UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Der Uni-Dienst 'Teamchat 2.0' im Kontext der UB – eine kurze Einführung in Matrix und die App Element

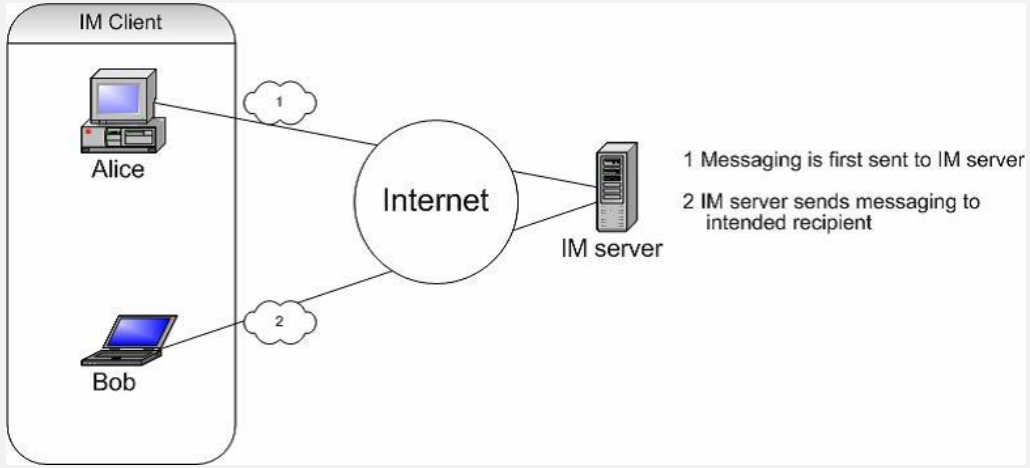
element

Jochen Schirrwagen
18. Juni 2021

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Was ist Instant Messaging (IM)?

- Eine Kommunikationsmethode zur sofortigen internetbasierten Nachrichtenübermittlung
  - Übertragung von Text, Dateien, Audio, Video
- „Instant Message“ wurde durch Paul Linebarger in Science-Fiction Geschichten in den 60er Jahren geprägt
- Erster Instant Messaging Dienst *ICQ* startete in 1996
- Offene Protokolle, z.B. das Extensible Messaging and Presence Protocol (XMPP) durch die IETF seit 2002, 2004; WebRTC u.a.
- Proprietäre Protookolle, z.B. bei WhatsApp, Skype
- Siehe auch: https://de.wikipedia.org/wiki/Liste_von_Instant-Messaging-Protokollen



http://cryptowiki.net/index.php?title=Secure_instant_messaging&oldid=13438

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Messenger Stand: 15.06.2021	Briar	Conversations (XMPP)	Delta Chat	Element (Matrix)	iMessage	Jami	Signal	Siskin (XMPP)	Skype	Telegram	Threema	aTox (Tox)	WhatsApp	Wire
Systemunterstützung														
Android	ja	ja	ja	ja	nein	ja	ja	nein (siehe Conversations)	ja	ja	ja	ja	ja	ja
iOS	nein	nein (siehe Siskin)	ja	ja	ja	ja	ja	ja	ja	ja	ja	nein	ja	ja
Web/Desktop	nur Linux	ja (diverse Clients)	ja	ja (diverse Clients)	nur macOS	ja	ja	ja (diverse Clients)	ja	ja	ja	ja (diverse Clients)	ja	ja
Sicherheit & Datenschutz														
Quelloffen	GPLv3	GPLv3	GPL	Apache 2.0	nein	GPLv3	GPLv3	GPLv3	nein	GPLv2 (nur Client)	AGPLv3 (nur Client)	GPLv3	nein	GPL
Kommt ohne proprietäre Bibliotheken aus	ja	ja	ja	ja	nein	ja	nein	ja	nein	ja (nur F-Droid Version)	nein	ja	nein	nein
Verschlüsselungs-Protokoll / -Bibliothek	Bramble	OMEMO (Signal-Protokoll)	OpenPGP mit Autocrypt	Olm / Megolm (Signal-Protokoll)	proprietär, Unbekannt	RSA-Keys (4096-Bit)	Signal-Protokoll	OMEMO (Signal-Protokoll)	proprietär / Signal-Protokoll	MTProto 2.0	NaCl (kein PFS)	NaCl (kein PFS)	Signal-Protokoll (nicht prüfbar)	Proteus (Signal-Protokoll)
Ende-zu-Ende-Verschlüsselung	ja	ja	Delta-Chat-Kontakte	ja	ja	ja	ja	ja	nein	nur Einzelchats (optional)	ja	ja	ja	ja
Lokale Nachrichtenverschlüsselung	ja	nein	nein	ja	ja	nein	ja	nein	nein	nein	ja	nein	ja	ja
Verifikation von Kontakten möglich	ja	ja	ja	ja	nein	ja	ja	ja	nein	nur in geheimen Chats (Secret Chat)	ja	ja	ja	ja
Hinweis, falls sich Kontakt-Fingerprint ändert	ja	ja (falls zuvor verifiziert)	nur in verifizierten Gruppenchats	ja	nein		ja	ja (falls zuvor verifiziert)	nein	nein	ja	nein	muss aktiviert werden	ja (falls zuvor verifiziert)
Letzter Sicherheitsaudit	2017	2016	—	2016	2016	—	2017	—	—	2017	2020	—	—	2017

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

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Was ist Matrix ?

