

COMMON CHALLENGES FOR ORGANIZATIONS WHEN DEPLOYING

[matrix] by  **fairkom**

Jan Krammer · Philipp Monz

The Matrix Conference 2026 · Malmö
Thursday, 22 October 2026 · 15:15 · Room Katherine · Public Sector Track

WHO WE ARE



Jan Krammer

INFRASTRUCTURE ENGINEER

Linux and FOSS enthusiast
Infrastructure for universities
Matrix, Jitsi, Kubernetes



Philipp Monz

SOFTWARE DEVELOPER · FAIRKOM

Open source initiatives at fairkom
Schulchat RLP for schools
Clients, tooling, integrations



[MATRIX] PROJECTS



Schulchat RLP
school messenger since
2022



HU Berlin
BigBlueButton integration
for Element



TU Wien
migration from
Rocket.Chat to [matrix]



Uni Graz
[matrix] video
conferencing concept

... and many more public sector projects with fairkom



AGENDA



01

Users and identity



02

Law and compliance



03

Administration and
moderation



04

Infrastructure



05

Clients, video,
extensions



06

Custom solutions



01

USERS AND IDENTITY

@ THE MATRIX ID

- MatrixID schema: `@localpart:domain`
- allowed localpart characters: `a-z` `0-9` `.` `_` `=` `-` `/` `+`
- decision: human-readable or a UUID?
- ID cannot be changed later

@ UUID AS LOCALPART

- example: `@8db6f8a6-1ba4:domain.com` or `@m28561287265:domain.com`
- technically easier (uniqueness, immutability)
- inconvenient to share mxid
- no "glance value" to match mxid to user
- compromise: mix (preferred?) username+UUID
`@<preferred_username>-<xxxxx>:domain.com`
 - still bad if username is lastname

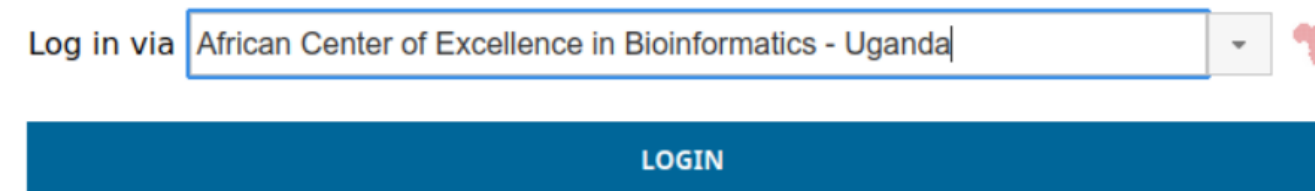
@ HUMAN-READABLE ID

- similar to Email-Addresses: e.g.
`@firstname.lastname:domain.com`
- technically more involved, more planning needed, tradeoffs
 - name changes are challenging: new matrix account or keep "wrong" name?
 - user-chosen names can cause chaos
 - could be viable in non-federated setups (`Displayname` is updated easily)
- uniqueness + immutability over time (or impersonation/takeovers possible)
- unique even across AD-domains
- future solutions?

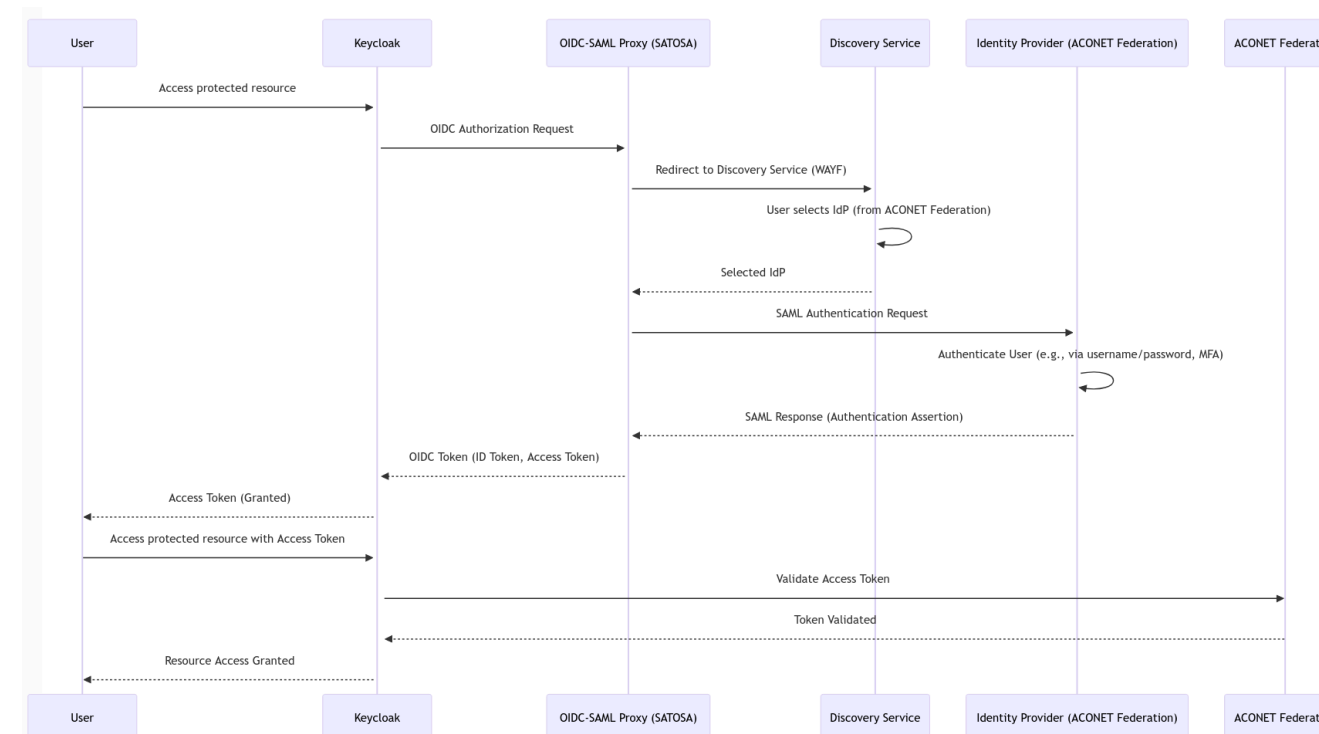


IDP, SSO, AUTH

- use a modern OIDC IDP (e.g. Keycloak)
- university challenge: federated identities (eduid, metadata, discovery)¹



