Faire confiance, c'est bien... contrôler, c'est mieux

Autor(en): **Baessler, Felix**

Objekttyp: **Article**

Zeitschrift: **Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology**

Band (Jahr): **75 (1997)**

Heft 9

PDF erstellt am: **11.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-876967

MailGuard®[1]: signature et confidentialité dans le trafic électronique des messages

Faire confiance, c'est bien... contrôler, c'est mieux

Cet article s'adresse aux lecteurs intéressés par la technique et qui travaillent avec des systèmes de messagerie électronique – ou systèmes E-mail – que ce soit en tant qu'utilisateurs ou en tant qu'exploitants. Nous traiterons d'abord des fonctions de base nécessaires pour protéger les systèmes de messagerie, puis de la configuration de l'interface utilisateur à l'aide d'un prototype développé par Télécom PTT.

FELIX BAESSLER, BERNE

Quand nous recevons par la poste une lettre privée ou professionnelle qui nous est adressée personnellement, nous nous attendons naturellement à ce qu'elle nous soit remise signée et fermée. Cette «tradition» est ancrée si profondément dans notre vie sociale que si un expéditeur ne la respecte pas, cela suscite forcément en nous une certaine irritation.

Rien de tel avec la poste électronique! Des privés et des entreprises reçoivent chaque jour des dizaines de communications, sans se préoccuper du fait que ni la confidentialité, ni l'identité de l'auteur ne sont garanties. Il semble évident que la plupart d'entre nous se soient accommodés – consciemment ou inconsciemment – du fait que les systèmes électroniques de messagerie courants présentent en général de grosses lacunes en matière de sécurité. Cet état de fait ne devrait pas pour autant porter à conséquence, car pour les messages vraiment importants, nous continuons à nous en remettre à notre «bonne vieille poste».

Le courrier électronique circule effectivement dans la plupart des cas sans protection, que ce soit dans les réseaux publics ou privés. Pour illustrer ce fait, prenons un exemple parmi tant d'autres: dans les cercles spécialisés, il y a longtemps que ce n'est plus un secret pour personne que sur Internet on peut falsifier des adresses d'expéditeur, voire des voies d'acheminement complètes, même avec des connaissances limitées. Il faudrait donc toujours demander confirmation d'un message suspect reçu via Internet (invitation, commande, etc.) en utilisant un autre canal, par exemple le téléphone, si l'on ne veut pas courir le risque de devenir la victime d'une mauvaise plaisanterie ou, plus grave, d'un acte criminel!

Par chance, les moyens techniques disponibles à l'heure actuelle nous permettent de réduire au minimum les risques, apparemment inévitables, que présente la poste électronique. Sans entrer dans les détails, nous sommes en mesure d'affirmer que la qualité et les garanties offertes aux utilisateurs par un système de messagerie électronique protégée sont les mêmes que celles auxquelles nous a habitués la poste conventionnelle. Celui qui reçoit un message électronique protégé peut en particulier vérifier à tout moment l'identité de l'auteur/expéditeur au moyen de la signature[2] électronique. De même, la confidentialité du message peut être garantie par un codage.

Un essai pilote mené par la direction Recherche et développement avec le système de messagerie «MailGuard®», qui est muni de fonctions de sécurité, a montré concrètement que les exigences posées aux utilisateurs en matière d'utilisation peuvent être maintenues à un niveau si faible qu'elles ne représentent en aucun cas un obstacle à une future installation à grande échelle de produits protégés, que ce soit au sein de l'entreprise ou dans le cadre d'un service public.

Evolution historique de la messagerie

Les exigences fondamentales des expéditeurs et des destinataires en ce qui concerne un système de messagerie reposant sur du papier sont:

- identification de l'expéditeur du message/de la transaction
- vérification de l'identité de l'auteur/l'expéditeur
- vérification que le message/la transaction envoyé et reçu sont identiques, sans modification aléatoire ou intentionnelle
- preuve que l'échange de messages ou la transaction a bien eu lieu
- confidentialité du contenu du message/de la transaction vis-à-vis de tiers non autorisés
- disponibilité de l'infrastructure du système de communication de base.

A travers les siècles, les règles de la correspondance se sont établies progressivement en une convention sociale extrêmement stable, avec laquelle nous nous familiarisons dès l'enfance et que nous acceptons la plupart du temps sans arrière-pensée parce que «c'est comme ça».

Ces règles héritées du passé, qui se sont développées manifestement à partir d'un besoin de sécurité et de garantie universelles, sont à la base du traitement des exigences analogues dans le cadre de la messagerie électronique.

Les services de sécurité dans les télécommunications

Dans les télécommunications, les services de sécurité sont traités de manière approfondie et très détaillée par les organisations internationales que représentent l'ISO (International Organization for Standardization) et l'ECMA (European Computer Manufacturers Association). Dans le fond, il s'agit là cependant des mêmes critères et des mêmes dangers que ceux qui nous sont familiers dans un système basé sur le papier.

[1] Marque déposé par Télécom PTT

[2] Ne pas confondre la signature électronique (fig. 1) avec une signature numérisée, soit une image de la signature scannée et mémorisée dans un fichier sous forme d'une matrice de points.

