

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



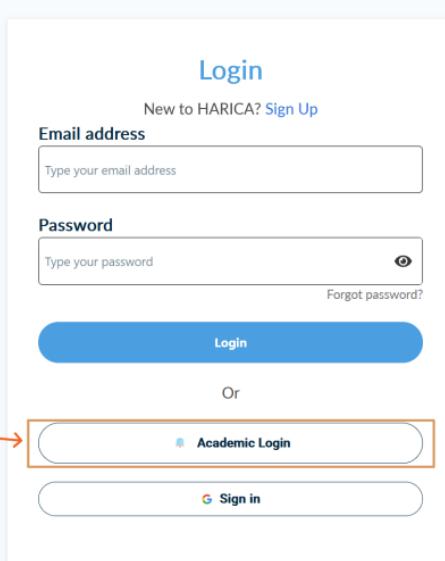
Afin de pouvoir signer des messages vous devez au préalable obtenir un certificat personnel.
Vous pouvez le faire en visitant cette adresse :

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

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

HARICA

EN | GR



The screenshot shows the HARICA login interface. At the top center is the word "Login". Below it is a link "New to HARICA? [Sign Up](#)". There are two input fields: "Email address" and "Password", both with placeholder text "Type your email address" and "Type your password" respectively. To the right of the password field is a "Forgot password?" link. Below these fields is a large blue "Login" button. Underneath the button is the word "Or". Below "Or" are two other login options: "Academic Login" (highlighted with an orange border and a red arrow pointing to it) and "Sign in". At the bottom of the form, there is small text: "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**

The screenshot shows a search interface with a large orange border. At the top, the text "Find Your Institution" and "Your university, organization or company" is displayed. Below this is a search bar containing "UPHF" with a magnifying glass icon. A red arrow points from this search bar down to a result card. The result card also has an orange border and displays "Examples: Science Institute, Lee@uni.edu, UCLA" and a checkbox labeled "Remember this choice" with "Learn More" text. The result itself is "Université Polytechnique Hauts-de... uphf.fr".

- Connectez-vous vec vos identifiants ENT



Service Central d'Authentification (CAS)

The screenshot shows the CAS login page. It features a light blue header with the text "Service Central d'Authentification (CAS)". Below this is a white form area with a red border. The form contains two input fields: "Identifiant :*" and "Mot de passe :*". The "Mot de passe :*" field includes a visibility toggle icon. Below the fields is a yellow "Se connecter" button. To the left of the fields, there is a note: "Entrez votre identifiant et votre mot de passe." and a placeholder "Vous devez entrer votre identifiant.". At the bottom left, there is a note about security: "Pour des raisons de sécurité, veuillez vous [déconnecter](#) et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés." and a note about confidentiality: "Vos identifiants sont strictement confidentiels et ne doivent en aucun cas être transmis à une tierce personne." To the right of the form, there is a dark blue sidebar with white text links: "Mot de passe oublié?", "Activer mon compte", and "Besoin d'aide?".

- Cliquez sur "Email"

The screenshot shows the HARICA dashboard interface. On the left sidebar, there is a list of options: My Dashboard, eSign Documents, Certificate Requests, eSignatures, eSeals, Server, Code Signing, Email (which is highlighted with a red box and has a red arrow pointing to it), and Client Authentication. Below this list is a section titled "More" containing Validated Information and Data privacy statement. At the top right, there is a user profile for "UNIVERSITE POLYTECHNIQUE HAUTS-DE-FRA... Djany". The main content area is titled "My Dashboard" and contains a message: "Your Dashboard is empty, proceed with a certificate request." Above the main content area, there is a navigation bar with buttons for SSL, eSignature, Token, eSeal, S/MIME, Remote, Code Signing, and Client Authentication.

- Selectionnez "Email only"

Email / Request New Certificate

1. Request 2. Payment 3. Activation

Product Details Authorization Summary Submit

Select the type of your certificate

Email-only
S/MIME certificate to sign/encrypt email messages.
Includes:

- Your email address(es)

For individuals or sole proprietorships (IV)
S/MIME certificate to sign/encrypt email messages.
Includes:

- Your email address(es)
- Your personal information

For enterprises or organizations (OV)
S/MIME certificate to sign/encrypt email messages.
Includes:

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

Select Free

Select from 33€ year

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

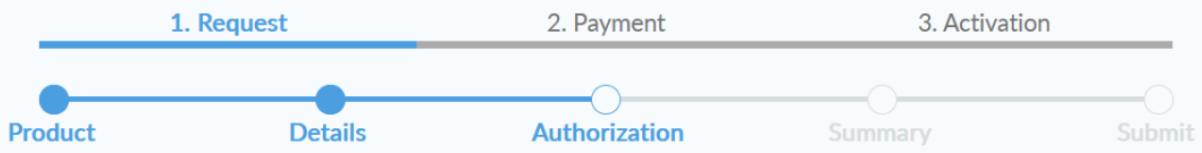
Email Addresses

Include one or more email addresses in your certificate.