- offener Standard und Kommunikationsprotokoll für Echtzeitkommunikation seit 2014
  - basierend auf HTTP und WebRTC
- ermöglicht Diensteanbieter übergreifende Kommunikation zwischen Benutzern in Form von Chat, IP-Telefonie und Video-Telefonie
- Nutzt einen dezentralen Ansatz im Gegensatz zu etwa WhatsApp
- Auch bei Nutzung von Matrix fallen Metadaten an, die aber nicht notwendigerweise zentral an einem Ort gesammelt werden, darunter Kontaktlisten, Mitgliedschaften in Räumen bzw. Gruppenchats, Persönliche Informationen, verschlüsselte Nachrichteninhalte

https://matrix.org/

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Analogien zum E-Mail Dienst

- Festlegung auf ein Protokoll (hier Matrix; bei E-Mail SMTP, POP3, IMAP)
- Nutzung von Clients, die ein oder mehrere (offene) Protokolle unterstützen
- Server oder Diensteanbieter, der Matrix unterstützt
- Föderiertes System, d.h. Nachrichten können von Server zu Server gesendet werden

Vs.

Zentralisierte und untereinander inkompatible Messenger

Auswahl an Matrix Clients

	weechat-matrix	Element Web/Desktop	Element (Android)	SchildiChat (Android)	Spectral	Element (iOS)	gomuks	Quaternion	matrixcli	nhek Rebo	NeoChat	Ditto Chat	Mirage	Fractal	Nio	FluffyChat	Seaglass	Miitrix	kazv	matrix-commander	SchildiChat Web/Desktop	Syphon
Linux	✓	✓			✓		✓	✓	✓	✓	✓		✓	✓		✓			✓	✓	✓	✓
Mac	✓	✓			✓		✓	✓		✓						✓	✓			✓	✓	✓
Windows	✓	✓			✓		✓	✓		✓	✓					✓				✓	✓	
Android			✓	✓							✓	✓				✓						✓
iOS						✓						✓			✓	✓						✓
Ubuntu Touch																						
Web		✓														✓					✓	
Nintendo 3DS																		✓				

Features

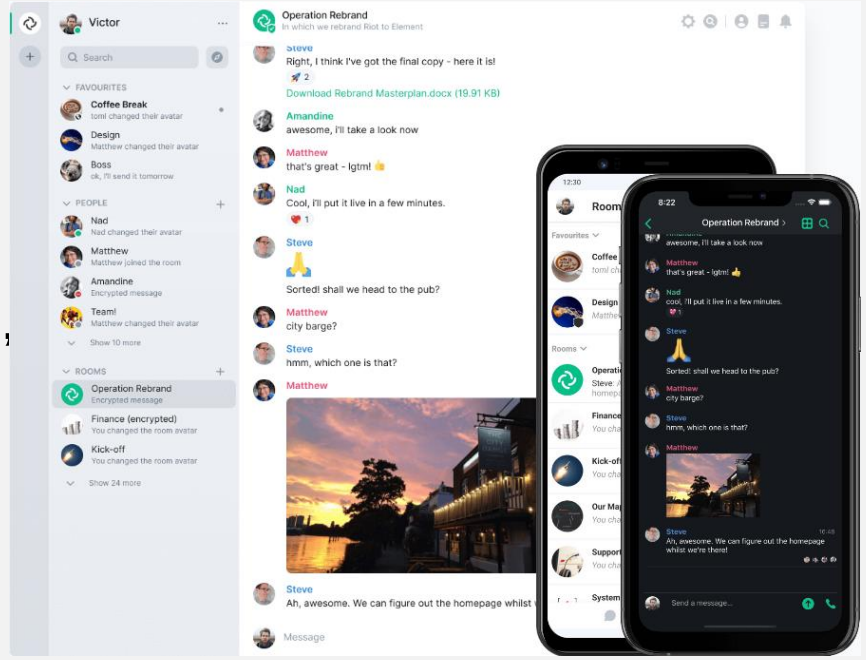
	weechat-matrix	Element Web/Desktop	Element (Android)	SchildiChat (Android)	Spectral	Element (iOS)	gomuks	Quaternion	matrixcli
Room directory	✓	✓	✓	✓	✗	✓	✗	✗	✗
Room tag showing	✗	✓	✗	✗	✗	✗	✓	✓	✗
Room tag editing	✗	✓	✗	✗	✗	✗	✓	✓	✗
Search joined rooms	✗	✓	✓	✓	✓	✓	✓	✗	✗
Room user list	✓	✓	✓	✓	✓	✓	✓	✓	✗
Display Room Description	✓	✓	✓	✓	✓	✓	✓	✓	✗
Edit Room Description	✓	✓	✓	✓	✓	✓	✗	✓	✗
Highlights	✓	✓	✓	✓	✓	✓	✓	✓	✗
Pushrules	✗	✓	✓	✓	✗	✓	✓	✗	✗

