OpenPGP-Schulung – Einrichtungs-Merkzettel (Version 1.3.1, 12.04.2014)

1. mein Fingerprint:

____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____

____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____

short ID

2. Was ich NICHT tun DARF

1. Die Passphrase des Hauptschlüssels in einem unsicheren System eingeben (reines Speichern der Datei dort ist OK) oder in die Hände von Dritten gelangen lassen (ein sicheres System ist z.B. eins, das von einem vertrauenswürdigen Nurlese-Medium (CD, DVD) gestartet wurde, etwa Knoppix).
2. Die Hauptschlüssel-Passphrase auf einen unsicheren Wert ändern.
3. Den geheimen Hauptschlüssel oder dessen Passphrase verlieren; dann ist es vorbei.

3. Was ich NICHT tun SOLL

1. Die Unterschlüssel mit einer unsicheren Passphrase transportieren (z.B. auf USB-Sticks).
2. Schlüssel ohne angemessene Prüfung beglaubigen, ohne dies zu dokumentieren (cert-level 1/2).
3. Am Web of Trust teilnehmen, bevor ich viel über OpenPGP gelernt habe – insbesondere keine aktive Teilnahme (d.h. öffentliche Schlüsselsignaturen (statt lokaler) erzeugen und verteilen).
4. (standardmäßig) PGP/Inline verwenden (sondern PGP/MIME).

4. Was ich TUN SOLL

1. sicher verwahrtes Backup: kompletter Schlüssel (**.secret-mainkey.asc*) & Passphrase
2. Eigene Schlüsselrichtlinie erstellen, veröffentlichen (policy URL) und strikt befolgen.
3. Immer ein paar Zettel mit Name, E-Mail-Adresse und Fingerprint dabei haben.
4. Regelmäßig nach Updates aller Schlüssel suchen (`gpg --refresh-keys`).
5. Die Verbreitung von OpenPGP fördern: www.openpgp-schulungen.de/fuer/unterstuetzer/

5. Wie ich neue Kommunikationspartner einbinde

1. *deren öffentlichen Schlüssel (Zertifikat) besorgen und importieren*
   von einer Webseite oder von einem Keyserver oder per E-Mail schicken lassen
2. *den Fingerprint besorgen*
   Also die Zeichenkolonne dieser Art: CF51 CB88 7D9A B184 AD50 21F4 DA6B 2836 5A21 B2D0
   Über einen sicheren Kanal (gut: persönlich; bedenklich: telefonisch; keinesfalls: Webseite) den Fingerprint vom Besitzer beschaffen.
   Falls das nicht möglich ist, auf jeden Fall den Hinweis in die Signatur aufnehmen, dass nicht geprüft wurde!
3. *den Fingerprint des importierten Schlüssels anzeigen lassen und vergleichen*
4. *Schlüssel beglaubigen (erst mal nur mit dem lokalen Zertifizierungsschlüssel: lckey-lsign)*
   Vor der Festlegung auf eine Zertifizierungsrichtlinie nur lokale Signaturen (lsign) erzeugen.

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:

Info-Webseite: www.openpgp-schulungen.de – Support per XMPP: gnupg-support@jabber.org