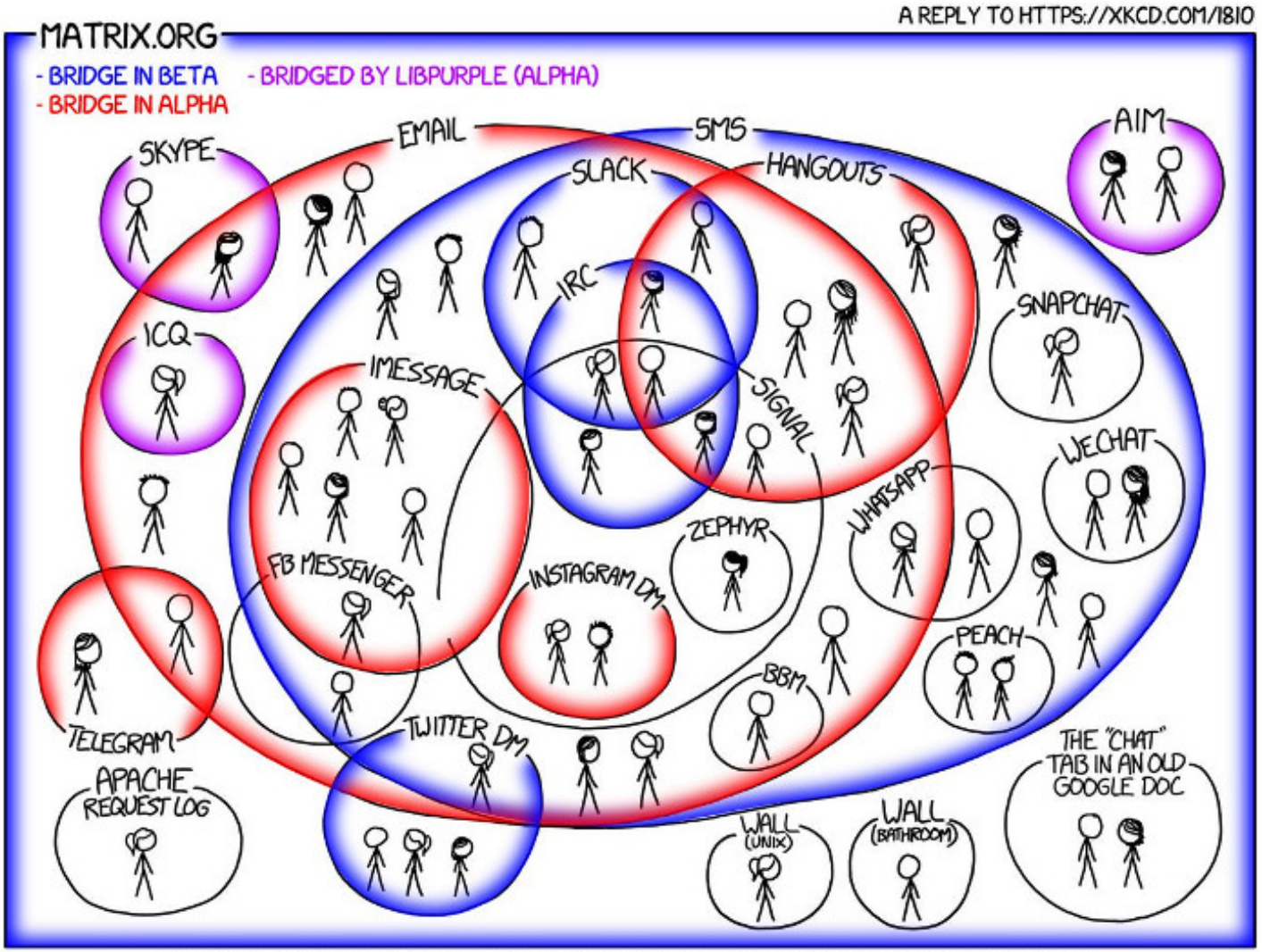
MATRIX | OLEG FIKSEL | FROSCON 2019



~~I HAVE A HARD TIME KEEPING TRACK OF WHICH CONTACTS USE WHICH CHAT SYSTEMS.~~
THIS IS ONE OF THE MAIN REASONS WE CREATED MATRIX.ORG :)

THANKS!

Special thanks for great support to:

- Matthew Hodgson - Co-Founder @matthew:matrix.org
- Ben Parsons - Developer Advocate @benpa:matrix.org

Oleg Fiksel

- DevOps Engineer
- Passionate about tech
- Like to automate everything

Goal of this talk

GOAL OF THIS TALK

- Part 1: Provide an overview of Matrix architecture and ecosystem

Goal of this talk

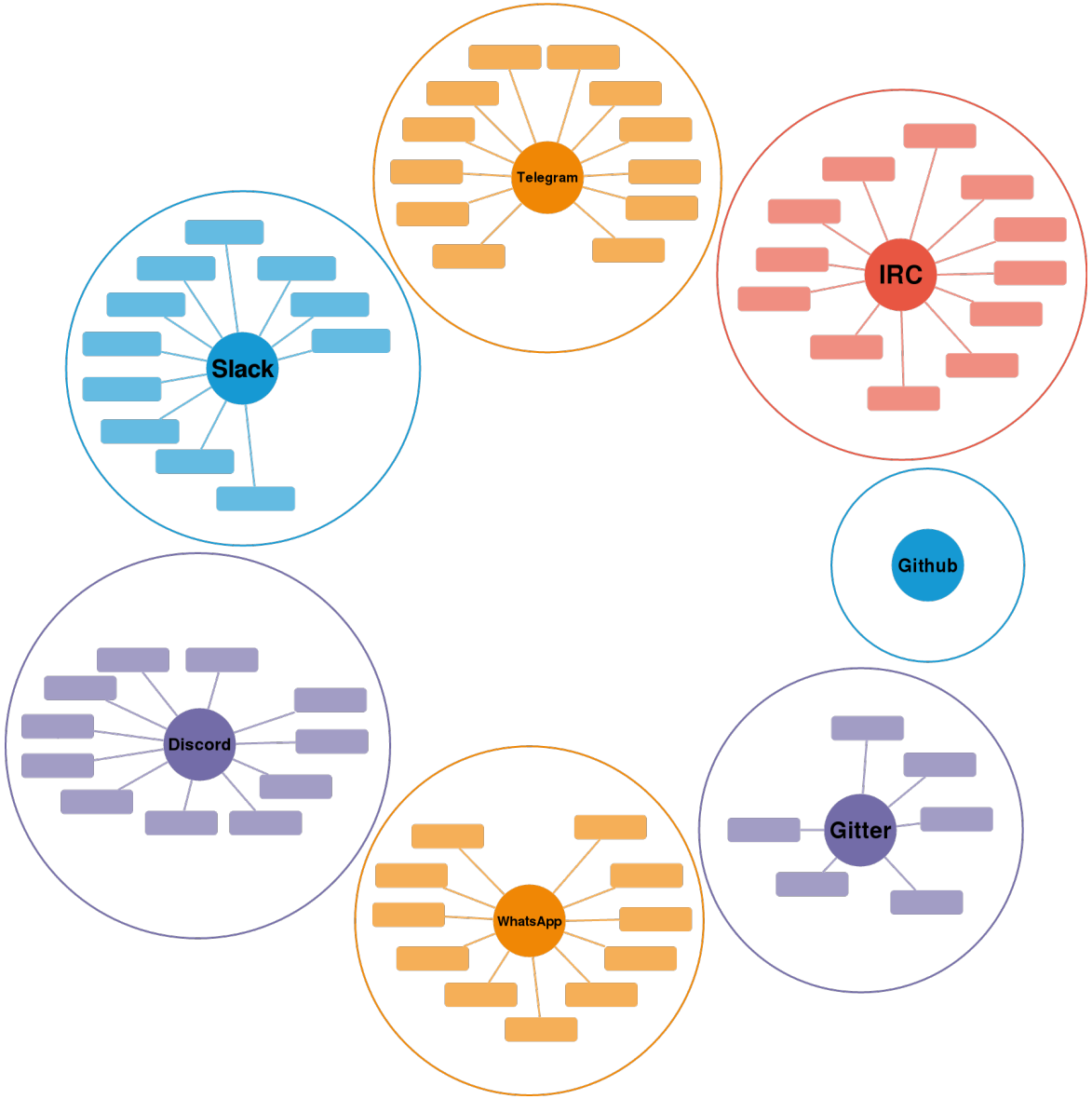
- Part 1: Provide an overview of Matrix architecture and ecosystem
- Part 2: Get hands-on experience with a Matrix demo environment (get your laptops ready)

WHAT IS MATRIX?

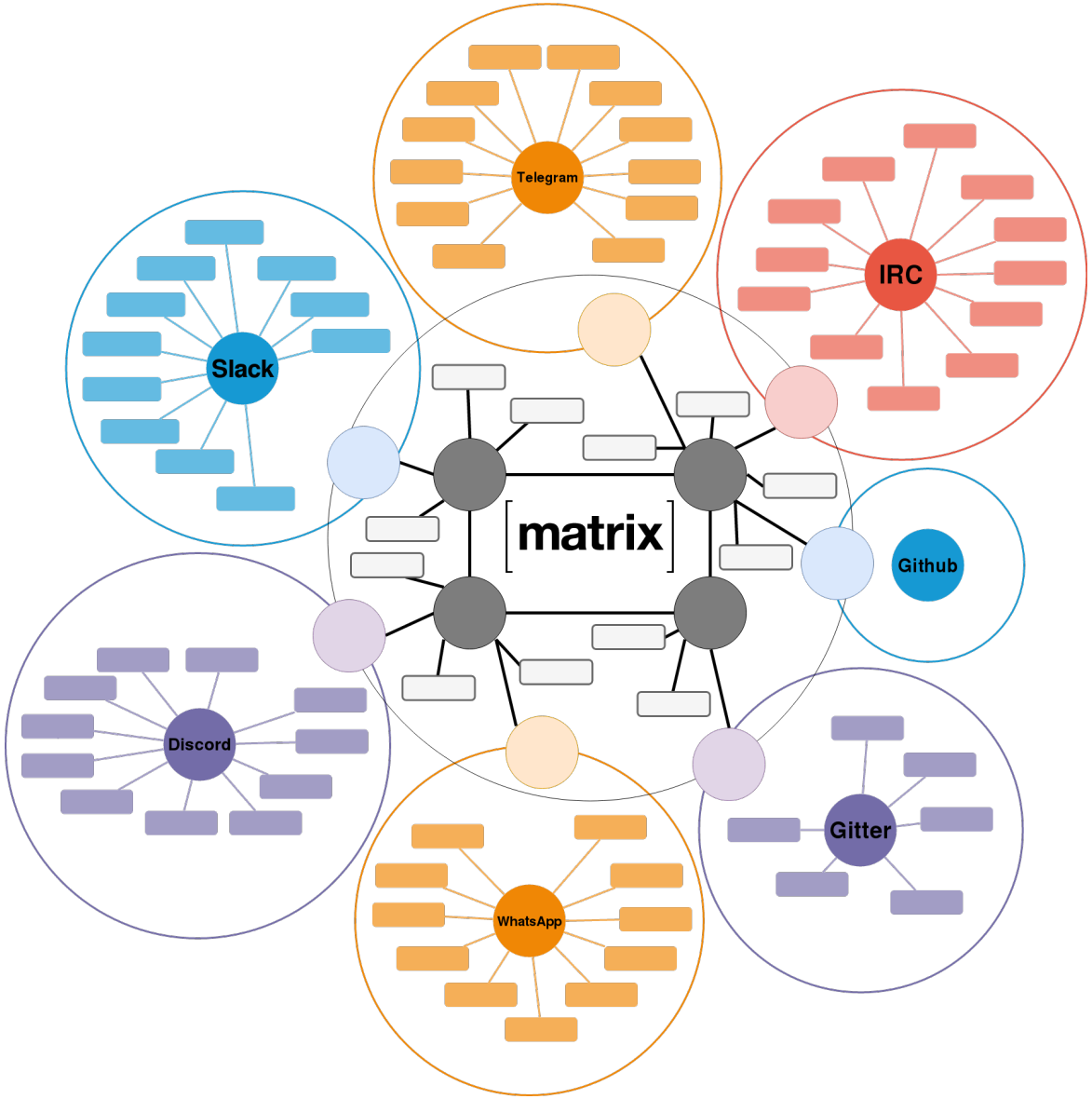
WHAT IS MATRIX?

Matrix is an open network for secure, decentralised real-time communication.

WHAT IS MATRIX?



WHAT IS MATRIX?



