

[matrix]

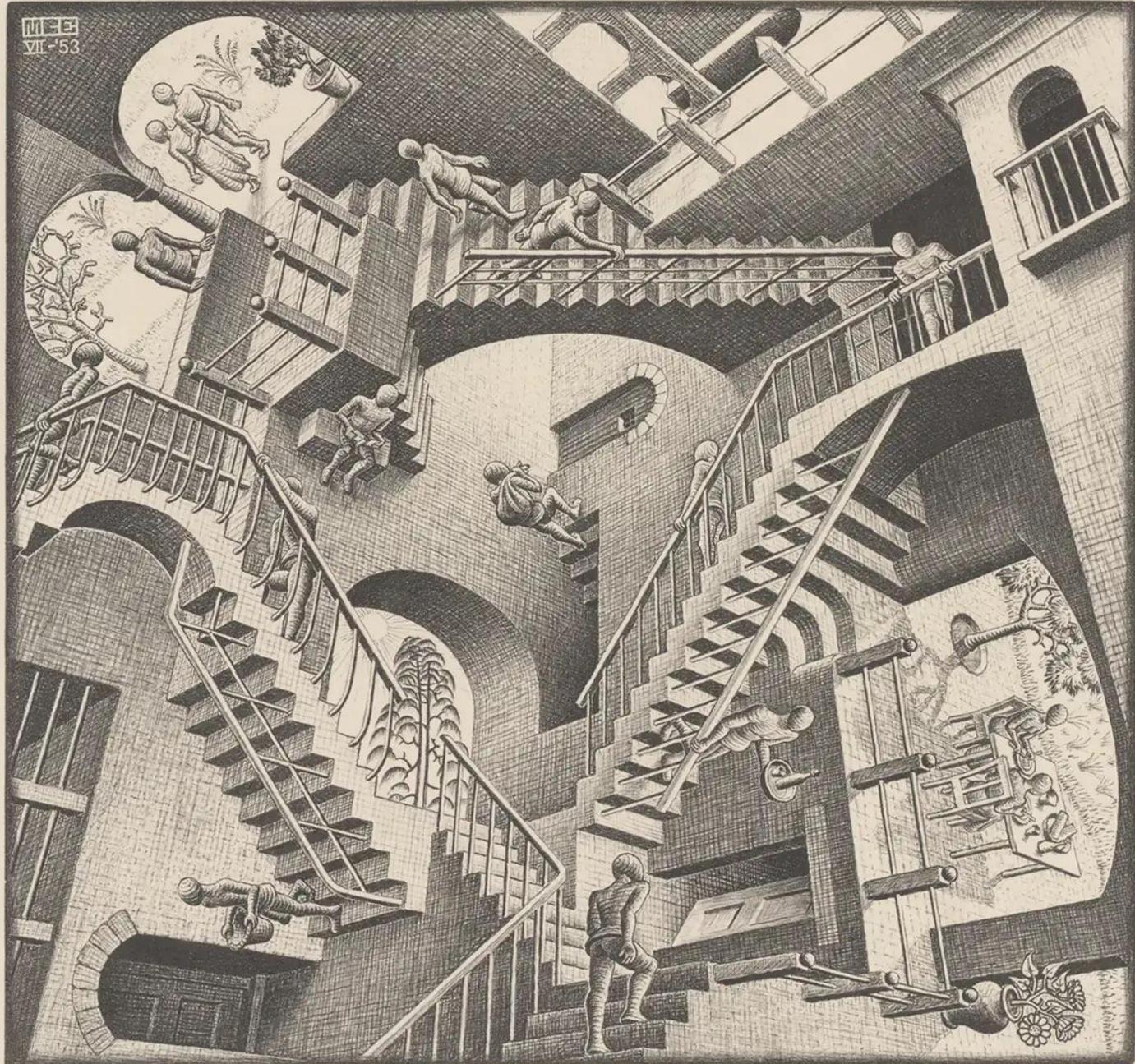
The Road to Mainstream Matrix

FOSDEM 2025

matthew@matrix.org

@matthew:matrix.org

VI-53



M. G. Lewis

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



Interoperable chat



Interoperable VoIP



Open comms for VR/AR



Real-time IoT data fabric

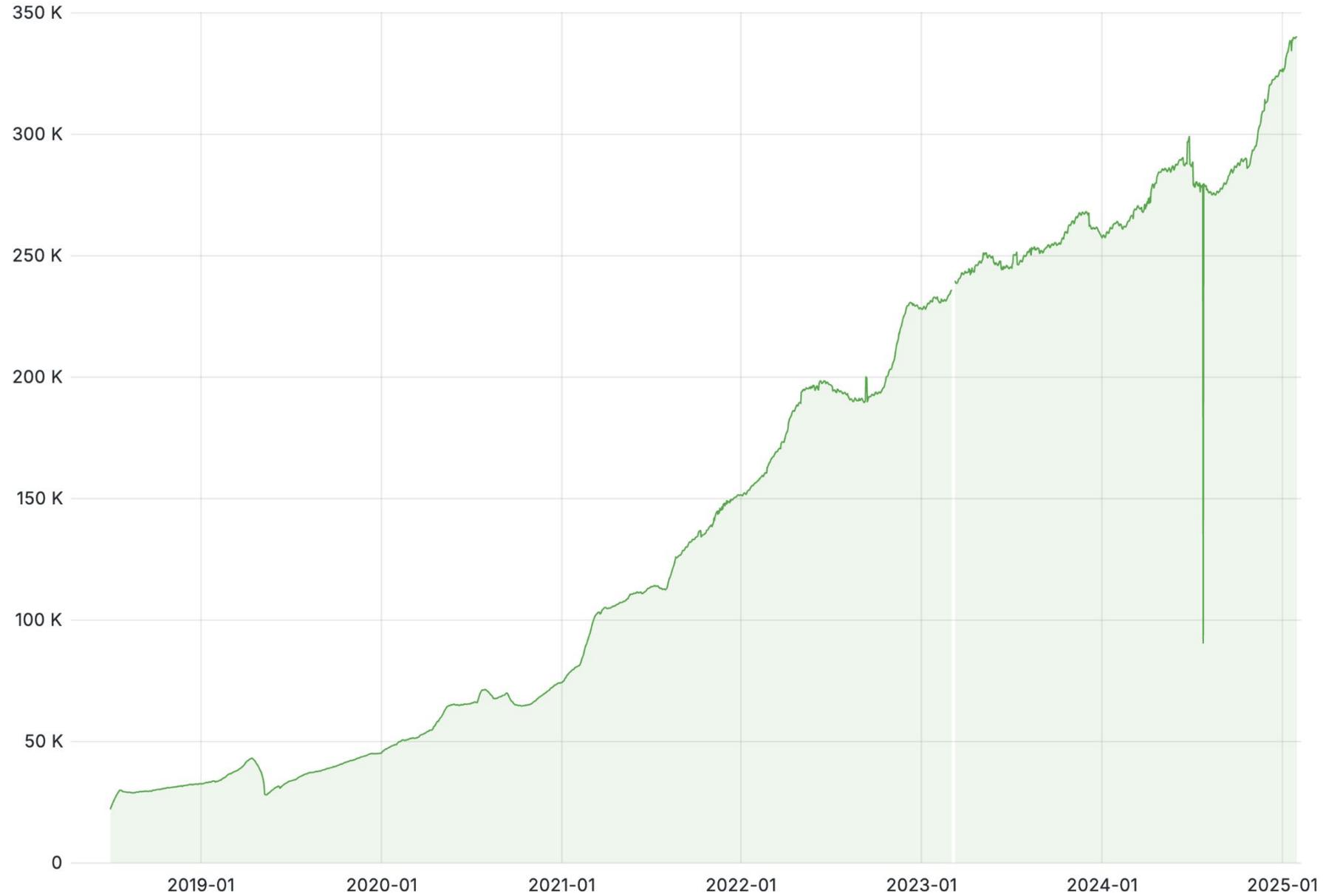
**Our mission:
To build the real-time
communication layer of the
