sichere-Kommunikation

- E-Mails per PGP verschlüsseln
- Wissenswertes über Signal
- Signal auf dem Laptop nutzen
- Mehrere Signal Accounts auf Android

E-Mails per PGP verschlüsseln

E-Mail-Verschlüsselung Einrichten

Wenn du eine E-Mail an z.B. legal@letztegeneration.org schickst, dann kannst du diese vor dem Abschicken auf deinem Gerät verschlüsseln. So können dein und unser Mailprovider sowie dein und unser Internetprovider nicht mitlesen.

Diese Anleitung erklärt wie die PGP-Verschlüsselung für den E-Mail-Anbieter ProtonMail oder den E-Mail-Client Thunderbird eingerichtet werden kann.

> **ProtonMail** ist ein Anbieter mit dem man direkt im Browser PGP-verschlüsselte E-Mails senden und empfangen kann. ProtonMail ist relativ einstiegsfreundlich und kann **für deine private E-Mail-Adresse** verwendet werden, um damit verschlüsselt mit AGs/WiGs zu kommunizieren.

> PGP-Verschlüsselung funktioniert aktuell nicht mit unserem Webmail.

> Wenn du bei einem **anderen Anbieter** bist oder mit deiner **AG/WiG-Adresse** verschlüsselte E-Mails senden und empfangen willst, brauchst du einen E-Mail-Client mit PGP-Unterstützung wie z.B. **Thunderbird**.

Die Anleitung behandelt folgende Themen (jeweils für ProtonMail und Thunderbird):

- PGP-Verschlüsselung einrichten: Schlüsselpaar erzeugen und öffentlichen Schlüssel verbreiten
- Öffentlichen Schlüssel importieren (brauchst du, um an diese E-Mail eine verschlüsselte Nachricht zu schicken)
- Nur Thunderbird: Es existiert bereits ein Schlüsselpaar, z.B. von deiner AG/WiG (du bekommst privaten und öffentlichen Schlüssel, die du importieren möchtest)

Bei Fragen wende dich bitte an die IT-AG: it-support@letztegeneration.org.

ProtonMail

> ProtonMail ist zwar sehr einstiegsfreundlich, aber aufgrund der webbasierten Architektur nicht so sicher wie ein nativer E-Mail-Client mit PGP-Verschlüsselung wie z.B. Thunderbird.

PGP-Schlüsselpaar erzeugen

ProtonMail generiert automatisch ein Schlüsselpaar für deinen Account.

Unter https://account.proton.me/u/0/mail/encryption-keys kannst du deinen Schlüssel sehen.

Schlüssel veröffentlichen

Wenn du anderen Menschen das Hinzufügen deines Schlüssel erleichtern willst, dann lade deinen **öffentlichen** Schlüssel bei keys.openpgp.org hoch.

Dazu hier deinen Schlüssel exportieren und auf https://keys.openpgp.org/upload hochladen. Klicke auf "verifizieren" und auf den Link in der E-Mail.

Öffentlichen Schlüssen importieren

Bei ProtonMail muss der öffentliche Schlüssel der:des Empfängerin:Empfängers im Adressbuch hinterlegt werden. So geht es:

1. In die Weboberfläche einloggen, bis du deinen Posteingang siehst.
2. Oben rechts auf das Kontakte Icon mit den 2 Köpfen klicken:

ProtonMail-Adressbuch

1. nach legal@letztegeneration.org suchen beziehungsweise diese Adresse anlegen.
2. Den Kontakt öffnen und auf das Zahnrad klicken.
3. Erweiterte PGP-Einstellungen einblenden.
4. Den öffentlichen Schlüssel hier herunterladen:
   - AGs und WiGs: pgp.letztegeneration.org/
   - Umwelt-Treuhandfond
   - restliche Welt: https://keys.openpgp.org
5. den öffentlichen Schlüssel in ProtonMail wieder hochladen (im Bild rot 1.).
6. die Verschlüsselung immer aktivieren „E-Mails verschlüsseln“ (im Bild rot 2.).

   Nun sollte es so aussehen (nur mit letztegeneration.org statt letztegeneration.de, der Screenshot ist etwas älter):

Adressbucheintrag in ProtonMail

1. Nach Klick auf das Zahnrad öffnet sich dieser Dialog zum Hochladen des öffentlichen Schlüssels.

Privaten Schlüssel importieren

> Bitte lade den **privaten** Schlüssel deiner AG/WiG **nicht** auf ProtonMail hoch, sondern verwende zum Entschlüsseln von AG/WiG-E-Mails einen E-Mail-Client wie Thunderbird.

Thunderbird

> Thunderbird muss installiert und das entsprechende Postfach einrichtet sein.

PGP-Schlüsselpaar erzeugen

Dieser Abschnitt ist in folgenden Fällen für dich relevant:

- Du willst von deiner privaten E-Mail-Adresse verschlüsselte E-Mails verschicken.
- Du willst von deiner AG/WiG verschlüsselte Emails senden, aber ihr habt noch keinen Schlüssel.
  Dazu musst du dir in Thunderbird ein Schlüsselpaar für deine E-Mail-Adresse erzeugen.
  Hier findest du Anleitungen dazu:
- https://www.youtube.com/watch?v=NyOkgvVtZ10&t=101s (ab min 1:41)
- https://www.privacy-handbuch.de/handbuch_32j.htm

Schlüssel veröffentlichen

Wenn du anderen Menschen das Hinzufügen deines Schlüssel erleichtern willst, dann lade deinen **öffentlichen** Schlüssel bei keys.openpgp.org hoch.
Dazu bei Thunderbird den öffentlichen Schlüssel exportieren und auf https://keys.openpgp.org/upload hochladen. Klicke auf "verifizieren" und auf den Link in der E-Mail.
Wenn du einen Schlüssel für eine @letztegeneration.org-Adresse erstellt hast, dann kannst du deinen Schlüssel auch auf pgp.letztegeneration.org veröffentlichen.

Schreibe dazu eine E-Mail (am besten signiert bzw. verschlüsselt) an it-support@letztegeneration.org.

Öffentlichen Schlüssel importieren

Bevor zu mit jemanden verschlüsselt kommunizieren kannst, musst du den öffentlichen Schlüssel der anderen Person in Thunderbird importieren. Wenn du beispielsweise eine verschlüsselte E-Mail an legal@letztegeneration.org schreiben möchtest, musst du erst den öffentlichen Schlüssel von legal@letztegeneration.org importieren. Du kannst das auf verschiedene Weise machen. Nützlich dabei ist das Fenster "OpenPGP-Schlüssel verwalten" in Thunderbird. Du kannst es folgendermaßen öffnen: Rechtsklick auf dein Postfach » Einstellungen » Ende-zu-Ende-Verschlüsselung » OpenGPG-Schlüssel verwalten
Hier drei Wege, wie du einen öffentlichen Schlüssel importieren kannst

- Im Fenster 'OpenGPG-Schlüssel verwalten': Schlüsselserver » Schlüssel online finden: legal@letztegeneration.org » Suchen -> auf 'Akzeptiert' klicken
- Gehe auf die Webseite pgp.letztegeneration.org » Lade die Datei 'LG_AG_Legal-678A9D067546A58E11341B7E61B9ED32301F7A23.asc` herunter » Öffne die Datei mit Thunderbird. Oder klicke auf 'Datei' » 'Öffentlichen Schlüssel aus Datei importieren' im Fenster 'OpenPGP-Schlüssel verwalten'
- Schreibe eine unverschlüsselte E-Mail an legal@letztegneration.org und frage nach dem öffentlichen PGP-Schlüssel. Die Antwort-E-Mail enhält dann den öffentlichen Schlüssel im

Anhang.

Schaut euch auch gerne dieses Youtube-Video (zweite Hälfte ist relevant) an, darin wird das auch nochmal erklärt.

Privaten Schlüssel importieren

Diese Anleitung ist für dich relevant, wenn du in einer WiG/AG mitarbeitest, die PGP-Verschlüsselung nutzt. Es wird davon ausgegangen, dass der private Schlüssel für das entsprechende Postfach vorhanden ist.

