



Delta Chat – privat, sicher, dezentral

Helmut Schweinzer

9. Mai 2026

Linuxtag der Erlanger Linux User Group



Inhalt

Getting Started

Andere Messenger

Geschichte

Was ist Delta Chat (Basics / Eigenschaften)

Technik

Goodies

Ausblick

Demo



Getting Started

Zum Loslegen mit Delta Chat braucht es recht wenig:

1. Delta Chat installieren (<https://get.delta.chat>)
2. Profil anlegen: Profilnamen eingeben und Anlegen klicken
3. Kontakt hinzufügen (QR-Code oder Invite-Link)
4. Los-chatten

Was man wissen sollte:

- Chats sind end-to-end verschlüsselt
- Es werden keine persönlichen Angaben (Tel-Nr., Email-Adresse ...) benötigt

Ich habe schon mal eine Gruppe zum Probieren und Austauschen angelegt.
QR und Link unter [https:// erlug.de / blogs / delta](https://erlug.de/blogs/delta)



Wer nutzt was?

Ein paar Fragen vorweg:

- Wer nutzt WhatsApp?
- Wer nutzt einen “WhatsApp-Proxy”?
- Wer nutzt Signal?
- Wer nutzt Matrix?
- Wer nutzt andere Messenger?
- Wer nutzt gar schon Delta Chat?



WhatsApp?

Wer heute Whatsapp (noch/nicht) verwendet ...
weiß entweder, was er tut ... oder er weiß es eben nicht!

- **(Fast) jeder hat es**
- **Leicht zu bedienen**
- **Inhalt End-to-End verschlüsselt**
- **Browser-Version**
- **Kommerziell**
- **Datenschutz ???**
- **Tracking**
- **Werbung**
- **Spam**
- **Sicherheitslücken**
- **US-Server**
- **Account kann willkürlich gesperrt werden**
- **Telefonnummer nötig**
- **Telefonnummern von Kontakten werden zu Server geleakt**
- **Datenschutzrechtlich in D illegal**

2009 gegründet,
seit 2014 (erst Facebook, dann) Meta

User: ~3,3 Mrd. Weltweit

58 Mio (84%) in D



Wer heute (schon) Signal verwendet ...
weiß entweder, was er tut ... oder er weiß es eben nicht!

- **Datenschutz und Privacy**
- Sehr sparsam mit Meta-Daten
- Recht gut verbreitet
- Leicht zu bedienen
- End-to-End verschlüsselt
- Desktop-Version
- Nicht kommerziell
- Kein Tracking
- Keine Werbung
- Telefonnummer nötig
- US-Server (Cloud)
- Kann relativ einfach (z.B. für Europa) komplett abgeschaltet werden
- Proprietär, intransparente Entscheidungsstrukturen
- "Nicht ganz" nach EU-Recht

2010 als TextSecure, ab 2014 dann
Signal

User: ~100 Mio weltweit, ~10 Mio in D



Matrix

Wer heute Matrix verwendet ...
weiß (hoffentlich) entweder ungefähr, was er tut ...
oder er weiß es eben nicht!

- **Föderiert**
- End-to-End verschlüsselt (oft)
- Browser-Version
- Datenschutz und Privacy
- Nicht kommerziell
- Kein Tracking (Serverabhängig)
- Keine Werbung
- Server selbst hostbar
- Account auf einem Home-Server
- Nicht so trivial zu verstehen
- Gelegentliche Verschlüsselungsprobleme
- Inkonsistentes Blockieren

Eingeführt 2014, Releases 2018
User: 50+ Mio weltweit



Geschichte

- Email (SMTP, POP3, IMAP) (seit ~1980)
- Verschlüsselung
 - PGP (seit 1991)
 - (S/MIME) (seit 1995)
 - Autocrypt (seit 2017)
- Instant Messenger (seit ca. 2005)



Was ist Delta Chat?

