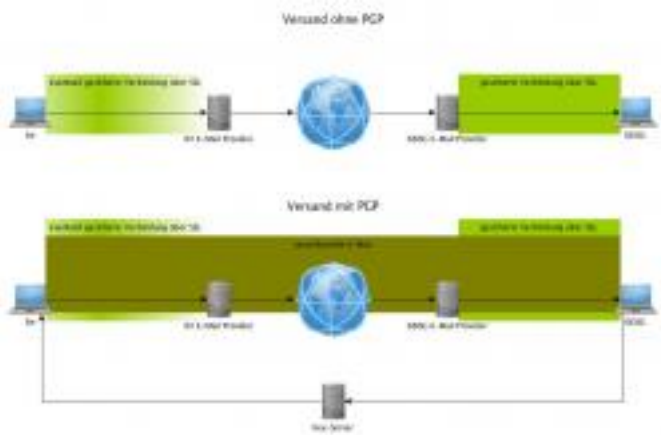
PGP - Pretty Good Privacy

Funktionsweise von PGP

PGP ist die Abkürzung für den englischen Ausdruck „Pretty Good Privacy“ und lässt sich mit „sehr guter Privatsphäre“ übersetzen. Es ist ein 1994 von Phil Zimmermann entwickeltes Verfahren zur Generierung von digitalen Signaturen und Verschlüsselung von digitalen Informationen und lässt sich somit dazu nutzen, Kommunikation über das Internet, zum Beispiel über E-Mail, zu verschlüsseln. Dies ist zum Austausch vertraulicher Informationen und Daten notwendig, da sich E-Mails mit Postkarten vergleichen lassen. Wenn eine E-Mail versendet wird, ist sie für jeden lesbar, an dem sie vorbei kommt.

Angenommen Sie möchten dem ISDSG eine E-Mail mit vertraulichen Informationen auf herkömmlichen Wege zukommen lassen. Dann verfassen Sie Ihre E-Mail auf Ihrem Computer und sende diese zu dem E-Mail Server Ihres E-Mail Providers. Möglicherweise ist Ihre E-Mail bei diesem Schritt schon geschützt, da Sie bereits eine sichere Übertragung über SSL eingestellt haben. Nun versucht Ihr Provider die E-Mail unserem Provider zuzustellen. Insofern es nicht der selbe Provider ist oder die Server im selben Netz stehen, wird die E-Mail im Klartext über das Internet versandt. Sobald die E-Mail bei unserem Provider angelangt ist, ist der Inhalt wieder vor unbefugtem Zugriff sicher, da wir E-Mails nur über eine gesicherte Verbindung abrufen.

Um nun einen durchgehenden Schutz zu gewährleisten kann die E-Mail mittels PGP verschlüsselt werden. Dazu haben wir unseren Public-Key auf einen Key-Server hoch geladen, damit man uns verschlüsselte Nachrichten zusenden kann. Diesen Schlüssel würden Sie sich nun herunterladen und mit diesem Ihre Nachricht verschlüsseln. Das PGP-Verfahren garantiert, dass diese Nachricht nun nur vom Besitzer des zum Public-Key gehörigen Private-Key entschlüsselt werden kann. Auf diese Weise lassen sich E-Mails über das ganze Internet auf vertrauliche Art und Weise versenden.



[1]

Nicht vergessen werden darf dabei, dass es keine hundertprozentige Sicherheit gibt. Mit genügend Rechenleistung lässt sich auch die beste Verschlüsselung knacken.

Digitale Verschlüsselung

Um die genaue Funktionsweise von PGP zu erläutern, müssen verschiedene Kryptographieverfahren dargestellt werden, die sich PGP zu nutze macht.

Symmetrisch

Bei symmetrischen Verfahren wird für die Ver- und die Entschlüsselung der selbe Schlüssel genutzt. Ein bekanntes und einfach zu verstehendes Verfahren dafür ist die Cäsarverschlüsselung, bei der jeder Buchstabe um eine bestimmte Anzahl an Schritten im Alphabet verschoben wird. In der Praxis wird häufig der Rijndael oder AES Algorithmus benutzt. Beim PGP-Verfahren wird der IDEA genutzt, bei dem die beiden Schlüssel zwar nicht identisch sind, aber sich leicht auseinander berechnen lassen.

