Messenger

Hier findest du:

- Empfehlungen für verschiedene Messenger-Apps
- Detaillierte Infos zum Messenger *Signal* auf verschiedenen Plattformen
- Tipps und Empfehlungen zur Erhöhung der Sicherheit bei den Einstellungen

---

Für eine vertiefende Auseinandersetzung empfehlen wir die Artikelreihe zu Messengern vom Kuketz-Blog.

Signal-Messenger

Signal ist eine auf Privatsphäre und Sicherheit fokussierte App für verschlüsselte Nachrichten und Telefonie. Die Nachrichten können sowohl Gruppen- oder Einzelnachrichten sein und aus Text, Bild, Video oder Audio bestehen. Die Telefonate werden über die Internetverbindung des Mobilgeräts aufgebaut und sind deswegen keine klassischen Anrufe via Telefonnetz. Sowohl Telefongespräche als auch Nachrichten sind vollständig Ende-zu-Ende verschlüsselt. Das heißt, dass weder die Server von Signal, noch jemand, der die Nachricht unterwegs abfängt, den Inhalt entschlüsseln kann, da die zur Ver- und Entschlüsselung benötigten Schlüssel, die Geräte der Kommunikationsteilnehmer:innen nie verlassen. Signal wurde als OpenSource-Programm entwickelt, seit 2021 ist ein Teil ihres Server-Codes nicht mehr öffentlich. Signal argumentiert dies mit der Verbesserung des Spam-Schutzes und Sicherheit ihrer Services. Signal ist nach wie vor der Messenger unseres Vertrauens.

Sag es deinen Freund:innen: Weg von WhatsApp und Telegram - Signal ist eine vollwertige und sichere Alternative.

Signal versucht verschlüsselte Kommunikation so einfach wie möglich, möglichst vielen Menschen zur Verfügung zu stellen. Dafür muss Signal jedoch Abwägungen zwischen Sicherheit und einfacher Nutzung treffen. Signal ist sehr gut geeignet, um im Alltag verwendet zu werden und auch, um im politischen Kontext schnell Nachrichten verschlüsselt auszutauschen. Kritisiert werden jedoch häufig die zentralisierten Server. Dabei werden zB alle Metadaten (auch wenn im Fall von Signal nicht so viele anfallen) zentralisiert gespeichert und den Betreiber:innen dieses Servers muss vertraut werden, was in Folge mit den gespeicherten Daten geschieht. Dies hat zwar für die alltägliche Nutzung - gerade im Sinne der Benutzer:innenfreundlichkeit - einige Vorteile, die jedoch auf Kosten der Sicherheit gehen können. Für sensiblere Kommunikation und Zusammenhänge sollte deswegen auch über andere Formen nachgedacht werden (wie zb Briar). Deshalb weil Signal auf zentralisierte Server zurückgreift und du eine Telefonnummer zur Nutzung benötigst, die deine Identität preisgeben kann. Was im Alltag sehr angenehm ist, kann in zugespitzter Situation zum Problem werden.

Signal am Smartphone

Signal kann direkt auf der Website, im Aurora Store, Play Store und IOS-store runtergeladen werden. Im F-droid wird es leider nicht angeboten.

Signal ist eine äußerst benutzer:innenfreundlich designte App, die sichere Kommunikation komplett im Hintergrund stattfinden lässt.

- Nachrichten und Telefonate sind Ende-zu-Ende verschlüsselt.
- Profil- und Gruppeninformationen sind verschlüsselt und werden dem Server nicht mitgeteilt. Nur deine Kontakte bzw. die jeweiligen Gruppenmitglieder können diese sehen. Um herauszufinden, ob deine Kontakte auch Signal haben, muss die App deine Kontakte mit dem Server abgleichen. Der Abgleich geschieht aber anonymisiert und deine Kontakte werden nicht auf dem Signal-Server gespeichert.
- Du kannst Signal mittlerweile auch für Gruppentelefonie mit wenigen Leuten verwenden. Auch diese ist dabei Ende-zu-Ende verschlüsselt.
- Bilder werden vor dem Verschicken automatisch von Exif Metadaten (GPS-Standort,…) gereinigt.
- key verification

Signal: Einstellungen

In deinem Signal auf dem Smartphone solltest du am besten noch einige Sachen einstellen:

- **Bildschirmsperre aktivieren**
  Einstellungen → Datenschutz → Bildschirmsperre
  Stelle ein Passwort ein um deine Signal Nachrichten nochmal extra zu schützen. Das Passwort ist dabei das gleiche wie auf deinem Smartphone.

