

[matrix]

für das KIT

Motivation

- Juni 2022: Abschaltung XMPP (Jabber)

- Juni 2022: Abschaltung XMPP (Jabber)
- Nachfolger als Alternative zu MS Teams von vielen Seiten gewünscht

- Juni 2022: Abschaltung XMPP (Jabber)
- Nachfolger als Alternative zu MS Teams von vielen Seiten gewünscht
- Arbeitsgruppe im SCC, um Bedarf und mögliche Lösungen zu ermitteln

- Juni 2022: Abschaltung XMPP (Jabber)
- Nachfolger als Alternative zu MS Teams von vielen Seiten gewünscht
- Arbeitsgruppe im SCC, um Bedarf und mögliche Lösungen zu ermitteln
- ⇒ Matrix soll eingesetzt werden

Was ist [matrix]?

Matrix is an open standard for interoperable, decentralised, real-time communication over IP.

<https://matrix.org/docs/guides/introduction>

- Nicht speziell für Chat
- Vieles ist möglich (Voice / Video / Shared Whiteboards / ...)

- Matrix ist ein **offener Standard**
 - Kann jeder lesen und Änderungen vorschlagen
 - Frei implementierbar

- Matrix ist ein **offener Standard**
 - Kann jeder lesen und Änderungen vorschlagen
 - Frei implementierbar
- Matrix ist **interoperabel**
 - Kann Informationen mit anderen Kommunikationssystemen austauschen
 - Interoperabilität einfach zu verstehen und umzusetzen

- Matrix ist **dezentralisiert**
 - Es gibt keinen zentralen Server, jeder kann sein eigenes System betreiben und die Kontrolle über die eigenen Daten behalten
 - Dadurch datenschutzfreundlich

- Matrix ist **dezentralisiert**
 - Es gibt keinen zentralen Server, jeder kann sein eigenes System betreiben und die Kontrolle über die eigenen Daten behalten
 - Dadurch datenschutzfreundlich
- Matrix ist für **Echtzeitkommunikation**
 - Ideal für den Aufbau von Systemen, für die sofortiger Austausch von Daten nötig ist (z.B. Instant Messaging / Chat)

- Matrix ist Ende zu Ende verschlüsselt*
 - nativ im Protokoll vorgesehen
 - Basiert auf Double-Ratchet-Algorithmen
 - olm
 - mego lm

- Matrix ist Ende zu Ende verschlüsselt*
 - nativ im Protokoll vorgesehen
 - Basiert auf Double-Ratchet-Algorithmen
 - olm
 - mego^llm
- Verschlüsselung und Authentizität
 - Verschlüsselung stellt Vertraulichkeit der Nachricht sicher
 - Authentizität stellt Identität der Chat-Teilnehmer sicher
 - Wie bei E-Mail: Verschlüsselung, Signatur

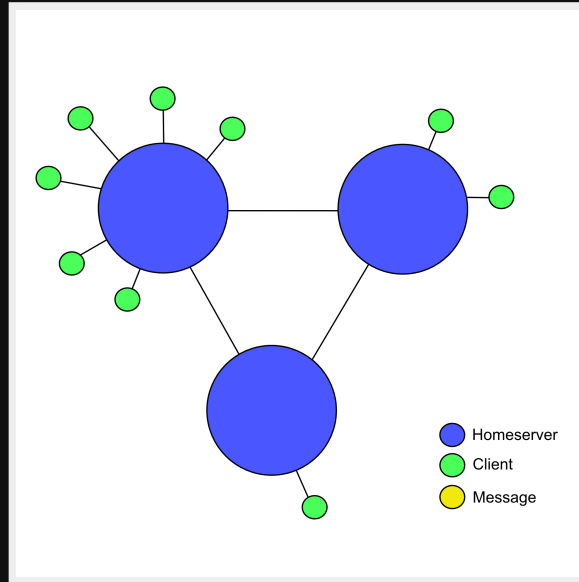
In der Praxis

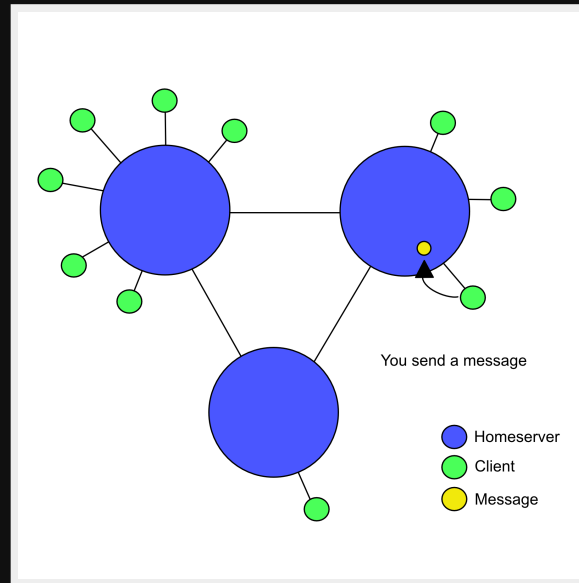
- **Server** werden Homeserver genannt
 - KIT-Homeserver ist `kit.edu`
 - Verwendete Software: `matrix-synapse` (Python)
 - System aus mehreren VMs, am SCC gehostet
 - möglichst hohe Ausfallsicherheit
 - Verteilt auf CN und CS
 - mehrere Worker
 - Frontend aus zwei Load-Balancern