1. Los gehts: Rechte Maustaste auf das Postfach, im Kontextmenü **Einstellungen** auswählen:

1. Links im Menü **Ende-zu-Ende-Verschlüsselung** auswählen:

1. Rechts **Schlüssel hinzufügen** auswählen:

1. Dann **Bestehenden OpenPGP-Schlüssel importieren** auswählen:

1. **Datei für den Import auswählen** klicken:

1. Die Datei mit dem privaten Schlüssel auswählen:

1. Das Passwort für den Schlüssel eingeben (das muss dir jemand von der WG/AG geben):

1. Einmal **Weiter** klicken:

1. Der Import ist jetzt abgeschlossen:

1. Jetzt muss der Schlüssel noch explizit ausgewählt werden, damit er in Zukunft für verschlüsselte E-Mails verwendet wird:

1. Und als letztes ein paar Einstellungen anpassen. Zum einen **Verschlüsselung für neue Nachrichten verwenden** und **Unverschlüsselte Nachrichten digital unterschreiben**.

1. Am besten auch weiter unten noch den Haken setzen bei "öffentlichen Schlüssel automatisch anhängen" (bzw. "Attach public key when adding an OpenPGP digital siganture"). Dann kann die andere Person den öffentlichen Schlüssel gleich importieren.

2. Fertig!

Signal auf dem Laptop nutzen

Signal auf dem Laptop nutzen

Installation von Signal Desktop

Es ist möglich, den Signal-Account auch auf dem Laptop zu nutzen (egal ob Windows, Linux oder Mac). Dazu sind folgende Schritte notwendig:

1. Signal Desktop von der Webseite herunterladen (auf der rechten Seite): https://signal.org/de/download/
2. Signal Desktop installieren: Dazu den heruntergeladenen Installer öffnen und durchklicken (weiter, weiter, ..., fertigstellen)
3. Signal Desktop öffnen (auf dem Desktop müsste eine Verknüpfung liegen, ansonsten im Startmenü danach suchen). Beim Start wird ein QR-Code angezeigt.
4. Den Signal Account auf dem Handy mit dem Laptop verknüpfen: Dazu die Signal App auf dem Mobiltelefon öffnen, rechts oben auf die drei Punkte klicken, Settings/Einstellungen => Linked Devices/verknüpfte Geräte und dann auf "Neues Gerät verknüpfen" ("Link a new device") => QR Code scannen => fertig.

Da du jetzt alle Signal Nachrichten auch auf dem Laptop hast: Schaue bitte, dass dein Laptop verschlüsselt ist. Mehr Infos zur Verschlüsselung findest du hier.

Mehrere Signal-Accounts gleichzeitig auf dem Laptop nutzen

Nehmen wir mal an, du hast zwei Signal Accounts, z. B. einen privaten und einen für die (Aktivismus-)Arbeit. Du kannst in Signal Desktop leider keinen zweiten Signal Account hinzufügen. Allerdings gibt es trotzdem wege, wie du auf deinem Laptop mehrere Signal Accounts nutzen kannst.

Variante 1 (ohne zusätzliche Software, dafür etwas hakelig)

Für Variante 1 musst du keine zusätzliche Software installieren. Die Video-Anleitung ist für Windows, die Idee dahinter funktioniert aber grundsätzlich auch für Mac/Linux:

Youtube Tutorial

Variante 2 (benötigt ein Tool)

Es gibt ein Tool Namens `signal-account-switcher`. Damit kannst du am Laptop vier zusätzliche Signal Desktop Accounts nutzen.

Wie du das Tool herunterladen und starten kannst, wird hier beschrieben: https://github.com/kmille/signal-account-switcher/blob/main/README.md

Die Anleitung ist auf Englisch. Wenn du sie in deutscher Sprache brauchst, kannst du den Google Übersetzer nutzen und die URL von oben einfügen, um die Anleitung auf Deutsch übersetzen zu lassen.

Mehrere Signal Accounts auf Android

Es kann sehr praktisch sein, 2 verschiedene Signal-Accounts auf dem Handy zu haben.

Beispielsweise neben dem privaten Account noch einen Account für alle LG-Sachen, den kann man dann nämlich einfach ausmachen, ist für Freund*innen aber trotzdem erreichbar. Das verhindert, dass man die ganze Zeit unter Strom steht, fördert das Abschalten und ist deswegen eine sehr gute Burnout-Prävention!

Signal

Jeder Signal-Account ist mit einem bestimmten Smartphone verknüpft. Du kannst ihn zwar mit bis zu 5 PCs teilen (Signal-Desktop), aber der Account befindet sich auf dem Smartphone, und normalerweise kann deswegen nur ein einziger Signal-Account pro Handy genutzt werden.

Es gibt aber Möglichkeiten, bis zu 4 verschiedene Accounts auf einem Android-Handy zu betreiben:

1 weiterer Account (Molly)

Du kannst sehr einfach einen zusätzlichen Account pro Handy einrichten, indem du die App Molly nutzt. Molly ist eine verbesserte Version der normalen Signal-App, welche sicherer verschlüsselt ist. Du kannst beide Apps parallel nutzen und in jeder einen eigenen Signal-Account haben. Molly ist also Signal mit einem anderen Logo plus ein paar Extras.

Bewährt hat sich eine Aufteilung in einen Arbeits- (Molly) und einen Privat-Account (normale Signal-App).

Für jeden Account brauchst du eine eigene Nummer. Die SIM-Karte muss sich dafür nicht in deinem Handy befinden, du brauchst sie nur einmal, um eine SMS zu empfangen für die Account-Erstellung, danach solltest du die sicher irgendwo verwahren und alle paar Monate etwas Guthaben

aufladen, damit die Nummer nicht verfällt (sonst hast du nach Verlust deines Handys keine Möglichkeit, deinen Account auf ein neues Handy zu übertragen). Aldi Talk ist anscheinend sehr einfach und günstig, aber jede andere SIM geht natürlich auch.

> *Auf https://sms-man.com/ kann man sich, ggf. sogar anonym, ein "einzelnes SMS-Empfangen" kaufen. Ist dann deutlich billiger als mit einer SIM-Karte. Allerdings ist so dein Account garantiert verloren, sobald du das Handy verlierst. Das liegt daran, dass man da mit einer Nummer wirklich nur EIN MAL eine Sms empfangen kann.*

Alternativ kannst du dir auch bei Easybell eine Voice-Over-IP-Telefonnummer holen (https://www.easybell.de/voice-over-ip/). Das kostet ca 10 Euro im Jahr. Das heißt: Du hast eine zusätzliche Telefonnummer, mit der du telefonieren kannst. Dazu installierst du dir auf dem Computer oder Smartphone eine VoIP-App (z. B. Zoiper https://www.zoiper.com/en/voip-softphone/download/current) , mit der du die Telefonnumer nutzen kannst.

Du kannst die (Festnetz-)Nummer von Easybell auch verwenden, um damit eine Signal-Account zu registrieren. Dann bekommst du die SMS als Sprachanruf. Danach kannst du die App wieder deinstallieren. Der Vorteil daran: Wenn dein Handy defekt ist und du Signal auf einem neuen Gerät instsallieren möchtest, brauchst du wieder Zugriff auf die hinterlegte Telefonnummer. Dann kannst du wieder die VoIP-App installieren und die SMS empfangen.

Ihr könnt auch auf dem Laptop beliebig viele Signal-Accounts nutzen, siehe unsere Dokumentation hier.

Zum Thema Anonymität

Signal lässt sich ja mittlerweile auch nutzen, ohne dass die Telefonnummer des Signal-Accounts angezeigt wird. Die Signal-Server kennen keine Metadaten. Heißt: Signal weiß nicht, wer wann mit wem kommuniziert. Signal hat auch keine Inhaltsdaten (Inhalt der Nachrichten, da Ende zu Ende verschlüsselt). Signal kennt allerdings den **aktuellen** Signal-Nutzernamen und die damit verbundene Telefonnummer. Heißt: Ihr könnt Signal anonym nutzen, selbst wenn die Telefonnummer auf euren Namen registriert ist - solange ihr den Nutzernamen geheim haltet. Den könnt ihr auch jederzeit löschen oder ändern, wenn ihr ihn verwendet habt. Wenn die Polizei mit alten Signal-Nutzernamen bei Signal anklopft, kann Signal das keinem Account mehr zuweisen. Anstatt euren Signal-Nutzernamen zu teilen, könnt ihr auch einen Link generieren und den teilen. Der Link enthält nicht euren Signal-Nutzernamen.

