FACT SHEET

Email Encryption

Échange d'email crypté à tous les niveaux grâce au cryptage des emails, pour une communication sécurisée et fiable des emails.

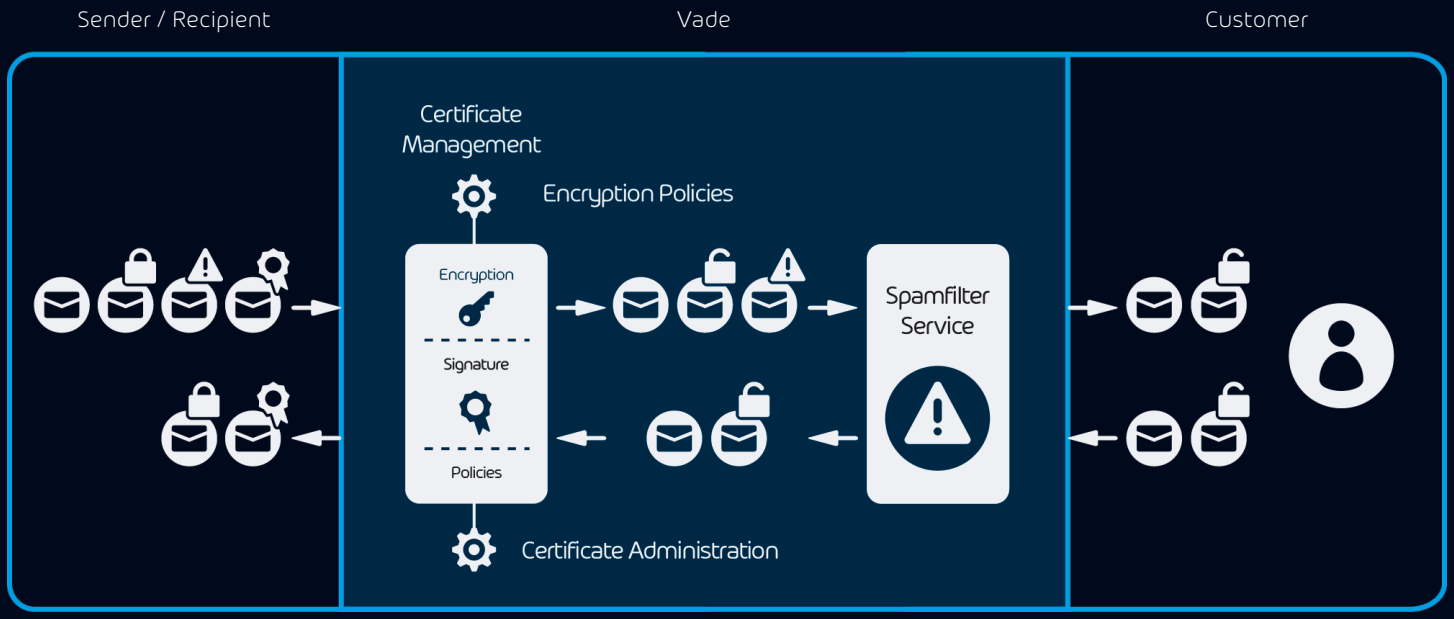
Les emails professionnels contiennent souvent des informations internes, personnelles ou sensibles qui pourraient être interceptées et consultées sans autorisation si elles n'étaient pas protégées de manière adéquate. Avec Email Encryption, les informations confidentielles contenues dans les messages électroniques sont cryptées de manière efficace et sécurisée.

Protection contre :

- **Manipulation de messages électroniques**
- **Espionnage**
- **Exploitation d'informations confidentielles**

Intégration du cryptage des emails dans le système de gestion des emails

Email Encryption de Vade prend en charge tous les aspects de la gestion des certificats.
Le cryptage, le décryptage et la signature s'effectuent de manière entièrement automatique et transparente pour les emails entrants et sortants. La et l'utilisation d'une protection contre le spam et les logiciels malveillants sont nécessaires pour garantir les fonctions et l'efficacité d'Email Encryption.



FACT SHEET

Email Encryption

Des fonctions complètes pour l'échange sécurisé d'email :

- Signature numérique automatique et cryptage des emails sortants via S/MIME et PGP : sécurisation des emails contre les modifications non autorisées ou l'inspection par des tiers lors de la transmission sur des réseaux publics.
- Gestion automatique des certificats et stockage des clés : Vade se charge de l'obtention et de l'installation des certificats nécessaires*, qui sont conservés et centralisés.
- Certificats de messagerie personnelle : Vade utilise des certificats codés sur 2048 bits provenant de l'une des autorités de certification (AC) les plus importantes et les plus réputées. Lors du cryptage avec S/MIME, chaque utilisateur reçoit son propre certificat. Il est également possible d'importer et d'utiliser des certificats fournis par le client.
- Décryptage automatique d'email entrant : Si la clé publique de l'expéditeur est disponible, les emails sont automatiquement déchiffrés et remis au destinataire.
- Configuration individuelle et définition des directives de cryptage : Le panneau de contrôle permet de définir les types de cryptage utilisés pour établir le contact avec les partenaires de communication : TLS, S/MIME, PGP ou Websafe. Ceci est possible soit en pack, soit individuellement pour des utilisateurs, des groupes ou des domaines spécifiques. En outre, vous pouvez définir comment procéder si la clé d'un destinataire n'est pas disponible.
- Test de l'option de cryptage : Dans le panneau de configuration, vous pouvez vérifier les options de cryptage prises en charge par le partenaire de communication. L'adresse email du destinataire est saisie et la technologie de cryptage qui peut être utilisée dans la communication avec cette adresse est ensuite affichée.
- Communication confidentielle via Websafe : Même si le partenaire de communication ne peut pas recevoir les emails cryptés, le cryptage et la confidentialité des communications par courriel avec certaines personnes sont garantis.

*L'abonnement à un certificat peut entraîner des frais supplémentaires conformément à la liste des prix.

Chiffrement automatique avec un minimum d'administration :

- Gestion des certificats d'utilisateur : De nouveaux certificats pour les utilisateurs peuvent être demandés, renouvelés ou obtenus définitivement via le panneau de contrôle (abonnement S/MIME).
- Évolutivité adaptable : Il est toujours possible d'adapter le nombre d'utilisateurs d'email crypté aux besoins du client.
- Mise à jour automatique : grâce au service de cryptage cloud, les entreprises disposent toujours de la dernière version du service.