Dossier technique

SECURITE DE LA MESSAGERIE

Septembre 2005

Groupe « Sécurité de la messagerie »

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS

30, rue Pierre Sémard, 75009 PARIS
Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88 – e-mail : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

Table des matières

Le CLUSIF III
Remerciements V
1 - Introduction 2
2 - Périmètre 3
3 - Architectures / protocoles 6
3.1. Les bases du courrier électronique 6
3.1.1 Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à la même entreprise (Intranet) 6
3.1.2 Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à des entreprises différentes (Internet ou extranet) 8
3.1.3 Illustration de l'accès à un serveur de messagerie à partir d'un navigateur (Webmail) pour le retrait d'un e-mail 10
3.1.4 Constitution de l'architecture de la messagerie 11
3.2. Structure et format de l'e-mail 13
3.3. Définition des protocoles 17
3.3.1 Le protocole SMTP (Simple Mail Transfer Protocol) 18
3.3.2 Le protocole ESMTP (Extended Simple Mail Transfer Protocol) 18
3.3.3 Le protocole POP3 (Post Office Protocol) 19
3.3.4 Le protocole IMAP (Internet Message Access Protocol) 20
4 - Menaces et Risques 21
4.1. Les atteintes aux flux identifiés par l'entreprise comme « légitimes/autorisés » .. 21
4.1.1 Perte d'un e-mail 21
4.1.2 Perte de confidentialité 21
4.1.3 Perte d'intégrité 22
4.1.4 Usurpation de l'identité de l'émetteur 22
4.1.5 Répudiation 22
4.2. Les atteintes à l'infrastructure et au SI 23
4.2.1 Programmes malveillants 23
4.2.2 Spam 23
4.2.3 La perte de pièces justificatives 23
4.2.4 L'interruption de service 24
4.2.5 Utilisation abusive d'« open relay » 24
4.3. Les atteintes à l'organisation 25
4.3.1 Les contenus illicites ou offensants 25
4.3.2 L'utilisation abusive 25
4.3.3 Accomplissement d'actes frauduleux par la messagerie 25
4.3.4 Le phishing 25
5 - Solutions de sécurité 26
5.1. Sécurisation des flux légitimes 26
5.1.1 Chiffrement et signature électronique des messages 26
5.1.2 La sécurisation des protocoles 29
5.1.3 Traçabilité des échanges 34
5.2. Sécurisation des Infrastructures 37
5.2.1 Architecture générale 37
5.2.2 Filtrage et analyse de contenu 38
5.2.3 Tableau d'analyse des options d'implémentation 42
5.3. Solutions Organisationnelles 46
5.3.1 Politique de sécurité et charte d'utilisation 46

 © CLUSIF 2005

5.3.2 Les bonnes pratiques de l'utilisateur 46
5.3.3 Les bonnes pratiques de l'administrateur 47
5.4. Critères de choix d'une solution 48
6 - Réglementation 51
6.1. Quels sont les risques de la non fiabilité d'un système de messagerie ? 51
6.2. Quelles sont les composantes d'un système de messagerie électronique fiable ? . 52
6.3. L'environnement légal 53
6.3.1 Le cadre législatif global 53
6.3.2 Le cadre législatif de la cyber–surveillance des salariés 54
7 - Annexes 58
7.1. Glossaire 58
7.2. Protocoles : références RFC 61
7.3. Codes retour SMTP 62
7.4. Exemples d'e-mails 64
7.4.1 E-mail signé 64
7.4.2 E-mail chiffré 65
7.5. Exemple de charte 66

LE CLUSIF

Le CLUSIF offre, depuis 1984, un espace d'échange dans lequel les acteurs de la sécurité des systèmes d'information peuvent se rencontrer, travailler et progresser ensemble. A ce jour, le CLUSIF rassemble plus de 600 membres, appartenant à 300 organismes ou sociétés. Sa particularité est d'accueillir les utilisateurs comme les offreurs. De cette complémentarité naît une synergie.

Sa mission

Echanger

La vocation du Clusif est de favoriser le partage des expériences.
Les utilisateurs sont ainsi tenus au courant des nouveautés en matière de sécurité et les offreurs ont accès à une meilleure connaissance des besoins et du marché.

Concevoir

La réalisation de travaux sur la sécurité couvre des domaines très étendus, tels que :

- l'état de l'art sur des solutions existantes, des méthodes d'analyse de risques, de conception et de développement sécurisés de projets, d'évaluation de la sécurité des systèmes d'information ;
- des prises de position sur des sujets d'actualité ;
- des enquêtes, des statistiques ;
- des guides et des recommandations à caractère didactique.

Promouvoir

Il entre dans les finalités du CLUSIF de sensibiliser et d'influencer un certain nombre d'acteurs de la vie économique et politique, avec le double objectif de promouvoir la sécurité et de faire valoir les besoins et contraintes des utilisateurs auprès des instances dirigeantes. Le CLUSIF s'adresse aux décideurs, utilisateurs, parlementaires, pouvoirs publics, médias, ainsi qu'à d'autres associations.

Eduquer

Le CLUSIF s'implique activement dans le processus d'éducation et de sensibilisation, en matière de sécurité, auprès de ses membres, des professionnels de la sécurité, des enseignants et des étudiants. Il intervient dans les programmes de formation afin que la sécurité des systèmes d'information soit incorporée dans les programmes pédagogiques.

Son fonctionnement

Le fonctionnement du CLUSIF repose principalement sur les commissions et les groupes de travail.
Les commissions, à caractère pérenne, sont au cœur de l'activité.
Les groupes de travail, à vocation temporaire, sont créés pour apporter une réponse à des sujets d'actualité ou aux préoccupations d'utilisateurs et d'offreurs. La contribution peut prendre la forme d'un document, d'une recommandation ou d'une prise de position sur un thème donné.

© CLUSIF 2005

Commissions :

- Espace RSSI
- Evaluation
- Méthodes
- Réseaux et Systèmes Ouverts
- Qualité et Sécurité
- Micro-informatique
- Menaces
- Techniques de Sécurité Logique
- Techniques de Sécurité Physique

Son réseau relationnel

Régional

Le CLUSIF dispose de relais dans les régions : les Clubs de la Sécurité des Systèmes d'Information Régionaux (CLUSIR). Ces associations indépendantes sont agréées par le CLUSIF et s'engagent à respecter le règlement intérieur et le code d'éthique du CLUSIF. Il existe à ce jour six CLUSIR : Est, Languedoc–Roussillon, Midi–Pyrénées, Nord–Pas de Calais–Picardie, Provence–Alpes–Côte d'Azur, Rhône–Alpes.

International

Le CLUSIF entretient des contacts avec des organismes et des associations en Allemagne, Argentine, Belgique, Canada, Italie, Luxembourg, Maroc, Suisse, Tunisie.

Associatif

Le CLUSIF entretient des relations avec des organismes qui partagent la même sensibilité sur des thèmes de la Sécurité Informatique. Les principaux sont :
AFAI (Association Française d'Audit et du conseil en informatique)
AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise)
CIGREF (Club Informatique des Grandes Entreprises Françaises)

Institutionnel

Des liens très étroits sont développés avec les pouvoirs publics afin de promouvoir la sécurité des systèmes d'information. Le CLUSIF participe ainsi à des groupes de travail internationaux sur la cybercriminalité.

Contact

Secrétariat du CLUSIF
30 rue Pierre Sémard
75009 PARIS
Tel : 01 53 25 08 80 - Fax : 01 53 25 08 88
Courrier électronique : clusif@clusif.asso.fr
Web : http://www.clusif.asso.fr

 © CLUSIF 2005

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Robert	**BERGERON**	*CAPGEMINI*
Michel	**BERTIN**	
Stéphane	**BOUCHE**	*SECUSERVE*
Annie	**BUTEL**	*BNP PARIBAS*
Eliette	**CHAMON**	
Jean-François	**GONEL**	*AFP*
Olivier	**GUERIN**	*CLUSIF*
Pierre	**HAUTEFEUILLE**	*CAISSE CENTRALE DE REASSURANCE*
Guy	**JOVER**	*CNAMTS*
Guy	**KHOUBERMAN**	*ACOSS CNIR-SUD*
Stéphane	**MOLERE**	*AMACOM*
Laurent	**TREILLARD**	*AGERIS CONSULTING*

 © CLUSIF 2005

 © CLUSIF 2005

1 - Introduction

Aujourd'hui, en 2005, environ 70% des e-mails[1] seraient des spams et 95% des infections par virus ou vers sont véhiculés par la messagerie électronique. Cependant, le courrier électronique est le plus populaire des services d'Internet. Au niveau de l'utilisateur, il présente toutes les caractéristiques du courrier classique : envoi par dépôt à la poste, centre de tri, acheminement, distribution, boîtes aux lettres.

En entreprise, la messagerie électronique est de plus en plus utilisée et est devenue une application Internet indispensable. Parce que la messagerie est un vecteur de communication, de productivité et de production, sa sécurité et sa disponibilité sont des préoccupations légitimes des entreprises.
Toutefois, le protocole SMTP (Simple Mail Transfer Protocol), lors de sa conception, n'a pas intégré les préoccupations de sécurité actuelles. C'est ce qui explique la prolifération des menaces techniques qui pèsent aujourd'hui sur la messagerie : virus, « hoax », spam, attaque en déni de service, usurpation d'adresse, ...
De plus, parce que c'est un outil simple, rapide et expansif, des dérives comportementales et légales peuvent en résulter et doivent être contrôlées dans le monde de l'entreprise : fuite d'information, confidentialité, contenus illicites et saturation des ressources informatiques.

Dans ce document, un Directeur Informatique ou un chef d'entreprise trouvera les aspects essentiels à prendre en compte dans le cadre de la sécurisation de la messagerie électronique.
Les caractéristiques techniques et les grands principes de fonctionnement de la messagerie électronique connus à ce jour : principes de fonctionnement, structure d'un e-mail, protocoles les plus utilisés seront présentés.
Ensuite sera présenté un inventaire non exhaustif des risques et menaces qui pèsent sur la messagerie électronique d'entreprise : menaces sur les flux autorisés, menaces sur les infrastructures et risques encourus par l'entreprise.
Puis seront vues les solutions techniques et organisationnelles qui peuvent être utilisées par l'entreprise pour se prémunir des risques propres à la messagerie.
Enfin, nous tracerons le cadre légal actuel dans lequel doit s'inscrire une politique de sécurisation de la messagerie.

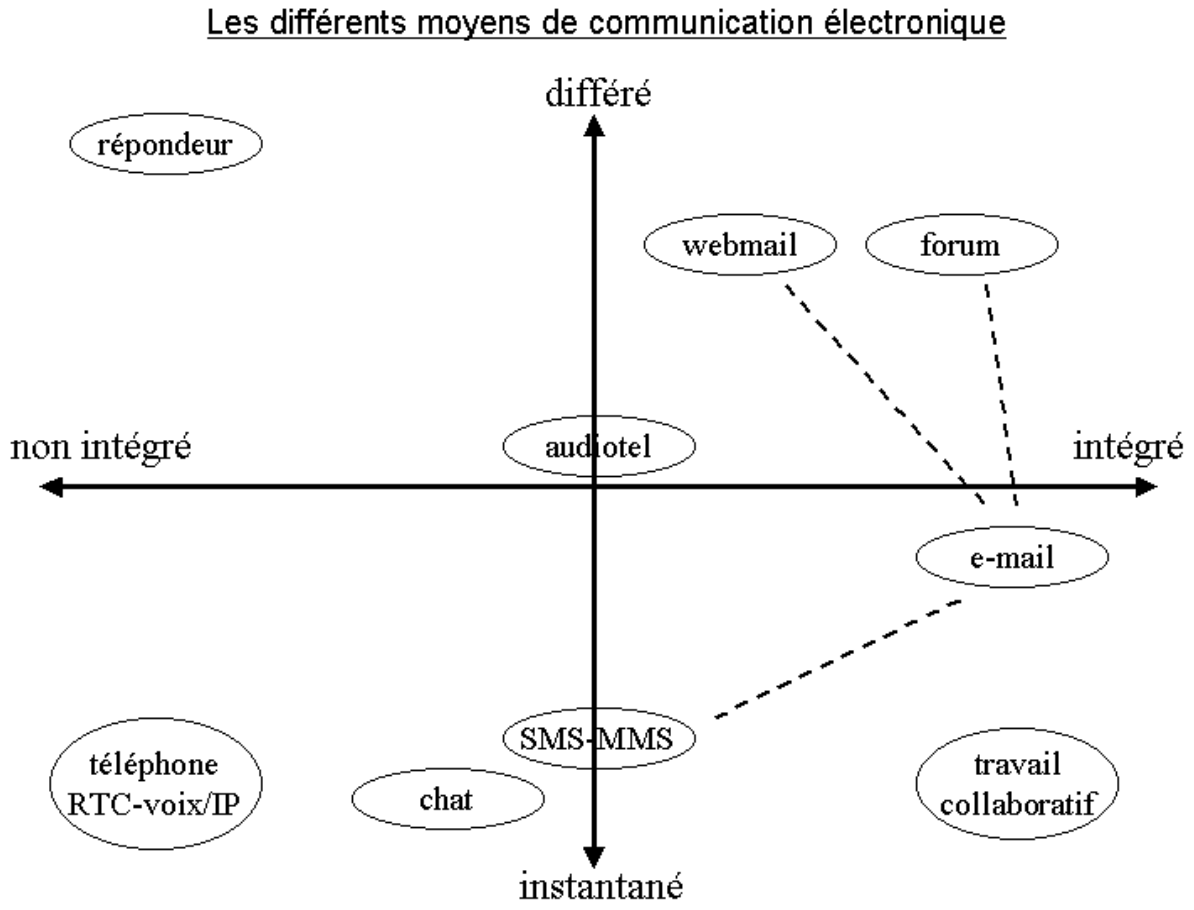
Comme nous l'avons indiqué ci-dessus, les menaces (et donc les contre-mesures) sont en perpétuelle évolution (cf. progression et évolutivité du spam et des techniques de spamming). Aussi, le présent document reflète une situation actuelle, tant sur le mode de fonctionnement de la messagerie que sur les menaces et les contre-mesures.

Enfin, si la messagerie est effectivement l'application la plus utilisée en entreprise et donc doit être au cœur des préoccupations de l'entreprise, une politique de sécurisation de la messagerie ne peut se concevoir, si elle n'est pas cohérente et intégrée dans la démarche globale de sécurisation du système d'information de l'entreprise.

[1] Le terme e-mail utilisé dans ce document est d'un usage courant, il est équivalent à courriel, mail, mèl, courrier électronique.

2 - Périmètre

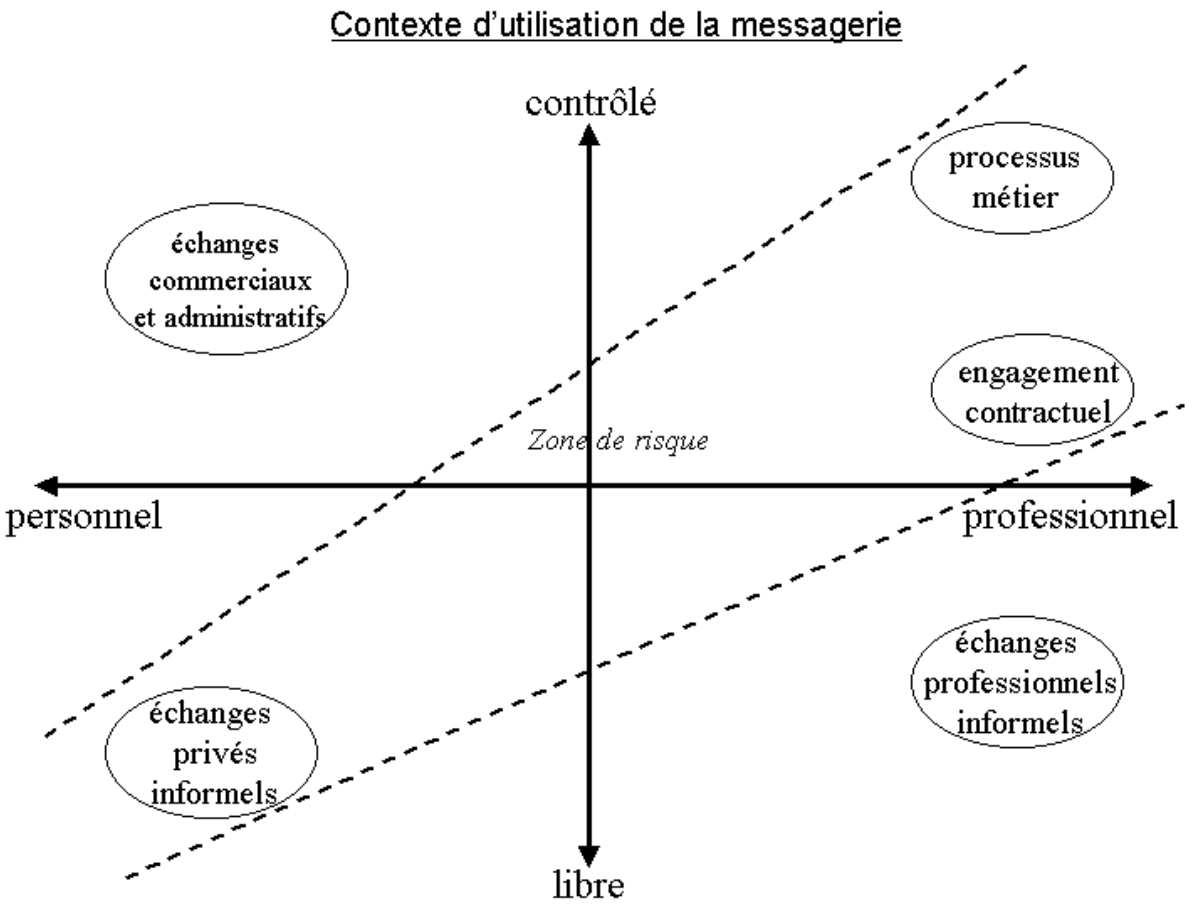
Internet permet de véhiculer des informations sous différentes formes (voix, données, images) : l'e-mail, le téléphone, le Web (World Wide Web), la vidéoconférence, le travail coopératif. Ces services sont plus ou moins intégrés au système d'information, plus ou moins instantanés. (Schéma ci-dessous)



Le document concernera essentiellement l'e-mail, constituant actuellement le moyen le plus utilisé pour échanger sur Internet.

Les risques associés à la messagerie dépendent de son contexte d'utilisation. Le schéma suivant présente les utilisations courantes de l'e-mail, personnelles ou professionnelles, libres ou répondant à des règles d'échange.
Dans une entreprise, plus les échanges sont libres, plus les risques d'attaque du système d'information sont importants.
Dans un contexte d'échanges professionnels, les risques sont ceux liés à la disponibilité, à la confidentialité, l'intégrité et la preuve du message ainsi que les risques d'engagement de responsabilité de l'entreprise et de l'émetteur.
Dans un contexte d'utilisation à titre personnel, les principaux risques sont les atteintes à la vie privée, le détournement d'informations personnelles ou l'engagement de sa responsabilité.
Nous attirons l'attention sur le fait que la distinction entre l'usage professionnel et l'utilisation personnelle des moyens de communication tend à disparaître, notamment avec la multiplication des équipements portables attribués par les entreprises à leurs salariés et par le

télétravail. Il est recommandé de préciser la frontière entre la sphère privée et la sphère professionnelle.



