

Tutoriel GpgFrontend

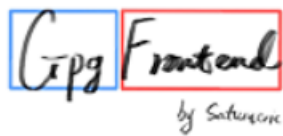


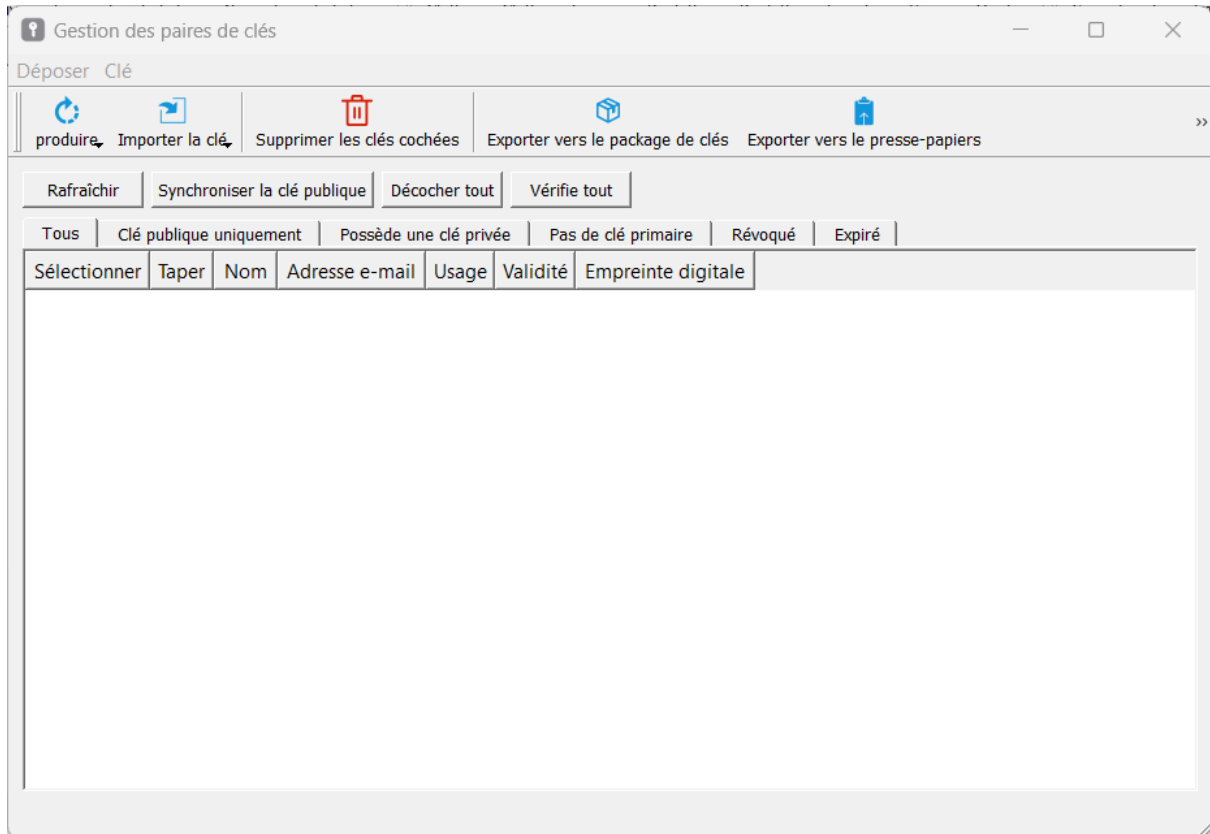
Table des matières

Création de la clé publique et privée	3
Cryptage et signature numérique	5
Cryptage	5
Signature	6
Crypter et signer	7
Échange de clés publiques.....	8
Exporter une clé publique	8
Méthode n°1 :	8
Méthode n°2 :	9
Méthode n°3 :	9
Importer la clé publique	10
Décrypter et/ou vérifier un message	11
Décrypter	11
Vérifier	12
Comment fonctionne OpenPGP en interne	13

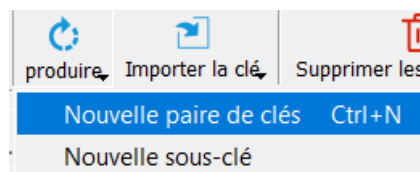
Création de la clé publique et privée

Après avoir ouvert le logiciel.

