Passphrase-Erläuterung

Version 1.0, 10.01.2016

In der Schulung kommt es gelegentlich zu Missverständnissen bezüglich der unterschiedlichen Passphrasen.

Hauptschlüssel-Passphrase

Die Hauptschlüssel-Passphrase ist die wichtigste, denn nur mit ihr kann der Schlüssel bearbeitet (v.a. verlängert und wiederrufen) werden und ggf. aus den bei der Schlüsselerzeugung generierten Dateien wiederhergestellt werden; nur mit ihm können andere Schlüssel signiert werden.

Diese Passphrase darf typischerweise nur in einer sicheren Umgebung eingegeben werden, weil die Sicherheit des Hauptschlüssels darauf basiert, dass ein Angreifer an die Passphrase nicht herankommt (alternativ könnte man mit physischer Sicherheit arbeiten, aber das würde das Backup erschweren) und dass sie so stark ist, dass man sie nicht knacken kann. Dadurch, dass man diese Passphrase auf hohem Niveau schützt, kann man durchaus ein Backup des Schlüssels auf seine Website packen. Und das o.Ä. sollte man tun, denn der Verlust von Schlüsseln auf Grund von Rechnercrashs (Hardwaredefekt oder planlose Neuinstallation) ist ein verbreitetes Problem. Ebenso der Verlust der Passphrase. Der Verlust aller anderen Passphrasen bringt nur überschaubare Unannehmlichkeiten mit sich, weil sie "aus der Hauptschlüssel-Passphrase" wiederhergestellt werden können.

Transport-Passphrase (Unterschlüssel)

Die privaten Unterschlüssel, die ins Arbeitssystem importiert werden (anders als der private Hauptschlüssel), müssen irgendwie dahin kommen. Nicht immer ist es möglich, sie bei der Erzeugung direkt ins System zu kopieren. Dann müssen sie auf einen USB-Stick kopiert werden, womöglich den von jemand anderem. Es kann sogar sein, dass die erzeugten Daten per (unverschlüsselter) E-Mail verschickt werden müssen (bei Leuten, die weder ihren Computer noch einen Stick mit zur Schlüsselerzeugung gebracht haben).

Man kann die Unterschlüssel für den Transport nicht sinnvoll mit der Hauptschlüssel-Passphrase schützen, denn beim Import muss die Transport-Passphrase eingegeben werden, und die Hauptschlüssel-Passphrase darf im normalen System ja gerade nicht eingegeben werden.

Zur Vereinfachung bekommen alle Teilnehmer eine zweite, genauso sichere Passphrase, die für Transport und Import verwendet wird. Das hat auch die Vorteile, dass die Daten auf dem Stick sicher sind (man sich also keine Gedanken über sicheres Löschen machen muss) und man den ganzen Ordner einfach auf weitere Rechner kopieren kann (auf welchem Weg auch immer).

Die Transport-Passphrase benötigt man immer dann, wenn der Original-Datensatz erneut importiert werden muss (auf einem anderen System oder nach einem Crash aus dem Backup). Im Extremfall wird sie nie wieder benötigt.

Alltags-Passphrase (Arbeitssystem)

In der Standardkonfiguration muss man die Passphrase ggf. auch mehrfach pro Tag eingeben. Das macht quasi niemand freiwillig mit einer kryptografisch sicheren Passphrase. Es ist auch nur begrenzt sinnvoll, auf einem normalen System eine derart sichere Passphrase zu verwenden.

Wenn die Schküssel ins Arbeitssystem importiert werden, haben sie noch die Transport-Passphrase. Die wird typischerweise direkt nach dem Import (das Importscript bietet das an) vom Nutzer geändert. Sie kann später problemlos und trivial erneut geändert werden (v.a. mit den grafischen Schlüsselverwaltungs-Programmen). Für die Wahl der Alltags-Passphrase sollte maßgeblich sein, dass man sie nicht vergisst (weswegen es sich anbietet, ein Passwort zu verwenden, das man regelmäßig nutzt) und dass man sie bereitwillig auch mehrfach pro Tag eingibt (es sei denn, man entscheidet sich dafür, sie vom System lange im Cache (gpg-agent oder Schlüsselverwaltung) halten zu lassen).

Verlängerungs-Passphrase

Um die Verlängerung der Schlüsselgültigkeit zu erleichtern, kann man schon bei der Schlüsselerzeugung Signaturen ("Eigenbeglaubigungen", "self-signatures") erzeugen, die länger gültig sind als der Schlüssel es normalerweise wäre. Da die Begrenzung der Gültigkeitsdauer ein Sicherheitsaspekt ist, sollten diese Verlängerungs-Signaturen gut geschützt werden. Sie werden deshalb mit einer Passphrase verschlüsselt, die genauso sicher ist wie die Hauptschlüssel-Passphrase. Für jedes Verlängerungsdatum muss eine eigene Passphrase genutzt werden; theoretisch könnte man auch die Hauptschlüssel-Passphrase nehmen, aber dann müssten die Dateien in einem sicheren System entschlüsselt werden, was die Arbeitserleichterung zum Großteil zunichte machen würde.

Der technische Prozess sieht allerdings etwas anders aus als bei den Schlüsseln. In Schlüssel ist die Passphrase gewissermaßen eingebaut; Signaturen dagegen haben keine Passphrase. Deshalb werden die Signaturdateien so synmetrisch verschlüsselt, wie jede andere Datei auch.