

Sécuriser sa messagerie électronique

Signer un message assure au destinataire de votre message que vous en êtes bien l'auteur.



- Signer assure l'identification de l'expéditeur.
- La signature du message que vous envoyez se fait à l'aide de votre clé privée et elle est vérifiée par le destinataire à l'aide de votre clé publique intégrée au message.
- Signer n'impose pas à votre correspondant d'utiliser un certificat.

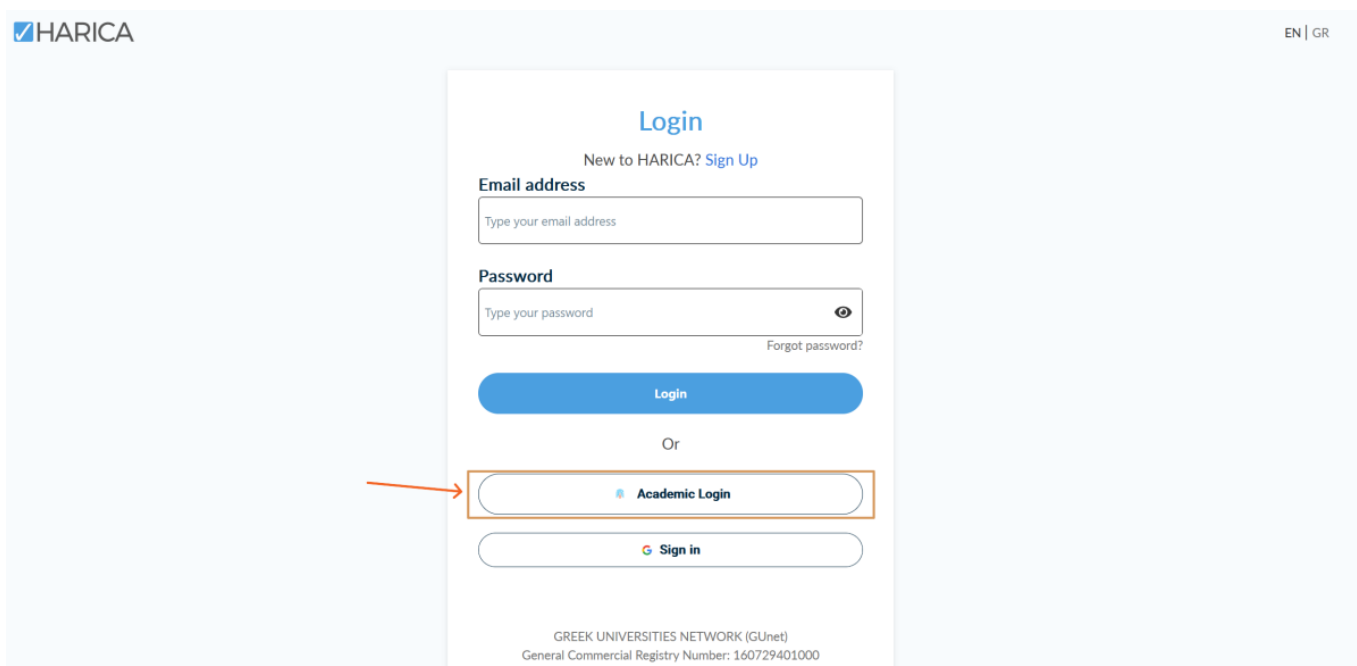
Obtenir un certificat personnel



Afin de pouvoir signer des messages vous devez au préalable obtenir un certificat personnel. Vous pouvez le faire en visitant cette adresse :