Installation

Anleitung kurz:

Installiere f-droid, füge die Paketquellen von Molly zu f-droid hinzu und installiere dann Molly.

Anleitung lang:

1. Lade den alternativen App-Store fdroid herunter.
2. Installiere f-droid, indem du die .apk-Datei öffnest, die du runtergeladen hast.
3. Lasse “Installation von Apps aus unbekannten Quellen” zu, wenn du danach gefragt wirst.
4. Erlaube ggf. “Apps aus dieser Quelle installieren”.
5. Gehe auf https://molly.im/download/fdroid/ und wähle Molly (wenn du gerade am Handy liest), oder scanne den QR-Code, wenn du den Artikel am PC liesst. Wähle Molly, nicht Molly-FOSS, außer du weißt, was du tust (zB keine Playdienste).
6. Öffne f-droid und wische vom oberen Rand nach unten; damit lädst du Infos über alle verfügbaren Apps, dies kann bis zu 2 Minuten dauern.
7. Suche in f-droid nach Molly und installiere es. Lass dafür ggf. wieder “installieren aus dieser Quelle” für f-droid zu.

Molly einrichten

Jetzt ist Molly bereit und du kannst die App ganz normal wie Signal einrichten.

Am Anfang wirst du jedoch gefragt, ob du eine zusätzliche Passwortverschlüsserlung nutzen möchtest, deine Wahl kann später nicht mehr geändert werden. Für sensible Accounts (z.B. PP) ist das sinnvoll, ansonsten ist es wie bei der normalen Signal-App.

Erstelle eine Signal-PIN, die du dir wirklich sicher merken kannst. Ansonsten speichere sie in deinen sicheren Passwortmanager, aber schreib sie nicht auf einen Zettel! Dieser kann nach einer Hausdurchsuchung von der Polizei genutzt werden, um Nachrichten an dich abzufangen.

Zeitliche Beschränkung für Nachrichten

Damit du nach der Arbeit deine Ruhe genießen kannst, solltest du Benachrichtigungsprofile erstellen welche festlegen, wann du wie erreicht werden kannst. Diese bieten 2 Optionen:

- festlegen, für was und welche Kontakte du Benachrichtigungen erhalten möchtest
- festlegen, wann sich das Profil automatisch aktiviert.

Um ein Profil zu erstellen, öffne oben rechts das Menü > Benachrichtigungsprofil > neues Profil. Hier kannst du Kontakte festlegen, von denen du Nachrichten erhalten willst, während dieses Profil aktiv ist. Im nächsten Schritt kannst du einen Zeitplan erstellen, der festlegt, zu welchen Tagen und Uhrzeiten dieses Profil automatisch aktiviert wird (du kannst dies jederzeit deaktivieren, um wieder normal Benachrichtigungen zu erhalten).

Bewährt hat sich eine Kombination aus 2 Benachrichtigungsprofilen:

- ein Nacht-Profil: wenn aktiv bekommst du gar keine Benachrichtigungen; aktivieren wenn du nicht arbeitest
- ein Tag-Profil: hier kannst du einstellen, dass du benachrichtigt wirst, wenn z.B.:
  - du in einem Beitrag markiert wirst
  - du angerufen wirst
  - du Nachrichten von Personen oder Gruppen bekommst, die du in deine Erlaubt-Liste aufgenommen hast

Sinnvoll ist, Profile dann aktiviert zu haben, wenn du nicht (zu doll) kontaktiert/gestört werden willst. Stelle dafür für jedes Profil einen eigenen Zeitplan ein (z.B. “Keine Benachrichtigungen”: 18:00-10:00, und “Nur Wichtiges”: 10:00-18:00).

Möchtest du normal alle Benachrichtigungen erhalten, deaktiviere das Profil einfach durch Antippen Das Menü öffnet sich durch Tippen auf das Mond-Symbol oben rechts. Wenn tagsüber ein “Nur Anrufe”-Profil aktiviert ist, kannst du es von Hand ausschalten, sobald du anfängst zu arbeiten. Du kannst den Zeitplan auch an feste Arbeitszeiten anpassen, falls du sowas hast.

2 weitere Accounts (App-Klone)

Einige Hersteller bieten eine Dual-App-Funktion, um mehrere Accounts auf einem Handy zu betreiben. Suche im Netz, ob dein Gerät über diese Funktion verfügt. Ab Android 14 könnte diese Option standardmäßig auf vielen Geräten vorhanden sein.

Du kannst diese Funktion auch nutzen, um Signal und Molly zu klonen, so dass du dann 4 Accounts hast. Du könntest damit auch auf die Nutzung von Molly verzichten und 2x Signal nutzen, Molly ist aber sinnvoller, da Molly über eine leicht bessere Verschlüsselung und Sicherheitsmechanismen verfügt, die im Falle einer Hausdurchsuchung einen Vorteil bieten.

Du kannst die Funktion einfach in den Android-Einstellungen aktivieren:

Samsung: Einstellungen > Erweiterte Funktionen > Dual Messenger

Huawei: Einstellungen > Apps > App Twin

LG: Einstellungen > Allgemein > Dual App

Daraufhin sollte ein Menü mit allen klonbaren Apps angezeigt werden, dort kannst du Signal (und ggf. weitere zu klonende Apps) einfach auswählen und verdoppeln.

D A N G E R Z O N E

Die folgenden Möglichkeiten sind schwierig, können nerven und ggf. zu Problemen führen und richten sich ausschließlich an fortgeschrittene Benutzer:innen. Diese Möglichkeiten verlassen die technische Komfort-Zone und sind eher für Sonder-Anwendungsfälle gedacht.

1 Unendlich viele Accounts nutzen

Möglich ist es (für die meisten aber nicht sinnvoll), einfach weitere Benutzerkonten auf dem Handy anzulegen. Wird ein Handy von mehreren Leuten genutzt, so kann jede:r ein ganz eigenes Profil haben, mit eigenen Apps, Daten, Einstellungen etc. Alle oben beschriebenen Tricks können pro

angelegtem Nutzerprofil wiederholt werden, theoretisch bis der Speicher voll ist.

Davon ist aber abzuraten, da das Einloggen in ein anderes Profil aufwändig ist, Zeit kostet, alle persönlichen Einstellungen nochmal vorgenommen werden müssen, man keinen Zugriff auf die persönlichen Daten im eigentlichen Profil hat. Im Alltag kann man keine Benachrichtigungen bekommen, dafür muss dann erst das Profil gewechselt werden, und im Zweitprofil gibt es dann wieder keine persönlichen Nachrichten aus dem Hauptaccount.

Diese Möglichkeit ist nur für den Notfall, oder für Usecases, in denen ein Signal-Konto nur sehr selten bei Bedarf angeguckt werden muss (z.B. Signal-Account für eine befreundete Person ohne Smartphone, die ihren Signal-Account ausschlieeßlich vom PC aus nutzt und ab und zu Bestätigungen auf dem Handy empfangen muss, um Signal-Desktop auf einem neuen Computer zu verknüpfen, wenn der alte beschlagnahmt wurde).

2 weitere Accounts (Arbeitsprofil)

Wer es unbedingt braucht, kann mit etwas Arbeit noch 2 Signal-Accounts hinzufügen. In Kombination mit einem eventuell vorhandenen Appklon-Feature sollten sich 6 Signal-Accounts auf einem Gerät installieren lassen. Das ist etwas umständlich, und setzt ein Mindestmaß an Technik-Verständnis voraus.

