

Messagerie sécurisée

Vous avez la possibilité dans Zimbra de **signer** et/ou **chiffrer** vos messages.

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.

Chiffrer un message assure au destinataire de votre message que lui seul pourra le lire (le message est enregistré chiffré sur les serveurs, et transite chiffré sur les réseaux).

Chiffrer assure la **confidentialité** du message entre l'expéditeur et le destinataire. Le chiffrement du message que vous envoyez se fait à l'aide de la clé publique de votre destinataire, qui ne pourra déchiffrer le message reçu qu'avec sa clé privée.

Chiffrer impose donc que votre correspondant utilise également un certificat qu'il vous aura communiqué.

Avant de vous lancer dans la procédure, gardez à l'esprit que **vous devez absolument conserver en lieu sûr une copie de votre certificat** (clé privée et clé publique).

Si vous perdez à jamais votre clé privée, vous ne pourrez plus accéder au contenu des messages chiffrés que vous aurez reçus.

A l'usage, n'utilisez le chiffrement que lorsque le besoin de confidentialité est réel.

Comment procéder ?

- [Obtention d'un certificat personnel](#)
- [Renouvellement d'un certificat personnel](#)
- [Import du certificat dans Zimbra](#)
- [Signer un message](#)
- [Chiffrer un message](#)

Obtention d'un certificat personnel

Afin de pouvoir signer et/ou chiffrer des messages vous devez au préalable obtenir un certificat personnel.

Vous pouvez le faire en visitant cette adresse : <https://cert-manager.com/customer/renater/idp/clientgeant>.

Dans le champ de recherche, indiquez "Lorraine" et cliquez sur "Université de Lorraine".

Find Your Institution

Your university, organization or company



Examples: Science Institute, Lee@uni.edu, UCLA

[Université de Lorraine](#)

[univ-lorraine.fr](#)



Université de Lorraine (old version)

[univ-lorraine.fr](#)

CROUS Lorraine

[crous-nancy-metz.fr](#)

Après authentification, renseignez le formulaire ci-dessous en choisissant un mot de passe et cliquez sur le bouton "Submit" :



Digital Certificate Enrollment

You have been authorized to enroll for a digital certificate. Please validate that your name and email addresses are correct.

Name **latoos ESUP**

Email **iatos.esup@univ-lorraine.fr**

Organization **Université de Lorraine**

Please select the correct certificate profile and desired private key format. If a private key is generated a password is required to protect the download.

Certificate Profile

- ☒ GÉANT Personal Certificate
- ☐ GÉANT IGTF-MICS Personal
- ☐ GÉANT IGTF-MICS-Robot Personal

Private Key

- ☒ Generate RSA
- ☐ Generate ECC
- ☐ Upload CSR Choose file No file chosen

P12 Password

P12 Password Confirmation

SUBMIT

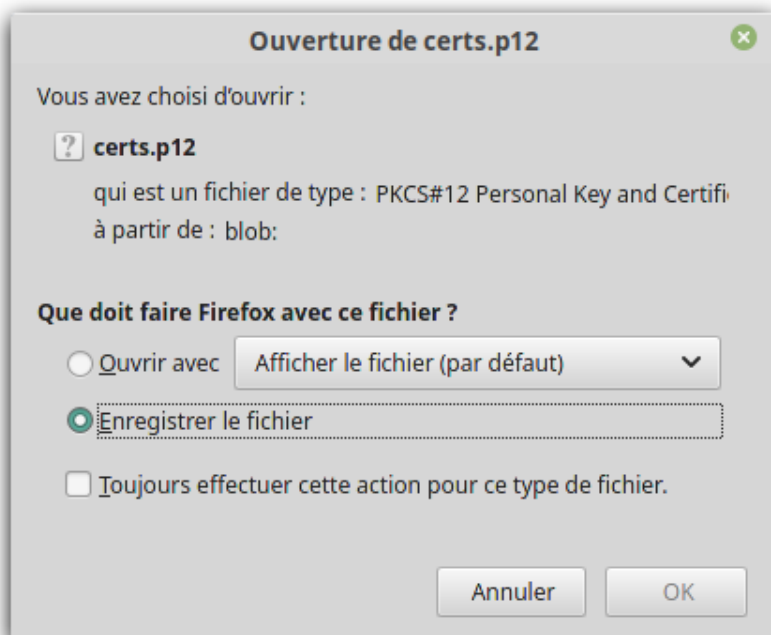
Après acceptation des conditions de licence, téléchargez le fichier nommé certs.p12 qui contient votre certificat et votre clé privée :