Cliquez sur **Clés > Gérer les clés**.



Cliquez ensuite sur le bouton en haut à gauche **Produire > Nouvelle paire de clés**.



Il faut ensuite compléter le formulaire par vos données personnelles comme votre nom, votre adresse mail.

Puis sélectionnez le type de clé et sa taille (vous pouvez laisser les deux par les données par défaut). Vous pouvez modifier la date d'expiration selon vos besoins. Si vous voulez que la clé n'expire jamais, il faudrait cocher la case **N'expire jamais**.

Générer la clé

Informations de base

Nom: meryem cevik

Adresse e-mail: adresse@gmail.com

Commentaire:

Date d'expiration: 25/01/2025 19:25:49 ☒ N'expire jamais:

Taille de clé (en bits): 2048

Type de clé: RSA

Sans phrase secrète: ☐

Utilisation des clés

☒ Chiffrement ☒ Signature

☒ Attestation ☒ Authentification

OK Cancel

N'oubliez pas de rentrer une phrase secrète composée de 8 caractères.
Ce mot de passe va protéger votre clé privée.

Recommandation : Choisissez un mot de passe fort, c'est-à-dire un mot de passe composé de 8 caractères, qui contient au moins une lettre minuscule, une lettre majuscule, un chiffre et un caractère spécial.

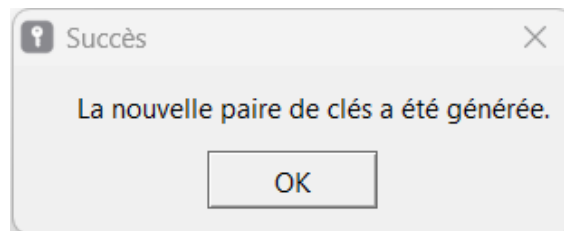
Pinentry

Veuillez entrer la phrase secrète pour protéger la nouvelle clef

Phrase secrète?: 12345678

OK Cancel

Enfin, vous devez obtenir cette fenêtre qui vous assure que la paire de clé a été bien créée.



Maintenant que vous avez votre clé privée et clé publique, vous pouvez crypter et décrypter des messages.

Cryptage et signature numérique

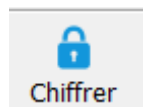
Cryptage

Pour crypter un texte, entrez votre texte dans le champ puis enregistrez-le OU sélectionner le fichier à crypter en cliquant sur **Ouvrir**.

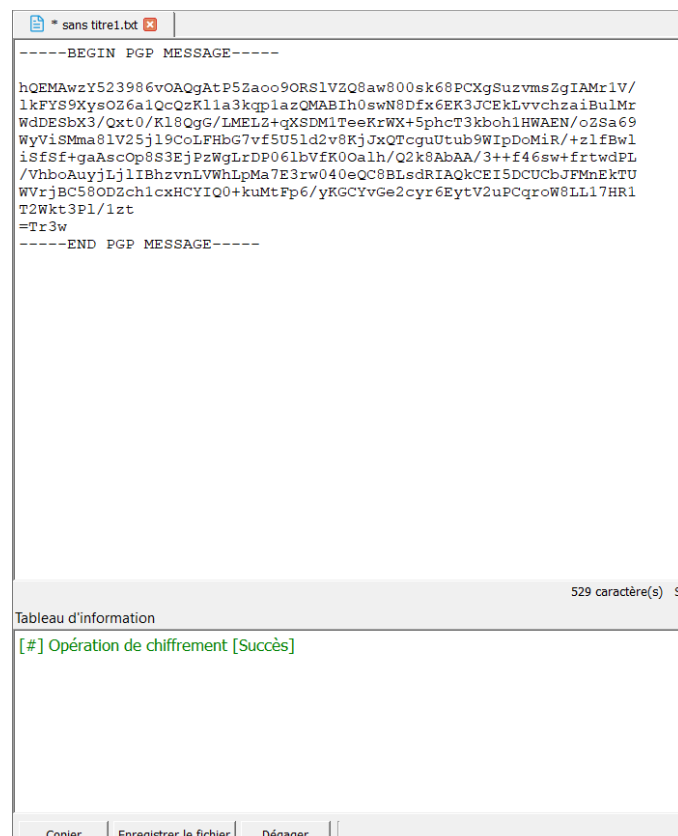
Puis sélectionnez la clé publique que vous venez de créer.