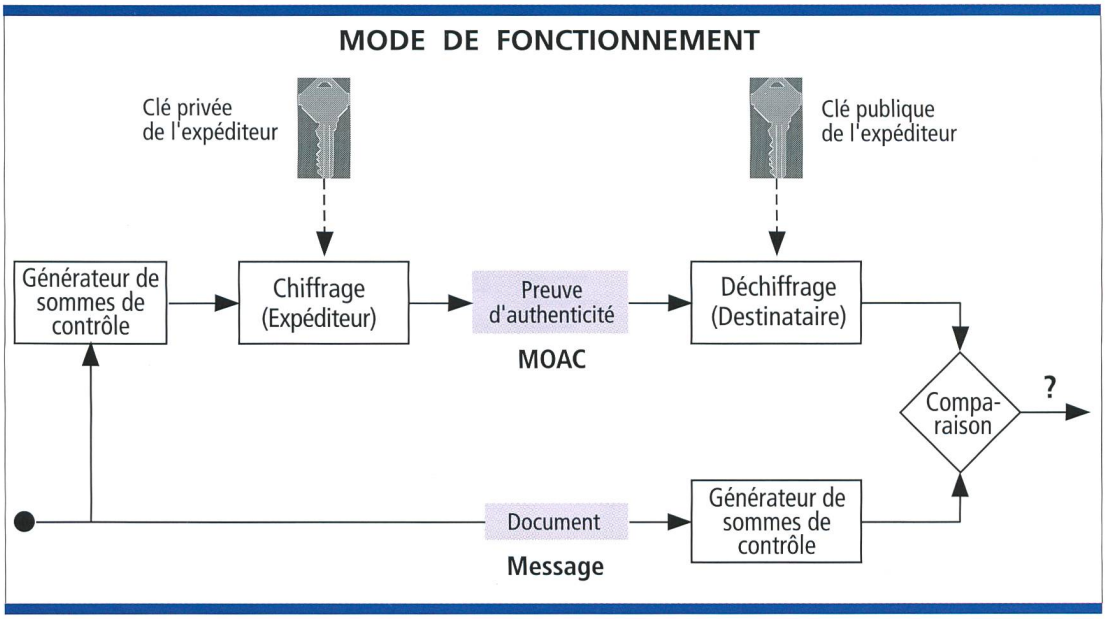

Fig. 1. Mode de fonctionnement des signatures électroniques.

Identification
L'expéditeur se fait généralement connaître en indiquant son nom et/ou son titre. Pour des transactions commerciales, ce sont souvent des logos préimprimés qui servent à identifier l'entreprise.

Authenticité/Falsification des signatures
Les signatures manuscrites sont le moyen le plus répandu pour identifier un individu. Les sceaux utilisés autrefois sont aujourd'hui habituellement réservés aux notaires. Ces derniers – en tant que troisième pouvoir indépendant – («trusted third party») jouent un rôle important, même avec les systèmes électroniques modernes.

Intégrité/Modification de documents
Afin d'assurer l'intégrité des documents (par rapport à la falsification), on a mis au point de l'encre qui, associée à du papier spécial, rend les manipulations visibles.

Incontestabilité (non repudiation)/ Contestation de documents
Pour éviter que des engagements pris puissent ensuite être contestés, on a introduit des procédés de vérification des signatures. En cas de désaccord, des ins-

Procédures d'envoi et de réception dans un échange de messages protégé

Procédure de l'expéditeur

1 Calcul de la somme de contrôle (empreinte digitale, valeur de hashing) du message
2. Signature de la somme de contrôle, par chiffrage avec la clé privée de l'expéditeur
3. Mémorisation des données ainsi obtenues dans le MOAC
4. Génération d'une clé de message DES secrète
5. Chiffrage du message avec la clé de message générée
6. Chiffrage de la clé de message avec la clé publique du destinataire
7. Mémorisation des données ainsi obtenues dans le MT
8. Signature du MT (y compris identité du destinataire) par chiffrage avec la clé privée de l'expéditeur
9. Composition de l'information protégée qui contient le message chiffré et les données de sécurité OC, MT, MOAC
10. Envoi de l'information protégée

Procédure du destinataire

1. Réception de l'information protégée
2. Vérification de l'authenticité des données de protection par déchiffrage des signatures de l'OC, du MT, du MOAC avec la clé publique de l'instance de certification (OC) ou de l'expéditeur (MT, MOAC)
3. Déchiffrage de la clé de message contenue dans le MT avec la clé privée du destinataire
4. Déchiffrage du message avec la clé de message extraite
5. Calcul de la somme de contrôle du message récupéré, du côté du destinataire
6. Déchiffrage de la somme de contrôle contenu dans le MOAC, du côté de l'expéditeur
7. Test de l'identité des deux sommes de contrôle

Tableau 1. Procédures d'envoi et de réception dans un échange de messages protégé. Structures des données de protection OC (Originator Certificate), MT (Message Token), MOAC (Message Origin Authentication Check).