Für mehr Accounts nutzen wir das Workprofile-Feature von Android, um Signal und Molly zu klonen. Eigentlich ist ein Workprofile ein von einer Firma verwaltetes Profil, um den Angestellten Daten und Apps zur Verfügung zu stellen. Die Daten und Apps des Arbeitsprofils sind im Handy getrennt von den privaten; Andoid denkt also, dass eine Signal-App privat ist und die andere für eine Firma. Du kannst damit auch jede andere App auf deinem Handy verdoppeln.

Wir können die App Shelter nutzen, um ein Workprofile auf unserem Gerät auch ohne Firma zu erstellen. Shelter sollte von f-droid installiert werden, da die f-droid-Version mehr Features hat (wichtig). Mit Shelter lässt sich jede App in das Arbeitsprofil klonen, sodass wir zwei getrennte Installationen derselben App haben, die in 2 voneinander getrennten Bereichen des Handys existieren, getrennte Speicher haben etc.

Das Ganze funktioniert aber nicht immer reibungslos und kann etwas nerven, denn im Arbeitsprofil existieren nur Apps, die wir hineinkopieren. Arbeits-Signal benötigt also auch einen Arbeits-Dateimanager, eine Arbeits-Galerie etc. Jede App die wir in Kombination mit Signal nutzen muss dort hinkopiert werden, das gilt auch für selbstinstallierte Tastaturen, microG (falls du ein Custom ROM nutzt), evt. sogar Google Playservices.

Das Datei-Transfer-Feature von Shelter erlaubt allerdings den Zugriff von Arbeits-Signal auf private Dateien und andersrum, du solltest es aktivieren.

Freeze: Nach Benutzung können Arbeits-Apps “eingefroren” werden, d.h. sie werden komplett beendet und nicht ausgeführt, bis du sie wieder aktivierst (kann auch ganz praktisch sein für sehr doll spionierende Apps). Füge dazu alle Arbeits-Apps zur Autofreeze-Liste hinzu. Erzeuge eine Verknüpfung zum Autofreeze-Button auf deiner Arbeitsfläche, diese Verknüpfung funktioniert dann wie ein Ausschalter für alle Arbeits-Apps

Mehr Details gibts hier: https://www.youtube.com/watch?v=yFZc2MKmPzE

Wissenswertes über Signal

"Signal Sicher benutzen"? Ich dachte Signal ist schon sicher!

So einfach ist das nicht. Signal benutzt sehr sichere Verschlüsselung. Aber es gibt Fallstricke. Bitte achtet darauf, dass eure Geräte (auch der Laptop!) verschlüsselt sind. Anleitungen findet ihr hier. Wenn die Polizei ein Handy beschlagnahmt und dieses benutzen kann, weil keine PIN eingestellt ist, helfen (quasi) keine der Sicherheitsmechanismen etwas.

Warum Signal und nicht Telegram/WhatsApp/Sonstwas?

Signal wurde von einem Hacker mit dem Pseudonym Moxie Marlinspike entwickelt. Moxie ist ein sehr bekannter und anerkannter Hacker und bereits seit mehr als einem Jahrzent bekannt für seine Recherchen zu Angriffen auf Verschlüsselung. Die Vorteile von Signal sind:

- Signal hat ein sehr sicheres Design und ist quelloffen (Open Source)
- Hinter Signal steht die "Signal Foundation", eine gemeinnützige Organisation, die rein auf Spenden basiert. Es gibt daher für Signal auch kein Geschäftsinteresse, auf diese Daten zugreifen zu wollen
- Durch “Verschwindende Nachrichten” werden Nachrichten automatisch gelöscht
- Signal-Chats können gebackuped werden (aktuell leider nur auf Android)

Signal kennt keine Metadaten (wer wann mit wem kommuniziert). Signal kennt auch keine Inhalts-Daten (was wurde kommuniziert, da die Chats Ende-zu-Ende verschlüsselt sind). Signal ist sehr transparent und veröffentlicht Anfragen der Polizei und Signal's Antwort (Beispiel).

Die Chats bei Telegram sind standardmäßig nicht verschlüsselt. Auch Gruppenchats sind nicht verschlüsselt. Um bei Telegram Ende-zu-Ende-Verschlüsselung zu nutzen, müssen explizit “private Chats” erstellt werden. Telegram kooperiert auch mit den Behörden (Tagesschau-Artikel).

Die Chats bei WhatsApp sind angeblich Ende-zu-Ende verschlüsselt. Allerdings kann das nicht verifiziert werden, da der Code von WhatsApp nicht öffentlich ist. Außerdem steckt hinter WhatsApp die Firma Meta (Facebook), die bekannt dafür ist, Daten zu sammeln.

Warum Anrufe über das Mobilfunk und SMS unsicher sind

Mit einem richterlichen Beschluss bekommt die Polizei sehr leicht Zugriff auf alle SMS-Inhalte sowie Telefongespräche. Allerdings ist dafür ein 129er-Verfahren notwendig (kriminelle Vereinigung), Ermittlungsverfahren wegen Straßenblockaden reichen dafür nicht aus.

Falls ein Beschluss (LG Beispiel) zur Überwachung eurer Telefonate vorliegt, wird fast immer die normale Telekommunikationsüberwachung (TKÜ) eingesetzt. Das Abhören der Kommunikation erfolgt über den Mobilfunkprovider und ihr könnt es nicht bemerken. Schlechter Empfang oder komische Geräusche sind kein Zeichen von Überwachung. Der Provider zeichnet die Gespräche auf und schickt sie dann der Polizei in Form von MP3-Dateien.

Das bedeutet, dass Ende-zu-Ende-verschlüsselnde Messenger-Apps einschließlich Signal weiterhin sicher sind, solange keine Quellen-TKÜ (Staatstrojaner) eingesetzt wird, was sehr selten passiert.

PIN für Signal einrichten

Es ist sehr wichtig, dass du in Signal eine PIN einrichtest. Diese schützt vor unberechtigter Neuregistrierung. Dein Netz-Provider muss auf richterlichen Beschluss hin SMS an die Polizei umleiten. Heißt: Die Polizei kann deinen Signal Account übernehmen, indem sie deinen Account auf einem anderen Handy einrichtet. Dies ist nicht möglich, wenn du eine Signal-PIN hinterlegst.

Wie du die PIN einrichtest, wird in der Signal Dokumentation gut erklärt: https://support.signal.org/hc/de/articles/360007059792-Signal-PIN

Am besten speicherst du deine PIN in deinem Passwort-Manager.

Verschwindende Nachrichten/Disappearing Messages

"Verschwindende Nachrichten" bedeuten: Nach einer eingestellten Zeitspanne (z. B. einer Woche) werden die Nachrichten auf allen Geräten gelöscht. Es lässt sich auch einstellen, dass das Feature für neue Chats automatisch aktiviert ist. Für die genaue Anleitung empfehlen wir die offizielle Signal Dokumentation: https://support.signal.org/hc/de/articles/360007320771-Verschwindende-Nachrichten-festlegen-und-verwalten

Einladungslinks für Gruppen: Die Gruppenbeschreibung ist öffentlich einsehbar

Wenn ihr für Gruppen Einladungslinks verwendet, macht euch bewusst: Wer den Link hat, kann auch die Gruppenbeschreibung lesen - auch ohne vom Admin der Gruppe hinzugefügt worden zu sein. Grundsätzlich solltet ihr keine geheimen Informationen (Links mit Zugangs-Berechtigungen oder Passwörter) in Gruppen nutzen, die ihr öffentlich teilt. Mehr Infos dazu hier:

https://blaeul.de/sonnenschein/signalgruppen-und-einladungslinks

Handynummer? Anonymität mit Signal

Jeder Signal Account benötigt eine Handynummer. Deine Handynummer ist mit deiner Person verbunden. Mittlerweile kann man einstellen, dass die eigene Handynummer in Signal nicht mehr angezeigt wird. Lest euch bitte den Signal Artikel dazu. Er klärt viele Fragen zu dem Thema: https://support.signal.org/hc/de/articles/6712070553754-Datenschutz-bei-Telefonnummern-und-Nutzernamen

Denkt auch daran, was passsiert, wenn ihr den Zugang zu eurem Signal Account verliert (Smartphone defekt/beschlagnahmt/verloren). Wenn ihr die Handynummern eurer Friends nicht mehr habt und euer Signal weg ist, könnt ihr die Menschen nicht mehr kontaktieren.