✓ 0 pub/sec Nom Prénom mcevik6738@gmail.com CESA Ultimat

Ensuite cliquez sur le bouton **Chiffrer** dans la barre en haut.



Vous obtenez votre message crypté.



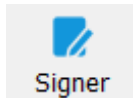
Vous pouvez l'enregistrer en cliquant sur **Enregistrez le fichier**.

Signature

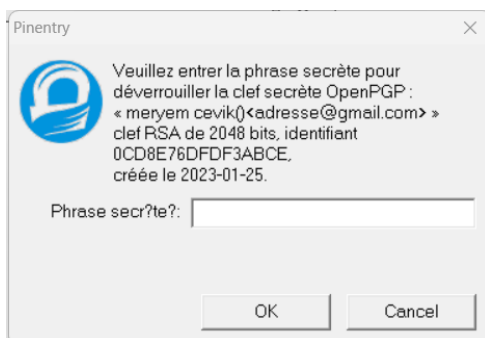
Il faut ensuite signer la clé : cela permet d'identifier une personne à partir du message signé.

Entrez votre message dans le champ ou ajouter le fichier en cliquant sur **Ouvrir**.

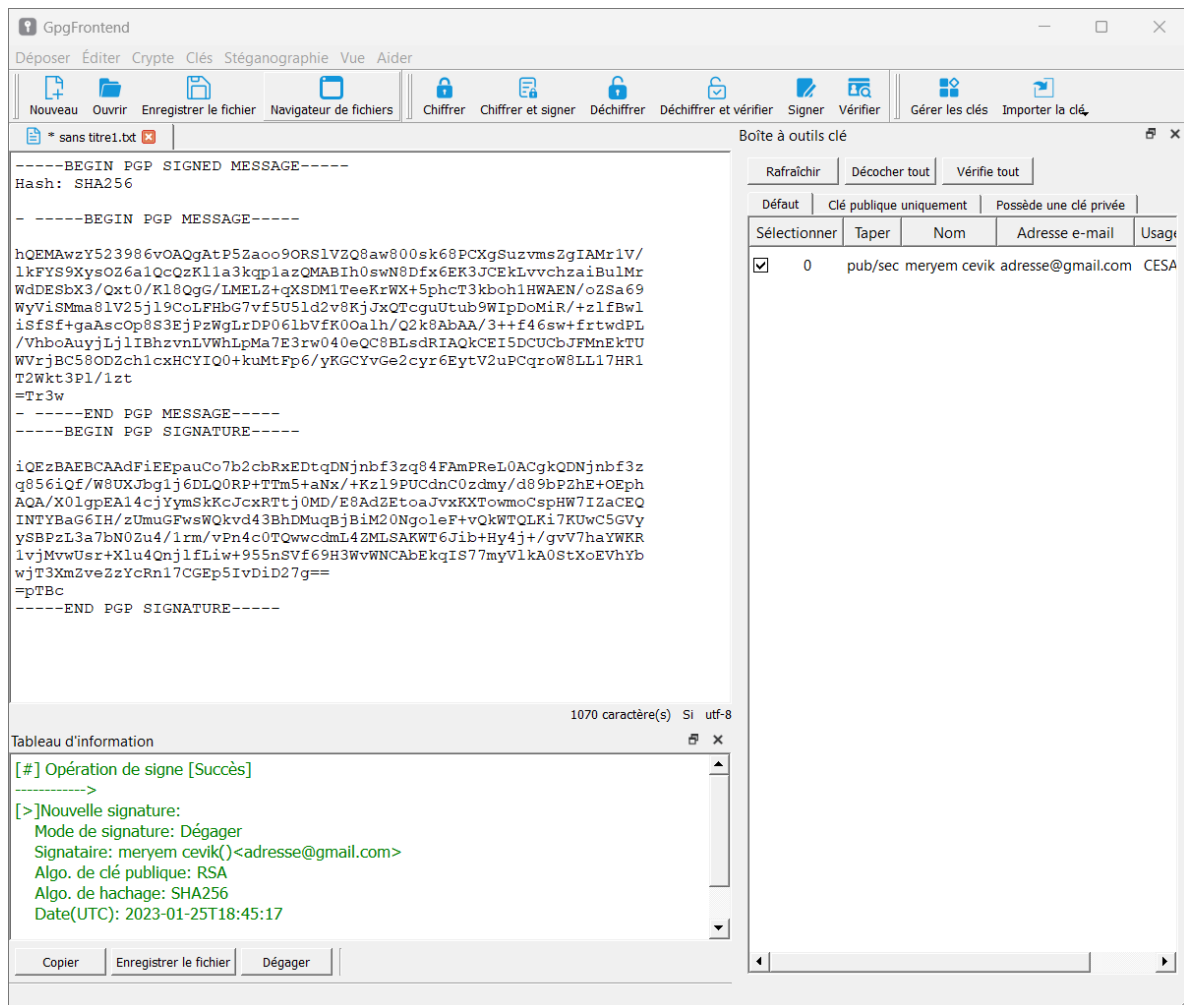
Pour signer votre message, cliquez sur le bouton **Signer** en haut.