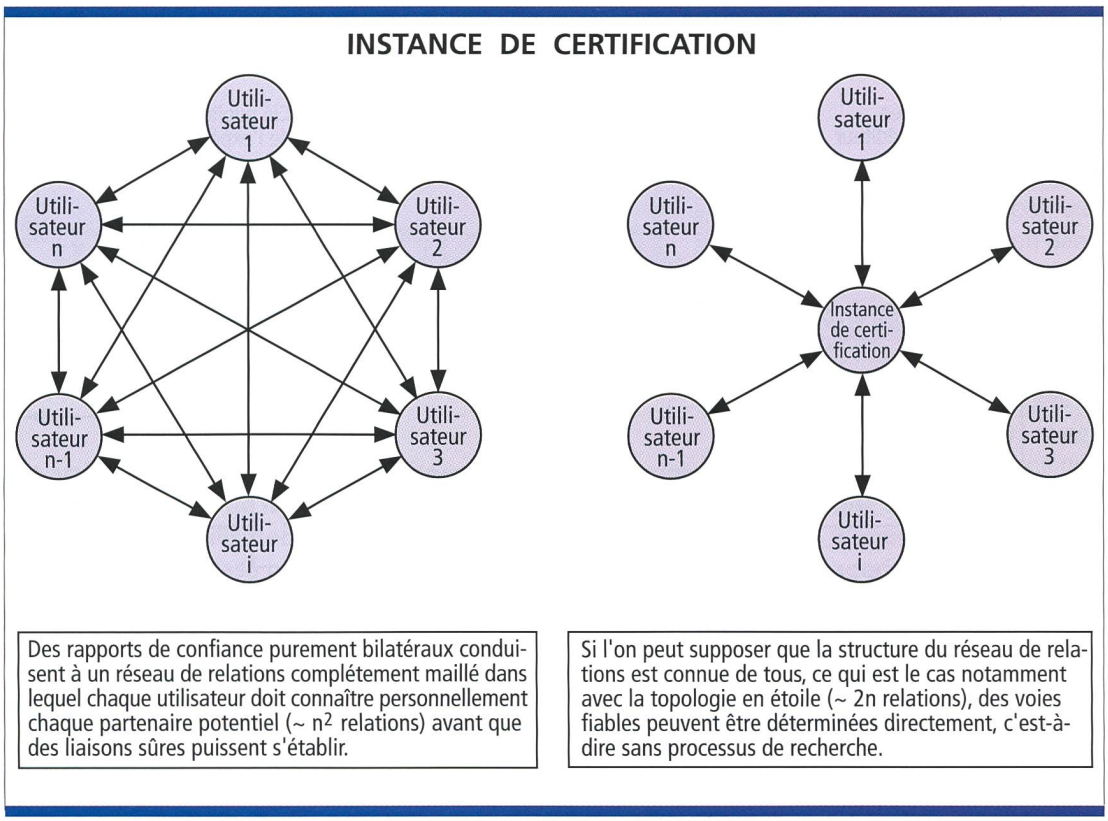

Fig. 2. Rôle de l'instance de certification pour des populations d'utilisateurs importantes.

tances indépendantes peuvent être sollicités comme tribunal arbitral.

Confidentialité/Accès aux informations
Des mesures de protection physiques comme la fermeture ou le cachetage de l'enveloppe permettent à des tiers de savoir que le contenu du message est à caractère privé. La cryptographie, qui joue un grand rôle dans le domaine de l'électronique, a longtemps été réservée à l'armée et aux services de renseignement.

Disponibilité/Perte d'information ou défaillances du service
La structure du réseau postal, par nature décentralisée, était autrefois garante de sa robustesse face à la violence, au vandalisme ou au terrorisme. A maintes reprises on a pu constater que même dans des situations exceptionnelles extrêmes, ce service fait preuve d'une résistance étonnante.
Dans le chapitre concernant les bases techniques et les options d'implémentation, nous reviendrons sur certains éléments de sécurité, notamment sur l'intégrité et l'authenticité, ainsi que sur la confidentialité et l'incontestabilité.

Besoins actuels du marché en matière de garantie et de protection
Les raisons pour lesquelles la correspondance privée et commerciale s'effectue de plus en plus par voie électronique sont faciles à déterminer:
- durée de transmission plus courte (à peu près indépendante de la distance)
- frais généraux réduits (en particulier si l'on tient compte de ce qu'on appelle le «handling»)
- meilleure intégration de la génération, de la transmission et de l'acceptation de messages (aspect compatibilité)
- archivage plus efficace (banques de données).

Il ne faut cependant pas oublier que l'évolution ultrarapide de la transmission de documents sous forme de papier vers la messagerie électronique accroît considérablement les risques en matière de sécurité, car l'accès direct à l'information via les réseaux de données facilite naturellement les attaques contre les critères de protection et de garantie mentionnés plus haut (authenticité, intégrité, confidentialité, etc.)
De plus, il faut considérer les points suivants:
- La diffusion des PC a considérablement accru la vulnérabilité de la messagerie électronique. En effet, alors qu'autrefois seuls quelques collaborateurs avaient accès, dans un petit nombre de centres de calcul, au domaine des télécommunications, aujourd'hui n'importe qui peut pratiquer le piratage sans aucun contrôle et en tout anonymat.
- Les systèmes électroniques de transmission peuvent déposer des copies de messages dans des centres de distribution sans que l'expéditeur ou le destinataire ne soient au courant. Les recherches dans ce domaine s'avèrent difficiles, car on ne sait même pas toujours par quel nœud du réseau un message a transité.
- Certains systèmes de traitement de texte se contentent de rendre invisibles les passages concernés au lieu de les effacer vraiment, sans les éliminer complètement ni réécrire par-dessus. On peut facilement imaginer que l'échange de données de ce type – même par disquette – peut conduire à des situations plus que désagréables.

Le dernier point évoqué met en évidence, pour les procédés électroniques, une faiblesse générale que l'on a parfois tendance à sous-estimer.
Alors que dans un service basé sur le papier, l'auteur/l'expéditeur peut encore voir concrètement ce qu'il met dans une enveloppe, nous devons aujourd'hui, à l'époque de l'électronique, «faire confiance» aux programmes de traite-

ment de texte, d'édition ou de publipostage. La situation esquissée devient encore plus critique en ce qui concerne la signature électronique, car nous n'avons même plus la possibilité de saisir vraiment la portée de ce que nous signons. Si autrefois nous avions l'habitude de parapher chaque page d'un document important avant d'y apposer notre signature finale, aujourd'hui nous devons accorder toute notre attention à ce que des programmes parfaitement dignes de confiance et dont la fiabilité a été éprouvée soient utilisés, surtout dans le domaine de la sécurité.

