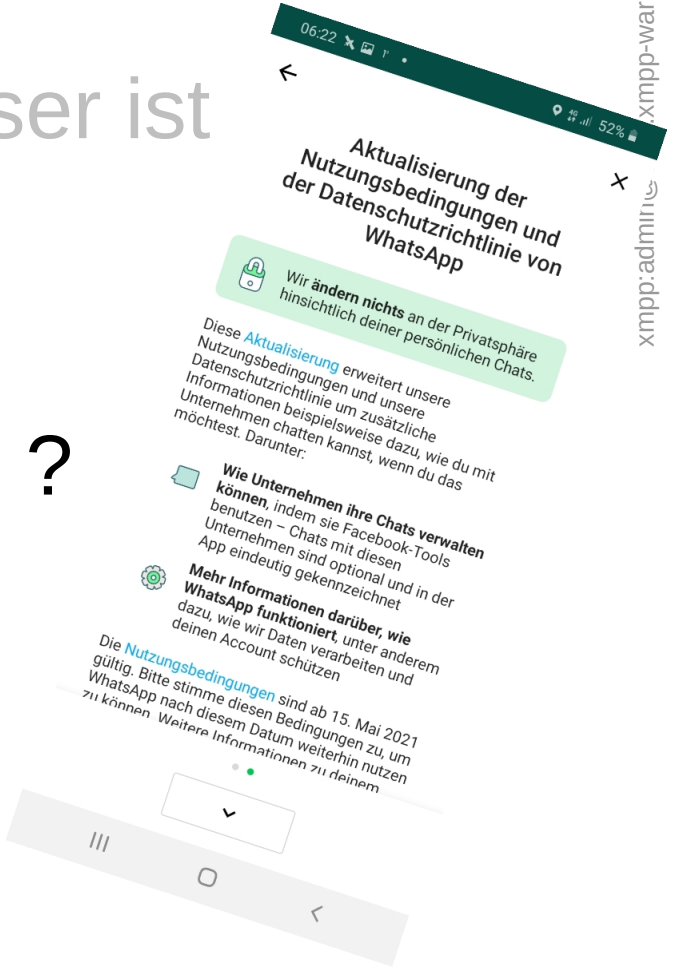
XMPP/Jabber und warum es besser ist

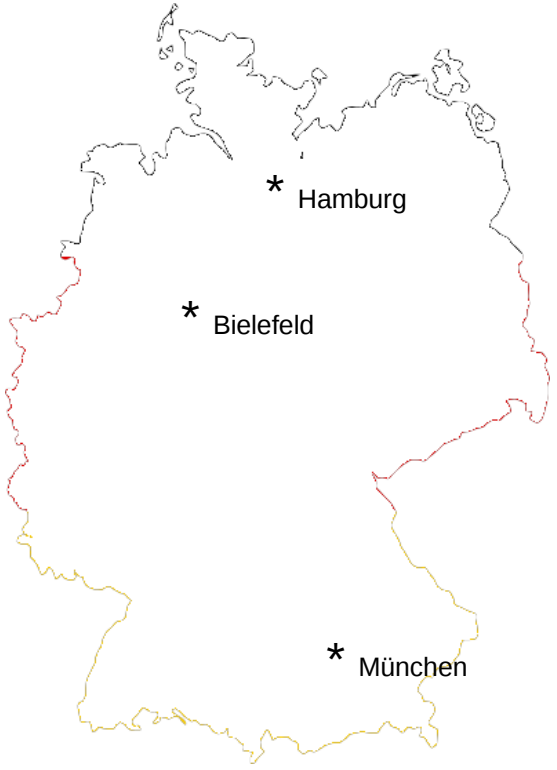
XMPP/Jabber und warum es besser ist

- oder auch -
Warum ist WhatsApp & Co böse ?



Etwas Historie:

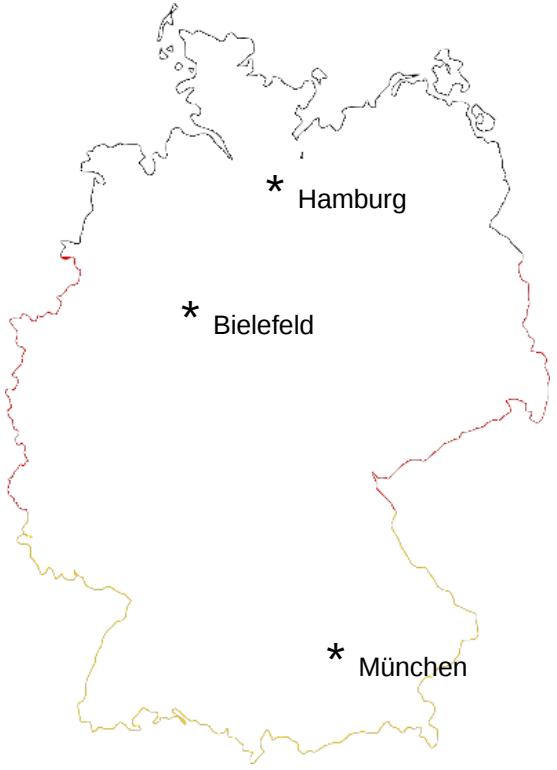
Damals, zur guten alten Zeit in Deutschland….



- Hatte jeder Ort seinen Marktplatz, einen Marktschreier und jeder unterhielt sich mit jedem
- Jeder konnte aus dem Dorffunk alles erfahren
- Es gab aber keinen Austausch von Hamburg nach München

Etwas Historie:

Als dann das Papier erfunden war, wurden Postkarten innerhalb des Ortes verschickt



- Die ersten Adressen wurden eingeführt:
  bürgermeister_von_Bielefeld
  schatzmeister_von_Bielefeld
  bürger1_von_Bielefeld
  ….
  bürgermeister_von_Hamburg
  hafenmeister_von_Hamburg
  ….

- Der Postbote konnte die Karten aber lesen, der Bäckersfrau davon erzählen und die Geschichte war rum im Dorf.

- Der Bürgermeister vertraute zwar seinem Briefträger, aber nicht dem aus dem Nachbarort, also gab es noch keinen Kontakt mit dem Nachbardorf und wenn einer eine Karte von Bielefeld nach Hamburg schreiben wollte, musste er nach Hamburg ziehen und den Hamburger Briefträger beauftragen.

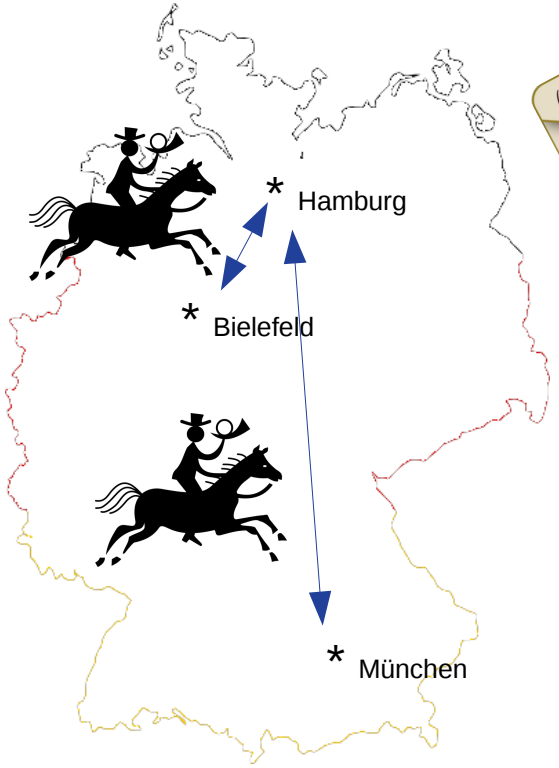
Etwas Historie:

Also wurde es Zeit für Briefumschläge

- Der **bürgermeister_von_Hamburg** konnte nun an den **hafenmeister_von_Hamburg** schreiben OHNE das der Briefträger mitlesen konnte.
- Es war nun auch möglich einen Brief von Bielefeld nach Hamburg zu schicken OHNE dort hin ziehen zu müssen. Also schrieb **bürgermeister_von_Bielefeld** AN **bürgermeister_von_Hamburg**
  Die Grenze war gebrochen, jeder hatte eine eindeutige Adresse, es gab ja nur einen Bürgermeister pro Dorf und die Bürger hiessen bald max.mustermann_von_Bielefeld, oder max.mustermann_von_Hamburg
  ….
- Aber wer garantierte das der Brief unterwegs nicht geöffnet wurde ?

Etwas Historie:

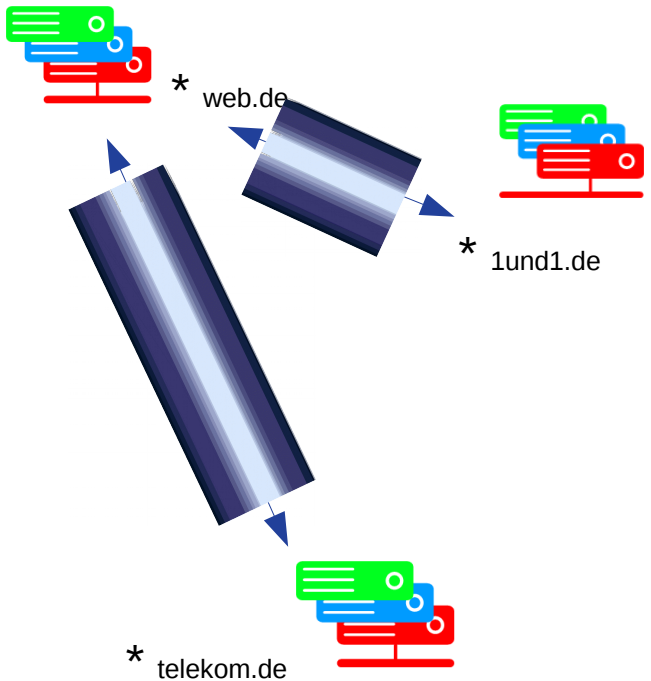
Also wurde es Zeit für Siegel. Daran konnte man erkennen ob ein Brief geöffnet worden ist



- Nun konnte man sicher sein das bei unversehrtem Siegel der Brief korrekt ist. Egal durch wieviele Hände er gegangen ist. Selbst der **bürgermeister_von_München** konnte nun den **bürgermeister_von_Hamburg** anschreiben und keiner unterwegs wusste was im Brief stand.
- Keiner musste mehr einen zweiten Wohnsitz haben
- Keiner musste Angst vor geänderten Inhalten haben
- **Es war also möglich ohne Umzug egal von wo nach wo zu schreiben und sich sicher sein zu können das keiner den Brief las bzw es wäre aufgefallen.**

Etwas jüngere Vergangenheit:

Die Technik schritt voran ...und aus Brief wurde eMail, die Städte wurden jetzt Provider aber ansonsten blieb alles beim alten.