open Web.**

**No single party owns your
conversations.**

**Conversations are shared
over all participants.**

30-day retained users across reporting servers

[matrix]



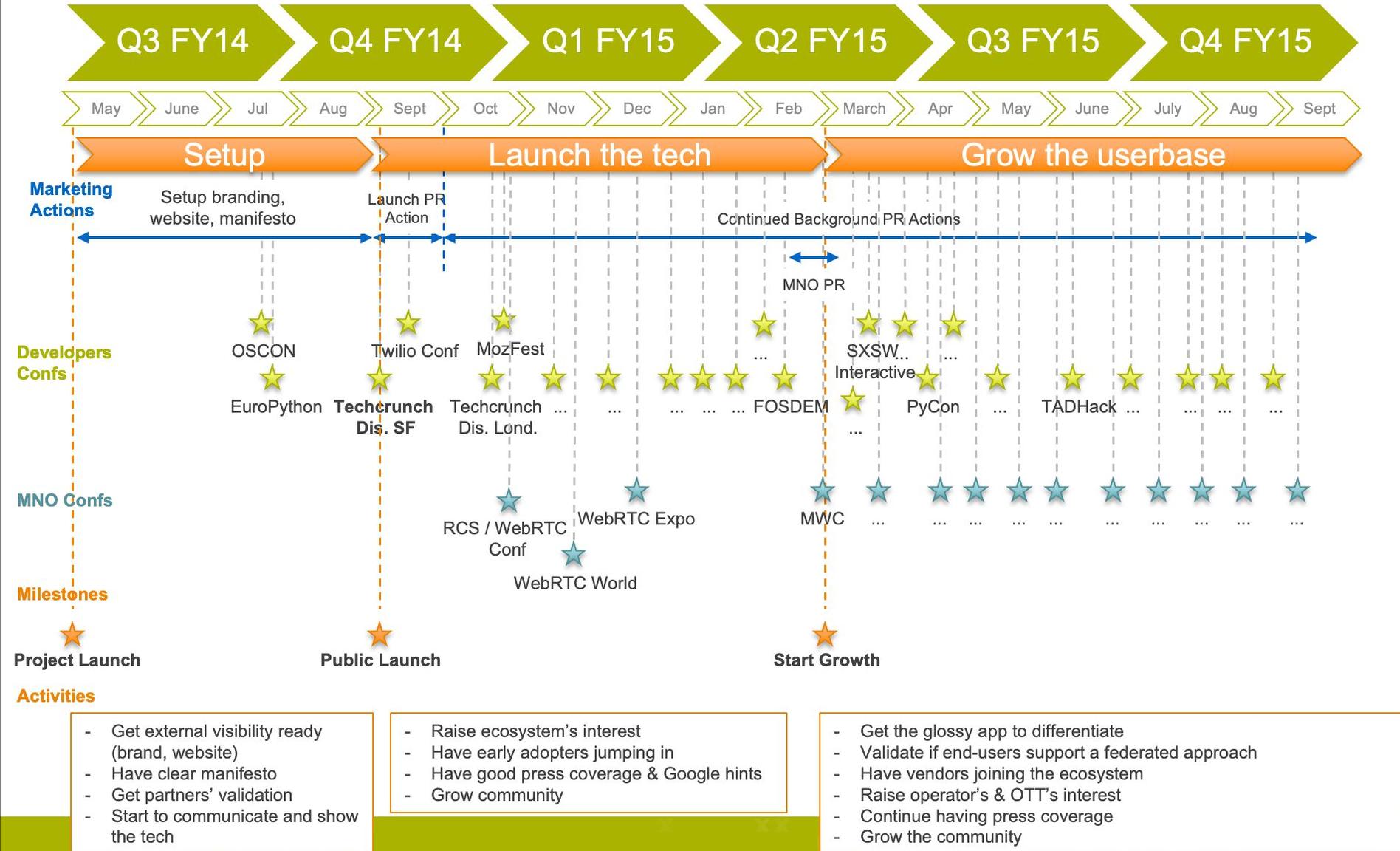
A dirt road winds through a dense forest. Sunlight filters through the trees, creating a warm, golden glow. The road is flanked by tall evergreen trees and undergrowth. The overall atmosphere is serene and natural.