Delta Chat – ein moderner, privater Messenger, der in Deutschland entwickelt wurde und wird (merlinux GmbH)

Delta Chat setzt auf die gut eingeführten und verstandenen Mail-Protokollen auf. Jeder hat/verwendet Email.

Markante Punkte:

- Multiplattform (Android, iOS, Linux, Windows, macOS)
- Multi-Profil
- Multi-Device
- Multi-Transport
- E2E-Verschlüsselung



Eigenschaften von Delta Chat?

Eigenschaften von Delta Chat

- Instant onboarding (anonym)
- FOSS (github)
- verwendet offene Standards
- dezentralisiert
- Works under bad network conditions
- diverse Security-Audits
- Transparente Finanzierung
- Eigene Server möglich



Privacy

- Keine Tel-Nr. oder andere private Daten nötig
- (Email-Adresse)
 - eigene Mailbox
 - Anonyme Random-Adresse(n)
- Kein Kontakt im Adressbuch
- kein Verzeichnis oder Discovery (Profil = Privat, keine Spam)
- Nur direkte Kontakte über QR-Code oder Einladungslink
- Kids-safe (keine SIM, kein Discovery, Privat-Familien-Chat)
- Keine Werbung, kein Tracking



- Mail-Protokolle SMTP und IMAP (IMAP-PUSH)
- DC ist ein spezieller Mail-Client (“Chat-over-Email”)
- “Mail-Nachrichten” als Messages anzeigen
- Verschlüsselung mit OpenPGP (rpgp)
- Aushandeln von Kontakten mit Secure-Join (Autocrypt)
- ID ist der PGP-Key und nicht die Email-Adresse
- Nachrichtenspeicherung nur im Client
- Kein zentraler Server
- Mail-Server sind nur “Transport-Puffer”



Email-Adresse

- Verwenden eigener Mailbox (Email-Adresse) möglich
 - Aber dann möglichst ausschließlich für DC
 - Nicht mehr anonym
 - Speicherung auf Mailserver
(Nachrichten muss man selber löschen)
 - Evtl. Einschränkungen je nach Provider
- Spezialisierte Mailserver (Chatmail)
- es gibt kein zentrales Verzeichnis der User



Gruppen

Gruppen sind primär private Gruppen

- Gegenseitiges Vertrauen – man kennt sich
- Alle sind gleichberechtigt (es gibt keinen Admin)
- Sichere und effiziente Schlüsselverteilung (Gossip)
- Jeder Post ist für jeden Teilnehmer individuell verschlüsselt
- Server wissen nichts von Gruppen
Gruppen sind nur zusammengefasste Chats

Neuer Gruppentyp “Channel” (wie Mailingliste)

Weitere Gruppen-Typen in Überlegung (z.B. moderiert, public)



Relays - Multi-Transport

- Ein Server mit (Transport-)Mailbox heißt in DC Relay
- Pro Profil sind mehrere Relays möglich/empfohlen (Redundanz)
 - Nachrichten werden über alle Relays ausgeliefert
 - Wenn ein Relay ausfällt, stört das nicht
 - Email-Adresse ist unwichtig (daher auch nicht als ID)
 - Optimalerweise Chatmail-Server als Relay verwenden
- Einstellungen → Erweitert → Relays



Chatmail-Server (Relays)

Chatmail-Server sind:

- Für DC optimierte/minimierte Mailserver
 - Explizit nur pgp-verschlüsselte Mails
 - Striktes TLS und DKIM
 - Angepasste Rate-Limits
 - Keine komplexen Spam-Filter oder Reputations-Checks
 - Schnelle Auslieferung von Nachrichten
 - Meta-Daten minimiert
 - Einfach selbsthostbar
- Bietet anonyme Random-Email-Adressen
- Nur "Durchleiten" von Nachrichten
 - Keine dauerhafte Speicherung von Nachrichten
 - Geringer Speicherbedarf
- Es gibt viele Chatmail-Server (einige Public, viele hidden)



In-Chat Mini-Apps

- HTML mit JavaScript (in Sandbox)
- Bestandteil eines Chats (Attachment zu einer Message)
- Apps laufen auch Offline
- Peer-to-Peer (iroh)
- Tools
 - Umfragen
 - Realtime Chat (ephemeral)
 - Terminkalender
 - Gemeinsam editierbare Dokumente
 - Einkaufs-, Todo-Listen
 - Expense sharing
 - Diverse Tools (Verschlüsselung, Taschenrechner, QR-Code-Generator, ...)
- Spiele
 - Single-Player (Tetris, Breakout, 2048, ...)
 - Multi-Player (Dame, Schach, Scramble, Dungeons, ...)