https://matrix.org/clients-matrix

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Was ist Element ?

- Bis 15. Juli 2020 unter dem namen Riot.im des Unternehmens New Vector
- Ein plattformübergreifender Client für Chat, IP-Telefonie und Video-Telefonie über die Matrix-Protokolle
- Open Source unter der Apache Lizenz
  https://github.com/vector-im
- Verfügbar über Web-Browser, Desktops (MacOs, Windows, Linux), mobile Endgeräte



UNIVERSITÄT BIELEFELD
Universitätsbibliothek

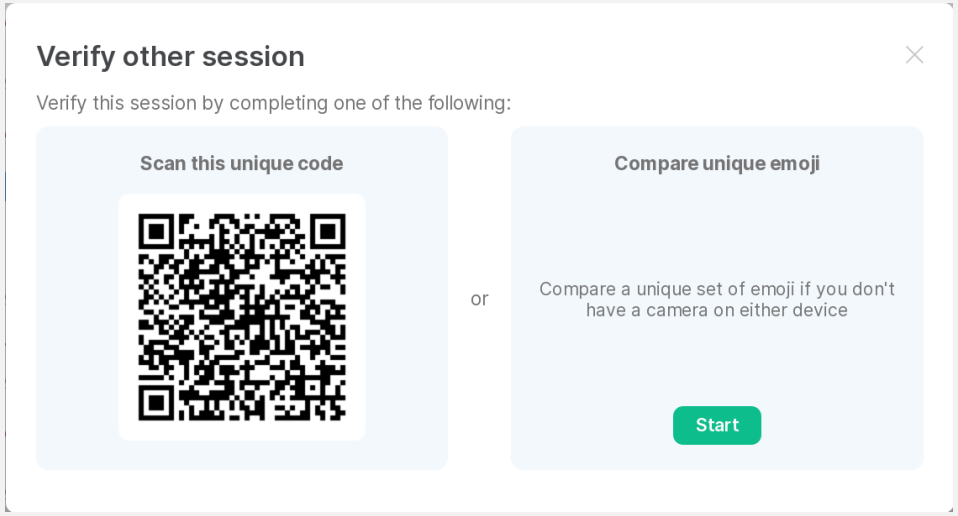
„Own your conversations“

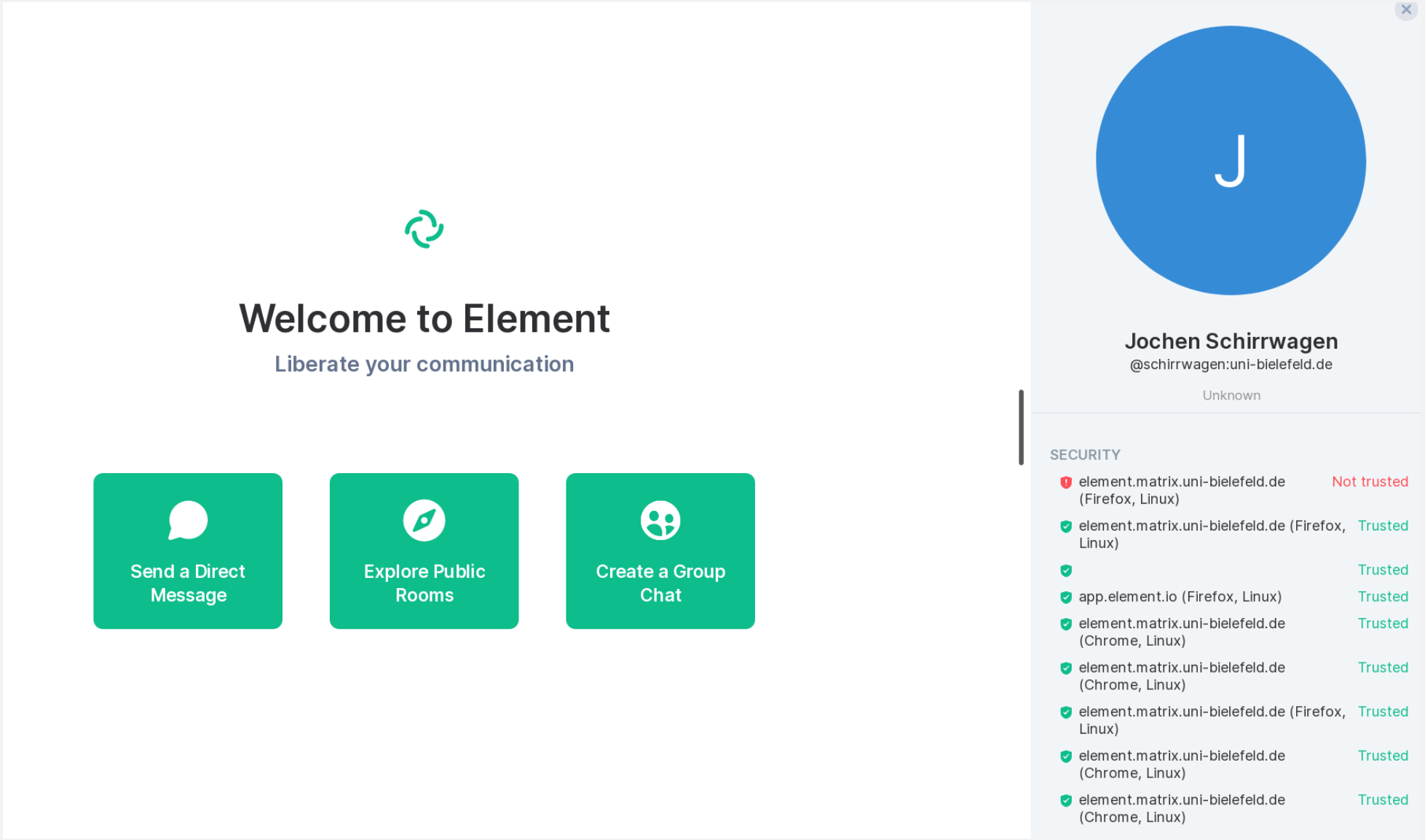
- Einzel- und Gruppenchats
- Ende-zu-Ende-Verschlüsselung inkl. automatischer Schlüsselsicherung auf Basis der Olm- bzw. Megolm-Kryptographie-Protokolle (ähnlich wie bei Signal)
