ConfiMail

Présentation OSSIR

La Messagerie Sécurisée sans déploiement logiciel

Guillaume Rigal

SAFE LOGIC

ConfiMail

Plan de la Présentation

- **Messagerie : constat et risques encourus**
- **La Solution ConfiMail**
- **Les Avantages supplémentaires**
- **L'Offre**
- **En résumé…**

SAFE LOGIC

Constat

Les principaux problèmes de sécurité avec les e-mails traditionnels (SMTP/POP3/IMAP) :

- Circulation des e-mails en clair sur Internet
- Stockage en clair et persistant sur les relais SMTP
- Pas d'authentification possible de l'émetteur
- Usurpation d'"identité" très facile
- Falsification possible du contenu

Constat

Les principaux inconvénients des solutions classiques de sécurisation de messagerie :

- Déploiement des logiciels sur les postes clients
- Gestion des clés ou de la PKI
- Complexité pour les utilisateurs
- Gestion complexe des nomades / en externe
- Coûts associés

Risques encourus

Dès qu'un e-mail circule ou est stocké en clair, les principaux problèmes sont les suivants :

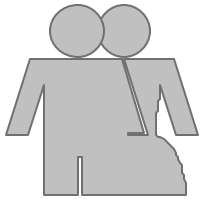
- Pas de confidentialité
- Pas de contrôle de l'intégrité
- Pas d'authentification des parties

Solution ConfiMail

ConfiMail

E-mails
Besoins en sécurité

Contraintes de mise en oeuvre



ConfiMail

Solution ConfiMail

ConfiMail a été conçu dès le départ :

- Pour garantir la confidentialité et l'intégrité des messages échangés de bout en bout
- Pour s'intégrer facilement à l'architecture existante (SMTP/POP3)
- Comme une application Web ("WebMail") simple d'utilisation et ne nécessitant pas de déploiement