- SAML needed? bridge OIDC-SAML (SATOSA proxy)²

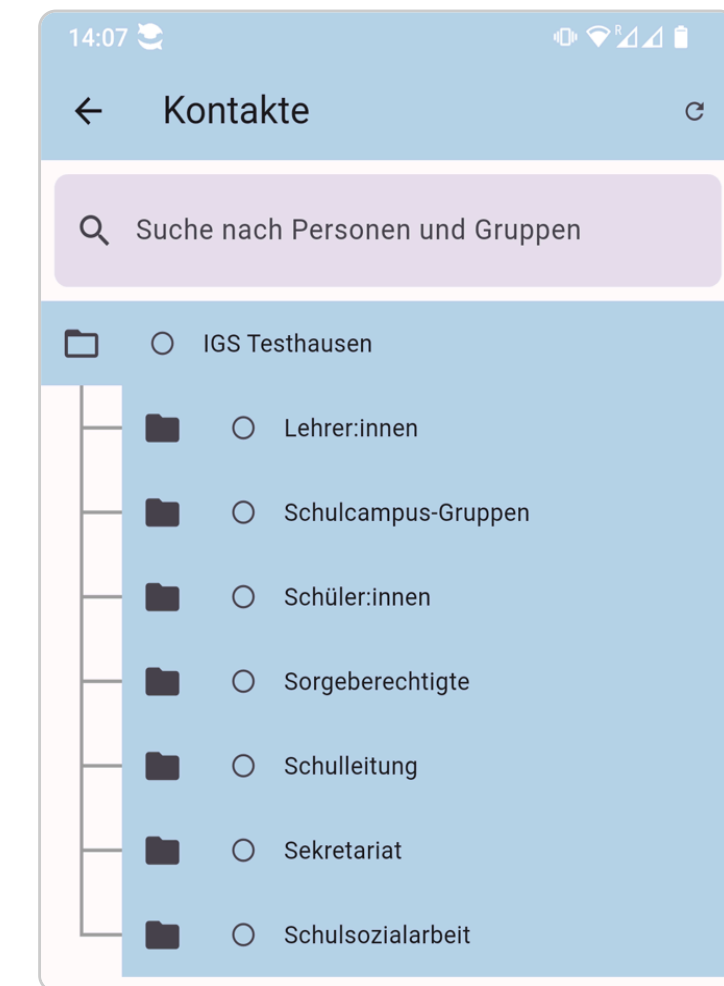


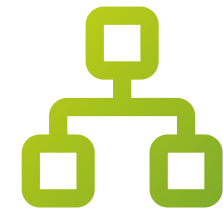
- TLDR: take care of immutability and uniqueness for the localpart



USER PROVISIONING: PRE-POPULATING USERS

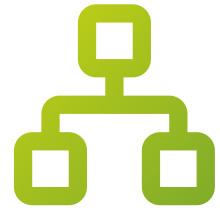
- problem: matrix account only created when user logs in
- other chat integrations need existing accounts already
 - Moodle (LMS): invite students into courses
 - address book (Schulchat)
- pre-populate from identity stores (LDAP, AD) with scripts
- custom: IDM-provisioner for Schulchat
 - IDM decides who may log in and who sees whom
 - class rooms exist before the first login





MAPPING OF ORG STRUCTURES

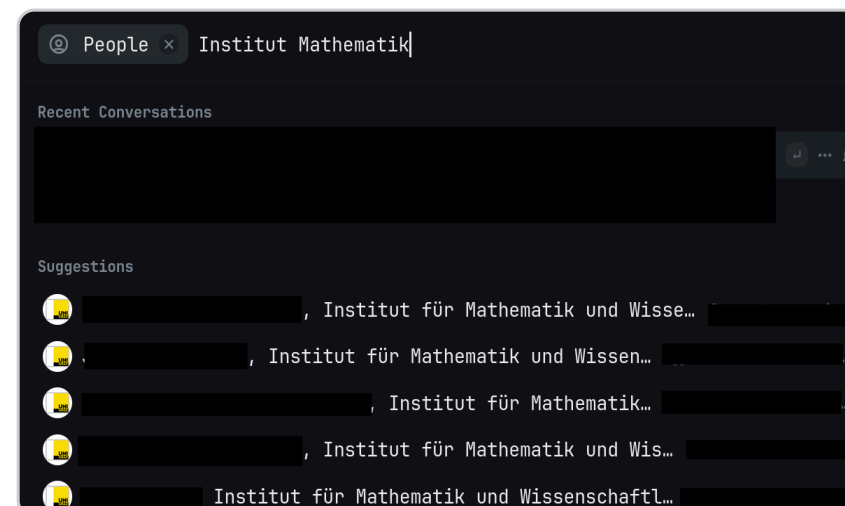
- Spaces + Rooms for hierarchical mappings
- fixed 1:1 mapping from store
 - nice for auto-syncs (whole LDAP groups)
 - needs a "clean" user-store, else cluttering
- user-created hierarchy
 - natural emerging structures, flexible
 - needs manual work (creation, maintenance)
- mixture
 - user-created hierarchy + some auto-syncs
 - less manual work, still flexible
 - only auto-sync specific (needed) groups



ORG MAPPING IN PRACTICE

LDAP group → room with ldap2matrixsync, and maiden search

```
- matrix_room_alias: "matrix_room_alias_and_name"
  # testing out the LDAP filter works best with the Apache Directory Studio
  ldap_filter_matrix_users: "(&|(sAMAccountName=username3)
(memberOf=CN=groupname,OU=organizational_subunit,OU=organizational_unit,DC=subdomain,DC=domain,DC=
com)))"
  # kicks all users from the room that are not in the filter
  auto_kick: true
  # gives the users in this filter moderator permissions (power level 50)
  # and invites them into the room if they are not in the filter above
  ldap_moderator: "(&|(sAMAccountName=username1)(sAMAccountName=username2)))"
```



maiden

custom search injection



02

LAW AND COMPLIANCE



GDPR AND FRIENDS

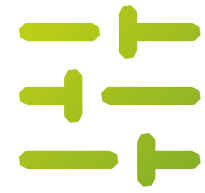
- Common GDPR misconceptions
- Federation
- Data retention
- E2EE settings



RELEVANT GDPR ARTICLES

- Art. 17 erasure: people can have their data deleted (hardest)
- Art. 16 rectification: people can fix wrong data
- Art. 5 storage limitation: keep data only as long as needed
- Art. 25 data-protection: privacy by design and by default
- Art. 12/13 transparency: tell people what you store and why

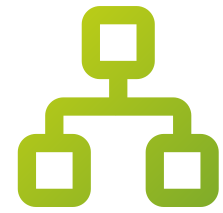
Plain-language summary, not legal advice.



GDPR IN PRACTICE

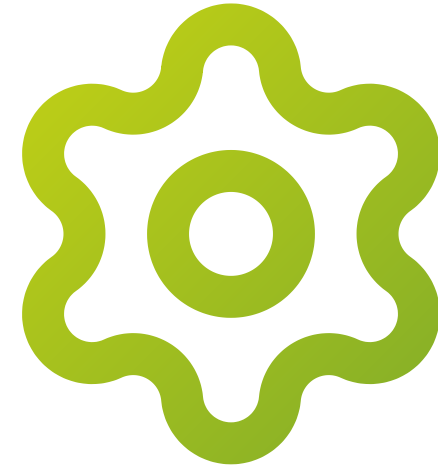
- Art. 17 erasure: redaction hides the content, keeps metadata
 - `redaction_retention_period` (7d): the unredacted copy stays in DB
 - `redaction_allowed_period` makes older messages unredactable
 - hard delete: `purge_jobs` / `purge_history`; account erasure: deactivate with `erase`
 - media needs its own purge (`media_retention` or admin delete)
 - federated: cannot force remote servers to delete; backups are separate
- Art. 16 rectification: Displayname and avatar yes, mXID never
- Art. 5 storage: no purge by default, set retention, media purge, short IP age
- Art. 25 by default: E2EE on, retention on
- Art. 12/13 transparency: what is stored, who can read, how to exercise rights

Not legal advice, verify with your DPO.



