

MDAemon et OpenPGP

Maxime - 2020-02-18 - MDAemon

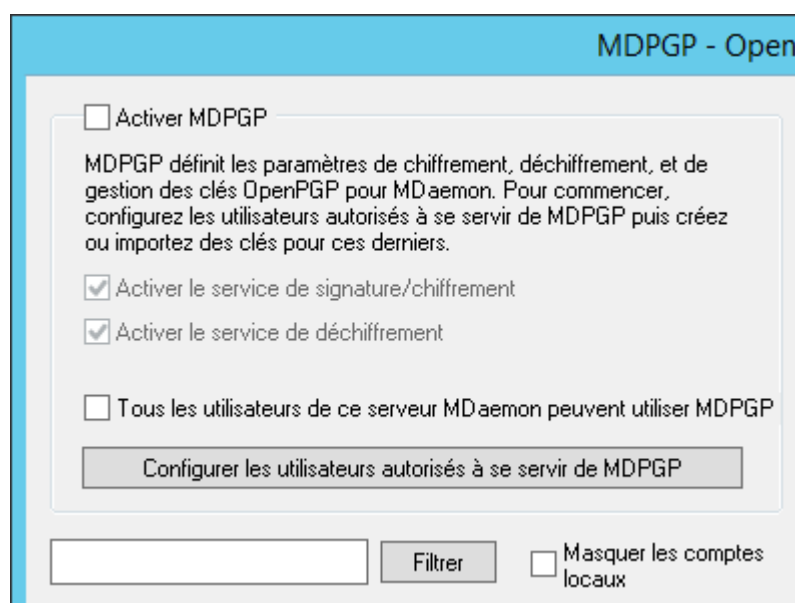
Aujourd'hui, les questions de surveillance et de confidentialité sont de plus en plus abordées. C'est pour cela qu'il est intéressant de se pencher sur le cryptage de mails, afin de garder les échanges de mails confidentiels.

Cet article va donc détailler une des nouvelles fonctionnalités de MDAemon arrivées en 15.5.0, à savoir MDPGP, basé sur le format de cryptographie OpenPGP.

Configurer MDPGP en trois étapes:

1 - Activation du service:

Afin de paramétrer MDPGP, il faut se rendre sur MDAemon puis dans Sécurité > MDPGP. Via ce menu, vous pouvez donc dans un premier temps activer le service, puis ensuite ajouter les utilisateurs qui seront autorisés à l'utiliser.



2 - Paramétrage des utilisateurs:

Après avoir cliqué sur le bouton pour configurer les utilisateurs, Un fichier texte s'ouvre avec des instructions et exemples de droits à affecter aux différents utilisateurs. On retrouve des droits séparés pour crypter, décrypter et signer les mails. Si vous ne voulez pas spécifier les droits pour chaque utilisateurs, vous pouvez bien sûr spécifier des droits pour l'ensemble des utilisateurs d'un domaine, ou pour tous les domaines.

3 - Création de clés:

Vous pouvez soit créer des clés automatiquement, soit créer des clés pour chaque

utilisateur, via le bouton prévu à cet effet. Si vous choisissez de créer les clés via le menu, vous pouvez envoyer la clé publique par mail à l'utilisateur concerné.

Paramètres

- ☒ Signer le courrier automatiquement si la clé privée de l'expéditeur est connue
- ☒ Chiffrer le courrier automatiquement si la clé publique du destinataire est connue
 - ☒ Chiffrer/signer le courrier envoyé entre utilisateurs du même domaine
 - ☒ Chiffrer/signer le courrier envoyé entre utilisateurs de domaines MDaemon locaux
 - ☒ Chiffrer/signer le courrier envoyé par des alias
 - ☐ Chiffrer/signer le courrier envoyé à soi-même
- ☒ Importer automatiquement les clés publiques envoyées par des utilisateurs authentifiés
- ☐ Créer des clés automatiquement

[Créer des clés pour un utilisateur spécifique](#)

Utilisation:

Ensuite pour utiliser les commandes de cryptage et autre, il faut placer au début ou à la fin de votre sujet les arguments suivants:

- pgps - pour signer tous les messages (si possible)
- pgpe - pour crypter tous les messages (si possible)
- pgpx - signifie que vous DEVEZ crypter ce message (bounce pas possible)
- pgpk - si vous mettez uniquement ça dans le sujet, vous recevrez un email avec votre clé publique
- pgpk<Email> si vous mettez uniquement ça dans le sujet, l'adresse e-mail spécifiée recevra sa clé publique par e-mail

Notes et compléments d'information:

- Seuls les messages arrivant en authentification SMTP sont éligibles au cryptage par MDPGP.
- Les messages transférés ne seront pas cryptés.
- Les messages d'auto-répondeur ne seront pas cryptés.
- La révocation de clé n'est pas implémentée
- U.I ne montre que les 500 premiers comptes
- MDPGPUTil.exe est un outil pour crypter et décrypter en ligne de commande
- Opérateur du filtre de contenu de cryptage ne fonctionne pas sur les messages déjà cryptés et obéit à la configuration globale de MDPGP.
- Les messages cryptés sont également signés et ne nécessite pas de faire les deux étapes.