SAFE LOGIC

ConfiMail

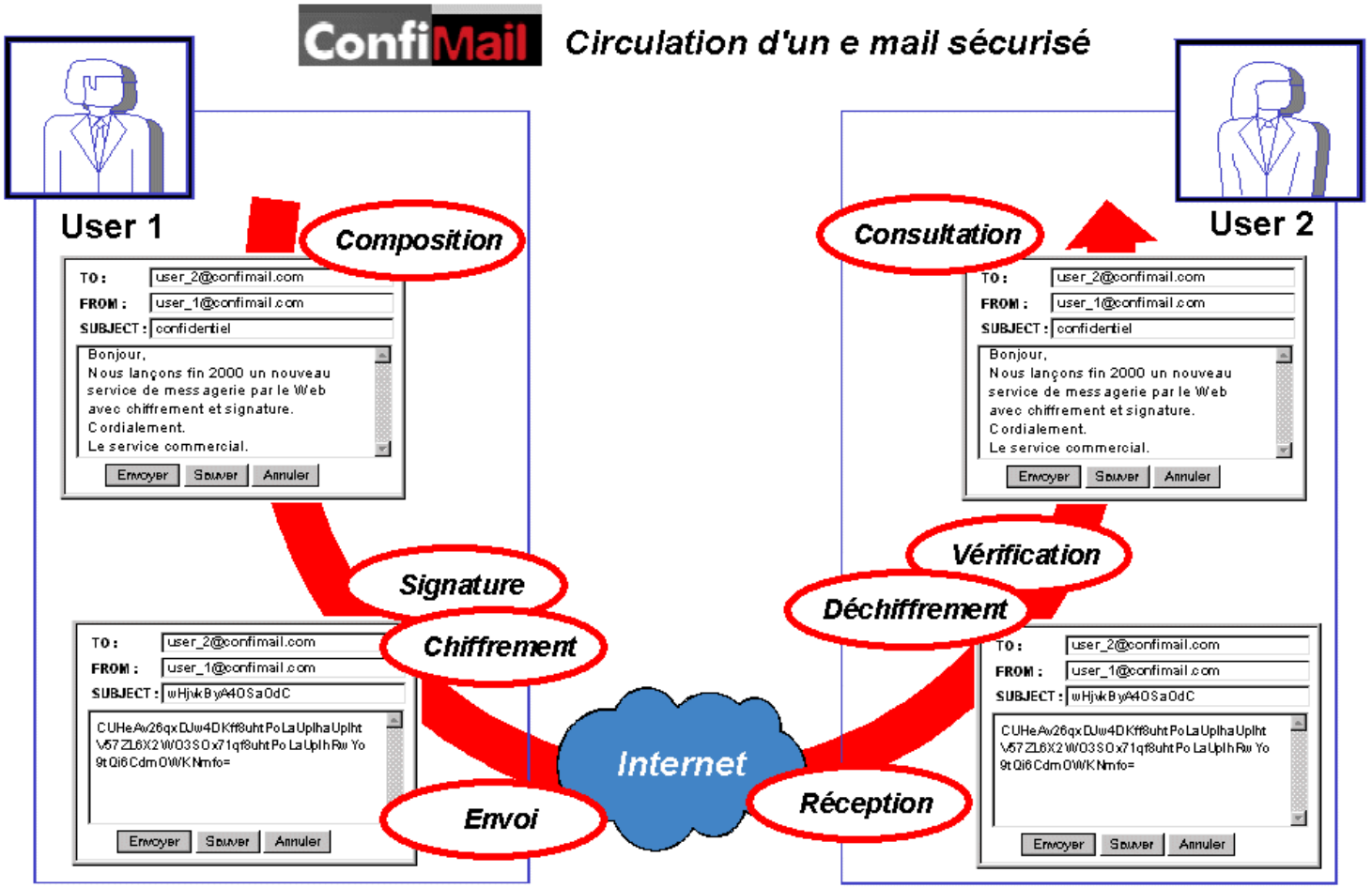
Solution ConfiMail

ConfiMail assure de **bout en bout** la confidentialité et l'authenticité des e-mails :

- **Signature** et **Chiffrement** sur le PC de l'expéditeur
- Le message "sort" chiffré du PC de l'expéditeur
- Le message "entre" chiffré sur le PC du destinataire
- **Déchiffrement** et **Vérification** sur le PC du destinataire

SAFE LOGIC

Solution ConfiMail



ConfiMail

Solution ConfiMail

ConfiMail utilise des algorithmes reconnus et largement utilisés en cryptographie :

- Chiffrement hybride avec
  - **RSA** en asymétrique (clés de 1024 ou 2048 bits)
  - **Blowfish** en symétrique (clés de 128 bits)
- Signature avec **RSA/MD5/PKCS#1**
- Hachage **MD5**
- Générateur de pseudo-aléa **ANSI X9.17**

SAFE LOGIC

ConfiMail

Solution ConfiMail

La technologie de chiffrement de bout en bout de ConfiMail garantit que :

- Aucune information ne circule en clair sur le LAN et/ou l'Internet.
- Aucune information n'est stockée en clair ni sur les points relais (serveurs SMTP), ni sur le serveur ConfiMail.
- Seuls l'expéditeur et les destinataires peuvent lire le message.

