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

Herausgeber: Swisscom

Band: 74 (1996)

Heft: 12

Artikel: Vertrauen ist gut, Kontrolle ist besser

Autor: Baessler, Felix

DOI: https://doi.org/10.5169/seals-876807

MAILGUARD®[1]: UNTERSCHRIFT UND VERTRAULICHKEIT IM ELEKTRONISCHEN MELDUNGSVERKEHR

VERTRAUEN IST GUT, KONTROLLE IST BESSER

Dieser Beitrag wendet sich an technisch interessierte Leser, die mit elektronischen Meldungssystemen, sogenannten «E-mail»-Systemen, arbeiten, sei es als Benutzer oder als Betreiber. Behandelt werden zu Beginn die grundlegenden Funktionen, die allgemein notwendig sind, um Meldungssysteme zu sichern; anschliessend wird anhand eines eigens entwickelten Prototyps auf die Gestaltung der entsprechenden Benutzerschnittstellen eingegangen.

FELIX BAESSLER, BERN

Erhalten wir von der Post einen persönlich adressierten privaten oder geschäftlichen Brief, erachten wir es als selbstverständlich, dass dieser unterzeichnet und verschlossen aufgegeben wurde. Diese «Tradition» ist so tief in unserem gesellschaftlichen Leben verankert, dass ein allfällig abweichendes Verhalten seitens eines Absenders unweigerlich Befremdung hervorruft.

Nicht so bei der elektronischen Post! Hier erhalten täglich Privat- wie auch Geschäftsleute Dutzende von Mitteilungen, ohne sich daran zu stören, dass weder Vertraulichkeit noch die Identität der Verfasser sichergestellt sind. Offenbar haben sich viele von uns – bewusst oder unbewusst – damit abgefunden, dass die heute üblichen elektronischen Meldungssysteme im allgemeinen grosse Sicherheitslücken aufweisen. Dieser Zustand dürfte nicht zuletzt deshalb einigermassen erträglich sein, weil für wirklich wichtige Meldungen nach wie vor auf die traditionelle «gute alte Post» zurückgegriffen werden kann.

Tatsächlich zirkuliert heute die elektronische Post in den meisten Fällen ungesichert sowohl in den öffentlichen wie auch in den privaten Netzen. Erwähnen wir zur Illustration nur ein Beispiel von vielen:

In einschlägigen Kreisen ist es seit langem kein Geheimnis mehr, dass im Internet bereits mit wenig Fachwissen Absenderadressen, ja sogar ganze Leitpfadvermerke gefälscht werden können. Eine suspekte, über Internet erhaltene Aufforderung in Form einer Bestellung, Einladung, Auftragserteilung usw. sollte daher unbedingt über einen anderen Kanal, beispielsweise telefonisch, bestätigt werden, wenn man nicht Gefahr laufen will, einem schlechten Scherz oder, schlimmer, einer kriminellen Handlung zum Opfer zu fallen!

Glücklicherweise können die angesprochenen, scheinbar so unüberwindbaren Sicherheitsrisiken der elektronischen Post mit den heute zur Verfügung stehenden technischen Mitteln auf ein Minimum reduziert werden. Etwas vereinfachend ausgedrückt, können Benutzer von einem sicheren elektronischen Meldungssystem dieselben Qualitäts- und Garantiemerkmale erwarten, wie wir uns das von der konventionellen Post seit jeher gewohnt sind. So kann der Empfänger einer gesicherten elektronischen Nachricht insbesondere jederzeit die Identität des Verfassers/Absenders anhand der elektronischen Unterschrift[2] überprüfen, und auch die Vertraulichkeit der Nachricht kann mittels Chiffrierung sichergestellt werden.

Ein Pilotversuch mit dem in der Direktion Forschung und Entwicklung mit Sicherheitsfunktionen ausgestatteten E-mail-System «MailGuard®» hat in der Praxis gezeigt, dass die Anforderungen an die Benutzer bezüglich Bedienung derart gering gehalten werden können, dass sie keinesfalls ein Hindernis darstellen, um gesicherte Produkte künftig in grossem Massstab, firmenintern oder im Rahmen eines öffentlichen Dienstes, einzusetzen.

[1] Registered trademark by Swiss Telecom PTT.

[2] Die elektronische Unterschrift (Bild 1) ist nicht zu verwechseln mit einer digitalisierten Unterschrift, bei der das Schriftbild optisch abgetastet und als Punktmenge in einer Datei abgespeichert wird.

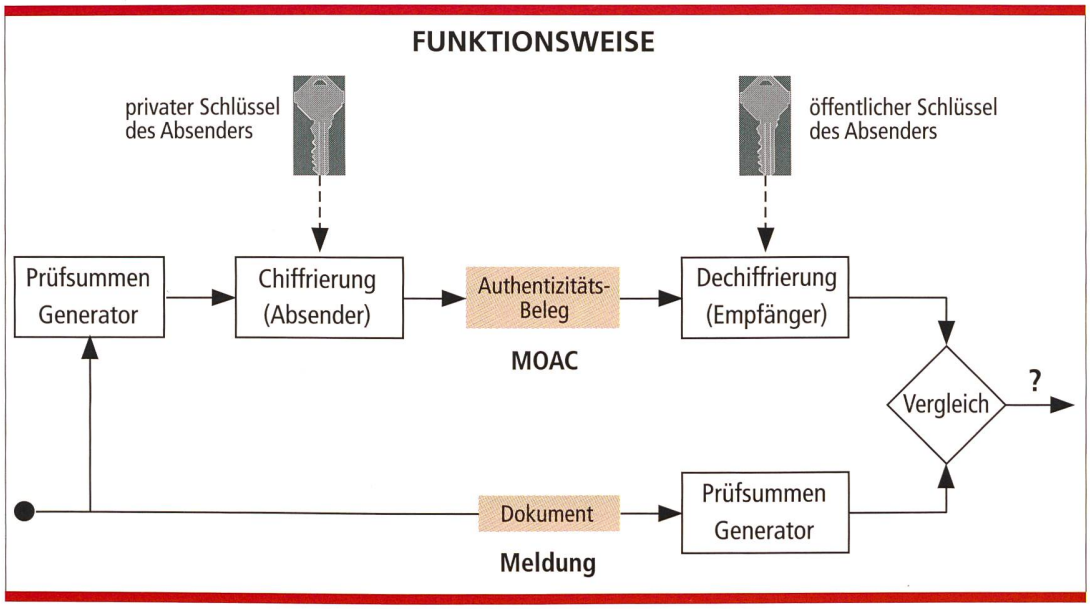


Bild 1. Funktionsweise von elektronischen Unterschriften.