PUBLIC, CLOSED, ARCHIVING

- federated: copies land on external servers you do not control
- closed: federation off but same GDPR duties
- forced E2EE off: no config switch (only a module)
 - a room cannot go back to cleartext
- forced cleartext archive:
 - legal hold beats erasure
 - needs a DPIA and staff consultation
 - no built-in archival tool



03

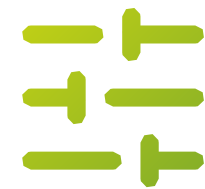
ADMINISTRATION AND MODERATION



RETENTION: PURGE JOBS IN STAGES

- retention is off by default
- if enabled: defaults to one daily job purge over every room
 - short-lived rooms then keep data up to a day too long
- tier the jobs by lifetime + a catch-all
- lifetime limits: `allowed_lifetime_min/max` cap the effective per-room policy

```
allowed_lifetime_max: 1y
purge_jobs:
- longest_max_lifetime: 3d
  interval: 6h
- shortest_max_lifetime: 3d
  longest_max_lifetime: 90d
  interval: 1d
- shortest_max_lifetime: 90d
  longest_max_lifetime: 1y
  interval: 7d
- shortest_max_lifetime: 1y
  interval: 30d
```



ADMINISTRATION

- Admin Tools: ketesa, synadm, matrix-wrench
- MAS
- Moderation Tools (Draupnir)
- Admin actions

Users										
Search [input] Show deactivated... Show locked users Exclude locked Show guests Exclude guests Show system [input] Find user + Create Export CSV Import										
	Avatar	User ID ↑	Display name	Guest	Server Administrator	Deactivated	Locked	Shadow banned	Erased	Created at
☐		@+123456:example.com		x	x	✓	x	✓	✓	04/08/2025, 03:56:42 PM
☐		@_webhooks_test:example.com	test (Webhook)	x	x	x	x	x	x	12/06/2025, 01:30:02 PM
☐		@admin:example.com	admin	x	✓	x	x	x	x	02/17/2025, 03:25:44 PM
☐		@aine:example.com	Aine etke.cc	x	x	x	x	x	x	02/01/2026, 04:07:39 PM
☐		@bailbot:example.com	bailbot	x	x	x	x	x	x	02/17/2025, 03:25:34 PM
☐		@beastafk:example.com	Beastafk etke.cc	x	✓	x	x	x	x	08/14/2025, 10:31:20 PM
☐		@blueskybot:example.com	Bluesky bridge bot	x	x	x	x	x	x	02/24/2025, 05:11:36 PM
☐		@buscarron:example.com	buscarron	x	x	x	x	x	x	02/17/2025, 03:25:41 PM
☐		@ci-test:example.com	CI Test Runner	x	✓	x	x	x	x	02/17/2025, 03:31:32 PM
☐		@dadsa:example.com		x	x	✓	x	x	✓	04/08/2025, 04:22:48 PM
☐		@discord_1438494822540378204:example.com	User (Discord)	x	x	x	x	x	x	11/13/2025, 12:05:59 PM
☐		@discordbot:example.com	Discord bridge bot	x	x	x	x	x	x	02/17/2025, 03:24:17 PM
☐		@draupnir:example.com	draupnir	x	✓	x	x	x	x	08/14/2025, 01:33:01 PM
☐		@emailbot:example.com	emailbot	x	x	x	x	x	x	02/17/2025, 03:25:39 PM

Ketesa

users, rooms, media, MAS sessions



CHALLENGES FOR USERS: E2EE

- keys live on the device (if key backup not setup)
 - lose the recovery key (or sign out everywhere): history is gone
 - "Unable to decrypt": backup not restored, device unverified/verified-only sharing
- key backup: encrypted copy of your keys on the server, unlocked with a recovery key
 - available in the main clients: enable it and prompt users to
- verification: cross-signing via emoji / QR
- search function in E2EE rooms
- bridges and bots need their own E2EE support



ROOM PERMISSIONS: DE-OPPING AND ADMINS

- room power levels:
 - default 0 user, 50 moderator, 100 admin
 - you cannot grant above your own
 - invites: default level 0, every member may invite
- two admins at 100 cannot demote each other
- deop the last admin and an older room is stuck
- room v12: the creator is privileged and cannot be demoted (MSC4289)
- no hierarchy: space roles do not apply inside rooms
- a server admin can impersonate a user via the admin API



ADMIN ACTIONS

- Room admin
 - report, redact, kick, ban, block
 - server ACL: cut one server from the room (devtools or bot)
- Server admin
 - suspend, shadow ban, purge history, delete room
 - media quarantine, make_room_admin, impersonation



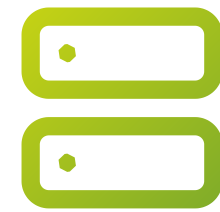
MODERATION

- Draupnir bot: one management room, policy lists, synapse-http-antispam module
- Actions in the management room:
 - ban / unban: every protected room + the policy list, unban removes the rule
 - kick, redact: single room, housekeeping
 - suspend, deactivate: whole account, needs a server admin account
 - takedown: shut a room down, purge and block it
 - setPowerLevel, hijackRoom: recover rooms that have no admin left
- Protections (automatic): JoinWaveShortCircuit, NewJoinerProtection, RoomTakedownProtection
- Media: quarantine by media ID, user or room



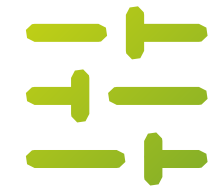
04

INFRASTRUCTURE



DEPLOYMENT

- Base deployment mode
 - k8s is the reference
 - one big VM with Ansible is okay too
 - pick what your team is familiar with
- Architecture
 - Synapse main + workers, Redis/Valkey bus
 - external Postgres
- Generic worker: sync, federation, client API. One-offs: media, presence
- Reverse proxy routes per path to workers



OPERATION TIPS

- Scale by replicas:
 - generic worker: add replicas, no Synapse config (pin SSO to one process)
 - event persisters: sharded by room, config entry + restart all workers
- One pod only:
 - main, media repo, presence, typing, to_device, account_data
- Add when needed:
 - initial-sync worker: isolate the heavy `/sync` without `since`
 - presence: off, or one dedicated pod. Federation makes it expensive
- External Postgres HA (Zalando / Patroni / Spilo) + raise `max_connections`
- Media on RWX (NFS), only media worker mounts. Back up media separately
- Monitoring: Prometheus / OTel, Loki, Grafana synapse dashboard



