LABO4 – Certificats S/MIME

1 CERTIFICAT S/MIME

1.1. Qu'est-ce que S/MIME ?

Dans la RFC 1847, deux extensions de sécurité ont été spécifiées pour la norme d'email **MIME** (Multipurpose Internet Mail Extension) :

1. Le format multipart/signé pour la signature des messages
2. Le format multipart/crypté pour leur cryptage.

4 ans plus tard, l'IEFT (Internet Engineering Tasking Force) a publié l'extension MIME **S/MIME** décrite dans la spécification RFC 2633 : une norme qui supporte le premier format de signature.

Vous pouvez choisir librement si un mail avec **S/MIME** doit être uniquement crypté, signé ou bien si les deux opérations doivent être appliquées.

Le cryptage **S/MIME** et la signature est possible sur tous les clients de messagerie courants, comme par exemple Microsoft Outlook, Thunderbird ou Apple Mail.

1.2. Comment fonctionne le chiffrement et la signature S/MIME ?

S/MIME est basée sur une méthode de chiffrement asymétrique et utilise donc une paire de clés composée d'une clé privée et d'une clé publique.

Alors que la clé publique est partagée avec tous les contacts par courriel, la clé privée n'est ouverte qu'à l'utilisateur. Elle est utilisée à la fois pour envoyer des messages cryptés en combinaison avec la clé publique du destinataire et pour décrypter les messages reçus.

Avec un certificat **S/MIME**, le client de messagerie peut générer et échanger des clés, un tel certificat peut être obtenu auprès de différents fournisseurs.

Pour que le chiffrement des courriers électroniques fonctionne, chaque message **S/MIME** est précédé de l'information d'en-tête qui fournit au client destinataire l'information nécessaire pour saisir et traiter le contenu. Entre autres, le type de contenu (par exemple « enveloped-data » pour les données cryptées), le nom de fichier correspondant (par exemple smime.p7m pour les données signées ou cryptées) ou la forme d'encodage sont spécifiés.

Un en-tête possible d'un email crypté ressemble à ce qui suit :

```
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m
```

La signature **S/MIME**, qui peut être automatiquement épinglée à un email, est pratique pour plusieurs raisons :

- Elle envoie la clé publique pour une communication sécurisée au destinataire, qui peut également vous envoyer des messages avec un contenu crypté. La signature prouve également au destinataire que l'email a bien été envoyé par vous. Contrairement à PGP ou GPG, l'ajout d'une signature n'entraîne pas l'apparition de caractères cryptiques. Si le client de réception détecte des incohérences lors de la vérification de la signature reçue, la légitimité du message n'est pas confirmée, ce qui permet à l'utilisateur de conclure que les données ont été manipulées.

1.3. Obtenir un certificat S/MIME ?

Comme nous l'avons déjà mentionné, l'utilisation de **S/MIME** nécessite un certificat (X.509). En principe, il est possible d'en créer un vous-même, cependant, vous avez d'abord besoin d'un certificat racine, que vous devez également générer dans ce cas. De plus, tous les partenaires de communication doivent d'abord importer ce certificat racine avant que l'échange de clés puisse être initié. La solution la plus simple et la moins compliquée est l'achat d'un certificat auprès d'un organisme de certification officiel, avec des offres payantes et gratuites.

La classification des certificats disponibles dans les trois classes suivantes est typique :