WHY I LIKE MATRIX

WHY I LIKE MATRIX

- Open source

Why I like Matrix

- Open source
- Distributed (no single party owns your conversations)

WHY I LIKE MATRIX

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen

WHY I LIKE MATRIX

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls

WHY I LIKE MATRIX

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design

WHY I LIKE MATRIX

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design
- Read & typing notifications

WHY I LIKE MATRIX

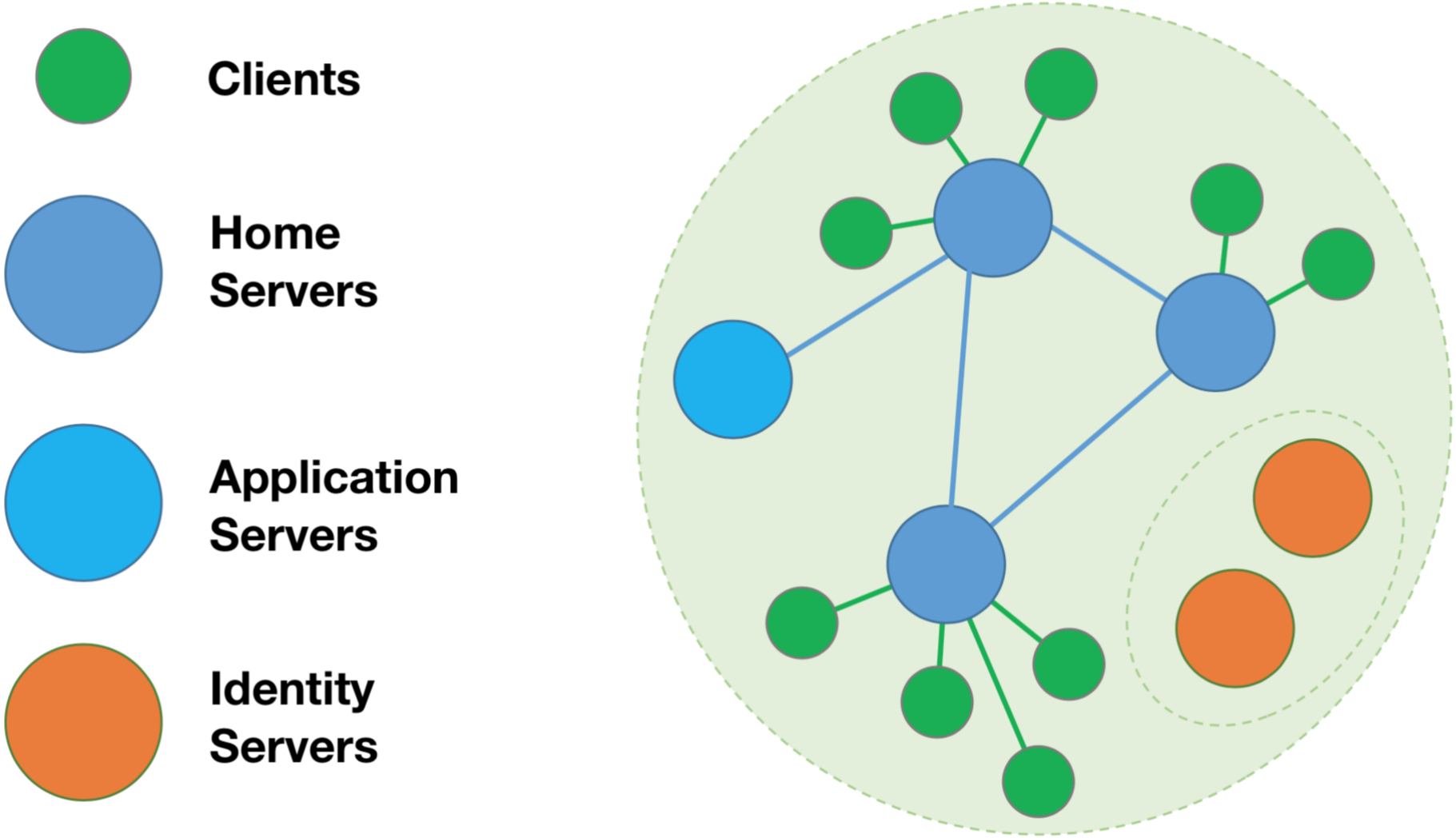
- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design
- Read & typing notifications
- Integrations

WHY I LIKE MATRIX

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design
- Read & typing notifications
- Integrations
- Healthy and friendly community

MATRIX DISTRIBUTED ARCHITECTURE

MATRIX DISTRIBUTED ARCHITECTURE



E2E ENCRYPTION

E2E ENCRYPTION

- Encryption without Open Source cannot be trusted (security by obscurity doesn't work)

E2E ENCRYPTION

- Encryption without Open Source cannot be trusted (security by obscurity doesn't work)
- Without end-to-end encryption, Matrix's replicated conversation history is a privacy problem

E2E ENCRYPTION

- Encryption without Open Source cannot be trusted (security by obscurity doesn't work)
- Without end-to-end encryption, Matrix's replicated conversation history is a privacy problem
- Two years spent building decentralised E2E crypto into the heart of Matrix

E2E ENCRYPTION

- Encryption without Open Source cannot be trusted (security by obscurity doesn't work)
- Without end-to-end encryption, Matrix's replicated conversation history is a privacy problem
- Two years spent building decentralised E2E crypto into the heart of Matrix
- Olm – a Double Ratchet implementation

E2E ENCRYPTION

- Encryption without Open Source cannot be trusted (security by obscurity doesn't work)
- Without end-to-end encryption, Matrix's replicated conversation history is a privacy problem
- Two years spent building decentralised E2E crypto into the heart of Matrix
- Olm – a Double Ratchet implementation
- Megolm - Entirely new ratchet for group chat with shareable history

Security Assessment

SECURITY ASSESSMENT

- libolm 1.3.0 assessed by NCC Group in Sept 2016
- Findings released to the public!
- Olm: 2x low risk finding, 1x informational
- Megolm: 1x high, 1x medium, 4x low risk.
- All findings fixed in libolm or the Matrix Client SDKs.
- No issues found in libolm since the audit!

ECOSYSTEM

ECOSYSTEM

Matrix Open Source Ecosystem

[matrix]

client-side

server-side

Synapse (1st gen Matrix Server)

Dendrite (2nd gen Server)

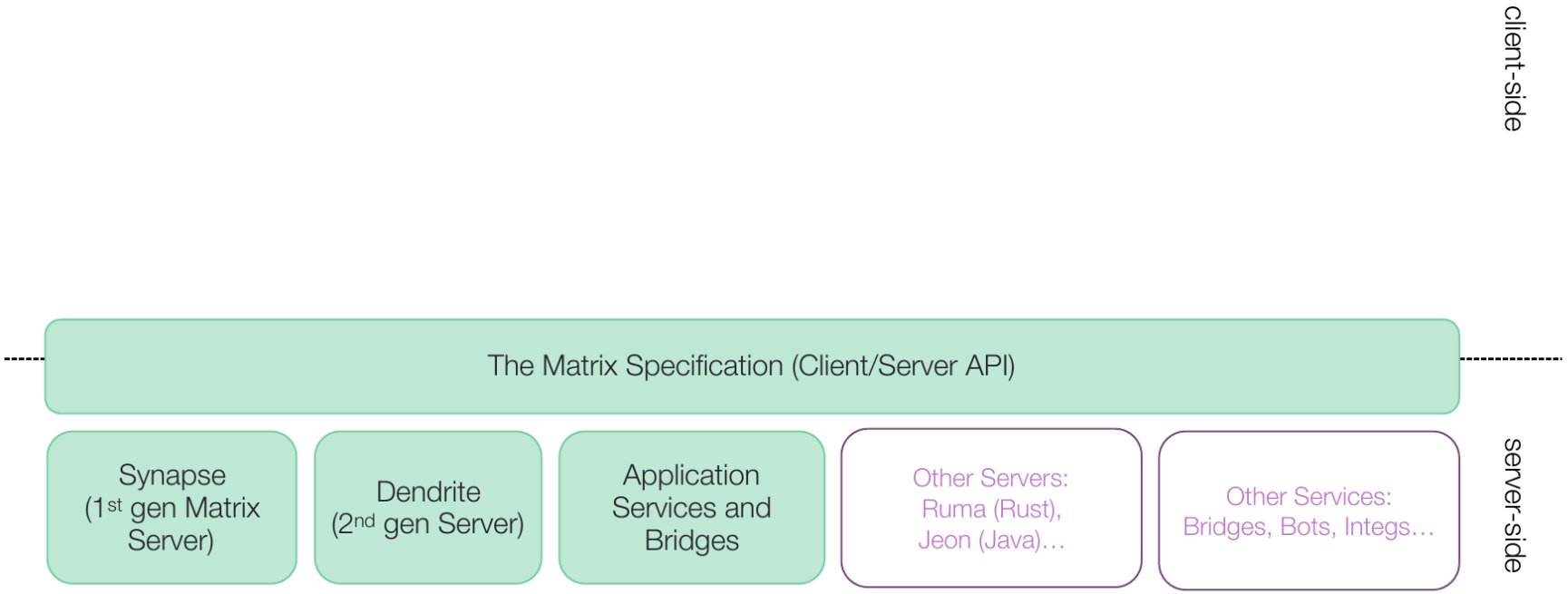
Application Services and Bridges

Other Servers: Ruma (Rust), Jeon (Java)…

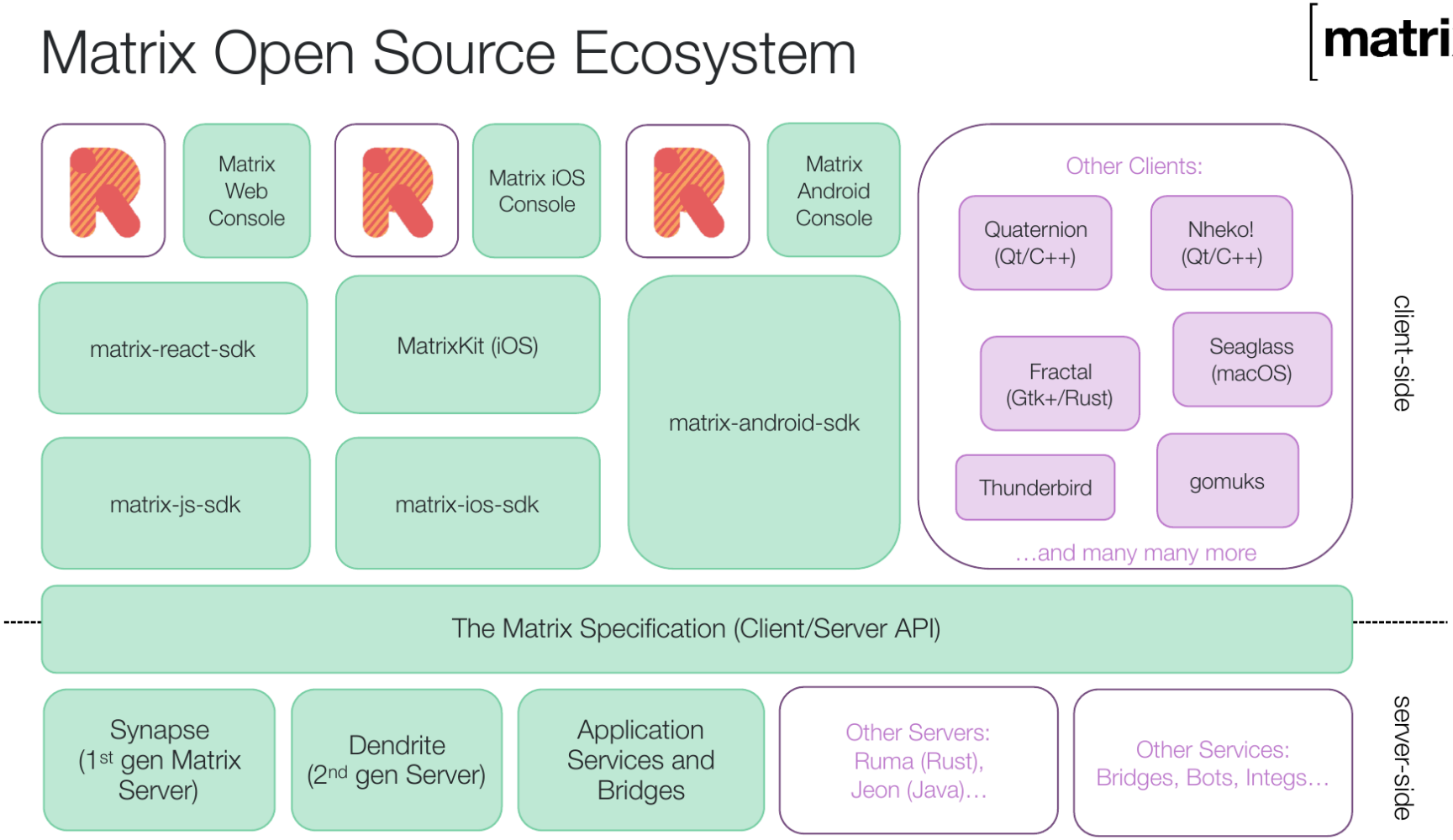
Other Services: Bridges, Bots, Integs…

ECOSYSTEM

Matrix Open Source Ecosystem



ECOSYSTEM


Matrix Open Source Ecosystem
[matrix]
Matrix Web Console
Matrix iOS Console
Matrix Android Console
matrix-react-sdk
MatrixKit (iOS)
matrix-android-sdk
matrix-js-sdk
matrix-ios-sdk
Other Clients:
Quaternion (Qt/C++)
Nheko! (Qt/C++)
Fractal (Gtk+/Rust)
Seaglass (macOS)
Thunderbird
gomuks
…and many many more
client-side
The Matrix Specification (Client/Server API)
Synapse (1st gen Matrix Server)
Dendrite (2nd gen Server)
Application Services and Bridges
Other Servers: Ruma (Rust), Jeon (Java)…
Other Services: Bridges, Bots, Integs…
server-side

