

CHIFFREMENT DES MESSAGERIES D'ENTREPRISE

Nouveautés V6: entretien des messages chiffrés (renouvellement de clés, maintenance du recouvrement...), migration depuis S/Mime, chiffrement sélectif (pièces jointes uniquement).

Chiffrement de bout en bout...

L'utilisateur envoie son email comme d'habitude, le corps du message et les pièces jointes sont chiffrés **automatiquement et de façon transparente**. Lors de la réception, les emails sont déchiffrés localement et le message original est reconstitué.

... avec le secret des utilisateurs

Les messages sont chiffrés puis déchiffrés avec le mot de passe ou le certificat de l'émetteur et du récepteur. Ces secrets ne sont donc pas confiés à des machines/logiciels tiers (VPN, boîtiers de chiffrement, etc.) garantissant ainsi la lisibilité des contenus par les seuls porteurs des clés (droit d'en connaître).

Intégré dans la messagerie d'entreprise

ZedMail est intégré à la messagerie de l'entreprise et est sans impact sur son ergonomie native: une fois l'utilisateur authentifié, les opérations de chiffrement/déchiffrement sont réalisées sans aucune intervention. Les messages transitent chiffrés sur le réseau et au sein du serveur de messagerie.

Échanges et synchronisation sécurisés avec les terminaux mobiles

ZedMail est compatible avec les fonctionnalités de push-mail des messageries d'entreprise. Les messages reçus chiffrés sur le terminal mobile de l'utilisateur seront **déchiffrés localement**.

Chiffrement par certificats

Pour chiffrer les emails, ZedMail utilise les **certificats des destinataires** qu'il recherche automatiquement dans les annuaires habituels de l'entreprise (AD, LDAP), et dans les magasins de certificats personnels de l'utilisateur.

Échanges sécurisés avec les partenaires

Afin d'échanger en chiffré avec des **correspondants externes** à l'entreprise, PRIM'X propose une version gratuite et multiplateforme. **Zed! FREE** permet de lire les messages chiffrés et ses pièces jointes quelle que soit la messagerie du destinataire et d'effectuer, si nécessaire, une réponse chiffrée.

Carnet de mots de passe

Lorsqu'aucun certificat n'est disponible pour le destinataire de l'email, ZedMail génère automatiquement un mot de passe pour ce correspondant et le mémorise dans un carnet

de mot de passe sécurisé qu'il gère pour l'utilisateur. L'émetteur peut donc envoyer ses emails à n'importe quel destinataire sans opération supplémentaire.

Recouvrement

Un plan de recouvrement peut être paramétré par l'entreprise. Il sera appliqué automatiquement et systématiquement par ZedMail de façon à permettre à l'Officier de Sécurité le recouvrement des messages.

Déploiement et administration aisés

L'installation de ZedMail sur les postes de travail est compatible avec les outils d'installation administrée (SMS et autres). La politique de sécurité applicable à la messagerie est définie par l'Officier de Sécurité à l'aide de Politiques de Sécurité.



CARACTÉRISTIQUES TECHNIQUES

ALGORITHMES

AES (128 à 256 bits) et RSA (1024 à 4096 bits).

TECHNOLOGIES

PKCS#1, PKCS#5, PKCS#11, X509, Microsoft CSP, LDAP, compatible PKIx.

SYSTÈME

Disponible pour Windows 7 à 10 et Microsoft Outlook 2007+.

APPLICATIONS MOBILE ZED!

pour iOS et Android.