- **Automatische Sperre bei Inaktivität**
  Einstellungen → Datenschutz → Autom. Sperre bei Inaktivität
  Stelle ein, dass dein Signal dich nach einer gewählten Zeitdauer wieder nach deinem Passwort fragt, also sperrt, wenn du es gerade nicht benutzt.

- **Bildschirmschutz aktivieren**
  Einstellungen → Datenschutz → Bildschirmschutz
  Damit sperrst du zB die Möglichkeit, Screenshots von deinen Chats zu machen, wodurch andere Apps eventuell versuchen könnten, den Bildschirminhalt mitzulesen.

- **Signal Pin machen (inklusive Registration Lock)**
  Einstellungen → Konto → Signal Pin (Pin und Reistrierungssperre)
  Über den „Registriation Lock“ können sich andere Geräte nur noch mit einem Passwort mit deinem Account verbinden. Über den Signal PIN, werden auch mehrere relevante Daten auf den Signal-Servern verschlüsselt gespeichert. Wenn du den PIN ausstellst, stimmst du dem Speichern der Daten nicht zu. Wenn du einen Pin einstellst, achte darauf, dass er lang genug ist. Er wird nämlich zur Entschlüsselung deiner Daten benötigt.

- **Stelle „Verschwindende Nachichten“ ein**
  Einstellungen → Daten und Speicher → Speicher verwalten → Höchstzahl an Nachrichten (pro Chat!)
  und *beliebiger Chat → drei Punkte rechts oben → Verschwindende Nachrichten*
  Im Sinne der Datensparsamkeit solltest du einstellen, dass Nachrichten nach einer gewissen Zeit gelöscht werden. So kann selbst im Falle einer Sicherstellung wenig gefunden werden. Vergiss dabei nicht den Chat „Notiz an mich“.

- **Nachrichten nicht komplett anzeigen lassen**
  Einstellungen → Benachrichtigungen → Anzeigen → Weder Name noch Nachricht
  Stelle ein, dass dir die Nachrichten am gesperrten Smartphone nicht komplett angezeigt werden, sondern zB nur der Name oder gar nichts. Dann bekommst du immer noch eine Nachricht, dass eine Nachricht gekommen ist, aber von wem und was wird dabei nicht automatisch offen gelegt.

- **Incognito Keyboard aktivieren**
  Einstellungen → Datenschutz → Inkognito-Tastatur
  Damit soll verhindert werden, dass die Eingabe auf der Tastatur von einer anderen App mitgelesen werden kann.

Artikel zu Signal-Einstellungen (englisch):
Locking down Signal

Signal am Desktop

Signal am Desktop ist eine gute Möglichkeit, um lange Nachrichten sicher zu verschicken. Signal am Desktop schickt immer noch Ende-zu-Ende verschlüsselte Nachrichten, unternimmt aber nur sehr wenige eigene Maßnahmen, um den lokalen Zugriff einzuschränken. Das heißt, deine Nachrichten sind, zB bei einer Beschlagnahmung durch die Repressionsbehörden, nur so sicher wie dein Computer. Vor allem ein **verschlüsselter Computer** ist hier Vorraussetzung.

So ihr könnt zwar sicher Ende-zu-Ende verschlüsselte Nachrichten austauschen, wenn du oder dein Gegenüber diese jedoch nicht sicher verwendet - also zB Signal auf dem Desktop verwendet, der Computer jedoch nicht verschlüsselt ist - können Repressionsbehörden wieder Zugriff darauf bekommen. Die Sicherste Variante is auf jeden fall Signal nur am Smartphone zu verwenden.

Signal in Gruppenzusammenhängen

Überlegung: Signal ist ein „Instant Messenger“ der für Smartphones gemacht wurde. Wir sollten ihn so auch verwenden.