CLIENTS

CLIENTS

- Riot (Web)

Clients

- Riot (Web)
- Nheko (Qt)

Clients

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)

CLIENTS

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
- Seaglass (MacOS)

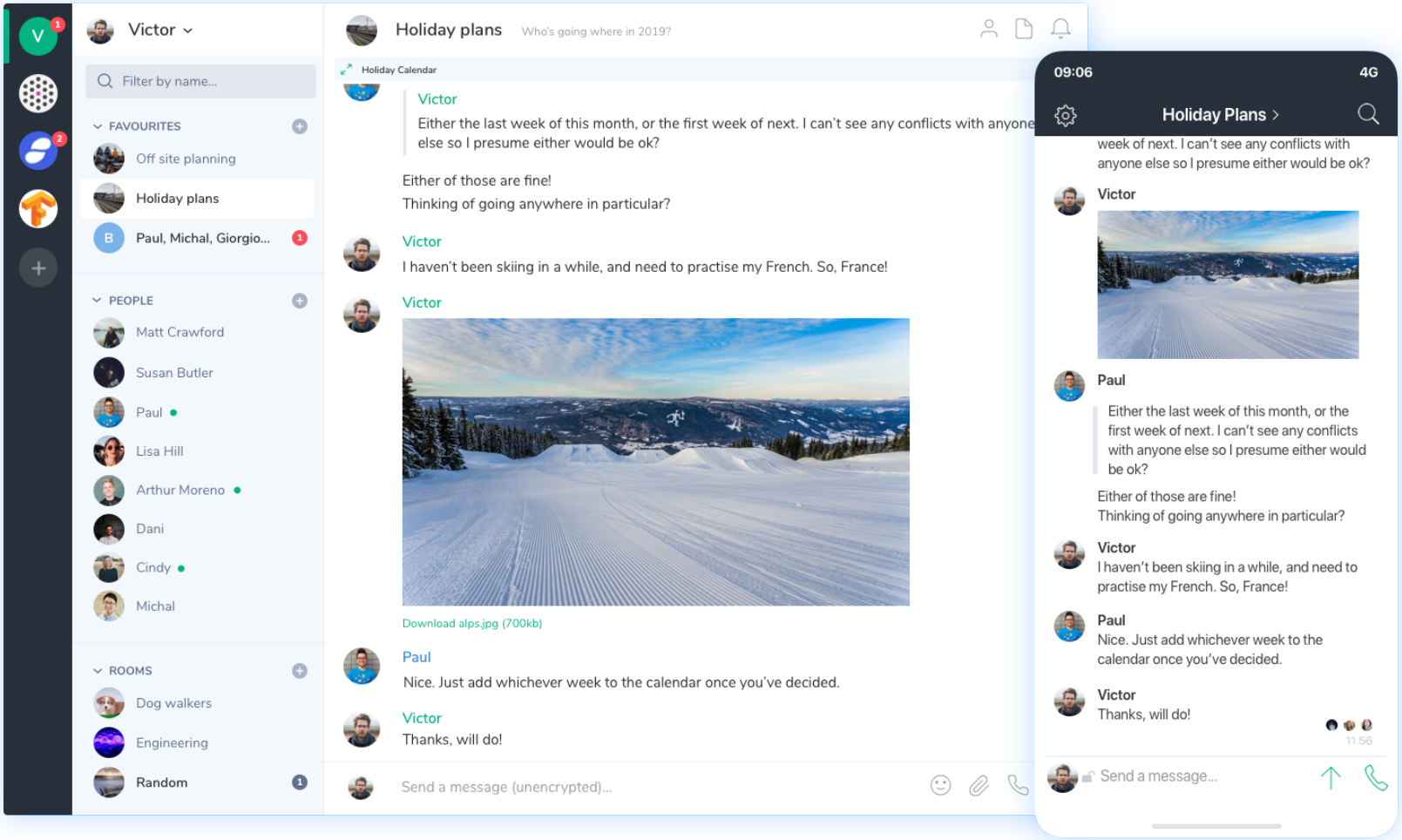
CLIENTS

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
- Seaglass (MacOS)
- Fractal (GTK)

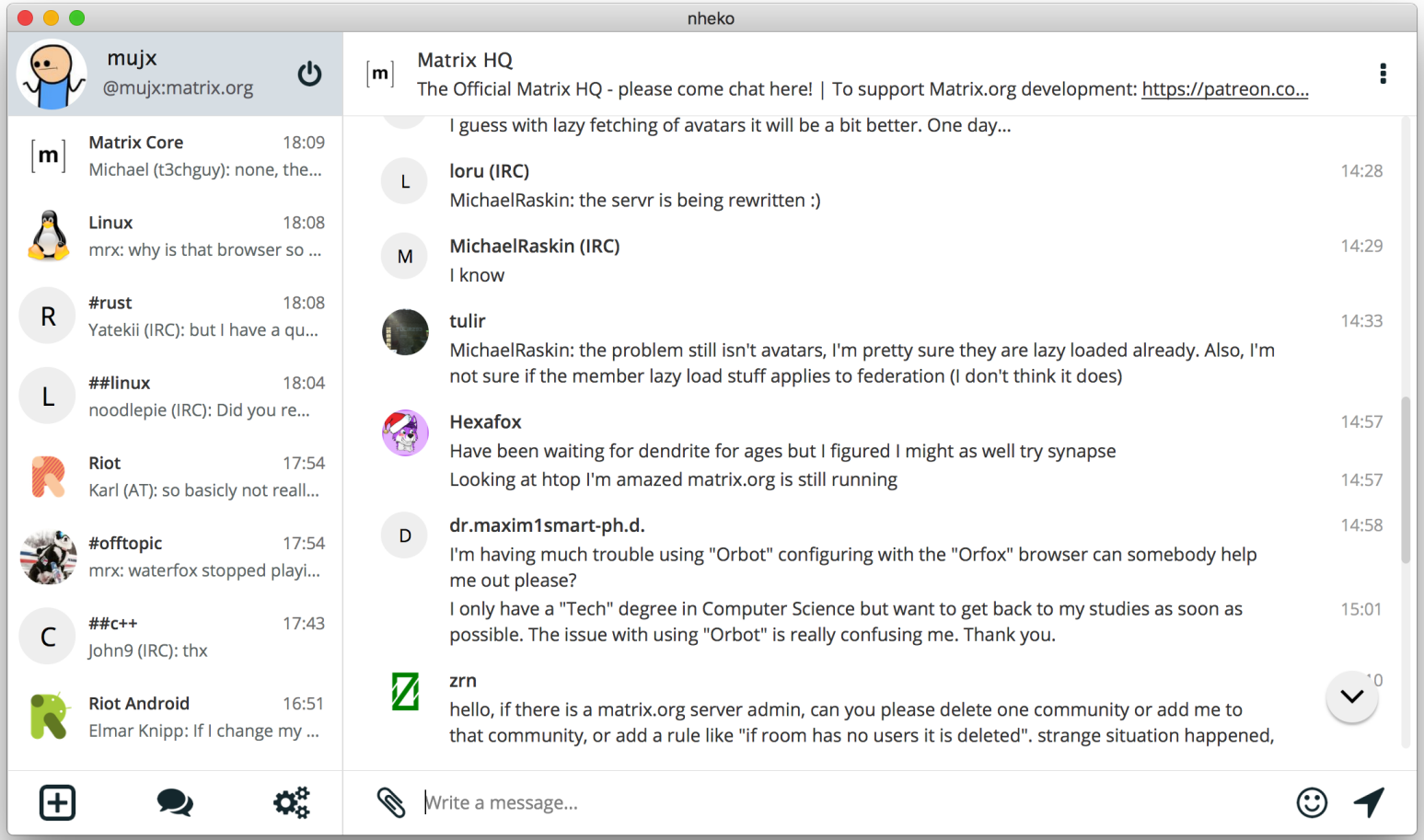
CLIENTS

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
- Seaglass (MacOS)
- Fractal (GTK)
- Gomuks (TUI)