SAFE LOGIC

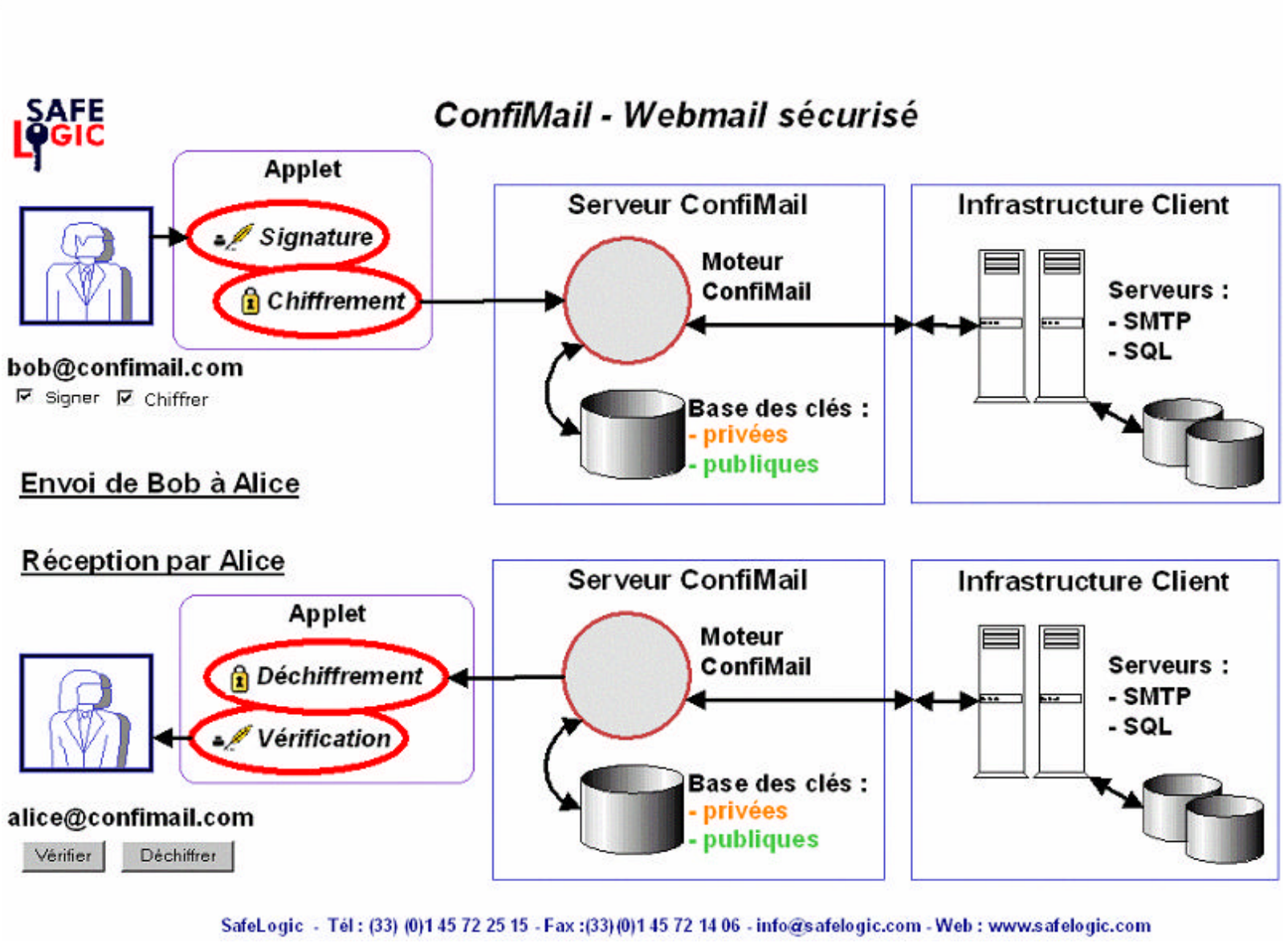
ConfiMail

Solution ConfiMail

ConfiMail s'intègre simplement à l'infrastructure existante :

- En complément des serveurs SMTP/POP3
- En passant les firewalls (requêtes sur les ports 80 et 443)
- Grâce à la souplesse de son architecture en racks