05

CLIENTS, VIDEO, EXTENSIONS



SO MANY CLIENTS



Element
Web /
Desktop



Element X



FluffyChat



Cinny



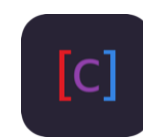
Nheko



chatrix



chatty



chooj



Commet



Element
Classic



Ement.el



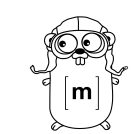
Extera



Extera Next



Fractal



gomuks



gotktrix



Hydrogen



iamb



kazv



Komai



Lightning



Mactrix



Mages



matrix-
commander



matrix-
commander-
rs



Miiatrix



mnotify



NeoChat



Neoment



polycule



Quadrix



Quaternion



Relay



Sable



SchildiChat
Legacy



SchildiChat
Next



SchildiChat
Revenge



Singularity



Syphon



Tacit



Tammy



Tesseract



Thunderbird



WanChat



Watch The
Matrix



WizardChat



Zam



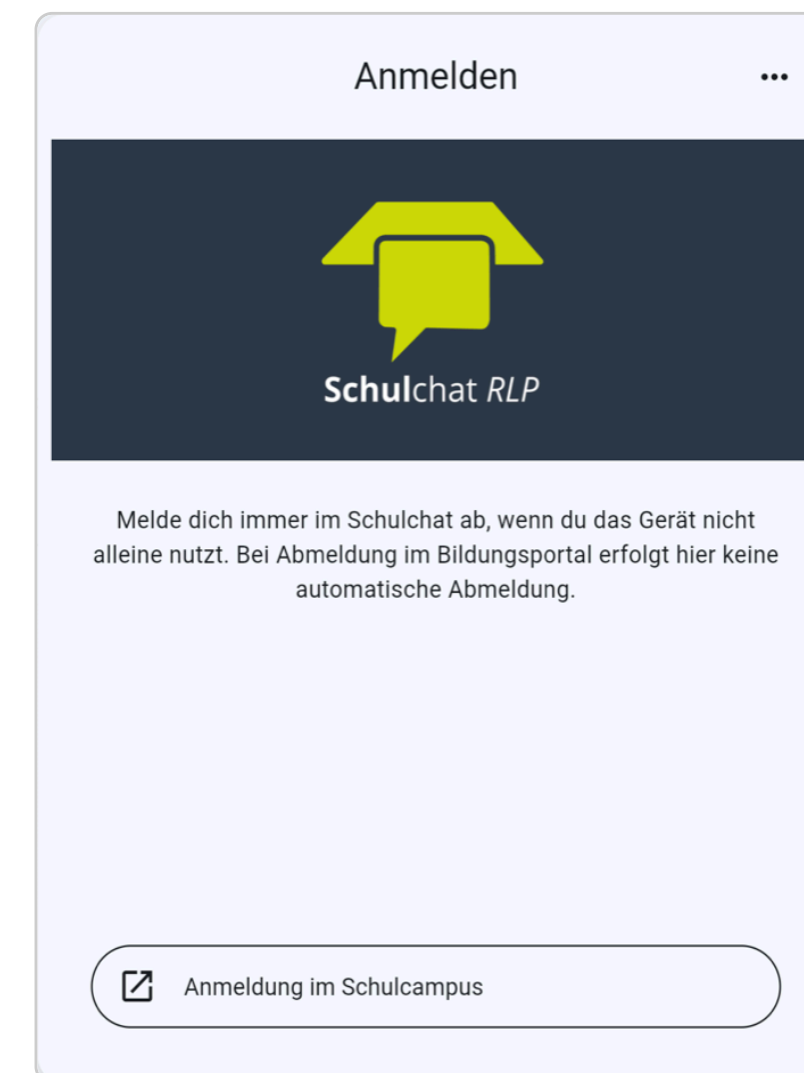
Zooid

Which feature set does your organization need,
and which clients support it?



VIABLE CLIENTS AND UX

- Which clients work for non-technical users?
- Non-technical users need a simple login
- Client configuration and branding
 - preset homeserver
 - enable or hide lab features (e.g. LaTeX)
 - rec: support one client per platform (power users may opt in)



VIDEO CALLS

- LiveKit / Element Call
- LiveKit / Fluffychat
- BigBlueButton, Jitsi
 - BBB 4.0: LiveKit default. Opt-in since 3.0
- Self-hosting the SFU



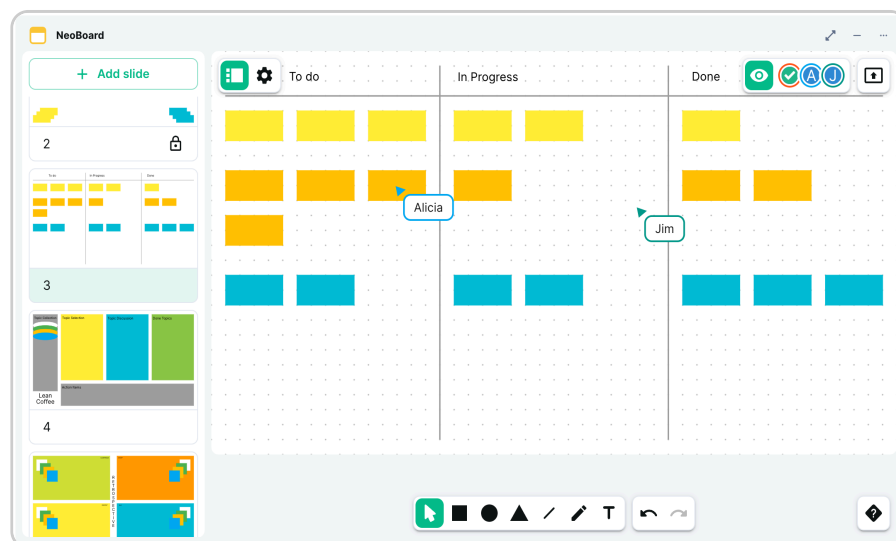
USEFUL WIDGETS

- Widgets:  NeoBoard (whiteboard), NeoDateFix (meetings), Etherpad (documents)
- Bots:  AI/LLM (baibot), auto translation, helpdesk
- Webhooks:  hookshot (alerts, Jira tickets, Git notifications, feeds)
- Bridges:  mautrix

More integrations: matrix.org/ecosystem/integrations

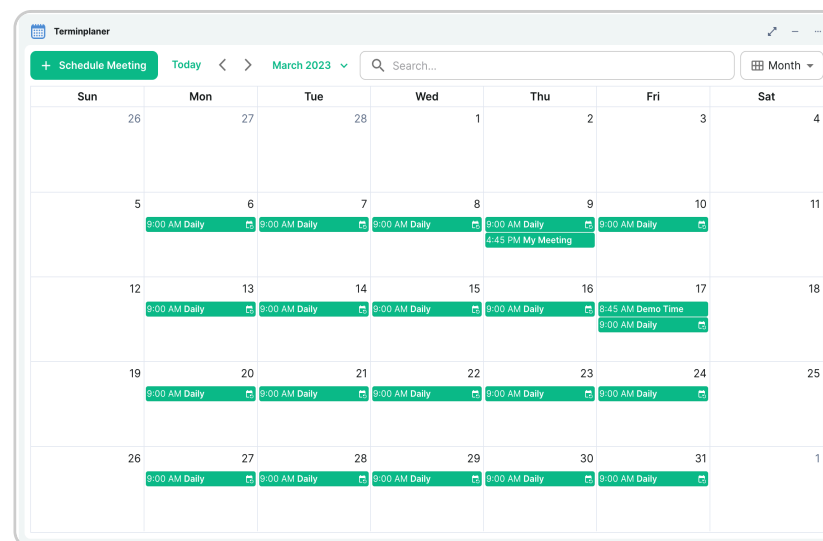


WIDGETS



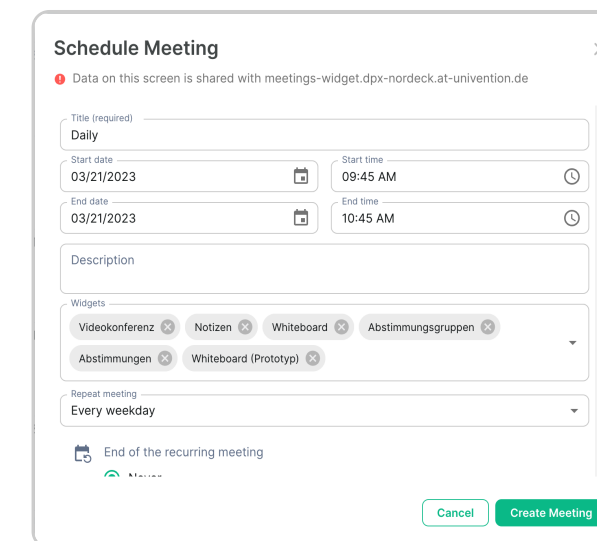
NeoBoard

collaborative whiteboard



NeoDateFix

meeting organizer

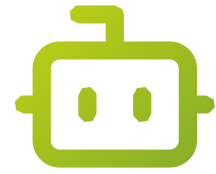


schedule a meeting,
pick widgets, repeat

- NeoBoard: whiteboard in the room: slides, Kanban, live cursors
- NeoDateFix: calendar widget + a bot creates a room per meeting, picks its widgets
- Etherpad: a simple collaborative text editor as a widget
- data stays in the Matrix room, E2EE; needs a widget-capable client



