie à tous ses contacts.
3. Lorsqu'un message est écrit, il est chiffré à l'aide de la clé publique d'un de ses contacts, ainsi seul ce contact peut déchiffrer le message.

Découverte de l'interface

Au lancement, Kleopatra affiche le résultat de ses tests internes (Figure 12). Le seul qui échoue « scdaemon » sert pour les lecteurs de cartes. Il n'est pas nécessaire pour la suite.

- Cliquer sur « ✓ Continuer » pour passer à la suite

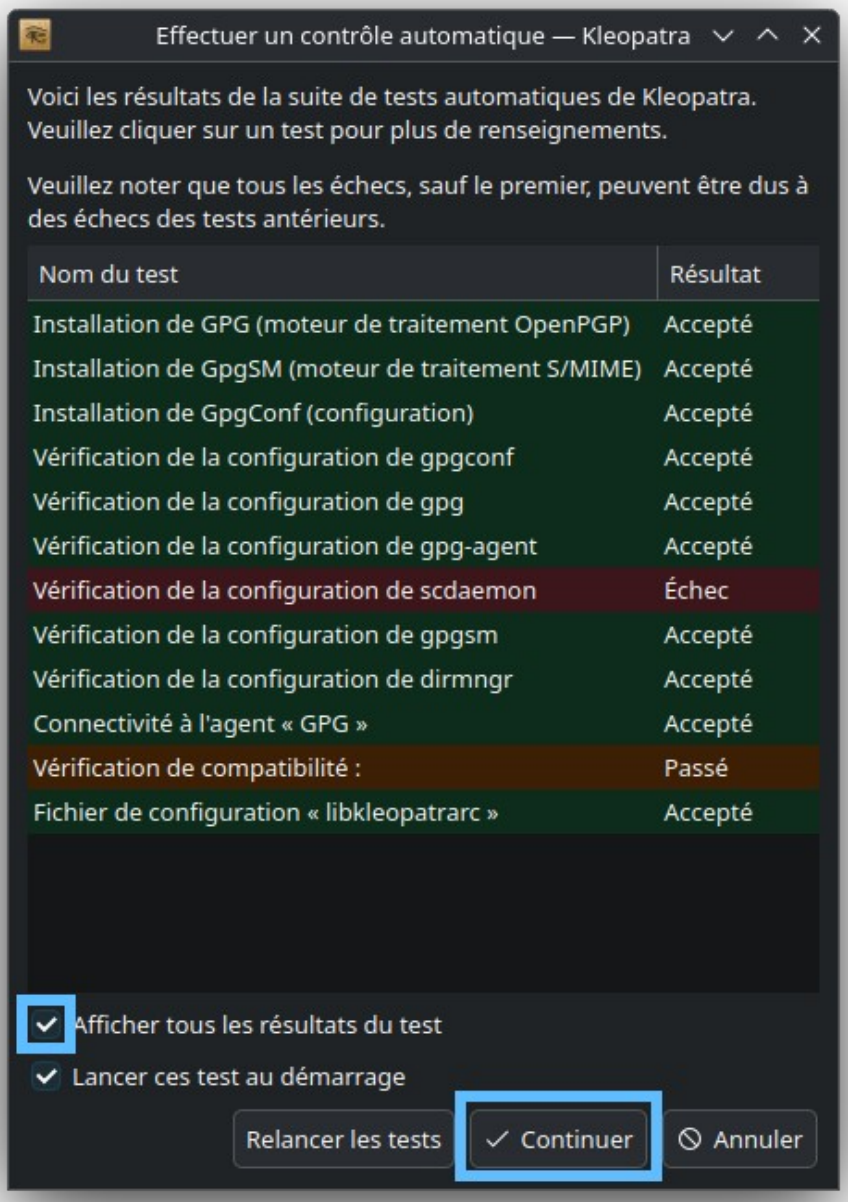


Figure 12: Contrôle automatique

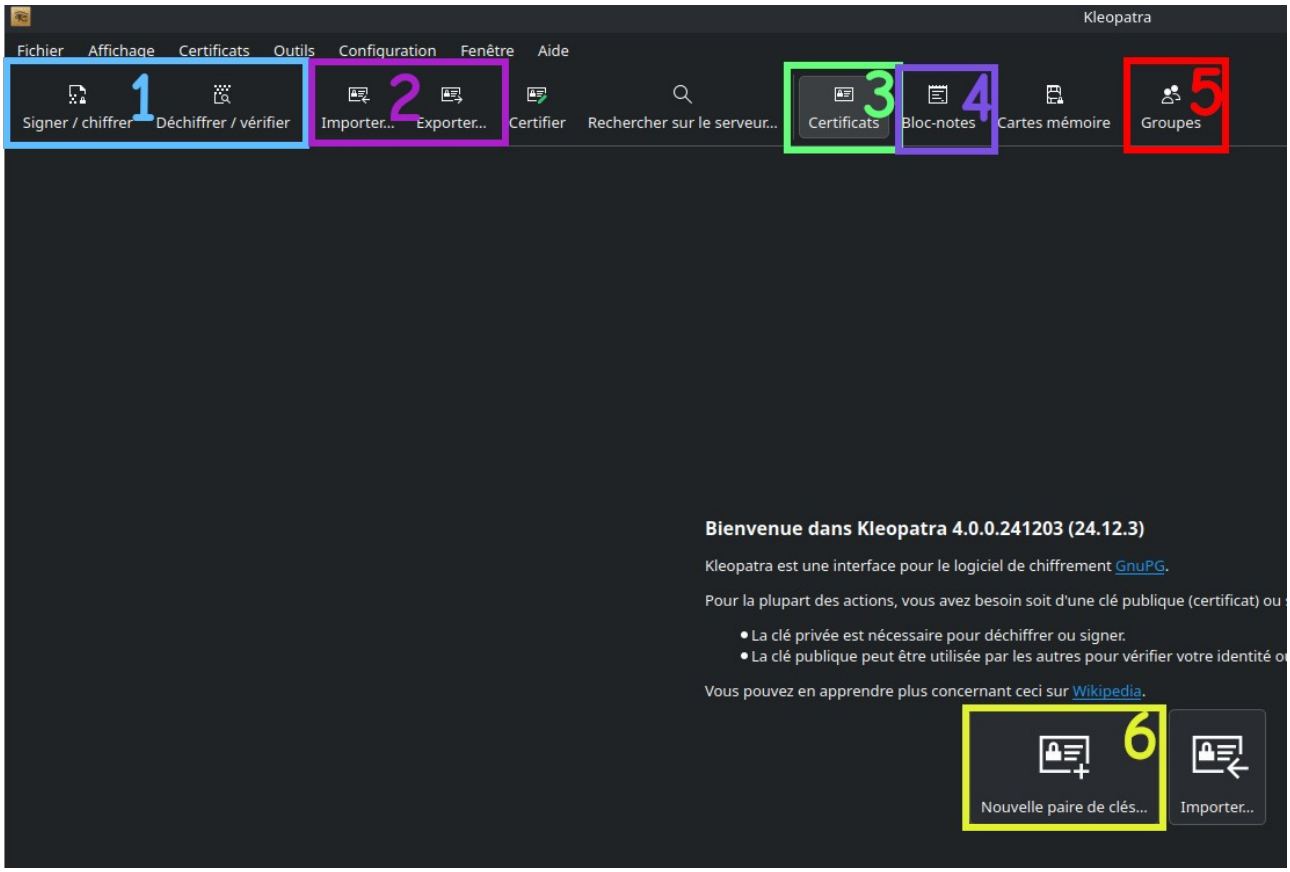


Figure 13: Interface de Kleopatra

Présentation de l'interface (Figure 13) :

1. Ces deux boutons servent à manipuler des fichiers, ils permettent de les chiffrer/déchiffrer ainsi que Signer/Vérifier. Les parties suivantes donneront plus de détail sur ces différentes opérations.
2. Ces boutons servent à importer les clés publiques de vos contacts et exporter votre clé publique.
3. C'est la liste des clés que vous connaissez, vous y trouverez vos contacts. Pour l'instant, c'est vide.
4. Le bloc-note permet d'effectuer des opérations cryptographiques sur du texte.
5. Permet d'organiser ses contacts sous forme de groupes pour simplifier les opérations cryptographiques.
6. Cliquer sur « Nouvelle paire de clés... » pour passer à la suite.