**The Road to Mainstream Matrix
has both past and future.**

May 2014: The Dream

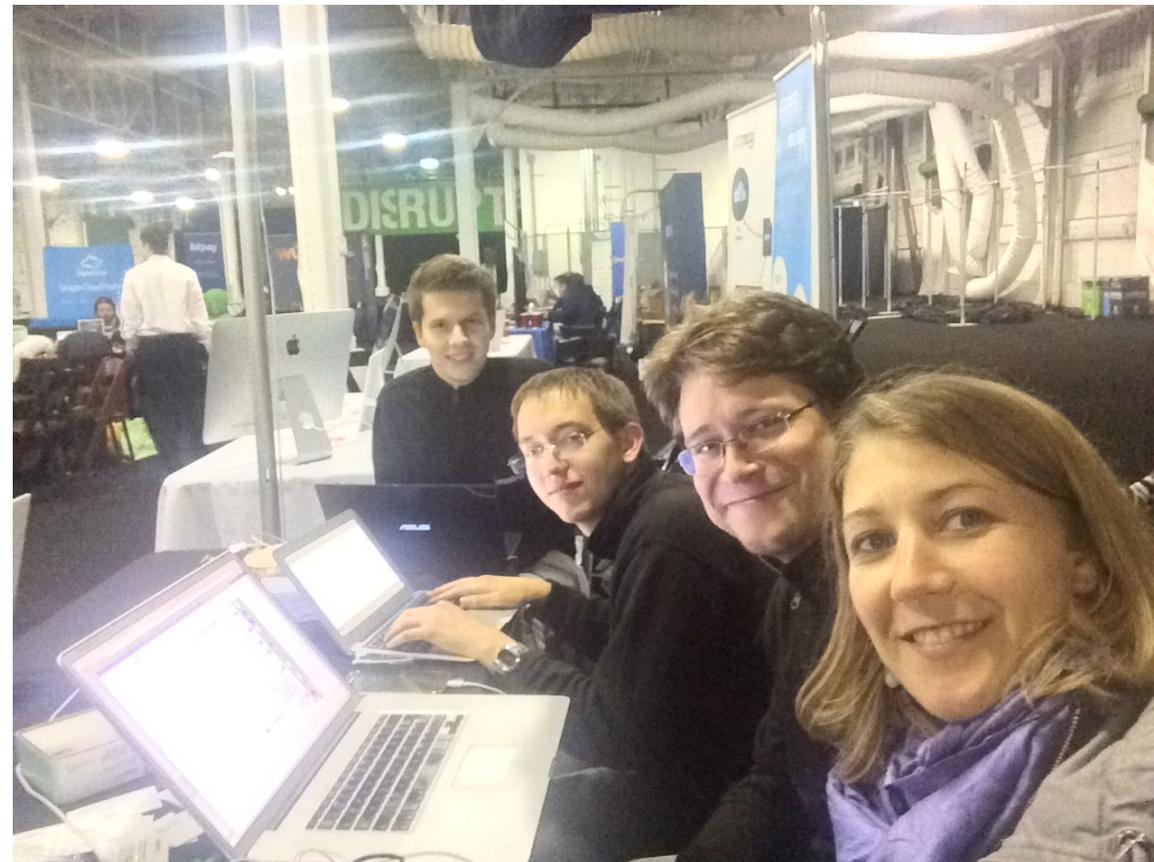
- Let's build the missing communication layer of the Web!
- Existing team of ~10 folks
- Build an implementation first.
- Use it to prove and figure out the protocol.
- *Then you spec* by updating the One True Spec.
- ⇒ Keep anchored in reality: killer app prioritised over protocol.

Project Synapse Timeline



Sept 2014: Liftoff!