matrix-neoboard · matrix-meetings

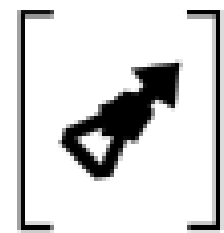


BOTS: AI, TRANSLATION, HELPDESK

- AI/LLM assistant: baibot: text, voice and images, OpenAI or local models
- voice messages: transcribe them, or answer as voice
- auto-translation: read a multilingual room in your own language
- helpdesk: Honoroit, a Matrix helpdesk bot



github.com/etkecc/baibot · [honoroit](#) · by [etke.cc](#)



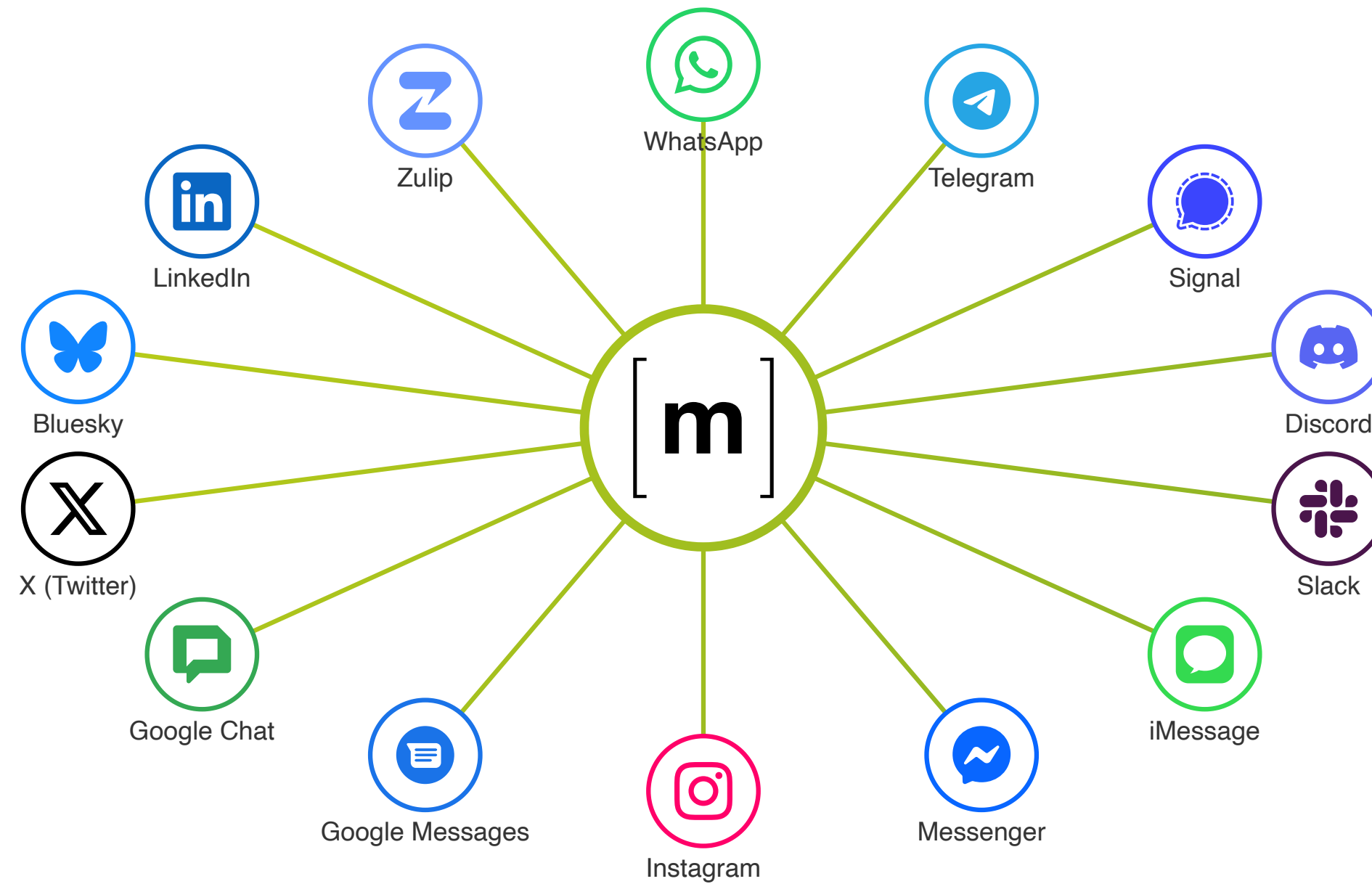
WEBHOOKS: HOOKSHOT

- connect services to rooms: GitHub, GitLab, Jira, generic webhooks
- Git: commits, merge requests, issues
- tickets: Jira updates and comments
- alerts and CI / monitoring notifications
- RSS / Atom feeds: news and blogs into a room
- templates written in JavaScript

 github.com/matrix-org/matrix-hookshot · maintained with Element



BRIDGES: MAUTRIX



 github.com/mautrix



06

CUSTOM SOLUTIONS



WHAT WE BUILT

- Custom search injection and ranking (maiden)
- ldap2matrixsync: rooms and moderators from LDAP groups
-  Schulchat RLP: based on our FluffyChat and Synapse forks
 - IDM provisioner
 - address book
 - working around the spec: deopping chat rooms, invite permissions
 - custom features for schools
 - dashboard
 - admin panel

