https://haydn2005.u-bourgogne.fr/dnum-ccub/spip.php?article1067

Messagerie Zimbra - Envoi de messages électroniques sécurisés (cryptés)

- Site Public - FAQ Messagerie -

Date de mise en ligne : mardi 24 mars 2020

Cette procédure de cryptage est à utiliser uniquement pour l'envoi de vos messages nécessitant un très haut niveau de confidentialité. En utilisant cette procédure, vous avez l'assurance que seul votre interlocuteur sera en mesure de décrypter votre message électronique.

Le dispositif comporte néanmoins un grand nombre de contraintes. Aussi, le service messagerie vous recommande de lire attentivement l'avertissement ci-dessous et de n'utiliser cette fonctionnalité que pour l'échange de données réellement sensibles.

AVERTISSEMENT :

Cette fonctionnalité permet de garantir l'authenticité du contenu et de l'expéditeur, ainsi que la confidentialité du contenu. Pour se faire, les deux personnes désirant s'échanger des messages électroniques sécurisés, doivent disposer d'un certificat numérique dont ils se seront échangés la partie publique au préalable. L'émetteur du message pourra chiffrer le contenu de son message à l'aide de la clé publique du destinataire, qui sera alors le seul à pouvoir déchiffrer le message électronique à l'aide de la partie privée de son certificat qu'il est le seul à posséder. De cette manière le message transite sur internet de manière indéchiffrable par les serveurs et administrateurs qui le transmettent.

Ce mécanisme apporte cependant des contraintes (liste non exhaustive) :

- une personne qui perdrait son certificat, ne serait plus en mesure de déchiffrer les messages qui lui ont été adressés de manière chiffrée. Dans ce cas, même les administrateurs du système de la messagerie ne seront plus en mesure de restituer l'accès à ces messages.
- Les outils d'indexation et de recherche des logiciels de messagerie ne sont plus capables d'opérer sur le contenu des messages.
- Les serveurs de messagerie ne peuvent plus assurer le filtrage anti-virus puisqu'ils n'ont plus accès au contenu des messages électroniques.

Cette fonctionnalité est activée sur les serveurs de messagerie de l'uB. Les personnels disposant d'un certificat peuvent transmettre leurs messages sécurisés/cryptés depuis le webmail ou des logiciels de messagerie du type Thunderbird, Outlook, Apple Mail, etc.

Les personnels de l'uB qui ne disposant pas de certificat à titre personnel ou via un organisme pourront se faire attribuer très prochainement des certificats numériques via le service de certification de RENATER en utilisant la fédération d'identités (Shibboleth).

Table des Matières

1- Remarques Préalables :

- Cette fonctionnalité est disponible uniquement dans le client Web évolué (ajax) ou en utilisant un client lourd (thunderbird, Apple Mail, Outlook,etc.). La fonction S/MIME vous permet d'envoyer et recevoir des messages signés numériquement et cryptés.
- Les exemples de configuration et d'utilisation ci dessous s'appliquent uniquement au webmail des personnels de l'université (http://webmail.u-bourgogne.fr)

2- Configurer S/MIME pour envoyer et recevoir des mails cryptés et signés

Pour activer la fonction S/MIME pour votre compte, aller dans Préférences puis Zimlets puis cocher la Zimlet "Messagerie sécurisée". Enregistrer votre modification (bouton en haut à gauche de la fenetre). Vous devrez alors recharger votre navigateur (Ctrl+R dans la plupart des navigateurs). Après rechargement de votre navigateur, une page Sécurité sera alors disponible dans vos Préférences.

Pour utiliser S/MIME avec Client Web de Zimbra, vous devez avoir un certificat de signature de messagerie électronique sécurisée adapté pour la signature et le cryptage S/MIME. Le certificat avec la clé privée doit être installé dans la mémoire de certificats locale sur un ordinateur Windows, Mac OSX, ou dans la mémoire de certificat du navigateur si vous utilisez Firefox. Pour plus d'informations sur la méthode d'installation de votre certificat, reportez-vous à la documentation de l'ordinateur ou du navigateur appropriée.

Pour envoyer et recevoir des messages cryptés et signés, votre clé publique et la clé publique de votre destinataire doivent être échangées. Pour obtenir une copie de la clé publique d'un destinataire, vous pouvez envoyer un message signé numériquement en utilisant votre certificat au destinataire et lui demander de vous envoyer en retour un message signé numériquement. Lorsque le message est reçu, le certificat du destinataire est archivé dans la page Contact du destinataire dans le carnet d'adresses, ou un contact est créé automatiquement.

