



Vertraulichkeit für E-Mail-Systeme

Vertraulichkeit für E-Mails

Warum E-Mails verschlüsseln oder signieren?

Das Internet ist ein freiwilliger Zusammenschluss von vielen Teilnetzen und wird im wesentlichen von ca. 7 Mio. sogenannten "Hosts" (= Knotenrechnern mit Standleitungsverbindungen) getragen. In der Regel passiert eine E-Mail-Nachricht auf ihrem Weg vom Absender zum Empfänger mehrere solche Knotenrechner.

Dabei ist es möglich, dass eine Nachricht von jemandem, der einen Internet-Host betreibt, abgehört und/oder verfälscht werden kann.

Dieses Risiko lässt sich mit modernen kryptographischen Verfahren vermeiden. Durch **Verschlüsselung** kann dafür gesorgt werden, dass nur der vorgesehene Empfänger eine Nachricht lesen bzw. verstehen kann, und durch **Authentisierung** mittels elektronischer Signatur lässt sich verifizieren, ob eine E-Mail auch tatsächlich von dem angegebenen Absender stammt.

Wie funktionieren Verschlüsselung und Signatur?

In der Frühzeit der Kryptographie benutzte man zum Ver- und Entschlüsseln noch geheim gehaltene Verfahren. Die moderne Kryptographie verwendet hingegen Verfahren, die nicht mehr geheim gehalten werden müssen, sondern so gestaltet sind, dass ihre Sicherheit von einer (sehr großen) geheim gehaltenen Zufallszahl abhängt, dem sogenannten "Schlüssel" (= der normalerweise als lange Zeichenfolge dargestellt wird).

Dabei gibt es 2 Techniken:

Bei konventioneller (= **symmetrischer**) Verschlüsselung wird eine Nachricht mit Hilfe eines geheimen Schlüssels so "durcheinandergewürfelt", dass sie nur durch erneute Anwendung des *gleichen* Schlüssels wieder lesbar gemacht werden kann. Kennt außer dem Absender und dem Empfänger einer Nachricht niemand den geheimen Schlüssel, so lassen sich auf diese Weise auch über einen unsicheren Kanal wie das Internet vertrauliche Nachrichten geschützt übermitteln. Diese Art der Verschlüsselung erfordert jedoch, dass der geheime Schlüssel vorher auf einem "sicheren" Weg (z. B. durch einen persönlichen Kurier) zwischen den Kommunikationspartnern ausgetauscht wurde. Das ist insbesondere dann unpraktisch, wenn die Anzahl der Kommunikationspartner steigt, mit denen ein "sicherer" Nachrichtenaustausch gewünscht wird.

Bei der für E-Mails üblichen **asymmetrischen** Verschlüsselung wird daher mit einem Schlüsselpaar gearbeitet. Diese beiden Schlüssel sind derart gestaltet, dass eine Nachricht, die mit dem einen Schlüssel kodiert wurde, anschließend nicht mit demselben Schlüssel, sondern nur mit seinem Gegenspieler entschlüsselt werden kann. Einer der beiden Schlüssel dieses Pairs wird streng geheim gehalten ("privater Schlüssel"), während der zweite Schlüssel ("öffentlicher Schlüssel") publik gemacht werden darf.

Mit diesem öffentlichen Schlüssel können dann andere dem Schlüsselinhaber verschlüsselte Nachrichten senden, die nur er lesen kann, da nur er den zugehörigen privaten Schlüssel kennt. (Mehr zur asymmetrischen Verschlüsselung und zum Umgang mit Schlüsseln siehe "<http://www.komforttext.de/signatur/intro.htm>".)

Über die asymmetrische Verschlüsselung lassen sich E-Mails auch **signieren**. Dazu lässt der Absender eine Art "Quersumme" des E-Mail-Inhalts errechnen und verschlüsselt diese mit seinem privaten Schlüssel. Der Empfänger kann dann mit Hilfe des öffentlichen Schlüssels des Absenders die "Quersumme" entschlüsseln und somit verifizieren, dass die vorliegende E-Mail auch tatsächlich von dem angegebenen Absender stammt und der Inhalt unverfälscht übermittelt wurde.

Wer oder was ist "PGP"?

Das erste Programm, das starke kryptographische Verfahren auf der Basis von asymmetrischer Verschlüsselung der breiten Öffentlichkeit zugänglich machte, war PGP ("Pretty Good Privacy"), das im Jahr 1991 erschien. Da das Programm frei im Internet (inkl. Quellcode) publiziert wurde, mauserte es sich binnen weniger Jahre zum de-facto-Standard für Verschlüsselung von E-Mails. 1998 wurde das "Open PGP Message Format" schließlich zum offiziellen Internet-Standard, der nun unabhängig von einem bestimmten Produkt ist (und mittlerweile von vielen Herstellern unterstützt wird).

Welcher Aufwand entsteht im Alltag durch Verschlüsselung/Signatur von E-Mail?

Da i. d. R. lediglich die Verbindungsstrecke außer Haus, d. h. vom Mailserver des Absenders zum Mailserver des Empfängers, gesichert werden muss, bietet sich der Einsatz einer automatisierten Ver- und Entschlüsselung an.

Diese kann, z. B. in Form des KT-Mail/Krypto-Gateways, zentral beim Mailserver-PC einer Firma installiert werden. Dadurch lässt sich eine verschlüsselte Verbindung zu Geschäftspartnern ohne jeglichen Zusatzaufwand für die Anwender erreichen.

Worin liegen die Vorteile des KT-Mail/Krypto-Gateways?