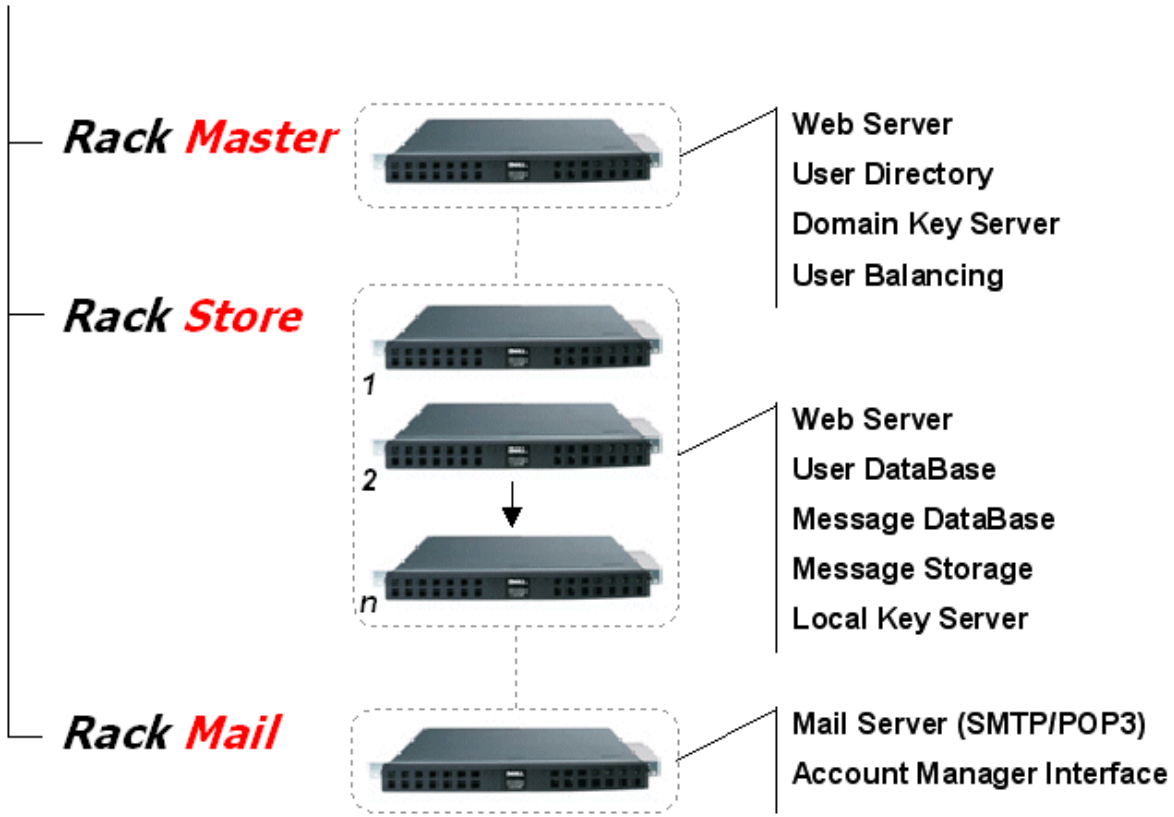
SAFE LOGIC


SAFE LOGIC
ConfiMail - Webmail sécurisé
Applet
Signature
Chiffrement
bob@confimail.com
Signer
Chiffrer
Envoi de Bob à Alice
Serveur ConfiMail
Moteur ConfiMail
Base des clés :
- privées
- publiques
Infrastructure Client
Serveurs :
- SMTP
- SQL
Réception par Alice
Applet
Déchiffrement
Vérification
alice@confimail.com
Vérifier
Déchiffrer
Serveur ConfiMail
Moteur ConfiMail
Base des clés :
- privées
- publiques
Infrastructure Client
Serveurs :
- SMTP
- SQL
SafeLogic - Tél : (33) (0)1 45 72 25 15 - Fax :(33)(0)1 45 72 14 06 - info@safelogic.com - Web : www.safelogic.com