Signal ist sicher und einfach zu bedienen, aber es ist nicht für jede Verwendung in Gruppen konzipiert. Es ist gemacht für den Austausch und die Diskussion von Inhalten, aber es ist eben NICHT dafür gedacht, diese Inhalte zu organisieren oder gar zu speichern. Es ist so vergesslich wie es „instant“ ist. Zum Beispiel ist es nett, um ein Bild oder einen Link schnell an alle in einer Gruppe zu teilen. Aber schon 2 Tage später ist der Link hinter mehreren neuen Nachrichten verloren oder auf deiner eigenen „Signal-Timeline“ ist die Gruppe schon weit nach unten gerutscht. Wenn du etwas mitteilen willst, das NICHT temporär ist, ist Signal nicht der richtige Ort. Die meisten Menschen haben Signal auf ihren Telefonen. Die gleichen Telefone, die bereits voll von Informationen und Aufmerksamkeit suchenden Apps und Benachrichtigungen sind. Es ist super einfach, davon überwältigt zu werden, vor allem in großen Gruppen die voll von Leuten sind, die diskutieren usw. Vielen ist es vielleicht schon passiert, dass die Gruppen stumm geschalten werden. Sobald dieser Punkt erreicht ist, verliert die Signal-Gruppe ihren Zweck. Der Zweck alle in einer Gruppe schnell und einfach über wichtige Dinge zu informieren. Bitte überdenkt also das Stummschalten und diskutiert stattdessen doch in der Gruppe wenn die Menge der Nachrichten überwältigend und nervig ist. Vielleicht sollte auch in der Gruppe über andere Formen der Kommunikation nachgedacht werden, wie zB ein Forum.

Auch wenn Signal sicher ist, ist es dein Handy nicht unbedingt. Dein Handy (Oder das deines Gegenübers) könnte in entsperrtem Zustand beschlagnahmt werden,… Achtet deshalb trotzdem darauf was über Signal geschrieben wird!

Telegram

Telegram ist entgegen seines Rufes nicht zu empfehlen. Die Chats sind nicht Ende-zu-Ende verschlüsselt, außer du aktivierst es aktiv. Schlimmer noch, Telegram speichert die Nachrichten bei sich auf dem Server. Für Gruppen gibt es gar keine Verschlüsselung. Warum ein Anbieter für 'sichere' Kommunikation, Nutzer:innen so einem Risiko aussetzt, ist nicht ganz klar. Daher sollte Telegram **nicht** genutzt werden.

Unsere Empfehlung: **Signal statt Telegram!**

WhatsApp

Weltweit nutzen mehr als eine Milliarde Menschen WhatsApp. Nachrichten sind auch mit dem Signal-Protokoll Ende-zu-Ende verschlüsselt. Ein Kritikpunkt bleibt aber: WhatsApp sammelt viele Metadaten und teilt Nutzer:innendaten mit Facebook, darunter auch die eigene Telefonnummer. Aber nicht nur das, WhatsApp lädt auch dein komplettes Telefonbuch auf Facebook-Server hoch. WhatsApp-Backups auf Google Drive, iCloud und lokal auf dem Gerät sind zwar ebenfalls verschlüsselt, aber nicht Ende-zu-Ende. Es gibt den begründeten Verdacht, dass die Schlüssel zu diesen Backups auf den Servern von WhatsApp liegen. Das würde bedeuten, dass der Dienst die gesicherten Inhalte einsehen kann.

Deswegen unsere Empfehlung: **Signal statt Whatsapp verwenden!**

Briar

Der Messenger *Briar* legt den Fokus in der Kommunikation auf Anonymität. Die Zielgruppe von Briar sind politische Aktivist:innen und Journalist:innen, also Menschen, die ganz konkret Angst vor staatlicher Repression haben für das was sie tun.

Briar ist Open Source und und die Nachrichten werden Ende-zu-Ende verschlüsselt. Der Messenger kommt ohne zentrale Server aus: In der Kommunikation setzt es auf ein Peer-2-Peer Netzwerk. Daher ist *Briar* auch ohne funktionierende Internet-Infrastruktur verwendbar und kann auch verwendet werden, wenn etwa das Internet zur gestört, abgeschalten wird oder ausfällt.