Historische Entwicklung des Meldungsaustauschs

Die grundlegenden Anforderungen von Absender und Empfänger an ein auf Papier beruhendes Meldungssystem umfassen:

- Identifikation des Absenders der Meldung/Transaktion
- Verifikation der Identität des Verfassers/Absenders
- Sicherstellen, dass gesendete und empfangene Meldung/Transaktion identisch sind, ohne zufällige oder beabsichtigte Modifikation
- Beweiserbringung, dass der Meldungsaustausch bzw. die Transaktion tatsächlich stattgefunden hat
- Geheimhaltung des Inhalts der Meldung/Transaktion gegenüber unbefugten Dritten
- Verfügbarkeit der Infrastruktur des zugrundeliegenden Kommunikationssystems

Über Jahrtausende hat sich mittlerweile die Abwicklung des Schriftverkehrs zu einer äusserst stabilen sozialen Konvention etabliert, mit der wir alle von Kindheit auf vertraut gemacht werden und die wir meist ohne zu hinterfragen als «einfach gegeben» akzeptieren.
Diese von alters her überlieferten Regeln, die sich offenkundig aus einem allseitigen Sicherheits- bzw. Garantiebedürfnis heraus entwickelt haben, dienen als Grundlage für die Behandlung der analogen Anforderungen im Rahmen des elektronischen Meldungsverkehrs.

Sicherheitsdienste in der Telekommunikation

In der Telekommunikation werden die Sicherheitsdienste von den internationalen Gremien ISO (International Organization for Standardization) und ECMA (European Computer Manufacturers Association) eingehend und sehr detailliert behandelt. Im Grunde geht es jedoch um dieselben Kriterien bzw. Bedrohungen, wie sie uns vom papierbasierten System her allgemein vertraut sind.

Identifikation/Maskeraden
Der Absender gibt sich in der Regel durch Angabe von Name und/oder Titel zu erkennen. Bei kommerziellen Transaktionen dienen oft vorgedruckte Firmenlogos der Identifikation des Unternehmens.

Authentizität/Fälschung von Unterschriften
Handgeschriebene Unterschriften bilden das verbreitetste Mittel zur Authentifizierung eines Individuums. Die früher verwendeten Siegel sind heute üblicherweise den Notariatsdiensten vorbehalten. Diese haben als unabhängige dritte Kraft («trusted third party») eine wichtige Funktion inne, auch bei den modernen elektronischen Systemen.

Integrität/Modifikation von Nachrichten
Tinte in Verbindung mit speziellem Papier, das Manipulationen sichtbar machen kann, wurden entwickelt, um die (Fälschungs-)Beständigkeit von Dokumenten sicherzustellen.

Unabstreitbarkeit (Nonrepudiation)/ Leugnen von Nachrichten
Um vorzubeugen, dass einmal eingegangene Verpflichtungen später geleugnet werden können, wurden Verfahren zur Verifikation von Unterschriften eingeführt. Bei Unstimmigkeiten können unabhängige Instanzen als Schiedsgericht beigezogen werden.

Vertraulichkeit/Mitlesen von Nachrichten
Physische Schutzmassnahmen wie Verschliessen und Versiegeln lassen Dritte erkennen, dass der Inhalt einer Mitteilung privaten Charakter hat. Die im elektronischen Bereich eine wichtige Rolle spielende Kryptographie war lange Zeit vorwiegend militärischen/nachrichtendienstlichen Anwendungen vorbehalten.

Verfügbarkeit/Nachrichtenverlust bzw. Dienstausfälle
Die von Natur aus dezentrale Struktur des Postnetzes bürgte in der Vergan-

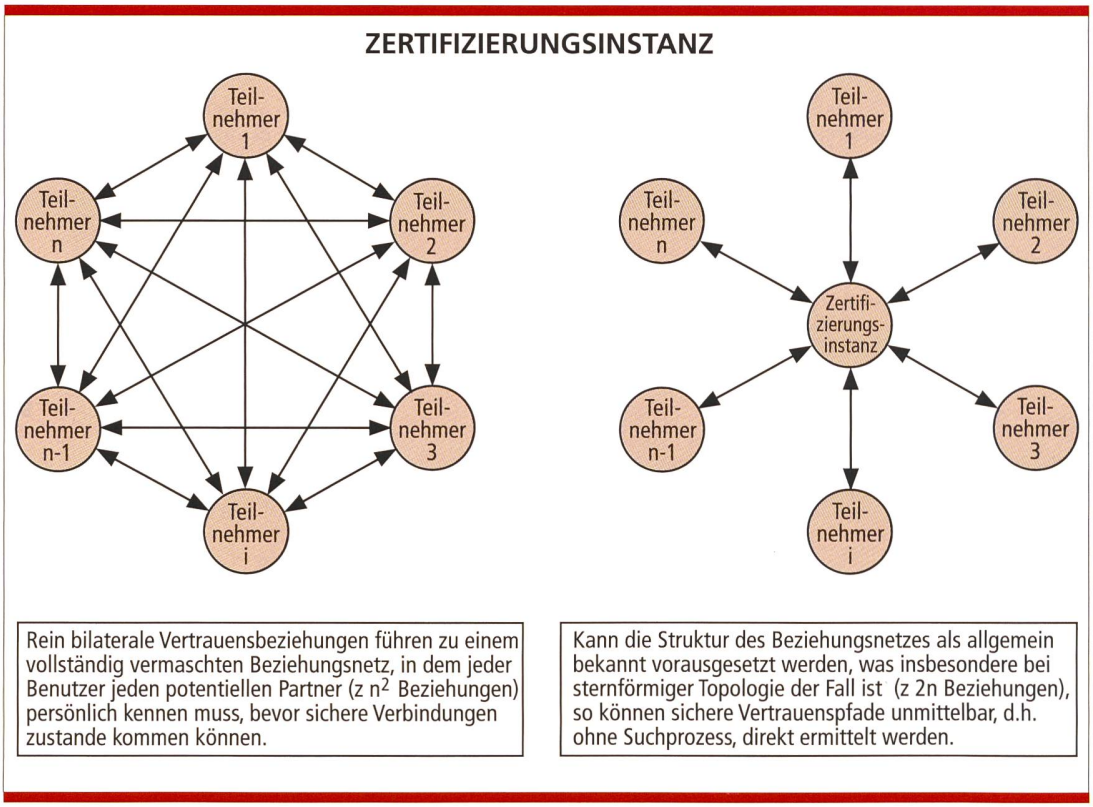


Bild 2. Rolle der Zertifizierungsinstanz bei grossen Teilnehmerpopulationen.

genheit für dessen Robustheit gegen höhere Gewalt, Vandalismus oder Bombenterror. Immer wieder hat es sich gezeigt, dass auch in extremen Ausnahmesituationen dieser Dienst erstaunlich gut aufrechterhalten werden kann.
Insbesondere auf die Sicherheitselemente Integrität und Authentizität sowie Vertraulichkeit und Unabstreitbarkeit werden wir im Kapitel technische Grundlagen und Implementationsoptionen zurückkommen.