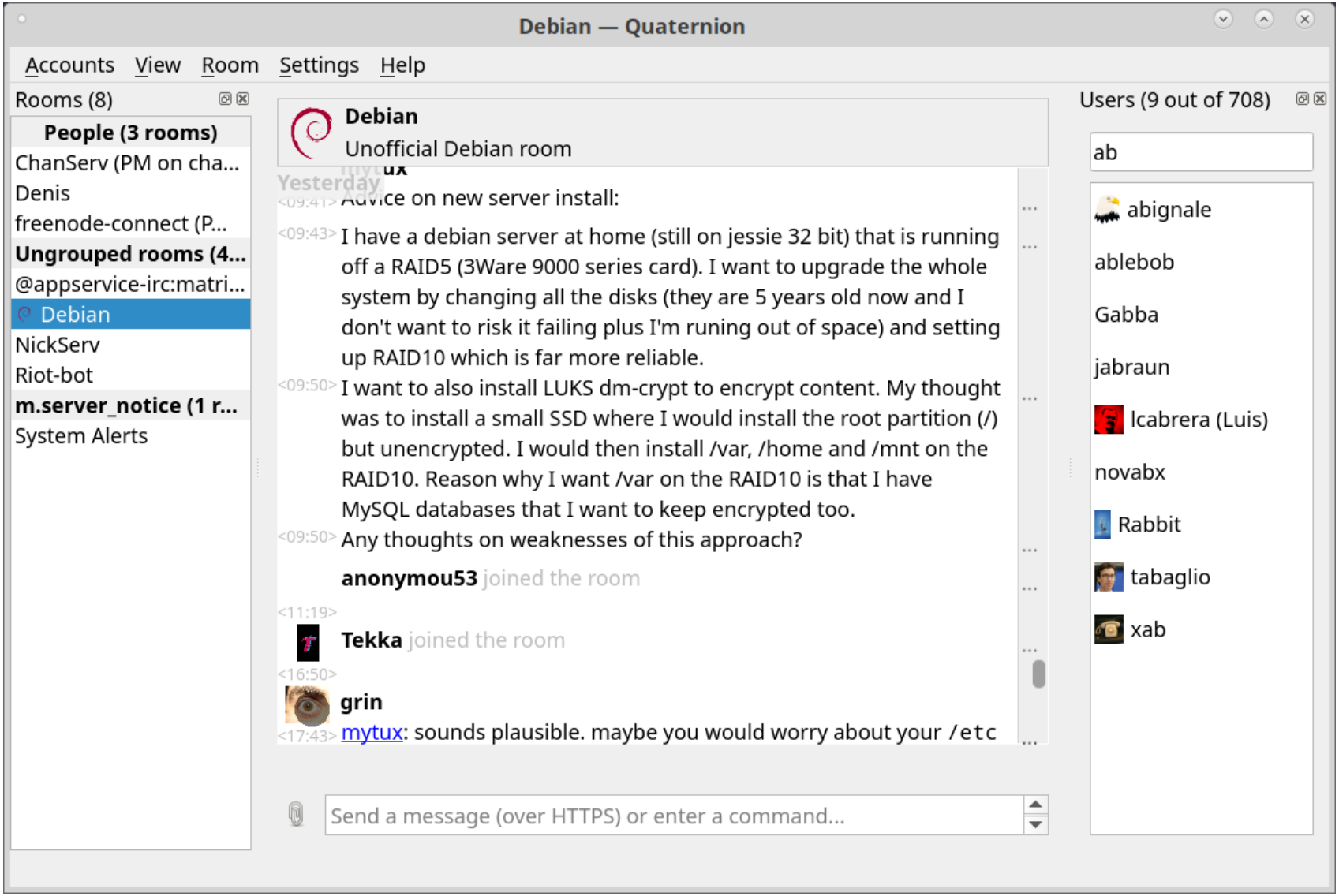
CLIENTS - RIOT



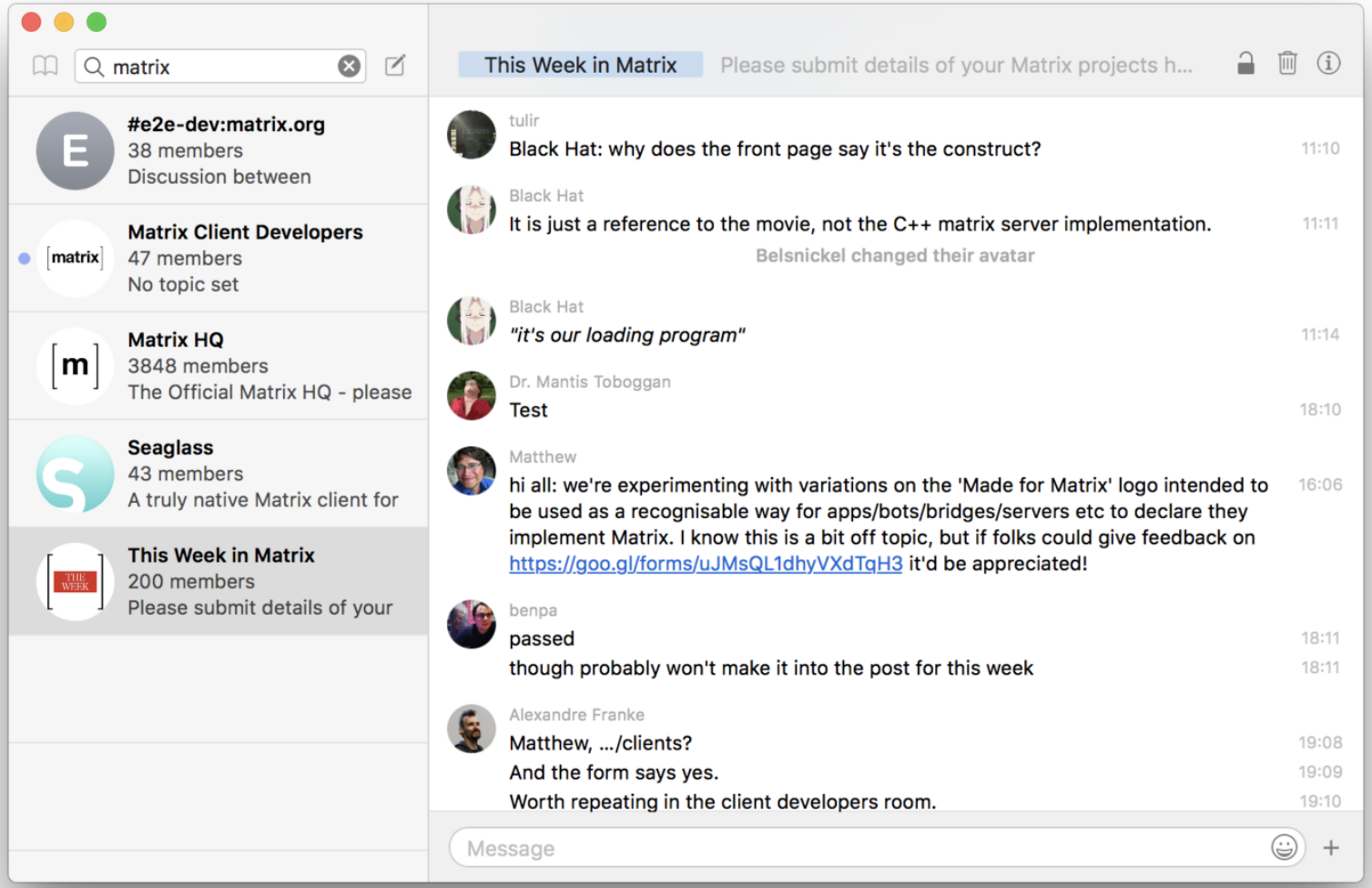
Clients - Nheko



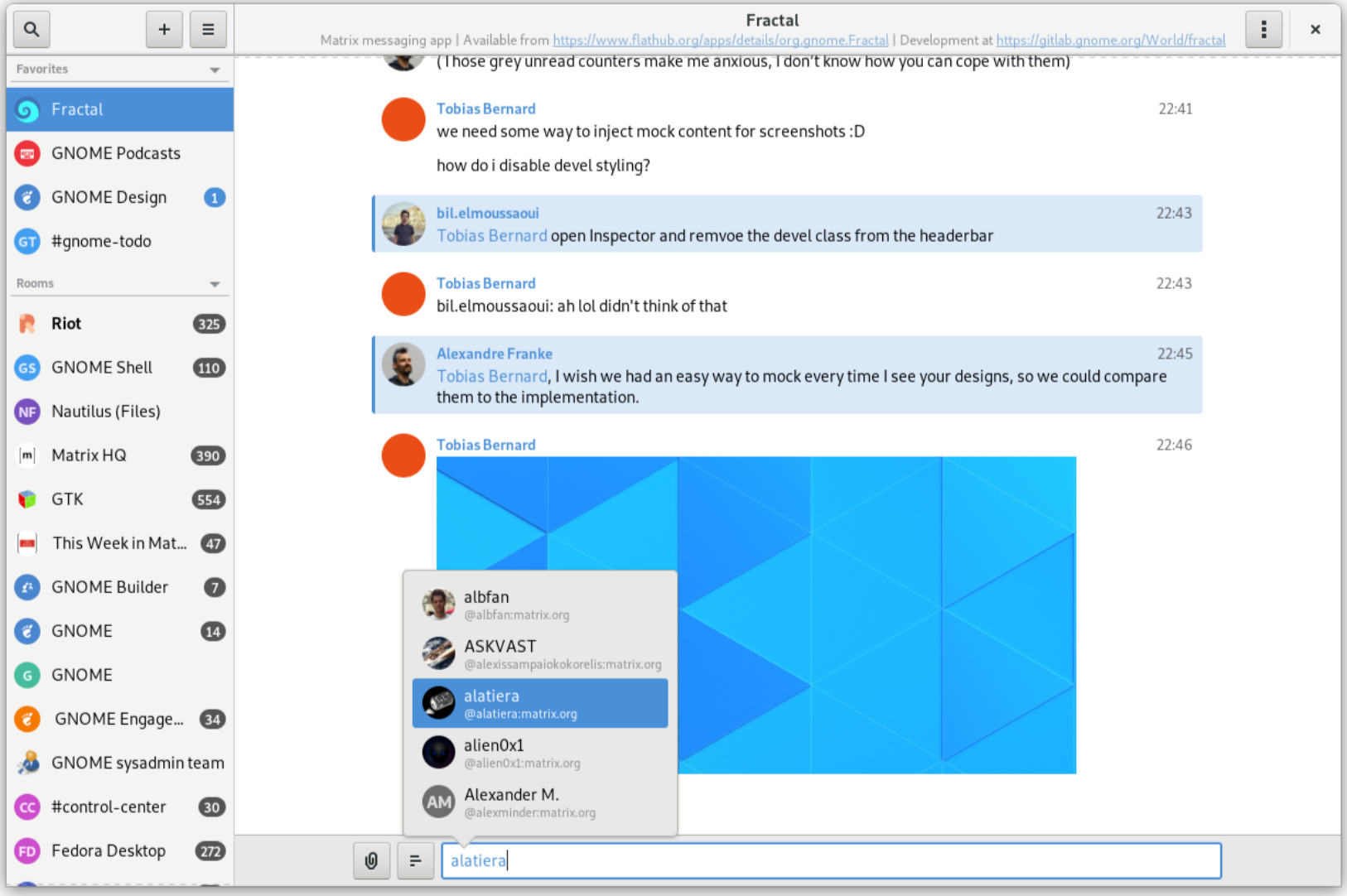
CLIENTS - QUATERNION



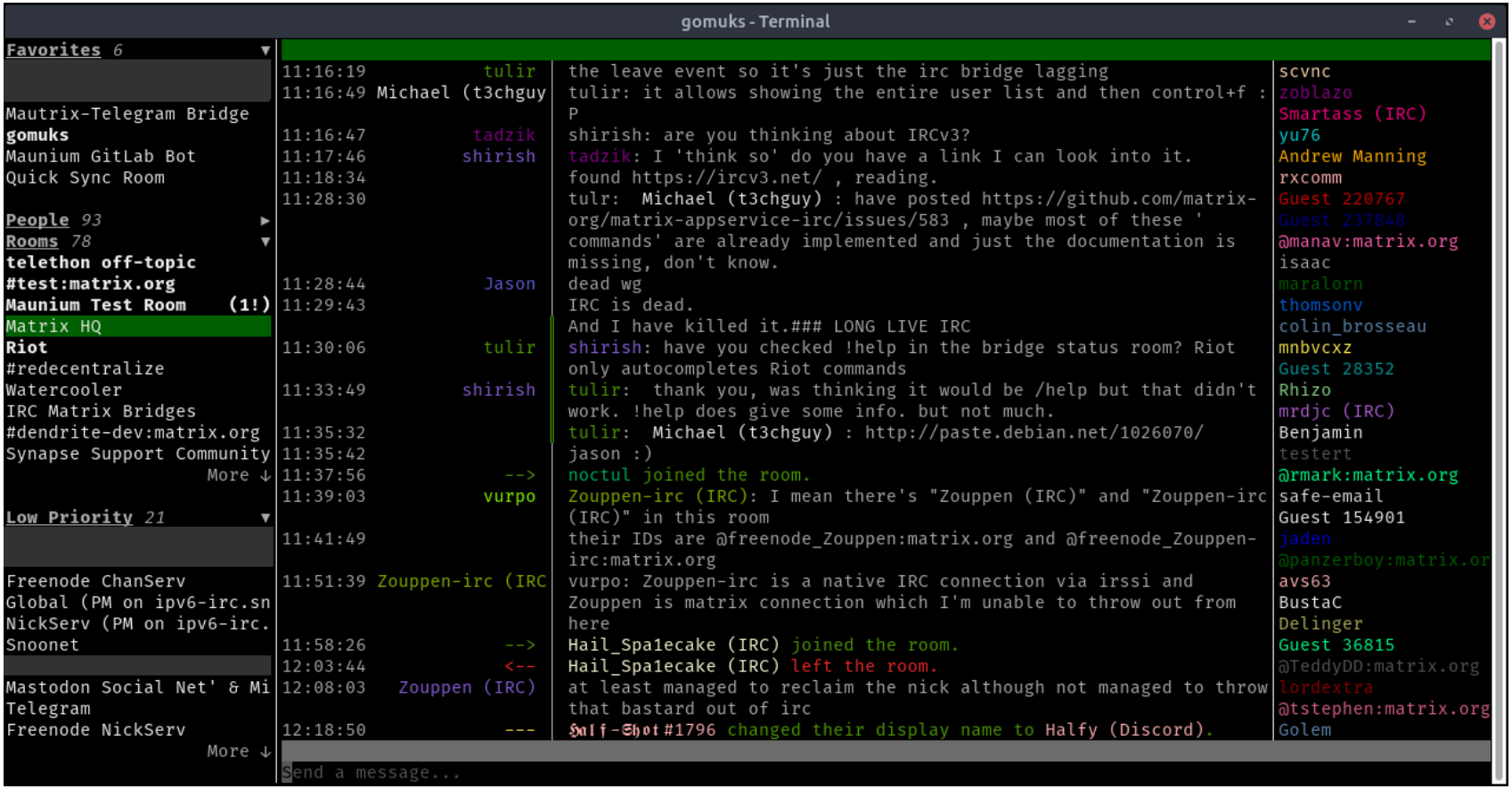
CLIENTS - SEAGLASS



CLIENTS - FRACTAL

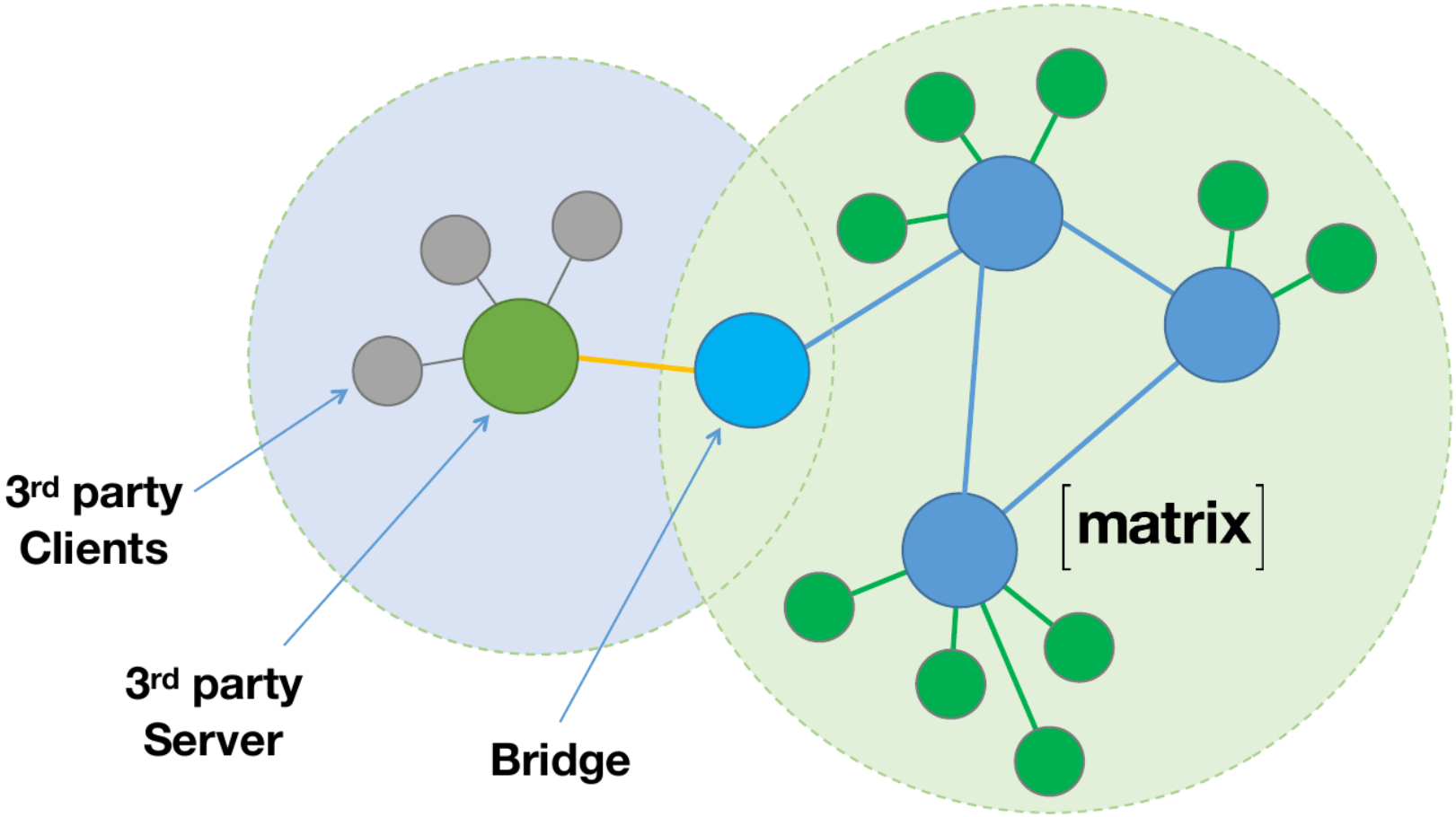