On peut distinguer sur ce schéma plusieurs types d'utilisation :

- La messagerie qui concerne l'échange de données interpersonnelles, à titre privé ou professionnel. Le format est libre. L'échange est direct entre des personnes qui ne sont pas disponibles au même moment.
- La messagerie qui concerne les échanges commerciaux ou administratifs et engagent la responsabilité de l'entreprise ou de l'individu. Le format est en général libre mais la traçabilité est importante.
  Ex : déclarations fiscales, commandes…
- La messagerie intégrée aux processus métiers. Ces échanges sont très formalisés et conditionnent le bon déroulement des processus. C'est par exemple l'échange de données commerciales : les commandes, les avis d'expédition, les factures entre les agents économiques. Ce sont des échanges normalisés et en principe sécurisés.

Exemples de risques d'utilisation de la messagerie

Utilisation de la messagerie	Menaces	Conséquences potentielles
Echanges commerciaux et administratifs	Menace juridique, fuite d'information	Falsification de document, atteinte à l'information de l'organisation
Echanges privés informels	Menace de détournement d'informations personnelles	Atteinte à la vie privée
Processus métier	Menace de fuite d'informations, de sabotage de données	Atteinte à l'information de l'organisation
Engagement contractuel	Menace de fuite d'informations, de sabotage de données	Atteinte à l'information de l'organisation / falsification de document
Echanges professionnels informels	Menace virale, d'intégrité	Atteinte au système d'information

Les risques liés à la messagerie sont présentés plus en détail dans le chapitre 4.

 © CLUSIF 2005

3 - Architectures / protocoles

On peut distinguer trois cas d'utilisation de la messagerie dans une entreprise :

- une utilisation purement interne, via le réseau privé de l'entreprise (Intranet),
- une utilisation étendue à des fournisseurs ou partenaires (Extranet),
- une utilisation ouverte vers l'extérieur via des réseaux publics (Internet)

Pour l'utilisateur, les mêmes outils répondent à ces trois cas d'utilisation.

3.1. Les bases du courrier électronique

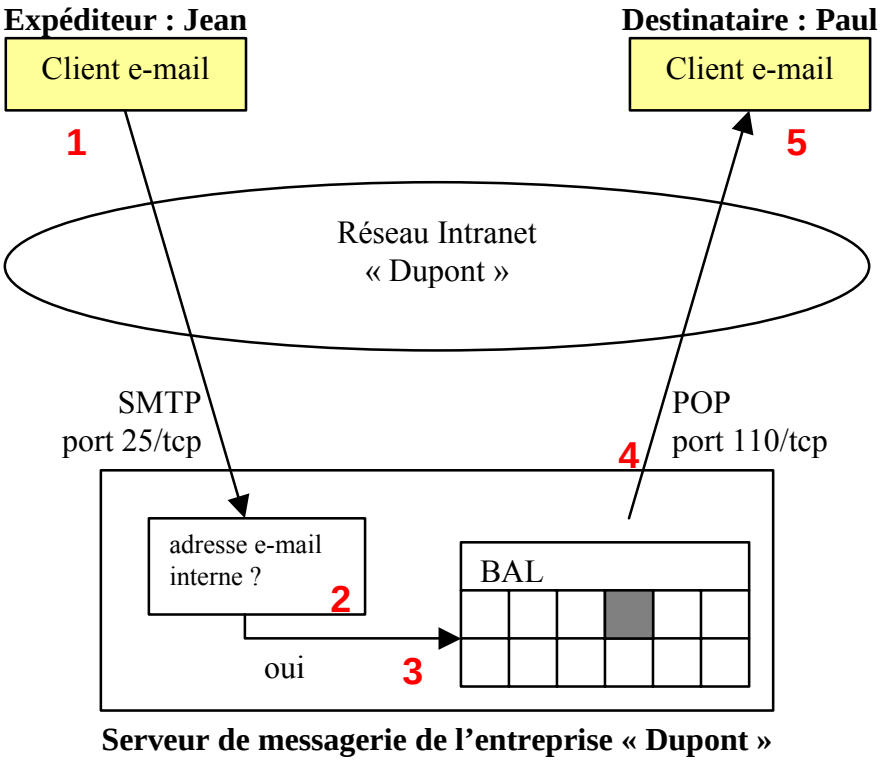
3.1.1 Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à la même entreprise (Intranet)

Exemple :

Entreprise : Dupont – 1 serveur de messagerie

Expéditeur : Jean Adresse e-mail : jean@dupont.fr

Destinataire : Paul Adresse e-mail : paul@dupont.fr



1. Jean expédie un e-mail, avec comme adresse de destination celle de Paul. Il utilise un *client de messagerie* configuré pour dialoguer avec le *serveur de messagerie* de son entreprise « Dupont ».

2. Le serveur de messagerie analyse l'adresse de destination de cet e-mail, il reconnaît que celle-ci correspond à une adresse interne à l'entreprise (xx@dupont.fr).
3. L'e-mail est donc déposé dans la *boîte aux lettres (BAL)* assignée à Paul.
4. Paul destinataire de cet e-mail, doit périodiquement interroger le serveur de messagerie (manuellement ou automatiquement), afin de savoir s'il a du courrier en attente.
5. Dans le cas positif, les e-mails en attente sur le serveur de messagerie peuvent être rapatriés sur le poste de travail du destinataire (Paul).

 © CLUSIF 2005

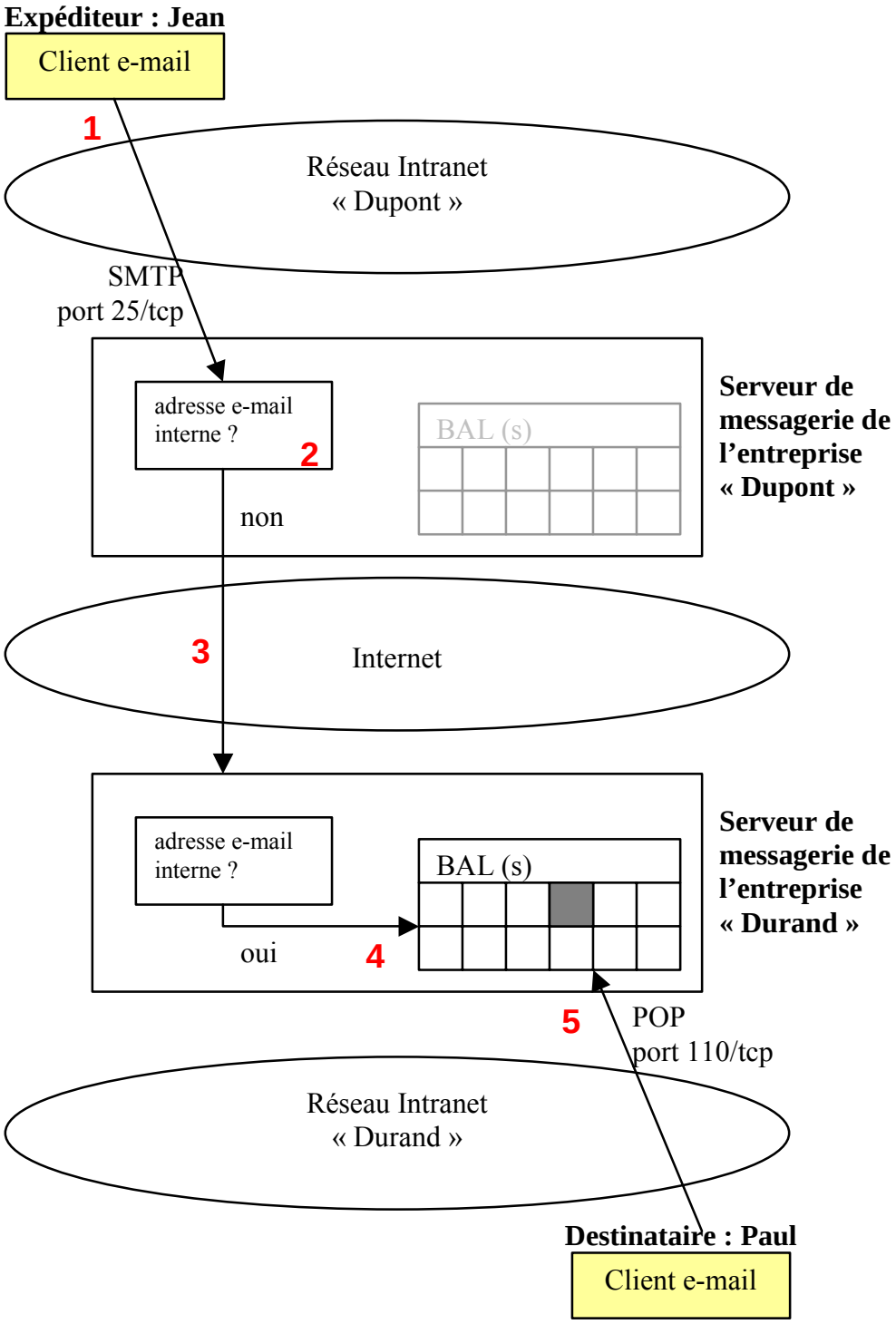
3.1.2 Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à des entreprises différentes (Internet ou extranet)

Exemple :

Entreprises : Dupont, Durand

Expéditeur : Jean Adresse e-mail : jean@dupont.fr

Destinataire : Paul Adresse e-mail : paul@durand.fr



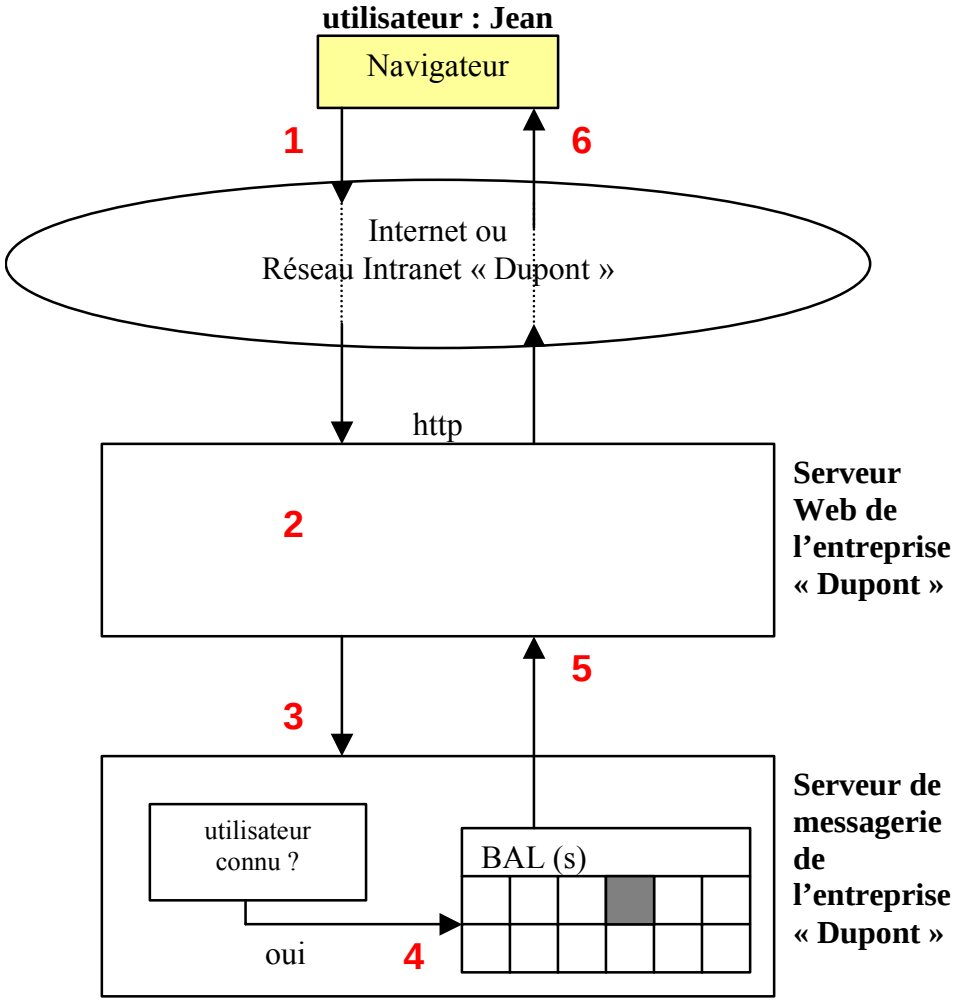
1. Jean expédie un e-mail, avec comme adresse de destination celle de Paul à l'extérieur de l'entreprise. Il utilise un *client de messagerie* configuré pour dialoguer avec le *serveur de messagerie* de son entreprise « Dupont ».
2. Le serveur de messagerie analyse l'adresse de destination.
3. Compte tenu que l'adresse de destination ne correspond pas à une adresse interne, le serveur de la messagerie « Dupont » oriente le message via Internet vers le serveur de messagerie de la société « Durand ». Une recherche de l'adresse IP du serveur de messagerie de l'entreprise destinataire est alors nécessaire, il s'agit d'une interrogation du DNS (Domain Name Server). La résolution DNS s'obtient à partir du nom de domaine situé à la droite du signe @ de l'adresse de l'expéditeur (xx@durand.fr). Eventuellement, l'e-mail peut transiter par plusieurs serveurs de messagerie intermédiaires.
4. Le serveur de messagerie de la société « Durand » analyse l'adresse de destination de l'e-mail, il constate que cette adresse correspond à une des adresses internes et référencées, il place donc l'e-mail dans la boîte aux lettres du destinataire.
5. Paul destinataire de cet e-mail, doit périodiquement interroger le serveur de messagerie (manuellement ou automatiquement), afin de savoir s'il a du courrier en attente.
6. Dans le cas positif, les e-mails en attente sur le serveur de messagerie peuvent être rapatriés sur le poste de travail du destinataire (Paul).

3.1.3 Illustration de l'accès à un serveur de messagerie à partir d'un navigateur (Webmail) pour le retrait d'un e-mail

Exemple :

Entreprise : Dupont

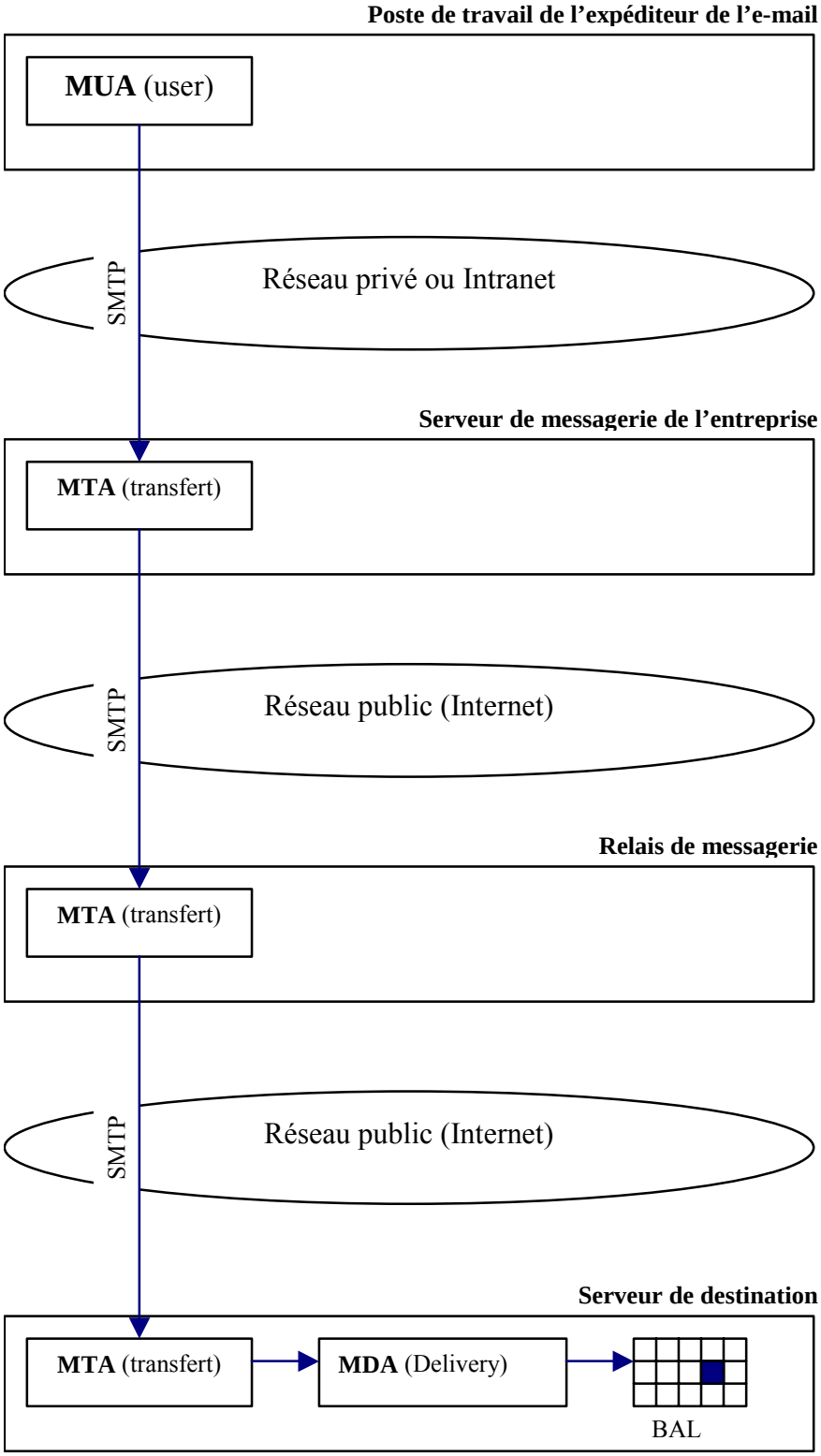
Utilisateur : Jean Adresse e-mail : jean@dupont.fr



1. L'utilisateur Jean se connecte au *serveur Web* de son entreprise à l'aide de son navigateur. Il accède à une page http permettant de solliciter le service *webmail* d'accès à sa messagerie. Un dialogue initial permet d'identifier et d'authentifier l'utilisateur.
2. Le serveur web élabore une requête destinée au serveur de messagerie.
3. La requête est transmise au serveur de messagerie de la société « Dupont »
4. Le serveur de messagerie de la société « Dupont » authentifie le propriétaire de la boîte aux lettres.
5. Tous les messages reçus sont transmis au serveur Web qui les reformate dans une page Web.
6. Le résultat est transmis en retour au navigateur de Jean qui peut alors consulter le contenu de ses e-mails.

3.1.4 Constitution de l'architecture de la messagerie

L'architecture de la Messagerie repose sur un ensemble de constituants logiciels distincts qui travaillent ensemble pour assurer le transfert d'un message d'un utilisateur vers d'autres utilisateurs. On peut distinguer trois types de constituants : le MUA, le MTA et le MDA.