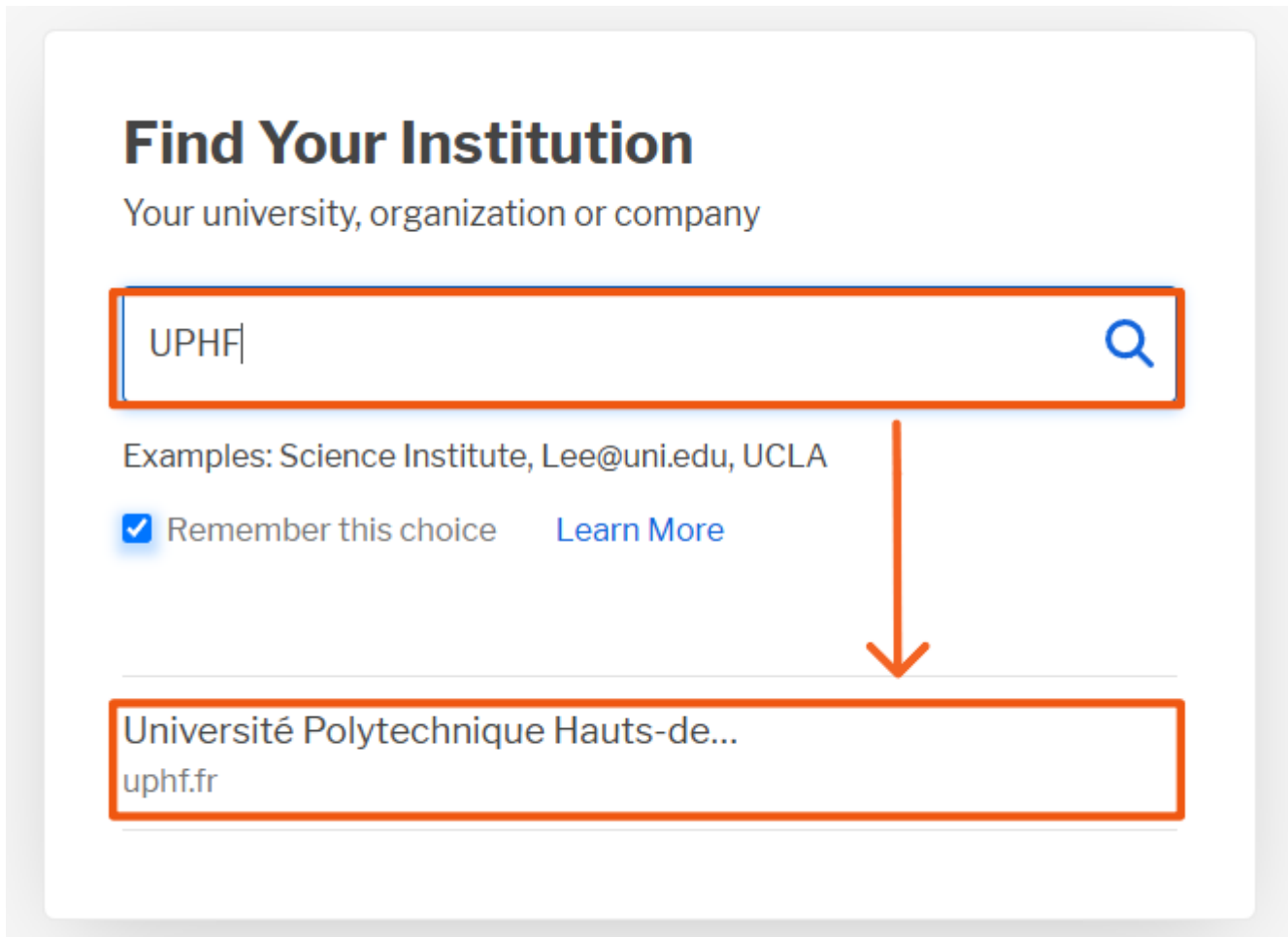
<https://cm.harica.gr/>.

- Accédez à la page de connexion et cliquez sur “Academic Login”



The screenshot shows the HARICA login page. At the top left is the HARICA logo and at the top right are the language options 'EN | GR'. The main content area is titled 'Login' and includes a link for 'New to HARICA? Sign Up'. Below this are two input fields: 'Email address' with the placeholder 'Type your email address' and 'Password' with the placeholder 'Type your password' and a 'Forgot password?' link. A blue 'Login' button is positioned below the password field. Underneath the button is the word 'Or' and a button for 'Academic Login' which is highlighted with an orange box and an arrow. Below that is a 'Sign in' button. At the bottom of the page, it says 'GREEK UNIVERSITIES NETWORK (GUnet)' and 'General Commercial Registry Number: 160729401000'.

