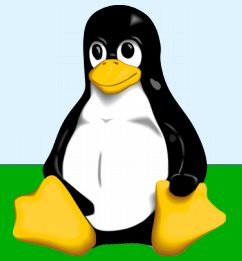
KiLUG

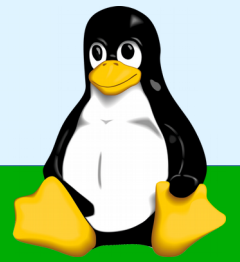
Kinzigtäler Linux User Group

# Instant Messenger-Alternativen zu WhatsApp



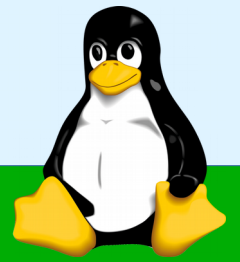
# Was genau ist Instant Messaging

- Mindestens zwei Teilnehmer unterhalten sich miteinander über kurze, formlose Textnachrichten ähnlich einem klassischen Chat-Programm
- Die Nachrichten kommen direkt und ohne große Verzögerung beim Empfänger an (Push-Notification)
- Die Teilnehmer verwenden hierfür ein spezielles Programm welches die Daten über einen Server im Internet zwischen ihnen austauscht
- Viele erwarten auch, dass nicht nur Texte sondern auch Bilder, Audio- und auch Videodateien und Sticker ausgetauscht werden können



# Was genau macht einen Messenger sicher?

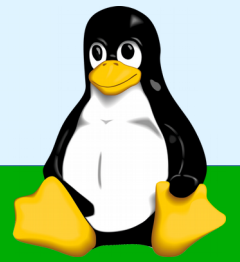
- Konnte der Quelltext des Programms durch Experten oder ein Sicherheits-Audit unabhängig überprüft werden (Open Source)?
- Wird eine anerkannte und sichere Ende-zu-Ende-Verschlüsselung verwendet?
- Muss sich der Besitzer authentifizieren, kann also sichergestellt werden das die Nachricht auch von der angegebenen Person stammt?
- Kann nachträglich nicht bewiesen werden, dass der Absender bestimmte Nachrichten versendet hat (glaubhafte Abstreitbarkeit)?



# Was genau macht einen Messenger sicher?

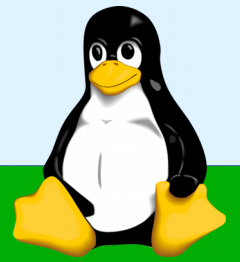
- Benutzt der Messenger eigene Server oder werden die Daten irgendwo im Netz (eventuell auf amerikanischen Servern) abgelegt?
- Wird verhindert das frühere abgefangene Nachrichten nachträglich gelesen werden können, falls der Schlüssel in fremde Hände gerät?

  - **Perfect Forward Secrecy** (PFS): Jede Nachricht wird mit einem neuen Kurzzeitschlüssel verschlüsselt. Dadurch können alte Nachrichten nicht im Nachhinein gelesen werden, falls der Schlüssel in fremde Hände gerät.



# Welche Kriterien müssen die Messenger erfüllen?

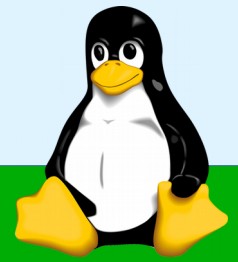
- Unterstützung möglichst vieler, gängiger Plattformen (Android, iOS, Windows, Linux, macOS)
- Telefoniefunktion
- Gruppenchats
- Sticker / GIFs
- Die Übertragung der Kontakte aus dem Adressbuch darf nur optional möglich sein, am Besten nicht im Klartext sondern als „Hash“
- Die Übertragung der Daten über eigene dem Messenger zugehörige Server



# WhatsApp

## Funktionen

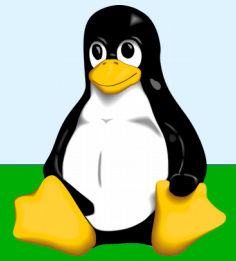
- Plattformen: Android, iOS, Blackberry, Windows, Chrome Browser
- Telefoniefunktion: Ja ✔
- Gruppennachrichten: Ja ✔
- Sticker / GIFs: Nein ✘/ Nein ✘
- Übertragung Telefonbuch: automatisch ✘
- Kosten: kostenlos



# WhatsApp

## Sicherheit

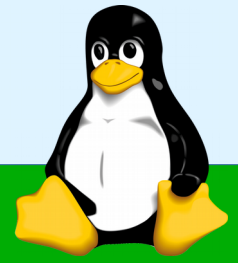
- Open Source: Nein ✘
- Ende-zu-Ende-Verschlüsselung: Ja ✔
- Authentifizierung: Ja ✔
- Abstreitbarteit: Ja ✔
- Perfect Forward Secrecy: Ja ✔
- Eigene Server: Nein ✘(Adressenaustausch mit Facebook)



# Threema

## Funktionen

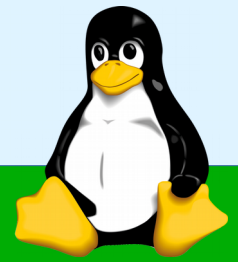
- Plattformen: Android, iOS, Chrome Browser
- Telefoniefunktion: Nein ✘
- Gruppennachrichten: Ja ✔
- Sticker / GIFs: Nein ✘/ Nein ✘
- Übertragung Telefonbuch: optional (als Hash) ✔
- Kosten: einmalig €1,79