Entrez votre mot de passe.



Après avoir signé, vos informations de signature et de validation sont marquées dans le tableau d'informations ci-dessous.



Vous pouvez l'enregistrer en cliquant sur **Enregistrez le fichier**.

Crypter et signer

Sélectionnez le fichier ou tapez dans le champ le message à crypter et signer.

Pour crypter et signé en une seule clique, il suffit de cliquer sur **Chiffrer et signer**.



On sélectionne le(s) signataire(s), en cochant la case avec la clé privée.

Signers Picker

Sélectionnez le(s) signataire(s):

Signataires				
Sélectionner		Nom	Adresse e-mail	Usage
<input checked="" type="checkbox"/>	0	meryem cevik	adresse@gmail.com	CESA

Veuillez sélectionner une ou plusieurs clés privées à utiliser pour la signature.
Si aucune clé n'est sélectionnée, la clé par défaut sera utilisée pour la signature

Confirmer

Annuler

On a ensuite un message de validation du chiffrement et signature dans le tableau d'information.

Tableau d'information

[#] Opération de chiffrement [Succès]

[#] Opération de signe [Succès]

----->

[>]Nouvelle signature:

Mode de signature: Normal

Signataire: meryem cevik()<adresse@gmail.com>

Algo. de clé publique: RSA

Algo. de hachage: SHA512

Date(UTC): 2023-01-25T18:56:47

Vous pouvez l'enregistrer en cliquant sur **Enregistrez le fichier.**

Échange de clés publiques

Ouvrez le gestionnaire de clé en cliquant sur **Gérer les clés.**



Exporter une clé publique

Méthode n°1 :

Exportez la clé publique en tant que package clé.

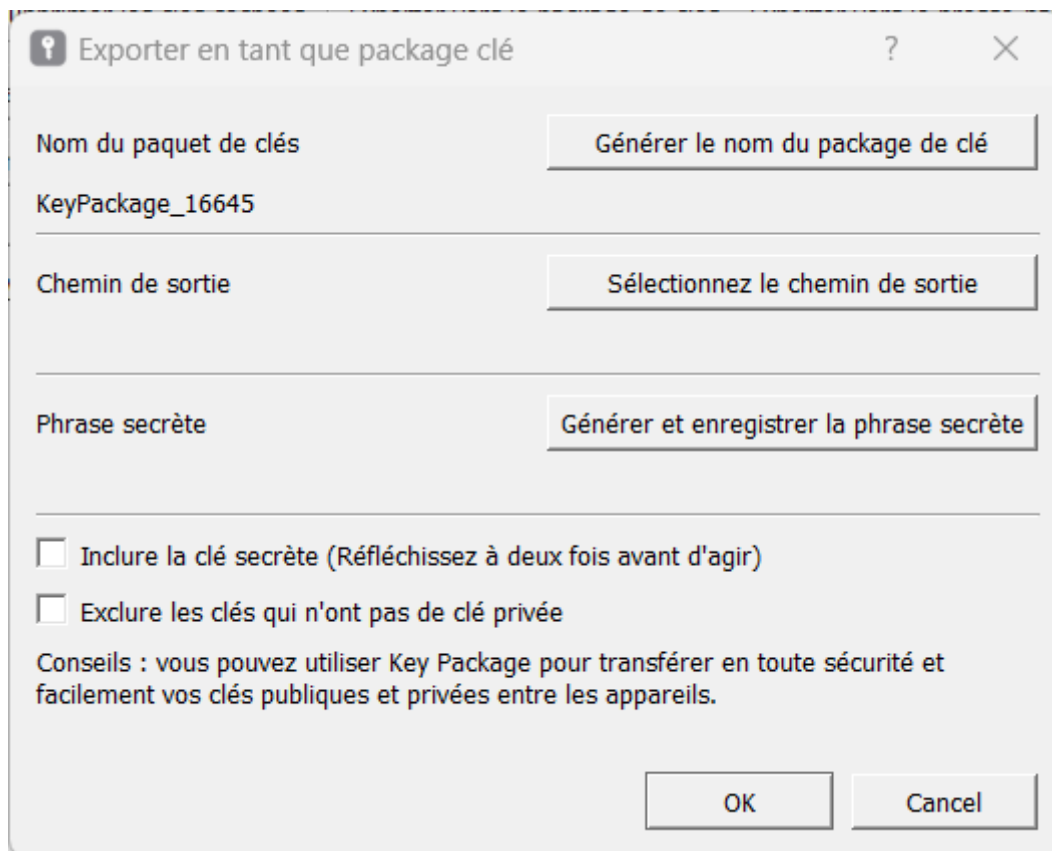
Sélectionnez la clé publique que vous voulez exporter.