Aktuelles Markt- und Schutz-/Garantiebedürfnis

Die Gründe, die dazu führen, dass Privat- und Geschäftskorrespondenz vermehrt auf elektronischem Weg geführt werden, sind leicht auszumachen:
- kürzere Übermittlungsdauer (nahezu distanzunabhängig)
- reduzierte Gesamtkosten (insbesondere bei Berücksichtigung des sogenannten «Handlings»)
- verbesserte Integration von Generierung, Übermittlung und Entgegennahme von Nachrichten (Kompatibilitätsaspekt)
- effizientere Archivierung (Datenbanken)

Bei der gegenwärtigen rasanten Migration von papierbasiertem Betrieb in Richtung elektronischen Meldungsaustausch darf jedoch nicht vergessen werden, dass damit verbunden gleichzeitig auch das Sicherheitsrisiko markant zunimmt, denn der direkte Zugriff zu On-line-Informationen über Datennetze erleichtert natürlich Angriffe gegen die eingangs diskutierten Bedürfnisse nach Schutz und Garantien in Form von Authentizität, Integrität, Vertraulichkeit usw.
Hinzu kommt,
- dass mit der Verbreitung der PCs die Verwundbarkeit des elektronischen Meldungsaustauschs massiv zugenommen hat. Denn im Vergleich zu früher, wo in relativ wenigen Rechenzentren nur eine überblickbare Anzahl von Mitarbeitern Zugang zum Telekommunikationsbereich hatte, kann sich heute unkontrolliert und weitgehend anonym praktisch jedermann als «Hacker« betätigen.
- dass elektronische Vermittlungssysteme Kopien von Nachrichten an Umschlagplätzen hinterlassen können, ohne dass der Absender oder der Empfänger davon in Kenntnis gesetzt wird. Auch Nachforschungen in diesem Bereich gelten als schwierig, da nicht einmal immer bekannt ist, über welche Netzknoten eine Nachricht geführt wurde.
- dass gewisse Textverarbeitungssysteme, anstatt wirklich zu löschen, die betreffenden Passagen gewissermassen nur unsichtbar machen, also weder vollständig eliminieren noch überschreiben. Man kann sich leicht vorstellen, dass es beim Austausch solcher Dateien – übrigens auch mittels Diskette – zu mehr als nur unangenehmen Situationen kommen kann.

Der zuletzt erwähnte Punkt weist auf eine manchmal unterschätzte generelle Schwachstelle der elektronischen Verfahren hin. Konnte nämlich beim papierbasierten Betrieb der Verfasser/Absender noch konkret feststellen, was er in einen Briefumschlag steckte, so sind wir jetzt im elektronischen Zeitalter darauf angewiesen, dass die verwendeten Text-, Editier- und Mail-Programme tatsächlich so arbeiten, wie wir das von ihnen erwarten. Im Zusammenhang mit der elektronischen Unterschrift gewinnt die skizzierte Situation sogar merklich an Brisanz, denn hier kann ja nicht mehr wirklich

Sende- und Empfangsprozeduren bei gesichertem Meldungsaustausch

Absenderprozedur	Empfängerprozedur
1. Ermitteln der Prüfsumme (Fingerabdruck, Hashwert) der Meldung	1. Empfangen der gesicherten Nachricht
2. Unterschreiben der Prüfsumme, durch Chiffrieren mit dem privaten Schlüssel des Absenders	2. Prüfen der Authentizität der Sicherheitsdaten durch Dechiffrieren der Unterschriften von OC, MT, MOAC mit dem öffentlichen Schlüssel der Zertifizierungsinstanz (OC) bzw. des Absenders (MT, MOAC)
3. Abspeichern der so gewonnenen Daten ins MOAC	3. Dechiffrieren des im MT enthaltenen Meldungsschlüssels mit dem privaten Schlüssel des Empfängers
4. Erzeugen eines geheimen DES-Meldungsschlüssels	4. Dechiffrieren der Meldung mit dem zurückgewonnenen Meldungsschlüssel
5. Chiffrieren der Meldung mit dem erzeugten Meldungsschlüssel	5. Ermitteln der empfängerseitigen Prüfsumme der zurückgewonnenen Meldung
6. Chiffrieren des Meldungsschlüssels mit dem öffentlichen Schlüssel des Empfängers	6. Dechiffrieren der im MOAC enthaltenen absenderseitigen Prüfsumme
7. Abspeichern der so gewonnenen Daten ins MT	7. Testen der beiden Prüfsummen auf Übereinstimmung
8. Unterschreiben des MT (inkl. Identität des Empfängers) durch Chiffrieren mit dem privaten Schlüssel des Absenders	
9. Zusammenstellen der gesicherten Nachricht, bestehend aus chiffrierter Meldung und Sicherheitsdaten OC, MT, MOAC	
10. Versenden der gesicherten Nachricht	

Tabelle 1. Sende- und Empfangsprozeduren bei gesichertem Meldungsaustausch. Sicherheitsdatenstrukturen OC (Originator Certificate), MT (Message Token), MOAC (Message Origin Authentication Check).

überblickt werden, was man eigentlich unterschreibt. Waren wir früher gewohnt, Seite für Seite zu paraphieren, bevor ein wichtiges Dokument abschliessend unterzeichnet wurde, müssen wir heute unser Augenmerk darauf richten, dass insbesondere im Sicherheitsbereich nachweisbar vertrauenswürdige Software zum Einsatz kommt.

Technische Grundlagen und Implementationsoptionen

Es mag vielleicht erstaunen, dass die meisten grundlegenden Prinzipien, die heute zur Sicherung elektronischer Meldungen eingesetzt werden, schon vor Jahrzehnten bekannt und auch weitgehend öffentlich verfügbar waren. Enorm zugenommen haben hingegen in jüngerer Zeit einerseits das bereits erwähnte Schutz-/Garantiebedürfnis der Benutzer und anderseits natürlich ganz besonders auch die am Arbeitsplatz verfügbare Rechenleistung. Die massiv gesteigerte Kapazität der PCs erlaubt es inzwischen, die für die Sicherung benötigten «End-zu-End»-Verfahren so schnell abwickeln zu lassen, dass die damit verbundene zusätzliche Verarbeitungsdauer vom Benutzer kaum mehr wahrgenommen wird.

Alle Sicherheitselemente von MailGuard® basieren auf dem Einsatz von kryptographischen Verfahren. Vereinfachend gesagt, werden dabei die zu schützenden Nachrichten durch zusätzliche Datenelemente derart ergänzt und chiffriert, dass sowohl der Empfänger daraus ableiten kann, wer die Mitteilung versandt hat, als auch umgekehrt der Absender nicht in Abrede stellen kann, dass tatsächlich er es war, der die betreffende Meldung versandt hat.