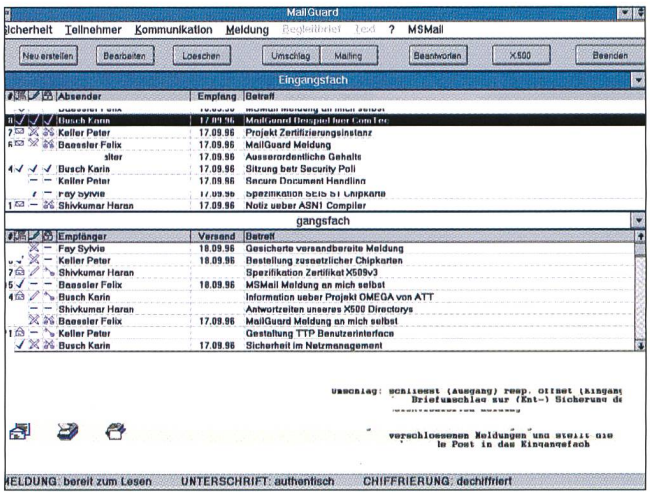

Fig. 3. Fenêtre principale de MailGuard® avec champs d'entrée/sortie.

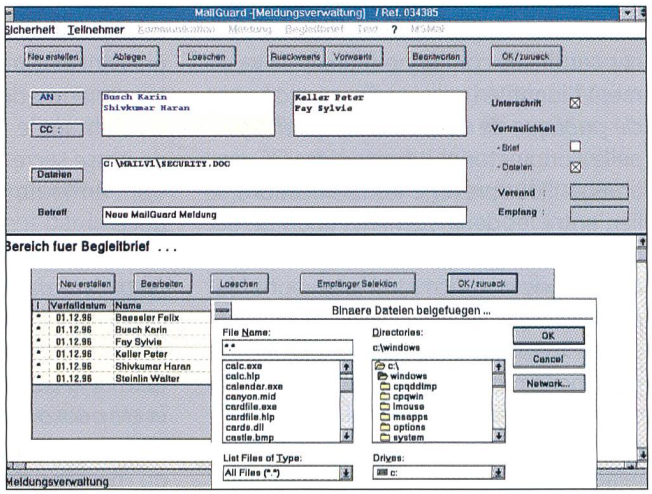

Fig. 4. Sous-fenêtre de gestion des messages: rédaction d'un message.

Fondements/Bases techniques et options d'implémentation

On s'étonnera peut-être d'apprendre que la plupart des principes de base utilisés de nos jours pour la sécurité électronique des messages étaient déjà connus depuis des décennies et même ouvertement disponibles dans une large mesure. Par contre, ce qui a énormément augmenté ces dernières années, ce sont d'une part les besoins en matière de protection et de garantie exprimés par les utilisateurs, dont nous avons déjà parlé, et d'autre part la puissance de calcul disponible sur les postes de travail. L'accroissement massif de la capacité des PC permet aujourd'hui de faire exécuter les procédures de sécurité «de bout en bout» si rapidement que l'utilisateur ne s'aperçoit plus guère que la transmission en est ralentie.

Tous les éléments de sécurité de MailGuard® sont basés sur l'utilisation de procédures cryptographiques. Pour simplifier, disons que les informations qui doivent être protégées sont complétées par des éléments de données supplémentaires et chiffrées de telle sorte que d'un côté le destinataire peut savoir qui a envoyé le message et de l'autre l'expéditeur ne peut pas en contester l'envoi. Dans les systèmes de messageries protégés, on utilise essentiellement des procédés cryptographiques symétriques et asymétriques. Des algorithmes de «hashing» entrent également en jeu, principalement pour des raisons techniques.

Procédés cryptographiques

Procédés symétriques

Les systèmes de cryptage «Conventional», «Private-Key», «One-Key» utilisent la même clé pour chiffrer et déchiffrer le message. MailGuard® utilise la norme DES (Data Encryption Standard), qui permet d'atteindre des vitesses relativement élevées de transfert de données, même sur un PC.

Procédés asymétriques

Les systèmes de cryptage «Public-Key», «Two-Key» utilisent des clés différentes pour le chiffrage et le déchiffrage. Les deux clés sont étroitement liées l'une à l'autre, mais ne peuvent pas sans autre être déduites l'une de l'autre. MailGuard® utilise la procédure RCA (Rivest-Shamir-Adleman), qui est nettement plus complexe que la méthode DES.

Procédures de «hashing»

Ces procédures servent à générer efficacement les «empreintes digitales» d'un message, sous forme de sommes de contrôle. Chiffrées, elles peuvent être ajoutées en tant que codes de «détection de manipulation», comme protection contre des modifications *intentionnelles* du message, sur le même principe que les codes de «détection d'erreurs» (par exemple le code de redondance cyclique, ou code CRC, qui sert de protection contre des modifications *aléatoires*). De tels algorithmes sont efficaces dans la mesure où seule une capacité de calcul incroyablement élevée pourrait permettre de modifier un message sans modifier en même temps les sommes de contrôle. MailGuard® utilise le procédé RIPEMD(RIPE Message Digest, un évolutif de MD4) pour le hashing.

Données de sécurité

Signatures électroniques

Ces «signatures» servent en général à garantir l'authenticité et l'intégrité de messages transmis électroniquement. La figure 1 illustre comment une telle signature est générée et testée au moyen du hashing et de la cryptographie Public Key. Il faut relever qu'il ne s'agit pas en soi de la contrepartie électronique de la signature manuelle, puisque, contrairement à celle-ci, elle n'existe qu'en association avec le document.

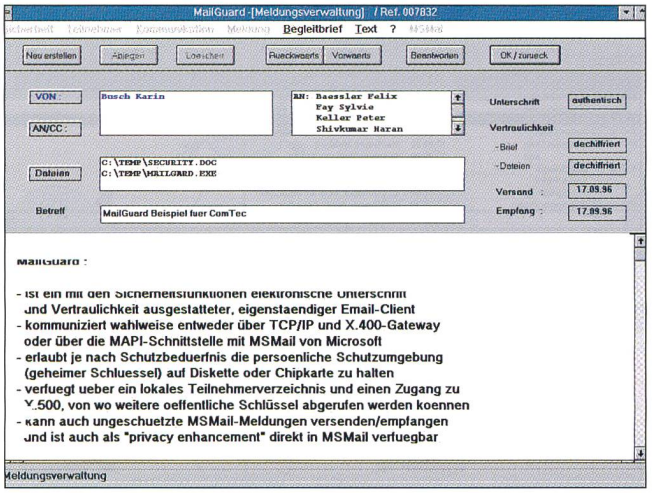

Fig. 5. Sous-fenêtre de gestion des messages: lecture d'un message.