CLIENTS - GOMUKS

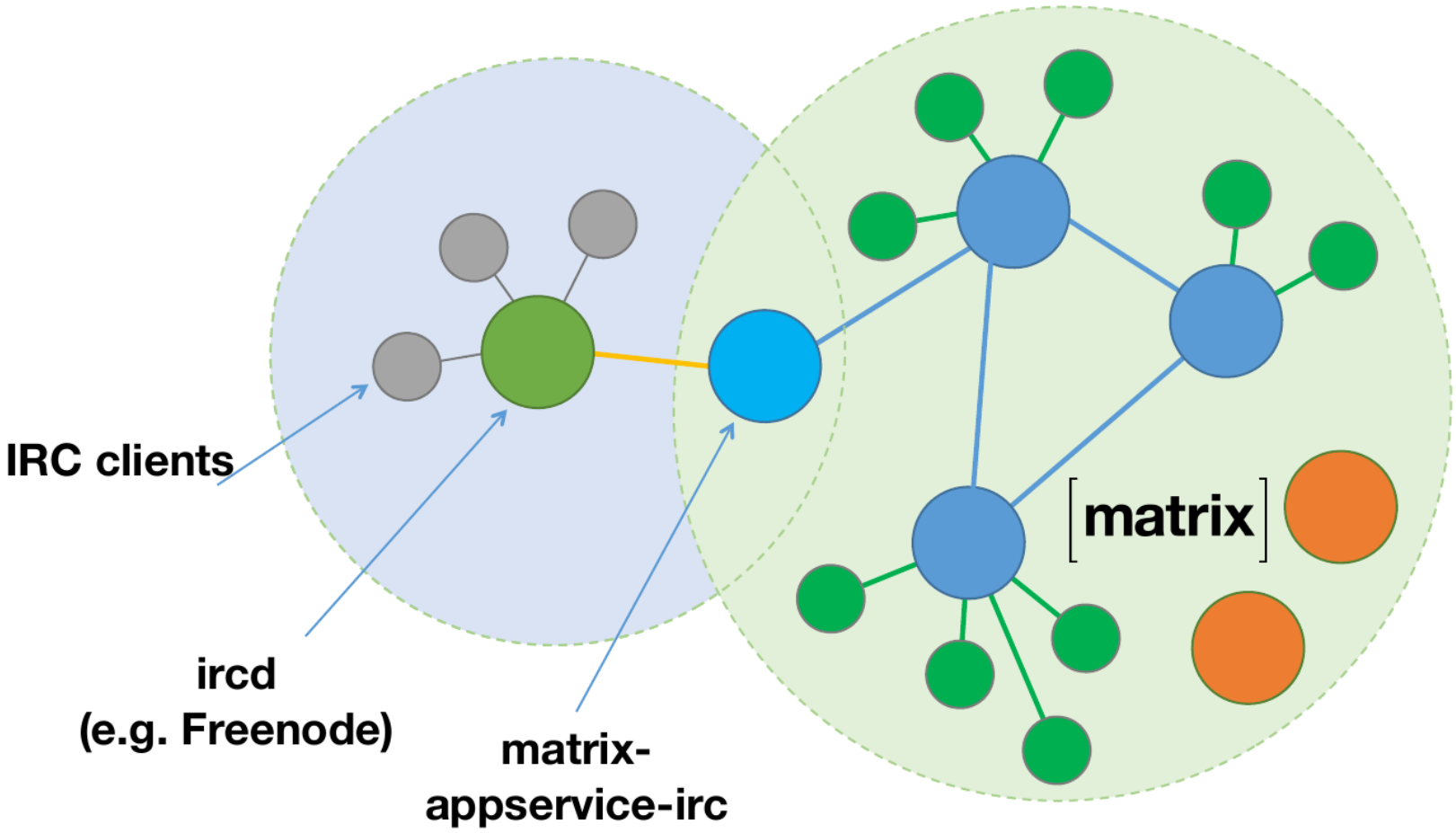


BRIDGES

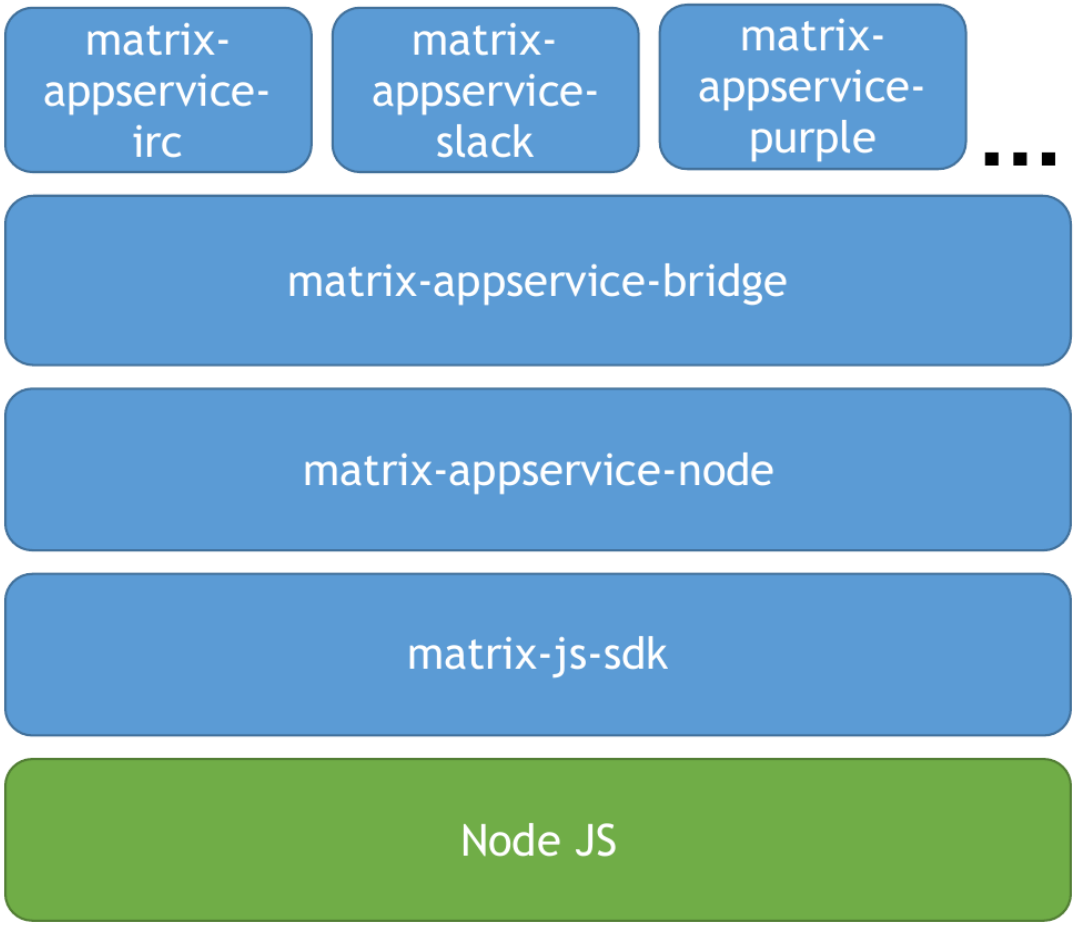
BRIDGES



Bridges



Bridges


matrix-appservice-irc
matrix-appservice-slack
matrix-appservice-purple
...
matrix-appservice-bridge
matrix-appservice-node
matrix-js-sdk
Node JS

