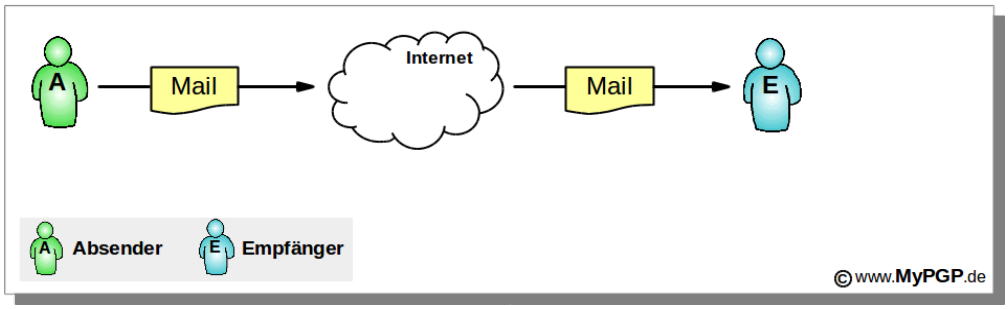
Einführung in die eMail-Verschlüsselung

(Klassische) eMails sind nicht sicher

eMails (elektronische Nachrichten) - oder kurz Mails - werden über das Internet verschickt: ein Absender (A) erstellt eine Textnachricht (evtl. mit Anhängen) und benutzt sein Mail-Programm für das Versenden der Textnachricht an den Empfänger (E) durch das Internet.

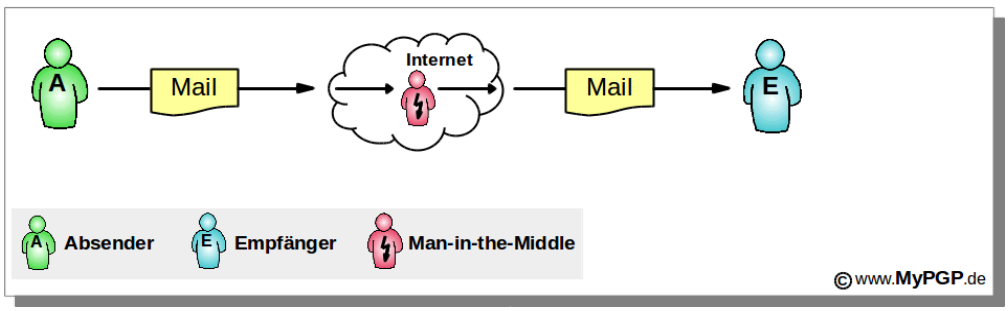


Im Internet wird die Mail über verschiedene (Computer-)Server bis zum Empfänger weitergeleitet. Jeder Server liest die Mail, um zu wissen, wohin die Mail weiterversendet werden soll. Nicht immer wird der direkte Weg zwischen Absender und Empfänger genommen.

In der Regel werden nur die Verbindungsdaten der Mail (z.B. die Empfängeradresse) für die Weiterversendung gelesen; es kann aber nicht ausgeschlossen werden, dass auch die Inhalte gelesen werden. Eine klassische Mail ist damit wie eine Postkarte, die jeder, der die Postkarte in Händen hält, lesen kann.

Anders als Postkarten können Mails ohne nennenswerten Aufwand kopiert und damit auch später gelesen und ausgewertet werden. Sie können sehr einfach geändert werden, ohne dass der Empfänger dies bemerken wird. **Klassische Mails sind daher sehr viel unsicherer als Postkarten.**

Man-in-the-Middle



(Computer-)Server und damit Personen, die sich in die Kommunikation zwischen Absender und Empfänger zum Mitlesen der Mails "einschmuggeln", werden im Fachjargon **Man-in-the-Middle** ("Mann in der Mitte") genannt.

Der Man-in-the-Middle könnte nicht nur Mails mitlesen, sondern könnte sie auch verändern, ohne dass der Empfänger die Manipulation entdecken könnte.

Transportverschlüsselung

Das Mitlesen und Manipulieren ließe sich durch eine Transportverschlüsselung verhindern. Serverbetreiber verschlüsseln die Daten beim Transport innerhalb des Internets. Die Verschlüsselung ist um so wirksamer je früher sie beginnt und je später sie endet.