Créer un certificat

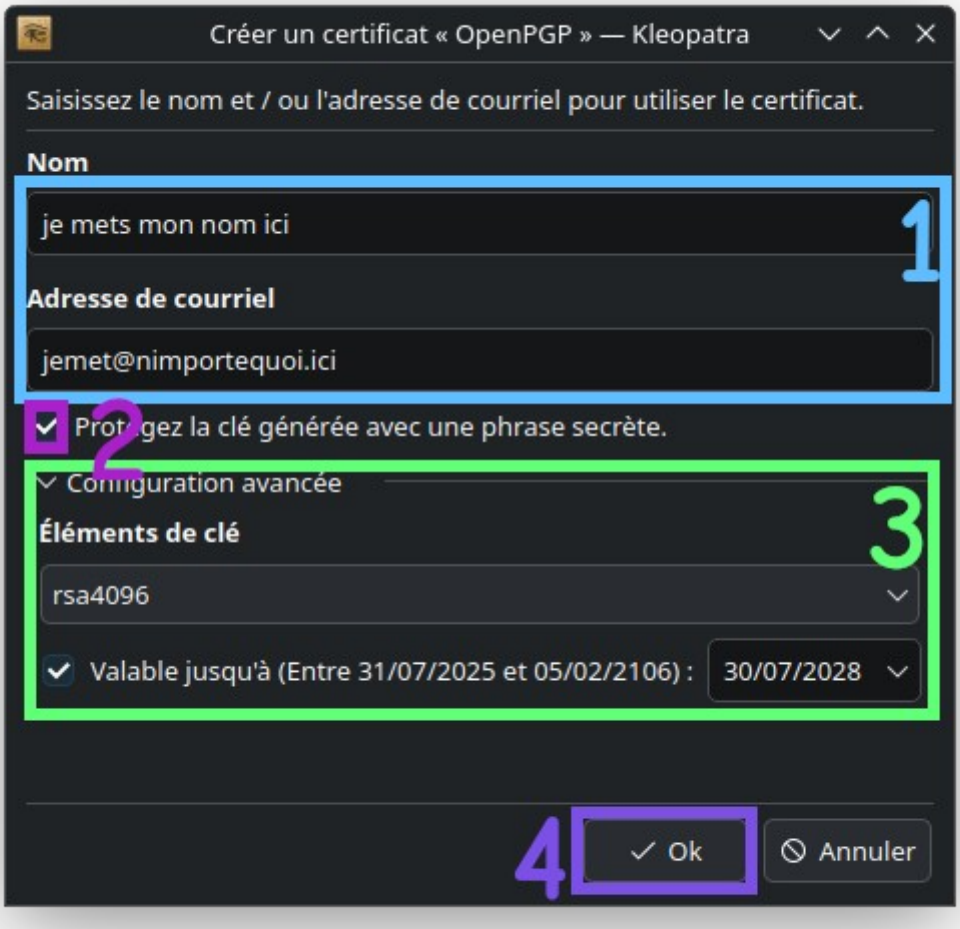


Figure 14: Créer un certificat

Pour créer un nouveau certificat (Figure 14) :

1. Saisie du nom et d'un e-mail (C'est possible de mettre n'importe quoi à la place de l'e-mail.).
2. **Important** : La clé doit être protégée avec un mot de passe afin de se prémunir contre les vols.
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.

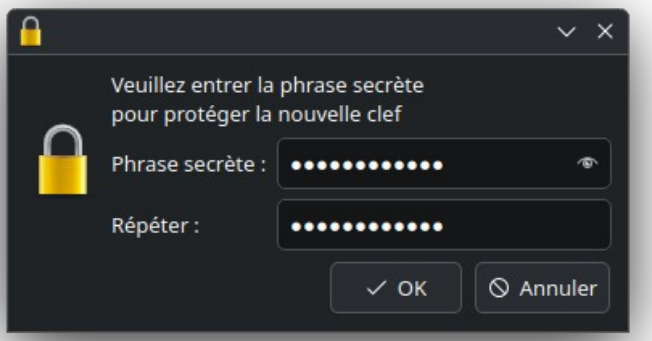


Figure 15: Saisie de mot de passe

5. Saisir un mot de passe (Figure 15).
6. Cliquer sur « ✓ Ok » pour passer à la suite.

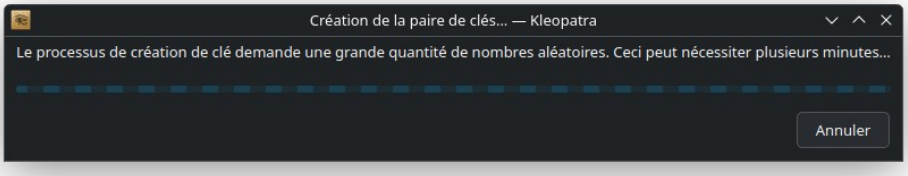


Figure 16: Création en cours

7. Attendre la fin de la création (Figure 16).

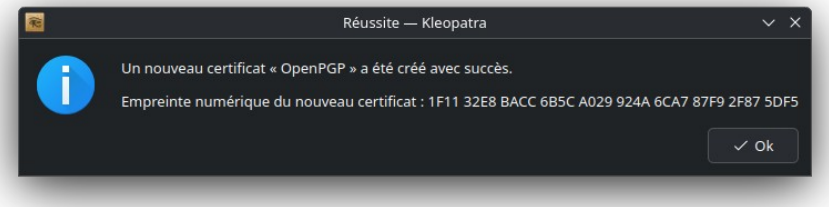


Figure 17: Création réussie

8. Cliquer sur « ✓ Ok » pour passer à la suite (Figure 17).
9. Si besoin, pour créer une nouvelle paire, faire : Fichier → Nouvelle paire de clés « OpenPGP »…

Sauvegarder sa clé privée

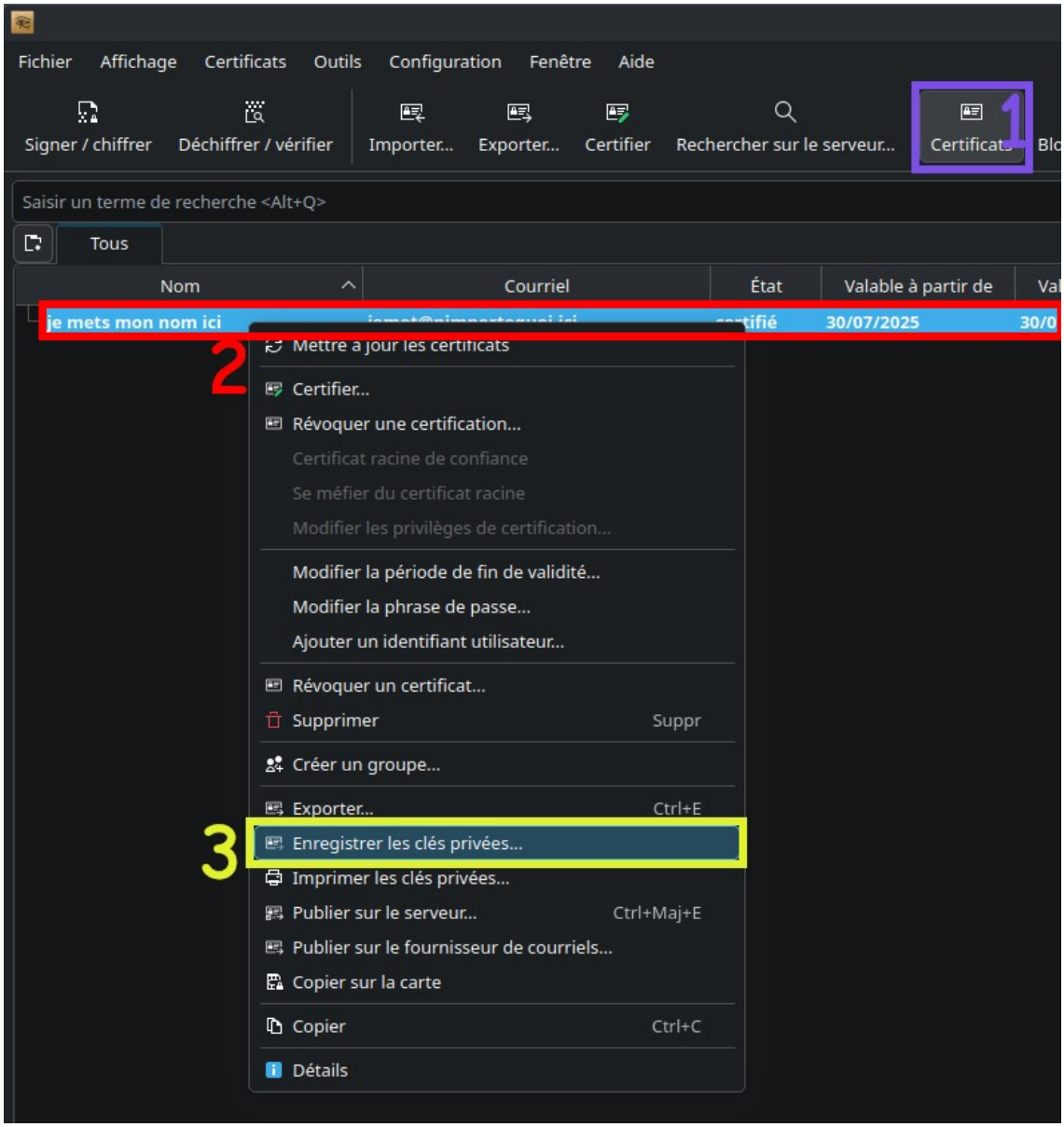


Figure 18: Enregistrer clés privées

Pour réaliser une copie de secours de sa clé privée (Figure 18) :