Digital Certificate Enrollment



Your certificate has been successfully generated and automatically downloaded to the computer.



Sauvegardez votre certificat .p12 en lieu sûr ! Et n'oubliez pas le mot de passe utilisé pour sa génération.

Vous pouvez à présent importer votre certificat dans Zimbra (cf. ci-dessous).

Renouvellement d'un certificat personnel

Votre certificat a expiré ? Pour le renouveler, suivez les étapes ci-dessous.

Commencez par extraire la clé privée (certs.key) du fichier certs.p12 à l'aide de la commande suivante :

```
openssl pkcs12 -in certs.p12 -out certs.key -nodes -nocerts
```

Ainsi que le certificat (certs.crt) à l'aide de la commande suivante :

```
openssl pkcs12 -in certs.p12 -out certs.crt -nodes -nokeys
```

Générez la demande de certificat (certs.csr) à l'aide de la clé privée (certs.key) et de l'outil [openssl](https://www.openssl.org/) (windows, linux, macOS) :

```
openssl req -key certs.key -out certs.csr -new
```

Rendez-vous sur <https://cert-manager.com/customer/renater/idp/clientgeant> et cette fois, cliquez sur "Upload CSR" et Choose file. Choisissez le fichier .csr généré à l'étape précédent.



Digital Certificate Enrollment

You have been authorized to enroll for a digital certificate. Please validate that your name and email addresses are correct.

Name **Iatoos ESUP**

Email **iatos.esup@univ-lorraine.fr**

Organization **Université de Lorraine**

Please select the correct certificate profile and desired private key format. If a private key is generated a password is required to protect the download.

Certificate Profile

- ☒ GÉANT Personal Certificate
- ☐ GÉANT IGTF-MICS Personal
- ☐ GÉANT IGTF-MICS-Robot Personal

Private Key

- ☐ Generate RSA
- ☐ Generate ECC
- ☒ Upload CSR certs.csr

SUBMIT

Cliquez sur "Submit" et téléchargez votre nouveau certificat (certs.pem).


Créez votre nouveau fichier certs.p12 à l'aide de la commande openssl

```
openssl pkcs12 -export -inkey ../certs.key -in certs.pem -out renew_certs.p12
```

Vous pouvez à présent importer votre nouveau certificat dans Zimbra (cf. ci-dessous).

Import du certificat dans Zimbra

Dans les Préférences de Zimbra, assurez-vous que la Zimlet "Secure Email" est activée. Si elle ne l'est pas, activez-là et rechargez l'interface.


UNIVERSITÉ DE LORRAINE

Mail
Voix
Contacts
Calendrier
Tâches
Porte-documents
Préférences
Chat

Enregistrer
Annuler
Annuler les modifications

Préférences


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

Zimlets

Les "zimlets" sont des applications complémentaires qui améliorent les fonctionnalités de votre client

