Signieren und Verifizieren

Was bietet die Verschlüsselung und was nicht ? • Integrität der Mail und Identität des Absenders • Signieren • Verschlüsseln und Signieren in einem Arbeitsschritt • Verifizieren • Zusammenfassung: Was wird wozu benötigt ?

Was bietet die Verschlüsselung und was nicht ?

Mit der Verschlüsselung einer Mail stellen wir sicher, dass der Inhalt der Mail nur noch vom Eigentümer des geheimen (= privaten) Schlüssels gelesen werden kann.

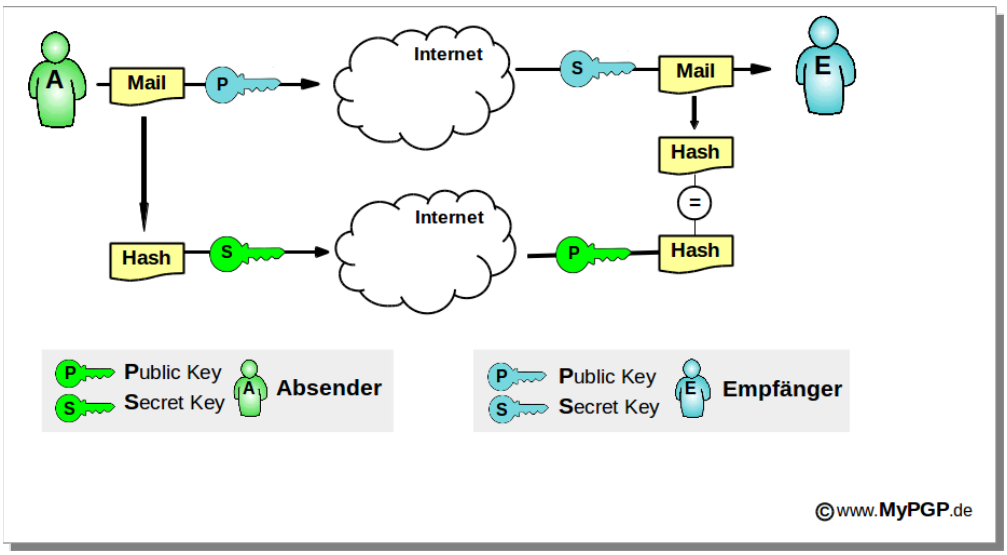
Wir können mit der Verschlüsselung **nicht** sicherstellen, dass die (verschlüsselte) Mail auf dem Weg zum Empfänger unverändert geblieben ist. Es wird wegen der Verschlüsselung unmöglich sein, den Inhalt einer Mail gezielt zu verändern; es bleibt aber die Möglichkeit, eine verschlüsselte Mail willkürlich zu verändern und dadurch irgendwelche Änderungen an der entschlüsselten Mail zu erreichen, ohne dass der Empfänger dies bemerken würde. Eine verschlüsselte Mail könnte auch durch technische Fehler unbeabichtigt verändert werden.

Neben der Verschlüsselung benötigen wir daher noch einen Mechanismus, der die Integrität (Unversehrheit) der Mail bestätigen kann.

Mit der Sicherstellung der Integrität ist noch nicht sichergestellt, dass der Absender auch derjenige ist, den er vorgibt, zu sein. Irgendeine Person könnte unter falschem Namen eine verschlüsselte Mail an den Empfänger schicken, denn zum Verschlüsseln wird nur der für jeden zugängliche öffentliche Schlüssel des Empfängers benötigt.

Neben der Verschlüsselung und der Sicherstellung der Integrität müssen wir für die vollständige Mail-Sicherheit die Identität des Absenders eindeutig feststellen können.

Integrität der Mail und Identität des Absenders



In der obigen Abbildung ist bereits der obere Weg bekannt: die Mail wird mit dem öffentlichen Schlüssel (= public Key) des **Empfängers** verschlüsselt. Nur noch der

Empfänger wird mit seinem geheimen Schlüssel (secret key) die verschlüsselte Mail entschlüsseln können.

Das bereits für die Verschlüsselung benutzte asymmetrische Verfahren mit einem öffentlichen und einem geheimen Schlüssel kann auch für die Integrität der Mail und für die Feststellung der Identität des Absenders benutzt werden.