Integrations

Integrations

- Etherpad

Integrations

- Etherpad
- RSS

INTEGRATIONS

- Etherpad
- RSS
- Grafana

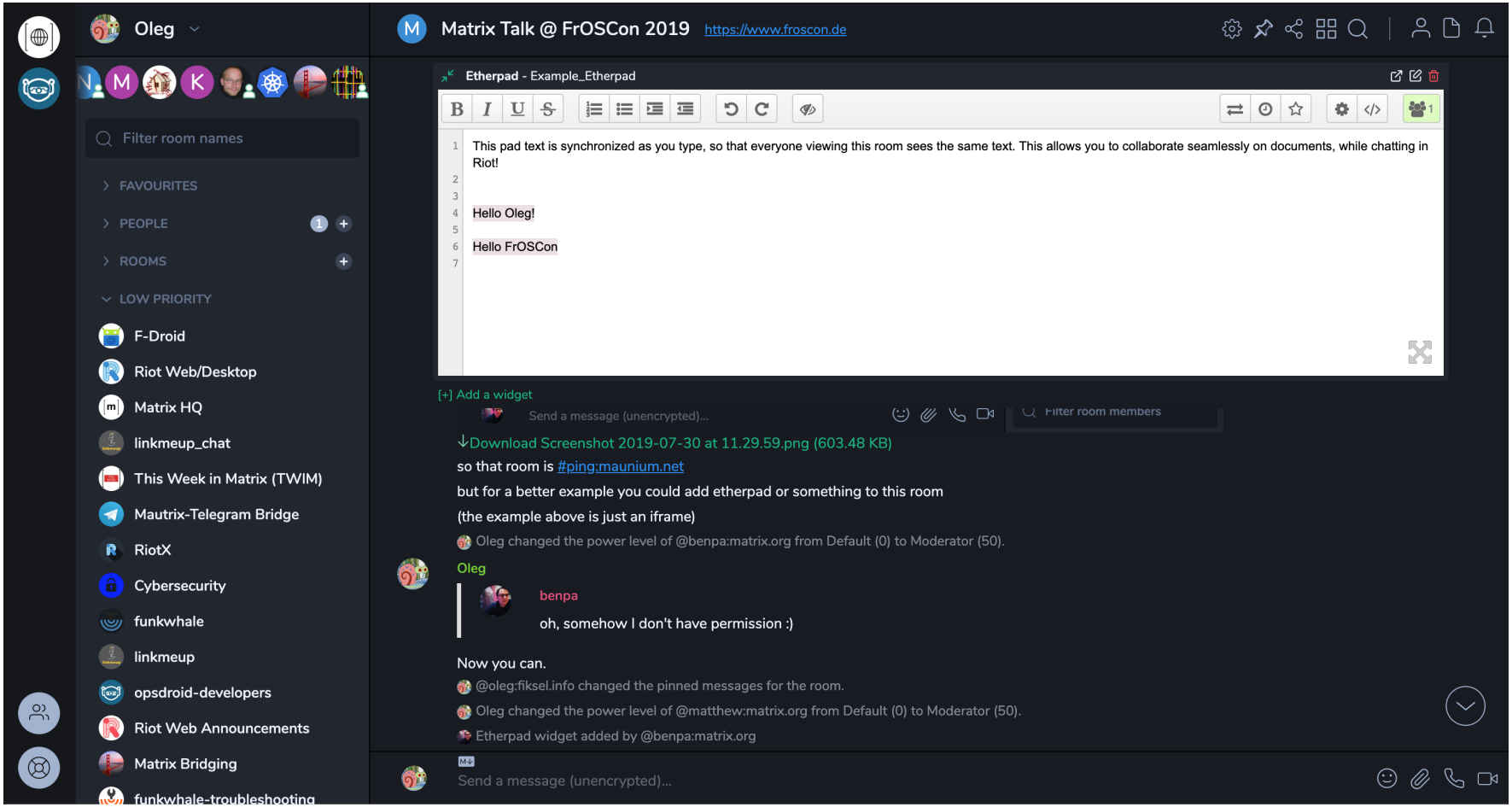
Integrations

- Etherpad
- RSS
- Grafana
- Jitsi

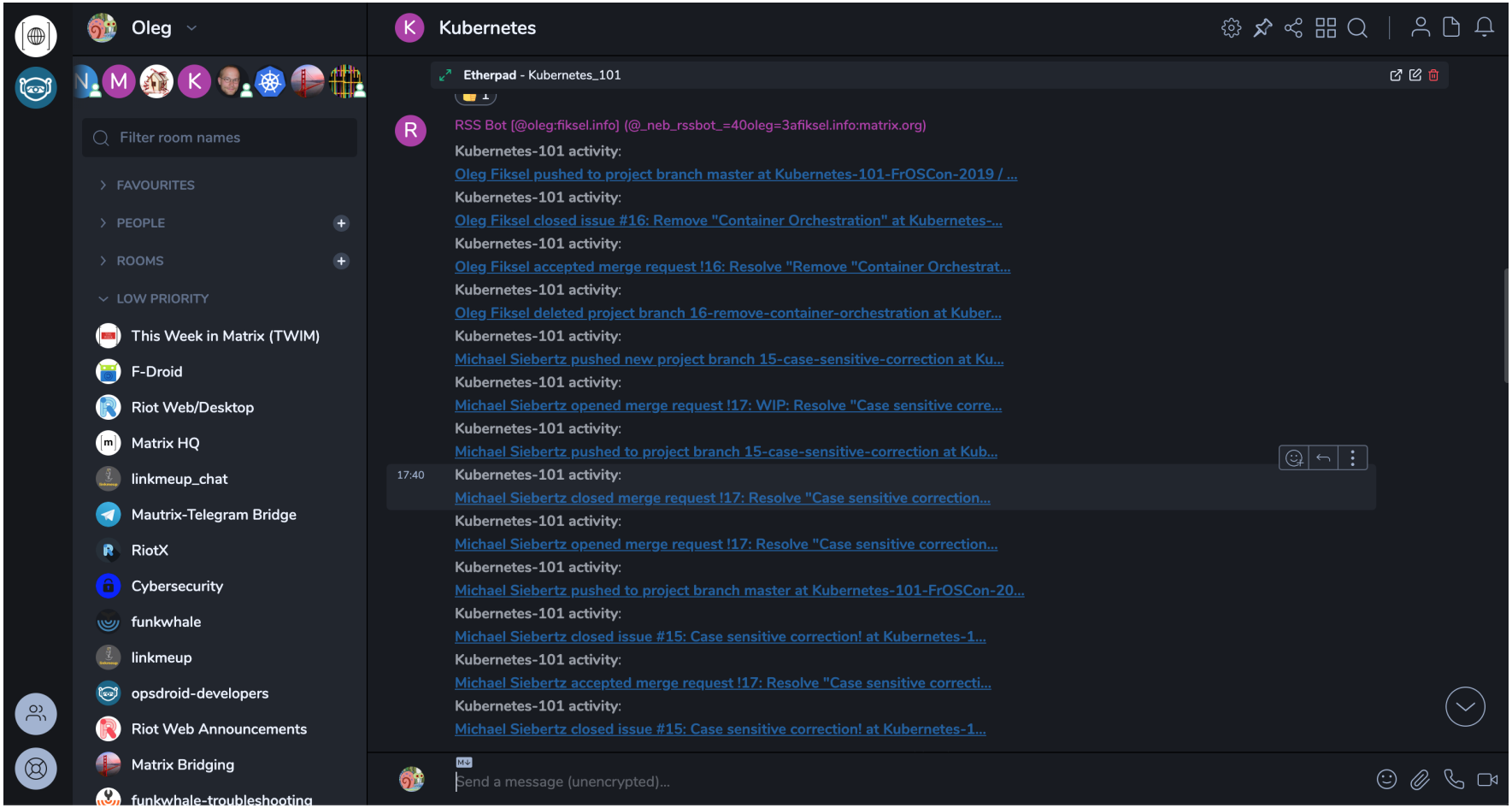
Integrations

- Etherpad
- RSS
- Grafana
- Jitsi
- Custom

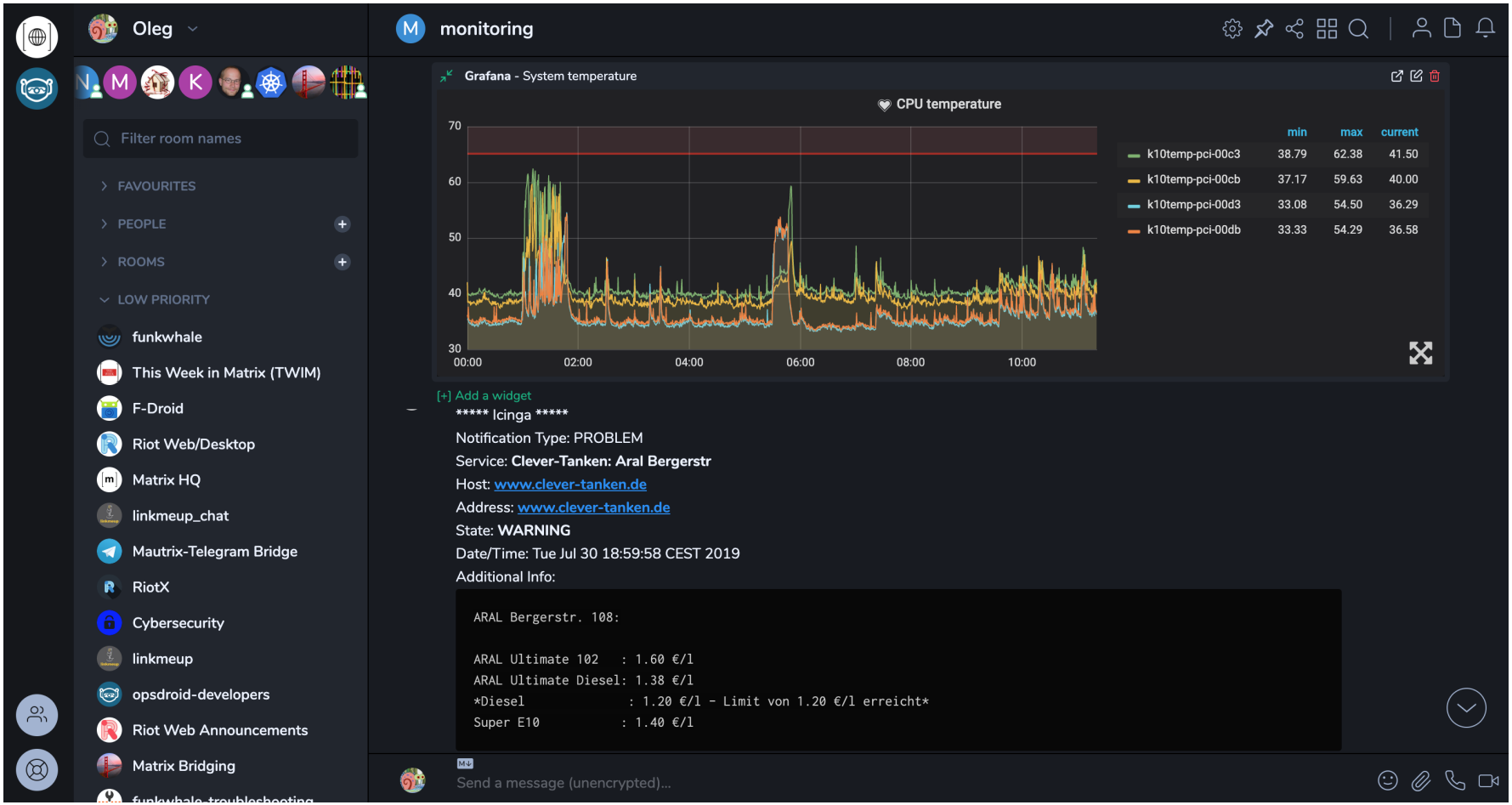
Integrations - Etherpad



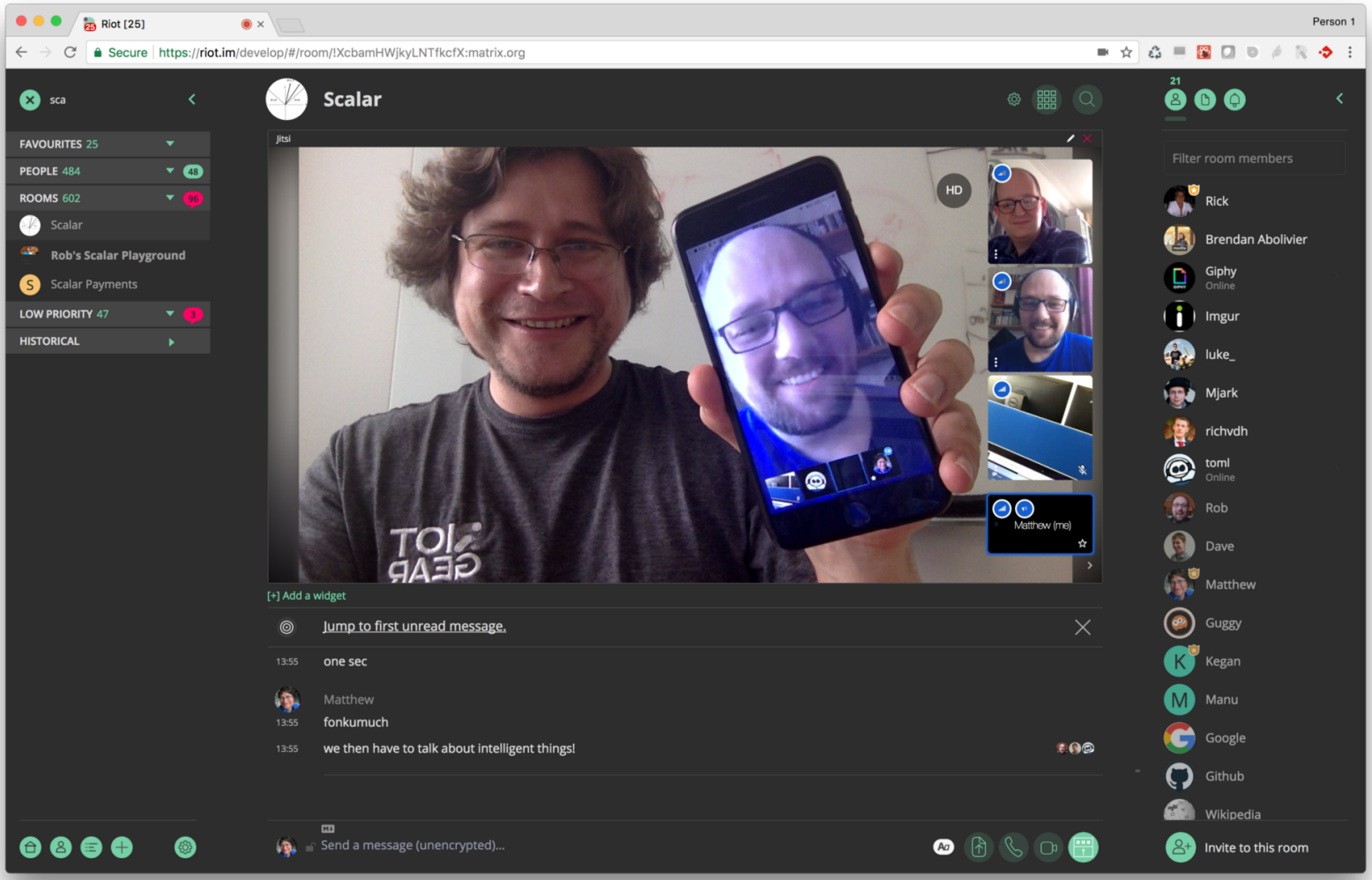
INTEGRATIONS - RSS



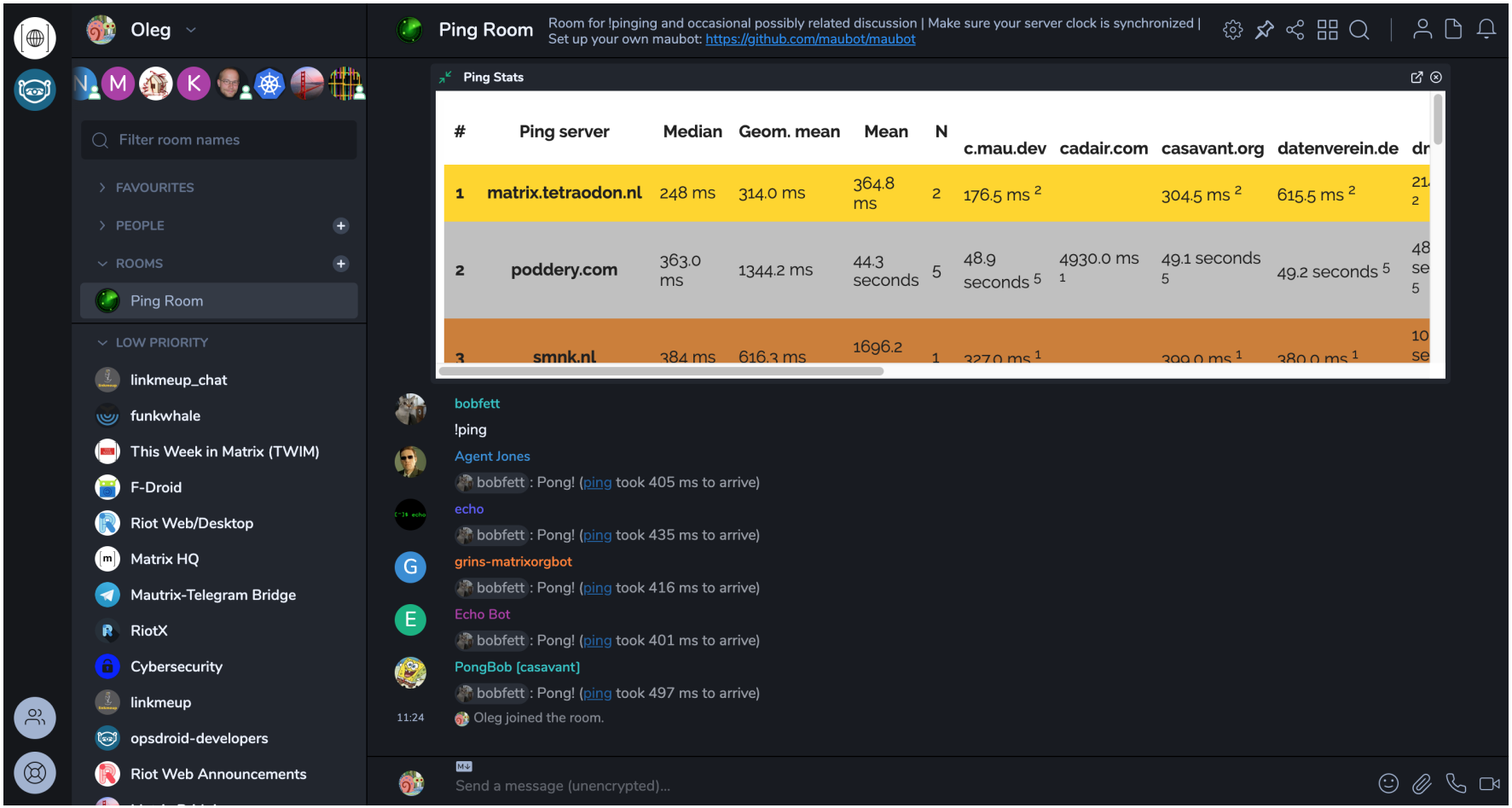
INTEGRATIONS - GRAFANA



Integrations - Jitsi



INTEGRATIONS - CUSTOM



Client-Server API

```
curl -XPOST -d '{"msgtype":"m.text", "body":"Wake up Neo..."}' "
    https://matrix.org/_matrix/client/r0/rooms/#matrix:matrix.
    org/send/m.room.message?access_token=ACCESS_TOKEN"
{
  "event_id": "YUwRidLecu"
}
```

Server-Server API

SERVER-SERVER API

- Synchronises messages and room state between servers, in real-time

SERVER-SERVER API

- Synchronises messages and room state between servers, in real-time
- Can retrieve historic messages from each other

SERVER-SERVER API

- Synchronises messages and room state between servers, in real-time
- Can retrieve historic messages from each other