ConfiMail

Solution ConfiMail

SafeLogic WebMail Racks Architecture



SAFE LOGIC

ConfiMail

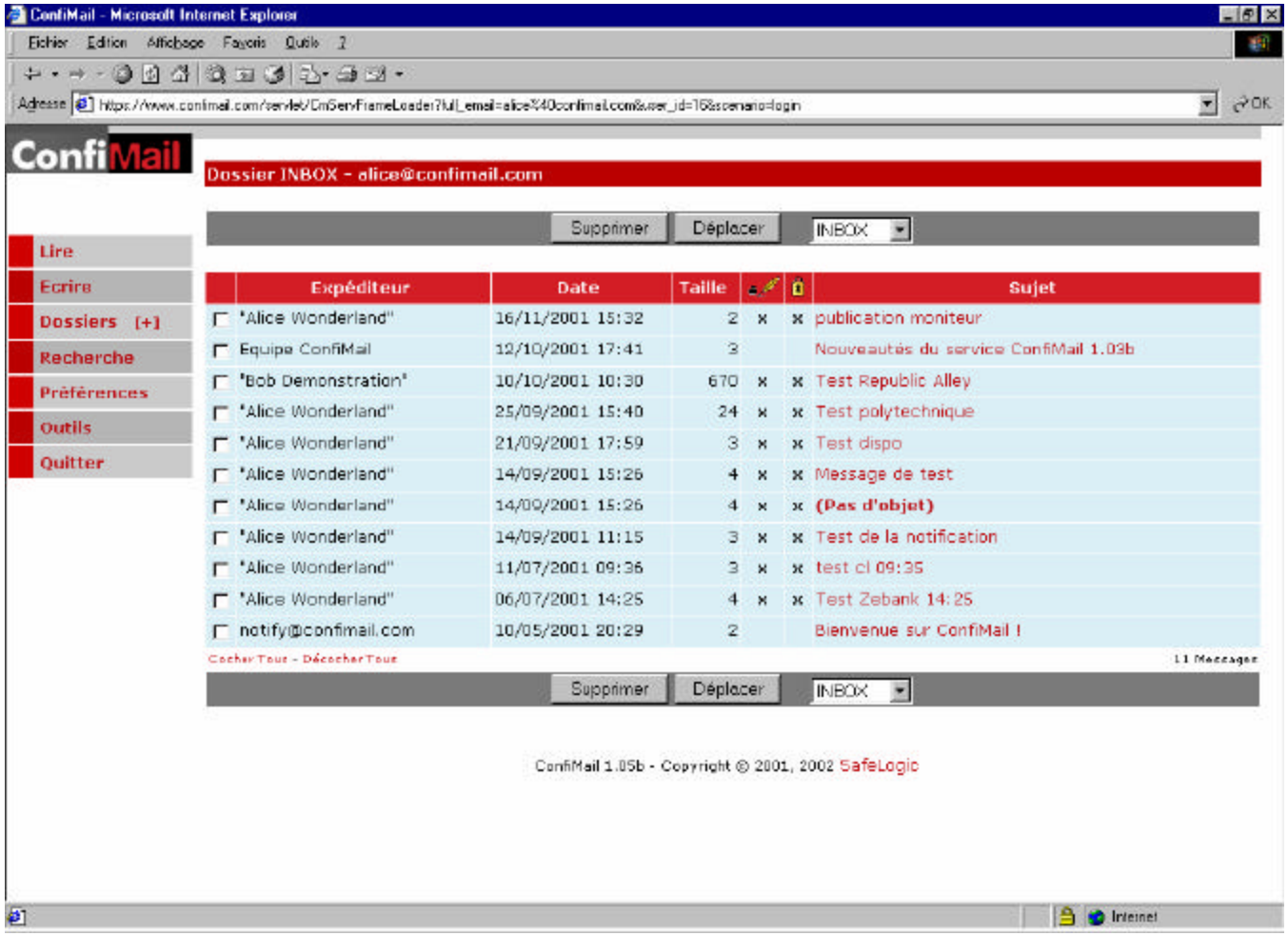
Solution ConfiMail

ConfiMail est un "**WebMail**" et bénéficie ainsi d'une interface :

- **Ergonomique et familière** (type Yahoo!Mail, …)
- Disponible pour les principaux navigateurs (**Internet Explorer** 4, 5, et 6 et Netscape 6)
- HTML et totalement **personnalisable** (HTML, CSS, charte graphique)
- Entièrement **Multilingue**
- Les opérations de cryptographie sont assurées par une Applet signée et invisible

SAFE LOGIC

Solution ConfiMail



Solution ConfiMail

Les principales caractéristiques de ConfiMail :

- Application de cryptographie utilisant des algorithmes et clés standards réputés fiables
- Application "WebMail" avec les fonctionnalités classiques (dossiers, filtres, recherche, …)
- Application de messagerie à part entière :
  - Protocoles standards (SMTP et POP3)
  - Fonctionnalités : to, cc, bcc, reply, forward, …

SAFE LOGIC

ConfiMail

Les autres Avantages

ConfiMail bénéficie d'atouts complémentaires :