- Launched at TC Disrupt!
- Shipped Synapse as a server
- “syweb” as an AngularJS webapp
- Chat, 1:1 VoIP, initial federation...
- Prove implementations; then spec.



localhost:8448/_matrix/client/#/room/#matrix:matrix.org

[matrix] @matthew:matrix.org Home Settings Log out

[matrix]

!!CYOakounNllvAxEs:matrix.org Sep 3 19:05
Call

#matrix:matrix.org Sep 3 19:03
@arathorn:arasphere.net: \

David Baker Aug 29 16:54
@matthew:matrix.org: gah, why doesn't this room have an alias

David Baker Aug 29 16:46
@matthew:matrix.org

!xolPEcMZCAEBTCESgL:matrix.org Aug 29 16:36
@matthew:matrix.org

!rSJOhPICLIHdwYYaCt:matrix.org Aug 29 16:36
@matthew:matrix.org

#donkey_channel:matrix.org Aug 29 15:46
@matthew:matrix.org

#test:matrix.org Aug 27 13:29
@jakdaw:matrix.org

Matthew Sep 3 01:03

SITUATION: THERE ARE 14 COMPETING STANDARDS.

HOW STANDARDS PROLIFERATE:
(SEE: ALC CHAIRS, GUNWATER ENDOWMS, INSTANT MESSAGING, ETC)

!H?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES. YEPH!

!SOON!

SITUATION: THERE ARE 15 COMPETING STANDARDS.

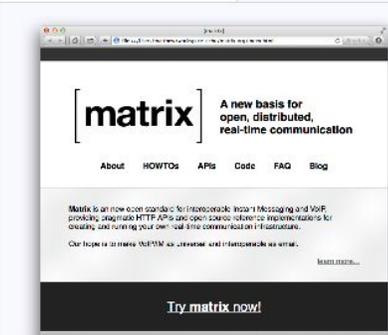
time for a screenshot for [http://matrix.org!](http://matrix.org)

beautiful. and very meta.

what we need next is a screenshot of the homepage in here... :->

that would be very silly

but quite tempting :D



Erik Johnston (@erikjkl.re) Sep 3 09:44
But your screenshot doesn't include the screenshot!

oddvar Sep 3 11:34
matrixception

#matrix:matrix.org

Matthew 5s ago

Erik Johnston (@erikjkl.re) 1m ago

@arathorn:arasphere.net 3m ago

LeoNerd (Leo Nerd:matrix.org) 53m ago

oddvar.org 1h ago

David Baker 3h ago

Kegan 3h ago

5h

@matthew:matrix.org Send Image

Invite a user: Invite Leave

[matrix]

TechCrunch
DISRUPT

SF
2014

TechCrunch
DISRUPT

SF
2014

Te

TechCrunch
DISRUPT

Animatrix

95

TechCrunch
DISRUPT

What does this tell you?

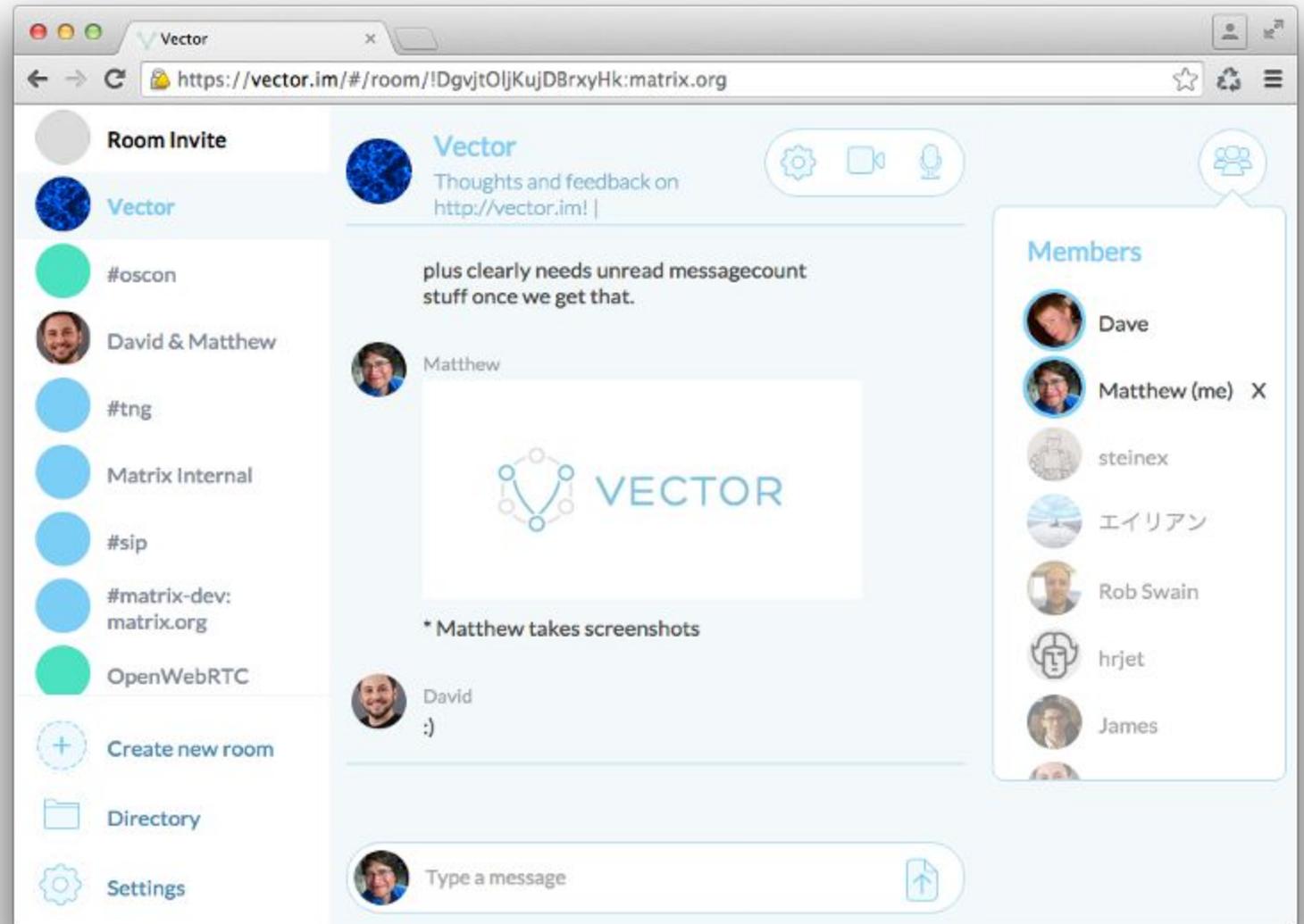
- We **really** want Matrix to be more than just chat.
- We **really** want Matrix to be mainstream, and not just for geeks and governments.
- We had more dev skillz than product skillz
- Matrix began as a centralised team (unlike a typical FOSS project)

