ZEDMAIL

FOR EMAILS

ENCRYPTED ENTERPRISE MESSAGING

News in V6: Encrypted message maintenance (key renewal, recovery maintenance, etc.), Migration from S/ Mime, Selective encryption (file attachments only)

End-to-end encryption...

Users send their emails as usual, and the body of the message and any email attachments are **automatically and transparently encrypted**. Upon reception, the emails are decrypted locally and the original message is reconstituted.

... with the users' secrets

The messages are encrypted then decrypted with the password or certificate of the sender and the recipient. These secrets are not therefore entrusted to third-party machines/ software (VPN, encryption units, etc.), thereby guaranteeing that the content can only be consulted by those with the keys (Right-toKnow).

Integration in the enterprise messaging application

ZedMail is integrated in the enterprise messaging system and has no impact on the way it runs. Once the user is authenticated, the encryption/ decryption operations take place entirely automatically. The messages transit encrypted over the network and the messaging server.

Secure exchanges and synchronization with mobile terminals

ZedMail is compatible with the push-mail features of enterprise messaging systems: the messages that are received encrypted on the user's mobile terminal will be **decrypted locally**.

Encryption by certificate

To encrypt emails, ZedMail uses the **certificates of the recipients** which it looks up automatically in the usual enterprise directories (AD, LDAP) and in the user's personal certificate stores.

Secure exchanges with partners

In order to **exchange encrypted messages** with correspondents outside the company, Prim'X proposes a free, multi-platform version: **Zed! FREE**. With this, it is possible to consult encrypted messages and attached files whatever the messaging system of the recipient, and for the latter to reply in encrypted form.

Integrated password wallet

When no certificate is available for the email recipient, ZedMail automatically generates a password for this correspondent and saves it in a password file (wallet) that it manages

for the user. The sender can therefore send emails to any recipient with no additional operation required.

Recovery

A recovery plan may be configured by the company. It will be applied automatically and systematically by ZedMail so as to enable the Security Officer to recover the messages.

Easy deployment and administration

The installation of ZedMail on workstations is compatible with the administered installation tools (SMS et al.). The security policy applicable to the messaging system is defined by the Security Officer using Windows Security Strategies (Policies).

TECHNICAL SPECIFICATIONS

ALGORITHMS
AES (128 to 256 bits) and RSA (1024 to 4096 bits).

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

SYSTEM
Available for Microsoft Outlook 2007+. Available for Windows 10 to Windows 7.

ZED! MOBILE APP
for iOS and Android.