- Architecture "scalable" (racks)
- Brevet "SafeStreaming" pour le chiffrement en flux
- Démarche Qualité et Audit
- La simplicité
- Gestion transparente des clés

SAFE LOGIC

ConfiMail

Les autres Avantages

La technologie ConfiMail s'appuie sur le brevet "SafeStreaming" :

- Dépôt Demande N° 01/02351 – 21/02/2001
- Technologie exclusive de "streaming" qui permet de chiffrer et déchiffrer en continu des flux de taille très importante
- Les opérations sont emboîtées et s'opèrent en série sur le buffer de données en envoi :

Signature > Compression > Chiffrement > Codage

SAFE LOGIC

Les autres Avantages

Avantages majeurs du brevet "SafeStreaming" :

- Permet de chiffrer et signer des envois de taille très importante (dizaines ou centaines de Mo)
- A niveau constant d'utilisation des ressources (CPU, bande passante, RAM)
- Sans recourir à des techniques de mémoire virtuelle (mémoire swap, fichiers tampons,...)
- Avantage concurrentiel fort

SAFE LOGIC

ConfiMail

Les autres Avantages

La solution ConfiMail fait l'objet d'une démarche « Audit et Qualité » pour les développements et la production :

- Qualité logicielle
- Audits de sécurité
- Fiabilité des serveurs

SAFE LOGIC

Les autres Avantages

Qualité logicielle :

- Conception et Développement Orienté Objet
- Langages : Java 1.3, SQL Ansi2
- Normes et protocoles : XML, MIME, SMTP, POP3, HTTP
- Subvention ANVAR en 2001 et 2002

ConfiMail

Les autres Avantages

Audits de sécurité :

- Audit conception du système par les experts en cryptographie de Cryptolog (www.cryptolog.com)
- Audits de vulnérabilités des serveurs par Qualys

Fiabilité de la plate-forme :

- Intégrité du système surveillée par Lastwall
- Fiabilité du serveur Linux RedHat avec Apache, Tomcat, Postgres

SAFE LOGIC

Les autres Avantages

La simplicité est un atout en terme de sécurité :

- ConfiMail est une application modulaire (COO)
- Simple à administrer
- Simple pour l'utilisateur final

La gestion des clefs :

- Transparente : Cette notion est « masquée » à l'utilisateur (ergonomie et confort)
- Arborescente et sûre (certification technique)

SAFE LOGIC

Offre ConfiMail

L'offre de logiciel et de service ConfiMail se décline selon 3 axes :

- Offre ***Enterprise Server***
- Offre ***Business*** en ASP
- Offre ***ConfiMail Online Shop***

ConfiMail

Offre ConfiMail

L'offre ***ConfiMail Enterprise Server*** :

- Destinée aux Grands Comptes et Portails
- Serveurs préconfigurés
- Architecture en racks :
  - Gestion de fortes charges.
  - "Scalability" et souplesse.
- Marque blanche (interface personnalisée)
- Vente en direct et indirect (via réseau de partenaires intégrateurs)

SAFE LOGIC

ConfiMail

Offre ConfiMail

Les offres en ASP ***Business*** et ***Online Shop*** :

- Vente de comptes sur le site confimail.com
- Paiement sécurisé en ligne par CB
- Offre à destination :
  - Des PME/TPE
  - Des particuliers
  - Des clients de comptes disposant déjà de ConfiMail

SAFE LOGIC

ConfiMail

En résumé

ConfiMail est une application Web ("WebMail") de sécurisation de messagerie simple d'utilisation.

SafeLogic met en œuvre son expertise, notamment en cryptographie et réseau, pour garantir la confidentialité des échanges de ses clients.

ConfiMail est disponible en infrastructure de serveurs flexible et en ASP.

SAFE LOGIC

Questions / Démonstration

http://www.confimail.com

Guillaume RIGAL - Directeur R&D
grigal@safelogic.com

SafeLogic
7, boulevard de Dixmude
75017 Paris - FRANCE
Tél : (33) 01 45 72 25 15
Fax : (33) 01 45 72 14 06