Richtlinie zum „Software-Sprint“

Delta-Chat-Channels

Schlussbericht

Zuwendungsempfänger*in:

Jonathan Schmiederer

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Forschung, Technologie und Raumfahrt unter dem Förderkennzeichen 16IS25S10 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei dem*der Autor*in.

Kurze Darstellung der Aufgabenstellung und Motivation in der Förderphase

Meine Motivation für dieses Projekt war es, den dezentralen, datenschutzfreundlichen und Ende-zu-Ende-verschlüsselten Messenger „Delta Chat“ um ein Feature zu erweitern, das in vielen Kontexten dringend fehlt: sichere Broadcast-Channels. Während Telegram und WhatsApp solche Kanäle längst anbieten, existierte bisher im europäischen und datenschutzsensiblen Bereich keine Alternative, die gleichzeitig dezentral, E2E-verschlüsselt, metadatenarm und ohne Telefonnummern funktioniert.

Gerade für zivilgesellschaftliche Gruppen, Journalist:innen und Menschen in autoritären Staaten sind solche Kommunikationskanäle essenziell: Sie ermöglichen es, viele Menschen anonym, sicher und ohne zentrale Infrastruktur zu erreichen. Das funktioniert selbst dann, wenn ein Land vom globalen Internet abgeschnitten wird, da Delta Chat föderiert aufgebaut ist und eigene Relay Server im Land betrieben werden können.

Mein Ziel war es daher, vollwertige, sichere Channels in Delta Chat einzubauen: vollständig symmetrisch ende-zu-ende verschlüsselt, leicht beitretbar über QR-Codes und Links und nahtlos integriert in die bestehende App.

Beitrag des Projektes zu den Zielen der Förderinitiative „Software Sprint“

Mein Projekt stärkte sowohl die digitale Infrastruktur als auch die Sicherheit im Sinne der Förderinitiative.

Im Bereich Infrastruktur verbesserte es die europäische Kommunikationslandschaft konkret: Es erweiterte eine dezentrale, offene Messenger-Infrastruktur, die ohne Telefonnummern und ohne zentrale Server auskommt. So lassen sich große Gruppen zuverlässig und resilient informieren, auch in Ländern, in denen staatliche Stellen sonst leicht Kommunikationswege kontrollieren oder abschalten.

Im Bereich Sicherheit entwickelte das Projekt erstmals symmetrische Ende-zu-Ende-Verschlüsselung für Broadcast-Channels und etablierte ein sicheres, praxistaugliches Protokoll für Channel-Einladungen. Anders als bei den Channel-Funktionen von WhatsApp und Telegram, die nicht Ende-zu-Ende-verschlüsselt sind, können Channel-Betreiber:innen und Empfänger:innen in Delta Chat sicher sein, dass Inhalte ausschließlich auf ihren Geräten sowie den Geräten der Empfänger:innen lesbar sind. Durch Review-Prozesse und die offene Entwicklung floss zudem das Wissen der internationalen Community direkt in die Sicherheit der Lösung ein.

Damit leistet das Projekt einen sichtbaren Beitrag zu einer unabhängigen, dezentralen digitalen Öffentlichkeit.

Ausführliche Darstellung der Ergebnisse in der Förderphase

Channels als eigener Chattyp

Ich habe erfolgreich implementiert, dass Broadcast-Nachrichten nicht mehr im 1:1-Chat landen, sondern in einem eigenen Channel-Chat. Channel-Ersteller:innen können Namen und Bild setzen, die bei allen Empfänger:innen erscheinen.

Symmetrische Ende-zu-Ende-Verschlüsselung

Asymmetrische Verschlüsselung lässt sich für Channels nicht verwenden, da sie die Identität aller Empfänger:innen verraten würde und bei vielen Empfänger:innen die Nachrichten sehr groß werden würden. Also habe ich die Ende-zu-Ende-Verschlüsselung in Channels wie geplant symmetrisch mit AES umgesetzt (statt asymmetrisch, wie in normalen Delta-Chat-Gruppen). Ein anfängliches Performanceproblem konnte ich durch Benchmarking und Optimierungen lösen. Der Support dafür war in der verwendeten “rpgp” (Rust-OpenPGP Implementierung) vorhanden.

QR-Codes und Einladungslinks

Ich habe ein technisches Design für Channel-QR-Codes entwickelt, diese implementiert, Sicherheitsanalysen durchgeführt und ein ein Datenschutzproblem identifiziert, das ich in Absprache mit anderen Delta-Chat-Maintainern entschärft habe.

Sicherheit und Tests

Ich habe mehrere potentielle sicherheitsrelevante Probleme gefunden und behoben, darunter einen potenziellen DoS-Angriff und erwähntes Privatsphäreproblem. Automatisierte Regressionstests stellen sicher, dass Channels auch in der Zukunft weiterhin zuverlässig funktionieren werden.