Das Krypto-Gateway garantiert verschlüsselte und signierte Verbindungen zwischen Geschäftspartnern ohne irgendeinen Zusatzaufwand für die Anwender. Auf Wunsch können ausgewählte E-Mail-Verbindungen auch so konfiguriert werden, dass eine E-Mail nur bei Bedarf (wenn der Anwender einen entsprechenden Zeichencode in der Betreff-Zeile der E-Mail eingibt) verschlüsselt werden. Das ist dann sinnvoll, wenn ein Geschäftspartner verschlüsselte E-Mails auf seinem System noch manuell entschlüsseln muss.

In der Umkehrrichtung werden eingehende E-Mails, die verschlüsselt oder elektronisch signiert sind, vollautomatisch entschlüsselt bzw. verifiziert und in entschlüsselter Form an den jeweiligen Arbeitsplatz geleitet. Somit entsteht auch bei eingehenden verschlüsselten E-Mails keinerlei Zusatzaufwand für den Anwender.

Auf diese Weise können vertrauliche E-Mails geschützt und abhörsichere Verbindungen zwischen verschiedenen Niederlassungen, Stadtverwaltungen, Geschäftspartnern u. ä. aufgebaut werden. Behörden können mit dem KT-Mail/Krypto-Gateway für ihre Bürger einen sicheren Kommunikationskanal schaffen, der allen Vorgaben der Landesdatenschutzbeauftragten für E-Mails mit personenbezogenen Daten genügt.

Im Unterschied zu anderen Lösungen, die ebenfalls "starke kryptographische Verfahren" einsetzen, benötigt das KT-Mail/Krypto-Gateway weder spezielle Hard- oder Software an den einzelnen Arbeitsplätzen noch eine besondere Schulung der Mitarbeiter. Lediglich der Mail-Administrator muss über Grundkenntnisse der Verschlüsselung und des Schlüsselmanagements verfügen (die er sich z. B. über das PGP-Tutorial auf unserer Website aneignen kann - siehe "<http://www.komforttext.de/signatur/index.htm#tutor>").

Was sind die Voraussetzungen für das KT-Mail/Krypto-Gateway?

Für das Krypto-Gateway gelten dieselben Voraussetzungen wie beim KT-Mail/Filter-Gateway, d. h. es kann jedem E-Mail-System hinzugefügt werden, das gegenüber dem Internet das SMTP-Protokoll verwendet, und erfordert keinerlei Änderungen an den Arbeitsplatz-PCs oder der dort installierten Software. An Betriebssystemen werden Windows (9x/ME/NT/2000/XP) und Linux unterstützt.

Ist bereits ein KT-Mail/Filter-Gateway installiert, so kann die Krypto-Gateway-Software auf diesem PC einfach als Zusatz hinzugefügt werden. Soll das Krypto-Gateway auf einem eigenen PC laufen, reicht dazu (bei normalem Mail-Aufkommen) auch ein Rechner älteren Datums.

Was kostet das KT-Mail/Krypto-Gateway?

Das KT-Mail/Krypto-Gateway besteht aus einem SMTP-Basis-Gateway (495 EUR) und dem eigentlichen Krypto-Gateway-Modul (745 EUR), so dass sich für die obige Lösung ein Gesamtpreis von 1240 EUR zzgl. MWSt ergibt. (Ist bereits ein KT-Mail/Filter-Gateway installiert, so entfallen die Kosten für das SMTP-Basis-Gateway, und es fallen lediglich 745 EUR zzgl. MWSt für die automatisierte Ver- und Entschlüsselung von E-Mails an.)

Die durchschnittliche Installations- und Konfigurationszeit für ein Krypto-Gateway durch uns bzw. unsere Systempartner beträgt ca. 3-4 Stunden vor Ort. Dazu kommt die Einweisung für den Mail-Administrator in das Schlüsselmanagement, für die - je nach Vorkenntnissen des Administrators - ca. 1-2 Stunden eingeplant werden sollten.

Laufende Wartungskosten für das Gateway fallen keine an. In Anspruch genommene Leistungen unseres technischen Supports berechnen wir mit 1,50 EUR/Minute (= 90 Euro/Std) + MWSt.

Die Eckdaten des KT-Mail/Krypto-Gateways im Überblick:

- automatische Ver-/Entschlüsselung/Signatur von E-Mails, dadurch keinerlei Zusatzaufwand der Anwender für das Ver- und Entschlüsseln von E-Mails
- Unterstützung des de-facto-Standards für Mail-Verschlüsselung ("OpenPGP"-Format nach den Internet-Standards RFC 2440 und RFC 3156), zusätzliche Unterstützung von S/MIME in Vorbereitung
- Schlüsselmanagement zentral durch den Mail-Administrator, dadurch keine Schulung der Endbenutzer erforderlich
- durch zentrale Ver-/Entschlüsselung werden Fehlermöglichkeiten der Endbenutzer (beim Verschlüsseln oder beim Schlüsselmanagement) oder ein Ausspionieren der Schlüssel an den Arbeitsplatz-PCs zuverlässig ausgeschlossen
- firmenweite Schlüssel können mit Abteilungsschlüsseln oder persönlichen Schlüsseln einzelner Anwender kombiniert werden
- bei Bedarf auch optionales Verschlüsseln (über einen Zusatz in der Betreff-Zeile der E-Mail) für bestimmte Empfänger einstellbar, um bei nur gelegentlichem Schutzbedarf einem E-Mail-Partner, der noch manuell entschlüsseln muss, keine unnötige Arbeit aufzubürden
- Kompatibilität mit allen verbreiteten Verschlüsselungslösungen auf PGP-Basis getestet