Infos zur verschlüsselten Kontaktaufnahme mit GnuPG für Webseiten

Dr. Arne Babenhauserheide

<2021-05-14 Fr>

Wenn ihr Leuten ermöglichen wollt, euch abhörsicher zu kontaktieren, ist der leichteste Weg, eine E-Mail-Adresse und einen GnuPG Schlüssel anzugeben.

- Der Weg für Windows ist Gpg4win.
- Für MacOS: GPGTools
- Für Linux installiert direkt `gnupg` aus den Paketquellen.

Speichert euch den erstellten Schlüssel am Besten als Papierkopie und legt die an einen sicheren Ort.

Informationen, die zur Kontaktaufnahme nötig sind:

- **E-Mail-Adresse** für verschlüsselte Kontaktaufnahme: <E-Mail-Adresse>
- **OpenPGP-Schlüssel**: <Fingerabdruck> (erstellen) (verlinkt auf ein exportiertes Zertifikat (erstellen))
- **Informationen**: Digitale Selbstverteidigung: E-Mails verschlüsseln mit OpenPGP oder E-Mail-Selbstverteidigung

Beispiele:

- Ein Beispiel für mich wäre:
  Kontakt: arne_bab -ät- web.de (OpenPGP: F34D 6A12 35D0 4903 CD22 D5C0 13EF 8D45 2403 C3EB)

- Beispielseite: https://www.draketo.de/ich/impressum
- Etwas kürzeres Beispiel: https://netzpolitik.org/ueber-uns

Wenn ihr mit anderen zusammen schreibt und wirklich auf Nummer sicher gehen wollt, könnt ihr das Passwort oder auch den gesamten Paperkey mit Shamirs Secret Sharing Scheme in mehrere Schlüssel aufteilen, von denen mindestens eine bestimmte Anzahl nötig sind, um das Passwort wiederherzustellen. Das ist dann aber auf dem Sicherheitsniveau von Update-Schlüsseln für Kryptosoftware: http://point-at-infinity.org/ssss/

Viel Erfolg!

FAQ

- Warum GnuPG und nicht was anderes?

  Der Hauptvorteil von GnuPG ist, dass ihr unabhängig von aller anderen Infrastruktur seid. Ihr liefert selbst den Schlüssel und könnt eine selbstgehostete E-Mail-Adresse verwenden. Ihr braucht keinen Eintrag in Zertifikats-Hierarchien, keine zentralisierten Vermittlungsserver, keinen festgelegten Gerätetyp, usw.

- Verschlüsselt ist nicht automatisch vertraulich?

  Nennt die Kontaktaufnahme nicht vertraulich. Sie ist verschlüsselt (niemand kann den Inhalt sehen), aber nicht vertraulich (es ist möglich, herauszufinden, dass ihr Kontakt hattet). Vertrauliche Nachrichten zu schicken ist weitaus komplizierter, weil dafür keine Metadaten bekannt werden dürfen. Wenn die euch Kontaktierenden auf Nummer sicher gehen wollen, können sie die Kontaktaufnahme allerdings vertraulich machen, indem sie dafür eine nicht zurückverfolgbare Wegwerf-E-Mail-Adresse erstellen — z.B. via Tor auf Sharklasers.