email: djany.i...@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

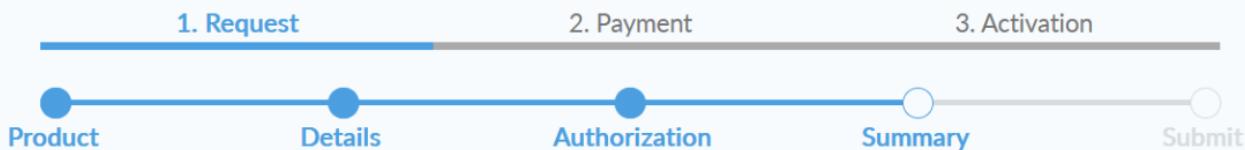
Selected

◀ 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. i@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 | 

 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](mailto: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 »

The screenshot shows the HARICA dashboard with the following interface elements:

- Left sidebar:** My Dashboard, eSign Documents, Certificate Requests, eSignatures, eSeals, Server, Code Signing, Email, Client Authentication, More, Validated Information, Data privacy statement.
- Main content area:** My Dashboard tab selected. Ready Certificates section. A table with columns: Product (S/MIME), Validity (djany. i@uphf.fr), and Actions (button labeled "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 »

The dialog box for Certificate Enrollment contains the following fields and options:

- Algorithm: RSA (default)
- Key size: 4096
- Passphrase: Set a passphrase (3)
- Confirm passphrase: Confirm passphrase (4)
- Checklist: I understand that this passphrase is under my sole knowledge and HARICA does not have access to it. (5)
- Buttons: Generate Certificate, Submit CSR manually, Close, Enroll Certificate (6)



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

Download



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

Close



Sauvegardez votre certificat "xxxx.p12" en lieu sûr !

Importer un certificat dans Zimbra

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

The screenshot shows the Zimbra administration interface under the 'Préférences' tab. On the left, a sidebar lists various configuration categories like Général, Comptes, Mail, etc., with 'Zimlets' selected. A red box labeled '2' highlights this selection. In the main content area, the 'Zimlets' section is displayed with a sub-header: 'Les "zimlets" sont des applications complémentaires qui améliorent les fonctionnalités de votre client. Cette table permet d'activer et de désactiver les zimlets disponibles.' A red box labeled '3' highlights the 'Surveiller la messagerie' checkbox. The table lists 16 zimlets, each with an 'Actif' (Active) checkbox and a 'Nom' (Name) and 'Description' column.

Actif	Nom	Description
<input checked="" type="checkbox"/>	Calendriers utiles	S'abonner à 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	Jointez 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 type="checkbox"/>	Messagerie sécurisée	Signer et vérifier les mails avec S/MIME
<input checked="" type="checkbox"/>	Surveiller la messagerie	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 »

Attention

Voulez-vous recharger l'application maintenant pour appliquer les modifications apportées au Zimlet ?
(Sinon, les modifications apportées au Zimlet apparaîtront lors de la prochaine connexion.)

Oui**Non**

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

The screenshot shows the Zimbra Admin interface with the following details:

- Top Navigation Bar:** Mail, Contacts, Calendrier, Tâches, Porte-documents, **Préférences**, Rocket.Chat.
- Buttons:** Enregistrer, Annuler, Annuler les modifications.
- Left Sidebar (Préférences):** Général, Comptes, Mail, **Messagerie sécurisée** (highlighted with a red box and numbered 1), Filtres, Signatures, Hors du bureau, Adresses acceptées, Contacts, Calendrier, Partage, Notifications, Péphériques et applis connectés, Importer/Exporter, Raccourcis, Zimlets.
- Main Content Area - Messagerie sécurisée:**
 - Section: Paramètre par défaut pour les nouveaux mails**

You pouvez modifier ce paramètre à chaque envoi de mail.