Certificats
Les certificats contiennent essentiellement l'identité (nom, prénom, etc.) et la *clé publique* de l'expéditeur, qu'on appelle «originator certificate», ou OC en abrégé. Pour prévenir les falsifications, le lien entre les deux éléments (identité et clé) est approuvé par *l'instance de certification,* une instance reconnue digne de confiance par les deux parties, c'est-à-dire l'expéditeur et le destinataire.
Comme le montre la figure 2, les certificats sont essentiels pour les systèmes protégés, car les applications mettant en relation un nombre important d'utilisateurs inconnus les uns des autres seraient impossibles sans eux.

Environnement personnel de sécurité
Le «personal security environment», ou PSE en abrégé, contient non seulement la *clé privée individuelle* et le *certificat*, mais aussi très souvent la clé publique de l'instance de certification. Cet environnement contient ainsi tous les outils nécessaires à la génération et à la vérification de signatures électroniques. MailGuard® prévient le danger que la clé privée tombe entre des mains étrangères soit en chiffrant le PSE au moyen d'un mot de passe secret (PIN), soit en l'enregistrant en toute sécurité sur une carte à puce.

Justificatif de réception du message
Le «message token», abrégé MT, contient notamment l'identité du destinataire et la *clé DES chiffrée au moyen de la clé publique du destinataire*, clé publique qui sert au chiffrage de l'ensemble du message. Comme pour le certificat, le lien entre les deux éléments de données (identité et clé) est signé par l'expéditeur. Le MT permet ainsi au destinataire non seulement de déchiffrer le message, mais également de prouver que ce dernier lui est bien destiné.

Preuve d'authenticité du message
Le «message origin authentication check», abrégé «MOAC», représente principalement *la signature de l'ensemble du contenu du message,* produite par *l'expéditeur;* dans MailGuard®, elle se compose d'une lettre d'accompagnement et de l'ensemble des fichiers joints. Si le MOAC déchiffré (avec la clé publique de l'expéditeur) correspond à la somme de contrôle du message, il est certain que d'une part le message n'a pas été modifié anormalement en route et d'autre part qu'il provient effectivement de l'expéditeur indiqué, car seul ce dernier possède la clé privée nécessaire pour générer le MOAC.

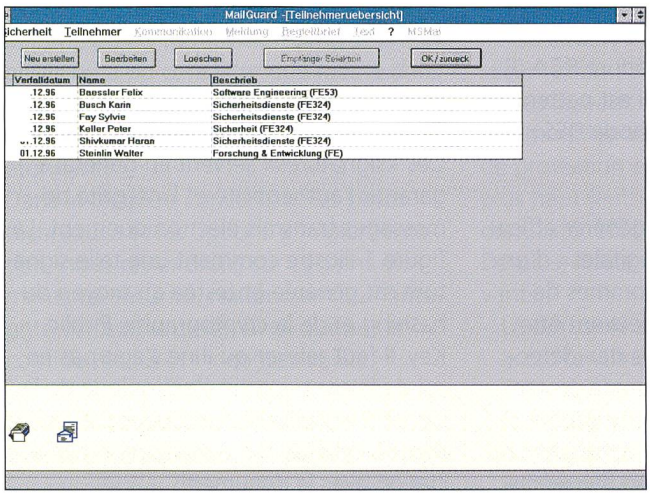

Fig. 6. Sous-fenêtre d'aperçu des utilisateurs.

Procédures d'envoi/de réception
Compte tenu des procédés cryptographiques présentés ci-dessus et des structures de données de sécurité introduites dans ce contexte (OC, MT et MOAC), les règles d'envoi et de réception (tableau 1) pour un échange de messages protégé peuvent se résumer ainsi:
La protection d'un message commence par la génération de la preuve d'authenticité (MOAC). Puis la somme de contrôle de l'ensemble du message doit être chiffrée au moyen de la clé personnelle de l'expéditeur. Lorsque l'environnement de sécurité personnel se trouve sur une carte à puce, cette étape peut être effectuée directement sur la carte si on connaît le PIN. Sinon, le PSE mémorisé dans un fichier doit d'abord être déchiffré à l'aide du PIN, afin qu'on puisse en tirer la clé privée et entreprendre le chiffrage de la somme de contrôle. L'avantage de la carte à puce est que la clé privée ne quitte jamais la carte et reste donc protégée de manière optimale. Les clés privées qui doivent provisoirement être stockées dans la mémoire du PC en clair seront irrémédiablement détruites après emploi par MailGuard® pour des raisons faciles à comprendre.
La prochaine étape consiste pour l'expéditeur à générer une clé secrète de message conforme au DES, avec laquelle il va chiffrer l'ensemble du message (lettre d'accompagnement et/ou fichiers joints). Cette clé sera ensuite elle-même chiffrée avec la clé publique du destinataire et mémorisée dans le justificatif de réception du message (MT). Enfin le MT est signé par l'expéditeur selon le processus déjà utilisé pour le MOAC. Si le même message est envoyé à plusieurs adresses, il faudra bien évidemment veiller à ce que chaque fois un nouveau MT spécifique à chaque destinataire soit préparé. Finalement, le message chiffré est envoyé avec les données de protection