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

Exporter sa clé publique

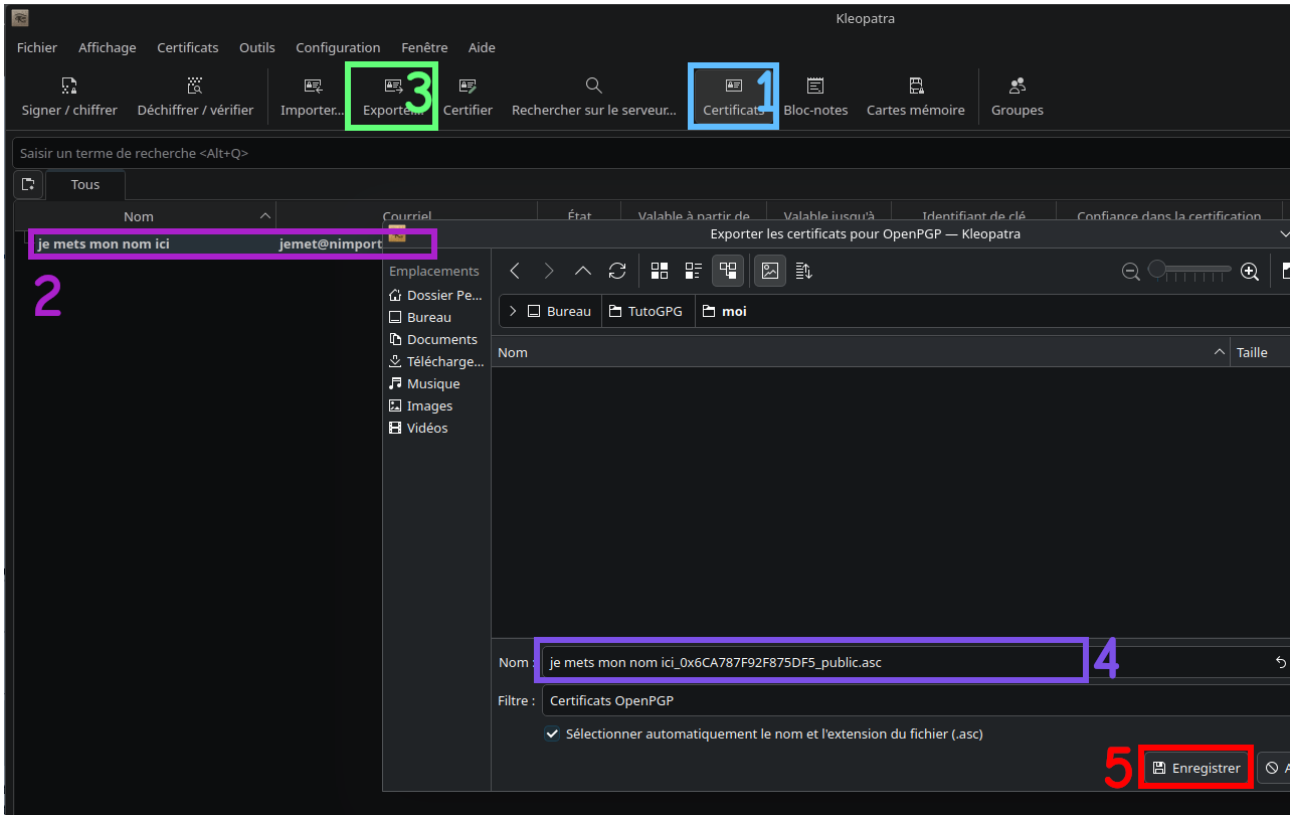


Figure 19: Exporter clé publique

Pour exporter sa clé publique (Figure 19) :

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.

Importer des clés

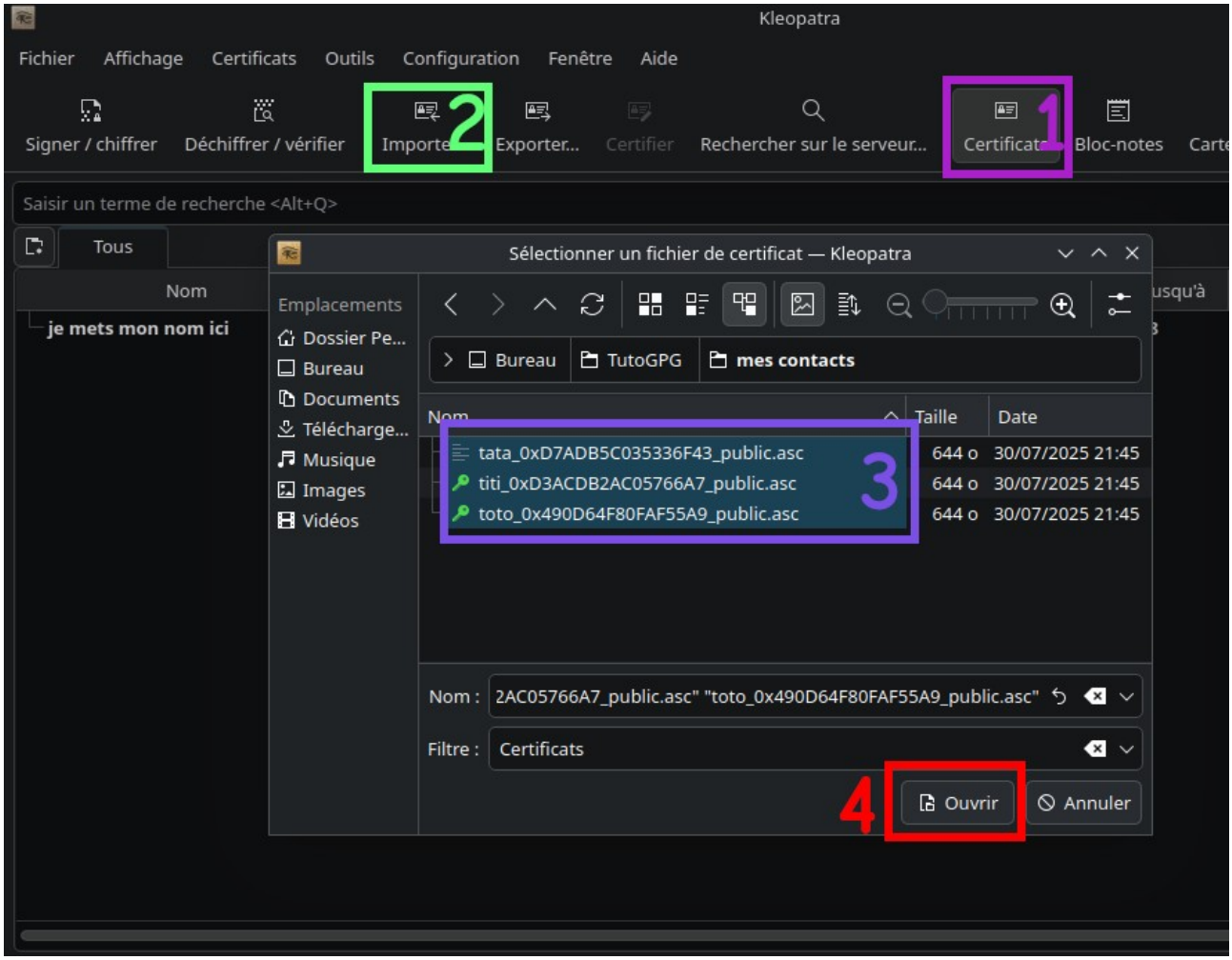


Figure 20: Importer des clés

Pour importer les clés de ses contacts (Figure 20) :