<input checked="" type="checkbox"/>	0	pub/sec	meryem cevik	adresse@gmail.com	CESA	Ultimate	A5AB82A3B6F671B471103B6A0CD8E76DFDF3ABCE
-------------------------------------	---	---------	--------------	-------------------	------	----------	--

Cliquez sur **Exporter vers le package key.**



Puis vous pouvez changer le nom du paquet, sélectionnez l'emplacement où vous voulez l'exporter et même ajoutez/enregistrez une phrase secrète.



Exporter en tant que package clé

Nom du paquet de clés Générer le nom du package de clé

KeyPackage_16645

Chemin de sortie Sélectionnez le chemin de sortie

Phrase secrète Générer et enregistrer la phrase secrète

☐ Inclure la clé secrète (Réfléchissez à deux fois avant d'agir)

☐ Exclude les clés qui n'ont pas de clé privée

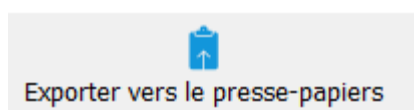
Conseils : vous pouvez utiliser Key Package pour transférer en toute sécurité et facilement vos clés publiques et privées entre les appareils.

OK Cancel

Enfin partagez le paquet avec la personne où vous voulez transmettre une clé publique.

Méthode n°2 :

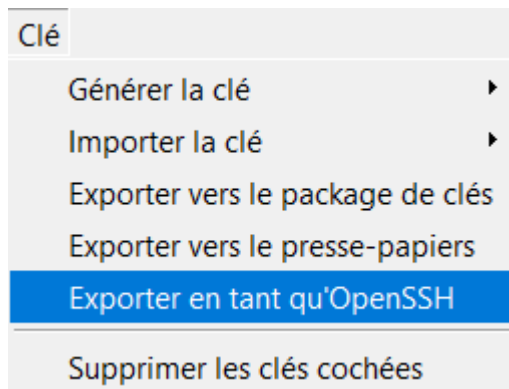
Une autre façon de faire serait d'exporter vers le presse-papier en cliquant sur le bouton **Exporter vers le presse-papiers**.



Partagez en collant la clé sur un champ d'envoi avec la personne où vous voulez transmettre une clé publique.

Méthode n°3 :

Une autre façon de faire serait d'exporter vers le presse-papier en cliquant sur **Clé > Exporter en tant qu'OpenSSH**.

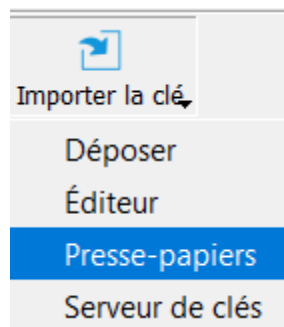


Sélectionnez l'emplacement où vous pouvez l'exporter.