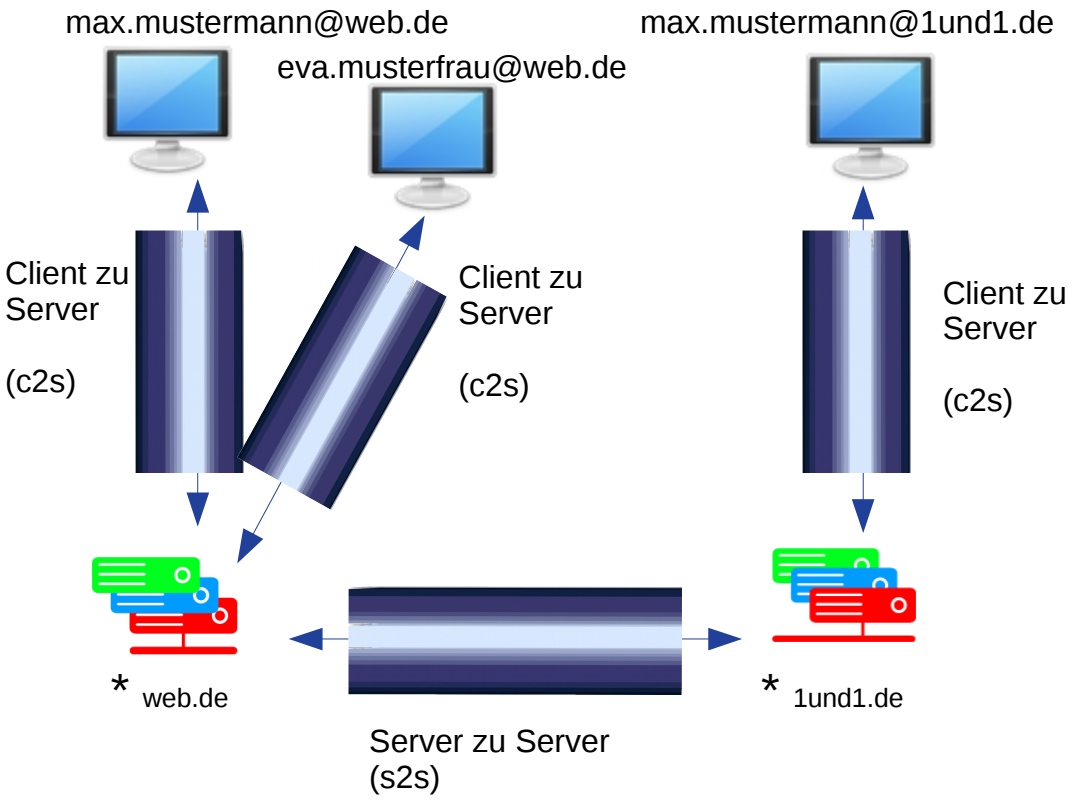


- Der Postkarte wurde zur eMail
- Die Stadt zum Provider
- Der Briefträger wurde zum Netzwerk
- Der Posträuber zum Hacker
- Die Adressen änderten sich
  bürgermeister.Hamburg@1und1.de
  bürgermeister.München@telekom.de
  max.mustermann@web.de
  max.mustermann@1und1.de
- Der Briefumschlag wurde zum Tunnel
- Das Siegel zur Verschlüsselung

- **Es war also möglich als web.de-Kunde an jemanden von 1und1.de zu schreiben und durch die Tunnel/Verschlüsselung konnte keiner mitlesen.**

Etwas jüngere Vergangenheit:

Aber wie funktioniert es genau das man von web.de an web.de oder an 1und1.de schreiben kann ?

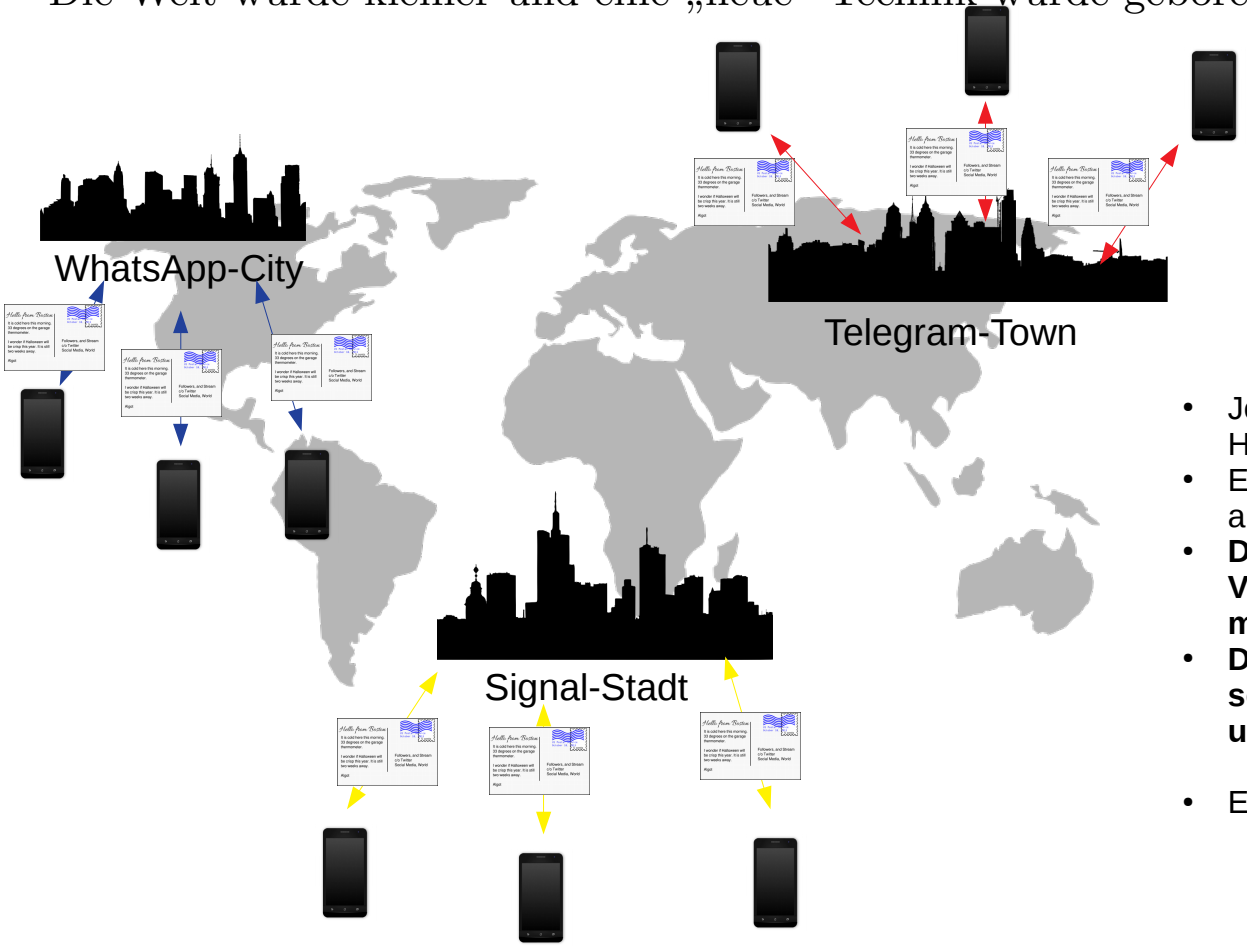


- Max.mustermann@web.de baut eine Verbindung mit seinem Mail-Provider auf und adressiert seine eMail
- Ggf benutzt er dabei einen Tunnel, ansonsten liest jeder unterwegs mit
- Web.de nimmt die eMail an und unterscheidet ob es lokal bleibt oder nicht.
- Bei eva bleibt die Mail bei web.de
- Beim Ziel 1und1 verbindet sich web.de mit dem Server von 1und1.de und gibt die eMail dort ab
- 1und1.de liefert die eMail an max.mustermann@1und1.de aus

- Wenn jemand max.mustermann@**web.de** kennt, bedeutet das noch lange nicht das er auch max.mustermann@**1und1.de** kennt. Es können ja nur Namensgleichheiten sein und ein eindeutiger Identifizierungscode ist nicht vorhanden.
  Der eine Max wohnt in Berlin, der andere in Kiel
- Bis auf den jeweiligen Provider weiss keiner wer Max ist
- **Leider sind die Tunnel bei Provider unterbrochen und man muss ihm vertrauen das er nicht mitliest**

Etwas Gegenwart (ca. 2015):

Die Welt wurde kleiner und eine „neue“ Technik wurde geboren, aber ……

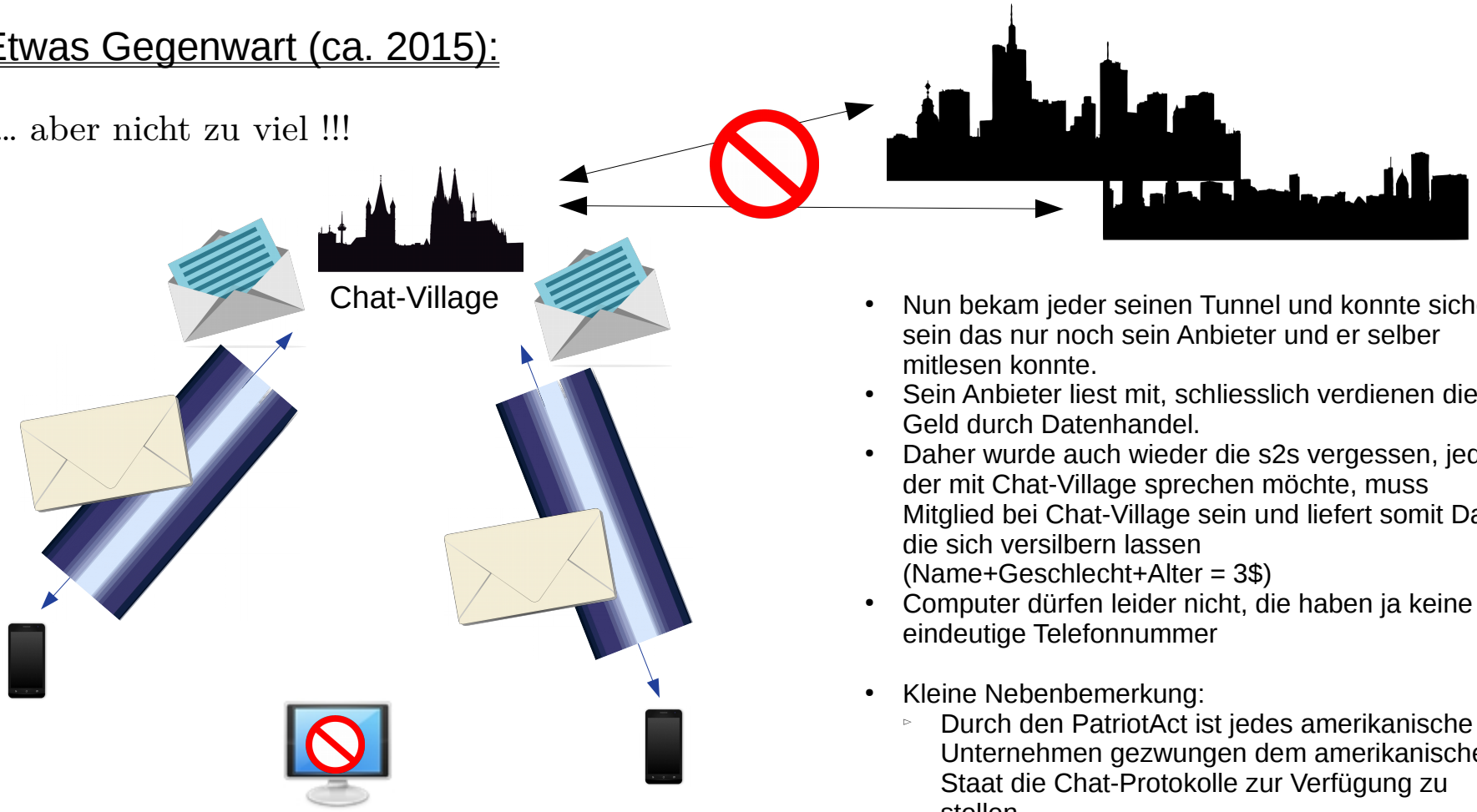


- Jeder bekam kostenlos eine eindeutige Adresse mit Hilfe seiner weltweit eindeutigen Telefonnummer
- Er brauchte sich auch kein Passwort mehr ausdenken, das machte der Provider für ihn
- **Da der Provider aber keinen Tunnel zur Verfügung stellte, konnnte jeder unterwegs alles mitlesen**
- **Die Funktion s2s wurde irgendwie vergessen, somit konnte sich nicht zwischen den Städten unterhalten werden.**

- Es musste nachgebessert werden...

Etwas Gegenwart (ca. 2015):

… aber nicht zu viel !!!