1. Dans le menu « Certificats ».
2. Cliquer sur Importer.
3. Sélectionner les clés publiques des contacts.
4. Cliquer sur Ouvrir
5. 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 mon empreinte

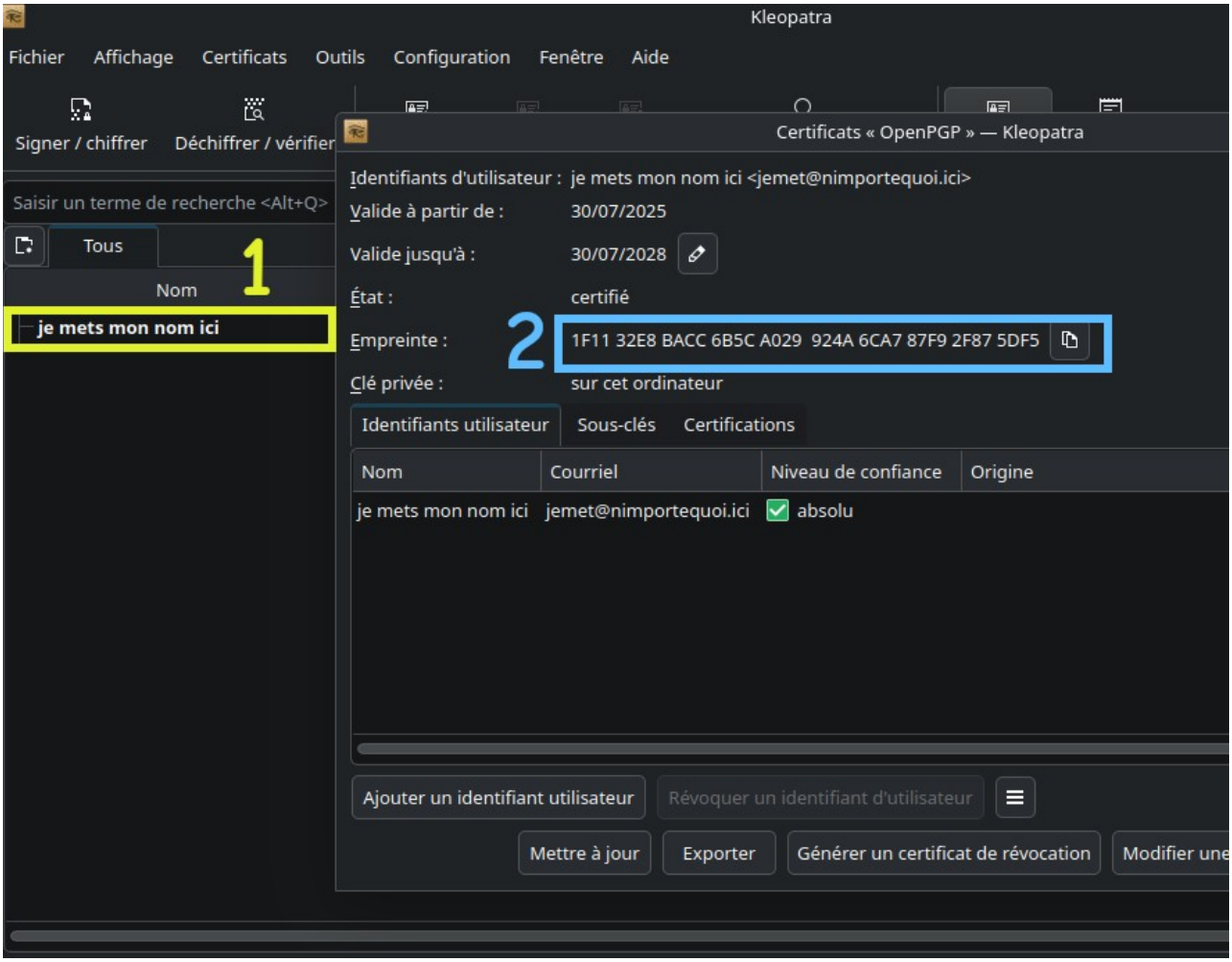


Figure 21: Récupérer son empreinte

Pour récupérer mon empreinte (Figure 21) :

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'échange des clés.

Certifier un contact

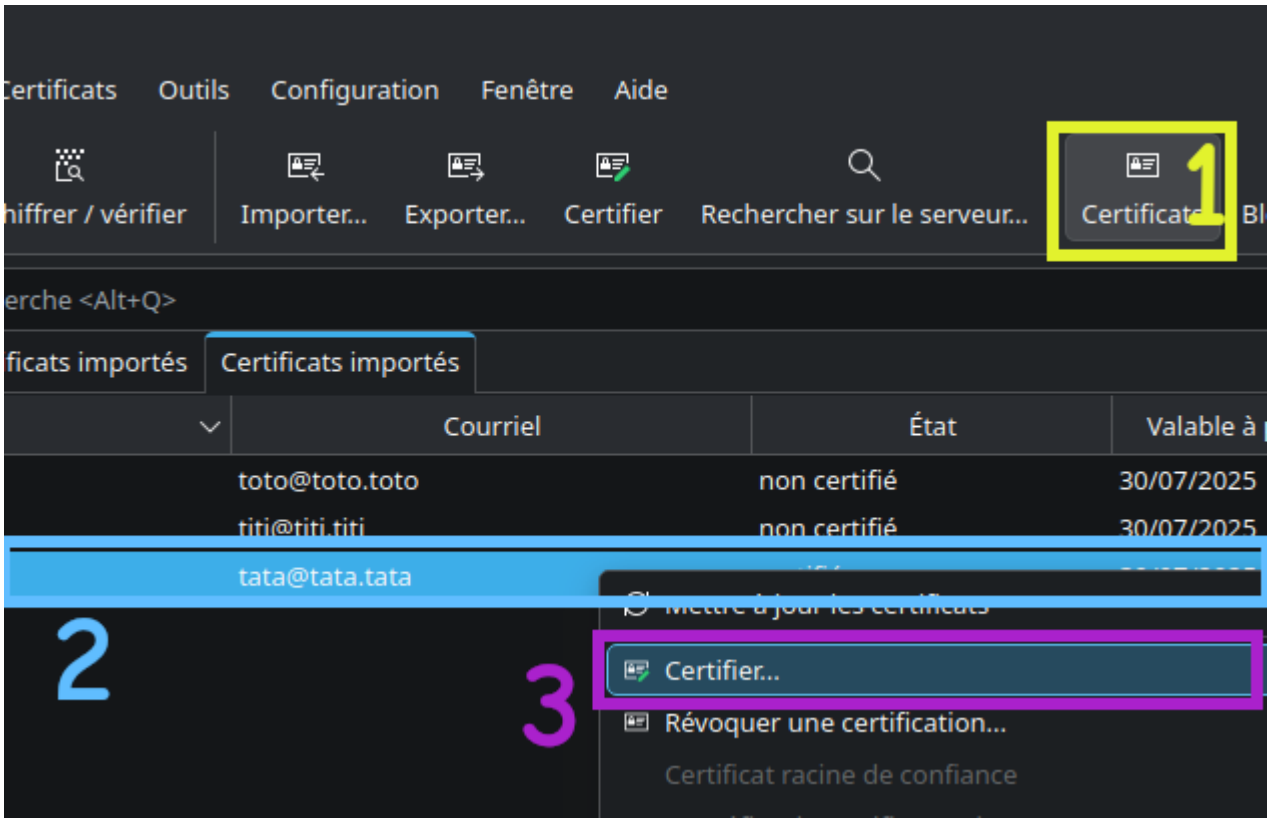


Figure 22: Ouvrir menu de certification

Pour certifier un contact (Figure 22) :

1. Dans le menu certificats.
2. Clic droit sur le contact à certifier.
3. Dans le menu déroulant, choisir « Certifier... ».