Bei gesicherten Meldungssystemen verwendet man grundsätzlich symmetrische und asymmetrische kryptographische Verfahren. Zusätzlich gelangen – hauptsächlich aus leistungstechnischen Gründen – die sogenannten Hashing-Algorithmen zum Einsatz. Da diese Verfahren zusammen mit den zugehörigen Sicherheitsdatenstrukturen im Beitrag Peter M. Keller, Seite 15 im Detail diskutiert werden, beschränken wir uns hier auf eine Zusammenfassung.

Kryptographische Verfahren

Symmetrische Verfahren

«Conventional», «Private-key»-, «One-key»-Kryptosysteme benützen denselben Schlüssel zur Chiffrierung und Dechiffrierung der Nachricht. MailGuard® verwendet das DES-Verfahren (Data Encryption Standard), mit dem selbst auf einem PC relativ hohe Durchsatzraten erreicht werden können.

Asymmetrische Verfahren

«Public-key»-, «Two-key»-Kryptosysteme benützen verschiedene Schlüssel für Chiffrierung und Dechiffrierung. Beide Schlüssel stehen in enger Beziehung zueinander, können aber nicht ohne weiteres voneinander abgeleitet werden. MailGuard® verwendet das RSA-(Rivest-Shamir-Adleman-)Verfahren, das im Vergleich zu DES wesentlich aufwendiger ist.

Hashing-Verfahren

Diese dienen der effizienten Erzeugung eines «fingerprints» einer Nachricht, das heisst eines Fingerabdrucks in der Art von Prüfsummen. Chiffriert können sie als «Manipulation-detection»-Codes zur Sicherung gegen *absichtliche* Modifikationen der Meldung beigefügt werden, ähnlich wie «Error-detection»-Codes (beispielsweise «cyclic redundancy check» gegen *zufällige* Modifikationen einge-

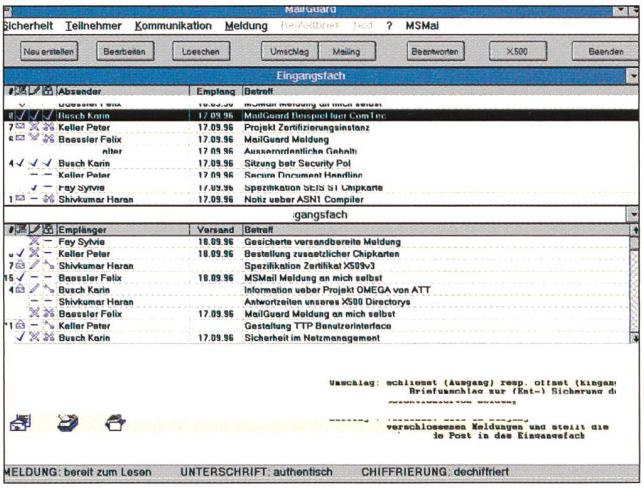


Bild 3. Hauptfenster von MailGuard® mit Ein-/Ausgangsfach.

setzt werden. Voraussetzung für die Wirksamkeit solcher Algorithmen ist, dass es nur mit unrealistisch hohem Rechenaufwand möglich ist, eine Nachricht zu modifizieren, ohne gleichzeitig deren Prüfsumme zu verändern. MailGuard® verwendet fürs Hashing das RIPEMD-Verfahren (RIPE Message Digest, eine Weiterentwicklung von MD4).

Sicherheitsdaten

Elektronische Unterschriften

«Signatures» dienen generell zur Sicherstellung von Authentizität und Integrität von elektronisch übermittelten Nachrichten. Bild 1 illustriert, wie solche Signaturen mittels Hashing und Public-Key-Kryptographie erzeugt sowie geprüft werden. Beachtenswert ist, dass im Gegensatz zur manuellen Unterschrift das elektronische Gegenstück an sich gar nicht existiert, da hier ja nur das Paar Urkunde/Signatur Sinn machen kann.

Zertifikate

Diese enthalten im wesentlichen die Identität (Name, Adresse usw.) und den *öffentlichen Schlüssel* des Absenders: «originator certificate», abgekürzt OC. Um Fälschungen vorzubeugen, wird die Verknüpfung beider Elemente (Identität und Schlüssel) von einer beidseitig, das heisst vom Absender und Empfänger, als vertrauenswürdig anerkannten Instanz der *Zertifizierungsinstanz* unterschrieben. Wie Bild 2 veranschaulicht, bilden Zertifikate eine wichtige Voraussetzung für gesicherte Systeme, da sie Anwendungen mit grossen, offenen Teilnehmerpopulationen erst eigentlich ermöglichen.

Persönliche Sicherheitsumgebung

«Personel security environment», abgekürzt PSE, enthält neben dem *eigenen privaten Schlüssel* und *Zertifikat* meist auch den öffentlichen Schlüssel der Zertifizierungsinstanz. Damit enthält diese Umgebung alle notwendigen Mittel, um elektronische Unterschriften zu erzeugen und zu verifizieren. Der Gefahr, dass der private Schlüssel in fremde Hände gerät, wird in MailGuard® dadurch begegnet, dass das PSE entweder mit einem geheimen Passwort (PIN) chiffriert oder auf einer Chipkarte sicher abgelegt wird.

Meldungsnachweis

«Message token», abgekürzt MT, umfasst insbesondere die *Identität* des Empfängers und den mit dem öffentlichen Schlüssel des *Empfängers chiffrierten DES-Schlüssel,* mit dem die Gesamtmeldung chiffriert wird. Ähnlich wie beim Zertifikat ist die Verbindung beider Datenelemente (Identität und Schlüssel) vom Absender unterschrieben. Dadurch setzt der MT den Empfänger nicht nur in die Lage, die betreffende Meldung zu dechiffrieren, sondern es ermöglicht ihm auch nachzuweisen, dass er tatsächlich der rechtmässige Adressat ist.

Meldungsauthentizitätsbeleg

«Message origin authentication check», abgekürzt MOAC, repräsentiert in erster Linie die vom *Absender* erzeugte *Unterschrift des gesamten Meldungsinhalts,* bei MailGuard® bestehend aus Begleitbrief einschliesslich sämtlicher beigefügter Dateien. Stimmt der (mit dem öffentlichen Schlüssel des Absenders) dechiffrierte MOAC mit der Prüfsumme der Nachricht überein, besteht Gewissheit, dass erstens die Mitteilung unterwegs nicht unrechtmässig modifiziert wurde und zweitens tatsächlich vom angegebenen Absender stammt, denn nur dieser besitzt ja den für die Erzeugung des MOAC benötigten privaten Schlüssel.