Integration in die offizielle App

Wie im Proposal vorgesehen habe ich einen Pull Request erstellt, um meine Implementierung in die offizielle Delta-Chat-Android-App zu integrieren. Dieser Pull Request wurde nach mehreren Review-Runden gemerged, sodass Channels inzwischen sogar Teil der offiziellen App sind und über den Play Store sowie F-Droid ausgeliefert werden. Da der Release-Prozess zwischenzeitlich durch einen anderen, unabhängigen Pull Request blockiert war, habe ich zusätzlich selbst Verbesserungen beigesteuert, um wieder reguläre Releases zu ermöglichen. Aktuell sind Channels noch als experimentelles Feature markiert und können in den Einstellungen unter „Erweitert“ aktiviert werden.

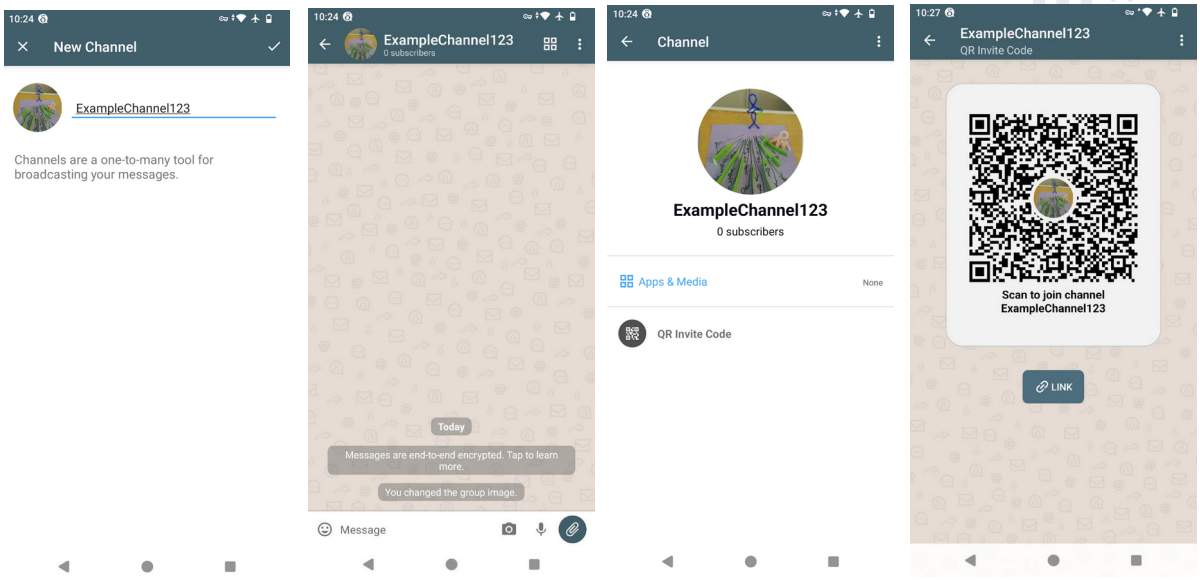
User Testing

Ich habe User-Tests durchgeführt, Bugs und UX-Hürden identifiziert, und diese direkt behoben. Dadurch ist das Feature für reale Nutzer:innen stabil und gut verständlich.

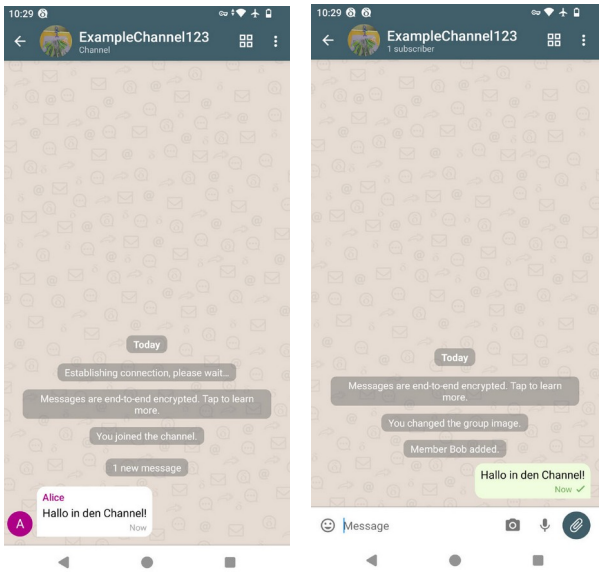
Ergebnis:
Alle Meilensteine wurden vollständig erreicht. Channels inklusive E2E-Verschlüsselung, QR-Einladungen und Einladungslinks sind fertig, sicher und sogar bereits offiziell veröffentlicht.