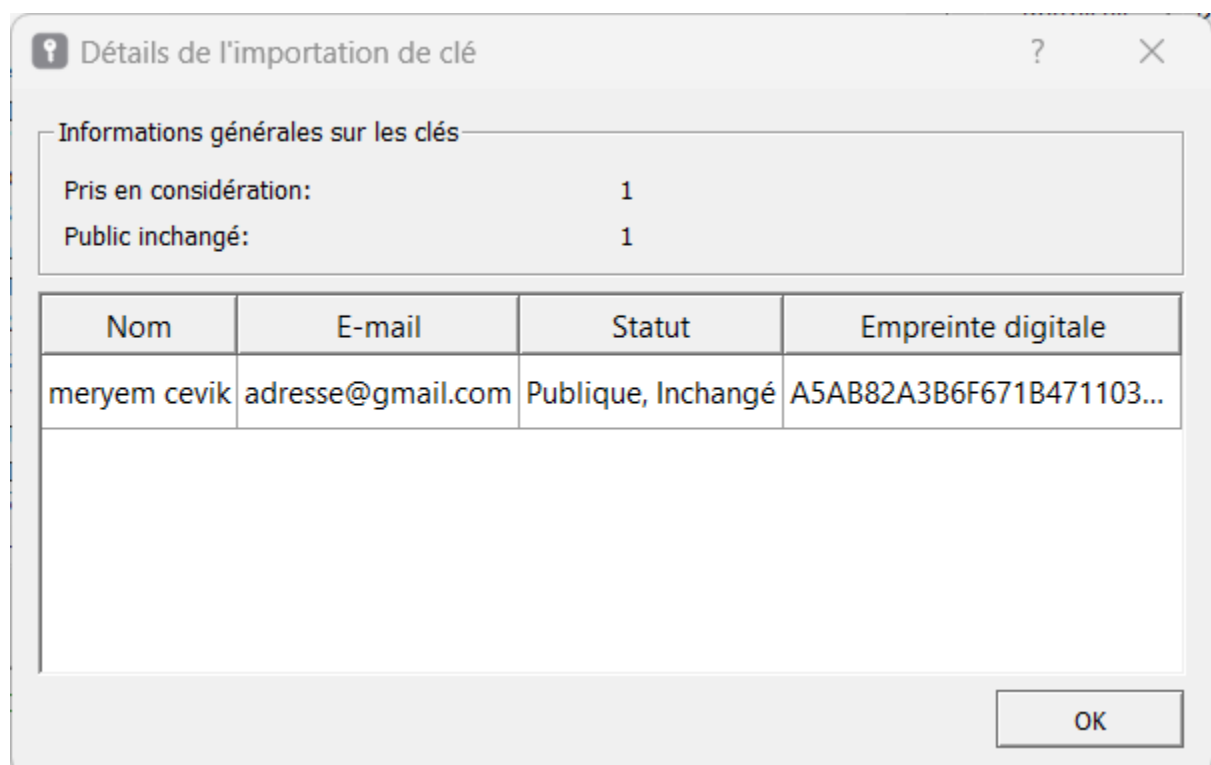
Importer la clé publique

Vous pouvez importer la clé de 2 façons.

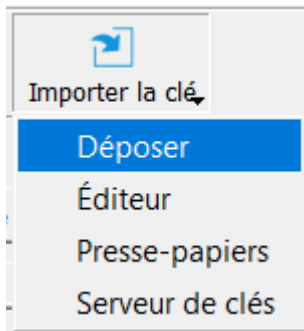
- 1) Copiez dans votre presse papier la clé envoyée par l'émetteur.
Cliquez sur **Importer la clé > Presse-papiers**.



Vous devez avoir une fenêtre qui vous indique que la clé a bien été importée.



Cliquez sur **Importer la clé > Déposer**.



Puis sélectionnez le fichier qui comporte la clé envoyée.

Vérifiez que la clé a été importée en cliquant sur **Clés >Gérer les clés** et vérifiez si la clé est présente.