May 2015: How will we fund this?

- Matrix needs a killer app that will go mainstream!
- Let's build glossy open source apps to drive Matrix uptake!
- Looked at 75 different products you can build on Matrix
 - Animatrix!
 - GovTech comms!
 - IOT backplanes!
 - Dating apps!
 - Live video mixing!
 - Virtual worlds!
- => **“Skype Done Right”** aka **“Open Hangouts”**
- How hard can it be?

May 2015: A Vector for Matrix!

- This then became **Vector**, launched at OSCON in July 2015...
- which became **Riot** in Sept 2016...
- ...and **Element** in Jul 2020.
- E2EE work starts at the same time - slowing down dev by ~10x 🤖



2015-2016: Premature success

- Around this point, Matrix started to get serious attention.
- Lots of pressure to improve the spec from independent implementers.
- Lots of time invested into spec governance.
- In retrospect, perhaps we should have ruthlessly prioritised polishing a killer app to drive mainstream adoption, over prematurely(?) focusing on the open ecosystem?
- Matrix could have been a decentralised communication app which was a trojan horse for a protocol - rather than setting expectations from the outset as The Missing Communication Layer Of The Web.
- This seems to be the bluesky attitude to atproto, which looks to be working out.

2017: A New Vector

- Team sets up Element to fund their Matrix work.
- Start setting up The Matrix.org Foundation as a non-profit to be the custodian of Matrix - ensure Matrix's independence from Element and other commercial Matrix vendors.
- Community steps up with donations to the Foundation - thank you!!
- Element raises \$M from Status - and then \$\$M later from financial VCs and other investors.
- Element spends ~70% of its funding on building out Matrix for everyone, transferring the IP to the Foundation.

2018-2021: Halcyon days

- Matrix grows and matures - finally declaring 1.0 in June 2020
- Loads of projects and companies grow on the protocol.
- FOSS communities like Mozilla, KDE, GNOME, FOSDEM go Matrix!
- Governments like France and Germany start rolling it out.
- Killer apps start to properly take shape: Element finally hires a design + Product team; Beeper forks and improves Element; etc.
- Lots of amazing experimental projects to grab attention/funding and demo Matrix's potential and inspire people to build on it:
 - P2P Matrix! Low bandwidth! Hydrogen! Dendrite! Gitter!
 - 3D calling! Matrix VR Demo! CRDTs! Element Drive! Applications Beyond Chat!
- But all this inspirational work stole energy from writing a killer app.

2022-2024: A series of unfortunate events

[matrix]

- Markets crash post-COVID.
- No more Zero Interest Rate Policy.
- No more investment.
- Element isn't yet profitable... and not in position to raise much more investment, having been routing all the \$ into Matrix.
- No other player is contributing \$ at the same level.
- But it'll be okay - Matrix is doing great!
- Really strong uptake in public sector continues: need for Digital Sovereignty. It's insane for your govt to be dependent on US-based SaaS.
- So to try to keep funding Matrix, Element increasingly focuses on Govt Matrix implementations in a bid to get profitable and sustainable.

Failure mode #1

- Government says:
 - “We want Matrix so we can have true digital sovereignty without sacrificing interoperability! Here’s a public tender for \$M to give us a Matrix deployment!”
- System Integrators (SIs) pitch for the tender.
- SI is well positioned to win thanks to providing the integration glue; local staff; financial qualifications; existing contracts; etc.
- Tender typically awarded to the cheapest proposal.
- To keep the price down, the System Integrator picks up an open source Matrix implementation and says they’ll support it themselves.
- ⇒ No money goes to the upstream project. 🦴
- Not a one-off: this happens repeatedly. 🦴 🦴 🦴

Failure mode #2

- Government says:
 - “Public Money For Public Code! We’ll fund some open source feature dev, but we don’t have budget for maintenance/support fees; we can run this ourselves. Otherwise we might as well be buying proprietary software”
- Therefore upstream gets paid to do features for the customer...
- ...which may not align with a coherent product.
- Funding is typically one-off \$
- And so doesn’t cover the maintenance cost of these new features.

Survival time.

- Matrix is taken for granted as a commons! 😊
- Open source creators are cut out, given there is no direct incentive to pay an open source project anything.
- ⇒ Dec 2023: To try to get sustainable, Element stops donating most of its work to the Matrix Foundation, and switches from Apache to AGPL - selling AGPL exceptions to folks who wish to customise it (e.g. SIs)
- ⇒ R&D projects are shelved in favour of focusing purely on stability and quality.
- Free-riding still poses an existential threat to the ecosystem.