- Dans le champ de recherche, entrez **uphf** et cliquez sur **Université Polytechnique Hauts-de-France**



- Connectez-vous vec vos identifiants ENT



Service Central d'Authentification (CAS)

Entrez votre identifiant et votre mot de passe.

Identifiant :*

Vous devez entrer votre identifiant.

Mot de passe :*

Pour des raisons de sécurité, veuillez vous [déconnecter](#) et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Vos identifiants sont strictement confidentiels et ne doivent en aucun cas être transmis à une tierce personne.

[Mot de passe oublié ?](#)

[Activer mon compte](#)

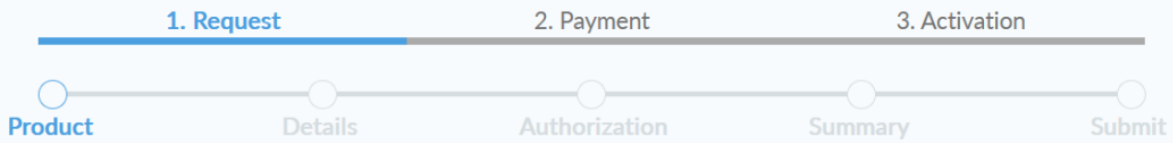
[Besoin d'aide ?](#)

- Cliquez sur “Email”

The screenshot displays the HARICA web interface. At the top left, there is a hamburger menu icon and the HARICA logo. The top right shows the user's name 'Djany' and the affiliation 'UNIVERSITE POLYTECHNIQUE HAUTS-DE-FRA...'. The main content area is titled 'My Dashboard' and features a row of service buttons: SSL, eSignature, Token, eSeal, S/MIME, Remote, Code Signing, and Client Authentication. Below this, a message states: 'Your Dashboard is empty, proceed with a certificate request.' The left sidebar lists various services under 'Certificate Requests': eSignatures, eSeals, Server, Code Signing, Email (highlighted with a red box and an arrow), and Client Authentication. Below this is a 'More' section with links for Validated Information and Data privacy statement.

- Sélectionnez “Email only”

Email / Request New Certificate



Select the type of your certificate

Email-only

S/MIME certificate to sign/encrypt email messages.

Includes:

- Your email address(es)

Select

Free

For individuals or sole proprietorships (IV)

S/MIME certificate to sign/encrypt email messages.

Includes:

- Your email address(es)
- Your personal information

Select

from
33€ year

For enterprises or organizations (OV)

S/MIME certificate to sign/encrypt email messages.

Includes:

- Your email address(es)
- Information of your organization

Select

from
71.5€ year

- Cliquez sur "Next" deux fois (Voir image)

Select the type of your certificate

[Change](#)

Email-only

S/MIME certificate to sign/encrypt email messages.

Includes:

- Your email address(es)

Selected

Free

Enter your email address

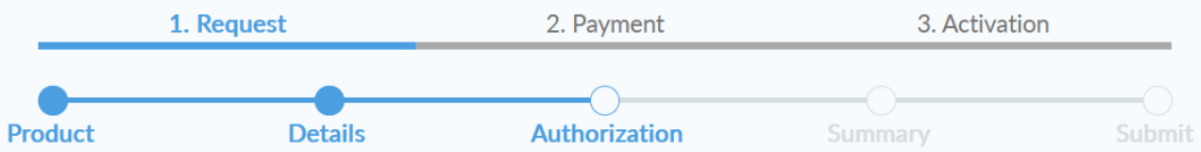
Email Addresses

Include one or more email addresses in your certificate.

email: `djany.1` `1@uphf.fr`

Next

Email / Request New Certificate



Select a method to validate your email address(es)

Validate via email to selected email address
Validate via email to selected email address