Actif	Nom	Description
<input checked="" type="checkbox"/>	Calendriers de vacances	Inscrivez-vous aux calendriers de vacances de plusieurs pays.
<input type="checkbox"/>	Cisco Click2Call	Active la fonctionnalité Click2Call de Cisco UC
<input type="checkbox"/>	Messagerie sécurisée	Signez, vérifiez, cryptez et décryptez vos mails avec S/MIME
<input type="checkbox"/>	Modèles de mail	Permet aux utilisateurs d'insérer des Modèles de mail
<input type="checkbox"/>	Préférences vocales	Configurez les paramètres de votre compte vocal
<input checked="" type="checkbox"/>	Secure Email	Sign & verify emails with S/MIME
<input type="checkbox"/>	StickyNotes	Add a sticky note to email messages.
<input type="checkbox"/>	Téléphone CISCO	Souligne les numéros de téléphone pour autoriser les appels de
<input checked="" type="checkbox"/>	YaZiba Chat	Chater avec mes amis
<input checked="" type="checkbox"/>	Émoticônes Yahoo!	Affiche des images Émoticônes Yahoo! dans les mails

Cliquez sur "Secure Email" dans les Préférences, puis importez votre fichier .p12 :


UNIVERSITÉ DE LORRAINE

Mail
Voix
Contacts
Calendrier
Tâches
Porte-documents
Préférences
Chat

Enregistrer
Annuler
Annuler les modifications

Préférences


- Général
- Comptes
- Mail
- Secure Email**
- Filtres
- Signatures
- Hors du bureau
- Adresses acceptées
- Contacts
- Calendrier

Secure Email

Default Setting for New Emails
You can change this when sending an email.


☒ Remember setting from last email
☐ Do not sign or encrypt
☐ Sign only
☐ Sign and encrypt

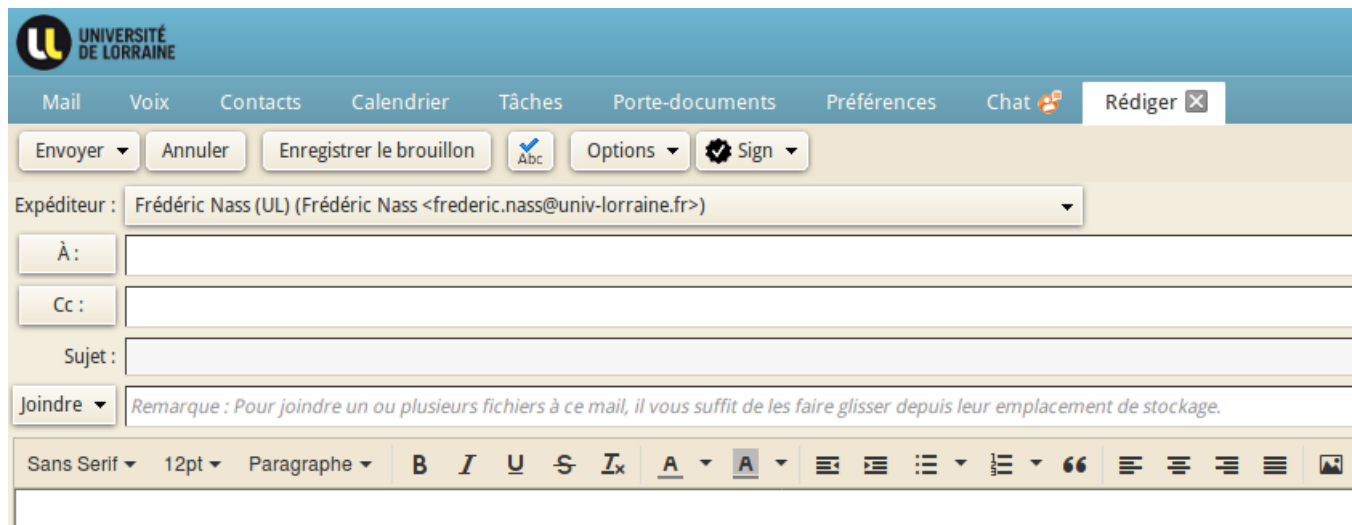
Certificate

 Frédéric Nass <frederic.nass@univ-lorraine.fr> | [View](#) | [Remove](#)