The Press is starting to notice.

[matrix]

welt+ KOMMUNIKATIONS-TOOL

Jetzt droht den Krankenkassen das nächste Sicherheitsrisiko



Von **Andreas Macho**
Reporter Wirtschaft & Innovation

“Ab Mitte Juli sollen Versicherte über eine Chat-App direkt mit ihrer Krankenkasse kommunizieren können. Doch die Mehrheit der Krankenkassen setzt dafür auf eine billigere Lösung.

Jetzt warnen einige Schöpfer der Technologie: Die Versicherer gehen damit hohe Risiken ein.”

The Press is starting to notice.

[matrix]

welt+ COMMUNICATION TOOL

Now health insurance companies are facing the next security risk



By **Andreas Macho**
Reporter Economy & Innovation

“From mid-July, insured persons will be able to communicate directly with their health insurance company via a chat app. However, the majority of health insurance companies are opting for a cheaper solution [by using FOSS without funding the upstream].

Now some of the creators of the technology are warning that insurers are taking high risks by doing so.”

But there is hope!

- There is a simple answer:
- **Commercial Matrix deployments should mandate that the upstream project is funded, by buying the upstream's product.**
- **“Pay for what you use, to keep it free”**
- **Only buy from vendors who fund upstream maintenance.**
- Normalise paying for open source products, much as folks pay for proprietary ones.
- If the upstream product isn't suitable, then switch upstream.
- This is *true* Public Money For Public Code.
- Some folks who get it right: ZenDiS! Sweden! UK, US, and NATO!

A photograph of a paved road winding through a dense forest. Sunlight filters through the tall trees, creating a bright path on the road. The text "So, where are we now?" is overlaid in white.

So, where are we now?

- **Matrix is closer to mainstream adoption than ever.**
- The path has been winding:
 - Quite a few Matrix vendors (e.g. Element) have ended up focusing on GovTech and Healthcare to survive - e.g. building enterprise features rather than mainstream consumer- and community-centric features.
- That said, what's good for GovTech is often good for mainstream uptake - after all, the competition is often WhatsApp/Slack/Teams.
- Matrix's strategy for mainstream adoption has been to focus on upgrading the foundations to be **excellent**.
- Matrix 2.0 is the long-running project to ensure Matrix can support mainstream uptake.

Matrix 2.0

[matrix]

- Make it work ⇒ Make it work right ⇒ **Make it fast & usable!**
- **Implementations** to prove the Matrix 2.0 MSCs **landed in Sept 2024!**
- **Next Gen Authentication** (MSC3861 & friends)
 - QR login! 2FA! MFA! Industry standard OIDC! Refresh tokens!
 - Implemented in matrix-authentication-service + Synapse + Dendrite + Element X + Element Web + Fractal...
 - **Final Call Period for merge proposed on Jan 25th!**
- **Simplified Sliding Sync** (MSC4186)
 - Instant login, instant launch, instant sync (with a simpler API!)
 - Implemented natively in Synapse and Conduwuit
 - Verrrrrry nearly proposed for FCP (need to handle 'deleted state' edge case)

Matrix 2.0

- **MatrixRTC** (MSC4143 & friends)
 - Native E2EE group VoIP/Video with pluggable media engines (e.g. LiveKit)
 - Implemented in Element Call + Element Web + Element X & Famedly
 - Still incorporating feedback for the MSCs from the release in Sept.
- **Invisible Crypto** (MSC4153 & friends)
 - E2EE should be invisible to users (as it is on Signal, iMessage, etc)
 - No more cryptic warnings about message authenticity or unverified devices.
 - Adds identity pinning too! Will require users to verify their devices at login.
- While the implementations in Element X + Web landed for The Matrix Conference in Sept, there wasn't a community-friendly distro (oops)
- FOSS (AGPL) Element Server Suite helm charts coming soon!
In the meantime...

Demo!

via element-docker-demo

The Matrix Conference

- The first ever global Matrix Conference happened Sept 2024!
- Super exciting to see so many independent prod-grade stacks in the wild:
 - **Native Rust:** matrix-rust-sdk (The Matrix.org Foundation; mainly Element funded)
 - **Flutter:** matrix-dart-sdk (Famedly)
 - **Kotlin Multiplatform:** trixnity (Connect2x)
 - **Go:** maatrix (Beeper / Automattic)
 - **React Native:** react-native-matrix-sdk (unomed, Filament)
 - **C++:** mtx-client (Nheko)
 - ...and many more!
- ...and an *amazing* set of talks: <https://2024.matrix.org/watch>

Friday 20th September

Opening & Welcome
The Matrix Foundation and Community welcome you to the first ever Matrix Conference of this nature and size.

Matrix 2.0 is Here!
10 years after the original launch of Matrix, and 3 years after the launch of Matrix 1.3 - we'd like to show of Matrix 2.0. The set...

Strengthening the Base: Laying the Groundwork for a more robust E2EE SDK
The past year has seen the introduction of several new APIs in the Matrix Rust SDK. In this technical discussion, we aim to...

From Protocol to Product: Taking Matrix into a typical workplace environment
The focus is build elements, where's it right to consider a paid-for solution, what's it you get and what's the return on...

How to fix security issues in a decentralized system with multiple vendors
Matrix is a decentralized and federated system with many different vendors or other many independent developers...

Using matrix to coordinate emergency services
Can matrix be used to coordinate emergency services? Is it worth waiting for other colleagues to arrive at the...