- Audio- und Videotelefonate (via Jitsi)
- Nachrichtensynchronisation
- Communitys (ähnlich wie bei Discord/Slack)
- Sticker und Bots
- Dateiaustausch
- Multi-Device und Multi-Platform-Funktionalität: Element lässt sich auf beliebig vielen verschiedenen Geräten und auf so gut wie jedem verbreiteten Betriebssystem verwenden.

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Verifizierung gegenüber anderen BenutzerInnen und Geräten

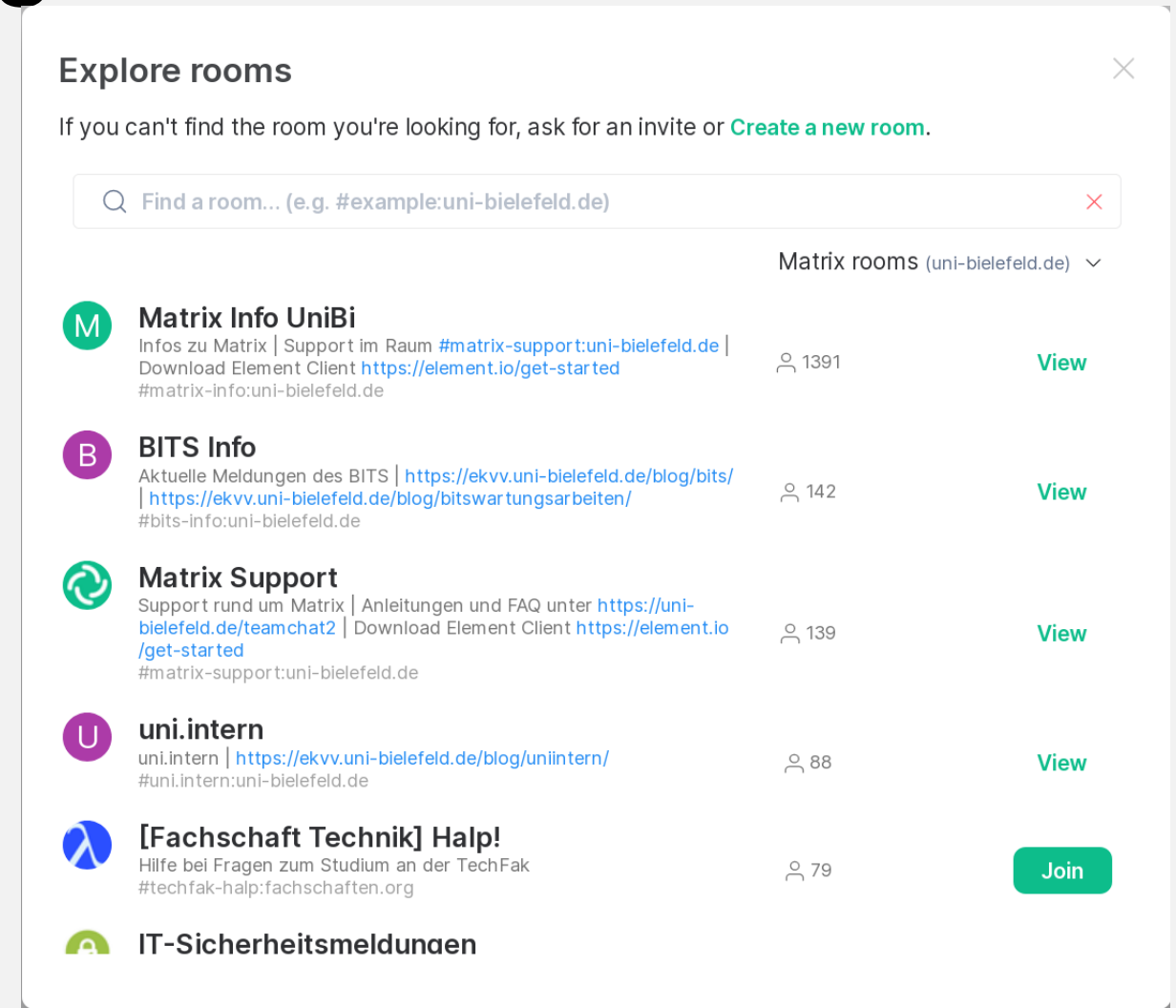
- Ein Benutzer kann sich identifizieren und gefunden werden über
  - seine Matrix-ID
  - zstzl. seine E-Mail-Adresse
  - zstzl. seine Telefonnummer




