E-Mail Verschlüsselung mit OpenPGP

Tiefere Infos unter gnupg.org. GnuPG (GPG) implementiert den OpenPGP Standard.

- Cheat Sheet Commands
- one key 2 e-mails
- keys mit Smartcard (yubikey)
- Key setup

Clients

Um verschlüsselte E-Mails versenden zu können benötigt man einen Client zum verwalten der **Schlüssel**, sowie einen E-Mail Client, welcher fähig ist verschlüsselte Mails zu senden und zu empfangen. Eine **Liste an E-Mail Clients** kann hier gefunden werden. Für Desktop empfehle ich Thunderbird, für Android FairMail, sowie OpenKeychain zum verwalten der Schlüssel.

Schlüssel erstellen

Ein Schlüssel Paar bestehen aus Privatem und Öffentlichem Key kann einfach in Thunderbird erstellt werden: **Extras --> OpenPGP-Schlüssel verwalten --> Erzeugen --> Neues Schlüsselpaar** Anschließend die E-mail auswählen und mit den Standardeinstellungen erzeugen.

Schlüssel verteilen

Wichtig niemals den privaten Schlüssel weitergeben!!

Privaten Schlüssel

Der Private Schlüssel kann in Thunderbird mit der Option **Datei --> Sicherheitskopie für geheimen Schlüssel erstellen** als Datei gespeichert werden. Diese Datei sollte dann über einen Sicheren Weg (z.B unsere Nextcloud) auf die anderen Clients(z.B. dein Handy), von denen du verschlüsselte Mails senden möchtest verteilt werden.

Öffentlicher Schlüssel

Um deinem E-Mail Empfänger deinen Öffentlichen Schlüssel zugänglich zu machen, sollte dieser auf einem Key-Server hochgeladen werden. key.openpgp.org wird als Standard von den meisten Clients verwendet. Der Öffentliche Schlüssel kann über das Webinterface hochgeladen werden.

Schlüssel eines Anderen suchen

Über Thunderbird sowie allen anderen Clients kann über eine Option wie z.B in Thunderbird **OpenPGP-Schlüssel verwalten --> Schlüsselserver --> Schlüssel online finden** der Öffentliche Schlüssel andere Leute importiert werden.

Verschlüsselte E-mails senden/empfangen/unterschreiben

Wichtig in Thunderbird muss möglicherweise unter den Konteneinstellungen den jeweiligen Identitäten unter **"Ende-zu-Ende-Verschlüsselung"** der richtige Schlüssel zugeordnet werden.

Senden

Zum Senden kann in den Mailclients mit einer Funktion, wie z.B. in Thunderbird **OpenPGP --> Verschlüsseln** beim verfassen der Mail diese verschlüsselt werden. Anschließend einfach Senden. **Wichtig** zum Senden einer verschlüsselten Mail wird der Öffentliche Schlüssel des Empfängers benötigt!

Empfangen

Beim Empfangen sollten die verschlüsselten Mails automatisch entschlüsselt werden.

Unterschreiben

E-mails können mit einem OpenPGP Schlüssel unterschrieben werden, sodass der Empfänger sicherstellen kann, dass diese nicht verändert wurde (Man-in-the-Middle). Um eine empfangene unterschriebene Mail als authentisch zu erkennen, wird der Öffentliche Schlüssel des Senders benötigt.

Created 2023-09-26 20:35:07 UTC by Luca Bauer
Updated 2023-09-26 20:42:39 UTC by Luca Bauer