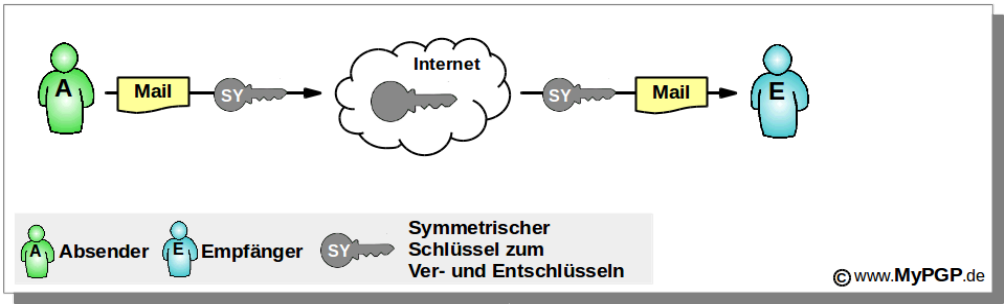
Bleibt das Problem, dass die Transportverschlüsselung weder vom Absender noch vom Empfänger kontrolliert werden kann und dass insbesondere Geheimdienste im Verdacht stehen, sich sogenannte Backdoors (Hintertüren) von den Serverbetreibern einrichten zu lassen.

Effiziente Verschlüsselung ohne Kosten

Eine garantiert sichere Mail-Übertragung ist letztlich nur möglich, wenn der Absender die Mail selbst verschlüsselt und der Empfänger die Mail selbst entschlüsselt.

Es gibt seit den 1990-er-Jahren hoch effiziente, zudem kostenfreie Verfahren, mit denen eine solche Ver-/Entschlüsselung einfach zu realisieren ist. Selbst Geheimdienste sind aktuell nicht in der Lage, diese Verschlüsselung in angemessener Zeit zu "knacken". Geheimdienste werden daher in der Regel nicht die Verschlüsselung selbst angreifen, sondern versuchen, die Computer der Absender und Empfänger auszuspähen.

Die folgende Abbildung zeigt, wie ein Absender seine Mail verschlüsselt und der Empfänger die verschlüsselte Mail wieder entschlüsselt.

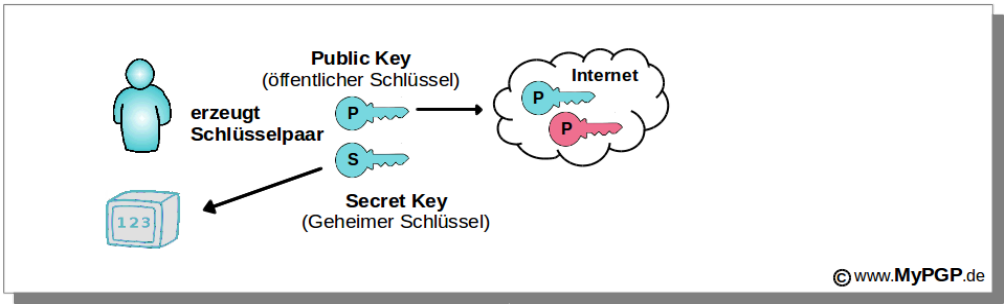


Der Absender und der Empfänger verwendet zum Ver- bzw. Entschlüsseln den selben Schlüssel (SY). Ein Schlüssel, mit dem ver- und entschlüsselt wird, heißt **symmetrischer Schlüssel**.

In der Praxis stellt sich das Problem, dass ein symmetrischer Schlüssel sowohl dem Absender als auch dem Empfänger bekannt sein muss. Den Schlüssel über das Internet zu versenden wäre fahrlässig, weil er dort von eimem Man-in-the-Middle abgefangen werden könnte.

Asymmetrischer Schlüssel

Es gibt seit Anfang der 1990-er-Jahre asymmetrische Schlüssel, die dieses Problem beheben. Ein asymmetrischer Schlüssel besteht aus zwei Schlüsseln, die gemeinsam ein Schlüsselpaar bilden.



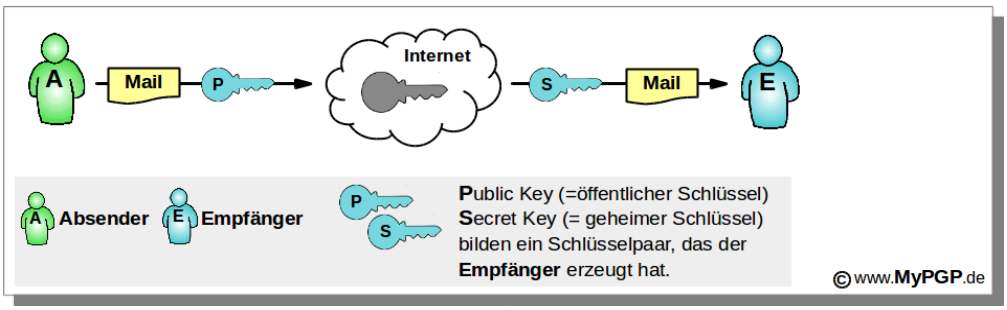
Ein Schlüsselpaar besteht aus einem öffentlichen Schlüssel (engl. public key) und einem geheimen Schlüssel, der auch privater Schlüssel genannt wird (engl. secret key = private key).