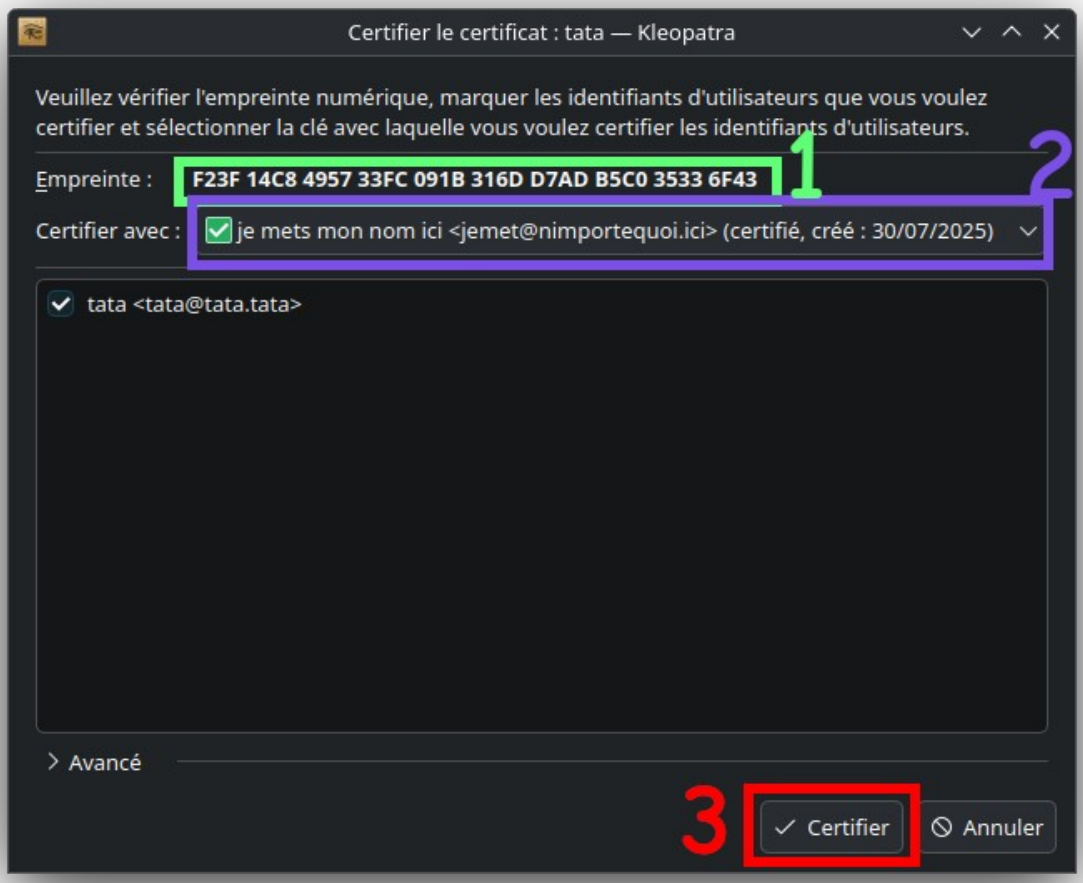


Figure 23: Certification d'un contact

Pour valider la certification (Figure 23) :

1. Vérifier que l'empreinte correspond bien à celle transmise par le contact.
2. Choisir l'identité avec laquelle valider la certification.
3. Cliquer sur « ✓ Certifier ». Le mot de passe du certificat qui valide peut être demandé.

Créer un groupe

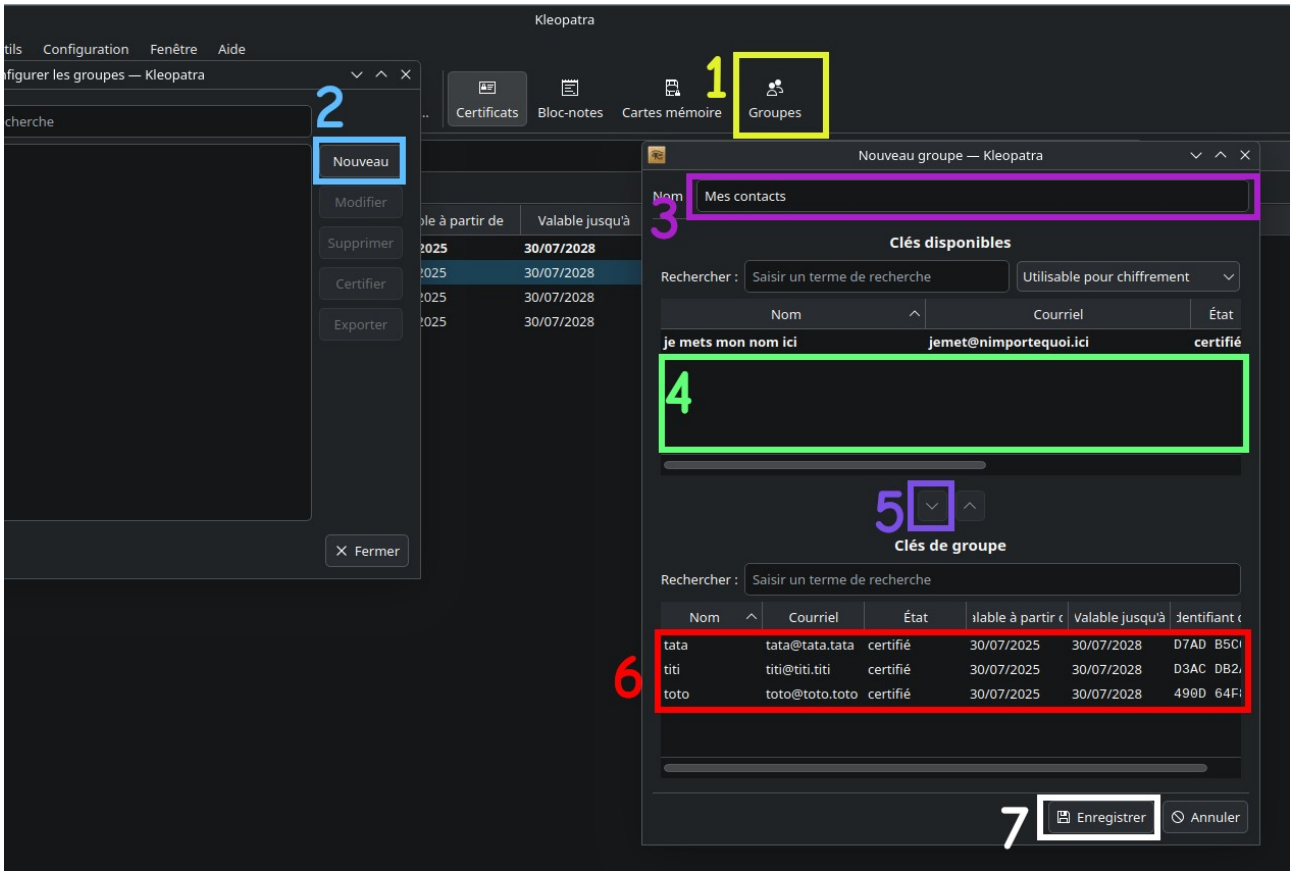


Figure 24: Création de groupe

Pour créer un groupe contenant les contacts (Figure 24) :

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.
7. Cliquer sur « Enregistrer ».