MUA (Mail User Agent ou Agent Utilisateur de Message)

Ce logiciel est situé sur le poste de travail de l'utilisateur qui émet le message et sur les postes de travail des utilisateurs qui reçoivent ce message (exemples : Outlook, Eudora, Netscape, Notes, Thunderbird, ...) . Il fournit l'interface entre l'utilisateur et la messagerie. Il permet à l'utilisateur la préparation des messages et leur envoi.

MTA (Mail Transfer Agent ou Agent de Transfert de Message)

Ce logiciel est situé sur chaque serveur de messagerie. Le MUA du poste de l'utilisateur est configuré pour travailler avec un MTA bien défini. Les messages émis par un utilisateur sont envoyés via le MTA pour lequel son poste est configuré. Les messages reçus par un utilisateur sont récupérés via le MTA pour lequel son poste est configuré.

Le transfert des messages entre utilisateurs est assuré par une chaîne de MTA selon la situation des utilisateurs sur le réseau. Cette chaîne peut être constituée d'un MTA ou de plusieurs MTA. A titre d'exemple, pour une société équipée d'un seul serveur de messagerie pour des échanges de messages en interne, la chaîne est réduite à un seul MTA. Quand la chaîne comprend plusieurs MTA, les messages sont « relayés » de MTA en MTA, du MTA « d'émission » au MTA « de réception ». Le MTA est souvent appelé « relais SMTP ».

MDA (Mail Delivery Agent ou Agent de Distribution de Message)

Ce logiciel est situé sur les serveurs de messagerie. Le MTA du serveur de destination transmet au MDA les messages qui sont destinés à ses utilisateurs. Le MDA les stocke dans les Boîtes à Lettres (BAL) associées aux destinataires concernés. Ceux-ci viendront les y chercher en utilisant le MUA de leur poste de travail.

3.2. Structure et format de l'e-mail

Un e-mail a une structure similaire à celle d'un courrier classique. Il est composé d'une enveloppe (aussi appelée « en-tête »), comportant les données relatives aux adresses des émetteurs et récepteurs, ainsi que le sujet du message, la date, etc... A la suite de l'en-tête s'ajoute évidemment le contenu de l'e-mail (appelé « corps du message »), comprenant éventuellement des pièces jointes.

En-tête d'un e-mail

L'en-tête contient donc les informations suivantes :

- Une adresse e-mail d'auteur du message
- L'adresse e-mail du (ou des) destinataires
- Une adresse à utiliser en cas de réponse
- Le chemin suivi par le message
- Le type d'encodage du message
- Des informations « subsidiaires » (champs X...) comme par exemple le type de logiciel qui a généré le message.

Lors de la lecture d'un e-mail, le « MUA » indique :

- L'expéditeur
- L'objet
- Le texte (ou corps) du message

Mais cet e-mail contient toute une partie « cachée » qui permet de connaître le chemin suivi par cet e-mail avant d'arriver dans la boîte aux lettres de destination.

 © CLUSIF 2005

Détail de l'en-tête d'un e-mail

Ce message est adressé par Jean de l'entreprise Dupont à Paul de l'entreprise Durand. Il comprend 3 parties :

- le message lui-même,
- une pièce jointe le fichier « ModeEmpl.txt » au format ".txt"
- une pièce jointe le fichier « Tableau.doc » au format ".doc"

Exemple	Explication
Return-Path: <jean@dupont.fr> **Received**: from mwinf1108.durand.fr (mwinf1108.durand.fr) by mwinb0703 (SMTP Server) with LMTP; Fri, 18 Feb 2005 11:06:11 +0100 **Received**: from me-durand.net (localhost [127.0.0.1]) by mwinf1108.durand.fr (SMTP Server) with ESMTP id 563751C0009E; Fri, 18 Feb 2005 11:06:11 +0100 (CET) **Received**: from [127.0.0.1] (pc0001.dupont.fr [192.168.6.24]) by mwinf1108.dupont.fr (SMTP Server) with ESMTP id 715011C000C2; Fri, 18 Feb 2005 11:06:09 +0100 (CET) **X-Sieve:** Server Sieve 2.2 **X-ME-UUID:** 20050218100609464.715011C000C@mwinf1108.dupont.fr **Message-ID**: <4215BEC8.2090503@dupont.fr> **Date**: Fri, 18 Feb 2005 11:09:12 +0100 **From**: ="Jean"= <jean@dupont.fr> **User-Agent:** Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.7.5) Gecko/20041217 **X-Accept-Language:** en-us, en **MIME-Version**: 1.0 **To**: paul@durand.fr **Subject**: Structure des messages **Content-Type**: multipart/mixed;	**Return-Path** : Adresse qui sera utilisée : o soit pour la réponse o soit pour renvoi du message s'il ne peut arriver à son destinataire **Received** : Chaque MTA qui reçoit le message y inscrit le nom du MTA qui le lui a envoyé, ainsi que le sien. On obtient la route complète suivie par le message, de l'expéditeur jusqu'au destinataire, en utilisant les zones « Received » de bas en haut. Ces indications ont l'inconvénient de révéler une partie de l'architecture de la messagerie. **X-….** : Champs non « officiels » - Extensions spécifiques aux différents composants de la messagerie (MUA, MTA, serveur POP, ...). **Message-ID** : Identifiant unique de message. Il est attribué par le premier MTA qui reçoit le message. **Date** : Date d'émission donnée par le MUA de l'expéditeur **From** : Adresse de l'expéditeur. Cette information peut être facilement usurpée. **MIME-Version :** Version du mode de codage des données **To** : Adresse du ou des destinataire(s) **Subject** : Objet du message **Content-Type**: le message comprend plusieurs parties.

 © CLUSIF 2005

Exemple	Explication
boundary="----------080902030604050701030301" This is a multi-part message in MIME format. ----------080902030604050701030301 **Content-Type**: text/plain; **charset**=ISO-8859-1; format=flowed **Content-Transfer-Encoding**: 8bit Ce message comporte 2 pièces jointes : une au format ".txt"et une au format".doc" Cordialement, Jean ----------080902030604050701030301 **Content-Type**: text/plain; name="texte.txt" Content-Transfer-Encoding: 8bit Content-Disposition: inline; filename="ModeEmpl.txt" Mode emploi du tableau …….. …… ----------080902030604050701030301 Content-Type: application/msword; name="word.doc" Content-Transfer-Encoding: base64 Content-Disposition: inline; filename="Tableau.doc" La pièce jointe en format « .doc » est ici, mais elle n'est pas figurée, car elle est présentée dans un codage interprétable mais en pratique illisible pour nous ----------080902030604050701030301--	**boundary=** séparateurs de parties du message ce message contient plusieurs parties ------= : séparateur, partie message **Content-Type :** Type de contenu **charset:** jeu de caractères utilisé **Content-Transfer-Encoding:** Codage (ici sur 8 bits) (le texte du message) ------= : séparateur, pièce jointe format « .txt » La pièce jointe en format « .txt » lisible ------= : séparateur, pièce jointe format « .doc » La pièce jointe en format « .doc » illisible (base64) ------= : séparateur, fin du fichier message

Le format MIME (Multi-purpose Internet Mail Extensions)

A l'origine, le courrier électronique était prévu pour ne transporter que des caractères du jeu us-ascii, sans aucun accent, ni enrichissement, codés sur 7 bits.
MIME est une spécification décrivant les formats de messages sur l'Internet et permet en particulier pour la messagerie :

- L'échange de textes écrits dans des jeux de caractères étendus ou différents
- L'échange de messages multimédia comprenant par exemple des images, des sons, des séquences vidéos, des fichiers binaires et même du logiciel exécutable.

3.3. Définition des protocoles

Chaque internaute possède une « boîte aux lettres » (BAL) identifiée par une adresse électronique du type « adresse_perso@[sous_domaine].domaine ».
L'acheminement de l'e-mail se fait en plusieurs étapes. Tout d'abord, le courrier est envoyé à un serveur de mail qui va se charger de l'acheminer à bon port.
Il va donc transmettre le message au serveur destinataire qui le stocke en attendant que l'internaute destinataire le récupère à partir de sa boîte aux lettres personnelle.
Contrairement au courrier postal, l'acheminement d'un message électronique est beaucoup plus rapide, et il peut être distribué automatiquement à plusieurs destinataires à la fois.
Différents protocoles applicatifs sont utilisés au-dessus des couches réseaux et transport (TCP/IP) d'Internet (SMTP, POP, IMAP) :

- Le protocole SMTP permet de transmettre les messages envoyés par les postes clients.
- Les protocoles POP3 ou IMAP permettent de dialoguer à partir de postes clients afin d'assurer l'interrogation des boîtes aux lettres et le rapatriement des messages du serveur sur le poste de travail.

 © CLUSIF 2005

3.3.1 Le protocole SMTP (Simple Mail Transfer Protocol)

Le protocole SMTP (Simple Mail Transfer Protocol) est le protocole standard permettant de transférer le courrier soit d'un client à un serveur, soit d'un serveur à un autre en connexion point à point.
Ce protocole fonctionne en mode commuté, encapsulé dans des trames TCP/IP, grâce à des commandes textuelles (chaîne de caractères ASCII terminée par les caractères CR/LF).
Dans un dialogue, par exemple entre un client et un serveur de messagerie, chaque commande envoyée du client est suivie d'une réponse du serveur SMTP. Une réponse est composée d'un numéro et d'un message afin de signaler si la commande est prise ou non en compte par le serveur.

RECAPITULATIF DES PRINCIPALES COMMANDES SMTP

Commande		Description
HELO adresse IP	:	ou nom de domaine de l'ordinateur expéditeur
MAIL FROM	:	adresse de l'expéditeur
RCPT TO	:	adresse du destinataire
DATA	:	partie de l'en-tête et corps du mail
HELP	:	permet de récupérer la liste des commandes supportées par le serveur SMTP
EXPN	:	la fonction d'expansion renvoi les adresses de la liste de diffusion passée en paramètre.
QUIT	:	permet de quitter la connexion sur le serveur SMTP.

3.3.2 Le protocole ESMTP (Extended Simple Mail Transfer Protocol)

Ce protocole est une amélioration du protocole SMTP avec lequel il est compatible. Il permet de passer davantage de commandes.
La commande d'ouverture « HELO » est remplacée par « EHLO » (Extended HELO). Le destinataire ne répond plus seulement « OK », mais donne aussi la liste des mots-clefs qu'il est capable de traiter. Dans le cas où le destinataire ne supporte pas le protocole ESMTP, il retourne un message d'erreur et la communication continue dans un mode SMTP.

EXEMPLES DE COMMANDES ESMTP :

Commande		Description
8BITMIME	:	permet au client d'envoyer des messages comportant des caractères 8 bits.
DSN	:	Delivery Status Notification : permet d'envoyer à l'expéditeur un accusé de délivrance au destinataire.
SIZE	:	indique, avant l'envoi par le client, la taille maximale de message admissible par le serveur.

3.3.3 Le protocole POP3 (Post Office Protocol)

Ce protocole permet de récupérer son courrier sur un serveur de mail, et ne fonctionne qu'en mode connecté.
Tout comme dans le cas du protocole SMTP, le protocole POP3 fonctionne grâce à des commandes textuelles envoyées au serveur POP3. Chacune des commandes envoyées par le client est composée d'un mot-clé, éventuellement accompagné d'un ou plusieurs arguments. A chaque commande, le serveur POP3 envoie une réponse (soit +OK ou –ERR).

RECAPITULATIF DES PRINCIPALES COMMANDES POP3

Commande		Description
USER <*identifiant*>	:	Cette commande permet de s'identifier. Elle doit être suivie du nom de l'utilisateur, c'est à dire une chaîne de caractères identifiant l'utilisateur sur le serveur. La commande *USER* doit précéder la commande *PASS.*
PASS <*mot_de_passe*>	:	La commande *PASS*, permet d'indiquer le mot de passe de l'utilisateur dont le nom a été spécifié lors d'une commande *USER* préalable. Combiné à l'identifiant, il permet d'authentifier l'utilisateur.
STAT	:	Information sur les messages contenus sur le serveur
RETR <*n°msg*>	:	Numéro du message à récupérer
DELE <*n°msg*>	:	Numéro du message à supprimer
LIST *[<n°msg>]*	:	Numéro du message à afficher
NOOP	:	Permet de garder les connexions ouvertes en cas d'inactivité
TOP <*n°msg*> <*n*>	:	Commande affichant *n* lignes du message, dont le numéro est donné en argument. En cas de réponse positive du serveur, celui-ci renvoie les en-têtes du message, puis une ligne vierge et enfin les *n* lignes du message.
UIDL *[<n°msg>]*	:	Demande au serveur de renvoyer une ligne contenant des informations sur le message éventuellement donné en argument. Cette ligne contient une chaîne de caractères, appelée *listing d'identificateur unique*, permettant d'identifier de façon unique le message sur le serveur, indépendamment de la session. L'argument optionnel est un numéro correspondant à un message existant sur le serveur POP, c'est à dire un message non effacé.

QUIT	:	La commande *QUIT* demande la sortie du serveur POP3. Elle entraîne la suppression de tous les messages marqués comme effacés et renvoie l'état de cette action.

3.3.4 Le protocole IMAP (Internet Message Access Protocol)

Ce protocole présente des avantages par rapport à POP3 :

- Possibilité de stocker des messages sur le serveur de manière structurée
- Gestion de plusieurs boîtes aux lettres
- Permet l'accès direct à des parties de messages
- Supporte des accès concurrents et des boîtes aux lettres partagées
- Les utilisateurs peuvent accéder à leur courrier à partir de plusieurs machines distantes.

Un service IMAP est un système de fichiers, dont les répertoires sont des classeurs. Chaque classeur contient des messages et éventuellement d'autres classeurs.
A chaque message sont associées des informations (en plus du corps et de l'en-tête des messages) telles que :

- Un numéro unique
- Un numéro de séquence dans son classeur
- Une série de drapeaux (message lu, réponse envoyée, message à effacer, brouillon, ...)
- Une date de réception du message.

Pour les serveurs qui supportent la RFC 2086 (cf. annexe) , une ACL (Access Control List) est associée au classeur. Cette ACL permet d'attribuer des droits à un utilisateur ou à un groupe d'utilisateurs.

Quelques commandes du protocole IMAP :

Commande	Description
LOGIN	Connexion au serveur IMAP
LIST	Liste des dossiers
SELECT	Sélection d'un dossier
SEARCH	Recherche de messages dans un dossier en fonction de critères
FETCH	Récupération d'un message
STORE	Association de drapeaux à un message
LOGOUT	Déconnexion du serveur IMAP

Le protocole IMAP permet de gérer plusieurs accès simultanés. Les commandes envoyées par le client sont précédées d'un identificateur (une chaîne de caractères quelconque mais unique pour une session). Les réponses du serveur sont également précédées par l'identificateur correspondant à la commande qui les a déclenchées.

4 - Menaces et Risques

Nous avons choisi de segmenter les menaces et risques potentiels touchant au système de messagerie autour de 3 problématiques :

- La sécurisation des messages autorisés au sein de l'entreprise
- La sécurisation de l'infrastructure sur laquelle repose le système d'échange
- La définition des règles d'utilisation du système de messagerie de l'entreprise

4.1. Les atteintes aux flux identifiés par l'entreprise comme « légitimes/autorisés »

4.1.1 Perte d'un e-mail

Deux cas sont à considérer :

- la perte d'un e-mail au cours de sa transmission, par exemple suite à un problème sur un serveur de messagerie nécessitant sa restauration (les derniers messages reçus peuvent être perdus), ou par exemple supprimé à tort par un logiciel anti-spam. Le destinataire n'a, dans ce cas, jamais connaissance de ce courrier.
- La disparition d'un message reçu, voire de l'ensemble des messages reçus. Ce risque est particulièrement important lorsque l'utilisateur stocke ses e-mails sur son propre ordinateur, car dans ce cas, les sauvegardes locales ne sont pas toujours réalisées.

4.1.2 Perte de confidentialité

La messagerie représente un facteur important de perte de confidentialité dans une entreprise. Cette perte de confidentialité peut être provoquée par différents événements :

- une divulgation accidentelle : le message a été envoyé trop rapidement, avant même que l'expéditeur n'ait eu le réflexe de vérifier la liste des destinataires. Dans le cas d'utilisation de listes d'envoi, il devient difficile de vérifier que tous les membres de la liste sont bien habilités à connaître le contenu du message ;
- une divulgation par négligence ou par méconnaissance des règles : lorsqu'un tiers demande une information, on lui répond immédiatement, éventuellement avec des pièces jointes, pour lui rendre service et sans se préoccuper de la nature des informations transmises ;
- une divulgation volontaire : par exemple l'envoi d'un fichier client à un concurrent ;
- un espionnage des messages lors de la transmission sur le réseau local : à l'aide d'un logiciel spécialisé (sniffer), il est souvent aisé de se connecter à un réseau local et de recueillir les échanges de messagerie. On peut ainsi prendre connaissance sans difficulté des mots de passe de messagerie et du contenu des messages reçus ou transmis.
  L'espionnage peut également être réalisé sur un réseau public.

4.1.3 Perte d'intégrité

Un message peut être altéré, accidentellement (dysfonctionnement d'équipement, modification de format entraînant une perte d'information, etc ...) ou par malveillance pendant sa transmission ou son stockage, sur un serveur de messagerie ou sur le poste destinataire.
La perte d'intégrité peut également provenir de modifications ou ajouts volontaires effectués au niveau du serveur de messagerie.

4.1.4 Usurpation de l'identité de l'émetteur

Dans un système de messagerie, l'adresse e-mail est un élément vulnérable. L'adresse e-mail de par sa fonction est diffusée à tous les destinataires et est stockée sur des centaines voire des milliers de carnets d'adresses. Des individus ou organisations malveillants exploitent des failles de sécurité via des vers ou des virus pour récupérer des adresses e-mail en accédant aux données personnelles de l'utilisateur ou à son carnet d'adresses. Cette récupération peut-être réalisée lors de navigation sur le Web ou lors d'une réception de messages malveillants.
Lorsqu'une adresse e-mail est connue, elle peut aisément être utilisée par n'importe qui dans l'intention de nuire. Comme il n'existe pas de mécanisme d'authentification dans le protocole SMTP, on peut par exemple vous envoyer un message au nom de votre responsable hiérarchique, pour vous demander d'exécuter certaines tâches ou de transmettre des documents sensibles.

4.1.5 Répudiation

La répudiation est le risque de reniement de l'envoi ou de la réception d'un message.
En l'absence de dispositif de sécurité spécifique, il est difficile de garantir le fait qu'un message ait été émis ou reçu.