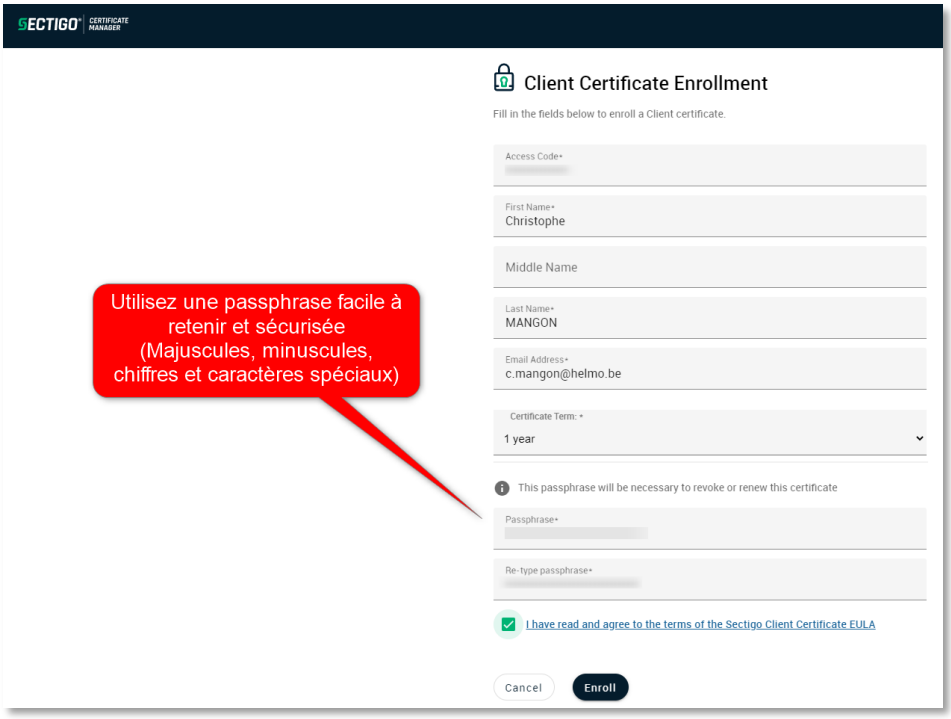
- **Classe 1** : le certificat délivré par l'autorité de certification garantit l'authenticité de l'adresse électronique fournie.
- **Classe 2** : le certificat garantit l'authenticité de l'adresse email spécifiée et du nom correspondant. En outre, le cas échéant, la société est également confirmée. Les informations sont vérifiées à l'aide de bases de données de tiers ou de copies de carte d'identité.
- **Classe 3** : les certificats de classe 3 diffèrent des certificats de classe 2 en ce que le demandeur doit s'identifier personnellement.

Si vous souhaitez crypter vos mails avec **S/MIME** et que vous recherchez un certificat, vous ne devez pas perdre de vue sa fonction principale : il est conçu pour sécuriser vos communications électroniques en empêchant l'interception et la manipulation du contenu des messages.

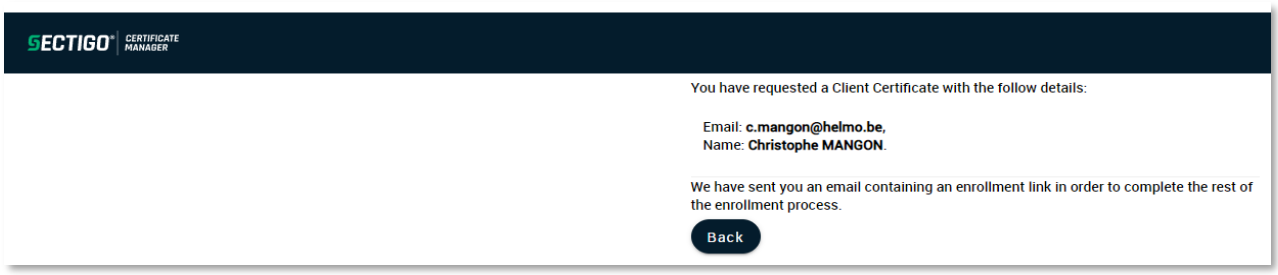
1.4. Sécurisation de vos mails @student.helmo.be