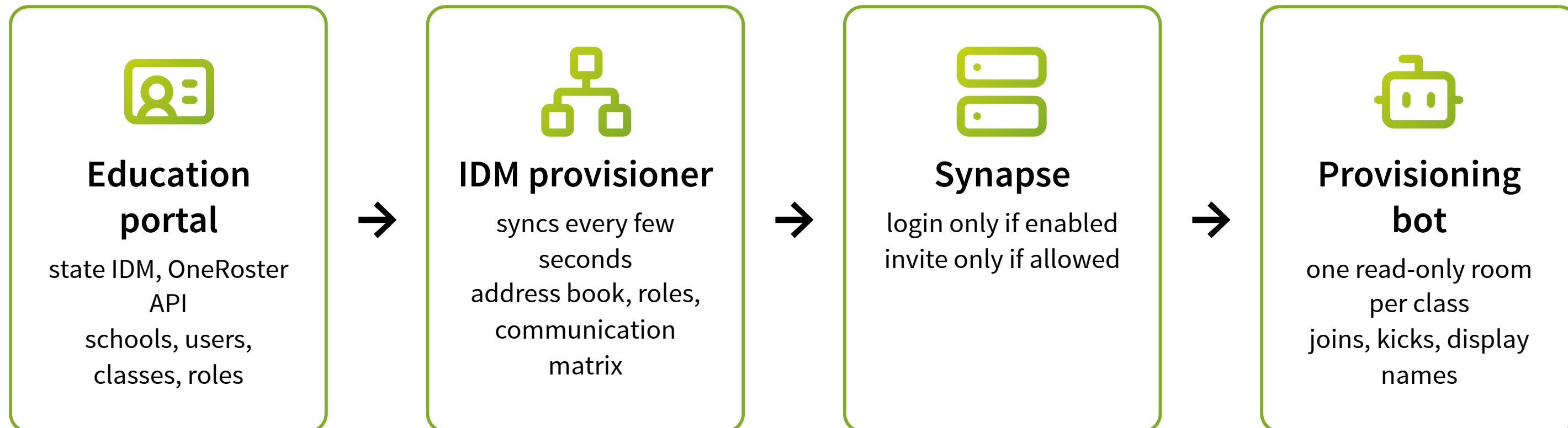
EDUCATION PORTAL

GS Testdorf		☐	Chat	Chef	c.chat	Schulleitung	Kollegium		☒	
Benutzer Übersicht Sorgeberechtigte Anlegen Importieren Accountbriefe OrgWechsel Gruppen Übersicht Anlegen Freischaltcodes Übersicht Anlegen		☐	Chat	Lehrer	l.chat	Lehrkraft	Fachschaft Biologie		☒	
		☐	Chat	Lehrkraftdrei	leh.chat	Lehrkraft	Fachschaft Biologie		☒	
		☐	Chat	Lehrkraftvier	lehr.chat	Lehrkraft			☒	
		☐	Chat	Lehrkraftzwei	le.chat	Lehrkraft	Fachschaft Biologie		☒	
		☐	Chat	Schüler	s.chat	Schüler	5aChat (2023/2024)		☒	
		☐	Chat	Schülerdrei	sch.chat	Schüler	5aChat (2023/2024)		☒	
		☐	Chat	Schülerfünf	schue.chat	Schüler	Schulgemeinschaft		☒	
		☐	Chat	Schülersechs	schuel.chat		Testgruppe		☒	
		☐	Chat	Schülervier	schu.chat	Schüler	5aChat (2023/2024)		☒	
		☐	Chat	Schülerzwei	sc.chat	Schüler	5aChat (2023/2024)		☒	
		☐	Chat	Sekretärin	se.chat	Sekretariat			☒	
		☐	Chat	Sozial	so.chat				☒	
		☐	Chatty	ElternsprecherNeuname	el.chat	Sorgeberechtigte	10a fairkom Test (2025/2026)		☒	
		☐	FreischaltungMatrix	Ohne	o.freischaltungmatri	Schüler	Schulgemeinschaft		☒	

Users, classes and roles live in the Education portal, our IDM provisioner syncs them via the OneRoster API.



IDM PROVISIONER





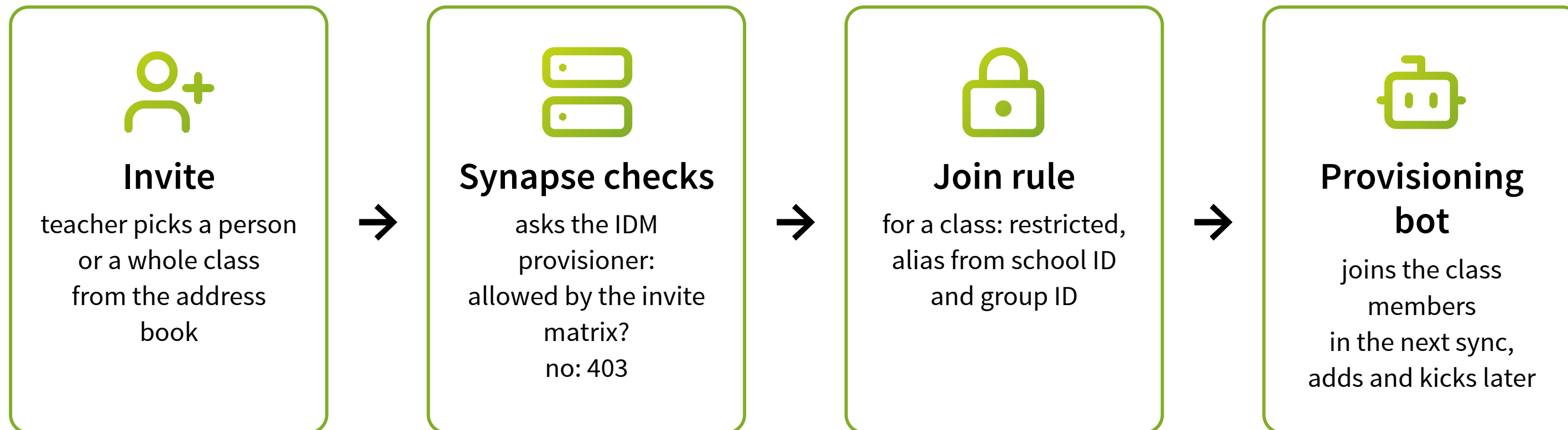
COMMUNICATION MATRIX

I→ Rolle Lehrkraft		I→ Rolle Schüler	
Lehrkraft	☒	Lehrkraft	☐
Schüler	☒	Schüler	☐
Sorgeberechtigte	☒	Sorgeberechtigte	☐
Schulleitung	☒	Schulleitung	☐
Sekretariat	☒	Sekretariat	☐
Schulsozialarbeit	☒	Schulsozialarbeit	☐
Elternbeirat	☒	Elternbeirat	☐
OrganisationsAdmin	☒	OrganisationsAdmin	☐
Bildungsportal-Gruppen	☒	Bildungsportal-Gruppen Du kannst diese Einstellung nicht ändern	☒

Each school decides which role may find and write which other role.