Screenshots:

Erstellen eines Channels und Einladungs-QR-Codes:



Senden einer Nachricht, nachdem jemand beigetreten ist:



Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Zielgruppen

Die Ergebnisse sind für alle Delta-Chat-Nutzer:innen relevant, besonders jedoch für Journalist:innen, NGOs, Aktivist:innen und Menschen in Ländern mit eingeschränkter Kommunikationsfreiheit. Um diese Zielgruppen zu erreichen und über das neue Feature zu informieren, plane ich zudem die Veröffentlichung eines Blogposts auf dem offiziellen Delta-Chat-Blog, in dem Channels vorgestellt, erklärt und Hinweise zur sinnvollen und sicheren Nutzung gegeben werden.

Nutzen

Channels ermöglichen es, große Personengruppen sicher, anonym, ohne Telefonnummern und ohne zentrale Server zu erreichen. Dank Ende-zu-Ende-Verschlüsselung und der dezentralen Architektur kann die Kommunikation selbst unter repressiven Bedingungen aufrechterhalten werden. Staaten können zwar einzelne Server abschalten, aber nicht das gesamte System. Das macht Delta Chat zu einer echten Alternative für Menschen, die auf sichere Information angewiesen sind.

Darüber hinaus tragen Channels zu einem offenen und freien Internet bei, indem sie zentrale Plattformen ersetzen können. Ein Nutzer aus dem Fediverse brachte dieses Potential gut auf den Punkt:

> *I say [channels] have a chance to succeed where #RSS feeds failed.*

Dass dieser Ansatz auch in der Praxis funktioniert, zeigt das Feedback aus der Community. A. Benitez, Maintainer des Delta-Chat-Forks „ArcaneChat“, berichtete kurz nach Einführung der Channels:

> *Channels finally give me a way for reaching my audience in a decentralized, private way. The new channel I created already has 277 subscribers, and is growing.*

Open-Source-Effekte

Andere Delta-Chat-Clients wie iOS, Desktop und Ubuntu Touch integrieren das Feature bereits nach und nach. Protokolle und Designs können wiederverwendet werden, und der öffentliche Review-Prozess erhöht die Sicherheit für die gesamte Community.

Weiterentwicklung

Zukünftig sollen ein neues, noch privateres Einladungsprotokoll, Channel-Implementierungen für weitere Plattformen und kleine Erweiterungen wie Channel-Beschreibungen folgen.

Persönliche und fachliche Weiterentwicklung

Ich konnte meine Kenntnisse in Kryptographie, Protokolldesign, Rust, Android-Entwicklung und Performanceoptimierung erheblich vertiefen. Ebenso habe ich praktische Erfahrung in der Zusammenarbeit mit einem internationalen Open-Source-Projekt gesammelt, inklusive komplexer Review-Prozesse.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Eine neu entwickelte Einladungslogik erwies sich im Detail als problematisch, weil Server über öffentlich gepostete Codes sensible Informationen hätten lernen können. Um die Projektziele zu halten, bin ich vorerst auf ein bewährtes älteres Protokoll zurückgegangen. Die neue Variante werde ich nach Projektende sauber und sicher umsetzen.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer*innen

Alle Ergebnisse des Projekts sind vollständig Open Source und öffentlich dokumentiert. Die zugrundeliegende Implementierung befindet sich in der Delta-Chat-Core-Library (https://github.com/chatmail/core/) sowie in der offiziellen Android-App (https://github.com/deltachat/deltachat-android/). Eine ausführliche technische Beschreibung ist zudem in einem öffentlich zugänglichen Issue dokumentiert (https://github.com/chatmail/core/issues/6884).

Delta Chat für Android ist über den Google Play Store unter sowie über F-Droid verfügbar. Zum Erstellen von Channels müssen diese aktuell als experimentelles Feature unter „Einstellungen → Erweitert → Kanäle“ aktiviert werden. Der Beitritt zu einem Channel ist ohne diese Einstellung möglich und erfolgt niedrigschwellig über einen Einladungslink oder durch das Scannen eines QR-Codes.

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Die Arbeitsplanung hat gut funktioniert. Zwei ungeplante Aufgaben, die Optimierung der Entschlüsselung und das Wiederherstellen des Release-Prozesses, haben zwar kurzfristigen Zusatzaufwand verursacht, aber den Gesamtzeitplan nicht gefährdet. Alle Meilensteine wurden erreicht.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Ein externer PR blockierte zeitweise die Release-Pipeline; ich habe dazu beigetragen, die Situation zu stabilisieren.

Parallel haben andere Teams begonnen, Channels für weitere Plattformen (iOS, Desktop und Ubuntu Touch) zu implementieren, wodurch das Feature deutlich schneller eine breite Nutzendenschaft erreicht und seine praktische Relevanz in der gesamten Delta-Chat-Ökosphäre zunimmt.