1.4.1 Génération d'un certificat

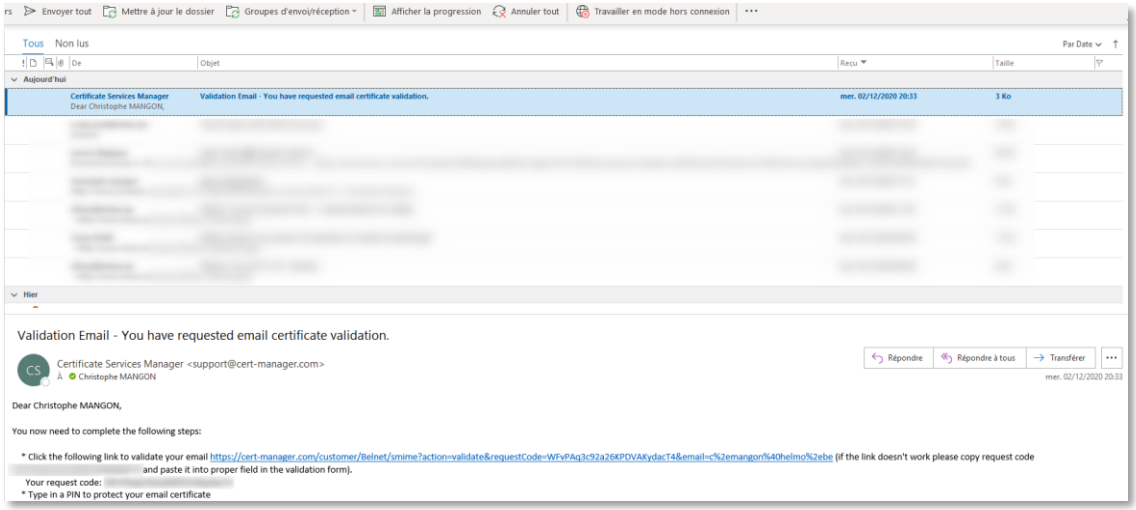
A l'aide de vos identifiants HELMo, connectez-vous sur la page https://apps.helmo.be/securemail/ et remplissez le formulaire de demande de certificat **S/MIME**.

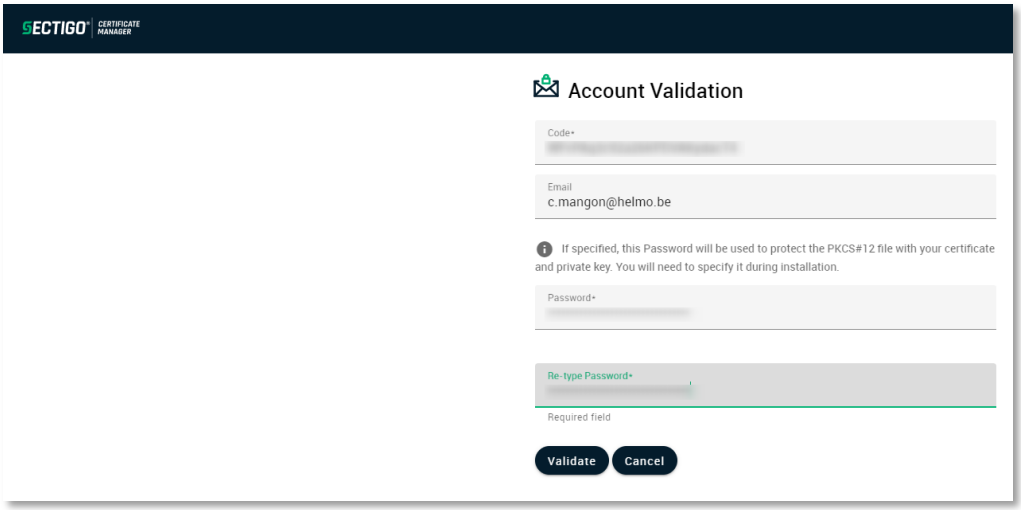


LABO4 – Certificats S/MIME



Après quelques secondes, vous devriez recevoir un mail vous invitant à valider votre demande de certificat.