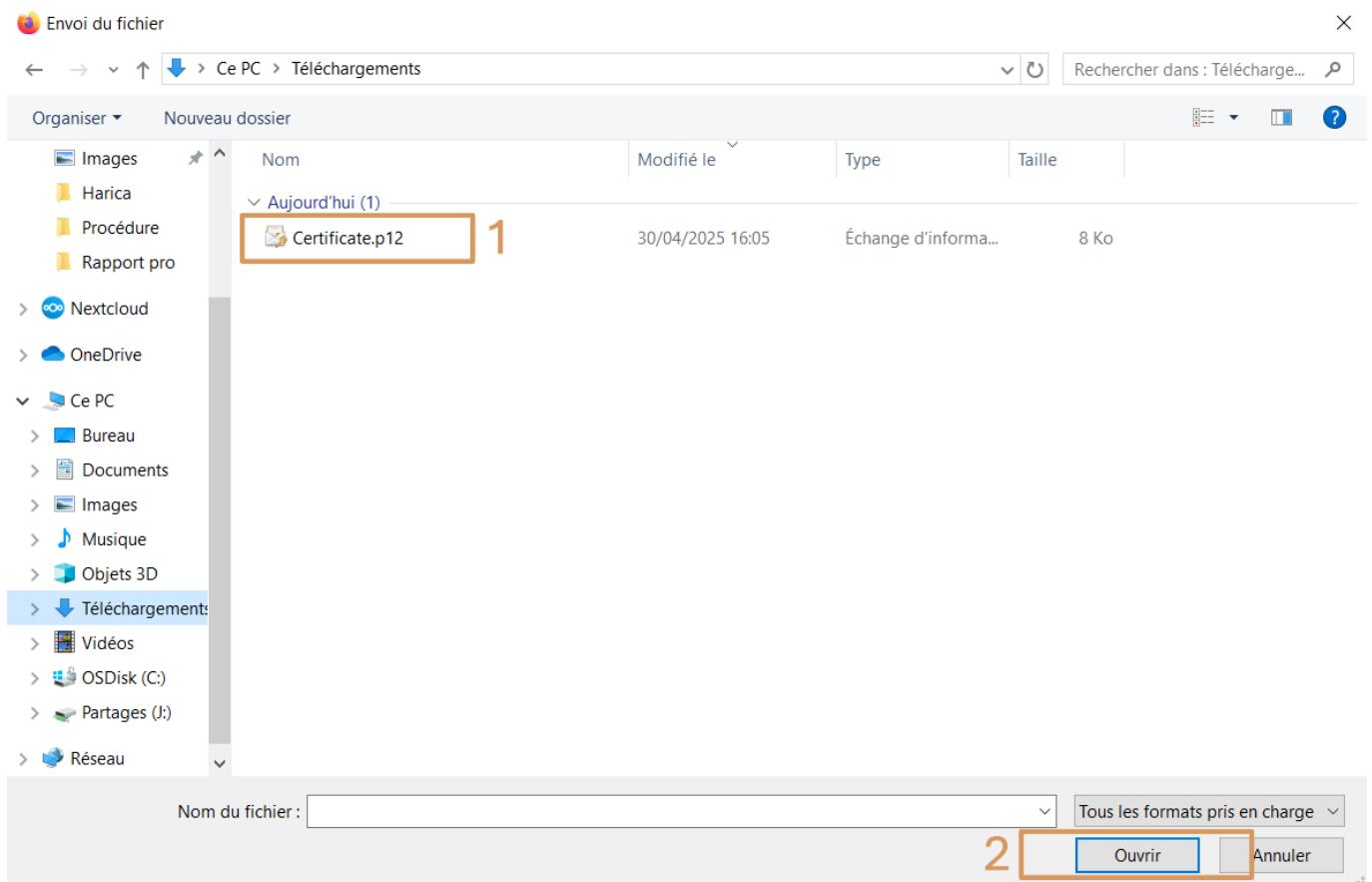
Mémoriser le paramètre du dernier mail
 Ne pas signer ni crypter
 Signer uniquement
 Signer et crypter
 - Section: Certificat**

Pour activer la messagerie sécurisée, vous devez uploader un certificat. Types de fichiers valides : .p12 et .pfx

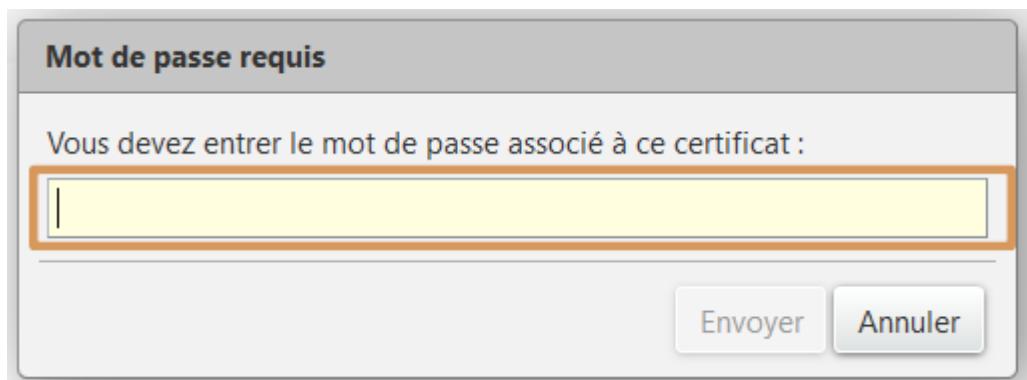
Glissez-déposez un certificat ici **3** ou **Rechercher le certificat...**

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

Last update: 2025/11/13 08:28
outils:communication:messagerie:securiser_sa_messagerie https://www.uphf.fr/wiki/doku.php/outils/communication/messagerie/securiser_sa_messagerie



- 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/outils/communication/messagerie/securiser_sa_messagerie

Last update: **2025/11/13 08:28**