E-Mails per PGP verschlüsseln

E-Mail-Verschlüsselung Einrichten

Wenn du eine E-Mail an z.B. legal@letztegeneration.org schickst, dann kannst du diese vor dem Abschicken auf deinem Gerät verschlüsseln. So können dein und unser Mailprovider sowie dein und unser Internetprovider nicht mitlesen.

Diese Anleitung erklärt wie die PGP-Verschlüsselung für den E-Mail-Anbieter ProtonMail oder den E-Mail-Client Thunderbird eingerichtet werden kann.

> **ProtonMail** ist ein Anbieter mit dem man direkt im Browser PGP-verschlüsselte E-Mails senden und empfangen kann. ProtonMail ist relativ einstiegsfreundlich und kann **für deine private E-Mail-Adresse** verwendet werden, um damit verschlüsselt mit AGs/WiGs zu kommunizieren.

> PGP-Verschlüsselung funktioniert aktuell nicht mit unserem Webmail.

> Wenn du bei einem **anderen Anbieter** bist oder mit deiner **AG/WiG-Adresse** verschlüsselte E-Mails senden und empfangen willst, brauchst du einen E-Mail-Client mit PGP-Unterstützung wie z.B. **Thunderbird**.

Die Anleitung behandelt folgende Themen (jeweils für ProtonMail und Thunderbird):

- PGP-Verschlüsselung einrichten: Schlüsselpaar erzeugen und öffentlichen Schlüssel verbreiten
- Öffentlichen Schlüssel importieren (brauchst du, um an diese E-Mail eine verschlüsselte Nachricht zu schicken)
- Nur Thunderbird: Es existiert bereits ein Schlüsselpaar, z.B. von deiner AG/WiG (du bekommst privaten und öffentlichen Schlüssel, die du importieren möchtest)

Bei Fragen wende dich bitte an die IT-AG: it-support@letztegeneration.org.

ProtonMail

> ProtonMail ist zwar sehr einstiegsfreundlich, aber aufgrund der webbasierten Architektur nicht so sicher wie ein nativer E-Mail-Client mit PGP-Verschlüsselung wie z.B. Thunderbird.

PGP-Schlüsselpaar erzeugen

ProtonMail generiert automatisch ein Schlüsselpaar für deinen Account.

Unter https://account.proton.me/u/0/mail/encryption-keys kannst du deinen Schlüssel sehen.

Schlüssel veröffentlichen

Wenn du anderen Menschen das Hinzufügen deines Schlüssel erleichtern willst, dann lade deinen **öffentlichen** Schlüssel bei keys.openpgp.org hoch.

Dazu hier deinen Schlüssel exportieren und auf https://keys.openpgp.org/upload hochladen. Klicke auf "verifizieren" und auf den Link in der E-Mail.

Öffentlichen Schlüssen importieren

Bei ProtonMail muss der öffentliche Schlüssel der:des Empfängerin:Empfängers im Adressbuch hinterlegt werden. So geht es:

1. In die Weboberfläche einloggen, bis du deinen Posteingang siehst.
2. Oben rechts auf das Kontakte Icon mit den 2 Köpfen klicken:

ProtonMail-Adressbuch

1. nach legal@letztegeneration.org suchen beziehungsweise diese Adresse anlegen.
2. Den Kontakt öffnen und auf das Zahnrad klicken.
3. Erweiterte PGP-Einstellungen einblenden.
4. Den öffentlichen Schlüssel hier herunterladen:
   - AGs und WiGs: pgp.letztegeneration.org/
   - Umwelt-Treuhandfond
   - restliche Welt: https://keys.openpgp.org
5. den öffentlichen Schlüssel in ProtonMail wieder hochladen (im Bild rot 1.).
6. die Verschlüsselung immer aktivieren „E-Mails verschlüsseln“ (im Bild rot 2.).

   Nun sollte es so aussehen (nur mit letztegeneration.org statt letztegeneration.de, der Screenshot ist etwas älter):

Adressbucheintrag in ProtonMail

1. Nach Klick auf das Zahnrad öffnet sich dieser Dialog zum Hochladen des öffentlichen Schlüssels.

Privaten Schlüssel importieren

> Bitte lade den **privaten** Schlüssel deiner AG/WiG **nicht** auf ProtonMail hoch, sondern verwende zum Entschlüsseln von AG/WiG-E-Mails einen E-Mail-Client wie Thunderbird.

Thunderbird

> Thunderbird muss installiert und das entsprechende Postfach einrichtet sein.

PGP-Schlüsselpaar erzeugen

Dieser Abschnitt ist in folgenden Fällen für dich relevant:

- Du willst von deiner privaten E-Mail-Adresse verschlüsselte E-Mails verschicken.
- Du willst von deiner AG/WiG verschlüsselte Emails senden, aber ihr habt noch keinen Schlüssel.
  Dazu musst du dir in Thunderbird ein Schlüsselpaar für deine E-Mail-Adresse erzeugen.
  Hier findest du Anleitungen dazu:
- https://www.youtube.com/watch?v=NyOkgvVtZ10&t=101s (ab min 1:41)
- https://www.privacy-handbuch.de/handbuch_32j.htm

Schlüssel veröffentlichen

Wenn du anderen Menschen das Hinzufügen deines Schlüssel erleichtern willst, dann lade deinen **öffentlichen** Schlüssel bei keys.openpgp.org hoch.
Dazu bei Thunderbird den öffentlichen Schlüssel exportieren und auf https://keys.openpgp.org/upload hochladen. Klicke auf "verifizieren" und auf den Link in der E-Mail.
Wenn du einen Schlüssel für eine @letztegeneration.org-Adresse erstellt hast, dann kannst du deinen Schlüssel auch auf pgp.letztegeneration.org veröffentlichen.

Schreibe dazu eine E-Mail (am besten signiert bzw. verschlüsselt) an it-support@letztegeneration.org.

Öffentlichen Schlüssel importieren

Bevor zu mit jemanden verschlüsselt kommunizieren kannst, musst du den öffentlichen Schlüssel der anderen Person in Thunderbird importieren. Wenn du beispielsweise eine verschlüsselte E-Mail an legal@letztegeneration.org schreiben möchtest, musst du erst den öffentlichen Schlüssel von legal@letztegeneration.org importieren. Du kannst das auf verschiedene Weise machen. Nützlich dabei ist das Fenster "OpenPGP-Schlüssel verwalten" in Thunderbird. Du kannst es folgendermaßen öffnen: Rechtsklick auf dein Postfach » Einstellungen » Ende-zu-Ende-Verschlüsselung » OpenGPG-Schlüssel verwalten
Hier drei Wege, wie du einen öffentlichen Schlüssel importieren kannst

- Im Fenster 'OpenGPG-Schlüssel verwalten': Schlüsselserver » Schlüssel online finden: legal@letztegeneration.org » Suchen -> auf 'Akzeptiert' klicken
- Gehe auf die Webseite pgp.letztegeneration.org » Lade die Datei 'LG_AG_Legal-678A9D067546A58E11341B7E61B9ED32301F7A23.asc` herunter » Öffne die Datei mit Thunderbird. Oder klicke auf 'Datei' » 'Öffentlichen Schlüssel aus Datei importieren' im Fenster 'OpenPGP-Schlüssel verwalten'
- Schreibe eine unverschlüsselte E-Mail an legal@letztegneration.org und frage nach dem öffentlichen PGP-Schlüssel. Die Antwort-E-Mail enhält dann den öffentlichen Schlüssel im

Anhang.

Schaut euch auch gerne dieses Youtube-Video (zweite Hälfte ist relevant) an, darin wird das auch nochmal erklärt.

Privaten Schlüssel importieren

Diese Anleitung ist für dich relevant, wenn du in einer WiG/AG mitarbeitest, die PGP-Verschlüsselung nutzt. Es wird davon ausgegangen, dass der private Schlüssel für das entsprechende Postfach vorhanden ist.