4.2. Les atteintes à l'infrastructure et au SI

4.2.1 Programmes malveillants

La messagerie permettant d'introduire des fichiers dans un ordinateur, elle constitue un vecteur important de diffusion de programmes malveillants (virus, chevaux de Troie, spywares, etc.). On peut considérer trois types d'attaques :

- l'introduction d'un virus par le biais d'une pièce jointe. De nombreux types de fichiers sont susceptibles de contenir des instructions exécutables. Il s'agit naturellement des programmes (extensions .exe, .dll, .bat, .vbs, ...), mais également de toutes sortes de fichiers de données « évolués » (extensions .doc, .xls, .pdf, .pps, ...) qui contiennent des macro-instructions exécutées à l'ouverture ou lors d'activation de certaines fonctions.
- l'introduction d'un code malicieux dans le corps même du message, lorsque celui-ci est dans un format de page web incluant des scripts. La fonction prévisualisation de certains clients de messagerie est capable de déclencher de tels scripts.
- enfin, on peut classer dans cette catégorie les faux virus (hoax), qui propagent de fausses informations ou qui font perdre beaucoup de temps de lecture aux destinataires. Ces faux virus peuvent être dangereux. Certains d'entre eux recommandent de supprimer des fichiers supposés être des virus alors qu'il s'agit de fichiers indispensables au fonctionnement du système d'exploitation.

4.2.2 Spam

Le spam est l'opération qui consiste à inonder les boîtes aux lettres de courriers indésirables et non sollicités. Ils exploitent des listes d'e-mail souvent obtenues à l'insu de leurs propriétaires. Leur but est soit la publicité pour des sites marchands plus ou moins recommandables, soit simplement de nuire aux systèmes de messagerie par saturation des réseaux et des boîtes aux lettres (« mail bombing »).
Le spam est également utilisé pour diffuser en masse de faux virus (hoax).

4.2.3 La perte de pièces justificatives

Les messages reçus/envoyés sont archivés soit sur un serveur, soit sur le poste de l'utilisateur. Dans ce dernier cas, ces messages ne sont en général pas sauvegardés. En cas de perte du disque, la perte de ces archives peut être préjudiciable (perte de trace d'un envoi ou de l'historique des échanges, perte de pièces jointes).

4.2.4 L'interruption de service

La messagerie fait de plus en plus partie intégrante de processus de l'entreprise. L'indisponibilité de la messagerie doit être prise en compte au même titre que les applications métiers, car elle peut conduire à une forte dégradation, voire à une interruption de service. L'interruption de service peut être accidentelle (panne, destruction de locaux) ou malveillante (attaques de type « déni de service » du serveur de messagerie, d'une attaque virale ou de l'envoi de spam).
L'interruption de service peut également provenir d'une inscription en « black-list », suite à des attaques opérées à partir des serveurs de l'entreprise, éventuellement en rebond ou suite à relai ouvert sur le serveur.

4.2.5 Utilisation abusive d'« open relay »

Il s'agit de l'utilisation du serveur de messagerie d'une entreprise tierce pour envoyer les messages hostiles ou des spams. Le risque pour cette entreprise est d'être inscrite en « black-list » chez les fournisseurs d'accès Internet (son adresse IP publique devient inutilisable tant que le relai reste ouvert).

4.3. Les atteintes à l'organisation

4.3.1 Les contenus illicites ou offensants

La loi interdit la diffusion de certains contenus (racistes, pédophiles, trafics divers...). Les auteurs mais également les entreprises qui offrent les services de messagerie peuvent être sévèrement condamnés.
Un autre risque de la messagerie est la diffusion de messages offensants, anonymes (utilisation d'une adresse d'émetteur factice), ou au nom d'une autre personne (cf. plus haut).

4.3.2 L'utilisation abusive

La messagerie d'entreprise est mise à disposition des employés pour les besoins du service. La jurisprudence reconnaît cependant un droit à son utilisation à des fins privées (Cf. chapitre 6). Si elle reste marginale, cette pratique est supportable par l'entreprise.

Une utilisation abusive peut cependant être la source de nuisances : encombrement des espaces disques par des fichiers volumineux (musique, vidéo), encombrement de la bande passante, sans compter la perte du temps consacré à ces activités.

4.3.3 Accomplissement d'actes frauduleux par la messagerie

Utilisation de la messagerie à des fins d'extorsion, de racket ou de chantage entraînant des préjudices pour l'entreprise (pertes financières, atteinte à l'image, divulgation d'informations confidentielles, etc.).

4.3.4 Le phishing

Le phishing a pour but le vol de mots de passe, de carte bancaire notamment. La messagerie est utilisée pour transmettre un e-mail avec par exemple le logo de la banque de la victime. Dans le message, un prétexte quelconque incite le destinataire à « cliquer » sur un lien pour se rendre sur le site de sa banque. La page web reçue est une réplique de la page d'accueil du site bancaire, sur laquelle on demande la saisie par exemple des références du compte et du mot de passe associé. En réalité, ces informations sont transmises à un site web pirate.

5 - Solutions de sécurité

Les solutions permettant de contrer les menaces présentées dans le chapitre précédent sont nombreuses, complémentaires et parfois contradictoires. Nous les présentons tout d'abord ci-dessous selon la segmentation déjà présentée :

- la sécurisation des flux légitimes
- la sécurisation de l'infrastructure et, d'une manière plus générale, du Système d'Information
- les solutions organisationnelles

La fin de ce chapitre aborde les problèmes de compatibilité de ces solutions et propose des solutions globales concernant l'architecture du système de messagerie.

5.1. Sécurisation des flux légitimes

5.1.1 Chiffrement et signature électronique des messages

La cryptologie permet d'apporter des réponses efficaces aux problématiques de sécurisation des flux légitimes. Elle permet d'assurer :

- la confidentialité des messages,
- l'authentification de l'émetteur,
- l'intégrité des messages

Elle permet également de garantir la non-répudiation des échanges.

5.1.1.1 Principes et outils de cryptologie

Les algorithmes de chiffrement peuvent être classés en deux catégories :

- Les algorithmes symétriques (AES, DES, triple DES, IDEA, …)
- Les algorithmes asymétriques (RSA, courbes elliptiques, …)

Le point commun à ces algorithmes est qu'ils utilisent un paramètre, la clé de chiffrement (ou de déchiffrement). La robustesse d'un algorithme tient à la difficulté, voire à l'impossibilité avec les moyens actuels, de retrouver la clé ayant permis de chiffrer un message.
Les algorithmes symétriques utilisent la même clé pour chiffrer puis déchiffrer un message. Cette clé doit donc être partagée par l'émetteur et le destinataire.
Les algorithmes asymétriques utilisent au contraire deux clés associées (bi-clé). Ces deux clés sont liées par des relations mathématiques complexes et sont telles que tout message chiffré à l'aide de l'une quelconque de ces deux clés ne peut être déchiffré qu'avec l'autre. La robustesse d'un algorithme asymétrique tient également à la difficulté, voire l'impossibilité avec les moyens actuels, de trouver l'une des deux clés, connaissant l'autre.

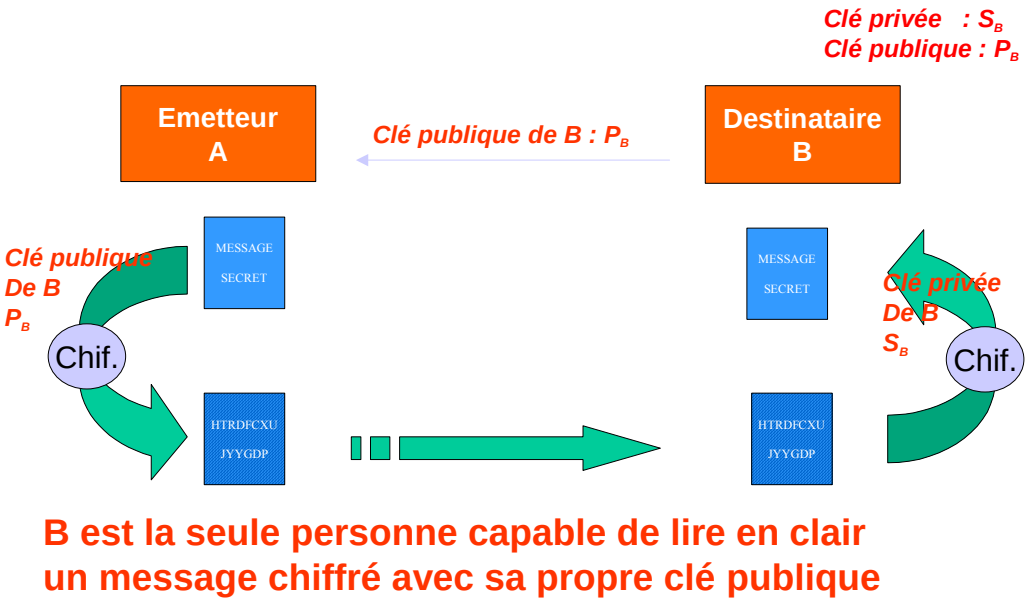
Les algorithmes asymétriques sont puissants mais plus gourmands en ressource que les algorithmes symétriques. Ils permettent d'éviter qu'un secret soit partagé par plusieurs

personnes et sont à la base des outils de chiffrement et de signature des systèmes de messagerie.

En réalité, le processus technique utilisé pour chiffrer un mail est un peu plus complexe. Les deux types de cryptographie (symétrique et asymétrique) sont mis en œuvre conjointement afin d'associer les avantages de l'un (rapidité d'exécution des algorithmes) et de l'autre (facilité de gestion des clés). Seul l'échange d'une clé de chiffrement (appelée habituellement clé de session) symétrique est réalisé en utilisant la bi-clé (clé privée et clé publique) du destinataire.

5.1.1.2 Le chiffrement des messages

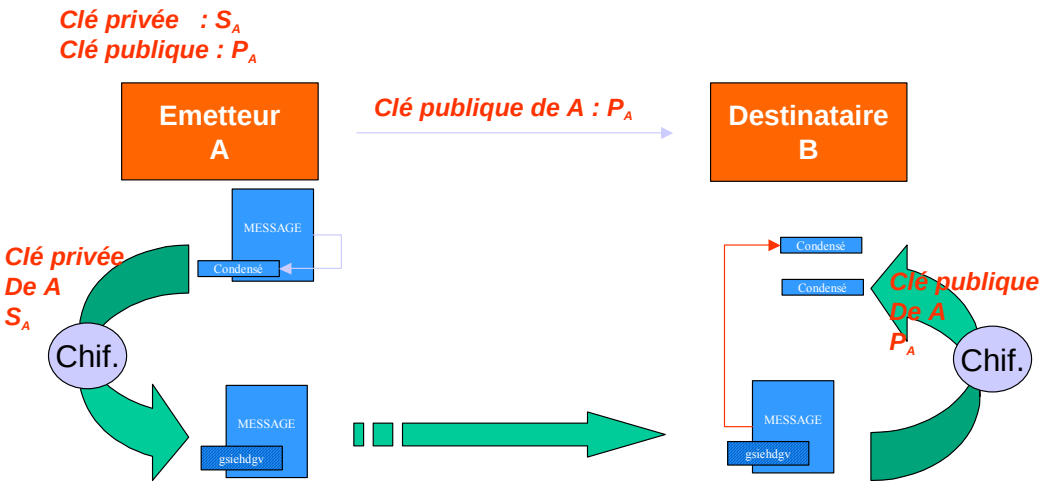
Le schéma suivant illustre le principe de chiffrement des messages s'appuyant sur des systèmes à clé publique et clé privée.



Le chiffrement est réalisé par l'émetteur en utilisant la **clé publique du destinataire**.
En réalité le chiffrement du message est réalisé par un algorithme symétrique, beaucoup plus rapide. La clé publique du destinataire est utilisée pour chiffrer la clé secrète de chiffrement du message. Dans ce cas, seul le destinataire peut récupérer la clé secrète, mais celle-ci est connue de l'émetteur du message.

5.1.1.3 La signature électronique des messages

La signature électronique est un dispositif qui permet de garantir l'authenticité de l'émetteur et l'intégrité du message. Le schéma suivant illustre les mécanismes de la signature électronique :



Le condensé n'a pu être chiffré qu'avec la clé secrète de A
=> Le message vient de A et est intègre.

Contrairement à la technique de chiffrement décrite dans le paragraphe précédent, c'est ici l'émetteur qui doit disposer d'une bi-clé (clé privée et clé publique associée)

L'émetteur calcule un « condensé » du message à transmettre. Ce « condensé », élaboré à l'aide d'un algorithme de « hachage » comme SHA-1 ou MD5, possède la propriété d'être sensible à la moindre modification du message d'origine.

Le condensé est ensuite chiffré par l'émetteur en utilisant sa propre clé privée. L'ensemble message + condensé chiffré est transmis au destinataire.

Le destinataire, dès réception du message recalcule le « condensé » par deux méthodes différentes, en utilisant le même algorithme de hachage sur le message reçu et en tentant de déchiffrer à l'aide de la clé publique de l'émetteur ce qui est supposé être le résultat chiffré du condensé calculé au départ.

L'égalité des deux résultats n'est possible que si :

- le condensé de départ a effectivement été chiffré par le bon émetteur (celui qu'il prétend être),
- le message n'a pas été modifié pendant le transfert (même condensé au départ et à l'arrivée).

5.1.1.4 Certificats et tiers de confiance

Les mécanismes de chiffrement à clé publique, nous l'avons vu, sont très séduisants car ils permettent de chiffrer des messages ou de réaliser des signatures électroniques de messages sans qu'il soit nécessaire de partager un secret entre l'émetteur et le destinataire.
Il subsiste cependant une difficulté liée à la diffusion de la clé publique. En effet, en cas de transmission d'une clé publique sur un réseau ou de récupération de cette clé publique dans un annuaire, rien ne prouve qu'il s'agit de la clé publique du bon interlocuteur.

La solution pour remédier à ce problème consiste à avoir recours à un tiers de confiance reconnu à la fois par l'émetteur et le destinataire. Le tiers de confiance vérifie l'identité du propriétaire de la clé publique (autorité d'enregistrement), puis scelle la clé publique, les informations d'identification associées ainsi que des informations de gestion liées à l'utilisation de la clé publique, à l'aide de sa clé privée (autorité de certification). Le résultat est un « certificat ». Cette organisation et les techniques associées constituent une « infrastructure de gestion de clé publique » (PKI : Public Key Infrastructure).

Toute personne faisant confiance à cet organisme tiers et s'étant procuré de manière sûre la clé publique de celui-ci peut alors vérifier l'authenticité des certificats et donc des clés publiques diffusées.

Pour être efficace, ce dispositif doit en outre permettre de vérifier, par consultation de listes de révocation, que le certificat est toujours valide.

La gestion des certificats est en général intégrée aux clients de messagerie et inclut en standard une liste d'autorités de confiance prédéfinie. On veillera à limiter cette liste aux autorités de confiance effectivement reconnues par l'entreprise.

5.1.2 La sécurisation des protocoles

La sécurisation des protocoles permet de sécuriser les communications entre les MTA et entre le serveur et le client de messagerie.

5.1.2.1 Protocole SSL/TLS

On désigne par Protocole SSL/TLS deux protocoles distincts, très proches l'un de l'autre :

- ✓ SSL (Secure Socket Layer) a été développé par Netscape. La version actuellement utilisée est la V3.
- ✓ TLS (Transport Layer Security protocol), reprise et normalisation du précédent protocole par l'IETF est décrit dans la RFC 2246. La version actuellement utilisée est la V1.

Le protocole SSL/TLS permet d'assurer l'authentification, la confidentialité et l'intégrité des données échangées.

Il s'intercale entre le protocole de transport (TCP) et les protocoles applicatifs tels que ceux utilisés dans l'application de la messagerie (SMTP, POP, IMAP, HTTP).

Il utilise un sous-protocole à négociation (on parle du « handshake » SSL) et un moyen de cryptographie reconnu : l'algorithme à clé publique RSA (du nom de ses concepteurs : Rivest – Shamir – Adleman) qui est le résultat d'opérations entre nombres premiers.

La sécurisation des connexions à l'aide du protocole SSL/TLS assure :

- La confidentialité des données transmises
- L'intégrite des données transmises
- L'authenticité des correspondants
- La fiabilité de la connexion.

Le protocole SSL/TLS est constitué des sous-protocoles suivants :

- Le sous-protocole SSL/TLShandshake
- Le sous-protocole SSL/TLSChange Cipher Spec
- Le sous-protocole SSL/TLSAlert
- Le sous-protocole SSL/TLSRecord

1. Le sous protocole SSL/TLShandshake

Ce sous-protocole permet au client et au serveur de s'authentifier mutuellement, de négocier les algorithmes de chiffrement, de négocier les algorithmes de MAC (Message Authentification Code) et enfin de négocier les clés symétriques qui vont servir au chiffrement.

2. Le sous protocole SSL/TLSChange Sipher Spec

Ce sous-protocole permet d'indiquer au sous-protocole « Record » la mise en place des algorithmes de chiffrement qui viennent d'être négociés par le sous-protocole « handshake ».

3. Le sous protocole SSL/TLSAlert

Ce sous-protocole spécifie les messages d'erreur que peuvent s'envoyer clients et serveurs. Si le niveau est « fatal », la connexion est abandonnée.

4. Le sous protocole SSL/TLSRecord

Ce sous-protocole permet de garantir :

- La confidentialité des données transmises (c'est le Handshake qui permet de négocier une clé symétrique partagée).
- L'intégrité des données transmises (c'est encore le Handshake qui négocie une clé partagée qui sert à faire des MAC sur les données).

Les algorithmes de chiffrement possibles sont :
3-DES 168 ; IDEA 128 ; RC4 128 ; Fortezza 80 ; DES 56 ; DES-40 ; RC4-40 ; RC2-40
SSL/TLS ne dépend pas des applications utilisées lors des transactions et s'applique aux protocoles HTTP, FTP, SMTP, POP, IMAP, etc…
Clients et serveurs commencent par s'authentifier mutuellement, puis négocient une clé symétrique de session qui servira à assurer la confidentialité des transactions.
L'intégrité de ces dernières est assurée par l'application de HMAC (Hashed Message Authentication Code).
Les clés asymétriques utilisées lors des transactions SSL sont encapsulées dans des certificats (X.509) générés par une autorité de certification ou par une PKI (Public Key Infrastructure) interne.

On distingue deux phases lors du déroulement du handshake SSL : authentification du serveur et authentification optionnelle du client.

1. Première phase :

Suite à la requête d'un client, le serveur envoie au client son certificat et lui liste les algorithmes qu'il souhaite utiliser. Le client vérifie la validité du certificat à l'aide de la clé publique du CA (autorité de certification) contenue dans son navigateur, des dates de validité et, éventuellement, en consultant une signature, puis, si le certificat est valide, génère une clé maître (symétrique), la chiffre à l'aide de la clé publique du serveur et la lui envoie. Les données échangées par la suite entre le client et le serveur sont chiffrées et authentifiées à l'aide de clés dérivées de la clé maître.

2. Deuxième phase, optionnelle (et souvent non utilisée) :

Le serveur envoie au client un challenge (une petite série de bits) que le client doit signer, à l'aide de sa clé privée correspondant à son certificat, puis renvoyer au serveur pour s'authentifier. Il lui envoie de même son certificat, que le serveur vérifiera avant de poursuive les transactions.

5.1.2.2 SSL – Authentification Client

Il s'agit de la deuxième phase optionnelle de la couche de négociation « handshake protocol » du protocole SSL.