- Query profile and presence information about users on each other's servers

Application Services API

Application Services API

- Have privileged access to the server

APPLICATION SERVICES API

- Have privileged access to the server
- Can subscribe to server traffic to provide custom application logic

APPLICATION SERVICES API

- Have privileged access to the server
- Can subscribe to server traffic to provide custom application logic
- Can masquerade as 'virtual users'

Latest features & Roadmap

Latest features

MATRIX 1.0 RELEASE

MATRIX 1.0 RELEASE

- First stable release of the protocol standard

MATRIX 1.0 RELEASE

- First stable release of the protocol standard
- Official SSL certificates for S2S needed

MATRIX 1.0 RELEASE

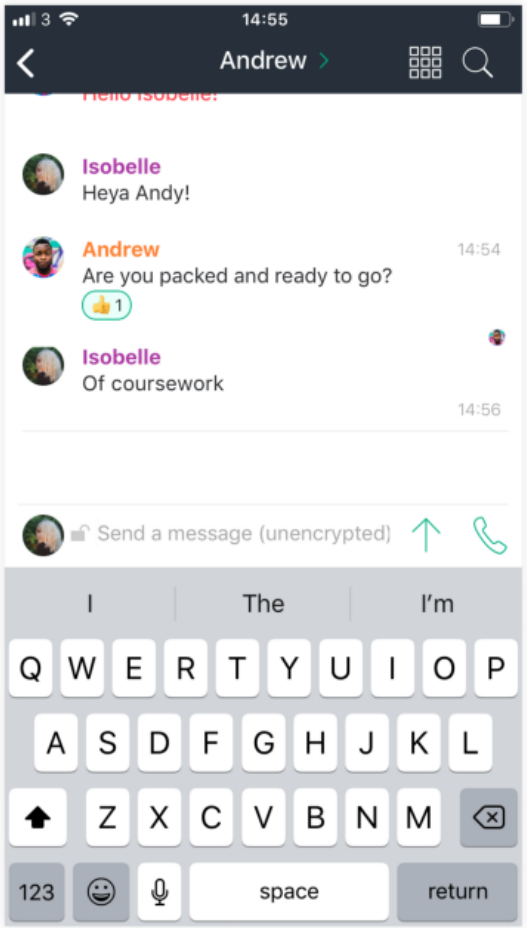
- First stable release of the protocol standard
- Official SSL certificates for S2S needed
- Using .well-known URIs to discover servers

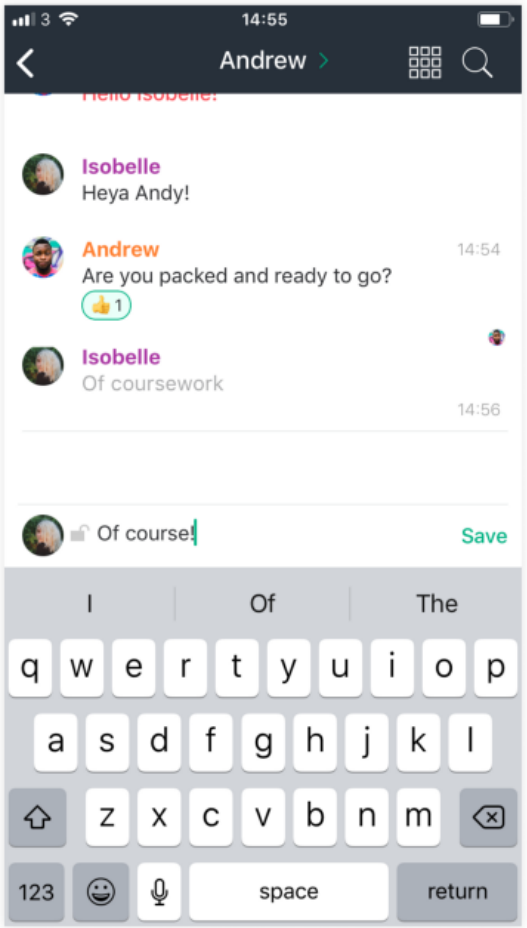
MATRIX 1.0 RELEASE

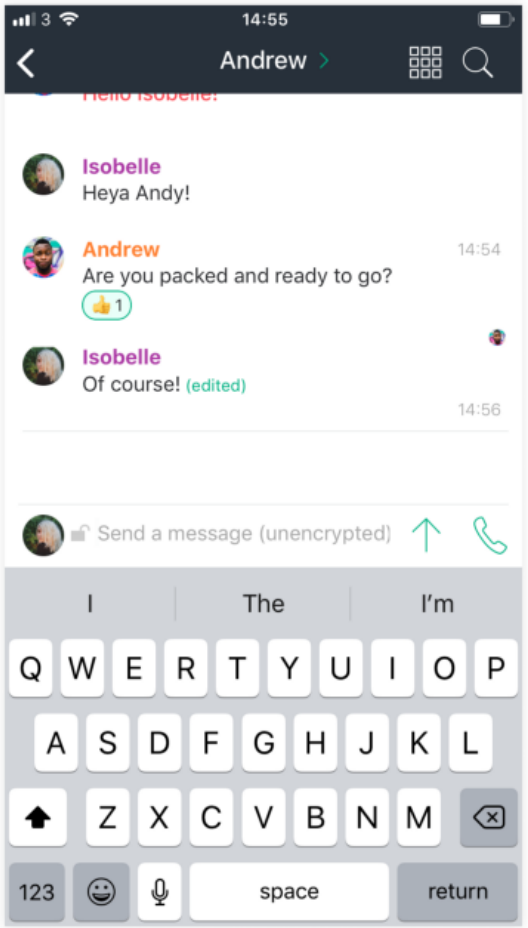
- First stable release of the protocol standard
- Official SSL certificates for S2S needed
- Using .well-known URIs to discover servers
- Switching to room version 4 for new rooms (fixes the Hotel California bug)