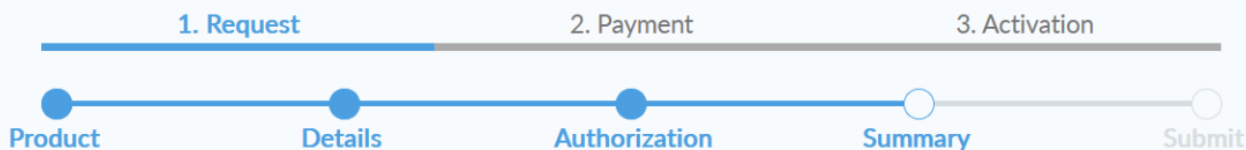
Selected

← Back

Next

- Vérifiez les informations et cliquez sur "Submit"

Email / Request New Certificate



Review the application before submitting

Certificate Type S/MIME email-only	Service Duration 2 years
Emails 1. @uphf.fr	

I, _____ declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[← Back](#)

[Submit](#)

- Rendez-vous dans Zimbra. Vous devez avoir reçu un mail. Ouvrez celui-ci et cliquez sur « Confirm »



Sur certains navigateurs, la redirection peut ne pas fonctionner. Dans ce cas, effectuez un clic droit sur le bouton "Confirm", puis copiez le lien. Ouvrez un nouvel onglet et collez-y le lien que vous venez de copier.



HARICA - Email confirmation for certificate issuance

30 Avril 2025 15:5

Expéditeur : HARICA Certificate Manager (CM)

À: Djany I



Les images externes ne seront pas affichées. [Afficher les images](#)
Toujours afficher les images envoyées par harica.gr ou noreply@harica.gr

Validate your email

We have received your request to issue an S/MIME email-only certificate for djany.i@uphf.fr.

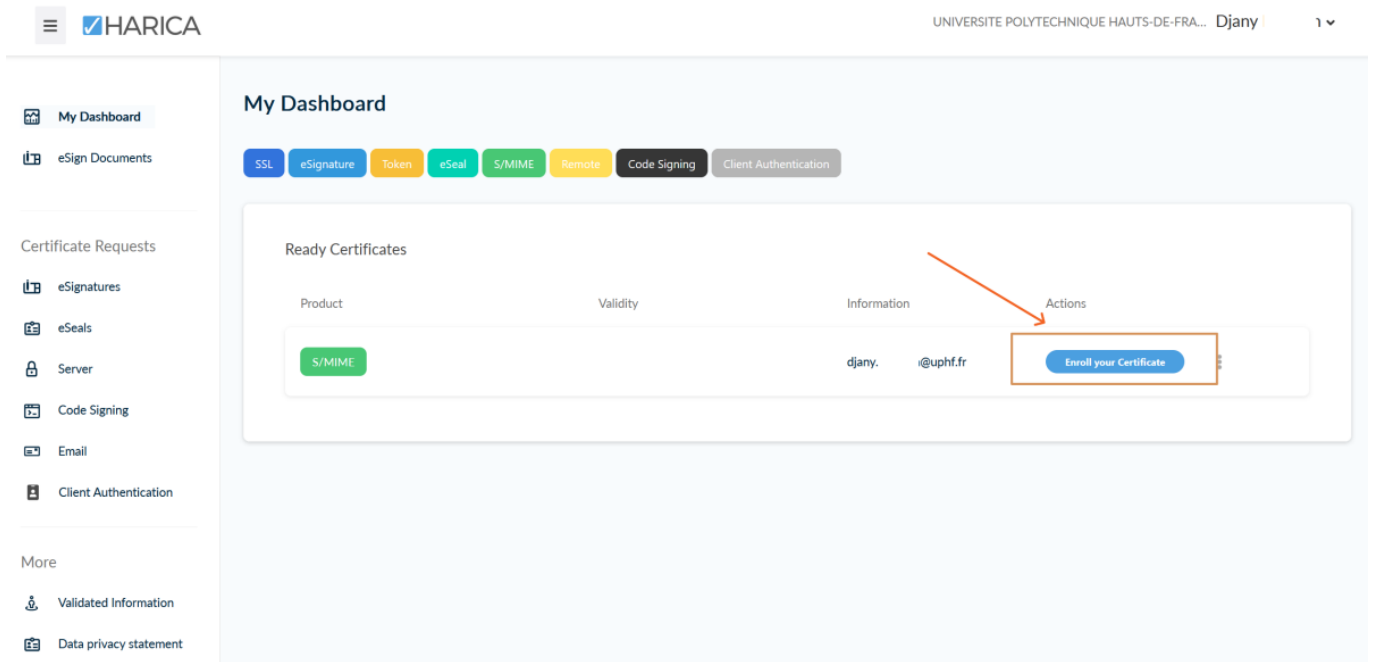
Please confirm that you control the specific e-mail address and that you authorize HARICA to issue a certificate on your behalf by clicking the link below.