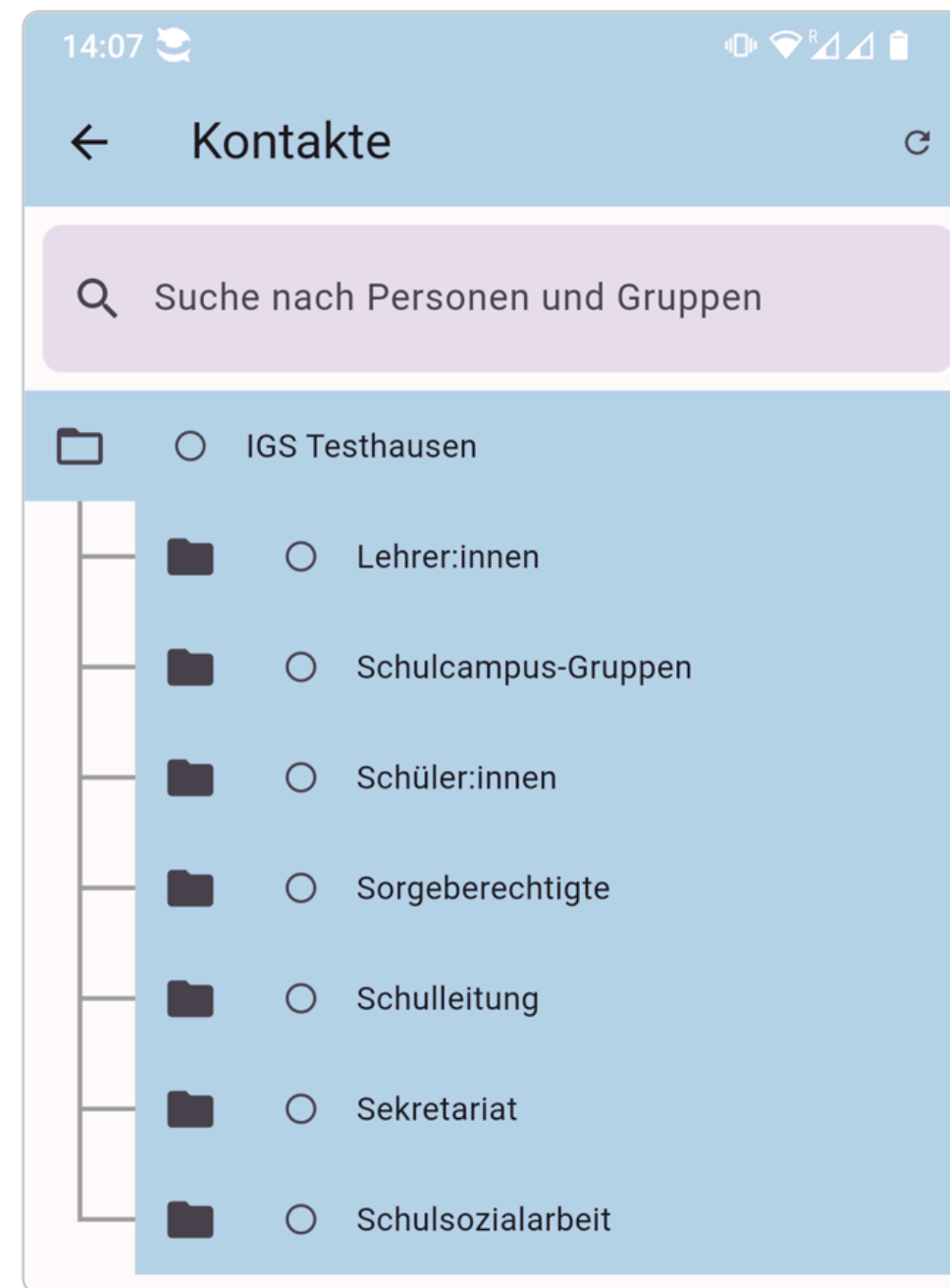
WHO MAY INVITE WHOM



- one person: checked on every invite, not allowed gets a 403
- a whole class: one click, the room follows the class
- each school's admin sets the rules, some are fixed



ADDRESS BOOK



Users find people by school, role, class or name, not by Matrix ID.

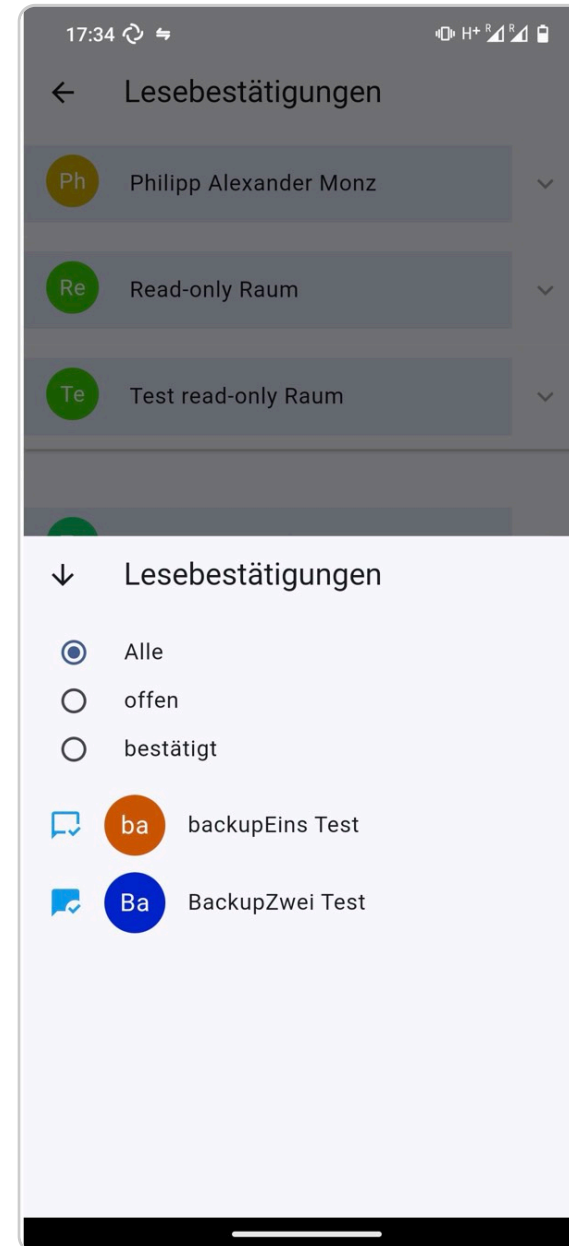


LAST MODERATOR STAYS

- leave or kick of the last admin (PL 100) is refused
 - "At least one moderator must remain in a room"
- exceptions: read-only rooms, and the last member may leave
- someone leaves the school: the bot makes their rooms read-only if no admin remains
- admin API: which rooms of a school lose their last moderator?



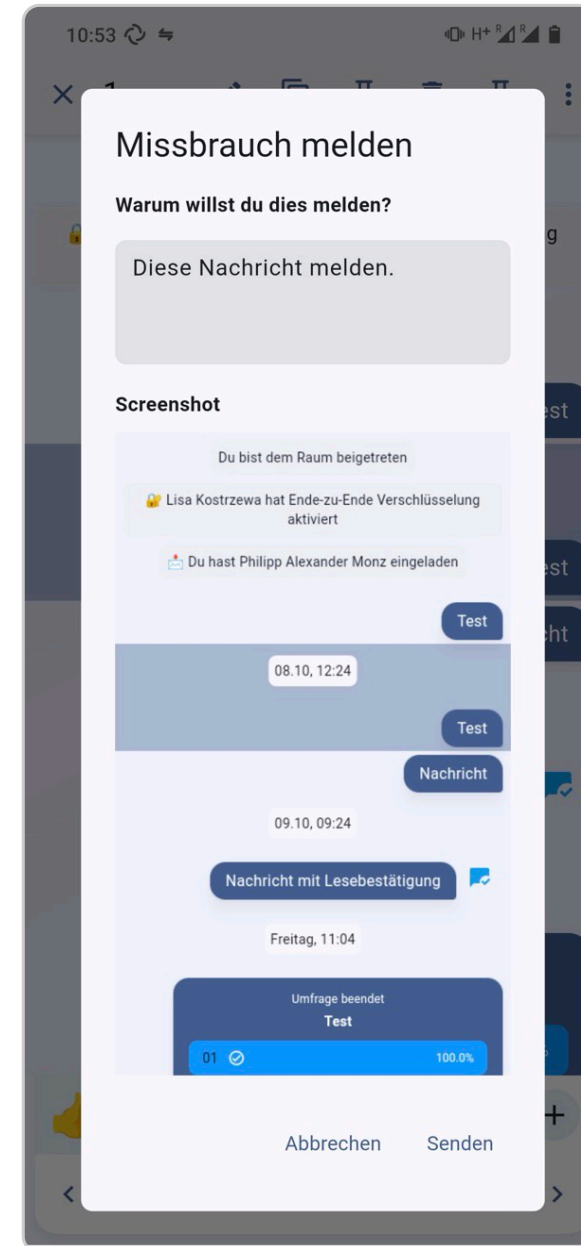
ACTIVE READ RECEIPTS



Notes on trips, for example, need active proof.



REPORT ABUSE



Schools are responsible for what happens in their chats: together against bullying.