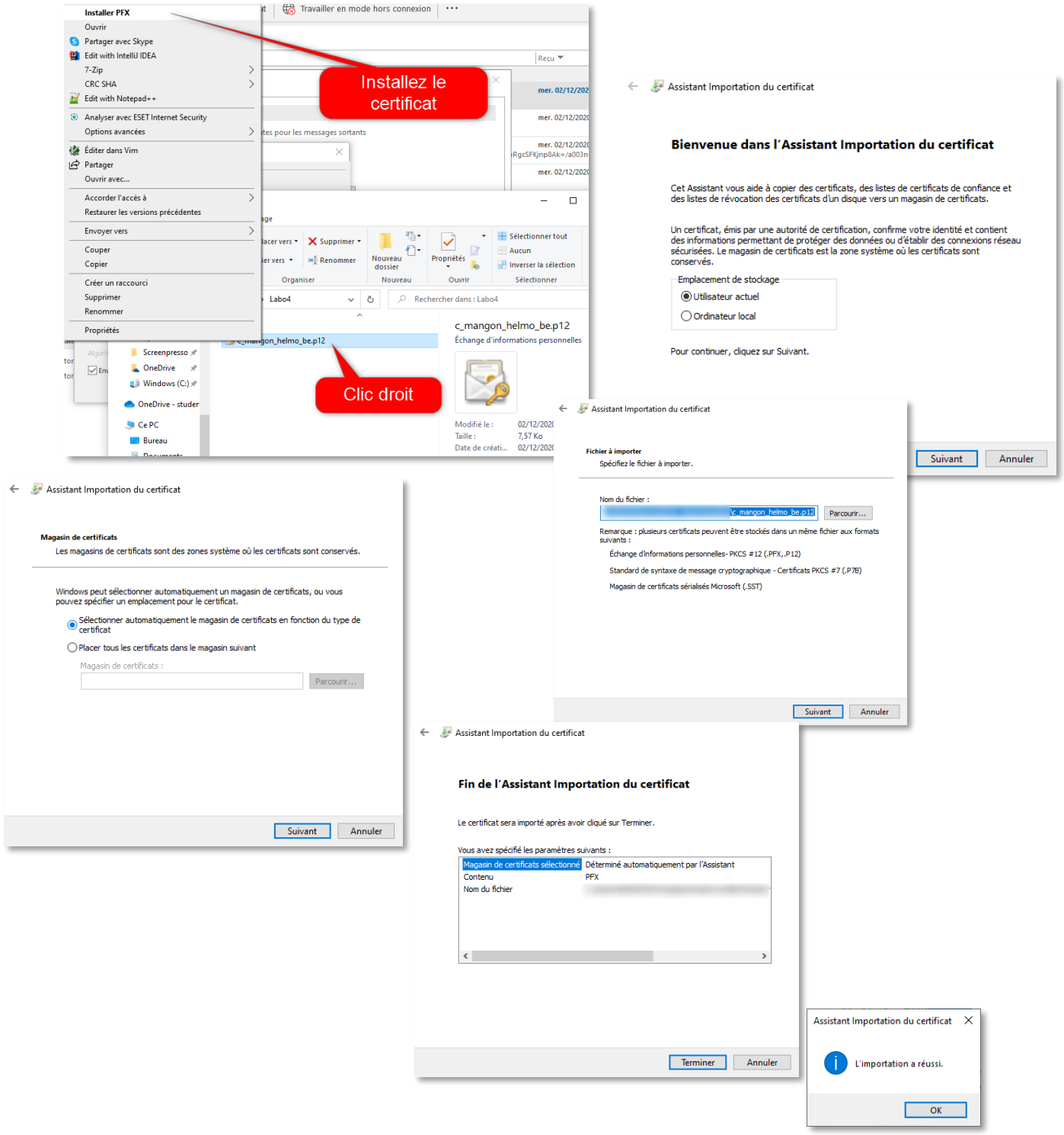


Validez votre demande une seconde fois en introduisant votre passphrase.