Der Vorteil von symmetrischen Verschlüsselungsalgorithmen ist ihre hohe Zeitperformanz. Problematisch ist jedoch, dass die Schlüssel zwischen Absender und Empfänger ausgetauscht werden müssen, wobei diese abgefangen werden können. Außerdem werden bei n Teilnehmern n(n-1)/2 Schlüssel benötigt, die alle geheim gehalten und verwaltet werden müssen.

Asymmetrisch

Diese Nachteile hat die asymmetrische Verschlüsselung nicht, da bei ihr mit zwei unterschiedlichen Schlüsseln ver- und entschlüsselt wird. Dabei veröffentlicht der Empfänger einer Nachricht einen öffentlich Schlüssel (auch Public-Key), mit dem ihm Nachrichten zugesandt werden können, deren Entschlüsselung nur mit seinem privaten Schlüssel (auch Private-Key) möglich ist.

Die asymmetrische Verschlüsselung basiert auf dem Prinzip von Falltürfunktionen. Dies sind Funktionen, die „leicht“ zu berechnen sind, deren Umkehrfunktion jedoch „schwer“ zu berechnen ist. Beispielsweise ist die Multiplikation zweier ganzzahliger Primzahlen sehr schnell zu berechnen, jedoch ist die Zerlegung des Produktes in seine Primfaktoren ungleich schwerer.

Damit niemand einen öffentlichen Schlüssel von jemand anderes vortäuschen kann gibt es Zertifizierungsstellen, bei denen man öffentliche Schlüssel erhalten kann, bei denen garantiert wird, dass diese zu den entsprechenden Empfängern gehören.

Die Nachteile der asymmetrische Verschlüsselung gegenüber der symmetrischen sind, zum Einen die wesentlich längere Rechenzeit zur Verschlüsselung und zum Anderen müssen Nachrichten, die an mehrere Empfänger gesendet werden, für jeden Empfänger einzeln verschlüsselt werden.

Hybrid

Hybride Verschlüsselungen versuchen durch Kombination von Techniken der symmetrischen und der asymmetrischen Verschlüsselung die Vorteile der jeweiligen Verschlüsselungsart zu nutzen, beziehungsweise deren Nachteile aufzuheben. Dazu wird ein zufälliger Schlüssel erzeugt, mit dem eine Nachricht symmetrisch verschlüsselt wird. Dieser Schlüssel wird anschließend mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und zusammen mit der E-Mail versandt. Auf diese Weise ist es möglich, die schnelle Verschlüsselung bei symmetrischen Algorithmen zu nutzen und gleichzeitig die Schlüsselübertragungs- und-verwaltungsprobleme zu lösen. Außerdem müssen E-Mails an mehrere Empfänger nur einmal verschlüsselt werden. Zusätzlich zu der verschlüsselten Nachricht wird noch der symmetrische Schlüssel für jeden Empfänger einmal verschlüsselt an die Nachricht angehängt.

Digitale Signatur

Mit einer digitalen Signatur kann sichergestellt werden, dass eine Nachricht auch wirklich von dem angegebenen Absender stammt und die Nachricht nicht verändert wurde. Dazu wird über den gesamten Inhalt der Nachricht ein Hashwert gebildet und dieser mit dem privaten Schlüssel des Absenders verschlüsselt. Wenn nun der Empfänger die Nachricht erhält kann er mithilfe des öffentlichen Schlüssels, den er bei der Zertifizierungsstelle erhalten kann, den übersandten Hashwert entschlüsseln. Bildet er nun ebenfalls einen Hashwert über die Nachricht, kann er bestimmen, ob die Nachricht unverändert geblieben ist und ob sie wirklich vom Absender stammt.

Weitere Beiträge zum Thema PGP:

Anleitungen zum Einrichten von PGP [2]

Copy: Erledigt

Source URL: https://www.isdsg.de/informationen/tipps-und-tricks/pgp-pretty-good-privacy

Links
[1] https://www.isdsg.de/sites/default/files/imagepicker/89/PGP-Email_0.jpg
[2] https://www.isdsg.de/informationen/tipps-und-tricks/pgp-einrichten