Welcome to Element
Liberate your communication
Send a Direct Message
Explore Public Rooms
Create a Group Chat
J
Jochen Schirrwagen
@schirrwagen:uni-bielefeld.de
Unknown
SECURITY
element.matrix.uni-bielefeld.de (Firefox, Linux) Not trusted
element.matrix.uni-bielefeld.de (Firefox, Linux) Trusted
Trusted
app.element.io (Firefox, Linux) Trusted
element.matrix.uni-bielefeld.de (Chrome, Linux) Trusted
element.matrix.uni-bielefeld.de (Chrome, Linux) Trusted
element.matrix.uni-bielefeld.de (Firefox, Linux) Trusted
element.matrix.uni-bielefeld.de (Chrome, Linux) Trusted
element.matrix.uni-bielefeld.de (Chrome, Linux) Trusted

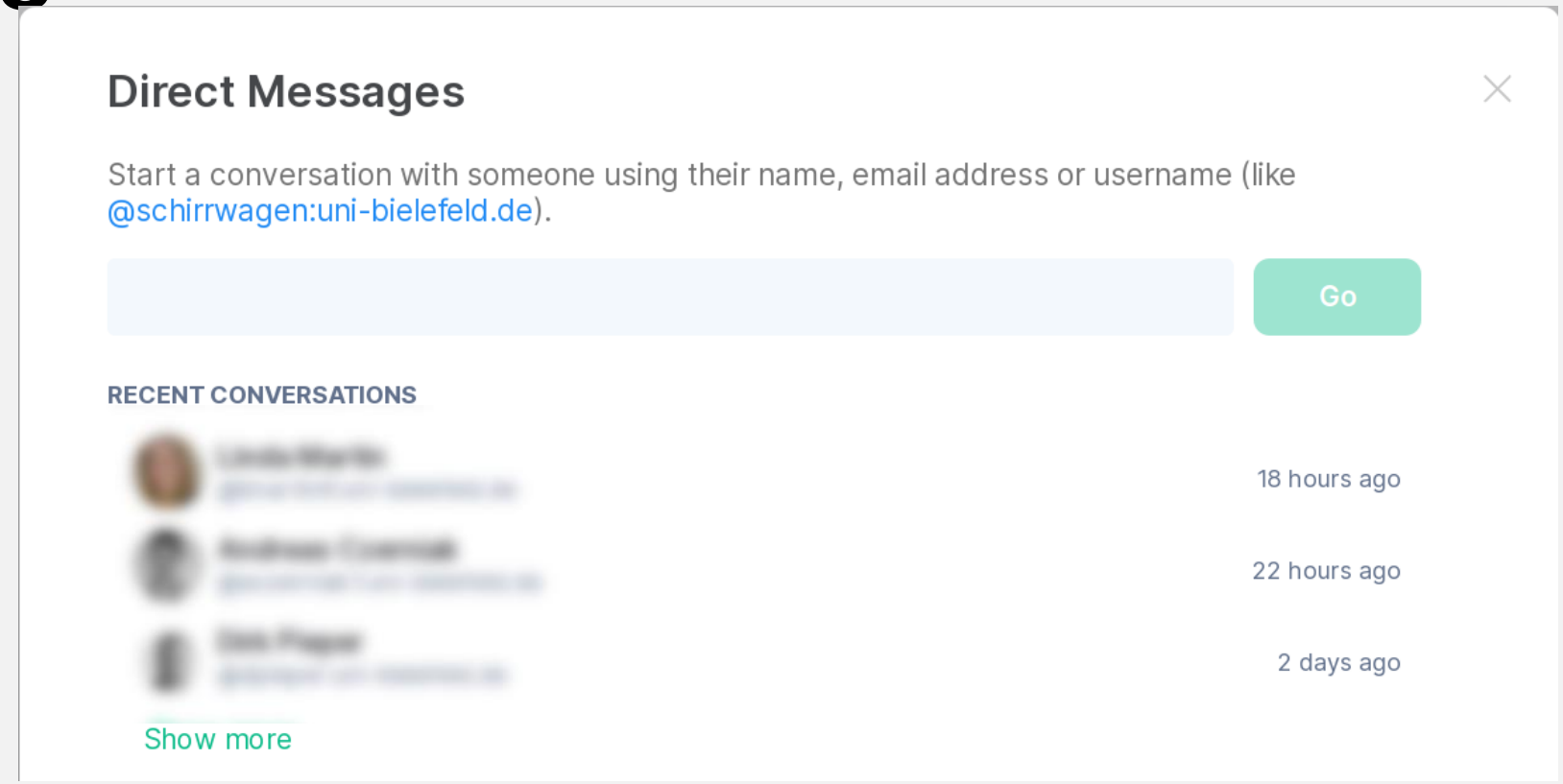
UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Nutzung von Element