1.4.2 Installation du certificat

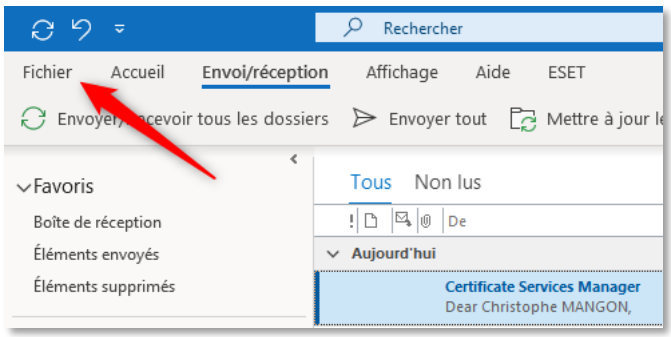
Téléchargez votre certificat au format **p12** sur votre disque dur et déplacez-le dans un dossier sûr. Le fichier **p12** est un fichier de données **#12 PKCS**. Où **PKCS** représente les normes de cryptographie à clé publique (**P**ublic-**K**ey **C**ryptography **S**tandard). Un fichier **p12** contient une représentation binaire d'un certificat, y compris ses clés publiques et privées.

Installez votre nouveau certificat sur votre système d'exploitation.