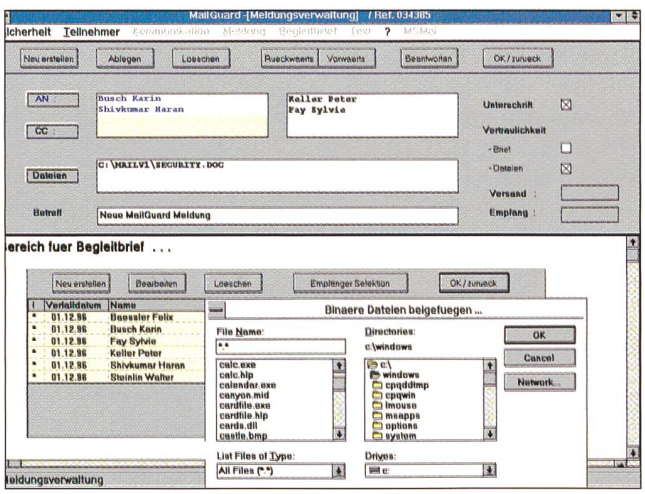


Bild 4. Unterfenster Meldungsverwaltung: Verfassen einer Meldung.

Sende-/Empfangsprozeduren

Auf der Grundlage der vorgestellten kryptographischen Verfahren und der in diesem Zusammenhang eingeführten Sicherheitsdatenstrukturen OC, MT und MOAC können die Sende- und Empfangsregeln (Tabelle 1) für gesicherten Meldungsaustausch wie folgt zusammengefasst werden:

Die Sicherung einer Meldung beginnt mit dem Bilden des Authentizitätsbelegs (MOAC). Dazu muss die Prüfsumme der Gesamtmeldung mit dem privaten Schlüssel des Senders chiffriert werden. Befindet sich die persönliche Sicherheitsumgebung auf einer Chipkarte, kann dieser Vorgang bei bekanntem PIN direkt auf der Karte durchgeführt werden. Andernfalls muss zuerst das in einer Datei abgespeicherte PSE mittels PIN dechiffriert werden, damit der private Schlüssel entnommen und die Chiffrierung der Prüfsumme vorgenommen werden kann. Der Vorteil der Chipkarte liegt darin, dass der private Schlüssel niemals die Karte verlässt und dadurch optimal geschützt bleibt. Private Schlüssel, die vorübergehend als Klartext im Speicher des PC abgelegt werden müssen, werden bei MailGuard® aus naheliegenden Gründen nach Gebrauch durch Überschreiben unwiderruflich vernichtet.

Der nächste Schritt des Senders besteht darin, einen DES-konformen geheimen Meldungsschlüssel zu generieren, mit dem die gesamte Meldung (Begleitbrief und/oder beigefügte Dateien) chiffriert wird. Danach wird dieser Schlüssel selbst mit dem öffentlichen Schlüssel des Empfängers chiffriert und im Meldungsnachweis (MT) abgespeichert. Schliesslich wird der MT nach demselben wie beim MOAC verwendeten Vorgehen ebenfalls vom Absender unterschrieben. Ist dieselbe Meldung an mehrere Adressaten gerichtet, so ist zu beachten, dass natürlich jedesmal ein neuer, empfängerspezifischer MT bereitgestellt werden muss.

Versandt wird schliesslich die chiffrierte Meldung zusammen mit den Sicherheitsdaten MOAC, MT und OC, dem Zertifikat, das den öffentlichen Schlüssel des Absenders enthält. Falls dieser dem Empfänger bereits bekannt ist, könnte allenfalls auf das Beifügen des OC verzichtet werden. In der Regel sollte sich aber der Sender nicht darauf verlassen, dass sein öffentlicher Schlüssel einem (öffentlichen) Verzeichnis entnommen werden kann (vgl. X.500). Schliesslich stehen bei MailGuard® für die eigentliche Übermittlung der gesicherten Nachricht zwei Möglichkeiten zur Verfügung: Entweder erfolgt die Telekommunikation über TCP/IP und einen X.400-Gateway, oder es kommt die MAPI-Schnittstelle zu MSMail® zur Anwendung.

Ist die gesicherte Nachricht am Bestimmungsort eingetroffen, überprüft der Empfänger zuerst einmal die Sicherheitsdaten MOAC, MT und OC auf Authentizität. Sollte dabei ein Problem auftreten in der Art, dass eine elektronische Unterschrift nicht verifiziert werden kann (Bild 1), so ist dies bereits ein erstes Indiz, dass die Meldung fingiert oder manipuliert sein könnte.

Im nächsten Schritt gilt es, mit Hilfe des privaten Schlüssels des Empfängers den im MT untergebrachten Meldungsschlüssel zu dechiffrieren. Dieser Schritt kann offenkundig ausschliesslich vom rechtmässigen Empfänger der Nachricht mit Erfolg durchgeführt werden, denn nur dieser verfügt über die passende Chipkarte bzw. PSE-Datei sowie den benötigten PIN. Demzufolge kann davon ausgegangen werden, dass der Meldungsschlüssel – und damit auch die Meldung – während der ganzen Übertragung zwischen den PCs für Unbefugte geheim bleibt.

Zum Abschluss wird die dechiffrierte Meldung einem Integritäts-/Authentizitätstest unterzogen. Dazu muss zunächst die seinerzeit vom Absender durchgeführte Prozedur zur Erzeugung der Prüfsumme wiederholt werden. Dann verwendet der Empfänger den öffentlichen Schlüssel des Absenders, der ja im OC enthalten ist, um den ebenfalls mitgelieferten MOAC zu dechiffrieren. Als Resultat ergeben sich zwei Prüfsummen, die jetzt mit-

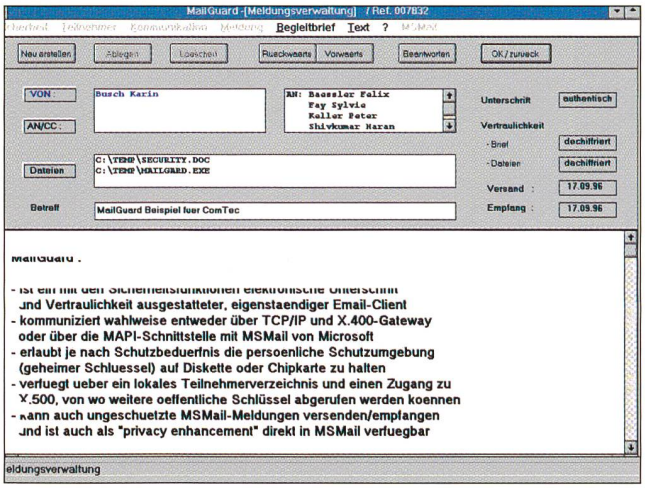
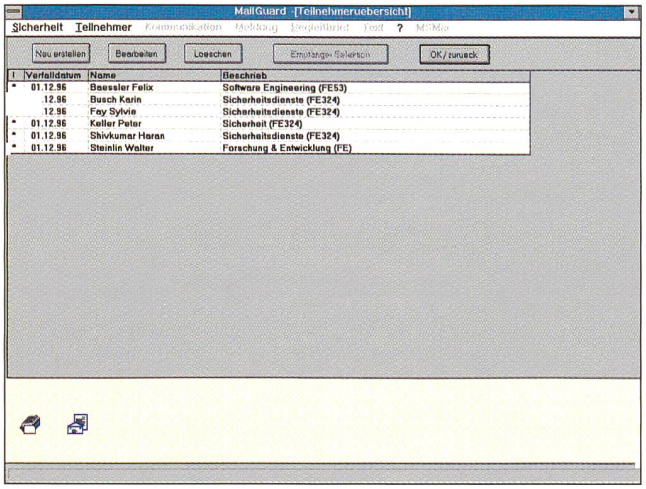


Bild 5. Unterfenster Meldungsverwaltung: Lesen einer Meldung.



