# Erzeugung von Offline-Hauptschlüsseln

Version 1.0, 09.03.2014

Diese Erklärung dient der besseren Verständlichkeit der Vorgänge auf den Einrichtungsterminen.

## Was ist ein Hauptschlüssel?

Der Hauptschlüssel ist die zentrale Komponente eines OpenPGP-Zertifikats, die als einzige nicht ausgetauscht werden kann. Der Fingerprint (und dementsprechend auch die short und long ID) bezieht sich auf den Hauptschlüssel. Ein Zertifikat besteht aus genau einem Hauptschlüssel und eventuell einem oder mehreren Unterschlüsseln. Technisch unterscheiden sich diese beiden Kategorien nicht nennenswert. Der Hauptschlüssel ist immer der zuerst erstellte Teil eines neuen Zertifikats, weil alles andere von ihm unterschrieben werden muss.

## Sicherheitsrelevanz von Offline-Hauptschlüsseln

Da Hauptschlüssel bei geeignetem Aufbau des Zertifikats im Alltag nicht benötigt werden, kann man sie von gefährdeten Systemen fernhalten. Dazu weitgehend äquivalent ist die reine Speicherung (also nicht Verwendung) in einem unsicheren System, wenn der Hauptschlüssel mit einer Passphrase geschützt ist, die unmöglich geknackt werden kann, und diese Passphrase – Achtung: An dieser Stelle passieren die meisten Fehler! – **nie** in einem unsicheren System eingegeben wird. Also insbesondere nicht aus schierer Blödheit *“mal zum Ausprobieren”*, weil irgendwas nicht so funktioniert, wie es soll, und man meint, in seiner Weisheit ruhig genau das Gegenteil dessen machen zu können, (1) was einem gesagt wird, (2) was in deutlichster Weise auf dem Zettel mit der Passphrase steht, den man (3) dafür auch noch aus einem verschlossenen Briefumschlag holen muss. Eine unentschuldbare Fehlleistung.

Dass man Hauptschlüssel schützen *kann*, reicht als Grund, das auch zu tun, noch nicht aus. Aber Hauptschlüssel sind von zentraler Bedeutung, so dass sich dieser Schutz auch lohnt:

1. *Fingerprint*
   Wenn Zertifikate direkt verifiziert werden, dann immer über den Fingerprint, der sich auf den Hauptschlüssel bezieht. Damit ist der Hauptschlüssel quasi die digitale Identität des Besitzers. Der Rest des Zertifikats (Unterschlüssel, User-IDs) ist austauschbar. Von so einem Austausch merken die Kommunikationspartner kaum etwas; sie müssen nur ihre Version des Zertifikats (typischerweise von einem Keyserver) aktualisieren.
2. *Langlebigkeit*
   Man kann (als Schadensbegrenzung bei früherer Kompromittierung) z.B. jährlich die Unterschlüssel tauschen. Einen sicheren Hauptschlüssel aber kann man 10+ Jahre verwenden. Dazu gehört aber ein gutes Backup!
3. *Web of Trust (WoT)*
   Das Web of Trust ist an Signaturen des Hauptschlüssels aufgehängt. Das WoT ist also nicht sicherer als die beteiligten Hauptschlüssel. Und wenn man nicht sorgfältig (und manipulationssicher) die Fingerprints seiner Kommunikationspartner (z.B. auf Papier) archiviert hat, kann man nach einer möglichen Kompromittierung des eigenen Rechners nicht einmal feststellen, welche der eigenen Schlüsselsignaturen korrekt sind.
4. *höhere Sicherheit für Daten*
   Idealerweise hat man einen eigenes Zertifikat für hochsichere Daten. Geschätzte 99,x% der OpenPGP-Anwender haben das nicht. Wenn man wenigstens einen (entsprechend konfigurierten) Offline-Hauptschlüssel hat, kann man (wenn auch mit Schwierigkeiten, die ein hohes Maß an Beherrschung des Umgangs mit GnuPG erfordern und deshalb einem hohen Fehlbedienungs-Risiko ausgesetzt sind) mit diesem einen insgesamt sichereren Schlüssel "simulieren". Eine Schlüsselrichtlinie sollte immer mit einem Offline-Hauptschlüssel signiert sein!

## Erzeugung und Import ins Arbeitssystem

Die Offline-Hauptschlüssel werden in einer sicheren Umgebung (typischerweise Knoppix von CD/DVD) erzeugt, weil ein Schlüssel immer nur so sicher ist wie das unsicherste System, auf dem er verwendet (oder unsicher gespeichert) wurde. In der sicheren Umgebung werden mehrere Versionen des Schlüssels erzeugt:

1. eine vollständige, mit dem privaten Hauptschlüssel, die mit der (sicher zu verwahrenden!) Hauptschlüssel-Passphrase geschützt ist
   Diese Version wird nur in einer sicheren Umgebung verwendet (z.B., um den eigenen Schlüssel zu verlängern oder andere Zertifikate auf hohem Niveau zu unterschreiben)
2. eine, die nur die privaten Unterschlüssel erhält und mit der Transport-Passphrase geschützt ist
   Nur diese Version wird ins Arbeitssystem importiert.
   Eine sichere Transport-Passphrase wird verwendet, damit auf USB-Sticks keine kritischen Schlüsseldaten zurückbleiben und der Schlüssel zur Not auch per E-Mail verschickt werden kann. Sie wird typischerweise gleich nach dem Import ins Arbeitssystem durch eine alltagstaugliche Passphrase ersetzt.

Aus dem vollständigen Schlüssel können die Unterschlüssel erzeugt werden (etwa aus einem Backup, wenn die Schlüsse auf dem Arbeitssystem zerstört wurden oder wenn es Probleme mit der Passphrase gibt); aber das darf nur in einer sicheren Umgebung passieren! Der umgekehrte Weg ist natürlich nicht möglich.