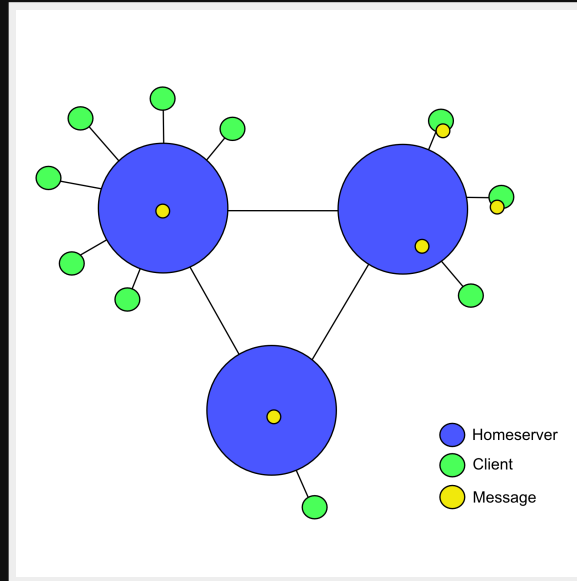
- **User:** Benutzer auf den einzelnen Homeservern
 - Jeder mit einzigartigem User-Handle (mxid)
 - am KIT:
 - @ab1234:kit.edu für Mitarbeiter und Partner
 - @uabcd:kit.edu für Studierende
 - „fremde“ Homeserver:
 - @s1234567:tu-dresden.de
 - @dominik:geschwafel.org

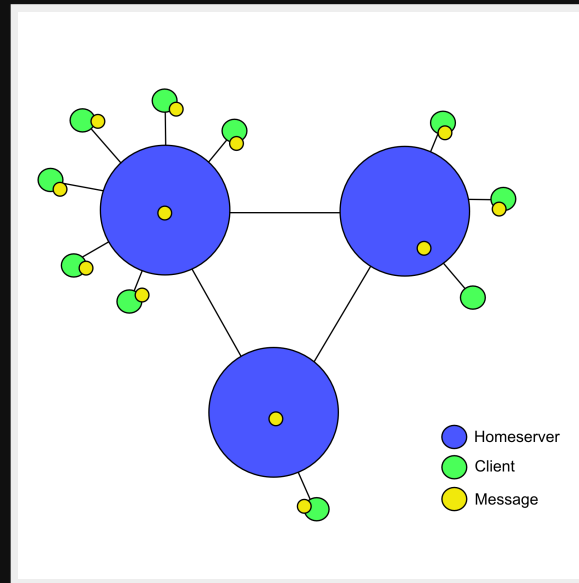
- **Rooms:** Räume in denen ein oder mehr User sind, die dann miteinander kommunizieren können.
 - Räume können offen, space-offen oder privat sein
 - Direktnachricht, Gruppe, oder nur ein Teilnehmer
 - (Öffentliche) Räume haben „Adressen“
 - Beispiele:
 - `#thisweekinmatrix:matrix.org`
 - `#scc-net-lobby:kit.edu`
- **Spaces*:** Sammlung von Räumen und Benutzern

- **Clients:** Schnittstelle für User zum Homeserver
 - Nur hier können die Nachrichteninhalte entschlüsselt werden
 - empfohlener Client: **Element** (verfügbar auf allen Plattformen & **als Web-Client**)
 - [matrix]-Clients gibt es in allen Formen und Farben: <https://matrix.org/clients/>
 - Desktop, Mobile, CLI es gibt für jeden den passenden Client









Features

- Ende-zu-Ende verschlüsselte
 - Direktnachrichten
 - Gruppenchats

- Bots
 - z.B. für GIT-Integration, Helpdesk, Reminder, ...
 - Auf selbst betreuten Servern betrieben, z.B. einer OE
 - Als Matrix-User können Serviceaccounts verwendet werden
 - alternativ: Account auf anderem Homeserver (eigener, ...)

- Bridges
 - Verbinden Matrix-Homeserver mit anderen Chatdiensten (z.B. IRC, Slack, ...)
 - Sicherheitstechnisch problematisch (brechen Verschlüsselung auf)
 - Am KIT **nicht** geplant

Demo

Da sind komische Symbole
in meinem Chat...

oder: Wieso sind da Schilder?



mind. eine Person
im Raum wurde
noch nicht
verifiziert.



mind. eine Person
im Raum, die
bereits verifiziert
wurde, aber
unverifizierte
Sitzungen hat.



Alle im Raum
befindlichen
Personen wurden
verifiziert.

siehe auch <https://docs.matrix.kit.edu/encryption/>

Weiterführende Infos

- Dienst-Seite: matrix.kit.edu
- Dokumentation: docs.matrix.kit.edu
- Support:
 - matrix@scc.kit.edu
 - Helpdesk Matrix-Room

Evtl. gibts demnächst auch einen Support-Bot
([Honoroit](#))

Fragen?