Bil. 6. Unterfenster Teilnehmerübersicht.

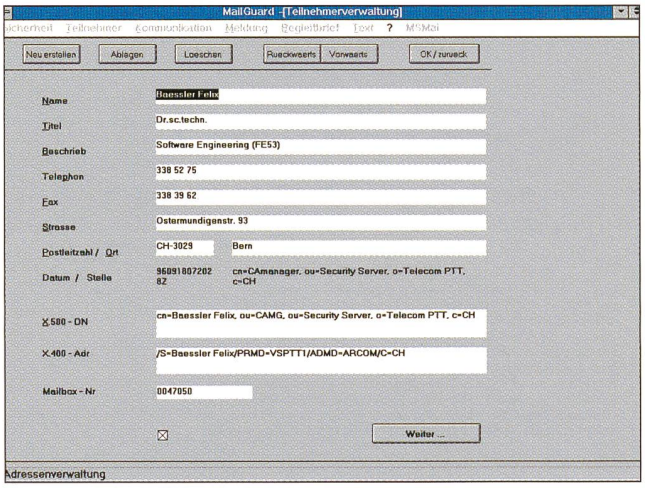


Bild 7a. Unterfenster Teilnehmerverwaltung: Adressdaten.

einander verglichen werden können. Sind die beiden identisch, so können wir insgesamt weitgehend sicher sein, dass wichtige Schutz- und Garantiebedürfnisse der Kommunikationspartner erfüllt sind:

- Die Nachricht kam ungelesen an (Vertraulichkeit).
- Sie wurde unterwegs nicht modifiziert (Integrität).
- Sie wurde von der richtigen Person gesendet (Authentizität).
- Der Absender kann später nicht in Abrede stellen, dass er selbst die Mitteilung unterschrieben hat (Nonrepudiation).
- Der Empfänger kann später immer nachweisen, dass er der rechtmässige – vom Absender im MT eingesetzte – Adressat der Mitteilung ist.

Organisatorische Rahmenbedingungen

Was soll man sich generell unter einer Zertifizierungsinstanz vorstellen? Wie kann sich der Absender den öffentlichen Schlüssel eines Kommunikationspartners beschaffen, wenn beispielsweise zum erstenmal Kontakt aufgenommen werden soll? Was kann unternommen werden, wenn einmal das Vertrauen in den eigenen privaten Schlüssel erlöschen sollte?

Zertifizierungsinstanz

Die Zertifizierungsinstanz «certification authority», abgekürzt CA, hat im Prinzip die Funktion eines unabhängigen Notars, das heisst einer von allen Kommunikationspartnern respektierten dritten Kraft («trusted third party»), welche beurkundet, dass ein öffentlicher Schlüssel zu einer ihr bekannten Person gehört. Eine solche Beurkundung könnte sich in einem einfachen Fall wie folgt abspielen:
Der Kunde stellt telefonisch oder schriftlich einen Antrag. Bereits aufgrund des Antrags wird ihm sofort ermöglicht, die MailGuard®-Software über das Netz auf seinen PC zu laden. Gleichzeitig leitet die Zertifizierungsinstanz alle notwendigen Vorbereitungen ein, einschliesslich Generieren des privaten/öffentlichen Schlüsselpaars, Bilden von Zertifikat und Sicherheitsumgebung sowie Personalisieren der Chipkarte des Kunden. Beim Abholen der Chipkarte auf der «Passausgabestelle» muss dieser sich dann nur noch ausweisen sowie den PIN-Code einprägen, und bereits ist er in der Lage, gesicherte MailGuard®-Meldungen zu versenden und zu empfangen.

Zertifikatsverzeichnis

Das Konzept von MailGuard® sieht vor, dass jeder Teilnehmer lokal in seinem PC über ein Verzeichnis der Zertifikate seiner persönlichen Kommmunikationspartner verfügt. Da eingehende Meldungen das Zertifikat des Absenders mitführen, kann dieses lokale Verzeichnis auf elegante Weise erweitert und nachgeführt werden. Sicherheitsprobleme sind damit keine verbunden, denn Zertifikate sind ja per Definition von jedem Teilnehmer verifizierbar, da der öffentliche Schlüssel der Zertifizierungsinstanz im allgemeinen in der Sicherheitsumgebung (PSE) zur Verfügung steht.
Umständlich wird diese Methode erst, wenn mit einem Teilnehmer zum erstenmal korrespondiert werden soll, ungefähr so, wie wenn man zuerst brieflich aufgefordert wird, seine Telefonnummer bekanntzugeben, bevor ein Gespräch geführt werden kann. Prädestiniert als «Telefonbuch der Zertifikate» sind die X.500-Verzeichnisse. Mit einer besonderen Schnittstelle erlaubt MailGuard®, in diesen weltweit vernetzten Directories zu suchen und entsprechende Zertifikate ins lokale Verzeichnis zu übernehmen. Für die Zertifizierungsinstanz ergibt sich dadurch natürlich eine neue Aufgabe,

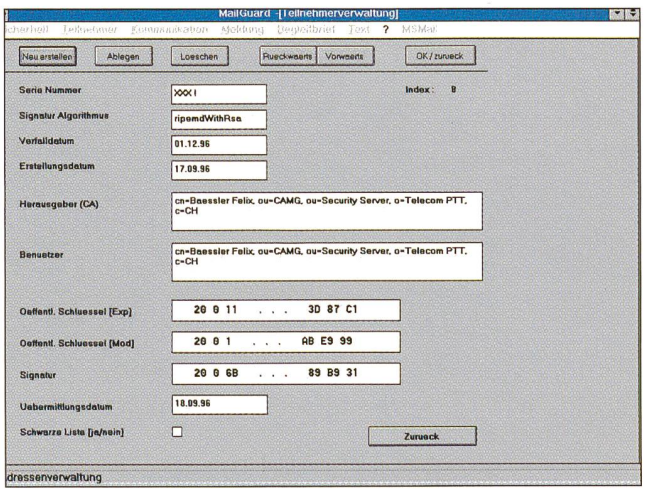


Bild 7b. Unterfenster Teilnehmerverwaltung: Sicherheitsdaten.

nämlich die Publikation der Zertifikate im Rahmen von X.500.