NextToolSuite: A productivity suite integrated with Matrix
NextToolSuite is a Nextcloud-based, federated NextToolSuite, plug-and-play and user-centric enhancements.

OMA, MIM, DJM/S, Linearized Matrix and more...
There has been lots of work in 2024 around Matrix and the EU Digital Markets Act, and other interoperability initiatives...

Tammy - a modular Matrix messenger
Do you have many ideas on how to change or enhance an existing Matrix app? But the hassle of keeping...

Element X Launch!
In which Element shows off all of the work which has gone into making Element X the world's fastest and most usable Matrix...

Tchap, the French administration federation: past, present and future
is Matrix only a means for the French administration? Tchap as we know it today, and where do we want to be in the future...

Federated, not out of control
Secure Border Gateway being federated: how do they work and what's the matrix?

The T1 Messenger: Advancing Secure Healthcare Communication within Germany
This presentation will provide a technical overview of the T1 Messenger, a fully federated communication service within Germany...

Running a large-scale matrix messenger at university medical center maina
This talk explores the deployment of a large scale Matrix-based messenger at University Medical Center Mainz process.

Matrix as enabler for the SwissPost nationwide ePost communication system
SwissPost is creating a digital easy to use and secure nationwide communication system including messaging based on...

A messenger for NATO and its members
An insight into how NATO is experimenting with Matrix to create a digitally sovereign and secure E2EE style messenger for...

Data Privacy and Signature Management: Battling Digital Surveillance
With the rise of Surveillance Capitalism, ubiquitous technical surveillance (UTS) poses a threat to the privacy, autonomy...

Föräldringskassan, Matrix and Sweden's public sector
Föräldringskassan, the Swedish Social Insurance Agency, offers a springboard of insights from building on Matrix to create...

Increasing Public Sector Collaboration with Secure, Open-Source Platforms
This presentation will explore the emerging market for commercial Matrix-based solutions tailored to Sweden's public...

Beyond Instant Messaging: Matrix in the Public Sector
Its openness and extensibility is what makes Matrix particularly interesting for government organisations. Privacy...

Working in a Purple Submarine: Matrix in openDesk
Imagine an office suite that can operate anywhere, from the boardroom to the most remote location - even in a submarine...

Polychat - Interoperability for the masses
Communication is a human right and the state of that messenger interoperability a social disaster.

Invisible Cryptography
Historically, confusing encryption has been one of Element's weakest usability points in this talk, we'll explain the process that...

Elem SDK - your favourite SDK, you'll never use
While it has become a household name in the Matrix ecosystem, the Elem SDK hasn't had a proper introduction for most people...

Looking at application performance of Sliding Sync in Dart
Deep-dive: I had too much time during work meetings - and what happened? T1 started experimenting with Sliding Sync...

Saturday 21st September

Advancing human rights with Tor
Censorship and surveillance are the biggest threats against civil rights online and tools that use encryption are the only...

The Macroeconomics Of Privacy and Dignity
We talk about privacy and dignity as individual concerns, and then zooms to the data, but if we are going to talk about...

The Walled Garden Dilemma: Privacy vs. App Choice in Messaging Ecosystems
What can managing interoperability learn from academic research on encryptions of messaging apps? In this talk, I present...

Migrating the gematik T1-Messenger spec from Matrix 1.3 to 1.11
A short experience report covering the journey of creating the T1-Messenger specification from Matrix 1.3 to 1.11.

Element Call
Element call is the federated Matrix-based VoIP solution. It is replacing the current call system with significant new...

Implementing a Matrix client inside WorkAdventure - A developer feedback
WorkAdventure is an open platform to build virtual universes for remote events and collaboration. In 2023, we decided...

So Long, and Thanks for All the SDKs: Meet Triptych!
Why use different SDKs for each use case when you can have one? Triptych is not only cross-platform capable, but also...

Regulatory compliance in decentralized environments
A look at how we approach user regulatory obligations for different types of Matrix use cases, with the Digital Services Act (DSA)...

Empowering activists and human rights defenders with Matrix
Wonder how the Matrix Protocol can be leveraged to amplify the voices of civil society movements and activists around...

Simplified Sliding Sync
The first version of Sliding Sync was implemented in Synapse and matrix-synapse with a simplified version of the original...

Authenticated media & how to ship spec features
All images, avatars, videos, and live audio in Matrix are represented as media for other servers to download, cache, and...

Meet the Governing Board
Matrix has had its first elected Governing Board. Join us to learn about the Governing Board - who is it, what it...

Matrix Cryptographic Key Infrastructure
Matrix has a lot of keys. These keys all provide different functionality. If you have ever wondered why do we need all of...

Unable to decrypt this message
If you've used Matrix for a while, you'll have likely seen at least 1 message you're unable to decrypt (UTS). This talk...

State of the Matrix Dart SDK 2024
The Matrix Dart SDK is one of the major features of Matrix client SDKs and there is a pretty quite a few matrix clients that...

MatrixRTC: The (not anymore) missing piece to enable great video conferences
MatrixRTC is poised to revolutionize how we do calls over Matrix. It will solve most of the shortcomings of the current call...

Harder, better, faster, stronger auth with OpenID Connect
Matrix Authentication Service is rebuilding the authentication logic in Synapse from the ground-up, using industry standards...

Introducing decentralised identity to Matrix
Matrix is an open protocol for decentralized, secure communications, the federation architecture is exemplary...