1. Los gehts: Rechte Maustaste auf das Postfach, im Kontextmenü **Einstellungen** auswählen:

1. Links im Menü **Ende-zu-Ende-Verschlüsselung** auswählen:

1. Rechts **Schlüssel hinzufügen** auswählen:

1. Dann **Bestehenden OpenPGP-Schlüssel importieren** auswählen:

1. **Datei für den Import auswählen** klicken:

1. Die Datei mit dem privaten Schlüssel auswählen:

1. Das Passwort für den Schlüssel eingeben (das muss dir jemand von der WG/AG geben):

1. Einmal **Weiter** klicken:

1. Der Import ist jetzt abgeschlossen:

1. Jetzt muss der Schlüssel noch explizit ausgewählt werden, damit er in Zukunft für verschlüsselte E-Mails verwendet wird:

1. Und als letztes ein paar Einstellungen anpassen. Zum einen **Verschlüsselung für neue Nachrichten verwenden** und **Unverschlüsselte Nachrichten digital unterschreiben**.

1. Am besten auch weiter unten noch den Haken setzen bei "öffentlichen Schlüssel automatisch anhängen" (bzw. "Attach public key when adding an OpenPGP digital siganture"). Dann kann die andere Person den öffentlichen Schlüssel gleich importieren.

2. Fertig!

Wissenswertes über Signal

"Signal Sicher benutzen"? Ich dachte Signal ist schon sicher!

So einfach ist das nicht. Signal benutzt sehr sichere Verschlüsselung. Aber es gibt Fallstricke. Bitte achtet darauf, dass eure Geräte (auch der Laptop!) verschlüsselt sind. Anleitungen findet ihr hier. Wenn die Polizei ein Handy beschlagnahmt und dieses benutzen kann, weil keine PIN eingestellt ist, helfen (quasi) keine der Sicherheitsmechanismen etwas.

Warum Signal und nicht Telegram/WhatsApp/Sonstwas?

Signal wurde von einem Hacker mit dem Pseudonym Moxie Marlinspike entwickelt. Moxie ist ein sehr bekannter und anerkannter Hacker und bereits seit mehr als einem Jahrzent bekannt für seine Recherchen zu Angriffen auf Verschlüsselung. Die Vorteile von Signal sind:

- Signal hat ein sehr sicheres Design und ist quelloffen (Open Source)
- Hinter Signal steht die "Signal Foundation", eine gemeinnützige Organisation, die rein auf Spenden basiert. Es gibt daher für Signal auch kein Geschäftsinteresse, auf diese Daten zugreifen zu wollen
- Durch “Verschwindende Nachrichten” werden Nachrichten automatisch gelöscht
- Signal-Chats können gebackuped werden (aktuell leider nur auf Android)

Signal kennt keine Metadaten (wer wann mit wem kommuniziert). Signal kennt auch keine Inhalts-Daten (was wurde kommuniziert, da die Chats Ende-zu-Ende verschlüsselt sind). Signal ist sehr transparent und veröffentlicht Anfragen der Polizei und Signal's Antwort (Beispiel).

Die Chats bei Telegram sind standardmäßig nicht verschlüsselt. Auch Gruppenchats sind nicht verschlüsselt. Um bei Telegram Ende-zu-Ende-Verschlüsselung zu nutzen, müssen explizit “private Chats” erstellt werden. Telegram kooperiert auch mit den Behörden (Tagesschau-Artikel).

Die Chats bei WhatsApp sind angeblich Ende-zu-Ende verschlüsselt. Allerdings kann das nicht verifiziert werden, da der Code von WhatsApp nicht öffentlich ist. Außerdem steckt hinter WhatsApp die Firma Meta (Facebook), die bekannt dafür ist, Daten zu sammeln.

Warum Anrufe über das Mobilfunk und SMS unsicher sind

Mit einem richterlichen Beschluss bekommt die Polizei sehr leicht Zugriff auf alle SMS-Inhalte sowie Telefongespräche. Allerdings ist dafür ein 129er-Verfahren notwendig (kriminelle Vereinigung), Ermittlungsverfahren wegen Straßenblockaden reichen dafür nicht aus.

Falls ein Beschluss (LG Beispiel) zur Überwachung eurer Telefonate vorliegt, wird fast immer die normale Telekommunikationsüberwachung (TKÜ) eingesetzt. Das Abhören der Kommunikation erfolgt über den Mobilfunkprovider und ihr könnt es nicht bemerken. Schlechter Empfang oder komische Geräusche sind kein Zeichen von Überwachung. Der Provider zeichnet die Gespräche auf und schickt sie dann der Polizei in Form von MP3-Dateien.

Das bedeutet, dass Ende-zu-Ende-verschlüsselnde Messenger-Apps einschließlich Signal weiterhin sicher sind, solange keine Quellen-TKÜ (Staatstrojaner) eingesetzt wird, was sehr selten passiert.

PIN für Signal einrichten

Es ist sehr wichtig, dass du in Signal eine PIN einrichtest. Diese schützt vor unberechtigter Neuregistrierung. Dein Netz-Provider muss auf richterlichen Beschluss hin SMS an die Polizei umleiten. Heißt: Die Polizei kann deinen Signal Account übernehmen, indem sie deinen Account auf einem anderen Handy einrichtet. Dies ist nicht möglich, wenn du eine Signal-PIN hinterlegst.

Wie du die PIN einrichtest, wird in der Signal Dokumentation gut erklärt: https://support.signal.org/hc/de/articles/360007059792-Signal-PIN

Am besten speicherst du deine PIN in deinem Passwort-Manager.

Verschwindende Nachrichten/Disappearing Messages

"Verschwindende Nachrichten" bedeuten: Nach einer eingestellten Zeitspanne (z. B. einer Woche) werden die Nachrichten auf allen Geräten gelöscht. Es lässt sich auch einstellen, dass das Feature für neue Chats automatisch aktiviert ist. Für die genaue Anleitung empfehlen wir die offizielle Signal Dokumentation: https://support.signal.org/hc/de/articles/360007320771-Verschwindende-Nachrichten-festlegen-und-verwalten

Einladungslinks für Gruppen: Die Gruppenbeschreibung ist öffentlich einsehbar

Wenn ihr für Gruppen Einladungslinks verwendet, macht euch bewusst: Wer den Link hat, kann auch die Gruppenbeschreibung lesen - auch ohne vom Admin der Gruppe hinzugefügt worden zu sein. Grundsätzlich solltet ihr keine geheimen Informationen (Links mit Zugangs-Berechtigungen oder Passwörter) in Gruppen nutzen, die ihr öffentlich teilt. Mehr Infos dazu hier:

https://blaeul.de/sonnenschein/signalgruppen-und-einladungslinks

Handynummer? Anonymität mit Signal

Jeder Signal Account benötigt eine Handynummer. Deine Handynummer ist mit deiner Person verbunden. Mittlerweile kann man einstellen, dass die eigene Handynummer in Signal nicht mehr angezeigt wird. Lest euch bitte den Signal Artikel dazu. Er klärt viele Fragen zu dem Thema: https://support.signal.org/hc/de/articles/6712070553754-Datenschutz-bei-Telefonnummern-und-Nutzernamen

Denkt auch daran, was passsiert, wenn ihr den Zugang zu eurem Signal Account verliert (Smartphone defekt/beschlagnahmt/verloren). Wenn ihr die Handynummern eurer Friends nicht mehr habt und euer Signal weg ist, könnt ihr die Menschen nicht mehr kontaktieren.

Signal auf dem Laptop nutzen

Signal auf dem Laptop nutzen

Installation von Signal Desktop

Es ist möglich, den Signal-Account auch auf dem Laptop zu nutzen (egal ob Windows, Linux oder Mac). Dazu sind folgende Schritte notwendig:

1. Signal Desktop von der Webseite herunterladen (auf der rechten Seite): https://signal.org/de/download/
2. Signal Desktop installieren: Dazu den heruntergeladenen Installer öffnen und durchklicken (weiter, weiter, ..., fertigstellen)
3. Signal Desktop öffnen (auf dem Desktop müsste eine Verknüpfung liegen, ansonsten im Startmenü danach suchen). Beim Start wird ein QR-Code angezeigt.
4. Den Signal Account auf dem Handy mit dem Laptop verknüpfen: Dazu die Signal App auf dem Mobiltelefon öffnen, rechts oben auf die drei Punkte klicken, Settings/Einstellungen => Linked Devices/verknüpfte Geräte und dann auf "Neues Gerät verknüpfen" ("Link a new device") => QR Code scannen => fertig.