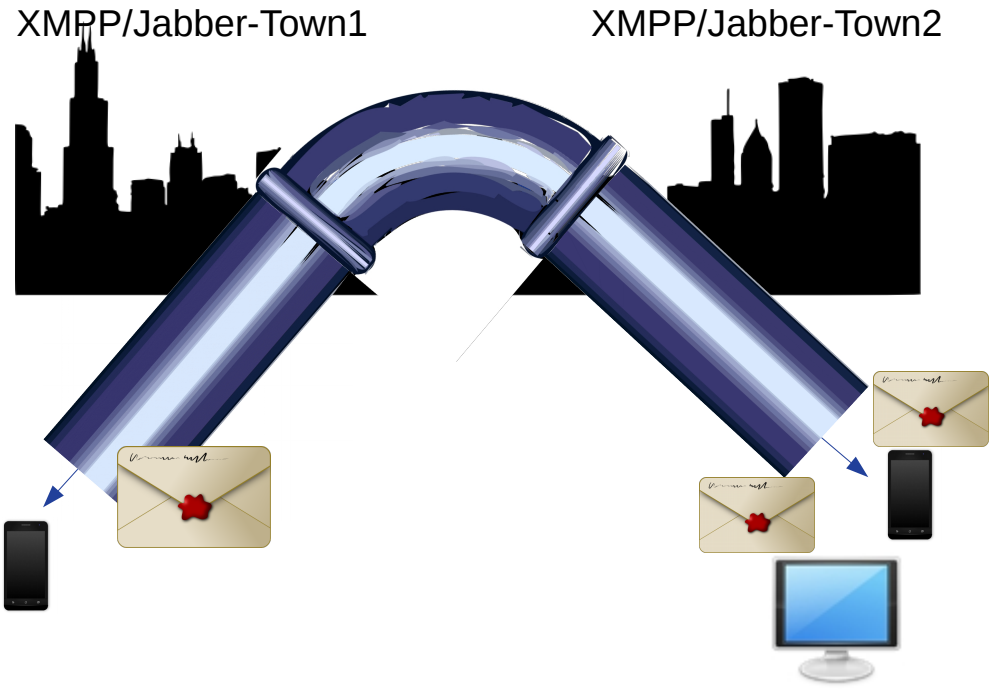


- Nun bekam jeder seinen Tunnel und konnte sicher sein das nur noch sein Anbieter und er selber mitlesen konnte.
- Sein Anbieter liest mit, schliesslich verdienen die ja Geld durch Datenhandel.
- Daher wurde auch wieder die s2s vergessen, jeder der mit Chat-Village sprechen möchte, muss Mitglied bei Chat-Village sein und liefert somit Daten die sich versilbern lassen (Name+Geschlecht+Alter = 3$)
- Computer dürfen leider nicht, die haben ja keine eindeutige Telefonnummer

- Kleine Nebenbemerkung:
  - Durch den PatriotAct ist jedes amerikanische Unternehmen gezwungen dem amerikanischen Staat die Chat-Protokolle zur Verfügung zu stellen.
  - Ist beim Russen nicht anders
  - Und beim Franzosen sind es nur Papierrollen als Tunnel

Etwas Vergangenheit (ca. 1998):

… aber nicht zu lange her !!!



- Die Grundlagen von WhatsApp & Co ist das XMPP-Protokoll, sie haben es halt bloss nicht komplett umgesetzt, sie haben ja den s2s-Teil unterschlagen.
- Der c2s-Teil ermöglicht es mit verschiedenen Geräten gleichzeitig unter einer Kennung erreichbar zu sein, auch das wurde bei den anderen nicht komplett umgesetzt.
- Auf allen Geräten sind die Nachrichten Ende-zu-Ende verschlüsselt (Siegel)
- Man kann verschlüsselte oder unverschlüsselte, private oder öffentliche Gruppen erstellen und beitreten
- **Man kann seinen eigenen Server betreiben und dem Netzwerk hinzufügen, somit bleiben die Daten bei einem selbst**
- **Es gibt keinen zentralen Server**
- **Es gibt keine Telefonnummer !!!**

Vor-/Nachteile:

... alles Ansichtssache

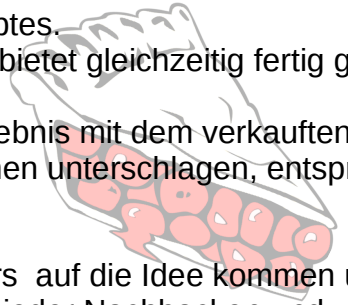
- Dadurch das man einen eigenen Server aufbauen kann, ist man nicht abhängig von den anderen
- Du hast eine EIGENE Chat-Adresse, also kein @whatsapp oder @signal sondern zB **vorstand@flotte-nadeln-strickverein.de** oder **kassenwart@sportverein-hinterm-wald-links.de** sofern dir die Domain gehört.
- Sollte der Staat Zugriff auf die Daten verlangen, bekommt man es als erster mit, schliesslich müssen sie ja beim Betreiber nachfragen
- Ein **ernst@i-want-more-beer.com** IST NICHT der **hutzelbaer@märchenwald.de** obwohl sie beide vom gleichen Handy aus tippen
- Es erfolgt KEIN Zugriff auf dein Adressbuch, es wird nichts hochgeladen, deine Kontaktliste (Roster) ist also leer und muss sich erst wie dein eMail-Adressbuch füllen
- Dadurch gibt es kein zentrales Userverzeichnis, somit ist dein Account nur den Leuten bekannt denen du ihn mitteilst.
  Du musst nicht deine Telefonnummer raus geben sondern nur eine deiner XMPP/Jabber-Kennungen welche du jederzeit wieder ändern oder löschen kannst
- Es gibt verschiedene Client-Programme für verschiedene Geräte/Betriebssysteme mit verschiedenen Funktionen, gefällt dir eins nicht, nimm das nächste
- Durch die Verschlüsselung kannst du gesichert kommunizieren (ja ich weiss, ihr habt alle nichts zu verbergen, was verdienst du noch mal, was ist beim Besuch vom Psychologen raus gekommen und was hat die Liebesdame dir letztes mal abgeknöpft als du mit deinen Sonderwünschen kamst ? Und das dein Schatz ihr Weihnachtsgeschenk in deinem Amazon-Warenkorb gesehen hat ist auch egal)
- Da jedes Gerät einen eigenen Schlüssel hat, bekommst du mit wenn dein Gegenüber sein Gerät austauscht oder ausgetauscht bekommt hat
- Da es sich um ein Protokoll handelt, gibt es diverse Entwicklungen von Client- und Server-Software, welche zum Teil als Open-Source zur Verfügung gestellt wird

- ....

Was ist OpenSource, was ist Quellcode, was ist der Vorteil einer Norm ?:

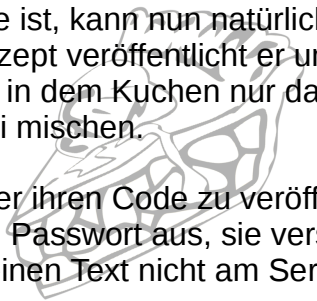
Bei OpenSource stellt der Entwickler seinen Quellcode öffentlich zur Verfügung und jeder ist (je nach Lizenz) berechtigt diesen Code zu ändern, zu benutzen ...

Der Quellcode eines Programms ist vergleichbar eines Backrezeptes.
Der Entwickler veröffentlicht zB ein Rezept für Kirschkuchen und bietet gleichzeitig fertig gebackenen Kirschkuchen an.



Nun gibt es Leute die das Rezept nachbacken und dann das Ergebnis mit dem verkauften Kuchen vergleichen.
Sollte der Entwickler also in seinem Kirchkuchenrezept die Kirschen unterschlagen, entspricht der selbst gebackene Kuchen nicht dem verkauften Kuchen und man solle misstrauisch werden.

Da das Rezept OpenSource ist, kann nun natürlich jemand anders auf die Idee kommen und die Kirschen gegen Birnen austauschen. Das neue Rezept veröffentlicht er und jeder kann wieder Nachbacken und vergleichen.
Somit ist sicher gestellt das in dem Kuchen nur das drin ist was im Rezept steht, also keiner kann mal eben Zucker gegen Salz austauschen oder Arsen bei mischen.



WhatsApp weigert sich leider ihren Code zu veröffentlichen, du musst ihnen glauben das sie kein Schindluder treiben.
Sie denken sich für dich ein Passwort aus, sie versiegeln für dich deinen Text und sie stellen ihn zu.
Woher weisst du das sie deinen Text nicht am Server wieder auspacken, lesen und neu verpacken ? Sie besitzen dein Siegel.

Telegram ist das russiche WhatsApp, also kein Unterschied ob nun der Ami oder der Russe mit liest.

Was ist OpenSource, was ist Quellcode, was ist der Vorteil einer Norm ?:

… und zu überprüfen ob er nicht die Katze im Sack bekommt

..und Signal oder Threema ?

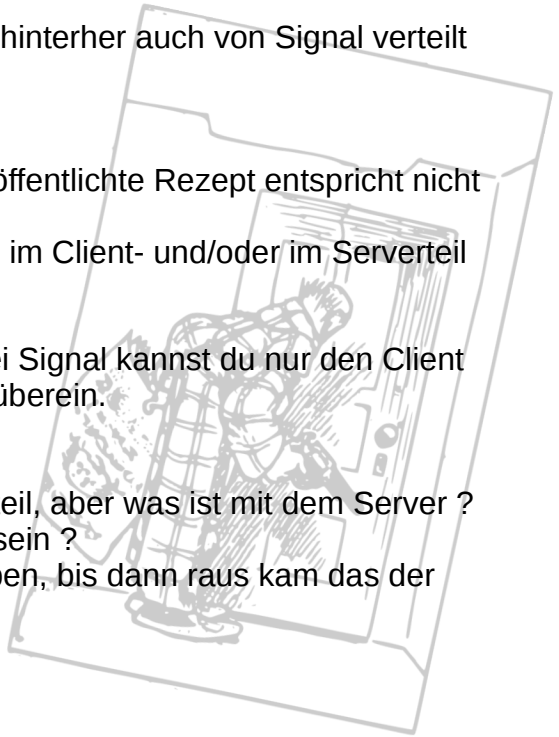
Signal ist bereit das Backrezept seiner Clientsoftware zu veröffentlichen.
Die Bäckermeister haben es überprüft und festgestellt das im Rezept genau das drin steht was hinterher auch von Signal verteilt wird. Löblich…

Aber wir brauchen ja auch noch einen Server-Teil..
Leider kommt beim Nachbacken des Servers NICHT das raus was rauskommen sollte, das veröffentlichte Rezept entspricht nicht dem verwendeten Produkt. Also sollte man dort auch vorsichtig sein, oder ?
Vor allem nachdem der deutsche Gesetzgeber ja nun auch auf Hintertürchen besteht und diese im Client- und/oder im Serverteil stecken können.

Bei WhatsApp/Telegram musst du glauben „Wir haben weder was im Client noch im Server“, bei Signal kannst du nur den Client überprüfen, da muss es dann im Serverteil sein, und dessen Backrezept wiederum passt nicht überein.
Nachtigall, ick höre dir stampfen

Bei Threema ist das Backrezept erst seit Dezember 2020 öffentlich, und da auch nur der Clientteil, aber was ist mit dem Server ?
Ein Stück Software einer Firma die in der Schweiz sitzt sollte doch über jeden Zweifel erhaben sein ?
Das dachten die Regierungen auch die für ihre Minister ein schweizer Cryptophone gekauft haben, bis dann raus kam das der Hersteller ein Joint-Venture vom BND und der NSA war.

Bleibt noch XMPP/Jabber ?



Was ist OpenSource, was ist Quellcode, was ist der Vorteil einer Norm ?:

… und wie sieht es nun bei XMPP/Jabber aus ?

Es gibt eine „Norm“ das jedes Fahrzeug an der roten Ampel stehen bleiben muss, egal ob Auto, LKW, Mopped, Fahrrad, …
Nun kann jeder der sich an die Norm hält am Strassenverkehr teilnehmen, es gibt auch verschiedene Erbauer von Fahrzeugen welche sich an Normen halten, es gibt kein „Nur-Aral-Auto“ oder ein „Nur Shell-Mopped“

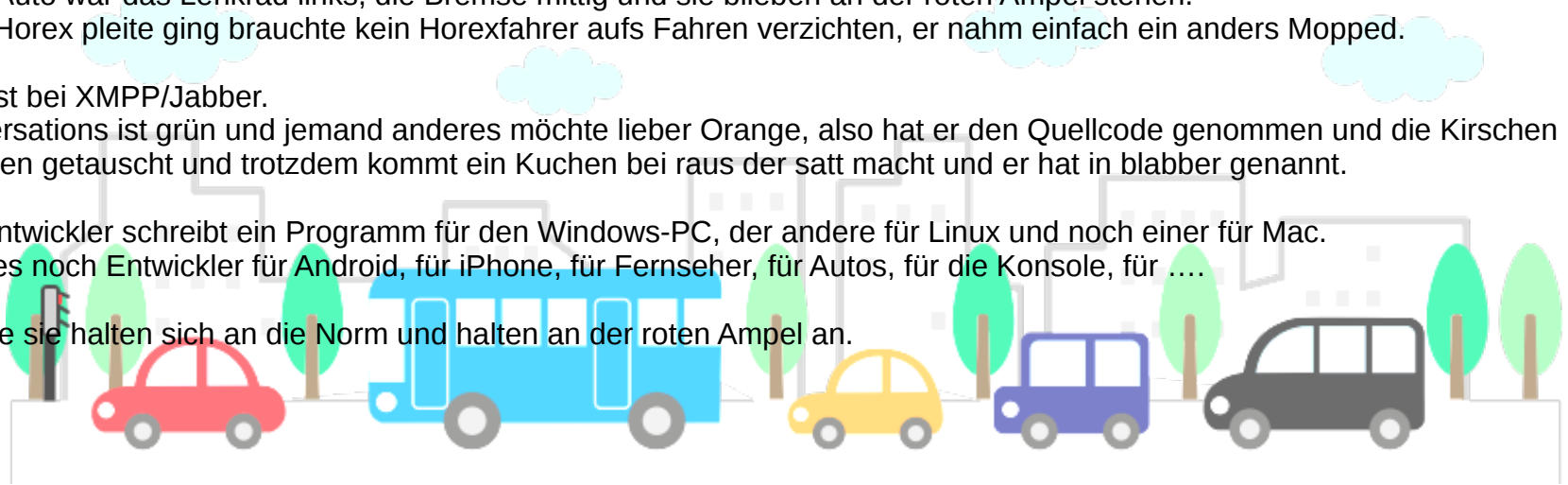
Dem alten Ford gefielen die Mercedes nicht und er baute seine eigenen Autos, dem Herrn Honda gefielen die Kawasakis nicht und er baute seine Moppeds …

Jeder konnte dann „sein“ Fahrzeug kaufen, das was ihm gefiel.
Bei jedem Auto war das Lenkrad links, die Bremse mittig und sie blieben an der roten Ampel stehen.
Selbst als Horex pleite ging brauchte kein Horexfahrer aufs Fahren verzichten, er nahm einfach ein anders Mopped.