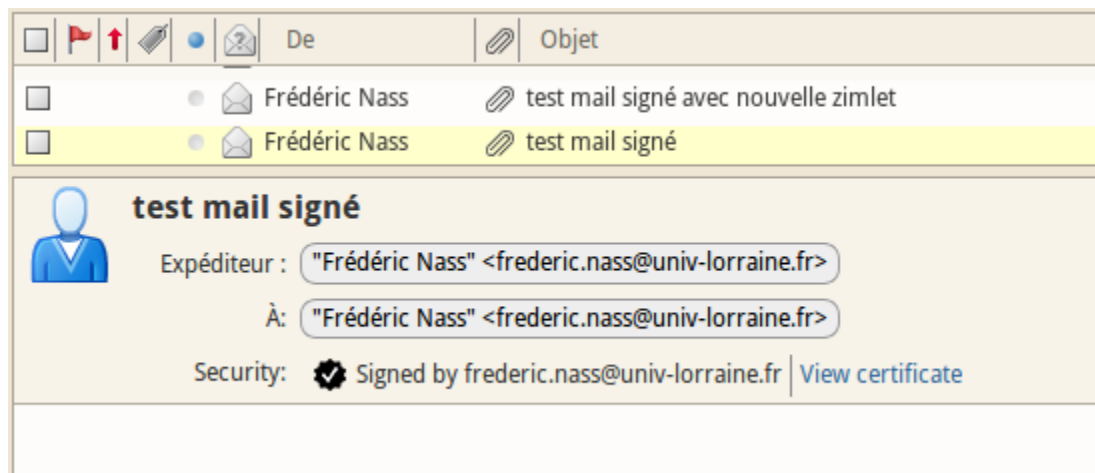
Si l'import échoue, c'est probablement parce que Zimbra ne connaît pas l'autorité de certification ayant émis votre certificat. Prenez contact avec l'équipe en charge de la messagerie via le Helpdesk.

Signer un message

Vous pouvez désormais signer vos messages. Créez un nouveau message, choisissez  Sign dans la barre supérieure et envoyez votre message.



Les messages reçus par vos contacts porteront désormais la mention "Signed by <votre.adresse@univ-lorraine.fr>" attestant que vous êtes bien l'auteur du message.




La coche indique que Zimbra reconnaît ce certificat comme valide.

Chiffrer un message

Vous pouvez désormais envoyer des messages chiffrés, à condition d'ajouter aux fiches de vos contacts, leur clé publique. Cette étape devrait s'effectuer automatiquement dans Zimbra à réception d'un message signé par votre correspondant.

Si toutefois ce n'était pas le cas, voici la procédure à effectuer pour ajouter une clé publique à une fiche contact.

Ouvrez la fiche d'un de vos contacts et ajoutez lui sa clé publique (qu'il vous aura, au préalable, fait parvenir), puis cliquez sur "Enregistrer".



Nass, Frédéric

»

Adresse mail :


Certificate: Valid file types are *.cer, .crt, .der, .spc, .p7b, .p7r, .sst, .sto* and *.pem*

Drag and Drop a certificate here

or

Browse to certificate...


Vous devriez voir ceci après l'ajout





Nass, Frédéric

»



Adresse mail :

Certificate:  frederic.nass@univ-lorraine.fr | [View certificate](#) | [Remove](#)

Créez un nouveau message, choisissez  Sign and Encrypt dans la barre supérieure et envoyez votre message.


UNIVERSITÉ DE LORRAINE

Mail Voix Contacts Calendrier Tâches Porte-documents Préférences

Envoyer Annuler Enregistrer le brouillon  Options  Sign and Encrypt

Expéditeur : Frédéric Nass (UL) (Frédéric Nass <frederic.nass@univ-lorraine.fr>)

À : "Frédéric Nass" <frederic.nass@univ-lorraine.fr>

Cc :

Sujet : test message chiffré

Joindre Remarque : Pour joindre un ou plusieurs fichiers à ce mail, il vous suffit de les faire glisser dep

Sans Serif 12pt Paragraphe B I U S Ix A A

Seul votre correspondant pourra ouvrir ce message, dans Zimbra ou dans son client de messagerie, pour peu qu'il y ait importé préalablement son certificat.