# Threema

## Sicherheit

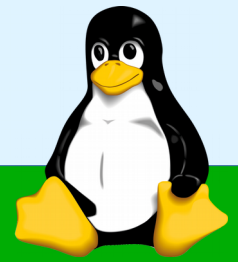
- Open Source: Nein (nur die Verschlüsselung ist Open Source) ✘
- Ende-zu-Ende-Verschlüsselung: Ja ✔
- Authentifizierung: Ja ✔
- Abstreitbarteit: Ja ✔
- Perfect Forward Secrecy: Nur Server-Client ✘
- Eigene Server: Nein (Server stehen aber laut Betreiber in Europa) ✘



# Telegram

## Funktionen

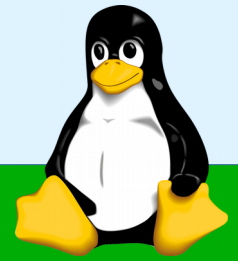
- Plattformen: Android, iOS, macOS, Windows, Linux
- Telefoniefunktion: Nein ✘
- Gruppennachrichten: Ja ✔
- Sticker / GIFs: Ja ✔/ Ja ✔
- Übertragung Telefonbuch: Pflicht ✘
- Kosten: kostenlos



# Telegram

## Sicherheit

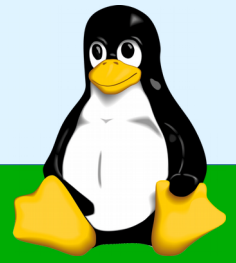
- Open Source: nur teilweise ✘
- Ende-zu-Ende-Verschlüsselung: Ja (nicht bei Gruppenchats) ✘
- Authentifizierung: optional ✘
- Abstreitbarteit: unbekannt ✘
- Perfect Forward Secrecy: optional ✘
- Eigene Server: Nein ✘



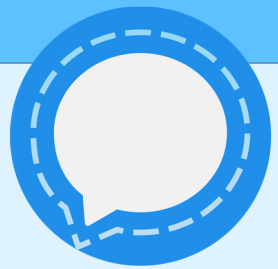
# Signal

## Funktionen

- Plattformen: Android, iOS, Chrome Browser (dadurch Windows, Linux und macOS)
- Telefoniefunktion: Ja ✔
- Gruppennachrichten: Ja ✔
- Sticker / GIFs: Ja ✔/ Ja ✔
- Übertragung Telefonbuch: optional (als Hash) ✔
- Kosten: kostenlos (wird über Spenden finanziert)

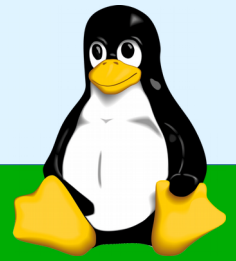


# Signal



## Sicherheit

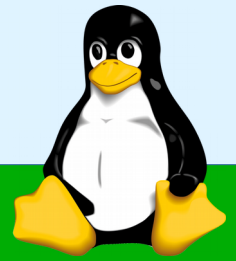
- Open Source: Ja ✔
- Ende-zu-Ende-Verschlüsselung: Ja ✔
- Authentifizierung: Ja ✔
- Abstreitbarteit: Ja ✔
- Perfect Forward Secrecy: Ja ✔
- Eigene Server: Ja ✔
- Von Edward Snowden empfohlen: Ja ✔



# Google Allo

## Funktionen

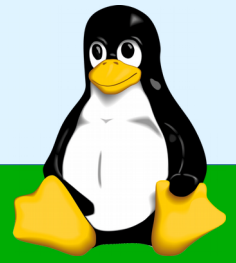
- Plattformen: Android, iOS
- Telefoniefunktion: Nein ✘
- Gruppennachrichten: Ja ✔
- Sticker / GIFs: Ja ✔/ Ja ✔
- Übertragung Telefonbuch: Pflicht ✘
- Kosten: kostenlos



# Google Allo

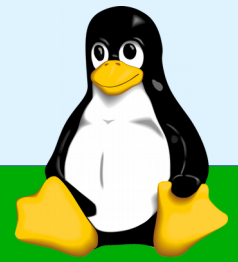
## Sicherheit

- Open Source: Nein ✘
- Ende-zu-Ende-Verschlüsselung: standardmäßig nicht aktiviert ✘
- Authentifizierung: Ja ✔
- Abstreitbarteit: unbekannt ✘
- Perfect Forward Secrecy: unbekannt ✘
- Eigene Server: Nachrichten werden durchsucht ✘



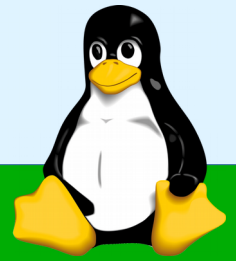
# Punktevergabe

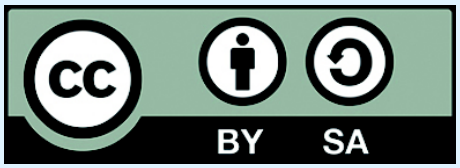
| | |
|---|---|
| Signal: | 10 / 10 |
| Threema: | 6 / 10 |
| WhatsApp: | 6 / 10 |
| Allo: | 4,5 / 10 |
| Telegram: | 4 / 10 |



# Links zur Präsentation

- https://de.wikipedia.org/wiki/Liste_von_mobilen_Instant-Messengern/
- https://www.whatsapp.com/
- https://threema.ch/de/
- https://telegram.org
- https://whispersystems.org
- http://elzpiraten.de








Mit Dank an die Elzpiraten
http://elzpiraten.de