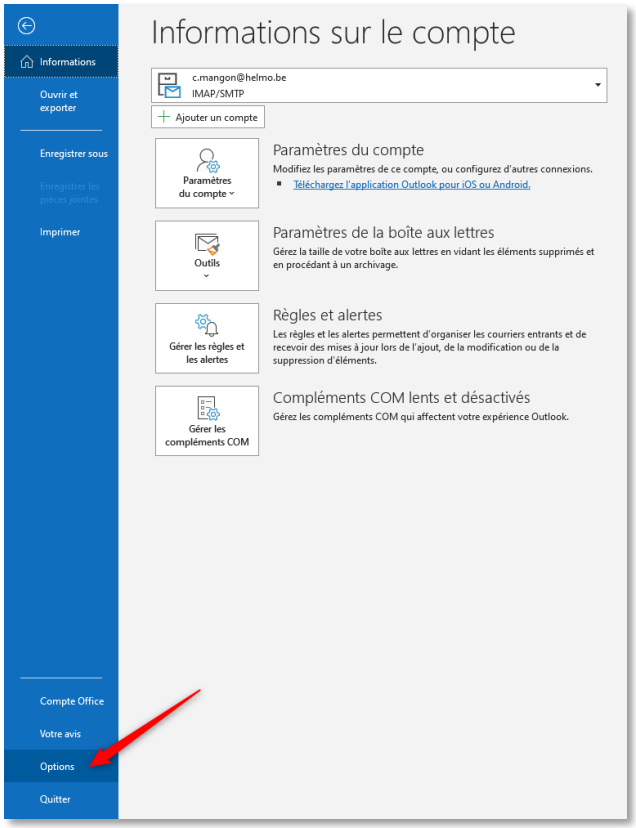


LABO4 – Certificats S/MIME

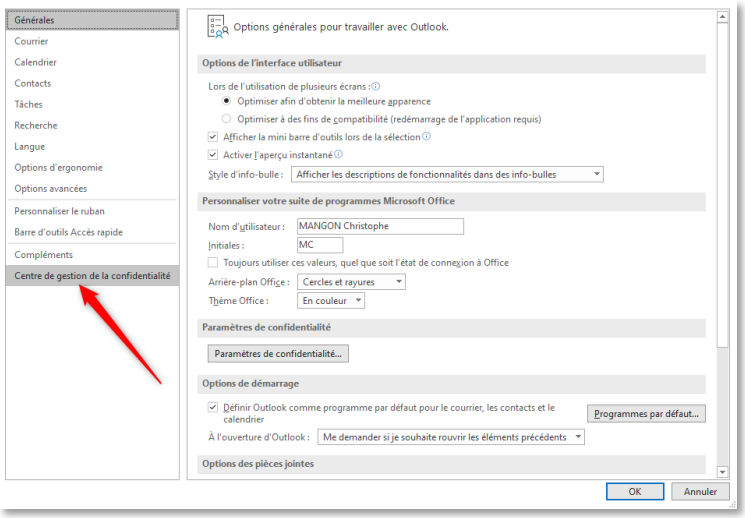
1.4.3 Configuration du client Outlook

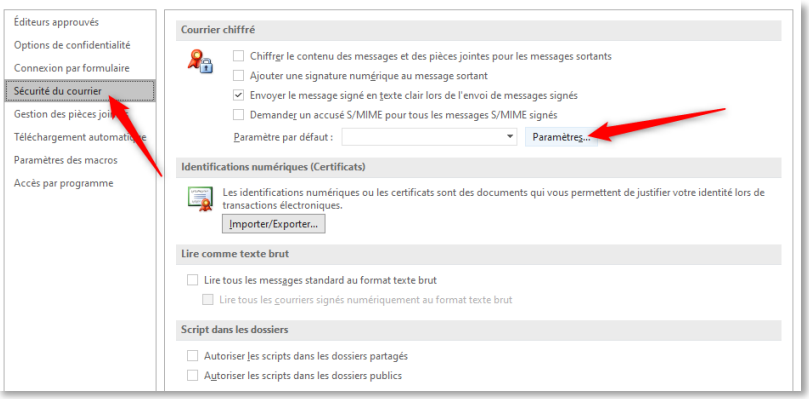


Dans l'onglet **Fichier** > **Options**

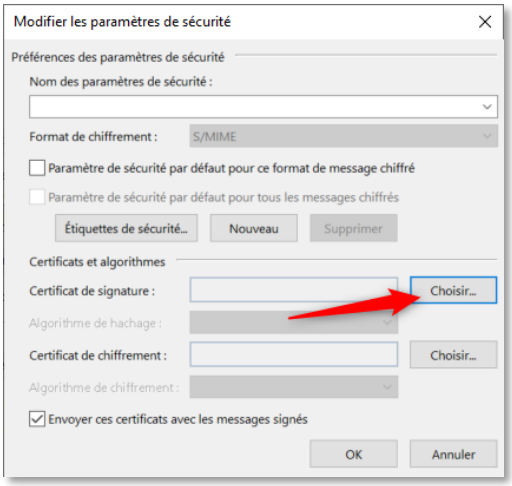


Sélectionnez **Centre de gestion de la confidentialité**.



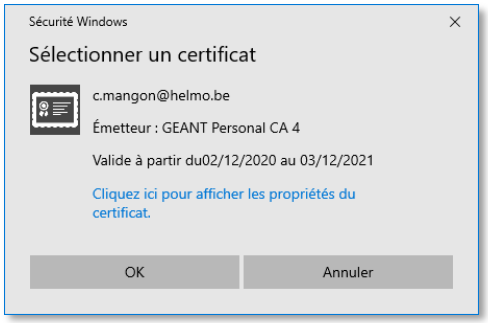


Sélectionnez **Sécurité du courrier**, ensuite **Para mètres...**



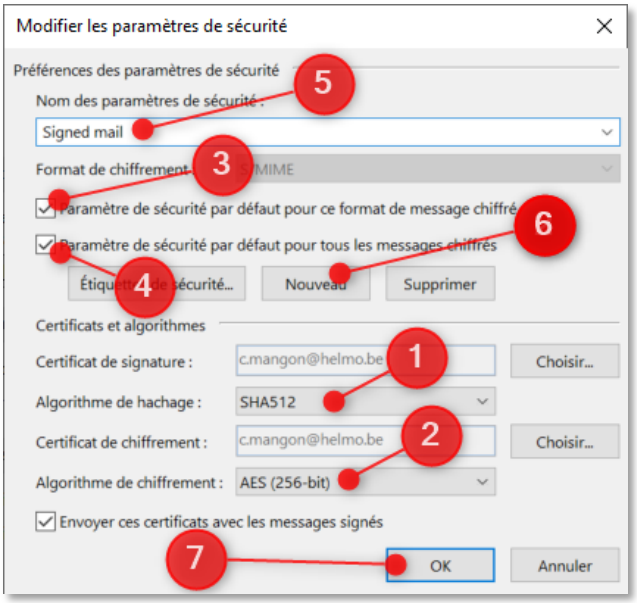
Cliquez sur **Choisir...** le certificat de signature.