1. Le serveur envoie un « challenge » , une petite série de bits.

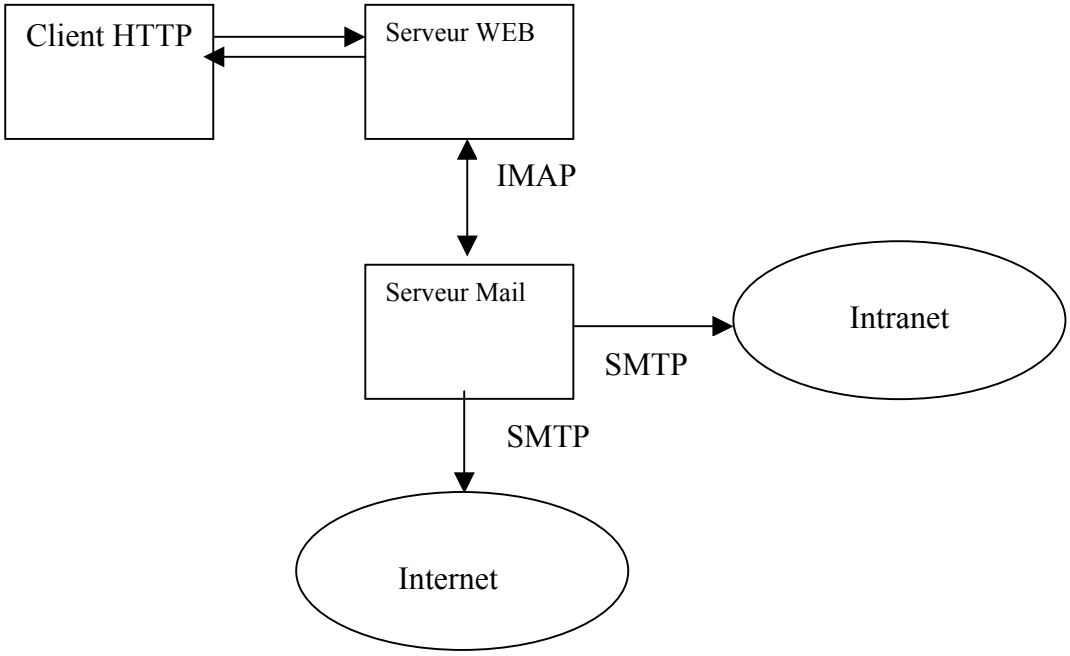
2. Le client signe à l'aide de sa clé privée ce challenge et le renvoie au serveur avec le certificat de sa clé publique

3. Le serveur déchiffre le challenge reçu du client.
4. Si challenge retourné du client = challenge initial alors l'authentification du client est positive et le serveur peut poursuivre les transactions SSL.

5.1.2.3 Solution WEBMAIL sécurisée par https

Le WebMail est un moyen d'accès à un système de messagerie basé sur une interface WEB. Il s'agit d'associer un serveur https à un serveur de messagerie, (par exemple par l'intermédiaire d'un client IMAP).

Cette architecture permet aux utilisateurs d'accéder à leur courrier à partir de n'importe quel poste client, sans nécessiter une configuration personnelle.



Le WebMail est un logiciel qui fonctionne en relation avec un serveur Web sécurisé par utilisation du protocole https, c'est à dire le traditionnel protocole http utilisant la couche de chiffrement SSL.
Cette solution évite de transmettre en clair son mot de passe d'utilisateur entre le poste client et le Webmail. Il permet en plus d'envoyer des mails et de consulter sa messagerie à partir de n'importe quel poste client relié à l'Internet.

5.1.2.4 Solution « Imaps »

Imaps est une version sécurisée du protocole Imap (Internet Message Access Protocol), elle permet l'authentification et le chiffrement via SSL.
En particulier, la transmission du mot de passe se fait au travers d'un tunnel chiffré SSL.
Cette solution nécessite l'utilisation de certificats pour assurer l'authentification du serveur, et éventuellement pour une authentification réciproque.

5.1.2.5 Intégration du protocole TLS au protocole SMTP

Le protocole TLS (Transport Layer Security) est dans ce cas complètement intégré dans SMTP grâce à une extension des commandes : STARTTLS.
Cette extension permet :

- L'authentification des serveurs SMTP,
- L'authentification du client, même dans le cas de l'utilisation d'une machine nomade,
- Le chiffrement des sessions SMTP entre serveurs et entre client et serveur.

L'authentification forte des serveurs et du client est réalisée grâce à l'utilisation de certificat X.509.
Lors de la phase de négociation de départ (EHLO), le serveur indique qu'il supporte le mode sécurisé STARTTLS, le client peut alors utiliser ce mode TLS qui permet de sécuriser l'échange des informations.

5.1.3 Traçabilité des échanges

La problématique de traçabilité a pour objectif d'établir et de conserver la preuve des échanges. Elle permet de rendre non répudiables les échanges. En matière d'e-mail, la preuve se construit principalement autour des notions d'identification et d'authentification des émetteurs et destinataires, du contrôle de l'intégrité des échanges, de confidentialité, d'horodatage, d'archivage.

Chacune des étapes de la chaîne de traçabilité est décrite plus en détail dans ce document.

La chaîne de traçabilité repose sur les principes de signature électronique qui permettent :

L'Identification et l'authentification des émetteurs :
L'e-mail et/ou sa pièce jointe sont signés ce qui permet d'attester :
- de l'identité du signataire du document émis,
- de la volonté de l'émetteur de diffuser l'information

Par ailleurs, elle fige le contenu des échanges dans le but d'en préserver l'intégrité.
Elle rend non répudiable l'envoi des documents

Le destinataire doit vérifier :
- que la signature est garantie par un certificat émis par une autorité de certification à laquelle le destinataire doit accorder sa confiance et
- que le dit certificat n'était pas révoqué au moment de la signature.

Il doit enregistrer le fait qu'il a procédé à ces vérifications.

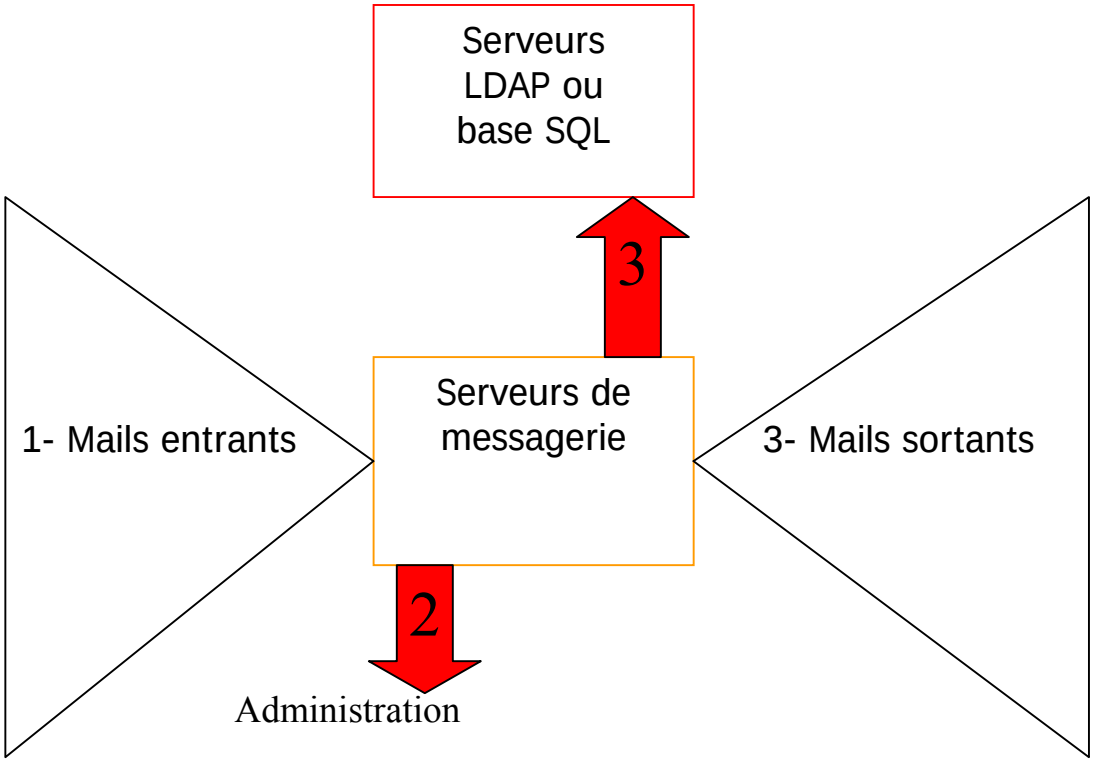
Accusé réception :
L'accusé réception doit attester de façon formelle l'ouverture d'un e-mail par son destinataire (et pas seulement de sa distribution) :
L'accusé réception d'un message chiffré permet en outre d'attester l'authenticité de son destinataire (si le message a été ouvert c'est bien que le destinataire possède la clé privée permettant de prendre connaissance du message)
La fonction d'accusé réception est en fait une fonction réciproque de la fonction d'envoi du mail :
C'est un mail de réponse qui doit être automatique émanant du poste de travail du destinataire du message et qui offre les mêmes garanties de sécurité que celles offertes par le mail qu'il a reçu.

Log et Archivage :
Lorsque les mails passent par un serveur de mail, on va enregistrer certains paramètres :
- Emetteur(s)
- Destinataire(s)
- Taille du message
- Date et heure …

Les mails dont on veut garantir la traçabilité devront aussi être archivés et indexés de sorte qu'ils puissent être retrouvés et restitués en cas de besoin.
Il convient alors de garantir l'intégrité des logs et du système d'archive, ce qui peut conduire à des difficultés en cas de chiffrement.

Horodatage :
L'horodatage consiste à attacher un temps certain à un événement (création, signature, envoi, réception…).
L'horodatage sera fourni par une autorité de confiance conjointement choisie par les émetteurs et destinataires.

N.B : Chiffrement et Archivage sont a priori deux fonctions incompatibles :
En effet, l'intérêt légal d'un archivage de mails chiffrés est très limité puisque seul le destinataire initial du mail pourra rouvrir ce mail.
Il conviendra de trouver une solution pour archiver le mail avant son chiffrement définitif.
Pour cette raison notamment, nous préconisons de confier le chiffrement des mails à un serveur et non pas au poste émetteur.



- 1- Pour éviter que les mails entrants circulent en clair, ils peuvent être chiffrés depuis le poste de l'émetteur jusqu'aux serveurs de messagerie
- 2- Les serveurs appliquent à ces mails toutes les règles de gestion définies dans la politique de sécurité (antivirus, anti spam, log, archivage…)
- 3- Les mails sortants sont chiffrés avec les clés publiques des destinataires auxquelles les serveurs de messagerie ont accès.

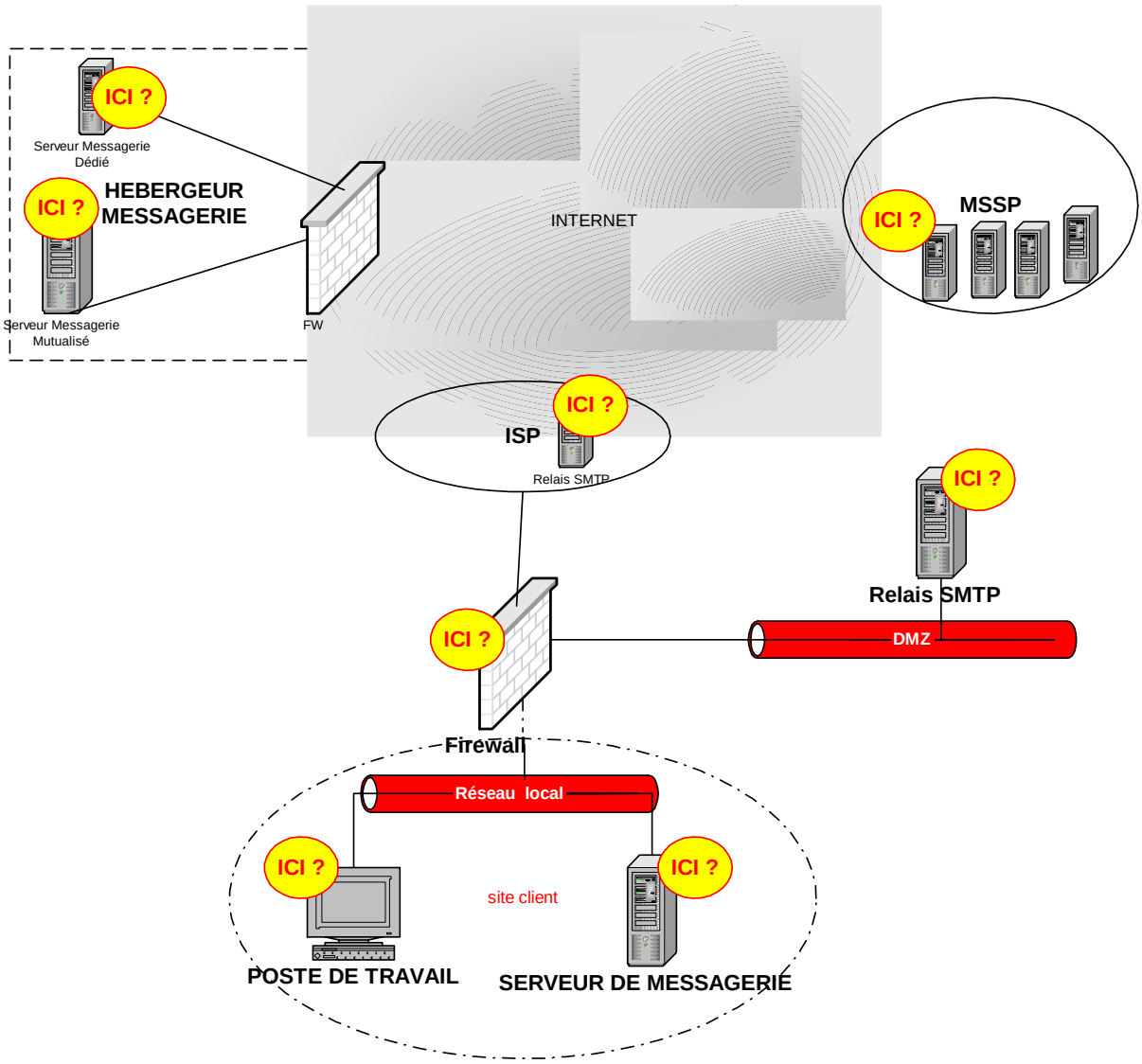
N.B : On préférera signer la pièce jointe plutôt que le mail pour les raisons suivantes :
1- Les informations importantes sont souvent véhiculées par la pièce jointe et c'est généralement elle qu'on archive

2- Si le mail est altéré pendant son transport (ajout d'un « disclaimer », marquage par un antivirus…), la signature apposée sur le mail devient invalide. Celle apposée sur la pièce jointe reste valide…

5.2. Sécurisation des Infrastructures

5.2.1 Architecture générale

Où positionner les fonctions de sécurité du contenu des emails ?



5.2.2 Filtrage et analyse de contenu

5.2.2.1 Protection contre les virus.

La majorité des virus se propagent aujourd'hui via la messagerie électronique.
(cf. document du CLUSIF « Les virus informatiques »)
Les virus sont plus en plus imbriqués dans la structure des e-mails. Par exemple, certains virus forment des e-mails non standard aux RFC SMTP. Ils sont reconnus par le client de messagerie, mais les antivirus SMTP ne peuvent pas les analyser. D'autres, se mettent dans une pièce jointe chiffrée par mot de passe et par conséquent non détectables par l'antivirus.

Un antivirus tout seul ne suffit plus. De part la diversité géographique d'apparition des virus, il est souhaitable d'utiliser plusieurs antivirus complémentaires.

Avec le mail, la problématique virale principale est la réduction de la fenêtre d'exposition aux nouveaux virus. Si par le passé, les virus de boot (sur disquette) se propageaient d'un PC à l'autre en quelques jours, avec les mails, les virus se propagent à plusieurs milliers de PCs en quelques minutes (grâce à des moteurs SMTP « embarqués » ils sont capables de se propager en utilisant l'ensemble d'un carnet d'adresses à l'insu de l'utilisateur).
La protection doit être permanente. Si les utilisateurs nomades peuvent désactiver l'antivirus lorsqu'ils sont chez eux, ils risquent d'infecter l'ensemble du réseau lors de leur première connexion le lundi matin !

Une protection efficace contre les virus doit vérifier les points suivants :

- Filtrage de l'e-mail à deux niveaux, dès leur entrée sur le réseau de l'entreprise et idéalement sur chaque poste de travail.
- Utilisation de plusieurs dispositifs antivirus complémentaires
- Maintien à jour en permanence des antivirus (automatique plusieurs fois par jour au niveau central et au moins à chaque connexion pour les postes de travail)
- Procédure d'alerte, d'inspection et de nettoyage du parc d'ordinateurs après détection d'une infection
- Procédure d'alerte paramétrable, permettant de limiter les effets collatéraux du « spamming viral » (génération d'alertes en masse)
- Maintien à niveau des outils de messagerie (application rapide des nouveaux patchs)

5.2.2.2 Protection contre les codes malicieux (macros, chevaux de troie…)

Un code malicieux peut être introduit dans une pièce jointe ou dans le corps du message.

Certains types de fichiers joints sont en effet susceptibles de contenir du code exécutable. Ils sont reconnaissables par leur extension (lorsque celle-ci n'est pas masquée) ou, pour certains d'entre eux, par leur empreinte ou « signature ».

Il faut savoir définir quel type de fichier on accepte ou pas en entrée (ou en sortie) du réseau.
L'analyse de l'extension du nom du fichier est insuffisante car elle peut être modifiée. Une analyse efficace devra identifier les types de fichiers par leurs empreintes.

Quelques exemples de structures de fichiers détectables :

Mime type	Description
application/futuresplash	Shockwave Flash Object
application/hta	HTML Application
application/mac-binhex40	Compressed file
application/ms-tnef	Outlook embedded message
application/msword	Microsoft Word Document
application/octet-stream	General binary file
application/pdf	Adobe Acrobat Document
application/pkcs10	Certificate Request
application/pkcs7-mime	PKCS #7 MIME Message
application/pkcs7-signature	PKCS #7 Signature
application/pkix-crl	Certificate Revocation List
application/streamingmedia	Standard Streaming Metafile
application/vnd.adobe.xfdf	Adobe Acrobat Forms Document
application/vnd.fdf	Adobe Acrobat Forms Document
application/vnd.ms-excel	Microsoft Excel Worksheet
application/vnd.ms-pki.certstore	Microsoft Serialized Certificate Store
application/vnd.ms-pki.seccat	Security Catalog
application/vnd.ms-pki.stl	Certificate Trust List
application/vnd.ms-powerpoint	Microsoft PowerPoint
application/vnd.rn-realmedia	RealMedia File
application/vnd.rn-realmedia-secure	Secure RealMedia File
application/vnd.rn-realplayer	RealPlayer File
application/vnd.rn-realsystem-rmx	RealSystem Secure Media Clip
application/vnd.rn-rsml	RealSystem ML File
application/x-cdf	Channel File
application/x-compress	WinZip File
application/x-compressed	Compressed file
application/x-gzip	Compressed file
application/x-internet-signup	Internet Communication Settings
application/x-iphone	Intel IPhone Compatible
application/x-ms-wmd	Windows Media Player Download Package
application/x-ms-wms	Windows Media Player Skin File
application/x-ms-wmz	Windows Media Player Skin Package
application/x-msdownload	Application Extension
application/x-pkcs12	Personal Information Exchange
application/x-pkcs7-certificates	PKCS #7 Certificates

Une première solution consiste à interdire certains de ces types de fichier, en fonction de la population concernée. Une solution plus sophistiquée consiste à identifier certains types de macros dangereuses sur le réseau (code mobile exécutable dans un document non signé par une source acceptée).