Dasselbe ist bei XMPP/Jabber.
Das Conversations ist grün und jemand anderes möchte lieber Orange, also hat er den Quellcode genommen und die Kirschen gegen Birnen getauscht und trotzdem kommt ein Kuchen bei raus der satt macht und er hat in blabber genannt.

Der eine Entwickler schreibt ein Programm für den Windows-PC, der andere für Linux und noch einer für Mac.
Dann gibt es noch Entwickler für Android, für iPhone, für Fernseher, für Autos, für die Konsole, für ….

Hauptsache sie halten sich an die Norm und halten an der roten Ampel an.



Was ist OpenSource, was ist Quellcode, was ist der Vorteil einer Norm ?:

… und wie sieht es nun bei XMPP/Jabber aus ?

Was ist mit den geforderten Hintertürchen ?

Der eine Entwickler kommt aus Deutschland, der andere aus Russland und noch einer aus China und einer aus Brasilien und aus …
Welches Gesetz soll denn da jetzt gelten ? Müssen sich die Russen an deutsche Gesetze halten ? Muss der Brasilianer den Chinesen Zugriff auf die Daten geben ?

Das gleiche bei dem Serverteil, muss der russische/englische/deutsche/amerikanische Serverentwickler dem deutschen Staat Zugriff gewähren ? Muss ich seinen Server verwenden wenn sein Backrezept nicht mit dem Produkt übereinstimmt ?

Hauptsache sie halten sich alle an die Norm und bleiben an der roten Ampel stehen.

Es gibt für den Staat nicht **den** Ansprechpartner, **den** Produkthersteller, keine zentrale Zugriffsstelle.
Ich kann meine mamorierte tierartengeschützte Spezialwolle bei einem Bekannten auf einem afghanischen Server ordern, der wiederum in Russland bestellt, der wiederum aus China den Order platziert und mir dann aus der Lüneburger Heide liefert.

Bis der Staat weiss wo ich die Wolle her habe oder warum der Alpaka-Züchter einen Beutel in der Lüneburger Heide verbuddelt und wer sie sich abgeholt hat, habe ich schon die ersten 300 Paar warme Socken fertig.

Die Zukunft ?

… und wie sie aussehen könnte

Warum das ganze ?

Jeder Regierung, jede Firma, will nur unser Bestes, sei es unser Geld, unsere Daten, unsere Freiheit.
Klar ist es bequemer und einfacher sich treiben zu lassen und nur noch die vorgefertigten Häppchen zu konsumieren.

Es gibt eine Norm für Telefonnummern (ITU-T E.164), und sie begrenzt die Anzahl auf 15 Stellen, 2 gehen für die Länderkennung weg, bleiben noch 13. Um den Hashwert von 0 000 000 000 001 bis 9 999 999 999 999 (das sind 10 Billion Möglichkeiten), zu berechnen, braucht es bei ca 5GB/s (xxHash) knappe 2000sec = 34 Minuten

Da in Deutschland kein Erwerb von anonymen Telefonkarten mehr möglich ist, ist eure Anonymität bei einer gehashten Telefonnummer nicht wirklich gegeben, oder ? Und ob der Inhalt eurer Nachricht nicht wirklich doch lesbar ist ?

Und da jeder der sich nicht an die Norm hält schon von Grund auf verdächtig ist, sollte das der wichtigste Beweggrund sein. Abgesehen von der AGB-Änderung bei WhatsApp „Wir verkaufen NIE eure Daten“ zum „Wir führen deine Daten mit Facebook zusammen“, oder die belauschten Polizei-WhatsApp-Gruppen, gibt es ja auch ständig Nachbesserungen bei den Überwachungsgesetzen.

Wer von euch bekommt es schon mit wenn bei WhatsApp/Signal/Threema/Telegram nach euren Verbindungsdaten gefragt wird weil ihr mit euren langen Haaren doch mit Sicherheit zum Linksradikalen Mob gehört und die Glatze da vorne ein untrügerisches Kennzeichen für einen NeoNazi ist



Die Zukunft ?

… und wie wir sie uns schaffen könnten.

Der Betrieb eines XMPP-Servers kostet nicht viel Geld, manche haben sogar schon einen Server wo sie ihre WebSeite drauf laufen lassen und zur Not gibt es noch freie kostenlose XMPP-Betreiber wo ihr eure Domäne hinterlegen könnt oder einfach nur einen Account generiert.

Also was spricht dagegen einen eigenen Chat auf zu machen, vergleichbar einem Vereinsheim ?
Einen öffentliche Raum mit dem Namen ***Kaffeeküche@….***. und einem privaten ***Hinterzimmer@ ….*** und einem privaten ***Mitarbeiter@…***. ?

So kann jeder bei jedem in der Kaffeeküche mal „Hallo“ sagen, jeder kann nachfragen „Seid ihr morgen da ?“, jeder bekommt mit wenn eine öffentliche Veranstaltung geplant ist.

Jeder ? Nicht wirklich, nur die welche sich bei euch in der Kaffeeküche aufhalten.
Da ihr sie nicht in das Hinterzimmer einladet oder da sie keine Mitarbeiter sind und somit nicht in Mitarbeiter kommen, bleibt es bei den Leuten die schon bei euch waren, die euch schon mal besucht haben. Ganz wie im wirklichen Leben.

Und was wirklich öffentliches ?
Was spricht gegen ein ***SchwarzesBrett@kneipen-szene-in-owl.de*** oder ein **Veranstaltungen@hamburger-strickszene.de** oder ganz gross gesponnen ein ***VeranstaltungsKalender_Nord@sportvereine-deutschland.de***
und einem **Stammtisch_Sued@sportvereine-deutschland.de** ?

Nichts, aber auch gar nichts spricht da gegen, ausser die Bequemlichkeit sich kein Passwort überlegen zu müssen.

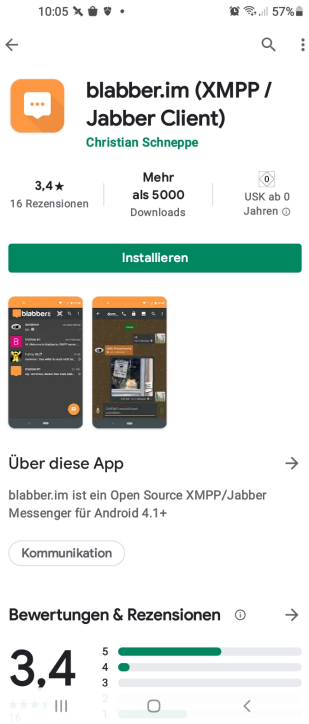
Das hält euch davon ab euch eure Freiheit wieder zu holen.

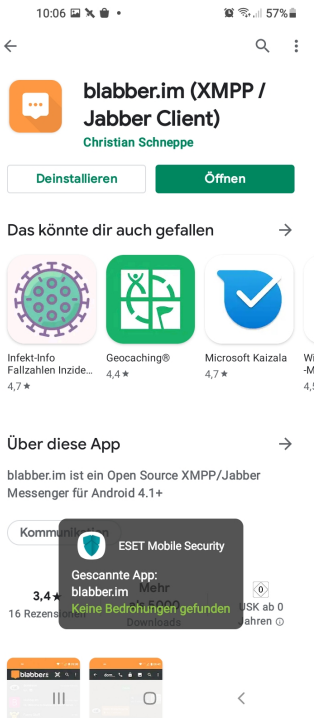
Praktische Übungen

Praktische Übungen:

Hier nun die Installation/Konfiguration am Beispiel vom kostenlosen Blabber auf einem Android-Handy

Installation aus dem Google-Store, ein Sideload via F-Droid ist natürlich ebenfalls möglich



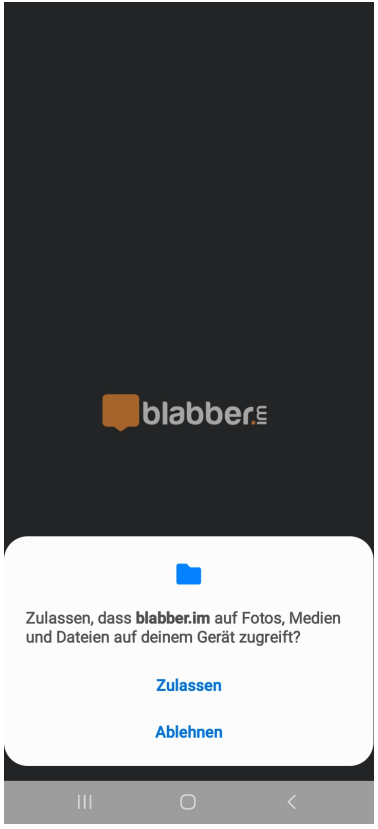


Praktische Übungen:

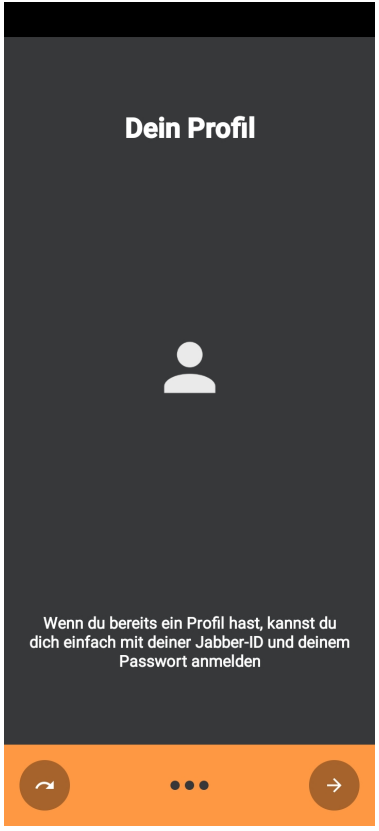
Das Intro

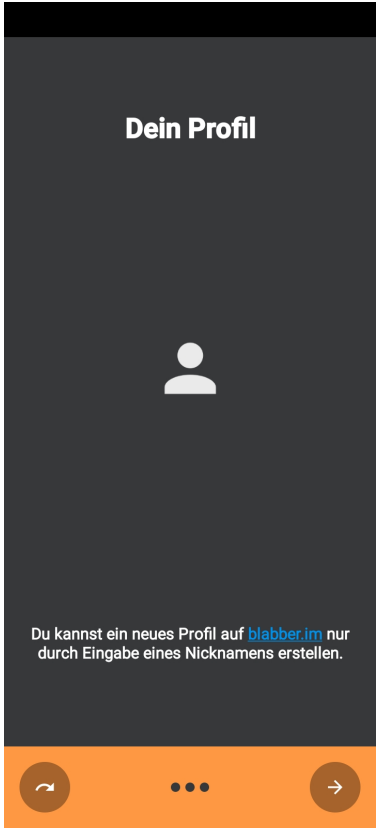
Praktische Übungen:

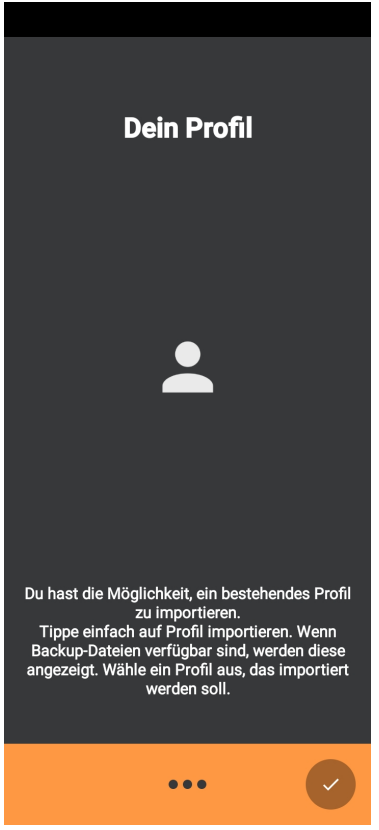
Das sollte man zulassen damit Bilder versendet werden können



Wir richten unseren Account ein

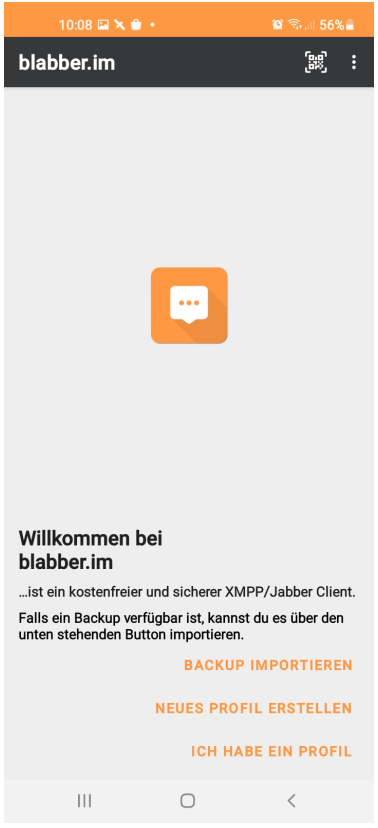






Praktische Übungen:

Wir richten unseren Account ein



Da wir nicht von einem anderen Gerät umziehen, haben wir kein BackUp welches wir importieren könnten.

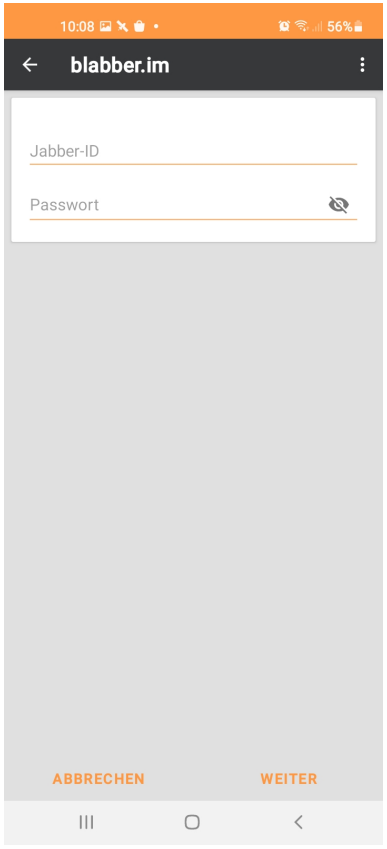
Ein neues Profil benötigen wir aber auch nicht, wir wollen ja keinen mglw kostenpflichtigen Account bei ihm @blabber.im sondern zB beim @auspuffschnüffler-deutschland.de

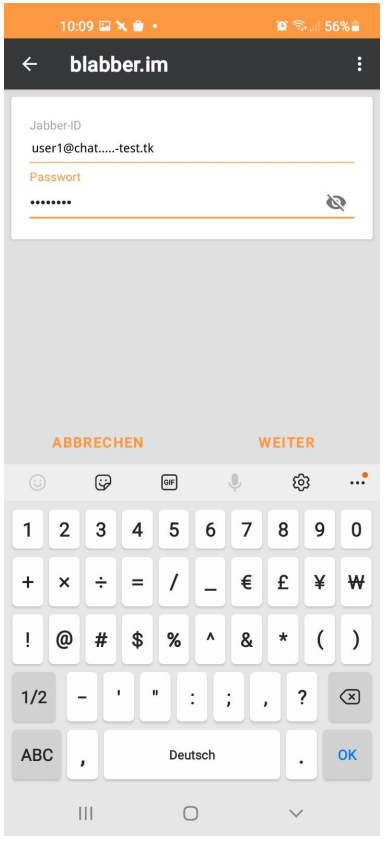
Es gibt genug kostenlose Accountanbieter, aber wir haben ja schon einen. (siehe Zugangsdaten bzw drittletzte Seite)

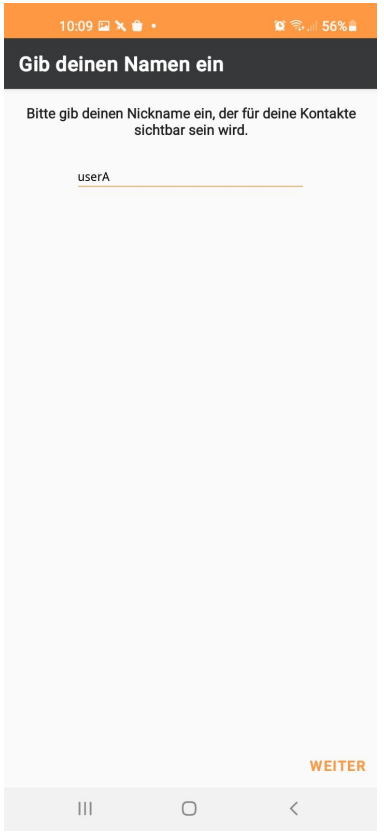
Also „Ich habe ein Profil“

Praktische Übungen:

Wir richten unseren Account ein





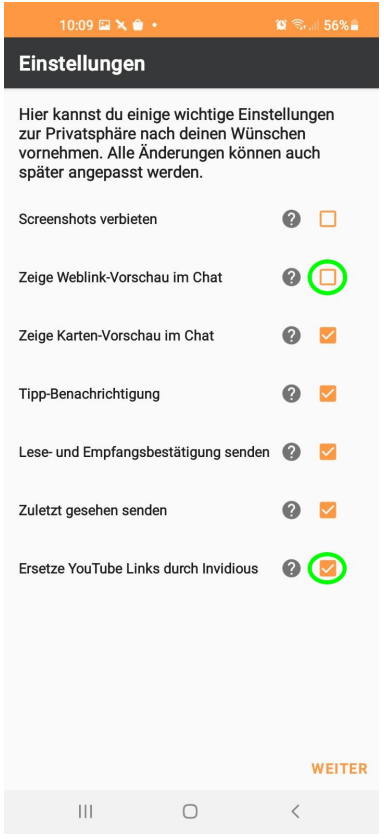


Wir haben einen Account als user1@chat.xmpp-warum.mooo.com und tragen diesen mit seinem Passwort ein.
(nur beim Vortrag, nicht in der Download-Version)

Gleichzeitig können wir noch einen Anzeigenamen vorgeben der in öffentlichen anonymen Gruppen angezeigt wird.

Praktische Übungen:

Wir richten unseren Account ein



Nun können wir die Einstellungen für den Acount vornehmen, entgegen der Default-Einstellungen würde ich die den Haken bei „Weblink-Vorschau“ raus nehmen und den bei „Ersetze Youtube durch Invidious“ aktivieren.

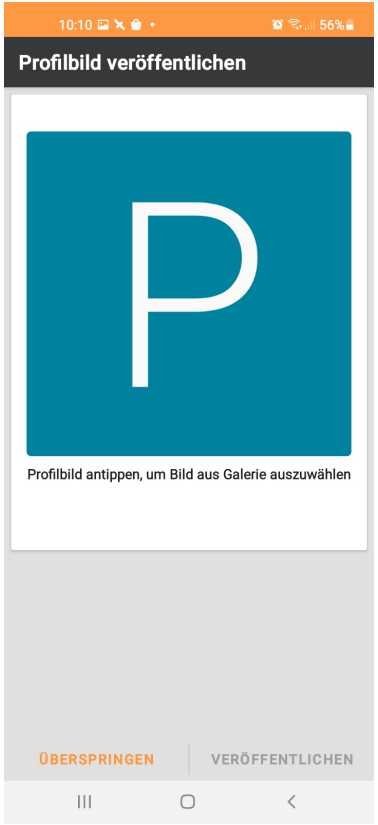
Durch den Weblink-Vorschau baut der Client eine Verbindung zur Webseite auf, obwohl du das vllt gar nicht möchtest.
Da kann der Webserver-Betreiber dann aber sehen von welcher Adresse du kommst und dich ggf gezielt angreifen oder Viren unterschieben.

Das Ersetzen der Youtube-Links durch Invidious hindert Youtube daran dich zu identifizieren und du kannst so auch eine Ländersperre umgehen und die Videos runter laden, dafür kann dann aber der jeweilige Invidious-Betreiber sehen welche Videos du dir angesehen hast, aber wer sagt dir das du immer den selben nehmen musst ?

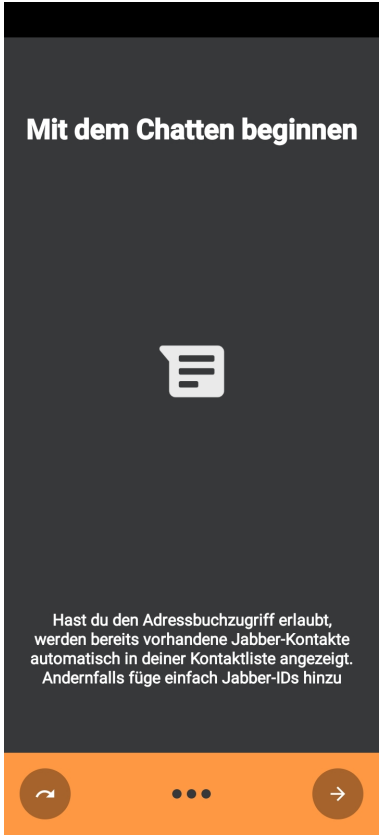
Praktische Übungen:

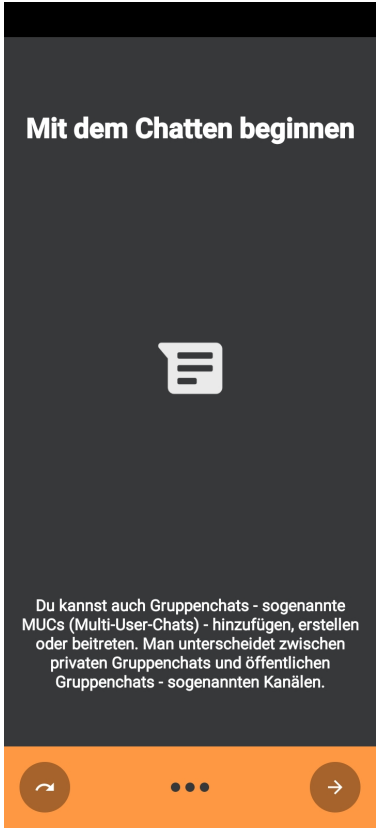
Wir richten unseren Account ein

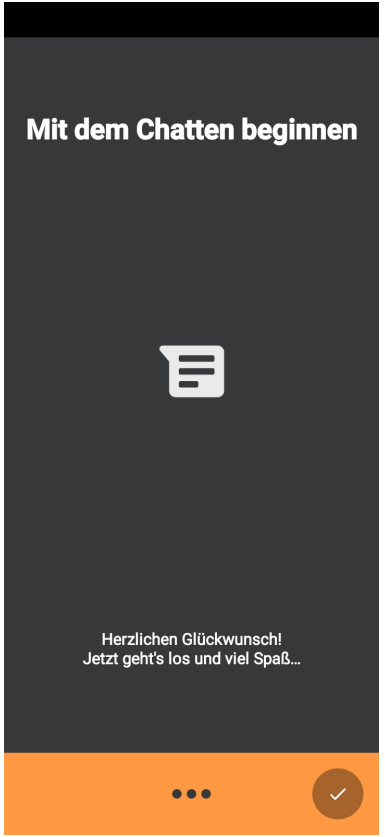
Nun können wir nun noch einen Avatar veröffentlichen



Noch ein wenig Intro und Begriffserklärung



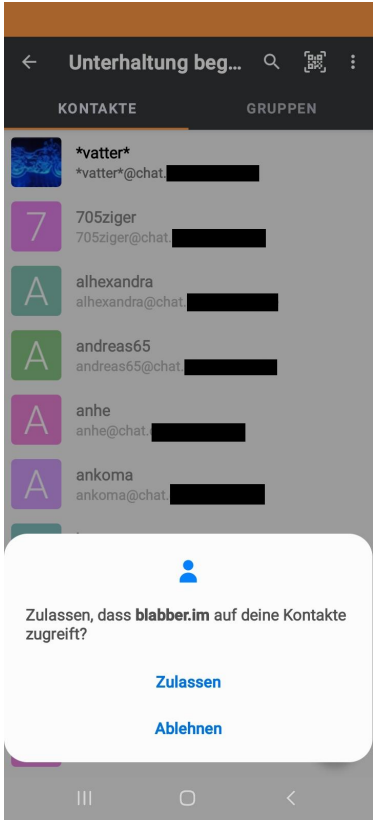




Praktische Übungen:

Wir richten unseren Account ein

...und wir sind fertig



Durch den Zugriff auf die lokalen Kontakte wird einmalig geguckt ob du schon XMPP/Jabber-Kontakte in deinem Adressbuch hast.