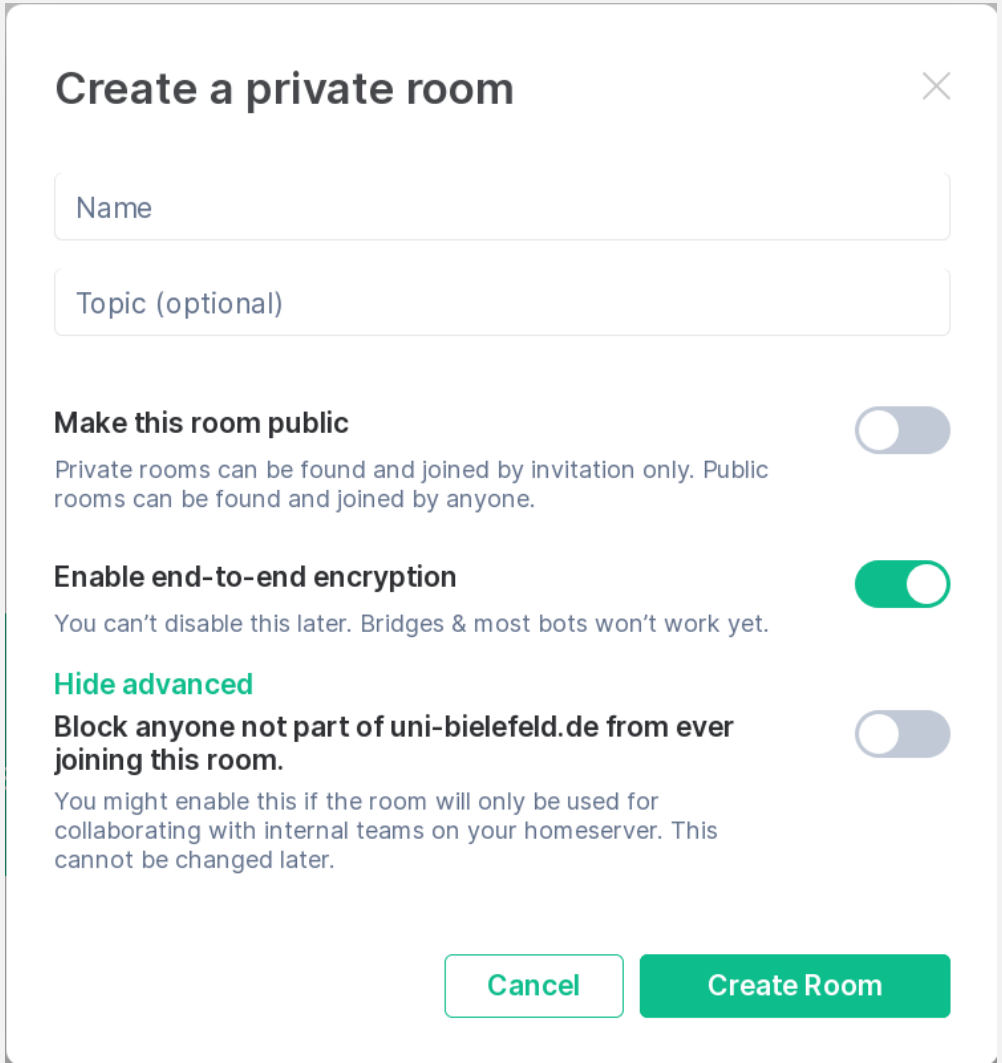
UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Nutzung von Element



UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Nutzung von Element



UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Benutzer, Räume und Communities

BenutzerInnen in Matrix haben eine Id, die dem Schema folgt: @nutzername:example.org

Matrix-Raum

In Matrix erfolgt die Konversation in Räumen

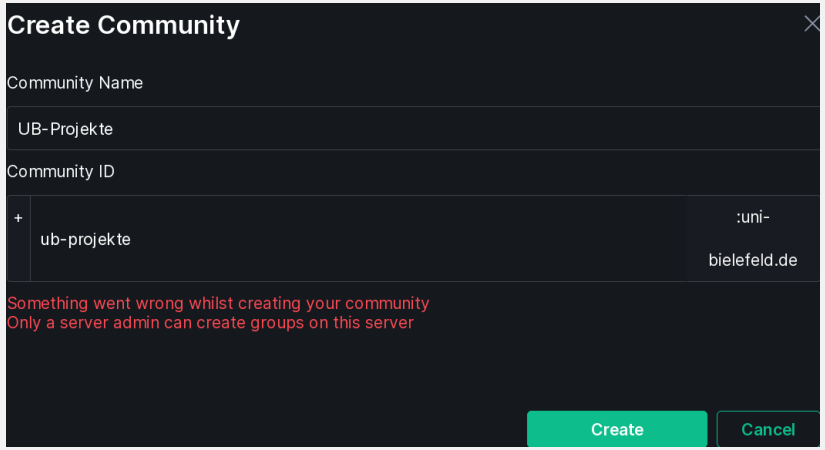
- Auch die direkte Konversation mit einem anderen Benutzer stellt einen Raum dar
- Für jeden Raum gibt es einen oder mehrere AdministratorInnen
- Aufbau des Namensschemas für Räume: #raumname:example.org

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Benutzer, Räume und Communities

Matrix-Community

- Communities in Matrix sind Grupppen bzw. Gemeinschaften, durch die mehrere Räume zusammengefasst werden können
- Aufbau des Namensschemas für Communities: +communityname:example.org
- Communities erlauben eine übergeordnete Struktur für Räume
  - Z.B. die UB als Community, die alle Räume für UB-MitarbeiterInnen zusammenfasst
    Oder für ein Dezernat, Abteilungen, Projekte,
    …-> zumindest in der Theorie



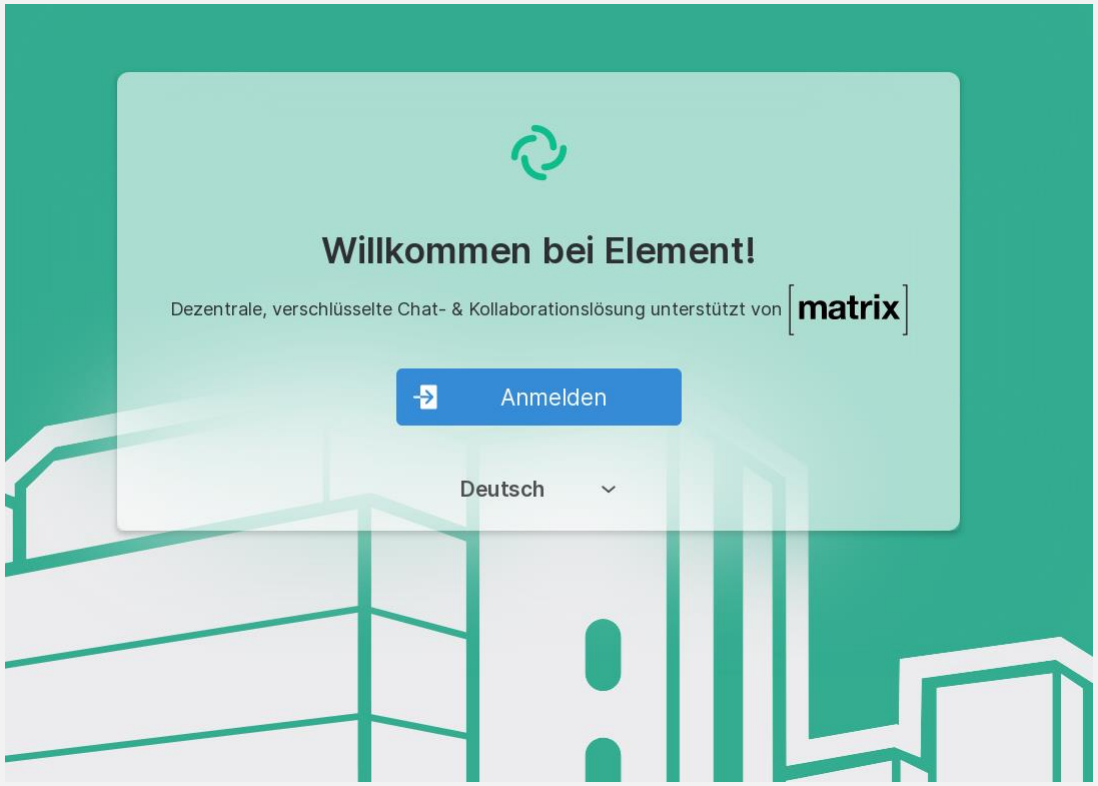
UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Element als „Teamchat 2.0“ an der Uni Bielefeld