Dans le cas des codes malicieux cachés dans le corps du message (ActiveX, applets Java), il faut s'assurer qu'une détection a été mise en place à la réception du message ou sur le relais SMTP.

5.2.2.3 Protection contre le spam.

Si les USA ont des taux de spam avoisinant les 80% (10 mails sur 12), nous constatons à ce jour en France des taux voisins de ou supérieurs à 50%.
Le spam soulève différents problèmes :

- Saturation des ressources informatiques et réseau de l'entreprise ;
- Perte de productivité ;
- Confort des utilisateurs.

Il n'y a pas de solution miracle et garantie. Nous constatons une lutte permanente entre les éditeurs d'antispam et les spammeurs (qui font évoluer leurs méthodes en fonction des techniques de détection). Une technique antispam perd au moins 50% de son efficacité tous les ans !

En terme de protection, les techniques actuelles principales sont :

- l'analyse lexicale : recherche de mots clés associée à un système de pondérations (bayesien) ;
- la mise en place de listes noires (Black Lists) et listes blanches (White Lists) : listes d'adresses ou de domaines interdits ou autorisés ;
- la technique de la liste grise (greylisting) qui consiste à refuser un triplet composé de l'adresse IP du serveur d'origine du message et des adresses de l'émetteur et du

destinataire lors de sa première réception. Cette technique est très efficace car en général les spammeurs ne renvoient pas les messages en erreur ;
- l'utilisation de RBLs (Realtime Blackhole List) : listes d'adresses ou de relais SMTP identifiés comme spammeurs ou relais ouverts ;
- l'analyse de signatures : consiste à comparer l'empreinte du message à des empreintes de messages de spam connus.

Le choix d'une solution antispam s'efforcera de s'appuyer sur la technicité de la solution mais également sur son administrabilité.
En effet, une politique globale pour l'entreprise n'est pas satisfaisante : la perception du spam est différente entre les individus, les services et les sociétés. Faut-il bloquer les mails contenant le mot VIAGRA pour un laboratoire pharmaceutique ? Faut-il bloquer les newsletters pour le service Presse & Communication ?

Actions à entreprendre en présence d'un spam :
- Mettre en quarantaine. Il faut ensuite informer l'administrateur ET/OU l'utilisateur du contenu de la quarantaine afin de lui permettre de la gérer. Plusieurs aspects sont à considérer : taille et durée de vie de la quarantaine, notamment en période de congés, rapports de quarantaine pré qualifiés, ...
- Détruire. Attention aux pertes de messages dans le cadre des faux-positifs.
- Marquer ou « Tagguer » (au niveau de l'objet ou de l'en-tête). Le fait de « tagguer » les mails permet de s'affranchir du problème de pertes de messages. Ces derniers parviennent dans la BAL utilisateur quoi qu'il arrive. Il est possible avec les derniers clients de messagerie de créer des règles qui classeront automatiquement. Cette solution ne répond pas au confort des utilisateurs et à la saturation des ressources informatiques.

Une bonne solution antispam doit allier :
- des techniques de détection mises à jour et évolutives ;
- une administration à la fois centralisée et individualisable (gestion des quarantaines de spam).
- Une réduction des « faux positifs » pouvant entraîner des pertes d'information.

Parallèlement au spam (envoi massif de mails non-sollicités), il sera intéressant de prévoir des parades contre le « spamming viral » : message d'erreur ou d'information virale, en provenance de serveur antivirus qui reçoivent des messages dont le nom de l'expéditeur a été usurpé. Le « spamming viral » représente 15% des flux mails à l'heure où nous écrivons ces lignes.

5.2.2.4 Définition des règles de communication

Est-il normal que les commerciaux d'une entreprise envoient des e-mails vers nos concurrents ?
Quels sont les domaines amis (clients, fournisseurs, prospects, partenaires) et non souhaités (spammeurs, concurrents, …) ?
Une solution de sécurisation des e-mails peut permettre de définir ces règles de communication.

5.2.2.5 Contrôle du contenu des messages – Analyse Lexicale

Est-il admissible que des contenus non professionnels, voire délictuels (termes offensants pornographiques, sexistes, racistes) circulent dans les messages entrants (protection des employés) ou sortants (préservation de l'image de marque de l'entreprise) ?
L'analyse lexicale permettra également de répondre au « spamming viral » par l'utilisation de listes de mots clés (« delivery failure », « alerte virus », …).

5.2.2.6 Contrôle des attachements dans les messages

Est-il souhaitable pour l'entreprise que le CV du Directeur Technique ou que le fichier client soit envoyé vers un concurrent ?
Est-il admissible de saturer les ressources informatiques avec des programmes exécutables, des jeux ou animation « folklorique » d'une taille trop importante ?
L'analyse des pièces attachées en fonction de leur émetteur, destinataires, taille et type, doit permettre de résoudre ces problématiques et d'accroître la sécurité du SI ainsi que la disponibilité des ressources informatiques.

5.2.2.7 Contrôle des mails chiffrés

Nous l'avons précédemment souligné, le chiffrement des mails ou des attachements limite les capacités de protection contre les virus.
Cependant, il sera souhaitable de limiter ces règles et ces contrôles en fonction des utilisateurs. Ainsi, ce n'est pas remettre en cause la sécurité que de laisser la DG de l'entreprise envoyer des mails chiffrés à destination de ses actionnaires.

5.2.2.8 Contrôle de la conformité au protocole SMTP

La non conformité au protocole SMTP peut parfois être utilisée pour contourner des protections mises en place. Ce type de message doit est filtré car il resterait activable par le client de messagerie.

5.2.2.9 Gestion et ajout des mentions légales

L'utilisation du mail et la sécurisation de la messagerie doit être en adéquation avec la charte d'utilisation de la messagerie et les spécificités légales du pays d'émission ou de destination. A cet effet, l'ajout automatique ou conditionnel (pas d'ajout si sujet = « personnel ») de mention légale (Legal Disclaimer) en haut ou bas de mail, permettra à l'entreprise de se décharger de sa responsabilité juridique.

5.2.3 Tableau d'analyse des options d'implémentation

Le tableau ci-dessous propose des solutions d'implémentation pour différentes fonctions de sécurité de la messagerie en déclinant les avantages et inconvénients de chacune.

	Solutions	**Installée en Interne**			
Fonctions		**Poste de travail**	**Serveur Mess. Int.**	**Relais SMTP DMZ**	**Firewall**
Antivirus (AV)	Avantages	• Protection des flux mail et autres (http, CDROM, flux réseau) • Blocage des virus inter-poste.	• Gestion centralisée des mises à jour • Blocage des virus inter-BALs • Blocage des virus à l'entrée et à la sortie	• Gestion centralisée des mises à jour • Blocage de virus à l'entrée et à la sortie	• Tout en un • Simple • Blocage de virus à l'entrée et à la sortie • Traite flux SMTP, http, FTP
	Inconvénients	• Mise à jour desactivable • Pas de contrôle centralisé • Occupation CPU et disque • La menace atteint le poste avant d'être bloquée • Ne supporte pas plusieurs AV	• La menace atteint le serveur avant d'être bloquée • Occupation CPU et disque • Attaque en déni de service / Indisponibilité • Supporte difficilement plusieurs AV.	• La menace atteint le réseau avant d'être bloquée ; • Occupation CPU et disque • Attaque en déni de service / Indisponibilité	• Tout en un et sécurité ne font pas bon ménage • Vérifier fréquence et modalités de mise à jour • Occupation CPU et disque (s'il existe) • Attaque en déni de service / Indisponibilité • Supporte difficilement plusieurs AV.
Anti-spam	Avantages	• Gestion personnalisée du filtre et des listes	• Gestion centralisée de la politique de spam	• Gestion Centralisée • Blocage du spam avant entrée sur réseau.	• Tout en un • Simple • Blocage des spam à l'entrée et à la sortie
	Inconvénients	• La menace atteint le poste avant d'être bloquée • Occupation disque et bande passante • Temps de gestion et MAJ important par user.	• La menace atteint le serveur avant d'être bloquée • Occupation disque et bande passante • Attaque en déni de service / Indisponibilité • Vérifier la gestion personnalisée des règles de spam	• La menace atteint le réseau avant d'être bloquée • Occupation CPU, disque et bande passante • Attaque en déni de service / Indisponibilité	• Tout en un et sécurité ne font pas bon ménage • Vérifier la pertinence des technologies embarquées • Occupation CPU et disque (s'il existe) • Attaque en déni de service / Indisponibilité • Vérifier la gestion personnalisée des règles de spam
Analyse lexicale	Avantages	Idem Anti-spam	• Gestion centralisée des règles d'analyse	• Gestion Centralisée	• Tout en un • Simple
	Inconvénients	Idem Anti-spam	• Vérifier la capacité réelle de la solution à remplir cette tâche • Attaque en déni de service / Indisponibilité	• La menace atteint le réseau avant d'être bloquée ; • Occupation CPU, disque et bande passante • Attaque en déni de Service / Indisponibilité	• Vérifier la capacité de la solution à remplir cette tâche • Vérifier la pertinence des technologies embarquées • Occupation CPU et disque (s'il existe)
Conformité aux RFC SMTP	Avantages	N/A	N/A	• Blocage des Indéterminés avant entrée sur réseau.	N/A

	Solutions	**Installée en Interne**			
Fonctions		**Poste de travail**	**Serveur Mess. Int.**	**Relais SMTP DMZ**	**Firewall**
	Inconvénients	N/A	N/A	• Vérifier la capacité réelle de la solution à remplir cette tâche	N/A
Ajout mentions légales	Avantages	N/A	• Gestion centralisée	• Gestion Centralisée	N/A
	Inconvénients	N/A	• Vérifier la capacité réelle de la solution à remplir cette tâche	• Vérifier la capacité réelle de la solution à remplir cette tâche	N/A
Règles de communication	Avantages	N/A	• Gestion centralisée	• Gestion centralisée	• Tout en un • Simple
	Inconvénients	N/A	• Vérifier la capacité réelle de la solution à remplir cette tâche • La menace atteint le serveur avant d'être bloquée • Occupation disque et bande passante	• Vérifier la capacité réelle de la solution à remplir cette tâche • La menace atteint le réseau avant d'être bloquée • Occupation CPU, disque et bande passante	• Vérifier la capacité de la solution à remplir cette tâche • Vérifier la pertinence des technologies embarquées • Occupation CPU et disque (s'il existe)
Contrôle attachements	Avantages	N/A	• Gestion centralisée	• Gestion centralisée	• Tout en un • Simple
	Inconvénients	N/A	• Vérifier la capacité réelle de la solution à remplir cette tâche (finesse des règles) • La menace atteint le serveur avant d'être bloquée • Occupation disque et bande passante • Attaque en déni de service	• Vérifier la capacité réelle de la solution à remplir cette tâche (finesse des règles) • La menace atteint le réseau avant d'être bloquée • Occupation CPU, disque et bande passante	• Vérifier la capacité de la solution à remplir cette tâche • Vérifier la pertinence des technologies embarquées • Occupation CPU et disque (s'il existe)
Mails chiffrés	Avantages	N/A	N/A	• Gestion centralisée	N/A
	Inconvénients	N/A	N/A	• Vérifier la capacité réelle de la solution à remplir cette tâche (finesse des règles) • Occupation CPU, disque et bande passante	N/A
Détection de codes malicieux	Avantages	• Protection des flux mail et autres (http, CDROM, flux réseau) • Blocage des codes inter-poste.	• Gestion centralisée	• Gestion centralisée	N/A
	Inconvénients	• Mise à jour desactivable • Pas de contrôle centralisé • Occupation CPU et disque • La menace atteint le poste avant d'être bloquée	• Vérifier la capacité réelle de la solution à remplir cette tâche (finesse des règles) • La menace atteint le serveur avant d'être bloquée • Occupation disque et bande passante • Attaque en déni de service	• Vérifier la capacité réelle de la solution à remplir cette tâche (finesse des règles) • Occupation CPU, disque et bande passante	N/A

	Solutions	Externes / Externalisée		
Fonctions		**ISP/Fournisseur d'Accès Internet**	**MSSP (Fournisseur de Service de Sécurité Gérée)**	**Hosting Ext. (Hébergeur de Messagerie)**
Antivirus	Avantages	• Virus bloqué ou détruit avant d'atteindre le réseau	• Virus bloqué ou détruit avant d'atteindre le réseau • Généralement Garanties de résultats	
	Inconvénients	• Vérifier administrabilité par client / domaine • Combien d'AV sont utilisés • Vérifier l'engagement de résultat et indemnités contractuelles	• Combien d'AV sont utilisés • Vérifier l'engagement de résultat et indemnités contractuelles	• Vérifier administrabilité par client / domaine • Combien d'AV sont utilisés • Vérifier l'engagement de résultat et indemnités contractuelles
Anti-spam	Avantages	• Economie de bande passante – Le spam est bloqué avant qu'il n'atteigne le réseau	• Economie de bande passante et ressources réseau • Le spam est bloqué avant qu'il n'atteigne le réseau • Administration possible par client / domaine / utilisateur • Définition de Liste Blanche / Noire par client et/ou domaine	• Administration possible par client / domaine / utilisateur
	Inconvénients	• Vérifier Administrabilité par client / domaine / utilisateur • Attention à la destruction des spams (Traçabilité ?) • Combien de technologies anti-spam sont utilisées • Si marquage des spams, intérêt faible	• Combien de technologies anti-spam sont utilisées • Si « marquage » des spams, intérêt faible • Risques d'atteinte à la confidentialité et l'intégrité des messages	• Attention à la disponibilité de Service en cas de saturation de BAL ou attaque en déni de service • Combien de technologies anti-spam sont utilisées • Si « marquage » des spams, intérêt faible
Analyse Lexicale	Avantages	N/A	• Bloquer les e-mails douteux ou illicites avant qu'ils n'entrent dans l'entreprise	N/A
	Inconvénients	N/A	• Vérifier administrabilité par client / domaine / utilisateur	N/A
Conformité aux RFC SMTP	Avantages	N/A	• Bloquer les sources potentielles de menaces sans AV	N/A
	Inconvénients	N/A	• Vérifier la disponibilité de cette fonction	N/A
Ajout mentions légales	Avantages	N/A	• Ajout automatique sans interférence avec des personnels internes	N/A
	Inconvénients	N/A	• Vérifier la possibilité de paramétrage de cette fonction (en entrée, en sortie).	N/A
Règles de communication	Avantages	N/A	• Economie de bande passante	N/A
	Inconvénients	N/A	• Vérifier la possibilité de paramétrage de cette fonction (en entrée, en sortie), par domaine, par groupe d'utilisateurs	N/A
Contrôle attachements	Avantages	N/A	• Economie de bande passante et protection légale	N/A
	Inconvénients	N/A	• Vérifier la possibilité de paramétrage de cette fonction (en entrée, en sortie), par domaine, par groupe d'utilisateurs	N/A
Mails chiffrés	Avantages	N/A	• Economie de bande passante et confidentialité	N/A
	Inconvénients	N/A	• Vérifier la possibilité de paramétrage de cette fonction (en entrée, en sortie), par domaine, par groupe d'utilisateurs	N/A
Détection de codes	Avantages	N/A	• Economie de bande passante et sécurité	N/A

	Solutions	Externes / Externalisée		
Fonctions		**ISP/Fournisseur d'Accès Internet**	**MSSP (Fournisseur de Service de Sécurité Gérée)**	**Hosting Ext. (Hébergeur de Messagerie)**
malicieux	Inconvénients	N/A	• Vérifier la possibilité de paramétrage de cette fonction (en entrée, en sortie), par domaine, par groupe d'utilisateurs	N/A

 © CLUSIF 2005

5.3. Solutions Organisationnelles

5.3.1 Politique de sécurité et charte d'utilisation

Comme dans tout autre domaine de la sécurité, les mesures retenues pour la messagerie électronique doivent, pour être efficaces, s'inscrire dans un cadre global cohérent – la politique de sécurité. L'efficacité des dispositifs techniques de sécurité dépend également en grande partie du comportement des utilisateurs. Celui-ci devra être encadré dans une charte d'utilisation.

La messagerie et la politique de sécurité.
La politique de sécurité de l'entreprise énonce des principes et des règles dont certains sont directement applicables à la messagerie électronique :

- les principes de classification des informations et les règles de conservation, de transmission et de destruction de ces informations selon leur nature (utilisation de moyens de chiffrement, règles d'archivage, ...).
- Les règles de protection antivirale (interdiction de certaines pièces jointes, formats de message admis, ...)
- Les règles visant l'efficacité du système (taille des fichiers transmis, utilisation des listes de diffusion, ...)
- Les principes de filtrage et de contrôle d'utilisation de la messagerie (filtres antispamming, quarantaine, ...)
- ...

La charte d'utilisation
Les règles d'utilisation de la messagerie seront consignées dans une charte d'utilisation de la messagerie, ou incluses dans une charte plus globale d'utilisation des moyens informatiques. Ce document, signé par chaque utilisateur, informe également le destinataire des différents types de contrôle susceptibles d'être effectués, dans les limites fixées par la réglementation.
La charte d'utilisation est un document qui doit être présenté aux instances représentatives du personnel avant diffusion.

La diffusion de ces documents pourra s'intégrer dans un plan de sensibilisation des utilisateurs (réunions, quiz, booklet, vidéo, ou tout autre support).

5.3.2 Les bonnes pratiques de l'utilisateur

Ce paragraphe ne reprend pas les obligations de l'utilisateur consignées dans une charte de bonne utilisation, mais propose quelques conseils pour une bonne utilisation de sa messagerie.

Dans la protection de son matériel, en absence d'une fonction d'administrateur :

- S'assurer que son « antivirus » est bien à jour.
- Utiliser les fonctionnalités de « pare-feu » et d'« anti-spam » lorsqu'elles sont disponibles.

Dans l'utilisation générale de la messagerie :

- Eviter de déléguer l'utilisation de sa messagerie.
- Protéger sa boîte aux lettres par un mot de passe.

- Limiter l'utilisation privée de son adresse professionnelle.
- Ne pas laisser son adresse e-mail professionnelle sur n'importe quel site Web, sur des forum, à des inconnus, ….
- Ne pas répondre au SPAM
- Désactiver les options d'envoi systématique d'information sur les sites Web.