Da du jetzt alle Signal Nachrichten auch auf dem Laptop hast: Schaue bitte, dass dein Laptop verschlüsselt ist. Mehr Infos zur Verschlüsselung findest du hier.

Mehrere Signal-Accounts gleichzeitig auf dem Laptop nutzen

Nehmen wir mal an, du hast zwei Signal Accounts, z. B. einen privaten und einen für die (Aktivismus-)Arbeit. Du kannst in Signal Desktop leider keinen zweiten Signal Account hinzufügen. Allerdings gibt es trotzdem wege, wie du auf deinem Laptop mehrere Signal Accounts nutzen kannst.

Variante 1 (ohne zusätzliche Software, dafür etwas hakelig)

Für Variante 1 musst du keine zusätzliche Software installieren. Die Video-Anleitung ist für Windows, die Idee dahinter funktioniert aber grundsätzlich auch für Mac/Linux:

Youtube Tutorial

Variante 2 (benötigt ein Tool)

Es gibt ein Tool Namens `signal-account-switcher`. Damit kannst du am Laptop vier zusätzliche Signal Desktop Accounts nutzen.

Wie du das Tool herunterladen und starten kannst, wird hier beschrieben: https://github.com/kmille/signal-account-switcher/blob/main/README.md

Die Anleitung ist auf Englisch. Wenn du sie in deutscher Sprache brauchst, kannst du den Google Übersetzer nutzen und die URL von oben einfügen, um die Anleitung auf Deutsch übersetzen zu lassen.

Mehrere Signal Accounts auf Android

Es kann sehr praktisch sein, 2 verschiedene Signal-Accounts auf dem Handy zu haben.

Beispielsweise neben dem privaten Account noch einen Account für alle LG-Sachen, den kann man dann nämlich einfach ausmachen, ist für Freund*innen aber trotzdem erreichbar. Das verhindert, dass man die ganze Zeit unter Strom steht, fördert das Abschalten und ist deswegen eine sehr gute Burnout-Prävention!

Signal

Jeder Signal-Account ist mit einem bestimmten Smartphone verknüpft. Du kannst ihn zwar mit bis zu 5 PCs teilen (Signal-Desktop), aber der Account befindet sich auf dem Smartphone, und normalerweise kann deswegen nur ein einziger Signal-Account pro Handy genutzt werden.

Es gibt aber Möglichkeiten, bis zu 4 verschiedene Accounts auf einem Android-Handy zu betreiben:

1 weiterer Account (Molly)

Du kannst sehr einfach einen zusätzlichen Account pro Handy einrichten, indem du die App Molly nutzt. Molly ist eine verbesserte Version der normalen Signal-App, welche sicherer verschlüsselt ist. Du kannst beide Apps parallel nutzen und in jeder einen eigenen Signal-Account haben. Molly ist also Signal mit einem anderen Logo plus ein paar Extras.

Bewährt hat sich eine Aufteilung in einen Arbeits- (Molly) und einen Privat-Account (normale Signal-App).

Für jeden Account brauchst du eine eigene Nummer. Die SIM-Karte muss sich dafür nicht in deinem Handy befinden, du brauchst sie nur einmal, um eine SMS zu empfangen für die Account-Erstellung, danach solltest du die sicher irgendwo verwahren und alle paar Monate etwas Guthaben

aufladen, damit die Nummer nicht verfällt (sonst hast du nach Verlust deines Handys keine Möglichkeit, deinen Account auf ein neues Handy zu übertragen). Aldi Talk ist anscheinend sehr einfach und günstig, aber jede andere SIM geht natürlich auch.

> *Auf https://sms-man.com/ kann man sich, ggf. sogar anonym, ein "einzelnes SMS-Empfangen" kaufen. Ist dann deutlich billiger als mit einer SIM-Karte. Allerdings ist so dein Account garantiert verloren, sobald du das Handy verlierst. Das liegt daran, dass man da mit einer Nummer wirklich nur EIN MAL eine Sms empfangen kann.*

Alternativ kannst du dir auch bei Easybell eine Voice-Over-IP-Telefonnummer holen (https://www.easybell.de/voice-over-ip/). Das kostet ca 10 Euro im Jahr. Das heißt: Du hast eine zusätzliche Telefonnummer, mit der du telefonieren kannst. Dazu installierst du dir auf dem Computer oder Smartphone eine VoIP-App (z. B. Zoiper https://www.zoiper.com/en/voip-softphone/download/current) , mit der du die Telefonnumer nutzen kannst.

Du kannst die (Festnetz-)Nummer von Easybell auch verwenden, um damit eine Signal-Account zu registrieren. Dann bekommst du die SMS als Sprachanruf. Danach kannst du die App wieder deinstallieren. Der Vorteil daran: Wenn dein Handy defekt ist und du Signal auf einem neuen Gerät instsallieren möchtest, brauchst du wieder Zugriff auf die hinterlegte Telefonnummer. Dann kannst du wieder die VoIP-App installieren und die SMS empfangen.

Ihr könnt auch auf dem Laptop beliebig viele Signal-Accounts nutzen, siehe unsere Dokumentation hier.

Zum Thema Anonymität

Signal lässt sich ja mittlerweile auch nutzen, ohne dass die Telefonnummer des Signal-Accounts angezeigt wird. Die Signal-Server kennen keine Metadaten. Heißt: Signal weiß nicht, wer wann mit wem kommuniziert. Signal hat auch keine Inhaltsdaten (Inhalt der Nachrichten, da Ende zu Ende verschlüsselt). Signal kennt allerdings den **aktuellen** Signal-Nutzernamen und die damit verbundene Telefonnummer. Heißt: Ihr könnt Signal anonym nutzen, selbst wenn die Telefonnummer auf euren Namen registriert ist - solange ihr den Nutzernamen geheim haltet. Den könnt ihr auch jederzeit löschen oder ändern, wenn ihr ihn verwendet habt. Wenn die Polizei mit alten Signal-Nutzernamen bei Signal anklopft, kann Signal das keinem Account mehr zuweisen. Anstatt euren Signal-Nutzernamen zu teilen, könnt ihr auch einen Link generieren und den teilen. Der Link enthält nicht euren Signal-Nutzernamen.

Installation

Anleitung kurz:

Installiere f-droid, füge die Paketquellen von Molly zu f-droid hinzu und installiere dann Molly.

Anleitung lang:

1. Lade den alternativen App-Store fdroid herunter.
2. Installiere f-droid, indem du die .apk-Datei öffnest, die du runtergeladen hast.
3. Lasse “Installation von Apps aus unbekannten Quellen” zu, wenn du danach gefragt wirst.
4. Erlaube ggf. “Apps aus dieser Quelle installieren”.
5. Gehe auf https://molly.im/download/fdroid/ und wähle Molly (wenn du gerade am Handy liest), oder scanne den QR-Code, wenn du den Artikel am PC liesst. Wähle Molly, nicht Molly-FOSS, außer du weißt, was du tust (zB keine Playdienste).
6. Öffne f-droid und wische vom oberen Rand nach unten; damit lädst du Infos über alle verfügbaren Apps, dies kann bis zu 2 Minuten dauern.
7. Suche in f-droid nach Molly und installiere es. Lass dafür ggf. wieder “installieren aus dieser Quelle” für f-droid zu.

Molly einrichten

Jetzt ist Molly bereit und du kannst die App ganz normal wie Signal einrichten.

Am Anfang wirst du jedoch gefragt, ob du eine zusätzliche Passwortverschlüsserlung nutzen möchtest, deine Wahl kann später nicht mehr geändert werden. Für sensible Accounts (z.B. PP) ist das sinnvoll, ansonsten ist es wie bei der normalen Signal-App.