MOAC, MT et OC, c'est-à-dire le certificat, qui contient la clé publique de l'expéditeur. Si le destinataire connaît déjà ce dernier, on pourrait éventuellement renoncer à joindre l'OC. Mais en règle générale, l'expéditeur ne devrait jamais compter sur le fait que sa clé publique puisse être extraite d'un annuaire (publique) (cf. X.500). En fin de compte, MailGuard® offre deux possibilités pour transmettre l'information protégée: soit la communication se fait via TCP/IP et une passerelle X.400, soit on utilise l'interface MAPI vers MSMail®.
Une fois que le message est parvenu à destination, le destinataire vérifie d'abord l'authenticité des données de protection MOAC, MT et OC. S'il survenait un problème tel que la signature électronique ne puisse pas être vérifiée (fig. 1), cela serait déjà un premier indice de simulation ou de manipulation du message.
L'étape suivante consiste à déchiffrer la clé de message incorporée dans le MT à l'aide de la clé privée du destinataire. Seul le bon destinataire du message peut mener à bien cette étape, car il est le seul à posséder la carte à puce ou le fichier PSE adéquat ainsi que le PIN nécessaire. On peut donc en conclure que durant toute la transmission entre les PC, la clé de message – et bien entendu le message lui-même – restent confidentiels aux yeux des personnes non autorisées. Pour terminer, le système soumet le message déchiffré à un test d'intégrité et d'authenticité. Pour ce faire, il doit répéter la procédure effectuée en son temps par l'expéditeur pour générer la somme de contrôle. Le destinataire utilise ensuite la clé publique de l'expéditeur, qui est contenue dans l'OC, pour déchiffrer le MOAC fourni de la même manière. Il en résulte deux sommes de contrôle, qui peuvent maintenant être comparés entre elles. Si elles sont identiques, nous pouvons être tout à fait sûrs que les importantes exigences du partenaire de communication en matière de protection et de garantie ont été satisfaites:
– Le message est arrivé sans avoir été lu (confidentialité).
– Il n'a pas été modifié en route (intégrité).
– Il a été envoyé par la bonne personne (authenticité).
– L'expéditeur ne pourra pas contester plus tard qu'il ait lui-même signé – le message (non repudiation).
– Le destinataire peut toujours prouver plus tard qu'il est bien le destinataire légitime du message, selon les informations introduites dans le MT par l'expéditeur.

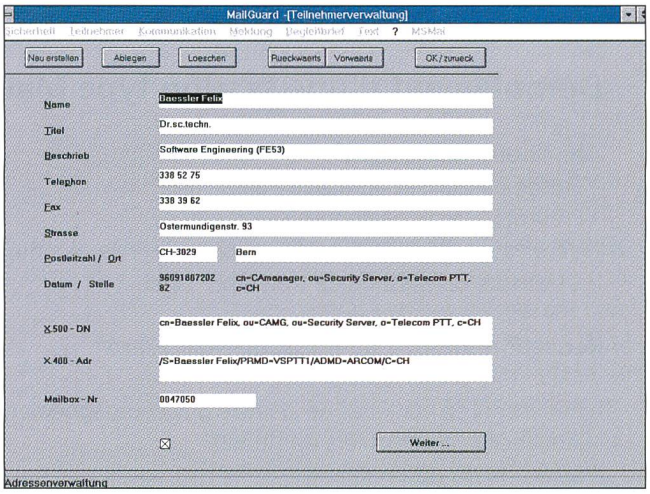

Fig. 7a. Sous-fenêtre de gestion des utilisateurs: adresses.

Conditions cadre d'organisation
Qu'entend-on généralement par instance de certification? Comment l'expéditeur peut-il se procurer la clé publique d'un partenaire de communication s'il doit prendre contact pour la première fois, par exemple? Que faire si l'on n'a plus confiance dans sa propre clé privée?

L'instance de certification
L'instance de certification (certification authority), CA en abrégé, exerce en principe la fonction d'un notaire indépendant, c'est-à-dire d'une troisième force («trusted third party») respectée par tous les partenaires de communication, qui atteste qu'une clé publique appartient à une personne connue de lui. Dans un cas simple, une telle authentification pourrait se dérouler de la manière suivante: Le client dépose une demande téléphonique ou écrite. Simplement sur la base de sa demande, on lui accorde immédiatement la possibilité de charger le MailGuard®-Software sur son PC via le réseau. Parallèlement, l'instance de certification lance tous les préparatifs nécessaires, y compris la génération d'une paire de clés privée/publique, l'élaboration d'un certificat et d'un environnement de sécurité ainsi que la personnalisation de la carte à puce du client. Lorsqu'il vient chercher la carte à puce au «bureau de délivrance du mot de passe», ce dernier doit encore justifier son identité et imprimer le PIN-code; il est alors prêt à envoyer et à recevoir des messages protégés par MailGuard®.

Répertoire des certificats
Le concept de MailGuard® prévoit que chaque utilisateur dispose localement, sur son PC, d'un répertoire des certificats de ses partenaires de communication personnels. Etant donné que les messages entrants contiennent le certificat de l'expéditeur, ce répertoire local peut

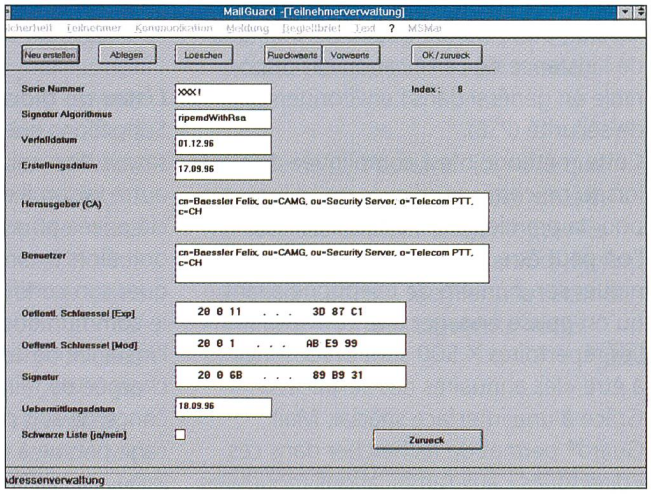

Fig. 7b. Sous-fenêtre de gestion des utilisateurs: données de sécurité.