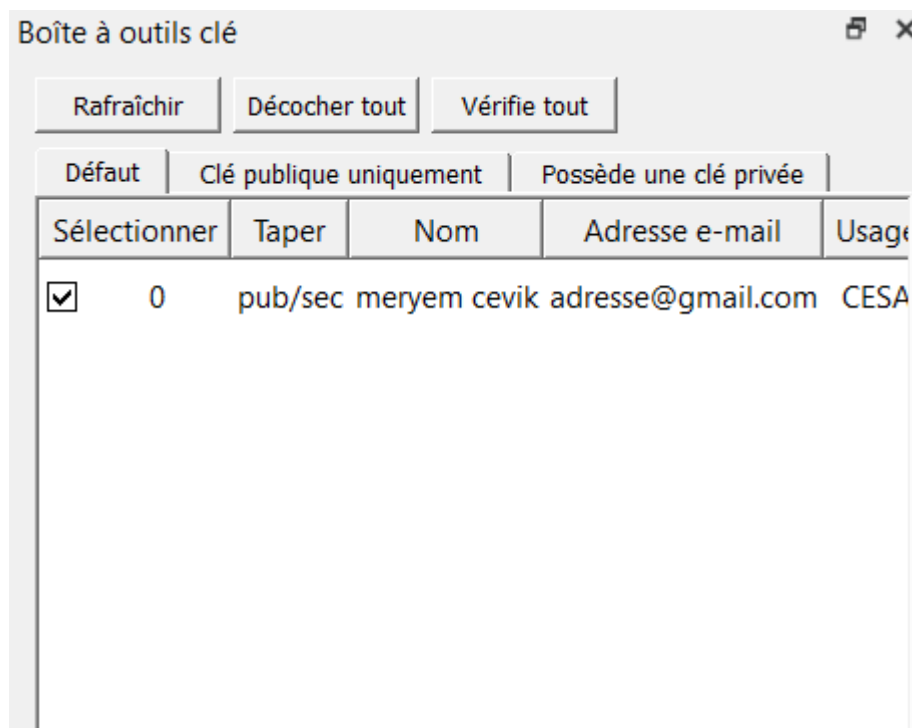
Décrypter et/ou vérifier un message

Décrypter

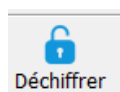
Pour décrypter le message crypté sans vérifier sa signature :

Sélectionnez le fichier à décrypter en cliquant sur **Ouvrir**.

Sélectionnez la clé publique en cochant la case.



Cliquez sur **Déchiffrer**.



Vous avez décrypté votre message avec succès si vous avez une confirmation dans l'output.

```
Tableau d'information
[#] Opération de déchiffrement[Succès]
----->
Destinataire(s):
{>} Destinataire: meryem cevik<adresse@gmail.com>
      Identifiant de clé: 0CD8E76DFDF3ABCE
      Algo. de clé publique: RSA
<-----
```

Vérifier

Pour vérifier la signature sans décrypter :

Sélectionnez le fichier à décrypter en cliquant sur **Ouvrir**.

Sélectionnez la signature.

Cliquez sur **Vérifier**.

```
Tableau d'information
[#] Vérifier le fonctionnement [Succès]
----->
[>] Signé le(UTC) 2023-01-25T19:57:30

[>] Liste des signatures:
Signature [1] :
UNE Bon Signature entièrement valide.
  Signé par: meryem cevik()<adresse@gmail.com>
  Algo. de clé publique: RSA
  Algo. de hachage: SHA512
  Date(UTC): 2023-01-25T19:57:30
```

Copier | Enregistrer le fichier | Dégager | Afficher les détails de vérification

La signature est bien valide.

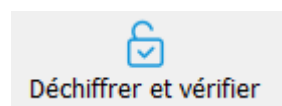
Décrypter et vérifier

Pour décrypter et vérifier la signature :