Erstelle eine Signal-PIN, die du dir wirklich sicher merken kannst. Ansonsten speichere sie in deinen sicheren Passwortmanager, aber schreib sie nicht auf einen Zettel! Dieser kann nach einer Hausdurchsuchung von der Polizei genutzt werden, um Nachrichten an dich abzufangen.

Zeitliche Beschränkung für Nachrichten

Damit du nach der Arbeit deine Ruhe genießen kannst, solltest du Benachrichtigungsprofile erstellen welche festlegen, wann du wie erreicht werden kannst. Diese bieten 2 Optionen:

- festlegen, für was und welche Kontakte du Benachrichtigungen erhalten möchtest
- festlegen, wann sich das Profil automatisch aktiviert.

Um ein Profil zu erstellen, öffne oben rechts das Menü > Benachrichtigungsprofil > neues Profil. Hier kannst du Kontakte festlegen, von denen du Nachrichten erhalten willst, während dieses Profil aktiv ist. Im nächsten Schritt kannst du einen Zeitplan erstellen, der festlegt, zu welchen Tagen und Uhrzeiten dieses Profil automatisch aktiviert wird (du kannst dies jederzeit deaktivieren, um wieder normal Benachrichtigungen zu erhalten).

Bewährt hat sich eine Kombination aus 2 Benachrichtigungsprofilen:

- ein Nacht-Profil: wenn aktiv bekommst du gar keine Benachrichtigungen; aktivieren wenn du nicht arbeitest
- ein Tag-Profil: hier kannst du einstellen, dass du benachrichtigt wirst, wenn z.B.:
  - du in einem Beitrag markiert wirst
  - du angerufen wirst
  - du Nachrichten von Personen oder Gruppen bekommst, die du in deine Erlaubt-Liste aufgenommen hast

Sinnvoll ist, Profile dann aktiviert zu haben, wenn du nicht (zu doll) kontaktiert/gestört werden willst. Stelle dafür für jedes Profil einen eigenen Zeitplan ein (z.B. “Keine Benachrichtigungen”: 18:00-10:00, und “Nur Wichtiges”: 10:00-18:00).

Möchtest du normal alle Benachrichtigungen erhalten, deaktiviere das Profil einfach durch Antippen Das Menü öffnet sich durch Tippen auf das Mond-Symbol oben rechts. Wenn tagsüber ein “Nur Anrufe”-Profil aktiviert ist, kannst du es von Hand ausschalten, sobald du anfängst zu arbeiten. Du kannst den Zeitplan auch an feste Arbeitszeiten anpassen, falls du sowas hast.

2 weitere Accounts (App-Klone)

Einige Hersteller bieten eine Dual-App-Funktion, um mehrere Accounts auf einem Handy zu betreiben. Suche im Netz, ob dein Gerät über diese Funktion verfügt. Ab Android 14 könnte diese Option standardmäßig auf vielen Geräten vorhanden sein.

Du kannst diese Funktion auch nutzen, um Signal und Molly zu klonen, so dass du dann 4 Accounts hast. Du könntest damit auch auf die Nutzung von Molly verzichten und 2x Signal nutzen, Molly ist aber sinnvoller, da Molly über eine leicht bessere Verschlüsselung und Sicherheitsmechanismen verfügt, die im Falle einer Hausdurchsuchung einen Vorteil bieten.

Du kannst die Funktion einfach in den Android-Einstellungen aktivieren:

Samsung: Einstellungen > Erweiterte Funktionen > Dual Messenger

Huawei: Einstellungen > Apps > App Twin

LG: Einstellungen > Allgemein > Dual App

Daraufhin sollte ein Menü mit allen klonbaren Apps angezeigt werden, dort kannst du Signal (und ggf. weitere zu klonende Apps) einfach auswählen und verdoppeln.

D A N G E R Z O N E

Die folgenden Möglichkeiten sind schwierig, können nerven und ggf. zu Problemen führen und richten sich ausschließlich an fortgeschrittene Benutzer:innen. Diese Möglichkeiten verlassen die technische Komfort-Zone und sind eher für Sonder-Anwendungsfälle gedacht.

1 Unendlich viele Accounts nutzen

Möglich ist es (für die meisten aber nicht sinnvoll), einfach weitere Benutzerkonten auf dem Handy anzulegen. Wird ein Handy von mehreren Leuten genutzt, so kann jede:r ein ganz eigenes Profil haben, mit eigenen Apps, Daten, Einstellungen etc. Alle oben beschriebenen Tricks können pro

angelegtem Nutzerprofil wiederholt werden, theoretisch bis der Speicher voll ist.

Davon ist aber abzuraten, da das Einloggen in ein anderes Profil aufwändig ist, Zeit kostet, alle persönlichen Einstellungen nochmal vorgenommen werden müssen, man keinen Zugriff auf die persönlichen Daten im eigentlichen Profil hat. Im Alltag kann man keine Benachrichtigungen bekommen, dafür muss dann erst das Profil gewechselt werden, und im Zweitprofil gibt es dann wieder keine persönlichen Nachrichten aus dem Hauptaccount.

Diese Möglichkeit ist nur für den Notfall, oder für Usecases, in denen ein Signal-Konto nur sehr selten bei Bedarf angeguckt werden muss (z.B. Signal-Account für eine befreundete Person ohne Smartphone, die ihren Signal-Account ausschlieeßlich vom PC aus nutzt und ab und zu Bestätigungen auf dem Handy empfangen muss, um Signal-Desktop auf einem neuen Computer zu verknüpfen, wenn der alte beschlagnahmt wurde).

2 weitere Accounts (Arbeitsprofil)

Wer es unbedingt braucht, kann mit etwas Arbeit noch 2 Signal-Accounts hinzufügen. In Kombination mit einem eventuell vorhandenen Appklon-Feature sollten sich 6 Signal-Accounts auf einem Gerät installieren lassen. Das ist etwas umständlich, und setzt ein Mindestmaß an Technik-Verständnis voraus.

Für mehr Accounts nutzen wir das Workprofile-Feature von Android, um Signal und Molly zu klonen. Eigentlich ist ein Workprofile ein von einer Firma verwaltetes Profil, um den Angestellten Daten und Apps zur Verfügung zu stellen. Die Daten und Apps des Arbeitsprofils sind im Handy getrennt von den privaten; Andoid denkt also, dass eine Signal-App privat ist und die andere für eine Firma. Du kannst damit auch jede andere App auf deinem Handy verdoppeln.

Wir können die App Shelter nutzen, um ein Workprofile auf unserem Gerät auch ohne Firma zu erstellen. Shelter sollte von f-droid installiert werden, da die f-droid-Version mehr Features hat (wichtig). Mit Shelter lässt sich jede App in das Arbeitsprofil klonen, sodass wir zwei getrennte Installationen derselben App haben, die in 2 voneinander getrennten Bereichen des Handys existieren, getrennte Speicher haben etc.

Das Ganze funktioniert aber nicht immer reibungslos und kann etwas nerven, denn im Arbeitsprofil existieren nur Apps, die wir hineinkopieren. Arbeits-Signal benötigt also auch einen Arbeits-Dateimanager, eine Arbeits-Galerie etc. Jede App die wir in Kombination mit Signal nutzen muss dort hinkopiert werden, das gilt auch für selbstinstallierte Tastaturen, microG (falls du ein Custom ROM nutzt), evt. sogar Google Playservices.

Das Datei-Transfer-Feature von Shelter erlaubt allerdings den Zugriff von Arbeits-Signal auf private Dateien und andersrum, du solltest es aktivieren.

Freeze: Nach Benutzung können Arbeits-Apps “eingefroren” werden, d.h. sie werden komplett beendet und nicht ausgeführt, bis du sie wieder aktivierst (kann auch ganz praktisch sein für sehr doll spionierende Apps). Füge dazu alle Arbeits-Apps zur Autofreeze-Liste hinzu. Erzeuge eine Verknüpfung zum Autofreeze-Button auf deiner Arbeitsfläche, diese Verknüpfung funktioniert dann wie ein Ausschalter für alle Arbeits-Apps

Mehr Details gibts hier: https://www.youtube.com/watch?v=yFZc2MKmPzE