- Für alle Mitarbeiter*Innen und Studierenden der Universität Bielefeld
- Ermöglicht durch sein Föderationskonzept die Kommunikation mit anderen Matrix-Instanzen (bswp. an anderen Hochschulen und Forschungseinrichtungen)
- Wird gemeinsam betrieben vom BITS und KIT (Konstruktive IT'ler an der Universität Bielefeld)
- https://www.uni-bielefeld.de/einrichtungen/bits/services/kommunikation/teamchat/
- Fragen von BenutzerInnen und Hilfestellungen auch im Matrix-Support Raum #matrix-support:uni-bielefeld.de

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Warum wurde Teamchat 1.0 durch Teamchat 2.0 ersetzt?
Welche Verknüpfungen sind möglich / noch geplant?



https://matrix.uni-bielefeld.de

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Fragen und Antworten

1. In jedem Chat-Raum gibt es die Möglichkeit, eine Suche durchzuführen.

   Leider liefert die Suche (zumindest bei mir) immer 0 Ergebnisse.

   - evtl. veraltete Version von Element -> Prüfen auf Update
   - Suche in verschlüsselten Räumen wird bisher nur in der Desktop-App unterstützt
   - die Suche findet nur ganze Wörter. Wenn z.B. nach Beiträgen gesucht wird, in denen das Wort “Sitzung” vorkommt, muss man auch “Sitzung” eingeben (und nicht z.B. “sitz” o.ä.)

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Fragen und Antworten

2. Besteht evtl. die Möglichkeit, zu jeder Nachricht im Chatsystem, die Option "Archivieren" einzubauen? Manchmal werden nützliche Tipps oder Hinweise von anderen mitgeteilt und es wäre praktisch, sie gesondert abzuspeichern.

- bisher in Element nicht vorgesehen, theoretisch als Funktion selbst implementierbar, da Open Source
- Ruhr-Uni Bochum sammelt Feature-Anfragen von anderen Hochschulen, Marcus Shopen wird es als Feature anfragen
- DSGVO-Aspekt bzgl. sensibler Daten und Löschfristen beachten

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Fragen und Antworten

3. Gibt es eine Möglichkeit, Nachrichten in Element "anzupinnen", so dass sie immer zuerst erscheinen, ähnlich wie bei Rocket.Chat?

- eine “Anpinnen”-Funktion gibt es bisher nicht
- Feature-Request -> Ruhr-Uni Bochum

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Fragen und Antworten

4. Welche Möglichkeiten bietet das Berechtigungskonzept in Element, welche Auswirkungen hat dies auf die Sichtbarkeit von Räumen / Communities / Chats für andere NutzerInnen?

- bestimmte Ereignisse, wieviele und welche NutzerInnen lesen Nachrichten im Raum, lässt sich nicht abstellen
- bei Bedarf an einer Community, soll die Einrichtungsleitung dies beim Teamchat-Support beantragen.
- Communities erlauben eine übergreifende Struktur für Räume; ein Raum kann in mehreren Communities sein
- “Spaces” wird das Nachfolgekonzept für Communities sein.

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Fragen und Antworten

5. Welche Einstellungen müssen in Element erfolgen, damit man ggf. über neue Nachrichten per E-Mail informiert wird (ähnliche Funktion gibt es bei Rocket.Chat)?

- theoretisch möglich, wird aber vom Teamchat-Support abgelehnt und nicht unterstützt
- ein Grund ist die Last des Exchange-Mail-Servers

UNIVERSITÄT BIELEFELD
Universitätsbibliothek

Fragen und Antworten

6. Wie kann man Videos oder Fotos kopieren/weiterleiten, insbesondere mit der Element App auf dem Smartphone?
   - dazu eine Nachricht etwas länger antippen und dann im aufklappenden Menu die Kopieren / Teilen-Funktionen nutzen