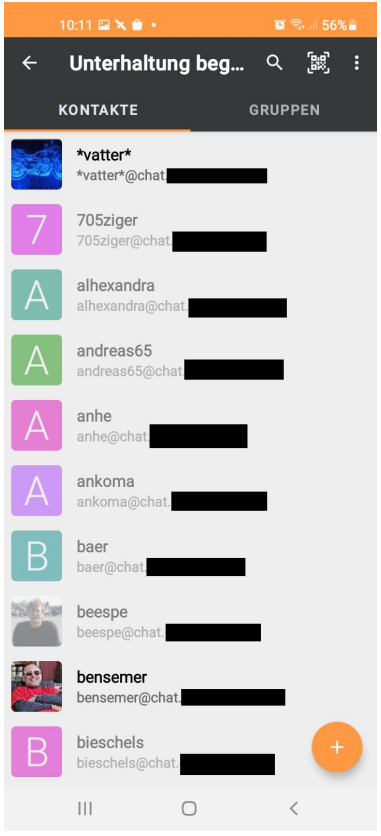
Die hier jetzt schon angezeigten Kontakte sind NICHT in meinem Adressebuch, aber durch ein anderes von mir benutztes Programm schon bekannt und in meinem Roster gespeichert.
Daher werden sie mir schon angezeigt.

Bei euch wird die Liste mglw noch leer sein, ihr baut euch euren Roster genau so auf wie damals eurer eMail-Adressbuch.

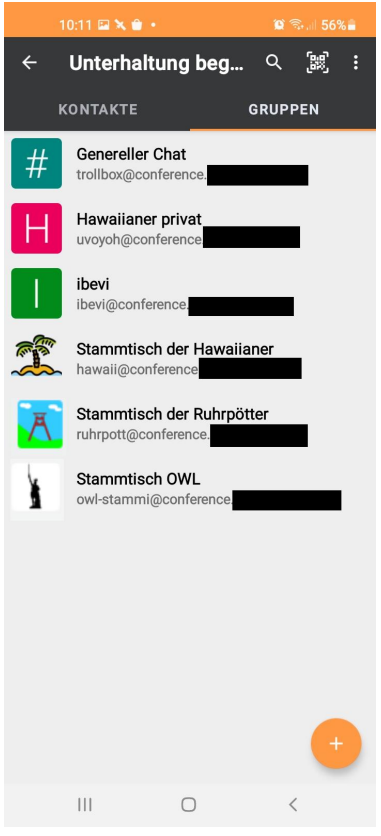
Praktische Übungen:

Wir richten unseren Account ein

Die ausgegrauten Kontakte sind meine zZt nicht online Bekannten



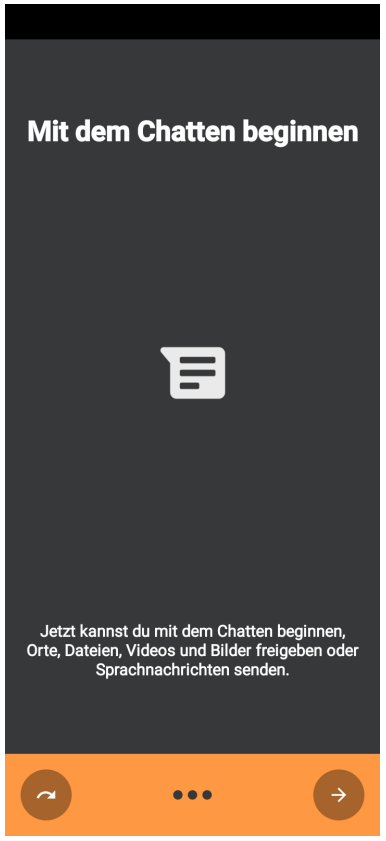
Und natürlich gibt es auch ein paar Gruppen wo ich dabei bin.

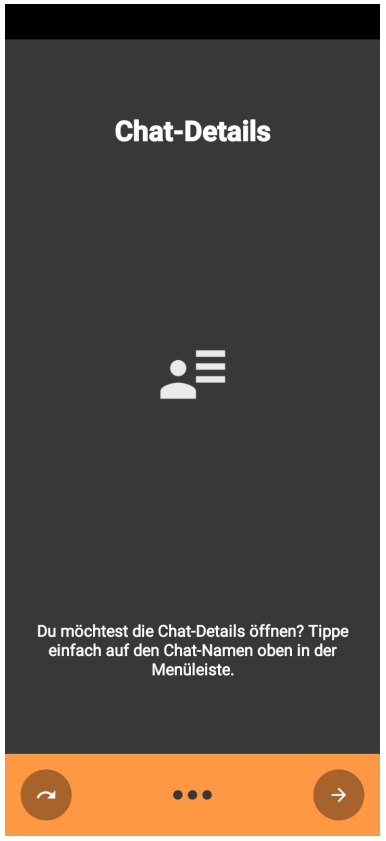


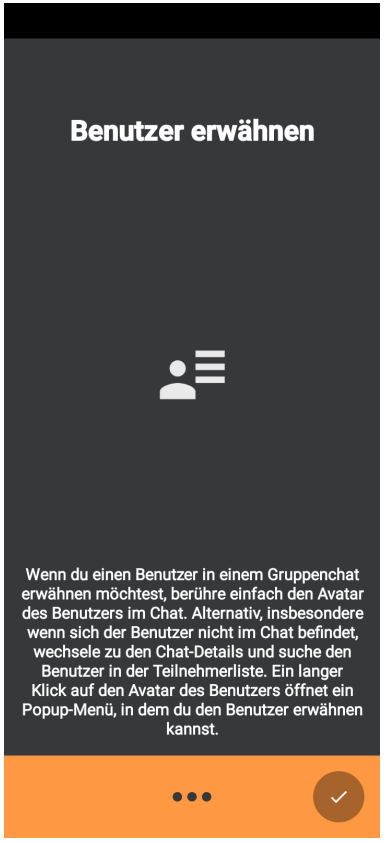
Aber jetzt erst mal auf „Unterhaltung beginnen“

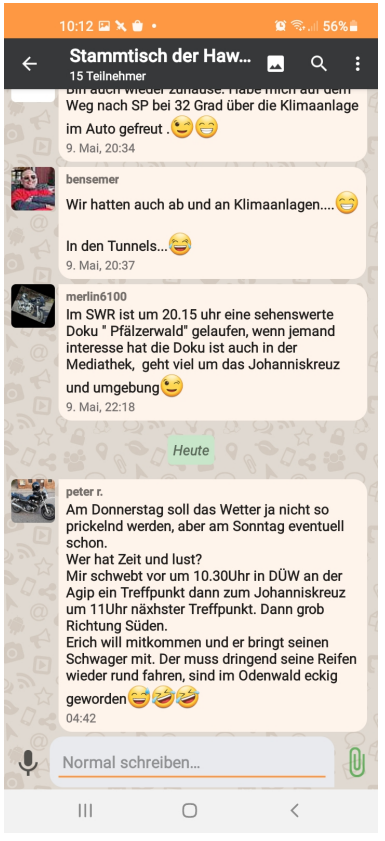
Praktische Übungen:

Wir chatten in der Gruppe









Hierbei handelt es sich um einen unverschlüsselten, anonymen Gruppenchat.

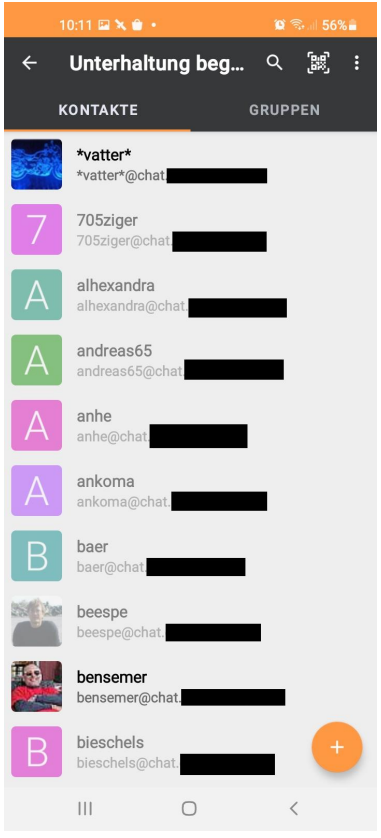
Das ist am „Normal schreiben“ unten im Eingabefeld zu erkennen. Weiterhin sind die Kennungen nicht sichtbar sondern nur die Spitznamen.

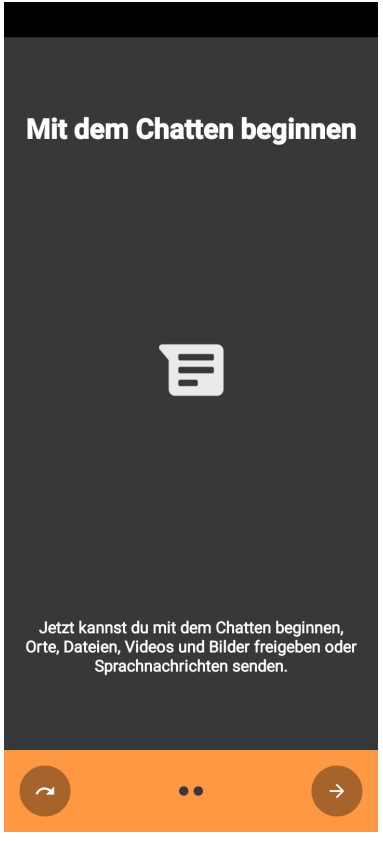
Mit der „Büroklammer“ sind Dateien/Bilder anhängbar.

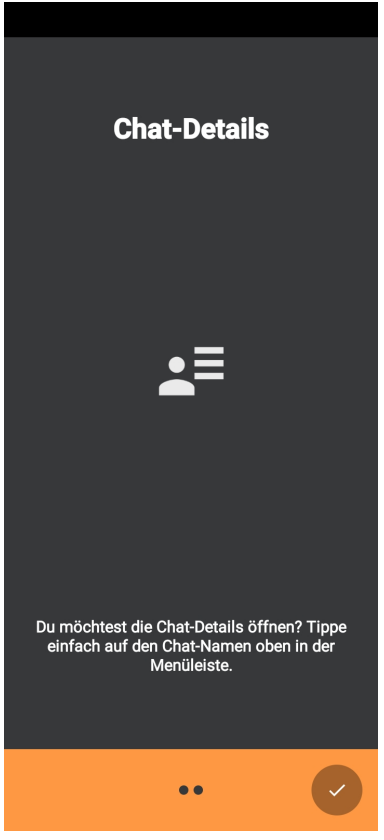
Praktische Übungen:

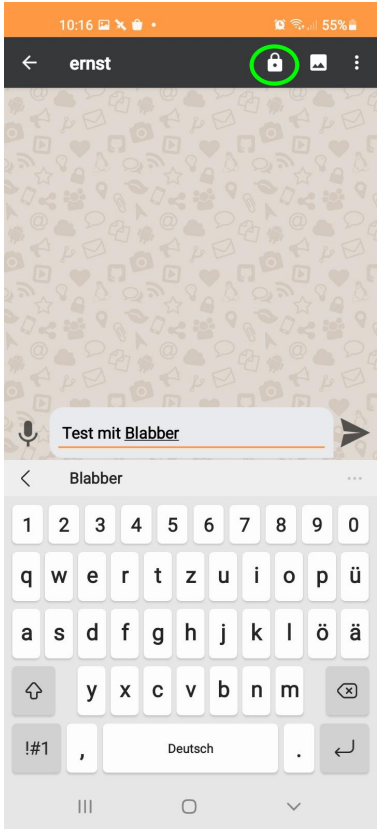
Wir chatten privat und verschlüsselt

Wir suchen uns einen unserer Bekannten aus der Liste oder tragen durch ein Klick auf das Plus unten rechts, einen neuen Kontakt ein.