RECOVERY MADE SIMPLE

Sicherheitsfrage beantworten um Chats zu entschlüsseln

Wie hieß bzw. heißt dein erstes Haustier oder Kuscheltier?

Wie hieß bzw. heißt dein erstes Haustier oder Kuscheltier?

Entsperre alte Nachrichten

Oder

Von anderem Gerät übertragen

Antwort auf Sicherheitsfrage vergessen?

Students want an easy recovery path instead of losing their recovery key.



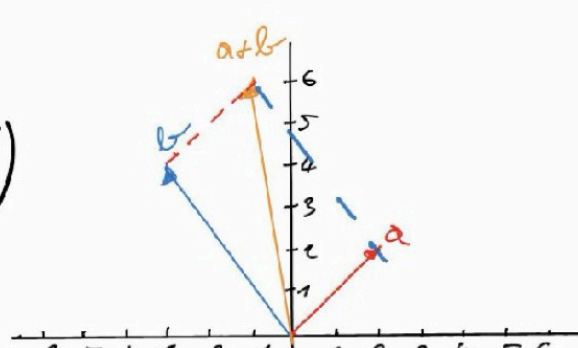
PDF PREVIEW

← aufgaben_loesung.pdf

< 1 / 5 >

1. Zeichnen Sie:

$$a = \begin{pmatrix} 2 \\ 2 \end{pmatrix}, b = \begin{pmatrix} -3 \\ 4 \end{pmatrix}, c = \begin{pmatrix} 5 \\ -1 \end{pmatrix}$$
$$a + b = \begin{pmatrix} -1 \\ 6 \end{pmatrix}, b + c = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

$$a + b = \begin{pmatrix} 2 \\ 2 \end{pmatrix} + \begin{pmatrix} -3 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 + (-3) \\ 2 + 4 \end{pmatrix} = \begin{pmatrix} -1 \\ 6 \end{pmatrix}$$


Worksheets shown as PDFs directly in the chat are handy for classwork and homework.



POLLS

Which statement is true? [matrix] ...

☞ Mehrfachauswahl

... is decentralized.	✓
25.0%	1
... supports end-to-end encryption.	✓
25.0%	1
... can bridge to other chat platforms.	✓
25.0%	1
... is an open standard.	✓
25.0%	1

🗳 1 Stimmen >

✎ Bearbeiten

Teachers wanted votes and quizzes inside the school messenger.



ADMIN PANEL: ROOMS

Räume

Benutzer

Medien

Suchen

Schule

Datenbank-Raumstatistiken

Sperren

Spalten

Exportieren

☐	Avatar	Raum-ID	Verschlüsselungs-Algorithmus	Name ↑	Mitglieder	Ersteller:in	Displayname	Sichtbar im Raumverzeichnis	Aktionen
☐					1			×	Raumadministrator zuweisen
☐					2			×	Raumadministrator zuweisen
☐					1			×	Raumadministrator zuweisen
☐					1			×	Raumadministrator zuweisen
☐					2			×	Raumadministrator zuweisen
☐					1			×	Raumadministrator zuweisen

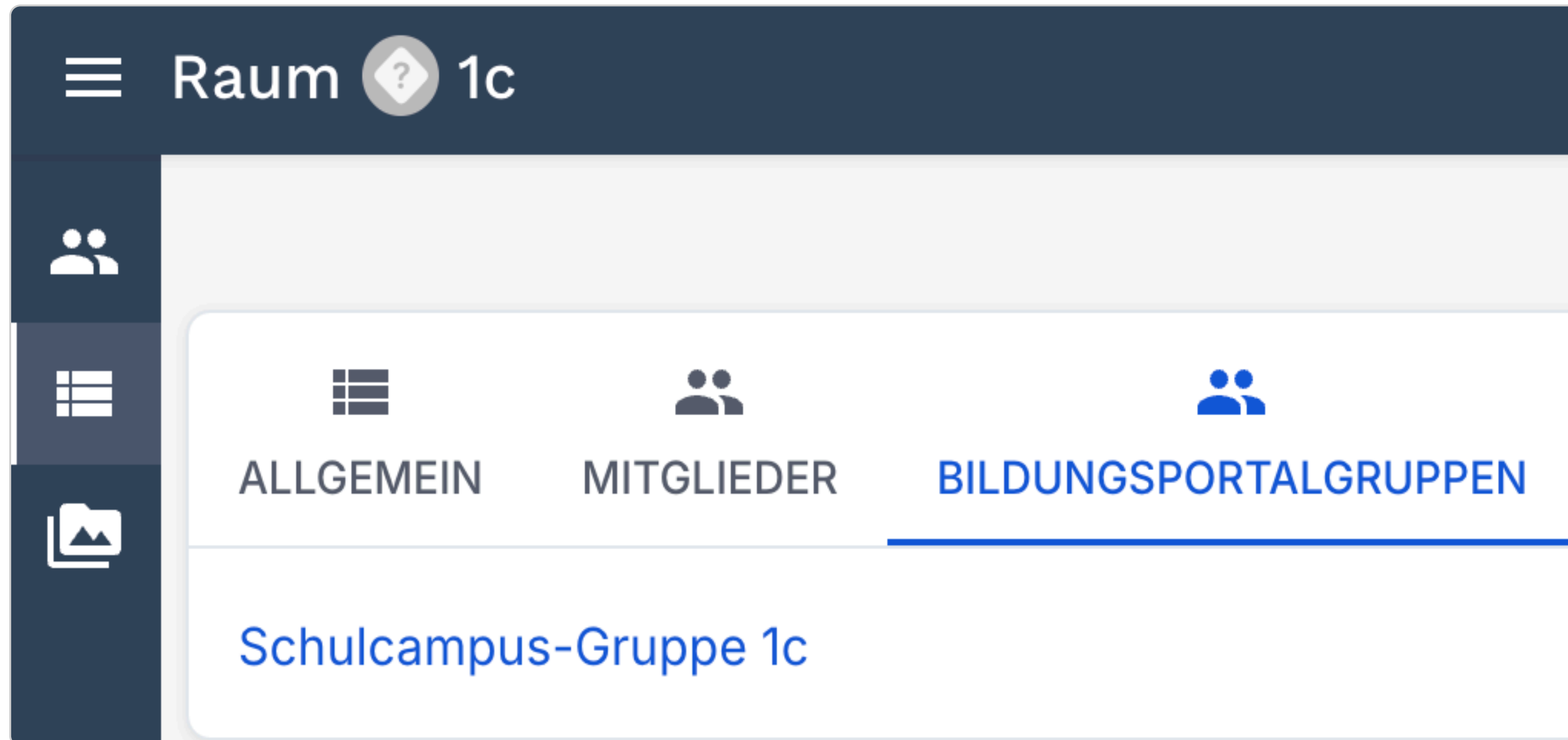
Rooms

filter by school, assign a room admin

Support can help a school without touching the database.



ADMIN PANEL: EDUCATION PORTAL GROUPS



Education portal groups
which class a room is opened to



TAKEAWAYS

- Plan identity and org mapping before the first user logs in
- Decide on federation, retention and E2EE early
- Moderation and admin tooling is not optional
- Vanilla Matrix is a great base, but expect to build some glue

THANK YOU!

Questions?

Jan Krammer

MATRIX @jan.krammer:fairchat.eu

MAIL jan.krammer@fairkom.eu

Philipp Monz

MATRIX @monz:fairchat.eu

MAIL philipp.monz@fairkom.eu