Für die Ver- und Entschlüsselung wurden die beiden **Schlüssel des Empfängers** verwendet. Für die Sicherungstellung der Integrität und Identität werden die beiden **Schlüssel des Absenders** verwendet.

Die obige Abbildung zeigt, dass ein Hash der Mail berechnet wird. Ein Hash ist eine mehrstellige Prüfzahl, die repräsentativ für das Original, hier für die Mail, steht. Ändert sich der Inhalt des Orignals muss sich auch die Prüfzahl ändern. Der Hash ist in aller Regel bedeutend kürzer als das Original und damit besser - auch manuell - mit anderen Hashes abzugleichen. Vergleichbar ist das mit einem Fingerabdruck, der stellvertretend für einen Menschen steht.

Der Hash wird mit dem **geheimen Schlüssel des Absenders** verschlüsselt und zum Empfänger geschickt. Der Empfänger entschlüsselt den Hash mit dem **öffentlichen Schlüssel des Absenders**. Nachdem der Empfänger die Mail des Absenders empfangen und entschlüsselt hat, bildet er ebenfalls einen Hash dieser Mail mit der selben Methode wie der Absender.

Der Empfänger besitzt jetzt zwei Hashes: einen, den er selbst gebildet hat und einen, den er vom Absender in verschlüsselter Form bekommen und mit dem öffentlichen Schlüssel des Absenders entschlüsselt hat. Da beide Hashes aus der selben Mail gebildet wurde, müssen auch die Hashs exakt übereinstimmen. Ist das der Fall, kann der Empfänger davon ausgehen, dass die Mail vom Absender kommt (Identität des Absenders) und die Mail nicht verändert wurde (Integrität der Mail).

Falls die Hashes nicht übereinstimmen, könnte es daran liegen, dass die Mail verändert wurde und der Empfänger zwangsläufig einen anderen Hash aus der Mail gebildet hat (Integritätsverletzung). Oder der geheime Schlüssel des Absenders, mit dem der gesendete Hash verschlüsselt wurde, passt nicht zum öffentlichen Schlüssel des Absenders, den der Empfänger zum Entschlüsseln verwendet hat. Wenn wir annehmen, dass der geheime Schlüssel des Absenders auch nur dem Absender bekannt, muss der gesendete Hash mit einem anderen (geheimen) Schlüssel unterschrieben worden sein oder ein öffentlicher Schlüssel zum Entschlüsseln verwendet worden sein, der nicht zum geheimen Schlüssel des Absenders passt. Die Identität des Absenders kann also nicht bestätigt werden (Identitätsverletzung).

Auch hier steht und fällt die Beurteilung der Sicherheit der Mail mit der eindeutigen Zuordnung des öffentlichen Schlüssels zu einer Person. MyPGP hilft, einen öffentlichen Schlüssel einer Person möglichst zweifelsfrei zuzuordnen.

Signieren

Das "Unterschreiben" einer Mail mit einem Hash nennt sich Signieren. Durch das Signieren wird die Mail-Integrität und die Absender-Identität sichergestellt.