Chiffrer et signer un message

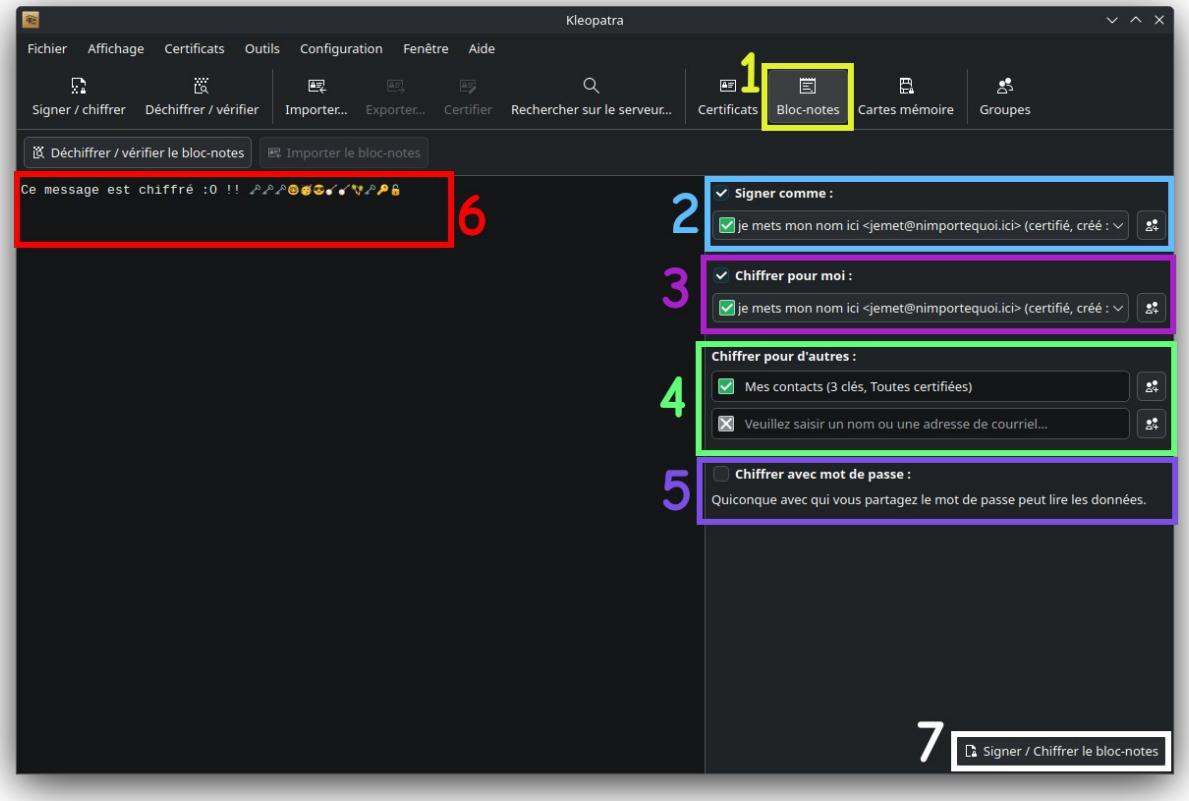


Figure 25: Chiffrer un message

Pour chiffrer un message (Figure 25) :

1. Cliquer sur « Bloc-notes ».
2. Signe le message avec l'identité sélectionnée (certificat).
3. Chiffrer pour moi permet de s'ajouter à la liste des destinataires, ce qui permet de déchiffrer ses propres messages.
4. Sélectionner les destinataires. Il est possible d'utiliser des groupes.
5. Chiffrer avec un mot de passe **remplace complètement** le système de certificats et permet à **n'importe qui** disposant du mot de passe d'en consulter le contenu.
6. Écrire un message.
7. Cliquer sur « Signer / Chiffrer le bloc-notes ». Le mot de passe du signataire peut être demandé.

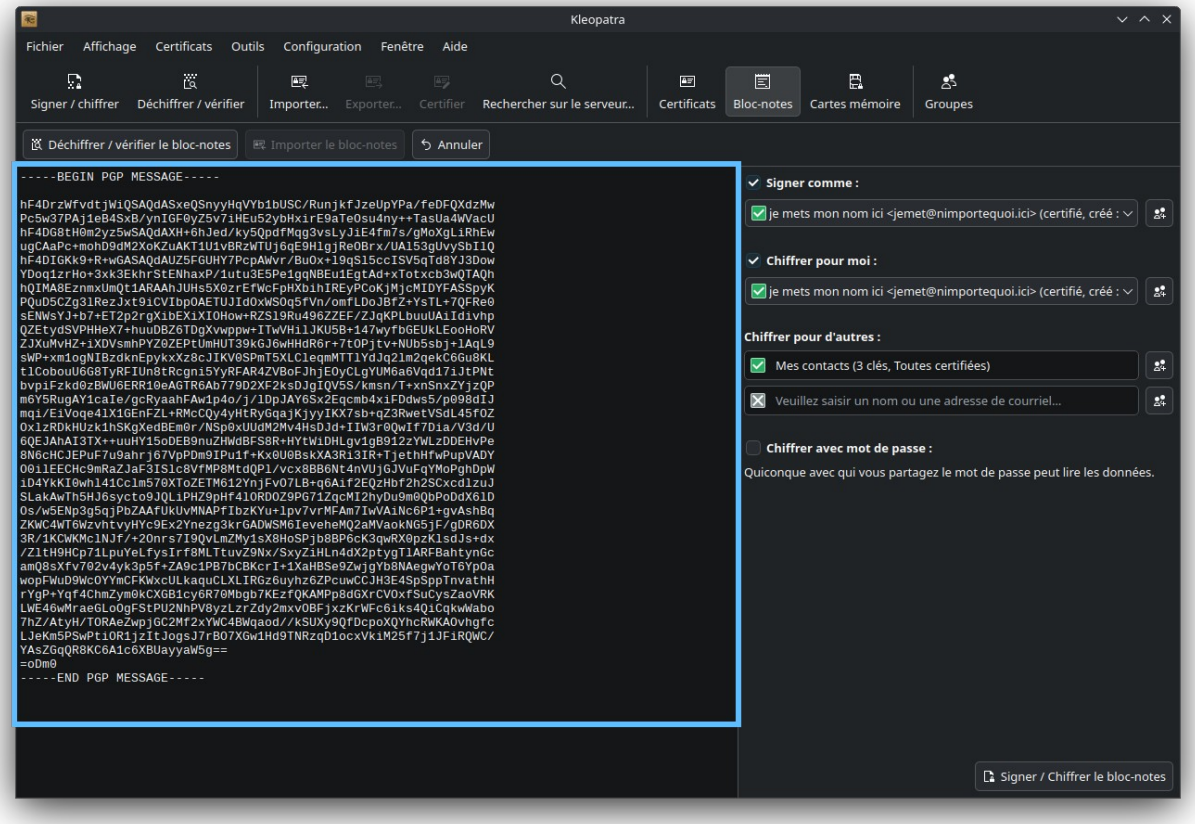


Figure 26: Le message est chiffré

Le message chiffré est dans la zone de texte (Figure 26). Il ne reste plus qu'à l'envoyer aux destinataires.

Déchiffrer et vérifier un message

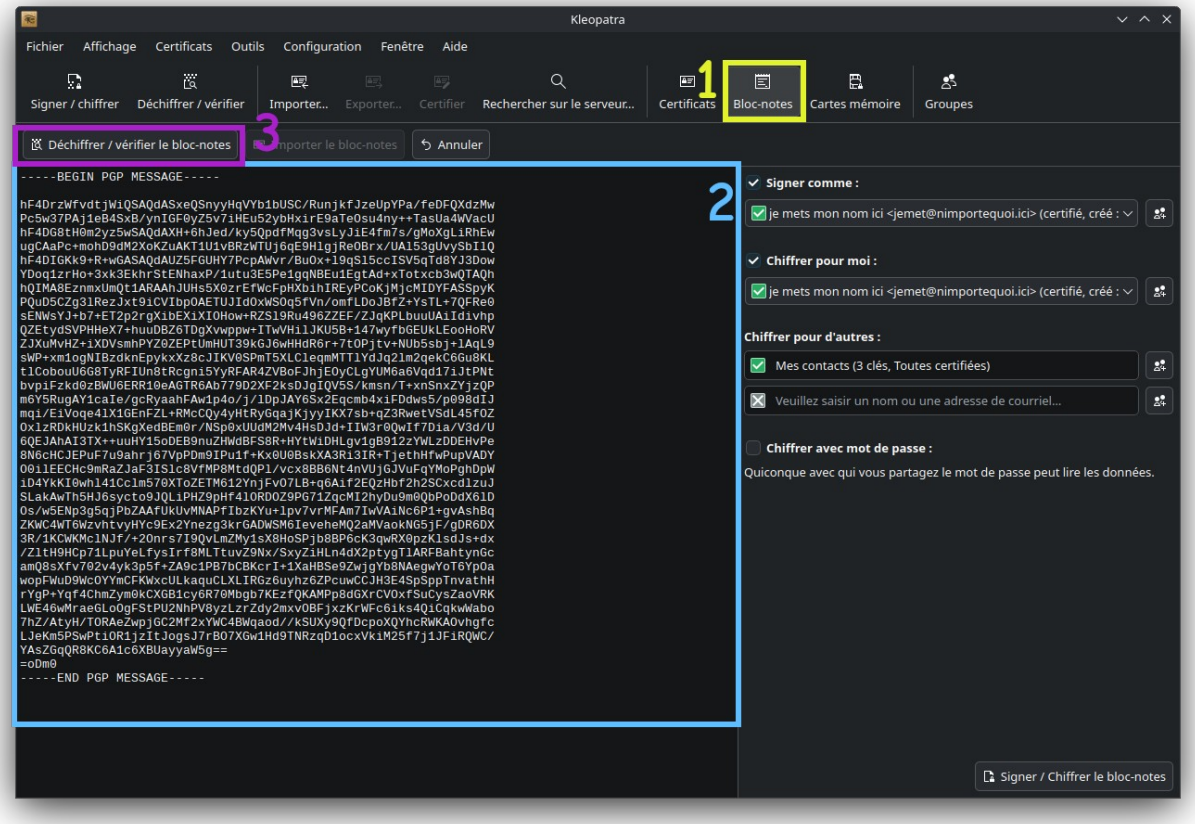


Figure 27: Déchiffrage d'un message

Pour déchiffrer un message (Figure 27) :

- Il faut faire partie des destinataires. Si par exemple, je suis « titi », je suis l'unique possesseur de la clé privée de « titi ». C'est la seule clé qui me permette de déchiffrer les messages qui sont à destination de « titi ».