Wenn Briar über das Internet kommuniziert, verschickt es alle Nachrichten über das Tor-Netzwerk, damit ist nicht mehr rückverfolgbar wer mit wem kommuniziert.

Leider geht die Anonymität auf die Kosten von Nutzungsfreundlichkeit und des Akkus: So müssen zB damit eine Nachricht zugestellt werden kann beide Beteiligten gleichzeitig online sein. Im Moment wird eine Nachricht so lange immer wieder gesendet, bis die andere Person online ist und die

Nachricht auch empfangen kann. Es wird jedoch an Lösungen gearbeitet damit dies nicht mehr notwendig ist.

Die App ist ausschließlich für *Android* verfügbar und ist im F-Droid und im Google-Play-Store erhältlich.

Briar ist für alle empfehlenswert die viel Wert auf Anonymität legen. Für den Alltag ist es leider nicht wirklich geeignet, hierfür würden wir Signal empfehlen.

Mehr zu Briar erfährt ihr in einem Artikel am Kuketz Blog

Element

Der Messenger Element, basiert auf dem Matrix-Protokoll und ist openSource. *Matrix* verfolgt einen dezentralen Ansatz, bei dem Nutzer:innen sich für einen Anbieter entscheiden können oder sogar einen eigenen Server in die bestehende Infrastruktur integrieren können. *Matrix* erlaubt es ein Kommunikationsnetzwerk zu betreiben, ohne von zentralen Anbieter:innen in irgendeiner Form abhängig zu sein. Das heißt es gibt nicht einen zentralen Server auf dem alles abgewickelt wird, sondern es gibt viele - eigenständige und voneinander unabhängige - Server, die miteinander kommunizieren.

Nutzer:innen sind also vollkommen frei in ihrer Entscheidung, bei welchem Matrix-Server bzw. welcher Anbieter:in ein Konto eröffnet werden soll, um es dann mit einem beliebigen Matrix-Client zu verwenden. Anders als bei einem zentralisierten Dienst wie WhatsApp, Telegram und Co. bestimmt also nicht ein:e Anbieter:in allein die Spielregeln. Die Architektur bzw. das Prinzip der Föderation verfolgt einen offenen Ansatz der kollektiven Vernetzung.

Diese Server können dann auch mit unterschiedlichen Apps verwendet werden, wobei hier unsere Empfehlung das App *Element* ist. Element ist für Android, iOS, Windows, macOS und Linux nutzbar und auch im F-Droid-Store erhältlich.

Der große **Vorteil von Element** ist, dass du für die Nutzung von Element keine Telefonnummer benötigst. Mensch kann sich mit einem Identifier (ähnlich einer E-Mail-Adresse) registrieren und ist anschließend darüber auffindbar. Alle Kommunikationsinhalte werden standardmäßig Ende-zu-Ende verschlüsselt, sowohl in Einzel- als auch in Gruppenchats.

Metadaten und Matrix
Was die Metadaten anbelangt schneidet Element (im Vergleich zB zu Signal) leider nicht so gut ab. So lässt sich aus den anfallenden Metadaten einiges rekonstruieren(zB wer mit wem, wann und wie häufig in Kontakt stand). Die Vermeidung von Metdaten bei föderativen Netzwerken ist jedoch auch schwieriger. Die Vermeidung von Metadaten ist demnach keine Stärke von *Matrix* und damit auch nicht von *Element*.

Die integrierte Ende-zu-Ende Verschlüsselung kann euch zwar vor dem Auslesen der Inhaltsdaten (bzw. Nachrichten) schützen – am Ende bleiben allerdings dann eben noch einige Metadaten (bspw. Kontaktliste) übrig, auf die ein:e Matrix-Server-Betreiber:in potenziell Zugriff hat. Das macht es umso wichtiger den Betreiber:innen des Matrix Servers zu vertrauen. Wir empfehlen hier den Matrix-Server von Systemli.

Gerade für das gemeinsame Arbeiten in politischen Gruppen würde sich Element anbieten.
Mehr zu Element erfährt ihr im Artikel vom Kuketz-Blog.