Sperrlisten

Nehmen wir an, dass einem Teilnehmer die Chipkarte abhanden kommt oder dass er aus einem anderen Grund Anlass hat zu vermuten, dass sein privater Schlüssel nicht mehr sicher sein könnte. Dann muss er die Möglichkeit haben, sein Zertifikat sperren zu lassen. In der einfachsten Form genügt dazu eine informelle Mitteilung an die Zertifizierungsinstanz, welche dann dafür besorgt ist, dass das betreffende Zertifikat auf die für solche Fälle vorgesehene Sperrliste, «revocation list», gesetzt wird.
Wie die Zertifikate werden auch die Sperrlisten im X.500-Verzeichnis veröffentlicht; allerdings können diese in der heute vorliegenden Version von MailGuard® noch nicht berücksichtigt werden.

Gestaltung der MailGuard® Benutzerschnittstelle

Eine typische Sitzung mit MailGuard® könnte, wie in Tabelle 2 angedeutet, beispielsweise folgendermassen ablaufen:

Anmeldung bei MailGuard®

Eine MailGuard®-Sitzung beginnt mit der Eingabe von Benutzername und dem zum eingesetzten elektronischen Ausweis passenden PIN. Als Träger der persönlichen Sicherheitsumgebung (PSE) kann als Option wahlweise entweder eine Sicherheitsdiskette oder eine Chipkarte verwendet werden, vorausgesetzt, dass der zur Verfügung stehende PC entsprechend ausgerüstet ist. Sobald Name, PIN und Ausweis eingegeben sind, stellt MailGuard® sicher, dass die angegebene Identität des Benutzers mit der im PSE (auf der Diskette oder der Chipkarte) eingetragenen Information übereinstimmt. Ist diese Prüfung bestanden, öffnet sich dem Benutzer die Hauptarbeitsfläche entsprechend Bild 3 mit den beiden Fächern für ankommende und abgehende Meldungen. Auffallend an den beiden Fächern sind die drei Kolonnen links im Bild, welche den aktuellen Meldungs-, Unterschrifts- und Vertraulichkeitsstatus einer Mitteilung symbolisieren. Zum Beispiel stehen gekreuzte Griffel für Unterschrieben, ein Schlüssel für Chiffrieren, und ein geschlossener Briefumschlag im Ausgangsfach würde eine versandbereite Meldung markieren. Weist eine ankommende Meldung im Statusfeld der Unterschrift ein Falschzeichen auf, wie etwa im Fall von Meldung 5 im Eingangsfach von Bild 3, so bedeutet dies, dass bei der Entsicherung die elektronische Unterschrift des Absenders (MOAC) nicht verifiziert werden konnte. Ob es sich dabei um ein Versehen (z. B. Verwendung eines inkompatiblen oder verfallenen Zertifikats) oder um ein Vergehen (z. B. Versuch einer Maskerade) handelt, muss von Fall zu Fall abgeklärt werden.

Verfassen/Senden einer MailGuard®-Meldung

Neue Meldungen werden auf sehr ähnliche Weise wie in MSMail® oder TeamLinks® abgefasst. Im für diesen Zweck vorgesehenen Unterfenster von Bild 4 werden der Begleitbrief editiert und allenfalls zusätzlich Dateien zur Meldung hinzugefügt. Die Auswahl der Dateien wird ebenso wie die Auswahl der Empfänger in einer separaten Arbeitsfläche vorgenommen. Über diese klassischen E-mail-Operationen hinaus kann jetzt aber der MailGuard®-Benutzer zusätzlich die für die Mitteilung erforderlichen Sicherheitsdienste anwählen: Wird als Option einerseits eine Unterschrift verlangt, so wird beim Sichern der Meldung (vgl. Schaltfläche «Umschlag» in Bild 3) ein Authentizitätsbeleg erzeugt; ist anderseits Vertraulichkeit erwünscht, so wird der Meldungsinhalt (Begleitbrief und/oder beigefügte Dateien) chiffriert. Solange sich eine Meldung im ungesicherten, durch einen offenen Umschlag repräsentierten Zustand befindet, kann der Benutzer nach Belieben Modifikationen vornehmen. Analog wie bei einem verschlossenen Brief kann aber eine einmal gesicherte, das heisst unterschriebene und chiffrierte Meldung nicht mehr modifiziert werden. Möchte der Benutzer dennoch Änderungen anbringen, so muss er sich zuerst eine Kopie der betreffenden Mitteilung anlegen lassen, in der er dann die Modifikationen anbringen kann. Schliesslich können mittels Schaltfläche «Mailing» in Bild 3 alle

Ablauf einer typischen MailGuard®-Sitzung

Anmeldung bei MailGuard®

- Eingabe von Name und Passwort (PIN)
- Präsentation des elektronischen Ausweises
- Überprüfung der persönlichen Sicherheitsumgebung
- Öffnen der Hauptarbeitsfläche

Verfassen/Senden einer MailGuard®-Meldung

- Öffnen einer leeren Meldung
- Verfassen von Betreff und Begleitbrief
- Beifügen allfälliger Dateien
- Selektionieren der Empfänger
- Setzen der Sicherheitsoptionen (Unterschrift/Vertraulichkeit)
- Ablegen der vorbereiteten Meldung
- Anbringen von allfälligen Modifikationen
- Sichern der Meldung und Versand

Empfang/Lesen einer MailGuard®-Meldung

- Einlesen der neuen Meldungen aus der Mailbox
- Selektion einer Meldung im Eingangsfach
- Entsichern der Meldung
- Prüfen des Meldungsstatus (Unterschrift/Vertraulichkeit)
- Öffnen der Meldung
- Aktivieren allfälliger beigefügter Dateien
- Schliessen der Meldung

Aufnahme (Suchen/Kopieren) eines MailGuard®-Teilnehmers

- Erweitertes Teilnehmerverzeichnis (lokal im PC)
- Öffnen des Fensters zum öffentlichen X.500-Directory
- Setzen von Basis und Suchfilter
- Initialisieren des Suchprozesses
- Selektion in der erhaltenen Resultatliste
- Kopieren der Teilnehmerdaten ins lokale Verzeichnis

Tabelle 2.
Ablauf einer typischen MailGuard®-Sitzung.

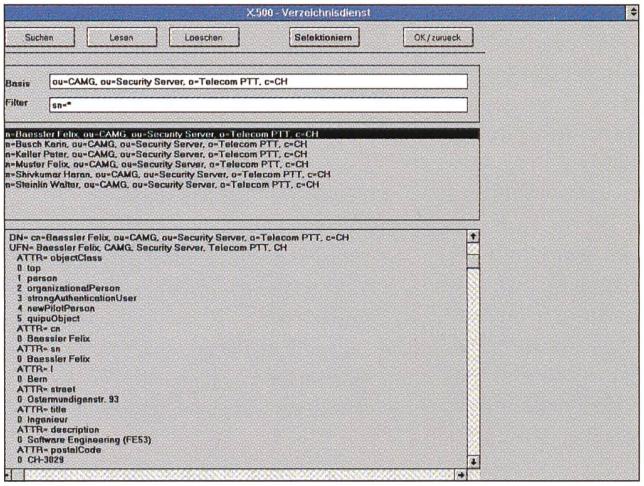


Bild 8. Unterfenster X.500-Verzeichnis.

gesicherten, im Ausgangsfach bereitstehenden Meldungen versandt werden.