Dans la gestion de sa messagerie :

- Eviter l'envoi de messages de taille importante ou préférer le mode différé (Priorité basse)
- Classer à l'arrivée ses messages dans des dossiers prédéfinis.
- Veiller à ce que les messages importants soient régulièrement sauvegardés.
- Faire un archivage périodique de ses messages.
- Supprimer les messages inutiles ou obsolètes.
- Activer les fonctionnalités de sécurité offertes par le client de messagerie (exemples : Chiffrement des données locales et de la liaison avec le serveur)

Dans la réception des messages :

- Ne pas ouvrir de messages ou de pièces attachées venant de personnes ou de sociétés non identifiées.
- Se méfier de messages dont l'objet est en langue étrangère.
- Ne pas porter crédit à des messages de type « Hoax ».

Dans l'envoi des messages :

- Ne pas renvoyer de messages qui demandent de relayer un message vers un grand nombre de personnes. (Comme ceux de chaînes en tous genres)
- Pour l'envoi des messages à plusieurs personnes et pour éviter la divulgation des adresses, utiliser la facilité « copie cachée ».
- Lors d'une réponse avec historique, ne pas retransmettre les pièces jointes inutiles.

Dans la gestion de son carnet d'adresse :

- Crypter son carnet d'adresse si le client de messagerie le permet.
- Rajouter une fausse adresse en tête de son carnet d'adresse pour être averti en cas d'envoi en masse à partir de son carnet d'adresse .

5.3.3 Les bonnes pratiques de l'administrateur

Le système de messagerie de l'entreprise doit être placé sous la responsabilité d'un « propriétaire » qui en validera les règles d'utilisation. L'administrateur a en charge le maintien opérationnel de la messagerie conformément aux règles d'utilisation décidées.

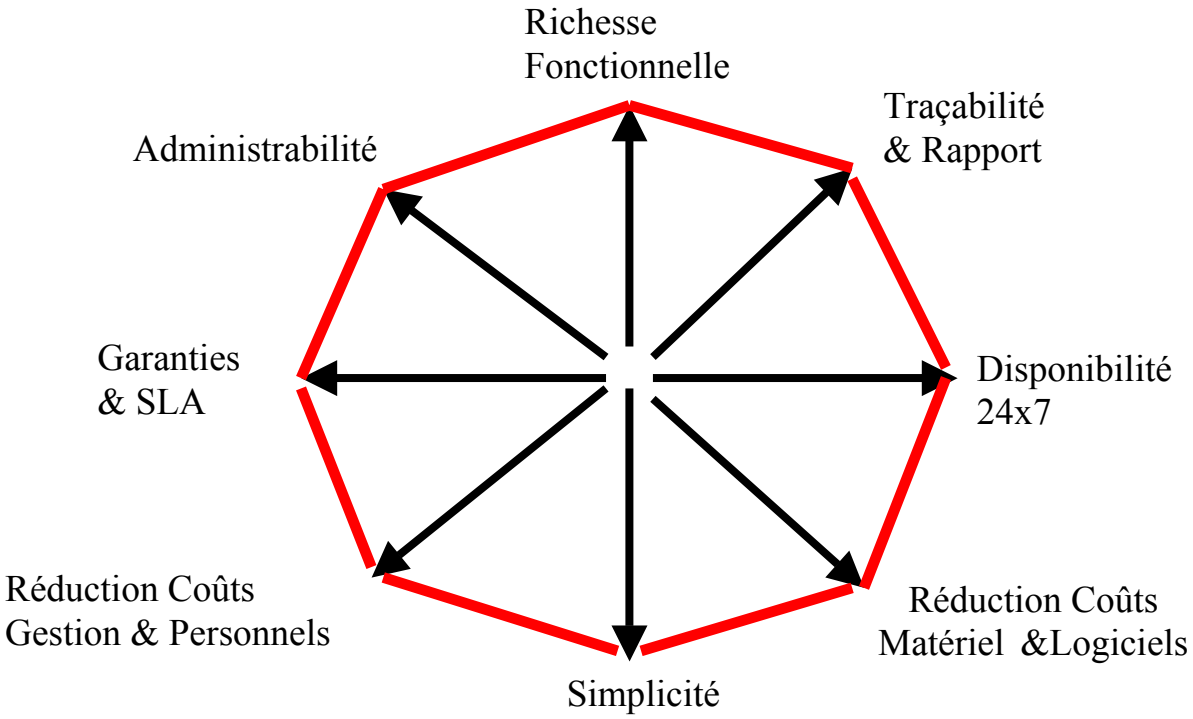
L'administrateur est un acteur clé de la sécurité de la messagerie. Parmi les bonnes pratiques à appliquer, l'administrateur veillera particulièrement à :

- Limiter l'usage des listes de diffusion. L'abus des listes de diffusion génère un encombrement des boîtes aux lettres avec des messages mal ciblés. Un autre danger est l'envoi d'informations sensibles à des destinataires non désirés car la liste des membres d'une liste de diffusion n'est pas toujours maîtrisée par l'utilisateur.

- Bloquer le « reply to all ». Le « reply to all » (réponse à l'émetteur du message et à l'ensemble des destinataires) est également une cause d'encombrement des boîtes aux lettres, particulièrement lorsque l'échange de messages correspond à une série d'échanges stériles entre quelques destinataires du message initial.
- Supprimer les certificats d'autorités non utilisées. Les clients de messagerie intègrent automatiquement lors de leur installation des certificats d'autorités de certification ayant une certaine notoriété au niveau mondial. Il est souhaitable de ne conserver que les certificats d'autorités qui ont été retenus dans la politique de sécurité de l'entreprise.
- Réaliser une veille technologique afin de mettre en place rapidement les correctifs d'anomalies susceptibles de constituer des trous de sécurité ou constituant déjà des trous de sécurité exploités.
- Mettre en place un système de trace et de surveillance en conformité avec les exigences légales en termes de protection des données à caractère personnel. Les logs doivent être régulièrement exploités, permettre l'identification de comportements anormaux et répondre aux besoins d'archivage légal.
- Mettre en place des points de contrôle continu de l'efficacité des dispositifs techniques mis en œuvre.

5.4. Critères de choix d'une solution

Pour chaque solution envisagée, il appartiendra de contrôler les éléments ci-après qui permettront d'apprécier l'adéquation de la solution avec les besoins et l'organisation de l'entreprise.



Traçabilité et Reporting :
La richesse des rapports permettra à l'administrateur d'évaluer le niveau de sécurité actuel et d'envisager des mises à jour et renforcement de la politique de sécurité. La traçabilité doit permettre de retrouver le cheminement d'un e-mail et de s'assurer de sa bonne livraison.

Richesse fonctionnelle :
Elle s'apprécie en fonction de la solution souhaitée au moment de la mise en œuvre et à sa capacité d'évolution dans le temps. Nous listerons plus bas les fonctions de sécurité du contenu possibles et leur intérêt.

Administrabilité :
La sécurité est une fonction vivante, et la solution de sécurité doit pouvoir évoluer avec les menaces. De plus, dans le cadre d'organisations importantes, il sera souhaitable de déléguer et de répartir tout ou partie des fonctions d'administration entre des personnels techniques et non techniques.
Exemple d'organisation :

- *Définition de la politique de sécurité du système de messagerie par le RSSI*
- *Définition de la politique d'utilisation de la messagerie par le responsable des Ressources Humaines ;*
- *Supervision et visualisation des rapports par le responsable géographique de la messagerie (c'est le resp. informatique de la zone Asie qui gère la sécurité du nom de domaine japonais @company.jp) ;*
- *Exploitation et gestion des zones de quarantaines par le prestataire informatique ou le technicien local.*

Garantie et Contrat de service (SLA - Service Level Agreement) :
Il sera opportun pour chaque solution d'évaluer les engagements en terme de disponibilité des machines et des process, ainsi que les temps de rétablissement (GTR) cible. De même, il faudra s'assurer des garanties de détection antivirale par exemple, voire des fréquences et des modes de mises à jour des antivirus.

Réduction des coûts de gestion et de personnels :
Comme nous l'avons souligné plus haut, la sécurité est une fonction vivante et en perpétuelle évolution. Il sera important d'étudier les charges de travail programmables et exceptionnelles découlant de l'installation, la formation, la gestion et la mise à jour de la solution.

Simplicité :
Une solution trop complexe pourra engendrer une réduction du niveau de sécurité due à une inadéquation avec les compétences internes. Voir Administrabilité.

Réduction des coûts de licence, matériels et maintenance :
L'évaluation budgétaire de la solution se fera de préférence sur la base de 3 années, en prévoyant les évolutions techniques à venir (doublement des machines lors d'une montée en puissance, acquisition d'un 2ème ou 3ème antivirus, ou d'une solution antispam complémentaire). Pour comparer les solutions, il sera judicieux de calculer un coût par utilisateur par mois ou par an.

Disponibilité :
La messagerie est une application sensible.
Dans le cadre d'une organisation internationale, il est évident que les fonctions de sécurité des e-mails doivent être disponible 24h/24, 7j/7.
Dans le cadre d'une organisation nationale, une indisponibilité de plus de 3 jours (Week-End prolongé, congés) d'un serveur de traitement des mails (ou du personnel compétent) peut être fort dommageable en terme d'image (renvoi à l'expéditeur).

6 - Réglementation

6.1. Quels sont les risques de la non fiabilité d'un système de messagerie ?

L'**actif** de la plupart des entreprises réside presque intégralement sur son système d'information dont le système de messagerie est un maillon fragile.

Une fragilité du système d'information peut résulter d'une faille dans le système de messagerie et peut conduire à la **mise en cause de la responsabilité civile et/ou pénale** de l'entreprise ou de son dirigeant. Cette responsabilité peut aussi être mise en cause en cas d'utilisation illicite du système de messagerie.

En cas de détérioration grave de l'actif, et si cette détérioration avait pu être évitée par une gestion « en bon père de famille » des actifs ;

- la responsabilité civile ou pénale du chef d'entreprise peut être engagée
- la responsabilité du DSI peut être engagée, soit pénalement si celui-ci dispose d'une délégation de pouvoir, soit au titre d'une sanction disciplinaire.

Il en est de même pour un certain nombre d'infractions liées à :

- La divulgation de données personnelles (salariés ou clients)
- La contrefaçon (licences piratées par l'entreprise ou ses salariés)
- Le non respect des dispositions de la Loi sur la Sécurité Quotidienne (LSQ) et la Loi sur l'Economie Numérique (LEN) sur la conservation des données de connexion et de chiffrement.
- La divulgation de savoir faire par un salarié de l'entreprise

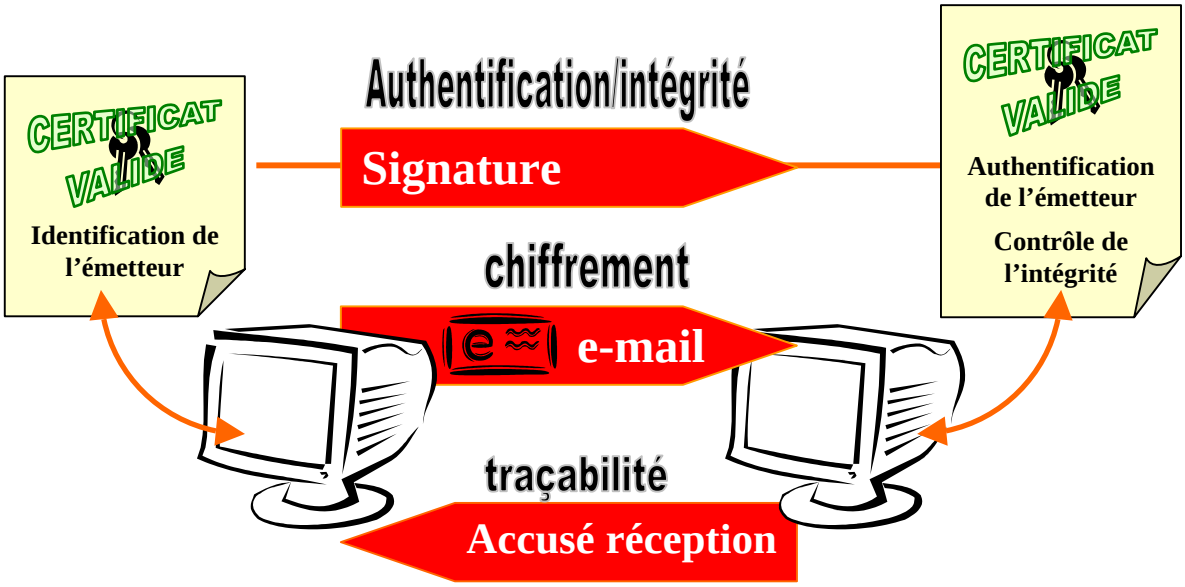
L'utilisation de la messagerie à des fins illicites engage également la responsabilité de l'utilisateur.

 © CLUSIF 2005

6.2. Quelles sont les composantes d'un système de messagerie électronique fiable ?

La confiance dans le monde numérique repose sur cinq piliers :

- La garantie de **confidentialité** des échanges, (chiffrement),
- La garantie de **l'identité de l'émetteur** du document, (Identification / Authentification),
- La garantie que le document **n'a pas pu être altéré** pendant sa création, son transport, sa restitution ou son archivage (Contrôle de l'intégrité),
- La fiabilité de la **traçabilité** des échanges numériques (conservation, horodatage….),
- Notion de **non répudiation** d'envoi (garantie par la signature du message).



6.3. L'environnement légal

Nous disposons en France d'un cadre juridique complet qui permet la mise en place d'un système d'échange par e-mail remplissant ces contraintes.

6.3.1 Le cadre législatif global

- Directive européenne 1999/93/CE du 13 décembre 1999,
- **Loi** n° 2000-230 du 13 mars 2000,
- Décret n° 2001-272 du 30 mars 2001,
- Décret n° 2002 -535 du 18 avril 2002,
- Arrêté du 31 mai 2002,
- Loi n° 2003-239 du 18 mars 2003 dite « loi pour la sécurité intérieure »
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,
- Loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle,
- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel,
- Plus un certain nombre de points de jurisprudence.

Avec la loi du 13 mars 2000 « *portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique* », la France a choisi d'opérer une modification en profondeur du droit de la preuve.

Cette loi ne rentre dans aucune considération technique. **Elle pose le principe de l'équivalence de l'écrit numérique et de l'écrit papier** sous réserve du respect de certaines conditions, explicitées dans des textes réglementaires techniques.

La loi française définit la signature par ses fonctions : identifier le signataire et attester de son consentement.

Elle définit les conditions qui permettent d'accorder la même valeur probatoire à l'écrit numérique et à l'écrit papier en posant deux conditions :

- L'utilisation d'un procédé fiable d'identification du signataire qui garantit notamment de façon fiable le lien de la signature électronique avec l'acte signé.
- La garantie d'intégrité de l'écrit numérique dans le temps.

Les décrets et la directive européenne sont des textes techniques qui préconisent les technologies à utiliser.

6.3.2 Le cadre législatif de la cyber–surveillance des salariés

Comment adapter un tel système aux obligations liées au respect de la vie privée ?

Les principes de droit qui découlent

- des conclusions du rapport de la CNIL du 5 février 2002
- de la position des tribunaux (arrêt Nikon)

A- 3 textes de loi :

- Code du Travail, article L120-2 : « **Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché** » - *PRINCIPE DE PROPORTIONNALITE*

- Code du Travail, article L432-2 : prévoit la **consultation du Comité d'Entreprise** lors de **l'introduction de Nouvelles Technologies** - *PRINCIPE DE DISCUSSION COLLECTIVE*

- Code du Travail, article L121-8 : prévoit **l'information préalable** des salariés sur tout dispositif et collecte de données les concernant personnellement – *PRINCIPE DE TRANSPARENCE*

B- Le rapport de la CNIL du 5 février 2002 : la cyber–surveillance sur les lieux de travail.

Conclusions du rapport :

- **Le contrôle des connexions à internet** : une interdiction générale et absolue de toute utilisation d'internet à des fins autre que professionnelles n'est pas réaliste, mais aucune disposition légale n'interdit à l'employeur d'en fixer les conditions et les limites.

  La CNIL préconise que ces informations ne puissent être conservées plus de six mois par l'employeur.

- **Le contrôle de l'usage de la messagerie** : pour la CNIL, un message est personnel si sa nature personnelle est indiquée de façon manifeste dans l'objet du message ou le nom du répertoire où il est archivé ; il est alors protégé par le secret des correspondances.

- **Le rôle des administrateurs de réseau :** Ils ne peuvent procéder à aucune exploitation des informations dont ils ont connaissance à des fins autres que le bon fonctionnement et la sécurité du système d'information, de leur propre initiative ou sur ordre hiérarchique *(sic!)* En particulier, ils ne peuvent divulguer des informations relevant du secret des correspondances ou relevant de la vie privée des utilisateurs si

celles-ci ne mettent en cause ni le bon fonctionnement du système, ni sa sécurité, ni les intérêts de l'entreprise (Cf. arrêt CA Paris décembre 2001, *infra*)

- **La désignation d'un « correspondant à la protection des données à caractère personnel »** : il est plus particulièrement chargé au sein de l'entreprise des questions relevant des mesures de sécurité, du droit d'accès et de la protection des données personnelles sur le lieu de travail. (Cf. loi du 6 août 2004 et décrets d'application).

C- L'arrêt « Nikon » de la Cour de Cassation, 2 octobre 2001

Le salarié a droit, ***même au temps et au lieu de travail****, au* ***respect de l'intimité de sa vie privée.*** *Celle-ci* ***implique en particulier le secret des correspondances***

L'employeur ne peut dès lors, sans violation de cette ***liberté fondamentale*** *prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci* ***même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur***

Cet arrêt NE DOIT PAS ÊTRE CONSIDERE COMME UN ARRÊT DE PRINCIPE, mais plutôt comme la PREMIÈRE PIERRE d'un édifice jurisprudentiel à construire

Il CONDAMNE EN EFFET LES INTERDICTIONS PURES ET SIMPLES de toute utilisation d'internet à des fins privées par le salarié, mais n'empêche en aucune façon d'encadrer celle-ci

D- L'arrêt de la Cour d'Appel de Paris du 17 décembre 2001

La ***préoccupation de la sécurité du réseau*** *justifie que les administrateurs systèmes fassent usage de leur position et des possibilités techniques dont ils disposent pour* ***mener les investigations et prendre les mesures*** *que cette sécurité impose*

Par contre, ***la divulgation du contenu des messages ne relève pas de ces objectifs***

Analyse de ces textes :

6.3.2.1 Ce qui est acquis :

A- L'EXISTENCE D'UNE SPHÈRE RÉSIDUELLE D'INTIMITÉ SUR LE LIEU DE TRAVAIL ET PENDANT LE TEMPS DE TRAVAIL

En réalité, LA FRONTIÈRE ENTRE VIE PRIVÉE ET VIE PROFESSIONNELLE TEND DE PLUS EN PLUS À SE BROUILLER : dans beaucoup d'entreprises, les salariés peuvent consulter et utiliser leur messagerie professionnelle aussi bien sur leur lieu de travail qu'ailleurs (chez eux, en week-end, pendant leurs vacances ...)