Déroulement d'une session type MailGuard®

Annonce à MailGuard®
- Entrée du nom et du mot de passe (PIN)
- Présentation du passeport électronique
- Vérification de l'environnement personnel de sécurité
- Ouverture du masque de travail principal

Rédaction/Envoi d'un message MailGuard®
- Ouverture d'un message vide
- Rédaction de l'objet et de la lettre d'accompagnement
- Attachement de fichiers éventuels
- Sélection du destinataire
- Détermination des options de sécurité (signature/confidentialité)
- Dépôt du message préparé
- Apport de modifications éventuelles
- Protection du message et envoi

Réception/Lecture d'un message MailGuard®
- Lecture des nouveaux messages à partir de la mailbox
- Sélection d'un message dans le champ d'entrée
- Déprotection du message
- Test de l'état du message (signature/confidentialité)
- Ouverture du message
- Activation des fichiers éventuellement attachés
- Fermeture du message

Chargement (recherche/copie) d'un utilisateur MailGuard®
- Répertoire étendu des utilisateurs (local sur PC)
- Ouverture de la fenêtre d'accès à l'annuaire X.500 public
- Détermination de la base et du filtre de recherche
- Initialisation du processus de recherche
- Sélection dans la liste de résultat obtenue
- Copie des données de l'utilisateur dans le répertoire local

Tableau 2. Déroulement d'une session type MailGuard®.

être étendu et complété de manière élégante. Cela n'entraîne aucun problème de sécurité, puisque par définition les certificats sont vérifiables par chaque utilisateur, étant donné que la clé publique de l'instance de certification est disponible en général dans l'environnement de sécurité (PSE).
Cette méthode n'est compliquée que lorsqu'on correspond avec un utilisateur pour la première fois, un peu comme l'on peut être prié par lettre de communiquer son numéro de téléphone avant qu'on puisse engager une conversation. Les répertoires X.500 sont prédestinés à être «les annuaires des certificats». Grâce à une interface spécial, Mail Guard® permet de rechercher dans ces «directories» aux ramifications mondiales et de télécharger les certificats correspondants dans un répertoire local. Il en résulte une nouvelle tâche pour l'instance de certification, la publication des certificats dans le cadre du X.500.

Listes de blocage

Supposons que la carte à puce d'un utilisateur disparaisse ou que pour toute autre raison il en vienne à penser que sa clé privée pourrait ne plus être sûre. Il doit alors avoir la possibilité de faire bloquer son certificat. Le plus simple est de le communiquer de manière informelle à l'instance de certification qui est alors chargée de faire en sorte que le certificat concerné soit placé sur une liste de blocage prévue à cet effet («revocation list»).
Comme les certificats, les listes de blocages sont publiées dans le répertoire X.500. La version de MailGuard® disponible à l'heure actuelle ne permet toutefois pas encore d'en tenir compte.

Configuration de l'interface utilisateur MailGuard®

Le tableau 2 montre comment pourrait, par exemple, se dérouler une session MailGuard® typique:

Annonce à MailGuard®

Une session MailGuard® commence par l'entrée du nom d'utilisateur et du PIN correspondant à l'identification électronique introduite. Pour le support de l'environnement personnel de sécurité (PSE), on a le choix entre deux options, soit une disquette de sécurité, soit une carte à puce, sous réserve que le PC à disposition soit équipé en conséquence. Dès que le nom, le PIN et l'identification ont été entrés, MailGuard® vérifie que l'identité de l'utilisateur entrée est conforme aux informations introduites dans le PSE (sur la disquette ou sur la carte à puce). Si le test est réussi, l'écran de travail principal (fig. 3) s'ouvre devant l'utilisateur, avec les deux champs pour les messages entrants et sortants. Sur la partie gauche de ces champs, trois colonnes symbolisent les états actuels d'une communication: message, signature et confidentialité. Par exemple, deux crayons croisés représentent la signature, une clé, le chiffrage et une enveloppe fermée dans le champ de sortie, un message prêt à être envoyé. Si un message entrant présente un symbole d'erreur dans le champ d'état de la signature, comme dans le cas du message 5 dans le champ d'entrée de la figure 3, cela signifie que lors de la déprotection, la signature électronique de l'expéditeur (MOAC) n'a pas pu être vérifiée. Il faudra éclaircir de cas en cas s'il s'agit d'une méprise (p. ex. utilisation d'un certificat incompatible ou échu) ou d'une malveillance (p. ex. tentative de falsification).

Rédaction/Envoi d'un message MailGuard®

Les nouveaux messages sont rédigés de manière très semblable à MSMAIL® ou à TeamLinks®. La lettre d'accompagnement est éditée et d'éventuels fichiers additionnels sont joints au message dans la sous-fenêtre prévue à cet effet (fig. 4). La sélection des fichiers ainsi que la sélection du destinataire se font dans un