Please note that the link is valid for a duration of 24 hours. In case the link expires, log in to [HARICA CertManager](#) and locate your Pending Certificate. Then, press the 3 dots on the right side and select the option to resend the email.

Do you need any assistance? Please contact us here!

- Sur Harica, cliquez sur « Enroll your Certificate »



1. Laissez RSA par défaut

2. Dans le menu déroulant **Key Size**, sélectionnez **4096**

3 et 4. Entrez un mot de passe et confirmez-le dans le champ du dessous

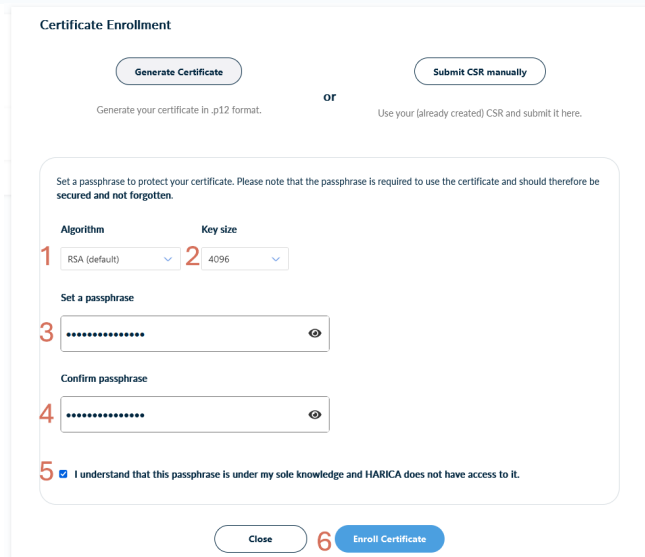
- Ce mot de passe vous servira à valider le certificat pour configurer Zimbra la première fois.

5. Cochez la case « **I understand that my passphrase is under my sole knowledge and HARICA does not have access to it** »

6. Cliquez sur le bouton **Enroll Certificate**

- Vous obtiendrez alors un fichier de certificat **xxxx.p12**

- Cliquez sur « Download »

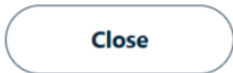




Your certificate is ready. Press the **Download** button to retrieve it.



ATTENTION: This is the ONLY TIME you can perform this action, you cannot download the certificate later.



Importer un certificat dans Zimbra

- Allez dans Zimbra → Préférences → Zimlets et cochez “Messagerie sécurisée”

Mail Contacts Calendrier Tâches Porte-documents 1 Préférences Rocket.Chat

Enregistrer Annuler Annuler les modifications

▼ Préférences

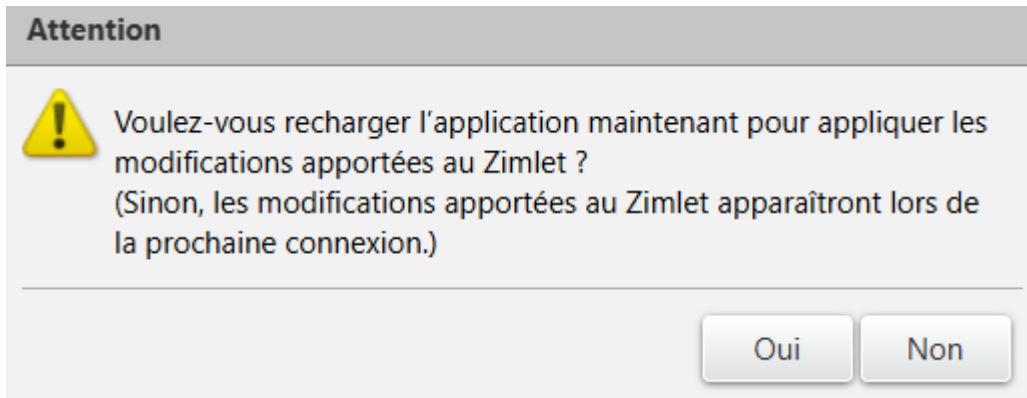
- Général
- Comptes
- Mail
- Filtres
- Signatures
- Hors du bureau
- Adresses acceptées
- Contacts
- Calendrier
- Partage
- Notifications
- Périphériques et applis connectés
- Importer/Exporter
- Raccourcis
- Zimlets 2