Depuis le début de l'année 2001, les employeurs peuvent même donner à leur salarié du matériel informatique neuf pour leur usage personnel, ce don n'étant pas soumis à cotisation sociale (art 4. Loi de finance pour 2001)

B- LA LÉGITIMITÉ DE L'EXISTENCE D'UN CONTRÔLE PAR L'EMPLOYEUR, dès lors qu'il est justifié par :

- La maîtrise des coûts de connexion ;
- Le bon fonctionnement technique du réseau (surcharges fréquentes dues à l'envoi en masse de fichiers très volumineux d'images ou de sons) ;
- La protection contre les virus ;
- La maîtrise de la responsabilité de l'entreprise en cas de comportements délictueux de ses préposés (accès à des sites illicites, élaboration de contenus illicites depuis son poste de travail, etc.) ;
- La sécurité de l'entreprise, compte tenu de son secteur d'activité ;
- Le cas échéant, la surveillance d'une éventuelle activité professionnelle concurrente…

6.3.2.2 Ce qui est discuté :

A- LA QUALIFICATION DE CERTAINS E-MAILS DE « CORRESPONDANCE PRIVÉE », ce qui entraîne du même coup :

- L'application du principe du secret des correspondances (rappelé en matière de télécommunications par la loi du 10 juillet 1991)
- L'irrecevabilité de la preuve correspondante pour fonder une mesure disciplinaire, et notamment un licenciement disciplinaire

Suffit-il **qu'un e-mail porte la mention « personnel », ou soit répertorié dans une librairie « personnel »** pour être automatiquement qualifié de correspondance privée et non consultable par l'employeur, dès lors qu'il respecte des contraintes techniques préétablies (pas de fichiers attachés, ou vidéo ou son par exemple) ?
Ou un message est-il personnel dès lors que son **contenu concerne des faits relevant de la vie privée du salarié** ?

B- LE ROLE ET LA RESPONSABILITE DES ADMINISTRATEURS RESEAUX

Etant acquis que l'entreprise exerce un contrôle, par l'intermédiaire de ses administrateurs systèmes, et que ceux-ci sont nécessairement amenés à connaître des informations relevant de la vie privée des salariés, **jusqu'où et dans quelle mesure peuvent et doivent ils en faire part aux dirigeants de l'entreprise** ?

Cet aspect, encore ignoré par la plupart des entreprises, **devra rapidement faire l'objet d'une organisation adéquate** car elle a un impact sérieux sur la responsabilité professionnelle des Directeurs de Système d'Information (ou administrateurs systèmes), et le cas échéant sur leur responsabilité pénale.

6.3.2.3 Ce qui est envisageable :

A- Sur le fond :

- **Une interdiction pure et simple de l'utilisation d'internet à des fins personnelles au lieu ou au temps du travail paraît difficile**, c'est du moins la position de la CNIL et de la Cour de cassation (Ce qui n'est pas anodin, si l'on considère qu'environ 80% des chartes actuelles interdisent au salarié l'usage du mail à des fins personnelles)

Les deux aspects essentiels vont maintenant concerner :

- La **détermination du caractère privé** d'un message envoyé ou reçu au lieu et au temps du travail, avec des moyens mis à disposition par l'employeur

- L**'encadrement** de l'usage de ces moyens à des fins privées par le salarié

B- Sur la forme :

- **Une charte** : document établi de façon unilatérale par l'employeur, valeur juridique faible (sauf si elle s'intègre au règlement intérieur)

- **Des négociations collectives** : ont la préférence de la CNIL, valeur juridique forte

- **Un accord individuel avec les salariés**

  Rappel : un règlement intérieur, donc à plus forte raison une « charte », doit être conforme aux lois et règlements (art L122-35 Code du Travail).

  Par ailleurs, c'est le juge qui en cas de conflit exercera le contrôle de proportionnalité au regard du respect de la vie privée consacré par l'article 9 du Code Civil, risquant ainsi d'invalider certains comportements de l'employeur alors même qu'ils auraient été individuellement acceptés par l'employé.

7 - Annexes

7.1. Glossaire

Adresse IP	Nombre binaire de 32 bits permettant d'identifier et d'accéder de manière unique à un ordinateur connecté à un réseau IP. Ce nombre est lui-même composé de 4 nombres compris entre 0 et 255 séparés par des points, par exemple : 10.0.0.123.
ACL	Access Control List ou Liste de Contrôle d'accès. Liste donnant pour l'utilisateur ses droits d'accès aux ressources.
Authentifier	Assurer l'origine d'un message et/ou l'identité de son émetteur.
BAL	Boîte Aux Lettres. Fichier où sont stockés les messages d'un destinataire à mesure qu'ils arrivent sur le serveur de messagerie.
Black-list	Liste d'adresses de serveurs suspects dont on refuse les messages.
Client	C'est un logiciel qui demande un service à un logiciel « Serveur » via un protocole.
Condensé	Chaîne de caractères associés à un message spécifique par un algorithme de hachage.
Confidentialité	Caractéristique d'une information que l'on considère comme n'ayant pas à être consultée par d'autres personnes que celles qui ont à la connaître.
Cryptographie	Chiffrement et déchiffrement des messages.
Déni de service	Engorgement volontaire d'un réseau pour l'empêcher de fonctionner. Synonyme : DOS (Denial of Service).
E-mail	C'est le terme anglo-saxon pour désigner un message électronique ou « courriel » en français. C'est le terme en usage dans le monde de la messagerie.
ESMTP	Le protocole ESMTP (Extended Simple Mail Transfer Protocol) est une amélioration du protocole SMTP avec lequel il est compatible.
Extranet	Intranet entre une entreprise, tout ou partie de ses clients et ses fournisseurs.
Hachage	Algorithme qui, à un message donné, associe une chaîne spécifique de caractères au texte d'un message. L'algorithme garantit une très faible probabilité pour que deux messages différents conduisent à la même chaîne de caractères.
Hoax	Messages alarmants, incitant leur lecteur à le router vers leurs contacts de messagerie pour les avertir, provoquant ainsi un engorgement des réseaux. Il incite parfois à supprimer certains fichiers indispensables au fonctionnement du poste de travail. Synonyme : Canular.

HTTP	Hyper Text Tranfer Protocol
HTTPS	Hyper Text Tranfer Protocol over SSL
IMAP	Le protocole IMAP (Internet Message Access Protocol) est une amélioration du protocole POP3
Intégrité	Caractéristique d'une information que l'on considère comme n'ayant pas été modifiée accidentellement ou par une tierce personne.
Internet	Ensemble des réseaux utilisant les protocole TCP/IP et tous interconnectés entre eux à travers le monde.
Intranet	Réseau privé d'entreprise qui utilise les technologies de l'Internet.
IP	« Internet Protocol », protocole du monde internet. Il assure le routage des paquets IP.
MDA	Mail Delivery Agent ou Agent de Distribution de Message. Ce logiciel situé sur les serveurs de messagerie distribue les messages dans les Boîtes à Lettres (BAL) des destinataires concernés.
MTA	Mail Transfer Agent ou Agent de Transfert de Message. Application TCP/IP qui achemine les messages électroniques entre les serveurs.
MUA	Mail User Agent, Logiciel Client, il fournit l'interface entre l'utilisateur et la messagerie.
POP3	Le protocole POP3 (Post Office Protocol) permet à un Client de messagerie de récupérer ses messages dans sa boîte à lettres.
Port	Numéro associé à un service (tcp ou udp) utilisé par un Client pour obtenir ce service d'un Serveur ; On dit que « le serveur écoute sur le port ». (25 est le port tcp pour le service SMTP).
Protocole	C'est un ensemble de règles qui définissent les formats des messages et le dialogue entre deux entités qui échangent ces messages.
Relayage de mail	Assure le routage des messages du MTA de l'expéditeur aux MTA des destinataires à travers un ou plusieurs MTA intermédiaires.
Répudiation	Refuser de reconnaître avoir reçu ou émis un message déterminé.
Serveur	C'est un logiciel qui fournit un service à un logiciel « Client » via un protocole. C'est aussi un ordinateur qui héberge un logiciel Client.
SMTP	Le protocole SMTP (Simple Mail Transfer Protocol) est le protocole standard permettant de transférer le courrier soit d'un client à un serveur, soit d'un serveur à un autre en connexion point à point.
Sniffer	Logiciel qui permet d'analyser le trafic sur une ligne de communication. Il permet entre autre de lire les identifiants et les mots de passe de l'utilisateur lorsque ceux-ci circulent en clair sur le réseau.
spam	Inondation de messages publicitaires sur le poste d'un utilisateur (pourriel).

TCP	Transmission Control Protocol, protocole de la suite TCP/IP qui assure le transport des paquets IP.
TCP/IP	Transmission Control Protocol / Internet Protocol, suite de protocoles réseau qui règlent les échanges entre Clients et Serveurs sur l'Internet.

7.2. Protocoles : références RFC

Le tableau suivant donne les références des normes IETF (Internet Engineering Task Force) qui définissent les protocoles cités dans cet ouvrage.

Protocoles	Norme IETF
Simple Mail Transfer Protocol (SMTP)	RFC 821
Format of mail messages	RFC 822
Domain Name System (DNS)	RFC 974
Message formats conversion with x. 400 mail	RFC 1327
Electronic mail vocabulary	RFC 1711
Security Multiparts for MIME	RFC 1847
SMTP services extensions	RFC 1869
SMTP Service Extension for Delivery Status Notifications	RFC 1891
POP Office Protocol (POP3)	RFC 1939
SMTP Service Extension for Returning Enhanced Error Codes	RFC 2034
MIME Part 1 : Format of Internet Message Bodies	RFC 2045
MIME Part 2 : Media Types	RFC 2046
Internet Message Access Protocol (IMAP)	RFC 2060
IMAP4 ACL Extension	RFC 2086
	RFC 2246
Intégration du protocole TLS au protocole SMTP	RFC 2407

 © CLUSIF 2005

7.3. Codes retour SMTP

SMTP est le protocole utilisé pour envoyer les messages. Si vous obtenez une erreur SMTP, cela signifie que votre message n'a probablement pas été envoyé. Il est utile de comprendre pourquoi ce message n'a pas été pris en compte, afin de régler le problème.

codes	Erreurs les plus répandues
421	Service non disponible, ce code peut apparaître à n'importe quel moment, avant coupure du service
432	Mot de passe de transition nécessaire.
450	Requête non prise en compte, boîte inaccessible ou occupée
451	Requête avortée, erreur de traitement local
452	Requête non prise en compte, espace mémoire insuffisant
454	TLS temporairement indisponible. Chiffrement requis par le mécanisme d'authentification interrogé
458	Impossible de mettre en file d'attente les messages pour le noeud
459	Le noeud "noeud" non autorisé : raison
500	Erreur de syntaxe, commande non reconnue, ligne de commande trop longue
501	Erreur de syntaxe, paramètres ou arguments erronés
502	Commande non supportée
503	Séquence des commandes incorrecte
504	Paramètre non supporté
521	Cette machine n'accepte pas de courrier.
530	Authentification requise. OU Doit être précédé d'une commande STARTTLS. Chiffrement requis par le mécanisme d'authentification interrogé
534	Mécanisme d'authentification trop faible
538	Chiffrement requis par le mécanisme d'authentification interrogé
550	Action non prise en compte, boîte invalide ou inaccessible
551	Utilisateur non déclaré localement
552	Action avortée, insuffisance de place disque
553	Action avortée, nom de la boîte invalide
554	Transaction avortée

codes	Messages de service
211	Etat du système
214	Message d'information
220	Service prêt
221	Fermeture du canal de transmission
250	Action exécutée
251	Utilisateur non local, message transféré
354	début de saisie du message, fin avec un . (point)

Composition des codes

Tous les codes SMTP comprennent 3 chiffres par exemple : 550, 221, 354, etc. Tous ne sont pas des codes d'erreurs, vous trouverez ci-dessous la signification de chaque chiffre. Si le premier chiffre est un 4 ou un 5, c'est un message d'erreur.

Premier chiffre	Message
1	Commande acceptée
2	Commande exécutée
3	Commande comprise, mais informations complémentaires requises
4	Commande avortée, erreur temporaire, la demande peut être répétée
5	Commande avortée, erreur grave

7.4. Exemples d'e-mails

7.4.1 E-mail signé

```
Return-Path: <claude.robin@fagguel.com>
Received: from strtrobin ([255.xx.xxx.xx])
      by alox.fagguel.com (8.12.9/8.12.9) with ESMTP id hACAd1Yb006717
      for <Jean-Francois.Beaucel@fagguel.com>; Wed, 12 Nov 2003 11:39:01
+0100 (MET)
From: "Claude ROBIN" <claude.robin@fagguel.com>
To: =?iso-8859-1?Q?Jean-Fran=E7ois_BEAUCEL?= <Jean-
Francois.Beaucel@fagguel.com>
Subject: essai
Date: Wed, 12 Nov 2003 11:39:08 +0100
MIME-Version: 1.0
Message-ID: <004901c3a909$34327e30$479c329e@strtrobin>
Content-Type: multipart/signed;
      protocol="application/x-pkcs7-signature";
      micalg=SHA1;
      boundary="----=_NextPart_000_0042_01C3A911.929C97A0"
X-Priority: 3 (Normal)
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook, Build 10.0.3416
Importance: Normal
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-MailScanner: Found to be clean
X-UIDL: I^W!!)`V!!50W!!hpl"!

This is a multi-part message in MIME format.

------=_NextPart_000_0042_01C3A911.929C97A0
Content-Type: multipart/alternative;
      boundary="----=_NextPart_001_0043_01C3A911.929C97A0"


------=_NextPart_001_0043_01C3A911.929C97A0
Content-Type: text/plain;
      charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

essai_message-sign=E9

------=_NextPart_001_0043_01C3A911.929C97A0
Content-Type: text/html;
      charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META HTTP-EQUIV=3D"Content-Type" CONTENT=3D"text/html; =
charset=3Diso-8859-1">
<TITLE>Message</TITLE>

<META content=3D"MSHTML 6.00.2722.900" name=3DGENERATOR></HEAD>
<BODY>
<DIV><FONT face=3DArial size=3D2><SPAN=20
class=3D296463710-12112003>essai_message-sign=E9</SPAN></FONT></DIV></BOD=
Y></HTML>

------=_NextPart_001_0043_01C3A911.929C97A0--
```

```
------=_NextPart_000_0042_01C3A911.929C97A0
Content-Type: application/x-pkcs7-signature;
      name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="smime.p7s"


MIAGCSqGSIb3DQEHAqCAMIACAQECzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIM8zCCA0kw
ggIxoAMCAQICBDryj7YwDQYJKoZhvcNAQEFBQAwXDETMBEGCgmSJomT8ixkARkTA2NvbTETMBEG
CgmSJomT8ixkARkTA2FmcDEVMBMA1UECxMMQXBwbGljYXRpb25zMQwwCgYDVQQLEwNQS0kxCzAJ
BgNVBAMTAkNBMB.........

........STELMAkGA1UEAxMCQ0ECBD31/FkwDQYJ
KoZIhvcNAQEBBQAEgYBLn5DqgQX+l/3OpDaLJVg3GrwXHfQ2har4+wwZIEs+wAQa+srbIT2wRKJ
qpwBCJogTn861BUOzQUTT2lWSZyPL/oK267+1b4O4nM0o0I+MdZASZLCEFPDSfDhbfA43Anx0hJ
hb5pUqTjtsOidCIOjlJaRpW++2bhXnAZurT1gAAAAAAAA==

------=_NextPart_000_0042_01C3A911.929C97A0—
```


7.4.2 E-mail chiffré


```
Return-Path: <claude.robin@fagguel.com>
Received: from strtrobin ([255.xx.xxx.xx])
      by alox.fagguel.com (8.12.9/8.12.9) with SMTP id hACCVvYb023351
      for <Jean-Francois.Beaucel@fagguel.com>; Wed, 12 Nov 2003 13:31:57
+0100 (MET)
Message-ID: <024801c3a919$68d4d100$2a9e329e@strtrobin>
From: =?iso-8859-1?Q?Jean-fran=E7ois_BEAUCEL?= <Jean-
Francois.Beaucel@fagguel.com>
To: "Claude ROBIN" <claude.robin@fagguel.com>
Subject: =?iso-8859-1?Q?essai_message_chiffr=E9?=
Date: Wed, 12 Nov 2003 13:34:59 +0100
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
      smime-type=enveloped-data;
      boundary="----=_NextPart_000_0245_01C3A921.C79BB070";
      name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
      filename="smime.p7m"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.50.4807.1700
X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4910.0300
X-MailScanner: Found to be clean
X-UIDL: ,IB"!>d]!!3J0!!amo"!
```

7.5. Exemple de charte

MESSAGERIE INTERNE ET SECURITE

La messagerie électronique est un outil très pratique dont l'utilisation requiert le respect d'un certain nombre de règles. Son utilisation peut être dangereuse. En conséquence :

Evitez d'encombrer la messagerie

La propagation de canulars ou autres chaînes de provenance externe est une cause d'encombrement de la messagerie. L'auteur malveillant joue sur le catastrophisme ou la sensibilité. Il se prévaut souvent d'autorités incontestées et se fait passer pour une société ou une marque de renom…et demande une très large propagation du message. Le cas le plus classique est l'annonce d'arrivée de virus.

Que faire dans ce cas ?

Surtout ne jamais ouvrir la pièce jointe et ne jamais la propager. Avertir votre service informatique et détruire le message.
Dans ce domaine, n'exécuter que les directives émanant du service informatique qui est le seul interlocuteur privilégié.
Attention aux envois trop volumineux qui encombrent et parfois bloquent la messagerie. Les boîtes aux lettres ne sont pas extensibles, il faut les purger régulièrement.
Eviter également les envois à un grand nombre de destinataires en même temps.

Préservez la confidentialité

Ce média facile d'utilisation n'est pas sûr. La confidentialité ne peut être assurée.
Ce moyen est amplificateur de certaines fuites d'information et d'erreurs de communication :

- listes de diffusion non à jour
- homonymie de destinataires

Enfin, lors du transfert d'un message s'assurer que les correspondants choisis sont habilités à lire ces informations.

Déléguez l'accès à votre boîte de réception à bon escient

Ce média permet d'offrir à des collègues ou des collaborateurs l'accès à votre boîte de réception. Cette faculté est indispensable à votre secrétaire. N'oubliez pas qu'il est absolument proscrit de communiquer son mot de passe. Faites attention à la propriété des messages.
Tous les messages que vous recevez sur votre poste ou que vous émettez appartiennent à l'entreprise Si besoin est, votre hiérarchie peut, dans le respect d'une déontologie, demander l'intervention des services techniques pour accéder à votre messagerie. Veillez à verrouiller votre station lorsque vous quittez votre poste de travail afin d'éviter l'utilisation de votre messagerie à votre insu.

EN CONCLUSION, N'UTILISEZ LA MESSAGERIE QUE POUR LES BESOINS PROFESSIONNELS, RESPECTEZ STRICTEMENT LES REGLES DES DIRECTIVES TECHNIQUES, LES RECOMMANDATIONS DU CODE DE DEONTOLOGIE ET ADRESSEZ-VOUS AU SERVICE INFORMATIQUE EN CAS DE DIFFICULTE.