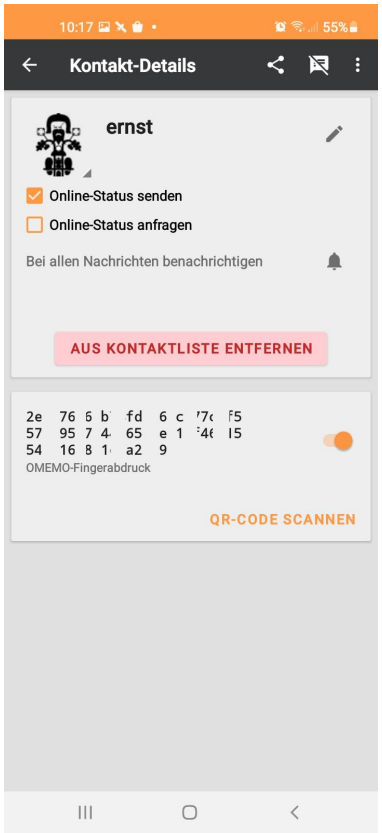


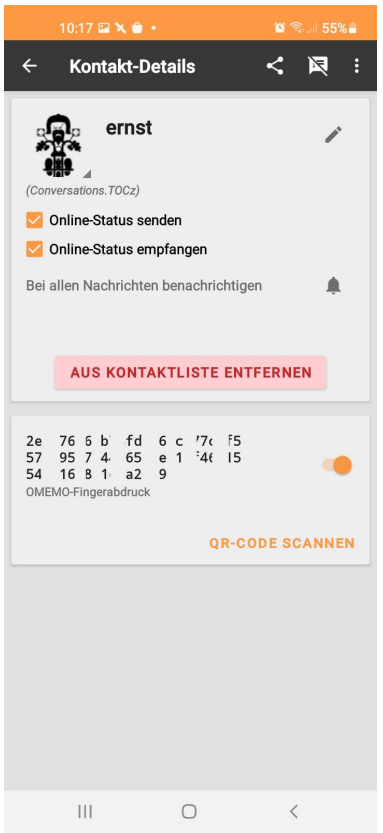


Durch das geschlossene Schloss ist ersichtlich das es sich um eine verschlüsselte Kommunikation mit ernst handelt.

Praktische Übungen:

Weitere Einstellungen





Ich sende meinen Status an *ernst* und frage seinen OnlineStatus an.
Dann sehe ich wenn er online ist.

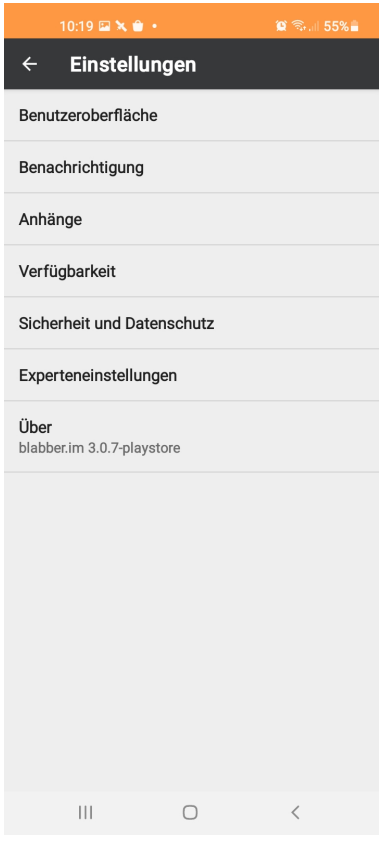
Die Zahlenkolone ist der Fingerabdruck von seinem Schlüssel dem ich vertraue.

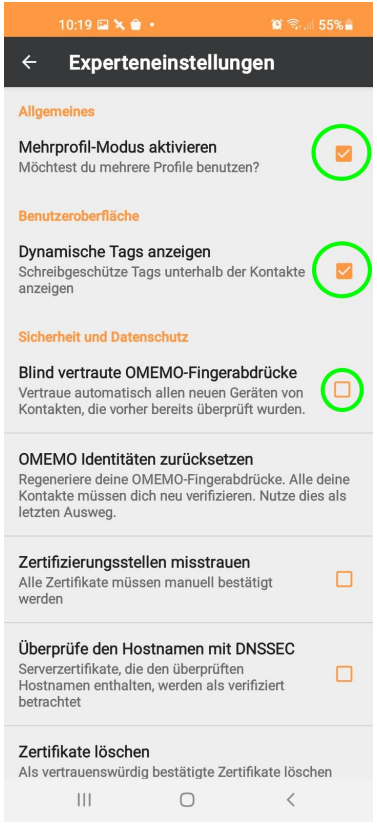
Sollte *ernst* nun weitere Geräte in Betrieb nehmen, tauchen dort weitere Schlüssel auf.

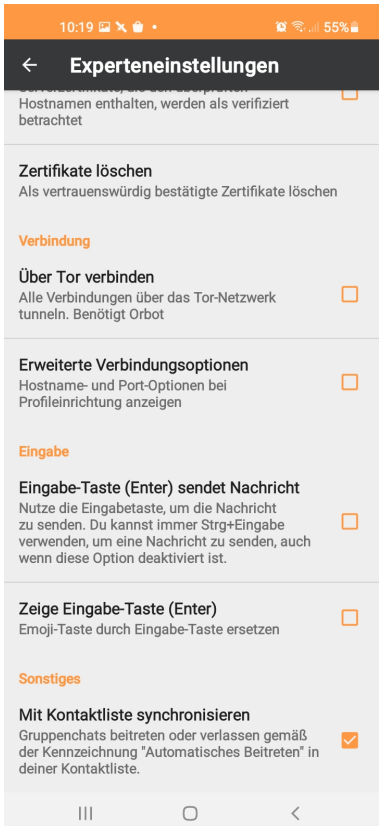
Praktische Übungen:

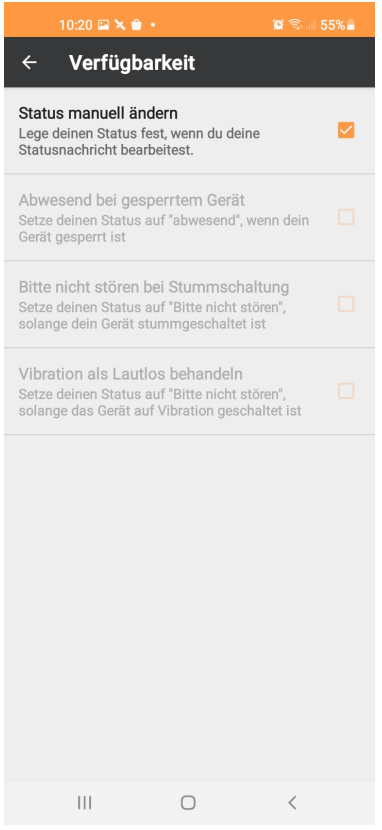
Weitere Einstellungen

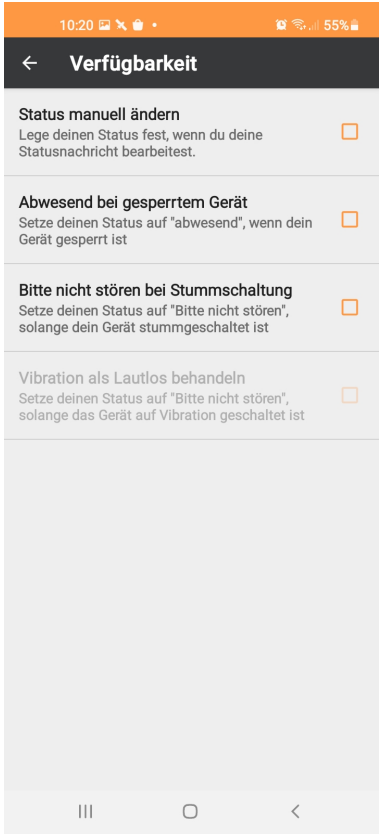
(benötigen weitere Erklärungen)







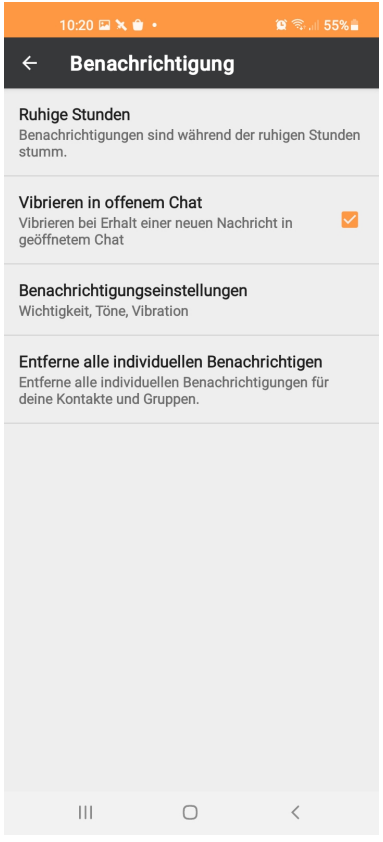


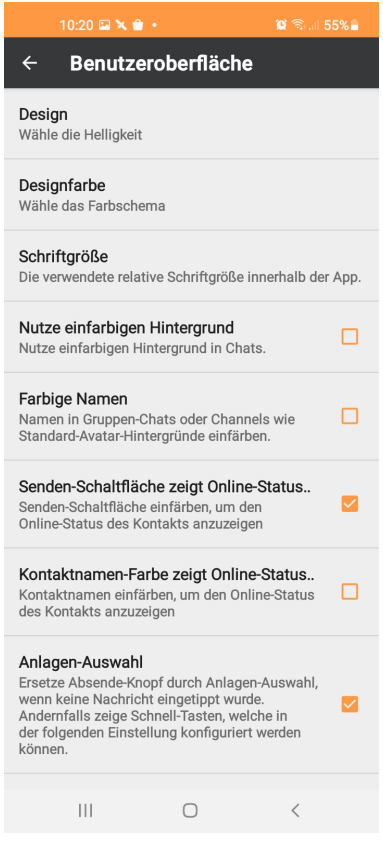


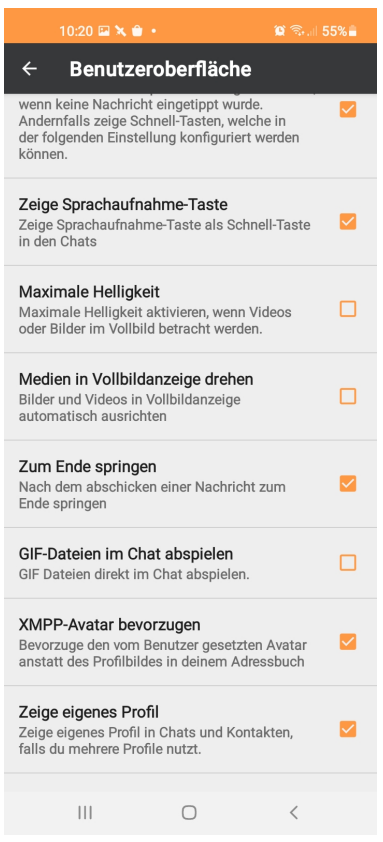
Praktische Übungen:

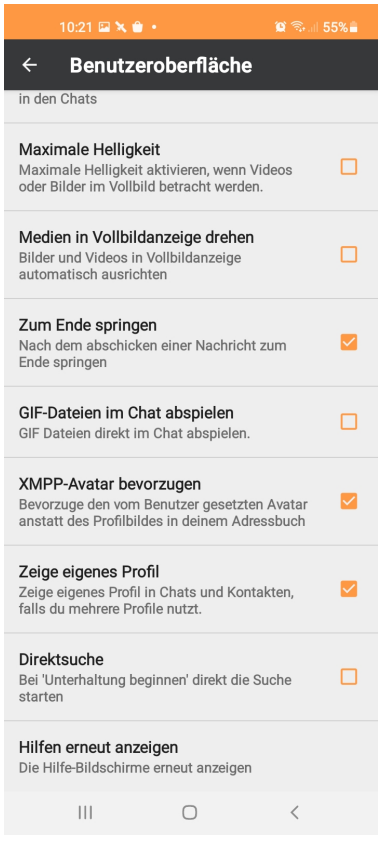
Weitere Einstellungen

(benötigen weitere Erklärungen)





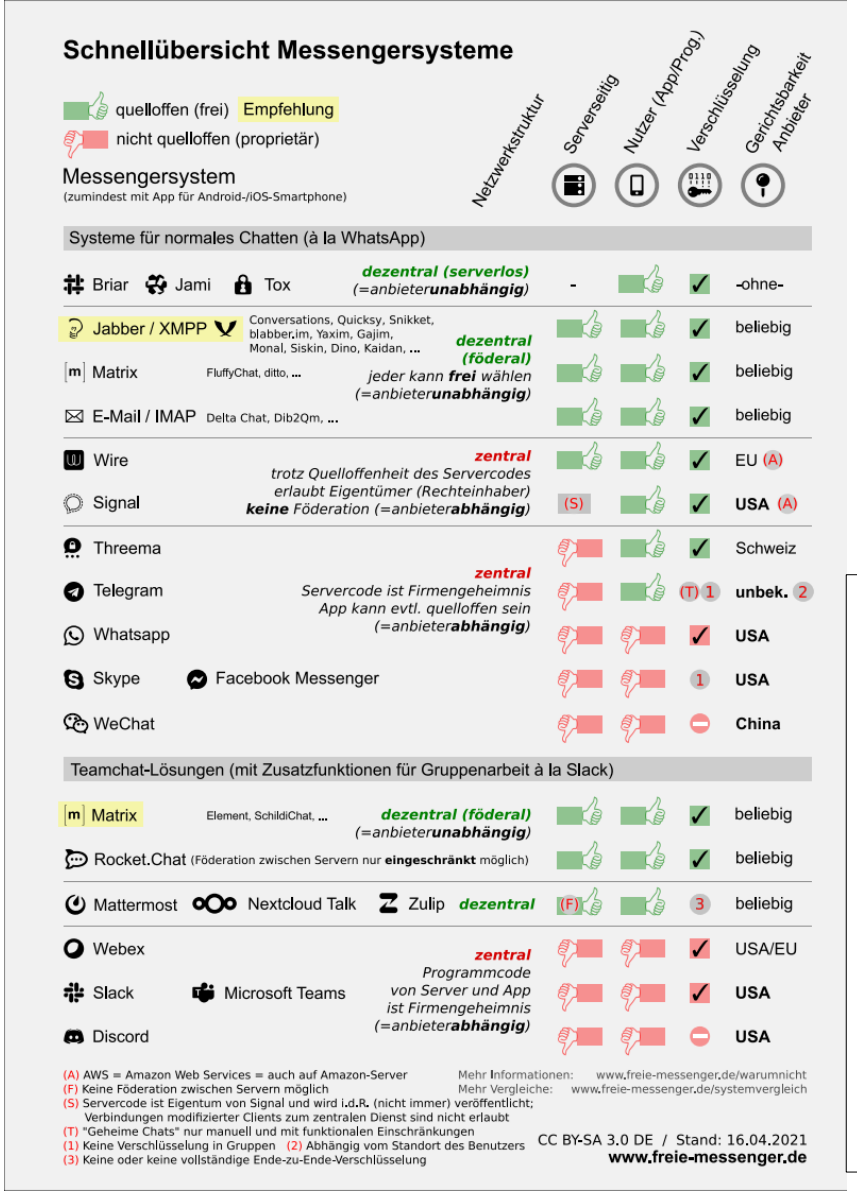




Merkmale	WhatsApp (funXMPP)	Jabber (XMPP) / Matrix (Matrix-Protokoll)	E-Mail (IMAP)	Briar
Grundsätzliches				
Inselsystem ("walled garden" [^1])	ja	nein	nein	nein
Freie Nutzung (keine "AGB", kein Mindestalter, keine geografischen Einschränkungen, keine Begrenzung auf Zeitraum usw.)	nein	ja	ja	ja
Offener Quellcode von Messenger-Programm(en) ("open source") - Code kann überprüft werden	nein	ja	ja	ja
Offener Quellcode von Server-Programm(en) ("open source")	nein	ja	ja	kein Server
öffentliches Verschlüsselungsprotokoll	nein	ja	ja	ja
Kostenlose Nutzung	ja	ja	ja	ja
Selber Messenger für Kommunikation erforderlich	ja	nein	nein	ja
Allgemeine Geschäftsbedingungen	ja	keine	keine	keine
Mindestalter für Nutzung	16	ohne	ohne	ohne
Anmeldung und Nutzung				
Mehrere Konten möglich	nein	ja	bedingt [^2]	nein
Anonymer Namen möglich	nein	ja	bedingt [^2]	bedingt [^3]
Auf mehreren Geräten gleichzeitig nutzbar (Multi-Client-Synchronisation)	nein	ja	ja	nein
Gruppen/Konferenzen				
Maximale Teilnehmeranzahl in Gruppen	256	unbegrenzt	unbegrenzt	unbegrenzt
Berechtigungen in Gruppen/Konferenzen	wenige	diverse	nein	diverse
- Eigentümer	nein	ja	alle gleich	nein
- Administrator	ja	ja	alle gleich	ja
- Mitglied	ja	ja	alle gleich	ja
- Teilnehmer/Leser	nein	ja	nein	nein
Öffentliche Räume/Gruppen	nein	ja	nein	nein
Datenschutz/Privatsphäre				
Unabhängig von Telefonnummer	nein	ja	ja	ja
Zentrales Sammeln und Auswerten von Metadaten	ja	nein	nein	nein
Ohne Adressbuchabgleich vollständig nutzbar	nein	ja	ja	ja
Auf Android-Geräten ohne Google-Konto nutzbar	ja	ja	ja	ja
Ohne Google Cloud Messaging (GCM) bei Android nutzbar	ja	ja	ja	ja

Merkmale	WhatsApp (funXMPP)	Jabber (XMPP) / Matrix (Matrix-Protokoll)	E-Mail (IMAP)	Briar
Online-/Offlinestatus möglich	ja	ja	nein	nein
Online-/Offlinestatus abschaltbar	ja	ja	kein Status	kein Status
Zentrale Erfassung Online-/Offlinestatus	ja	nein	kein Status	kein Status
Lese- und Empfangsbestätigung abschaltbar	teilweise	ja	ja	ja
Tipp-Benachrichtigung abschaltbar	?	ja	ja	ja
Sicherheit				
Ende-zu-EndeVerschlüsselung ("e2e")	ja	ja	ja	ja
"e2e"-Verschlüsselung in Gruppen	ja	ja	ja	ja
"e2e"-Verschlüsselung automatisch / zwingend aktiviert	ja	ja [^4]	ja [^4]	ja
Technik				
Infrastruktur	zentral	dezentrale, föderale Server	dezentrale, föderale Server	dezentral, direkt (p2p [^5])
Auswahl zwischen verschiedenen Messengern (Client-Software) möglich	nein	ja	ja	ja
Speicherort der Kontakte	zentraler Server	bei Serverbetreiber	auf Endgerät	auf Endgerät
Archivierbar (z.B. bei Firmen)	?	ja	ja	nein
Eigener Server möglich (z.B. für Firmen)	nein	ja	ja	nein
Sonstiges				
Finanzierungsmodell	Handel mit Daten	Spenden	Spenden	Spenden
Sonderfunktion "Telefonieren/Videotelefonie"	ja	ja	nein	nein
Sonderfunktion "Gruppen-Anruf" (verschlüsselt)	nein	nein	nein	nein
Direkte Kommunikation ohne Internet (LAN/WLAN/Bluetooth – p2p [^5])	nein	nein	nein	ja
Im Browser aufrufbar	ja	ja	ja	nein

[^1]: Walled garden = „ummauerte Gärten" = Bewußt abgegrenzte Systeme, mit denen durch das Anbieten von kostenlosen/günstigen Diensten Geld verdient wird, das in anderen Bereichen z.B. durch den Verkauf von Daten erwirtschaftet wird.
[^2]: Einschränkung: Anonyme Namen und mehrere Konten sind mit e-Mail zwar möglich, jedoch unterstützt Delta Chat derzeit nur ein Konto.
[^3]: Ein direkter Kontakt kennt die Identität - Aus der Perspektive anderer Personen kann man bei eigenen Blog-/Forum-Einträgen anonym bleiben.
[^4]: e2e = Ende zu Ende-Verschlüsselung ist möglich, jedoch nicht bei allen Messenger-Programmen verfügbar. Hier muss bei der Entscheidung welches Programm genutzt werden soll entsprechend gewählt werden.
[^5]: p2p = peer to peer = Direktverbindung der Klienten („clients"), d.h. den Programmen der Nutzer.



Bemerkungen:

Matrix ist auf 128bit-Verschlüsselung beschränkt.

Die Bundeswehr benutzt ihn zwar, aber alles ab Geheimhaltungsstufe „NfD“ muss extra verschlüsselt werden, also Kegelabend darf geplant werden, Diensteinsatzpläne aber nicht.

Das XMPP in Form von Conversations wird umbenannt als MOKA sogar von der Bundespolizei benutzt und hat dort diese Beschränkung nicht.

Ein Teamchat ist in XMPP möglich, aber zB noch keine Abstimmung (Ist in Entwicklung)

Ein paar weitere Links:

https://www.freie-messenger.de/systemvergleich/xmpp-matrix/

https://www.freie-messenger.de/systemvergleich/externe_vergleiche/

https://www.kuketz-blog.de/die-verrueckte-welt-der-messenger-messenger-teil1/

https://www.kuketz-blog.de/messenger-matrix-uebersicht-vergleich-der-aktuellen-messenger/

https://www.messenger-matrix.de/messenger-matrix.html

und hier gibt es kostenlose Accounts (falls ihr keinen eigenen Namen wollt):
https://list.jabber.at/

xmpp:admin@chat.xmpp-warum.mooo.com

Schlusswort:

Ja ich weiss das eure Kontaktlisten ziemlich leer sind, das ihr eure Freunde/Bekannte/Sportkameraden/... erst wieder neu dazu fügen müsst. Das ist der Preis der Sicherheit.

Wenn ihr wirklich so abhängig von einem gemeinsamen Adressbuch seid, der Programmierer vom Conversations hat auch ein Quicksy erstellt. Ihr braucht euch kein Passwort oder Userkennung auszudenken, das macht alles er für euch. Ihr bekommt einen kostenlosen Account auf seinem Server und alle die das gleiche Programm installiert haben liegen mit ihrer Telefonnummer auf dem Server und können durch andere gefunden werden. Aber wo ist dann die Sicherheit geblieben ? Es ist sein Beweis das XMPP/Jabber sich **nicht** von WhatsApp unterscheiden **muss aber kann und soll**

Aber ich bin nicht der einzige der auf Sicherheit erpicht ist, gerade in der heutigen Zeit wo schnell mal das politische Pendel/Status-Quo umschlägt und man plötzlich vor einer anderen Seite der Macht steht.
Der Datenschutzbeauftragte von Hamburg hat nun Facebook „verklagt“ und somit eine 3 monatige Sperre der Weitergabe der WhatsApp-Daten erwirkt. Zeitgleich wird gerade eine Anhörung vor dem Europäischen Datenschutzausschuss vorbereitet, das hat aber nur aufschiebende Wirkung, nun treibt die EU auch noch die Chat-Kontrolle durchs Dorf und fordert ein Aufbrechen der Verschlüsselung bei allen Chatprogrammen.

WhatsApp droht mit Einstellung der Funktion falls ihr nicht zustimmt, nutzt die Zeit und schreibt euren WhatsApp/Signal/Threema/Telegram/Wire/Wisper/WeChat/….-Kontakten das ihr ab jetzt unter XMPP/Jabber erreichbar seid. Teilt euren Sportkameraden eine „sportliche“ XMPP-Adresse mit, eurer Famile eine „private“, eurer Kneipe eine „öffentliche“, euren Clubs eine „persönliche“, eurem Arbeitgeber eine „offizielle“, euren ...

Es liegt in eurer Hand