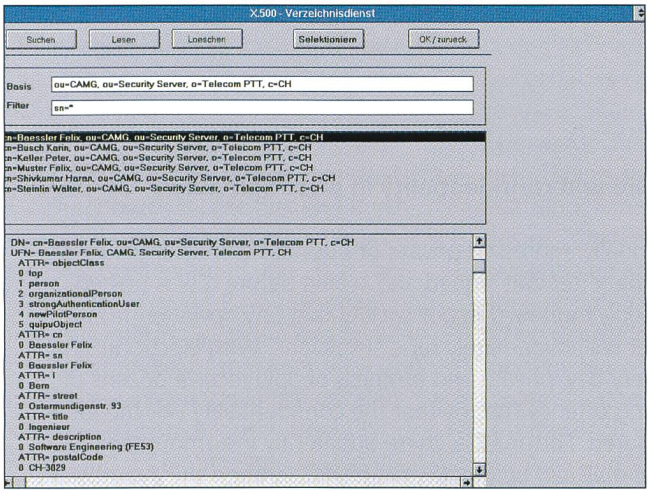

Fig. 8. Sous-fenêtre du répertoire X.500.

masque de travail séparé. A part ces opérations E-mail classiques, l'utilisateur MailGuard® peut en plus sélectionner les services de sécurité nécessaires pour sa communication: si l'on exige d'une part une signature comme option, une preuve d'authenticité sera générée lors de la protection du message (cf. bouton «enveloppe» à la figure 3); si l'on souhaite d'autre part la confidentialité, le contenu du message (lettre d'accompagnement et/ou fichiers joints) sera chiffré. Tant qu'un message se trouve dans un état non protégé, représenté par une enveloppe ouverte, l'utilisateur peut entreprendre toutes les modifications qu'il souhaite. Mais comme lorsqu'une lettre fermée, une fois que le message est protégé, c'est-à-dire signé et chiffré, il ne peut plus être modifié. Si l'utilisateur souhaite tout de même y apporter des modifications, il doit d'abord en faire une copie. Pour terminer, tous les messages protégés qui sont prêts dans le champ de sortie peuvent être expédiés à l'aide du bouton «Mailing» qu'on peut voir à la figure 3.

Réception/Lecture d'un message MailGuard®

Comme pour l'envoi, il suffit d'une seule commande à la réception pour lire tous les messages contenus dans la boîte aux lettres électronique dans le champ d'entrée de MailGuard®. On peut ensuite y sélectionner un message et le déprotéger individuellement en «ouvrant l'enveloppe». Si le contenu a été classifié comme confidentiel par l'expéditeur, il sera tout d'abord déchiffré automatiquement (lettre d'accompagnement et/ou fichiers attachés); suit – également automatiquement – la vérification de la signature, pour autant que l'expéditeur ait signé le message. Si la déprotection a pu se dérouler sans encombre, cela sera représenté par un «vu» dans les champs d'état correspondants et le message pourra alors être visualisé dans la fenêtre de la figure 5. Par mesure de sécurité, chaque processus de (dé)protection laisse derrière lui un journal du traitement, MailGuard® ayant été conçu pour que les processus puissent être répétés, ce qui peut s'avérer pratique en cas de discorde entre les partenaires de communication.

Enregistrement (recherche/copie) d'un utilisateur MailGuard®

Comme c'est habituel en messagerie électronique, MailGuard® permet également de sélectionner à l'aide de la souris le destinataire d'un message dans un répertoire d'utilisateurs. Pour les motifs exposés, un tel répertoire doit cependant, pour des produits protégés, contenir aussi le certificat des partenaires de communication en plus de leurs adresses générales. Si ce répertoire étendu est placé sur le PC de l'utilisateur (fig. 6 et 7), comme c'est le cas pour MailGuard®, des moyens doivent être mis à disposition pour pouvoir mettre à jour les données locales. Etant donné que, comme nous l'avons vu plus haut, les certificats ne peuvent être émis que par une instance de certification reconnue, deux possibilités ont été implémentées dans MailGuard®. Soit les données d'expéditeur (adresse et certificat) sont extraites d'un message reçu, soit l'utilisateur détermine le partenaire de communication recherché dans un répertoire X.500 public. Dans les deux cas, les nouvelles données sont copiées dans le répertoire local des utilisateurs, d'où elles peuvent être appelées directement pour un usage ultérieur.

L'interface utilisateur X.500 de MailGuard® reproduit à la figure 8 fait ressortir clairement la procédure suivante: Au sommet du masque de travail sont préparés la base et le filtre pour le processus de recherche. Une fois la transaction terminée, les utilisateurs qui remplissent les critères posés apparaissent dans la liste de résultat au-dessous. Si l'utilisateur recherché figure dans cette liste, ses données d'adresse et de protection peuvent être transférées dans le répertoire local d'utilisateurs MailGuard® par un simple clic sur le bouton prévu à cet effet.

Manque de produits E-mail?

Peu avant la parution du rapport final sur MailGuard® (voir rapport FE 322.066), on a pu lire dans la publication EMMS[3] du 31 octobre 1994: «The biggest problem with PEM (Privacy Enhanced Mail), I believe, is that there are not really any serious commercial products.» Bien que la situation se soit considérablement améliorée entre-temps, on peut encore se demander à l'heure actuelle pourquoi tout utilisateur final ne dispose pas encore de produits E-mail protégés. Les raisons de cet état de fait sont multiples:

- Premièrement, de tels produits sont considérés être relativement complexes, puisqu'ils doivent tenir compte d'une multitude d'interfaces (cartes à puce, cryptographie, X.400, X.500, etc.).
- Deuxièmement, les considérations de stratégie de marché jouent un rôle important, raison pour laquelle certaines entreprises renâclent à implémenter les standards internationaux spécialisés.
- Troisièmement, les produits de protection actuels continuent à n'être compatibles entre eux que dans la mesure où, à travers le monde, les lois et les infrastructures nécessaires sont harmonisées.

Et finalement, il apparaît ici ou là que même à l'époque actuelle des virus informatiques et du piratage, toutes les entreprises et tous les utilisateurs ne sont pas encore prêts à sacrifier à la sécurité en faisant les investissements nécessaires. 9.4

[3] Electronic Mail and Messaging Systems (EMMS).