Zimlets

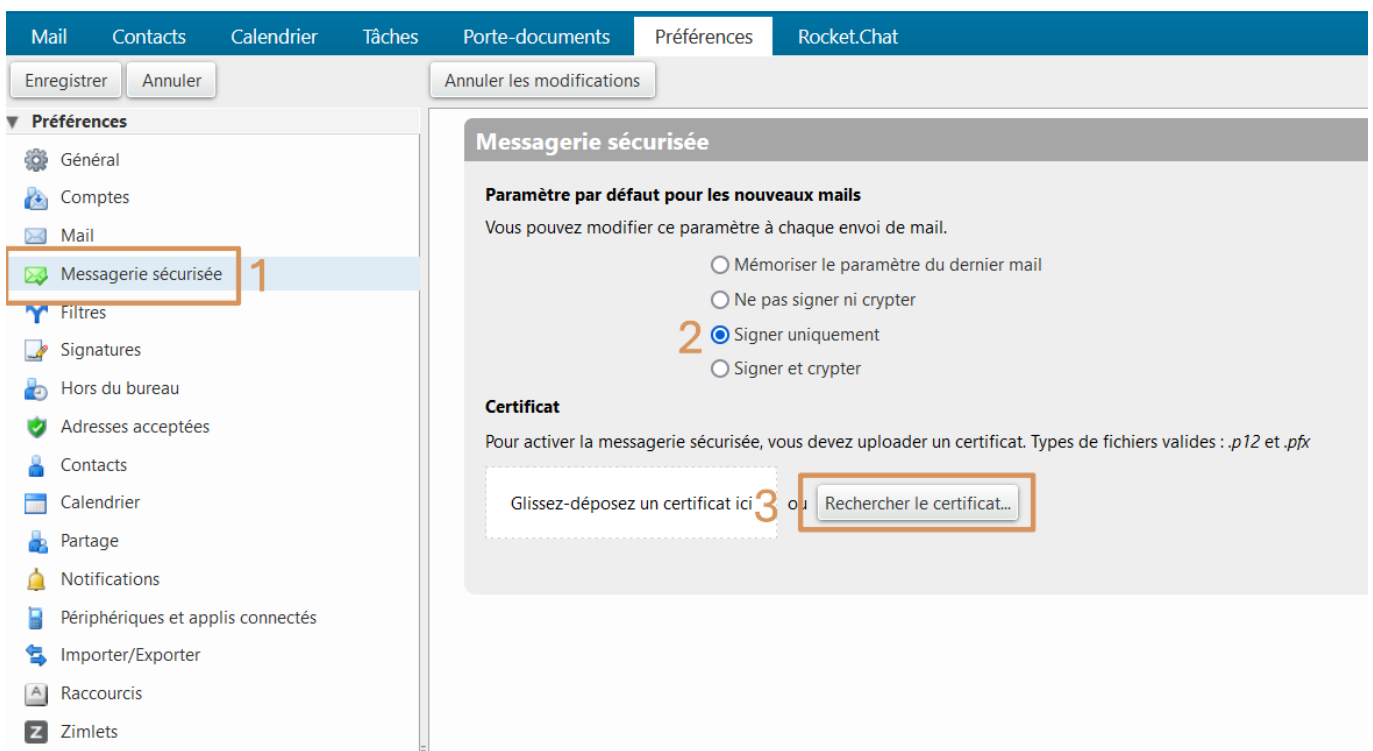
Les "zimlets" sont des applications complémentaires qui améliorent les fonctionnalités de votre client. Cette table permet d'activer et de désactiver les zimlets disponibles.

