OpenPGP-Schulung – Merkzettel für normale Schlüssel (Version 1.0, 13.04.2015)

1. mein Fingerprint:

____ ____

short ID

2. Was ich NICHT tun DARF

1. Die Benutzung von Schlüsseln mit Sicherheit für die verschlüsselten Daten verwechseln. Daten und Schlüssel sind immer nur so sicher wie der unsicherste Rechner, auf dem sie jemals verwendet wurden.
2. Die Schlüssel anders verwenden als geplant bzw. von den Beteiligten angenommen.

3. Was ich NICHT tun SOLL

1. Schlüssel ohne sicheres, verlässliches Backup für wichtige Daten verwenden
2. Schlüssel ohne angemessene Prüfung für die Öffentlichkeit beglaubigen.

4. Was ich TUN SOLL

1. Für alle Informationen bewerten, ob sie geschützt werden müssen und wovor (d.h. mit welchem Aufwand) und konsequent danach handeln.
2. Langfristig ein gutes Verständnis der Thematik erwerben und anderen dabei helfen. Sicherheit ohne Sachkenntnis ist de facto unmöglich. Irgendwann auf hochwertige Schlüssel umsteigen.
3. Immer ein paar Zettel mit Name, E-Mail-Adresse und Fingerprint dabei haben.
4. Regelmäßig prüfen, ob es für die Schlüssel anderer Leute Aktualisierungen gibt (womöglich einen Widerruf).
5. Die Verbreitung von OpenPGP fördern: www.openpgp-schulungen.de/fuer/unterstuetzer/

5. Wie ich neue Kommunikationspartner einbinde

1. *nicht einfach Adressen übernehmen*
   Wie sicher ist es, dass die angenommene Adresse korrekt ist? Niemand knackt Schlüssel, wenn Täuschen viel einfacher ist.
2. *deren öffentlichen Schlüssel (Zertifikat) besorgen und importieren*
   von einer Webseite oder von einem Keyserver runterladen oder per E-Mail schicken lassen
3. *den Fingerprint besorgen (falls aus unsicherer Quelle – Internet)*
   Also die Zeichenkolonne dieser Art: CF51 CB88 7D9A B184 AD50 21F4 DA6B 2836 5A21 B2D0
   Über einen sicheren Kanal (idealerweise persönlich) den Fingerprint vom Besitzer beschaffen.
4. *verifizieren und signieren*
   Den Fingerprint des importierten Schlüssels anzeigen lassen und mit der sicheren Quelle vergleichen. Bei Übereinstimmung den Schlüssel signieren (für einen selber oder die Öffentlichkeit).
   Falls Verifikation nicht möglich: Dies beim Versenden der Daten und Erhalt von Nachrichten bedenken!

6. Wie asymmetrische Schlüssel funktionieren – ich brauche:

den öffentlichen Schlüssel eines anderen	um Daten für ihn zu verschlüsseln
	um Signaturen von ihm zu prüfen („*korrekte Signatur*“)
meine privaten Unterschlüssel	um für mich verschlüsselte Daten zu entschlüsseln
	um Signaturen zu erzeugen
meinen privaten Hauptschlüssel	um meinen Schlüssel zu bearbeiten (z.B. Hinzufügen oder Löschen von User-IDs)
	um die öffentlichen Schlüssel (Zertifikate) anderer zu beglaubigen
den Fingerprint anderer Leute	um sicherzustellen, dass ich den richtigen Schlüssel importiert habe (ohne dies keine Sicherheit, sondern nur Spielerei!)

7. Erst fragen, dann handeln

http://www.openpgp-schulungen.de/support/