Wie in der obigen Abbildung dargestellt, kann das Verschlüsseln und Signieren

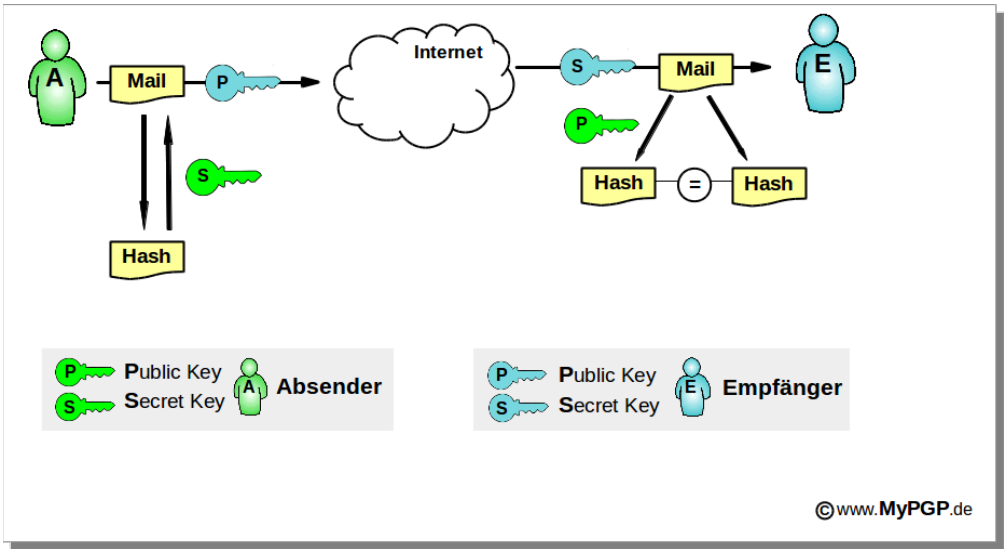
getrennt passieren und die Mail und die Signatur auch getrennt übertragen werden. Es kann auch auf die Verschlüsselung der Mail verzichtet werden und nur die Signatur übertragen werden. Die Mail könnte dann von Dritten mitgelesen werden, aber nicht verändert werden, ohne dass der Empfänger das merken würde. Die Signatur würde die Integrität der Mail und die Identität des Absenders auch alleine sicherstellen können.

In der Praxis werden Mails in der Regel gleichzeitig verschlüsselt und signiert, weil die Verfahren im wesentlichen identisch ablaufen.

Das Signieren kann aber auch auf Download-Dateien angewendet werden. Möchten wir sicherstellen, dass eine heruntergeladene Datei aus der "richtigen" Quelle bezogen wurde ("Absender-Identität") und der Download fehlerfrei erfolgte ("Datei-Integrität"), könnten wir eine separat geladene Signaturdatei mit der Signatur der heruntergeladenen Datei vergleichen. Voraussetzung ist, dass es zu einer Datei eine Signaturdatei gibt und dass der öffentliche Schlüssel des Absenders dem Absender zweifelsfrei zugeordnet werden kann. Die Zuordnung passiert häufig durch die Überprüfung des Fingerprints des öffentlichen Schlüssels des Absenders (der Quelle).

Verschlüsseln und Signieren in einem Arbeitsschritt

In der obigen Abbildung werden Verschlüsselung und Signierung noch getrennt durchgeführt. In der Praxis geschieht das häufig in einem Arbeitsschritt.



Bevor die Mail verschlüsselt wird, wird der Hash des Mail-Textes berechnet und mit dem geheimen Schlüssel des Absenders verschlüsselt. Der verschlüsselte Hash wird an den Text der Mail angehängt, wird also Bestandteil der Mail. Die gesamte Mail wird dann mit dem öffentlichen Schlüssels des Empfängers verschlüsselt und zum Empfänger versendet.

Verifizieren

Der Empfänger entschlüsselt die Mail mit seinem geheimen Schlüssel. Der Hash und der eigentliche Text der Mail werden voneinander getrennt. Der Hash wird mit dem

öffentlichen Schlüssel des Absenders entschlüsselt. Danach berechnet der Empfänger den Hash des eigentlichen Textes des Mail und vergleicht diesen mit dem Hash, den er in verschlüsselter Form am Absender erhalten hat. Beide Hashes müssen exakt übereinstimmen, um sagen zu können, dass die Mail korrekt übertragen wurde und der Absender tatsächlich der korrekte Absender ist.

Zusammenfassung: Was wird wozu benötigt ?

Der Absender benötigt für verschlüsselte und signierte Mails seinen geheimen Schlüssel zum Signieren der Mail und den öffentlichen Schlüssel des Empfängers zum Verschlüsseln der Mail.

Der Empfänger benutzt seinen geheimen Schlüssel zum Entschlüsseln der Mail und den öffentlichen Schlüssel des Absenders zum Überprüfen der Signatur.

Die absolut sichere Ende-zu-Ende-Übertragung einer Mail setzt voraus, dass eine Person ihren geheimen Schlüssel immer geheim hält und dass ein öffentlicher Schlüssel einer Person zweifelsfrei zugeordnet werden kann.