Mit dem öffentlichen Schlüssel wird eine Mail verschlüsselt, die dann nur mit dem geheimen Schlüssel wieder entschlüsselt werden kann. Der öffentliche Schlüssel heißt "öffentlich", weil er öffentlich (auch im Internet) bekannt gegeben werden kann. Der geheime Schlüssel bleibt **immer** geheim und ist nur dem Schlüsselpaar-Erzeuger bekannt. Er gehört also in einen Tresor (wenn er nicht immer wieder für das Entschlüsseln benutzt werden müßte).

Der rote Schlüssel in der Internetwolke soll andeuten, dass es im Internet viele öffentliche Schlüssel geben wird. Später in diesem Dokument werden wir beschreiben, was bei der Suche nach dem richtigen öffentlichen Schlüssel zu beachten ist.

Verschlüsselung mit einem asymmetrischen Schlüssel

Nehmen wir zunächst einmal an, dass der Absender einer Mail den richtigen öffentlichen Schlüssel des Empfängers kennt. Dann sieht die Ver- und Entschlüsselung einer Mail wie folgt aus:



Der Absender (A) verschlüsselt seine Mail mit dem öffentlichen Schlüssel (Public Key P) des Empfängers (E). Die Mail wird über das Internet an den Empfänger versendet.

Nur der Empfänger wird die Mail entschlüsseln können; dazu benötigt er seinen geheimen Schlüssel (Secret key S), den nur er kennt. Nicht einmal der Absender und

auch kein Man-in-the-Middle wird eine einmal verschlüsselte Mail wieder entschlüsseln können. Der gesamte Kommunikationsweg vom Absender zum Empfänger ist abgesichert - im Fachjargon sprechen wir von einer **Ende-zu-Ende-Verschlüsselung**.

In der Praxis: Verwendung von symmetrischen und asymmetrischen Schlüsseln

In der Praxis ist das Ver- und Entschlüsseln etwas komplizierter, da die Ver- und Entschlüsselung mit einem asymmetischen Schlüssel sehr viel Zeit beansprucht. Es wird daher eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung verwendet. Weder der Absender noch der Empfänger wird erkennen können, dass eine Kombination beider Verschlüsselungsverfahren benutzt wird.

Die Bedeutung der Auswahl des richtigen öffentlichen Schlüssels

Das Verschlüsseln mit dem öffentlichen Schlüssel und das Entschlüsseln mit dem geheimen Schlüssel ist absolut sicher, wenn der Absender den öffentlichen Schlüssel des Empfängers kennt.

Wenn der Empfänger seinen öffentlichen Schlüssel persönlich dem Absender übergibt, kann der Absender sicher sein, dass er den richtigen öffentlichen Schlüssel des Empfängers besitzt. Die persönliche Schlüsselübergabe macht die verschlüsselte Mail-Kommunikation absolut sicher.

In vielen Fällen ist eine persönliche Schlüsselübergabe nicht möglich oder nicht erwünscht - es müssen also andere Wege gefunden werden, den öffentlichen Schlüssel des Empfängers zu bekommen. In den meisten Fällen stehen die öffentlichen Schlüssel im Internet, entweder auf einer persönlichen Web-Seite des Empfängers oder in einem Schlüsselverzeichnis auf sogenannten "Public-Key-Servern".

Das Herunterladen eines öffentlichen Schlüssels ist also nicht das Problem - sicherzustellen, ob der heruntergeladene Schlüssel auch tatsächlich dem Empfänger gehört, ist schwierig. Dazu muss man wissen, dass jeder auch unter fremden Namen öffentliche Schlüssel auf Public-Key-Server hochladen kann. So könnte beispielsweise ein Man-in-the-Middle einen fingierten öffentlichen Schlüssel hochladen und so tun, also ob er der Empfänger wäre. Empfängt der Man-in-the-Middle verschlüsselte Nachrichten könnte er diese entschlüsseln und mit dem richtigen öffentlichen Schlüssel des Empfängers verschlüsselt an den Empfänger versenden. Weder Absender noch Empfänger würden bemerken, dass die Mails vom Man-of-the-Middle mitgelesen werden.

Es ist also sehr sehr wichtig, zu prüfen, ob ein heruntergeladener öffentlicher Schlüssel auch tatsächlich der angegebenen Person gehört.