Actif	Nom	Description
<input checked="" type="checkbox"/>	Calendriers utiles	S'abonner a un calendrier externe.
<input checked="" type="checkbox"/>	Date	Souligne les dates, donne un aperçu des rendez-vous associés et crée un lien vers le calendrier.
<input checked="" type="checkbox"/>	Détails contact mail	Souligne et donne un aperçu des détails contact associés à une adresse mail.
<input checked="" type="checkbox"/>	Email Attacher	Joignez des mails lorsque vous en rédigez un nouveau.
<input checked="" type="checkbox"/>	emailtemplates	Allows users to insert Email Templates
<input checked="" type="checkbox"/>	Joindre contacts	Permet de Joindre des contacts lorsque vous composez un nouveau message.
<input checked="" type="checkbox"/>	Liens URL	Surligner les URL Web à lier dans les mails.
<input checked="" type="checkbox"/>	Messagerie sécurisée	Signer et vérifier les mails avec S/MIME
<input checked="" type="checkbox"/>	Surligneur de recherche	Après une recherche de mail, ce Zimlet surligne les termes de la recherche en jaune
<input checked="" type="checkbox"/>	Undo send	Undo the sending of an email message
<input checked="" type="checkbox"/>	Zimbra Rocket	Zimbra Rocket
<input type="checkbox"/>	Émoticônes Yahoo!	Affiche des images Émoticônes Yahoo! dans les mails

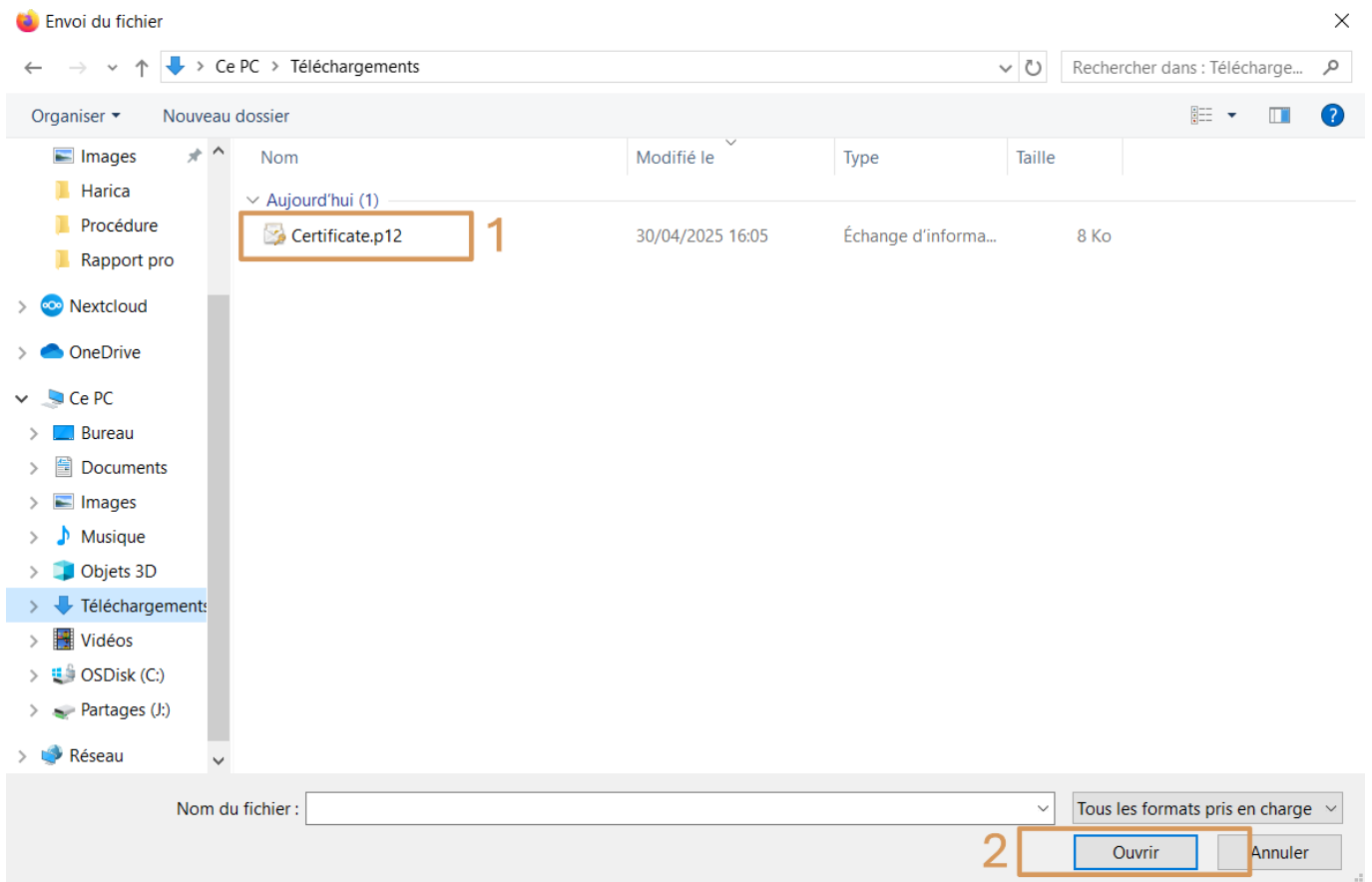
- Une fenêtre apparaîtra pour redémarrer Zimbra. Cliquez sur « Oui »