1. Cliquer sur « Bloc-notes ».
2. Copier le message chiffré
3. Cliquer sur « Déchiffrer / vérifier le bloc-notes »

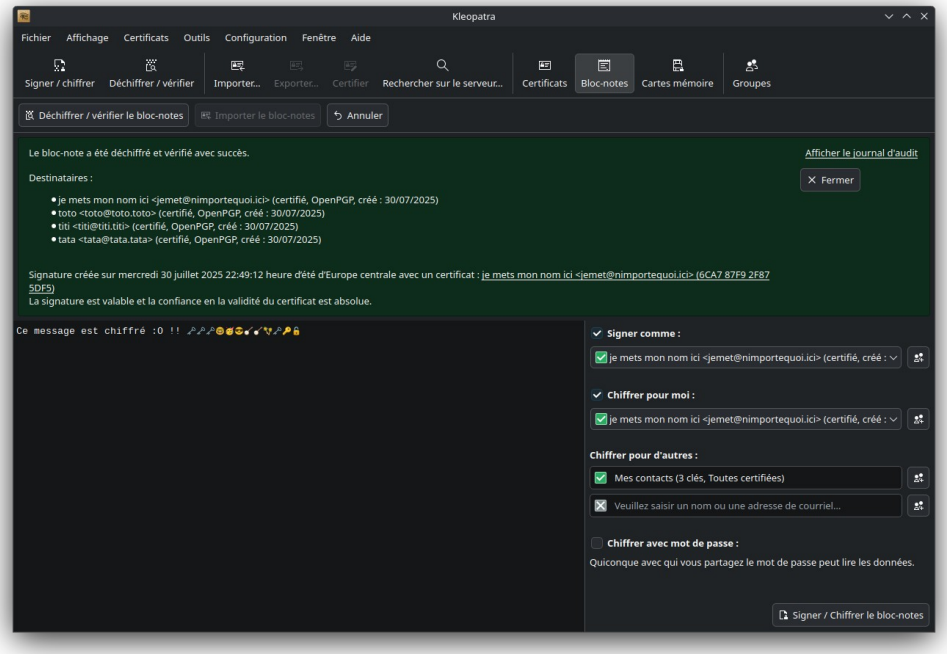


Figure 28: Message déchiffré

Le message est déchiffré (Figure 28), on peut y trouver la liste des destinataires puisqu'ils font tous partie du carnet d'adresse de « titi ». On y trouve aussi la signature qui permet de garantir la provenance du message.

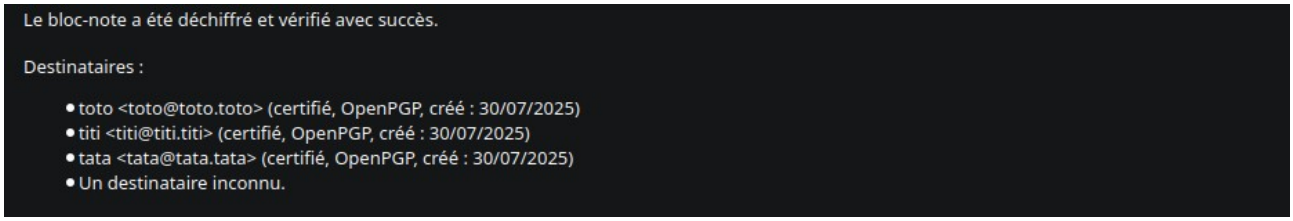


Figure 29: Destinataire inconnu

« toto » n'a pas ajouté « je mets mon nom ici » à sa liste de contact.
« toto » est destinataire et peut le déchiffrer. Pour « toto », « je mets mon nom ici » est inconnu et n'apparaît pas dans les autres destinataires (Figure 29).

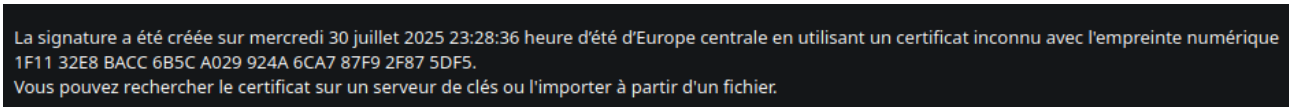


Figure 30: Signataire inconnu

Pour « toto », la signature est aussi inconnue (Figure 30).

Manipuler des fichiers

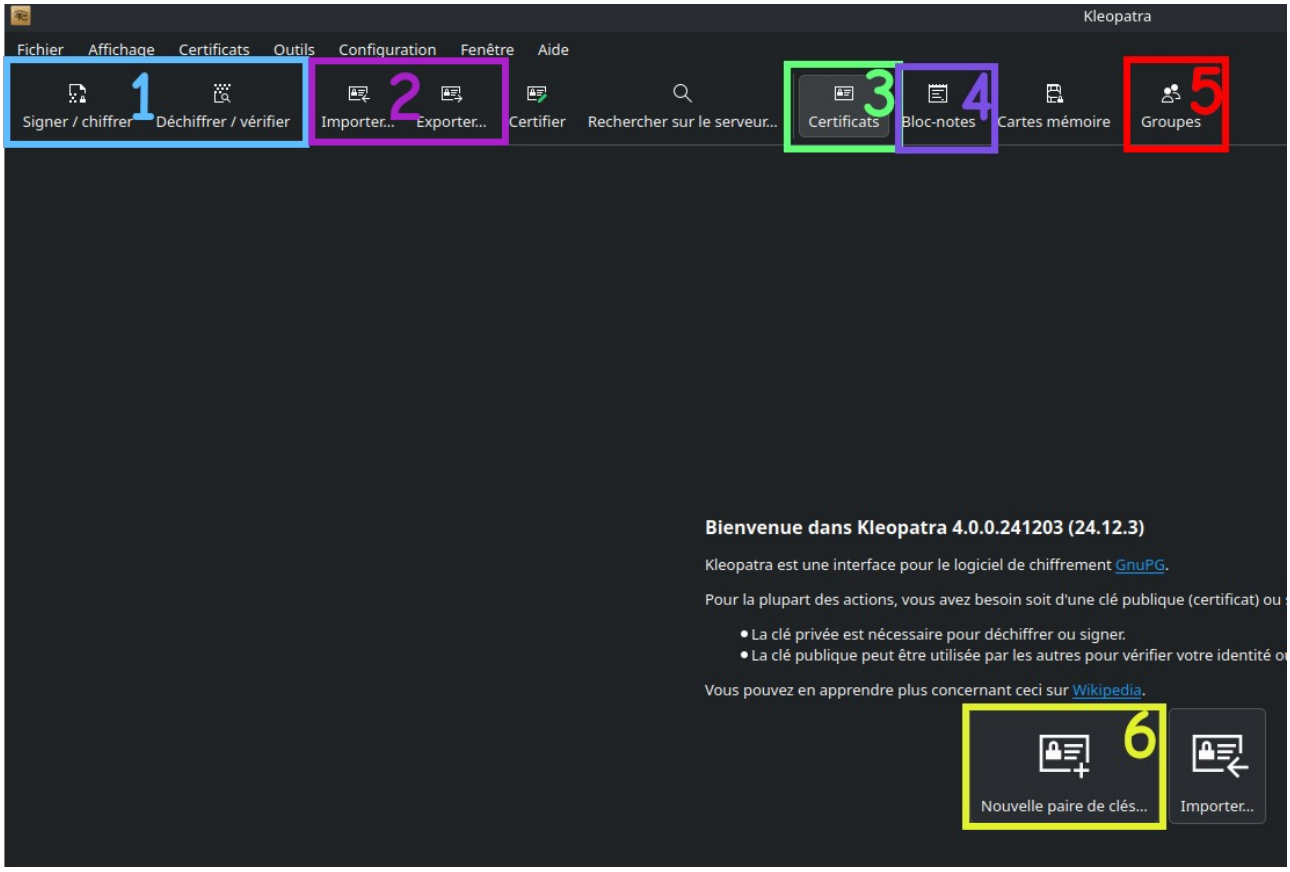


Figure 31: Interface de Kleopatra

Les boutons « signer / chiffrer » et « Déchiffrer / vérifier » qui figurent en « 1 » sur la capture (Figure 31) permettent de réaliser les mêmes manipulations qu'avec le « bloc-notes » sur des fichiers.