Empfang/Lesen einer MailGuard®-Meldung

Wie beim Versand genügt auch beim Empfang ein einziger Befehl, um sämtliche Meldungen aus dem elektronischen Briefkasten in das Eingangsfach von MailGuard® einzulesen. Hier kann dann eine Meldung ausgewählt und wiederum durch «Umschlag» individuell entsichert werden. Wurde der Inhalt vom Absender als vertraulich eingestuft, so wird in einem ersten Schritt automatisch dechiffriert (Begleitbrief und/oder beigefügte Dateien); dann folgt – ebenfalls automatisch – die Überprüfung der Unterschrift, sofern der Absender die Meldung unterzeichnet hat. Konnte die Entsicherung ohne Zwischenfälle vollzogen werden, wird dies in den betreffenden Statusfeldern mit einem Gutzeichen protokolliert, und die Meldung kann sodann im Fenster von Bild 5 eingesehen werden. Zur Sicherheit hinterlässt jeder (Ent-)Sicherungsvorgang ein Verarbeitungslog, wobei MailGuard® so konzipiert wurde, dass die Prozesse wiederholt werden können, was sich bei Uneinigkeit zwischen den Kommunikationspartern als vorteilhaft erweisen kann.

Aufnahme (Suchen/Kopieren) eines MailGuard®-Teilnehmers

Wie üblich beim elektronischen Meldungsaustausch, werden auch bei MailGuard® die Empfänger einer Nachricht mit Hilfe der Maus in einem Teilnehmerverzeichnis selektioniert. Aus den dargelegten Gründen muss jedoch ein solches Verzeichnis bei gesicherten Produkten neben den allgemeinen Adressdaten der Kommunikationspartner zusätzlich auch deren Zertifikat enthalten. Ist dieses erweiterte Verzeichnis, wie im Falle von MailGuard®, im PC des Benutzers untergebracht (Bilder 6 und 7), so müssen Mittel zur Verfügung stehen, die erlauben, dass die lokalen Daten nachgeführt werden können. Unter Berücksichtigung der erläuterten Vorschrift, dass Zertifikate ausschliesslich von einer anerkannten Zertifizierungsinstanz herausgegeben werden dürfen, wurden in MailGuard® zwei Möglichkeiten implementiert. Entweder werden die Absenderdaten (Adresse und Zertifikat) einer erhaltenen Meldung entnommen, oder der Benutzer ermittelt den gesuchten Kommunikationspartner in einem öffentlichen X.500-Directory. In beiden Fällen werden die neuen Daten ins lokale Teilnehmerverzeichnis kopiert, wo sie für den weiteren Gebrauch direkt abgerufen werden können.
Die in Bild 8 wiedergegebene X.500-Benutzerschnittstelle von MailGuard® lässt folgendes Vorgehen erkennen: Im Kopf der Arbeitsfläche werden die Basis und der Filter für den Suchprozess vorbereitet. Die Teilnehmer, welche die gestellten Kriterien erfüllen, erscheinen nach Abschluss der Transaktion in der darunterliegenden Resultatliste. Enthält einer der gefundenen Einträge den gesuchten Teilnehmer, so können dessen Adress- und Sicherheitsdaten über die dazu vorgesehene Schaltfläche per Mausklick ins lokale MailGuard®-Teilnehmerverzeichnis transferiert werden.

Fehlende E-mail-Produkte?

Kurz vor dem Erscheinen des Schlussberichts über MailGuard® (vgl. F+E-Bericht 322.066) war in der EMMS[3]-Ausgabe vom 31. Oktober 1994 zu lesen: *«The biggest problem with PEM (Privacy Enhanced Mail), I believe, is that there are not really any serious commercial products.»* Obwohl sich die Situation in der Zwischenzeit merklich verbessert hat, kann man sich auch heute noch fragen, weshalb gesicherte E-mail-Produkte noch immer nicht jedem Endbenutzer zur Verfügung stehen. Die Gründe dafür sind wohl durch mehrere Faktoren bedingt:

- Erstens werden solche Produkte als relativ komplex eingestuft, da eine Vielzahl von Schnittstellen berücksichtigt werden müssen (Chipkarten, Kryptographie, X.400, X.500 usw.).
- Zweitens spielen wohl auch marktstrategische Überlegungen eine Rolle, weshalb die einschlägigen internationalen Standards von einigen Unternehmen nur ungern implementiert werden.
- Drittens sind die heutigen Sicherheitsprodukte immer noch nur insoweit zueinander kompatibel, als weltweit die benötigten Gesetze und Infrastrukturen aufeinander abgestimmt sind.
- Und schliesslich macht es hier und da den Anschein, dass auch in der heutigen Zeit der Computerviren und der Hacker noch nicht jedes Unternehmen bzw. jeder Anwender bereit ist, die für Sicherheit benötigten Mehrinvestitionen aufzubringen.

9.4

[3] Electronic Mail and Messaging Systems (EMMS)

Felix Baessler, schloss sein Studium an der ETH Zürich mit dem Diplom als dipl. El.-Ing. ETH ab. Am Imperial College in London, Department of Computing Science, absolvierte er ein Nachdiplomstudium (Msc). An der EPU Lausanne, Département des mathématiques, erwarb er mit seiner Dissertation den Titel eines Dr. sec. techn. Von 1974 bis 1978 war er im Battelle-Forschungslabor in Genf, Gruppe für angewandte Mathematik und Informatik, tätig. Seit 1978 ist Felix Baessler in der Direktion Forschung und Entwicklung der Telecom PTT und beschäftigt sich schwergewichtig mit Informatiklösungen im Bereich Sicherheit, insbesondere elektronische Post und Verwaltung/Verzeichnis von öffentlichen Schlüsseln.

SUMMARY

MailGuard®: signature and confidentiality in electronic mail

When we receive personally addressed private or business correspondence we take for granted that the letter was signed and sealed before it was posted. This 'tradition' is so deeply ingrained in our society that any deviation from this norm by the sender will immediately raise suspicions. With electronic mail this is not the case! Every day, private and business people receive dozens of messages without taking offence that neither the confidentiality nor the identity of the sender is assured. Fortunately, these apparently insurmountable security risks in electronic mail can be greatly minimized through the available technology. This report addresses technically interested readers who work with electronic message systems, so-called 'E-mail' systems, be it as users or as network operators. The discussion starts with the basic functions that are generally necessary to make message systems safe and continues with a corresponding user interface based on the design of prototypes developed in-house.