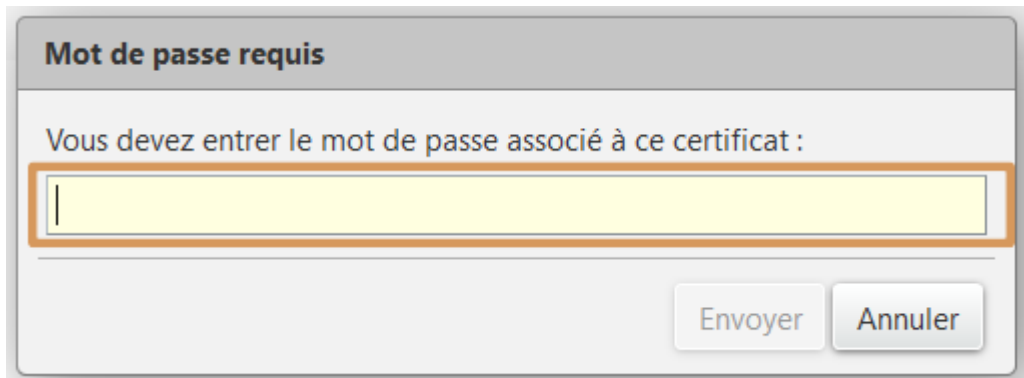
- Retournez dans “Préférences”, sélectionnez “Messagerie sécurisée”, cochez la case “Signer uniquement” et enfin cliquez sur “Rechercher le certificat”



- Sélectionnez votre fichier de certificat **xxxx.p12**



- Enfin, entrez le mot de passe précédemment utilisé lors de la création du certificat et cliquez sur le bouton **Envoyer**



Messagerie sécurisée

Paramètre par défaut pour les nouveaux mails

Vous pouvez modifier ce paramètre à chaque envoi de mail.

- Mémoriser le paramètre du dernier mail
- Ne pas signer ni crypter
- Signer uniquement
- Signer et crypter

Certificat



veronique.

@uphf.fr

[Afficher](#)

[Retirer](#)

- Maintenant que votre certificat est importé. Vous pouvez désormais cliquer sur “Enregistrer”.



Lorsque vous enverrez un mail, un bandeau attestant la certification de votre identité sera maintenant affiché.

La coche indique que Zimbra reconnaît ce certificat comme valide.

Axel Delor <Axel.Delor@uphf.fr>

17:24

À

Signé par Axel.Delor@uphf.fr | [Afficher le certificat](#)

From:

<https://www.uphf.fr/wiki/> - Espace de Documentation

Permanent link:

https://www.uphf.fr/wiki/doku.php/ouils/communication/messagerie/securiser_sa_messagerie

Last update: 2025/11/13 08:28