Keine Werbung
Kein Tracking
Kein Server beteiligt



Einfache Programme (= DC-User) können beliebige Aufgaben erledigen:

- EchoBot (reines Bot-Gerüst mit "Echo")
- Beispiele
 - InviteBot
 - StatusBot (Verfügbarkeit von DC-Versionen in div. Stores)
 - LoginBot (Forum - OAuth2)
 - RSS Bot
 - Bridges (Verbindungen zu anderen Messengern)
- Selbst programmier- und hostbar, z.B. auch im Handy!
- Achtung: Bots lesen Chat mit (wie Alexa)
- Achtung: Bei Bridges verlässt man die "private" Welt



Weitere Entwicklungen

Es gibt aktive Entwicklungen und Änderungen

- Viele Feature-Requests im Forum

Konkretere Pläne:

- Hin zu dyn. Relays, weg von fixen Emailadressen
- PFS und PQC (mit autocrypt2 – in 2026)
- Video-Chat nativ mit WebRTC (noch experimentell)
- UnifiedPush
- Verschiedene Gruppentypen
- ...



Wer ab heute Delta Chat verwendet ... weiß jetzt, was er tut

- End-to-end verschlüsselt
 - Desktop-Version
 - Datenschutz und Privacy
 - Anonym. Keine Telefon-Nr./Email-Adr. nötig
 - Offene Standards, OpenSource
 - Metadaten minimiert
 - dezentralisiert
 - Kein Discovery
 - Kein Tracking, keine Werbung
 - Lokale Speicherung - Kein zentraler Server
 - Eigene Server möglich
 - Multi-Profile
 - Multi-Transport
 - In-Chat-Apps
 - Läuft auch unter schwierigen Netzwerk-Bedingungen
 - Nicht kommerziell
 - Transparente Finanzierung (Förderungen)
 - Kein Discovery
 - Noch keine "Public-Groups"
 -
- Eingeführt 2019
Downloads > 1 Mio (Playstore)



Mitmachen

- Im Forum beteiligen (Feature-Requests)
 - Auf Github – Open Source
 - Eigenen Chatmail-Server aufsetzen
 - WebxDC-Apps schreiben
 - Bots erstellen und hosten
 - Donations für Weiterentwicklung
- Und natürlich ...
- Spread the Word



... wenn noch Zeit:

Zur Erinnerung:

Ich habe schon mal eine Gruppe zum Probieren und Austauschen angelegt.

QR und Link unter [https:// erlug.de / blogs / delta](https://erlug.de/blogs/delta)



Links

Delta-Chat Homepage

<https://delta.chat>

QR-Code-Howto

https://delta.chat/assets/howto/qrcodes_howto.pdf

Support-Forum / FAQ

<https://support.delta.chat> / <https://delta.chat/help>

Source

<https://github.com/deltachat>

Genutzte Standards

<https://github.com/chatmail/.../standards.md#standards-used-in-delta-chat>

WebxDC

<https://webxdc.org>

Chatmail(-Server)

<https://chatmail.at>

Autocrypt / Autocrypt2

<https://autocrypt.org> / <https://autocrypt2.org>



Danke für die Aufmerksamkeit

Danke für die Aufmerksamkeit

Fragen ?

Helmut Schweinzer

Email: hel@ki-aikido.de

PGP: 0xAE8E86EA

Fingerprint: B7A6 3FD8 534B D498 F2A5 C3C8 93CE AAD2 AE8E 86EA