Concepts et Définitions

Cryptographie

« La **cryptographie** est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de *secrets* ou *clés*. Elle se distingue de la stéganographie qui fait passer inaperçu un message dans un autre message alors que la cryptographie rend un message supposément inintelligible à autre que qui de droit.

Elle est utilisée depuis l'Antiquité, mais certaines de ses méthodes les plus modernes, comme la cryptographie asymétrique, datent de la fin du XXe siècle. »[4]

Chiffrement

« Le **chiffrement** (ou **cryptage**[1],[2],[note 1]) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement. »[5]

Clé de chiffrement

« Une **clé** est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature).

Une clé de chiffrement peut être symétrique (cryptographie symétrique) ou asymétrique (cryptographie asymétrique). Dans le premier cas, la même clé sert à chiffrer et à déchiffrer. Dans le second cas on utilise deux clés différentes, la **clé publique** est utilisée au chiffrement alors que celle servant au déchiffrement est gardée secrète : la **clé secrète**, ou **clé privée**, et ne peut pas se déduire de la clé publique. »[6]

4 https://fr.wikipedia.org/wiki/Cryptographie
5 https://fr.wikipedia.org/wiki/Chiffrement
6 https://fr.wikipedia.org/wiki/Clé_de_chiffrement

Certificat

« Un **certificat électronique** (aussi appelé **certificat numérique** ou **certificat de clé publique**) peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges[1]. »[7]

Cryptographie symétrique

« La **cryptographie symétrique**, également dite **à clé secrète** (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé. On a des traces de son utilisation par les Égyptiens vers 2000 av. J.-C. Plus proche de nous, on peut citer le chiffre de Jules César, dont le ROT13 est une variante.

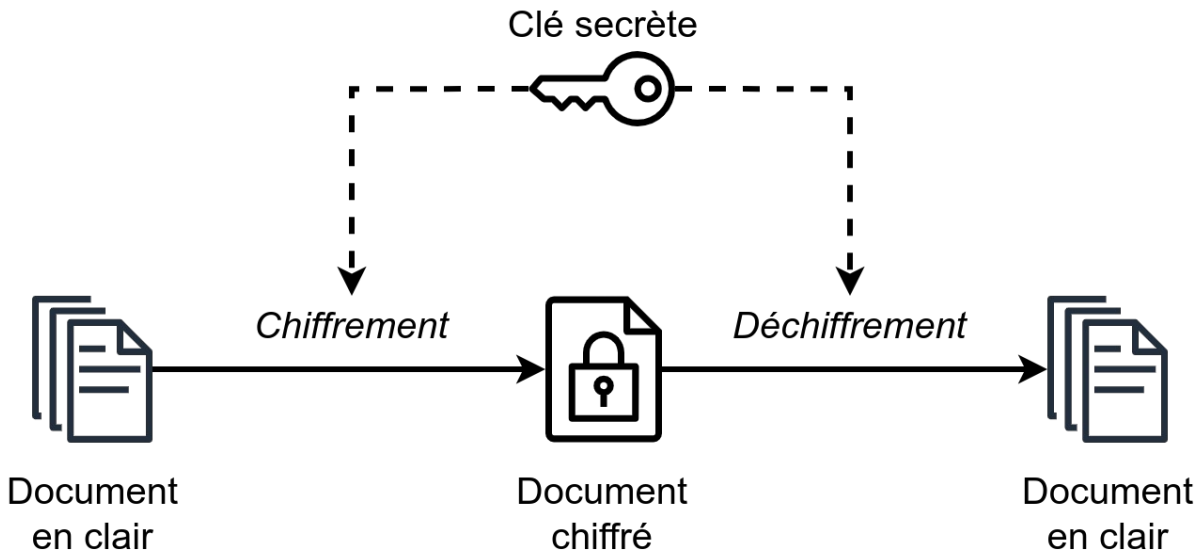


Figure 32: Schéma du chiffrement symétrique: la même clé est utilisée pour le chiffrement et le déchiffrement

»[8]

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

Pour aller plus loin

Méthodes de chiffrements symétriques connues :

- Chiffrement par décalage : Simulateur et Explications
- Chiffre de Vigenère : Simulateur et Explications
- Enigma : Simulateur et Explications
- Advanced Encryption Standard : Simulateur et Explications

Cryptographie asymétrique

« La **cryptographie asymétrique**, ou **cryptographie à clé publique** est un domaine relativement récent de la cryptographie. Elle permet d'assurer la confidentialité d'une communication, ou d'authentifier les participants, sans que cela repose sur une donnée secrète partagée entre ceux-ci, contrairement à la cryptographie symétrique qui nécessite ce secret partagé préalable[1].

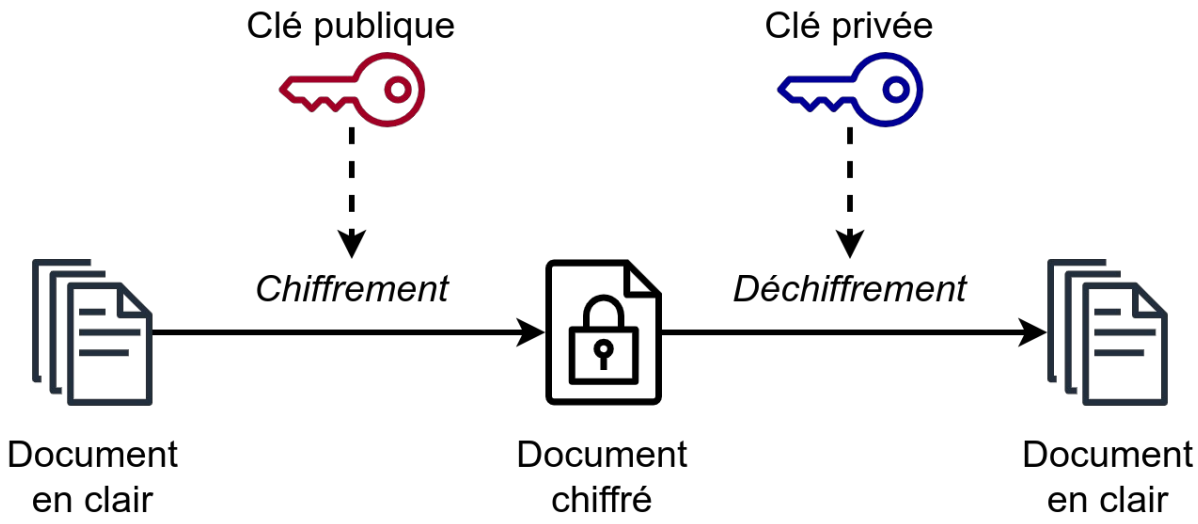


Figure 33: Schéma du chiffrement asymétrique: une clé sert à chiffrer et une seconde à déchiffrer

»[9]

9 https://fr.wikipedia.org/wiki/Cryptographie_asymétrique

Pour aller plus loin

Méthodes de chiffrements asymétriques connues :

- Chiffrement RSA
- Cryptographie sur les courbes elliptiques
- Échange de clés Diffie-Hellman

Cryptographie post-quantique

« La **cryptographie post-quantique** est une branche de la cryptographie visant à garantir la sécurité de l'information face à un attaquant disposant d'un calculateur quantique. Cette discipline est distincte de la cryptographie quantique, qui vise à construire des algorithmes cryptographiques utilisant des propriétés physiques, plutôt que mathématiques, pour garantir la sécurité. »[10]

Quelques percées majeures du domaine :

- https://www.csoonline.com/article/3562701/chinese-researchers-break-rsa-encryption-with-a-quantum-computer.html
- https://www.rsa.com/resources/blog/zero-trust/setting-the-record-straight-on-quantum-computing-and-rsa-encryption/
- https://lecanardquantique.com/index.php/2024/10/03/crystals-dilithium-la-cle-pour-des-signatures-numeriques-post-quantiques-securisees/
- https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsofts-quantum-resistant-cryptography-is-here/4238780

10 https://fr.wikipedia.org/wiki/Cryptographie_post-quantique