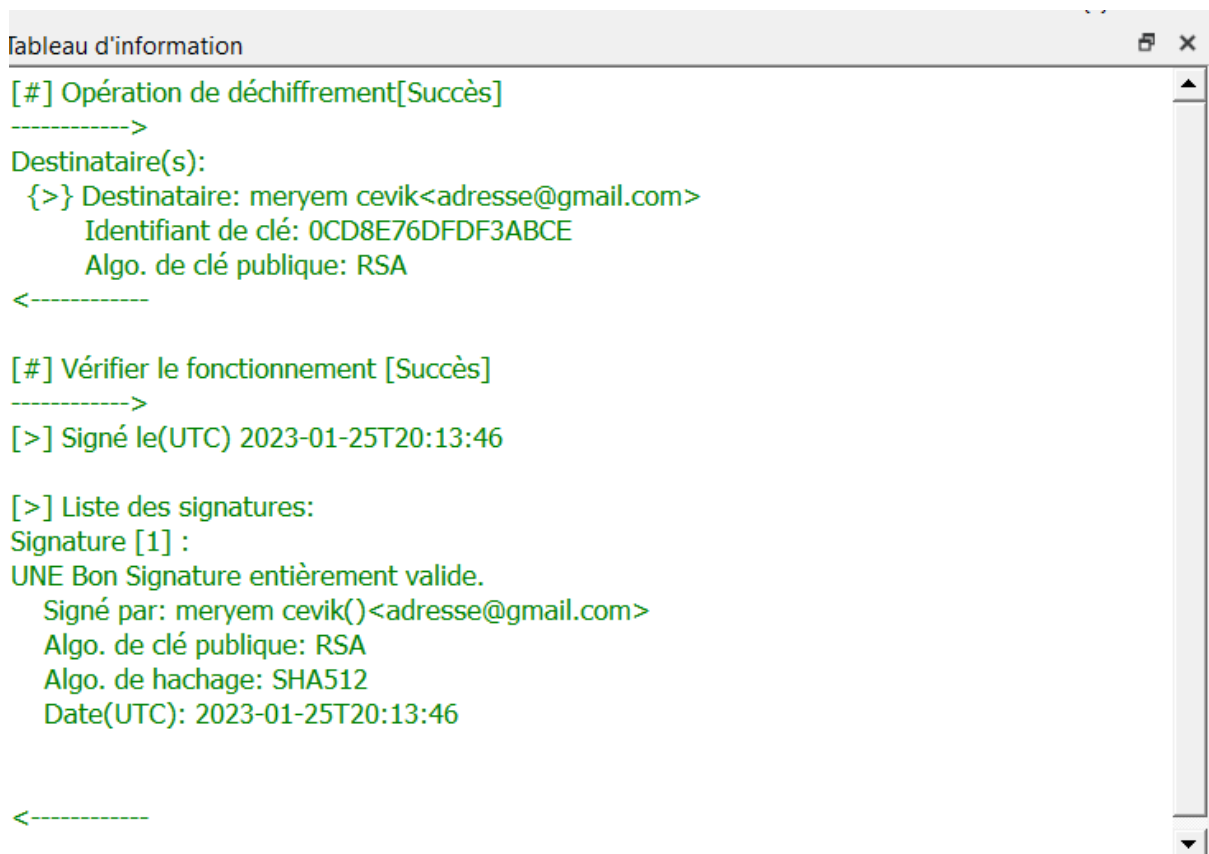
Sélectionnez le fichier à décrypter en cliquant sur **Ouvrir**.

Sélectionnez la clé utilisée pour signer et crypter le message.

Cliquez ensuite sur Déchiffrer et vérifiez.



Le logiciel doit afficher que le déchiffrement a été bien fait et que la signature est la bonne.



Comment fonctionne OpenPGP en interne

OpenPGP est un protocole pour le chiffrement/signature des données qui permet de crypter, décrypter, signer et vérifier les messages de manière sécurisée en utilisant des clés publiques et privées.

Le fonctionnement d'OpenPGP en interne :

- OpenPGP génère une paire de clés : une clé publique, qui ne sert qu'à chiffrer, et une clé privée, également appelée clé de session, qui sert à déchiffrer.
- OpenPGP chiffre : Quand une personne veut envoyer un message chiffré, il utilise la clé publique envoyée pour chiffrer le message. Le destinataire peut le déchiffrer que s'il possède la clé privée.
- Déchiffrement : Le message chiffré peut être déchiffré et être lu que si le destinataire utilise sa clé privée.
- Signer un message : La signature permet de vérifier l'identité de la personne qui a envoyé le message. Elle se fait en utilisant sa propre clé privée.
- Vérifier la signature : La personne qui veut vérifier si la signature est valide, elle utilise la clé publique de la personne qui l'a envoyé.
- Gestion de clés : OpenPGP gère les clés privées et publiques, permet de les exporter et partager aux autres en toute sécurité.