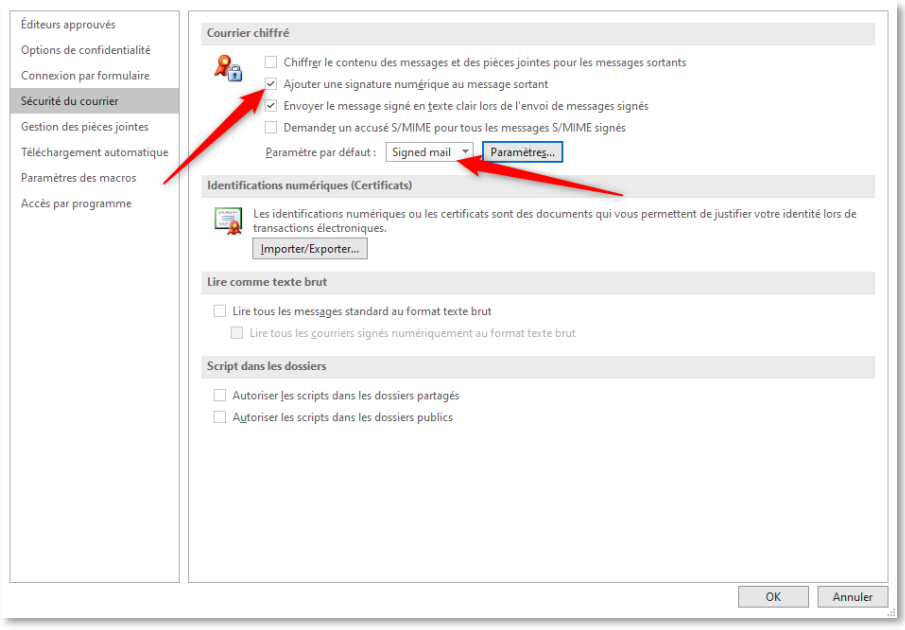
LABO4 – Certificats S/MIME



Votre certificat, associé à votre adresse mail vous est normalement automatiquement proposé.

Il vous reste à configurer la signature de vos emails et les protocoles de signature et cryptage.



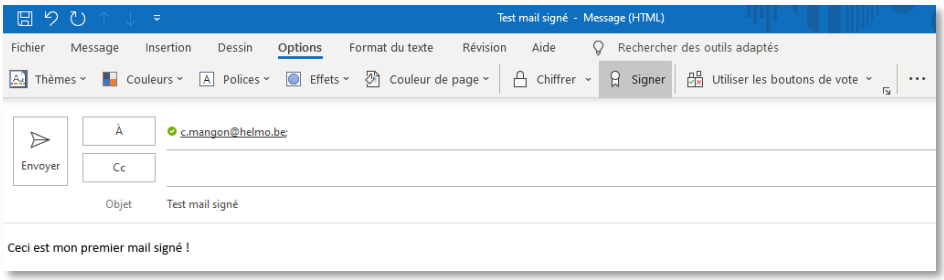


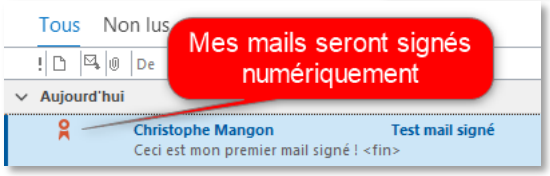
Sélectionnez le paramètre par défaut (voir point 5 sur la capture d'écran précédante).

Et cochez l'option **d'Ajouter une signature numérique au message sortant**.

1.4.4 Testez l'envoi d'un mail signé

Envoyez-vous un mail afin de valider votre configuration. Par défaut, normalement, l'option Signer sera sélectionnée.





Vous pouvez vérifier que vos mails sont signés numériquement par la présence de cet icône.

Pour valider ce laboratoire, envoyez un mail à mon adresse **c.mangon@helmo.com**.