Lorsque vous travaillez avec des messages cryptés, il existe certaines différences, notamment :

- Si vous partagez votre boîte de réception, les utilisateurs délégués ne peuvent pas lire vos messages cryptés à partir de leurs ordinateurs. Votre clé privée est nécessaire pour lire des messages cryptés.
- Vous ne pouvez pas enregistrer le brouillon d'un message crypté.
- Vous ne pouvez pas lancer le correcteur orthographique pour un message crypté.
- Vous ne pouvez pas rechercher de texte dans le corps ou la pièce jointe d'un message crypté. Seules les informations de l'en-tête telles que l'expéditeur ou le destinataire, la date d'envoi du message ou le sujet peuvent être trouvées lors d'une recherche.

3- Configuration de vos préférences de sécurité pour l'utilisation de S/MIME

Les paramètres par défaut des préférences de sécurité mémorisent automatiquement la dernière option de sécurité sélectionnée lors de l'écriture d'un mail.

Vous pouvez changer les préférences par défaut pour que vos mails soient toujours envoyés comme signés, signés et cryptés ou non signés et non cryptés. Vous pouvez changer cette option à partir de l'onglet Sécurité dans la fenêtre de rédaction du mail, mais le changement ne sera alors effectif que pour ce message.

1. Cliquez sur Préférences.

2. Dans le panneau des préférences, cliquez sur Sécurité.

3. Modifier les paramètres.

- Auto (se souvenir de la dernière configuration) est sélectionné par défaut. La dernière option de sécurité que vous sélectionnez est rappelée
- Sélectionner Ne pas signer ou chiffrer si vous n'utilisez pas du tout le protocole S/MIME ou rarement
- Sélectionner Signer seulement si vous envoyez toujours votre e-mail avec une signature numérique
- Sélectionner Signer et chiffrer si vous envoyez toujours votre e-mail avec une signature numérique cryptée

4. Cliquez sur Enregistrer.

4- Ajout de certificats aux contacts du carnet d'adresses

La page Contact du carnet d'adresses inclut un champ Certificat. Lorsqu'un message avec certificat est reçu d'une personne répertoriée dans votre carnet d'adresses, le certificat est archivé dans la page Contact du destinataire dans le carnet d'adresses.

Si un message signé est reçu à partir d'un destinataire qui n'est pas un contact existant dans votre carnet d'adresses, un nouveau contact est créé automatiquement dans le carnet d'adresses contacts envoyés et le certificat est stocké avec le contact nouvellement généré.

Vous pouvez également uploader le certificat du destinataire s'il est envoyé en pièce jointe.

5- Rédaction et envoi d'un mail signé numériquement

Les messages signés numériquement peuvent être envoyés à des destinataires qui vous ont envoyé leur clé publique et leur certificat. Le certificat du destinataire est archivé dans la page Contact du destinataire dans le carnet d'adresses.

1. Cliquez dans la barre d'outils.
2. Dans le champ À : entrez l'adresse de l'utilisateur ou cliquer sur À : pour rechercher une adresse dans votre carnet d'adresses.
3. Si vos préférences de sécurité ne sont pas configurées par défaut pour envoyer des messages signés numériquement, cliquez sur Sécurité et sélectionnez Signer uniquement.
4. Entrez l'objet du mail.
5. Rédigez le mail.
6. Pour ajouter une pièce jointe, cliquez sur Ajouter pièce jointe et recherchez le fichier ou glissez-déposez le

fichier de votre ordinateur vers l'en-tête du mail.
7. Cliquez sur Envoyer.

6- Rédaction et envoi d'un mail crypté

Remarque : cette fonctionnalité est pour ZCS Network Edition uniquement et est disponible uniquement dans le client Web avancé.

Les messages peuvent être envoyés cryptés à des destinataires qui vous ont envoyé leur clé publique et leur certificat. Le certificat du destinataire est archivé dans la page Contact du destinataire dans le carnet d'adresses.

1. Cliquez sur Nouveau dans la barre d'outils.
2. Si votre préférence de sécurité n'est pas configuré par défaut pour envoyer des messages chiffrés et signés numériquement, cliquer sur Sécurité et sélectionner Signer et chiffrer.
3. Dans le champ À : entrez l'adresse de l'utilisateur ou cliquer sur À : pour rechercher une adresse dans votre carnet d'adresses.
4. Entrez l'objet du mail.
5. Rédigez le mail.
6. Pour ajouter une pièce jointe, cliquez sur Ajouter pièce jointe et recherchez le fichier ou glissez-déposez le fichier de votre ordinateur vers l'en-tête du mail.
7. Cliquez sur Envoyer.

- Vous ne pouvez pas enregistrer le brouillon d'un message crypté.
- Vous ne pouvez pas lancer le correcteur orthographique pour un message crypté.