EDITS & REACTIONS

EDITS & REACTIONS

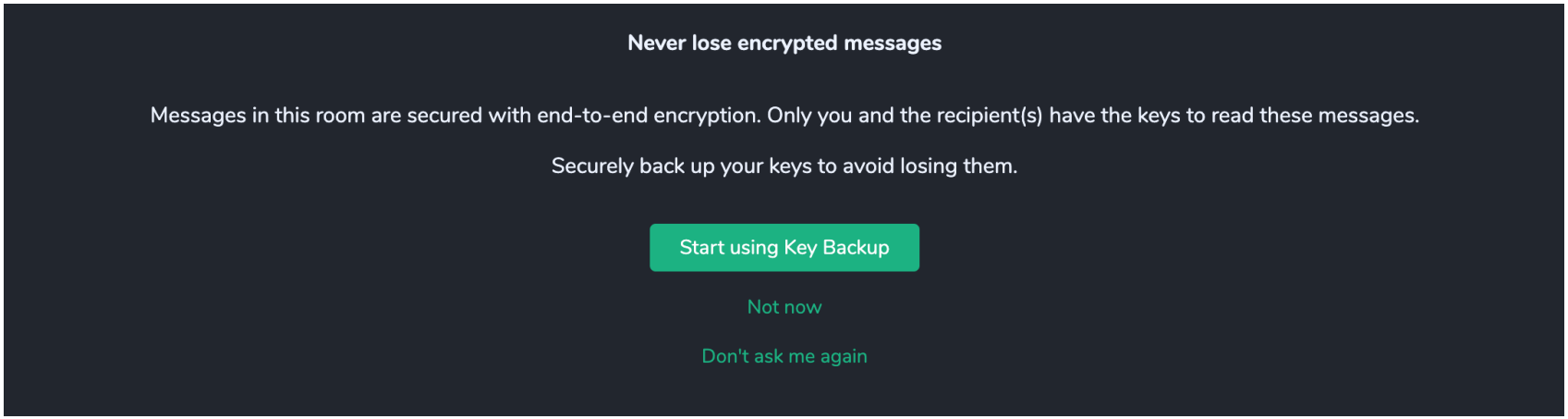




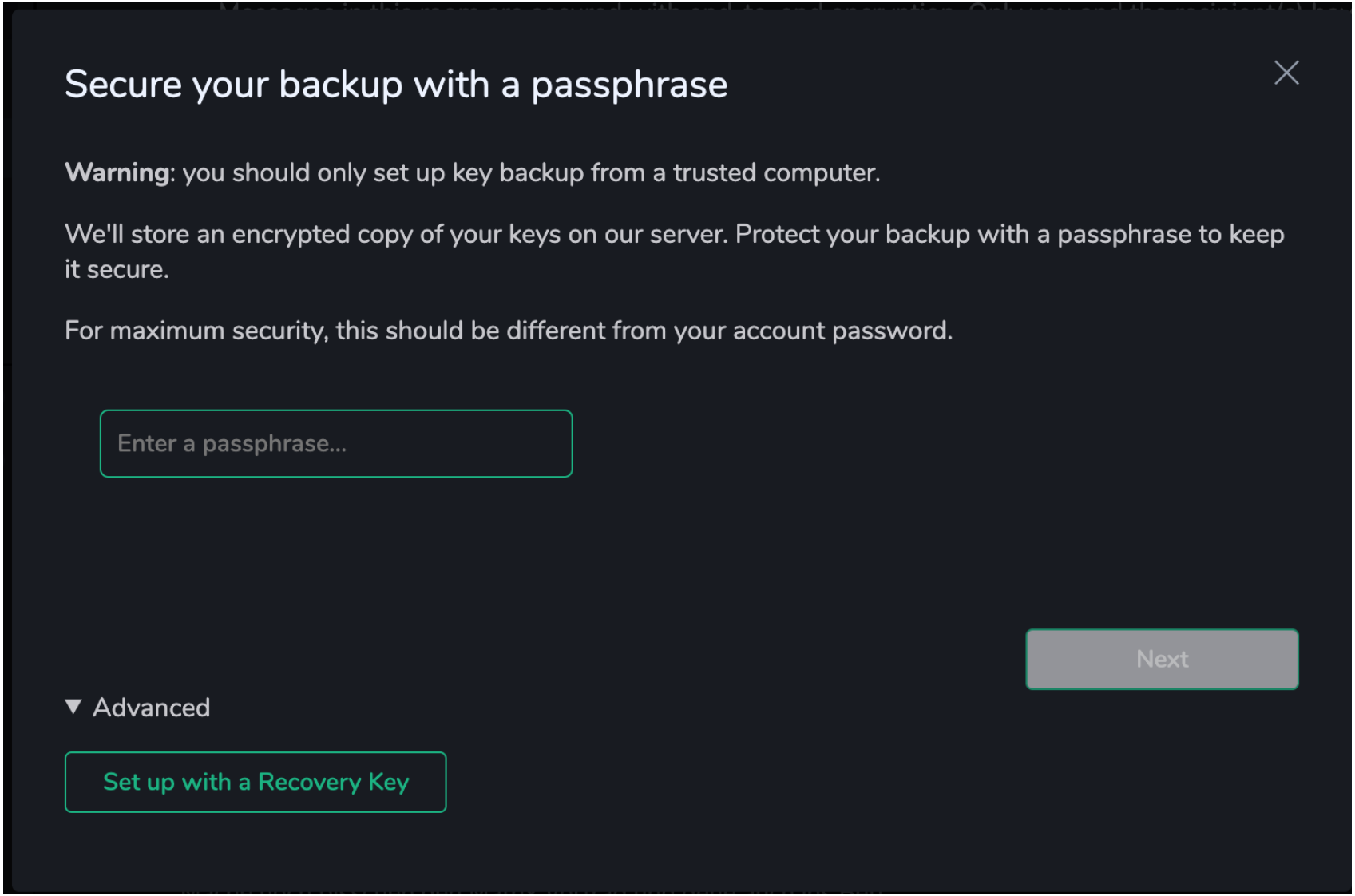


NEW KEY BACKUP (1/5)

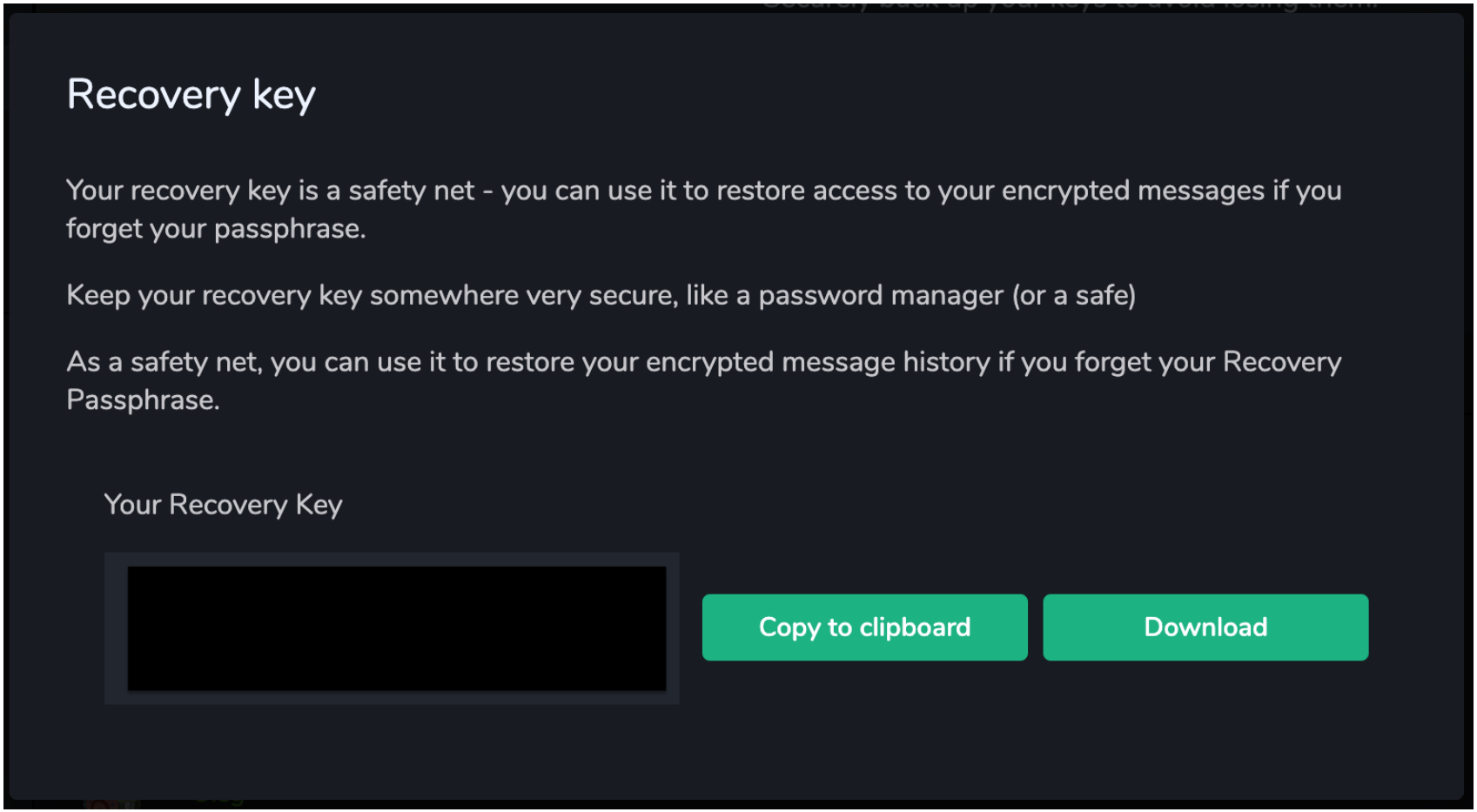
New key backup (1/5)



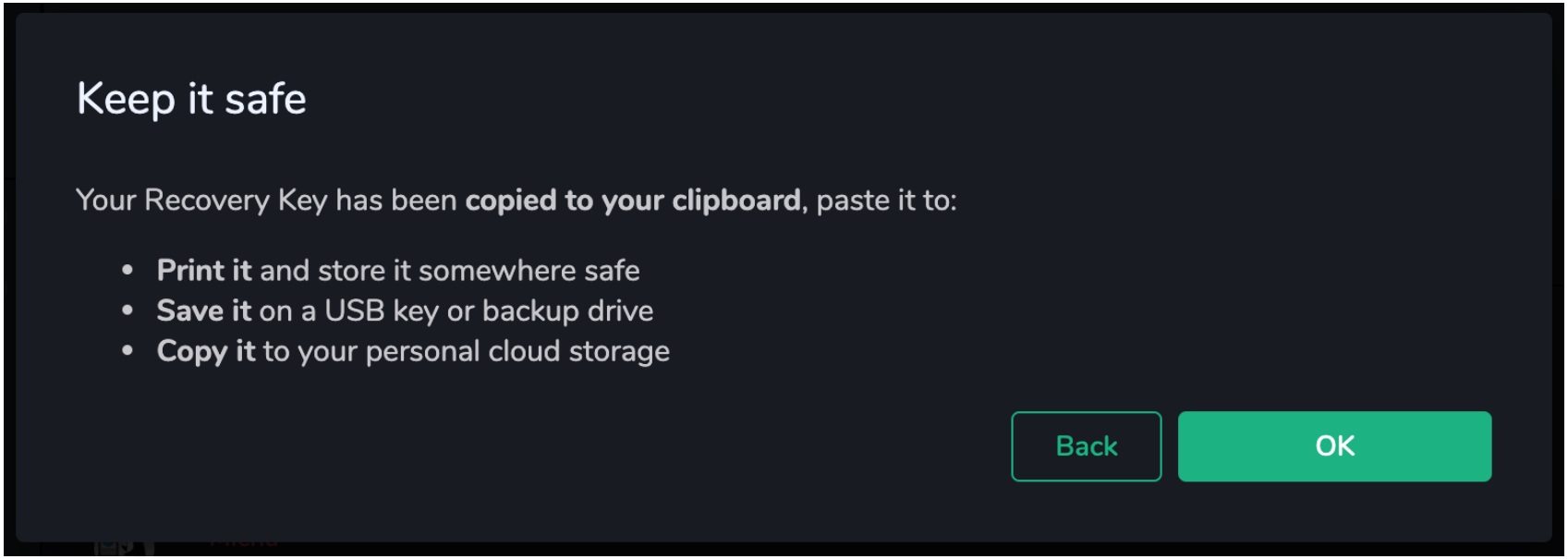
NEW KEY BACKUP (2/5)



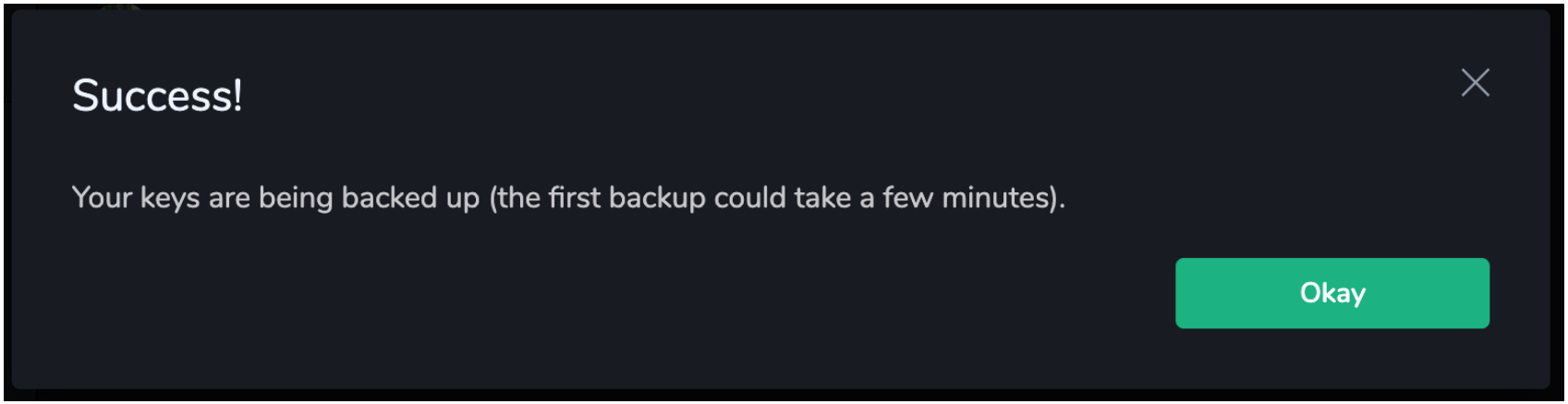
NEW KEY BACKUP (3/5)



NEW KEY BACKUP (4/5)



NEW KEY BACKUP (5/5)



Roadmap

Roadmap

ROADMAP

- Better Synapse scalability (Workers, UID Loadbalancing)

ROADMAP

- Better Synapse scalability (Workers, UID Loadbalancing)
- Improve Synapse's minimal footprint
  To run on smaller hardware.

ROADMAP

- Better Synapse scalability (Workers, UID Loadbalancing)
- Improve Synapse's minimal footprint
  To run on smaller hardware.
- New device trust (cross signing devices)
  Key step to enable E2EE by default.

Summary

SUMMARY

- The number of messaging platforms is growing every day

Summary

- The number of messaging platforms is growing every day
- Matrix solves the problem of uniting those platforms in a way **YOU** want it

SUMMARY

- The number of messaging platforms is growing every day
- Matrix solves the problem of uniting those platforms in a way **YOU** want it
- Matrix community is rapidly evolving

SUMMARY

- The number of messaging platforms is growing every day
- Matrix solves the problem of uniting those platforms in a way **YOU** want it
- Matrix community is rapidly evolving
- The community is great! Get involved!

GENTLEMEN, START YOUR ~~ENGINES~~ LAPTOPS

GENTLEMEN, START YOUR ~~ENGINES~~ LAPTOPS

- Browse to (use Chrome or Firefox): https://riot.froscon2019.fiksel.info

GENTLEMEN, START YOUR ~~ENGINES~~ LAPTOPS

- Browse to (use Chrome or Firefox): https://riot.froscon2019.fiksel.info
- Create an account

GENTLEMEN, START YOUR ~~ENGINES~~ LAPTOPS

- Browse to (use Chrome or Firefox): https://riot.froscon2019.fiksel.info
- Create an account
- Join the channel #FrOSCon2019:froscon2019.fiksel.info

GENTLEMEN, START YOUR ~~ENGINES~~ LAPTOPS

- Browse to (use Chrome or Firefox): https://riot.froscon2019.fiksel.info
- Create an account
- Join the channel #FrOSCon2019:froscon2019.fiksel.info
- Have fun!

Thanks!

Oleg Fiksel

Email: oleg@fiksel.info

Matrix: @oleg:fiksel.info

Links

- Matrix 1.0 release notes
- Message Editing & Reactions
- Deploy Matrix stack with Ansible
- Proposals for device trust