Brain of the community: Matrix as a viable system
This talk is based on the speaker's research of the Matrix ecosystem a few years ago while studying at 'The Open'...

Standalone Matrix-based apps using the Widget API
Despite being a limited access to the Matrix API, Widgets have shown to be useful in situations where you need to...

[matrix] Widget Starter
Matrix is not only an open network for secure, decentralized communication, it also features extensions, called Widgets...

Stop calling Matrix APIs directly
Most people who have seen an introductory talk about Matrix very likely remember the famous 'It is this easy to...'...

Tune Your Chat
This workshop is an interactive talk with an introductory talk about the Matrix Community Retreat which took place in Korea in 2024.

Matrix Community Retreat 2024
I like to share some impressions and results of the Matrix Community Retreat which took place in Korea in 2024.

Closing
So ends the Matrix Conference 2024 - what's next?



Some Matrix Conference Highlights

[matrix]

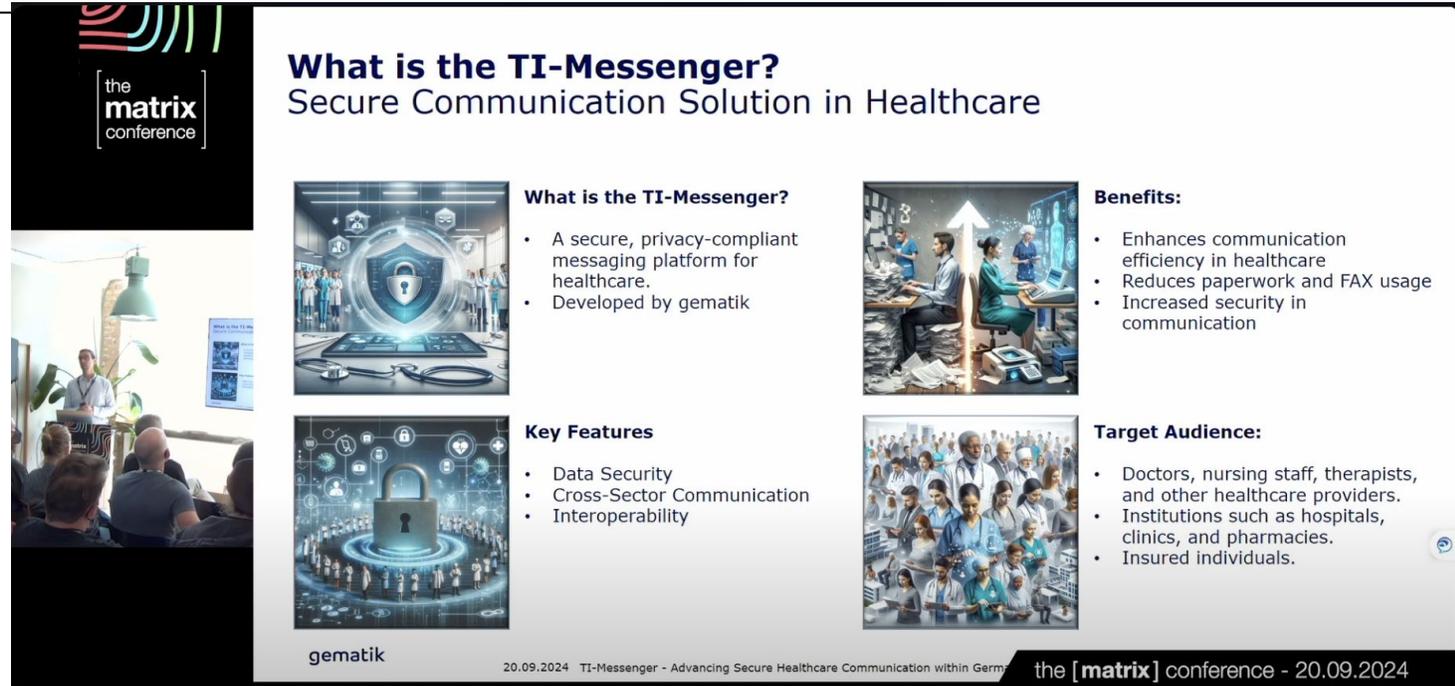
TI-Messenger (Germany)

Gematik is the agency for healthcare interoperability in Germany.

In 2021 gematik selected Matrix as the communication protocol to power TI-Messenger: interoperable secure communication across the entire healthcare industry - insurers, hospitals, pharmacies, doctors, patients.

So we're talking about a nationwide network of 150,000 businesses and 83 million people.

Suppliers' solution will need to be certified by Gematik (standardisation body).



the matrix conference

What is the TI-Messenger?

Secure Communication Solution in Healthcare

What is the TI-Messenger?

- A secure, privacy-compliant messaging platform for healthcare.
- Developed by gematik

Key Features

- Data Security
- Cross-Sector Communication
- Interoperability

Benefits:

- Enhances communication efficiency in healthcare
- Reduces paperwork and FAX usage
- Increased security in communication

Target Audience:

- Doctors, nursing staff, therapists, and other healthcare providers.
- Institutions such as hospitals, clinics, and pharmacies.
- Insured individuals.

gematik

20.09.2024 TI-Messenger - Advancing Secure Healthcare Communication within Germany

the [matrix] conference - 20.09.2024

Timeline:

- TI-M 1 - ad hoc comms between healthcare providers → 2024 ✓
- TI-M 2 - insurances to citizen comms → July 2025
- TI-M 3 - support for Digital Health apps → 2026

Some Matrix Conference Highlights

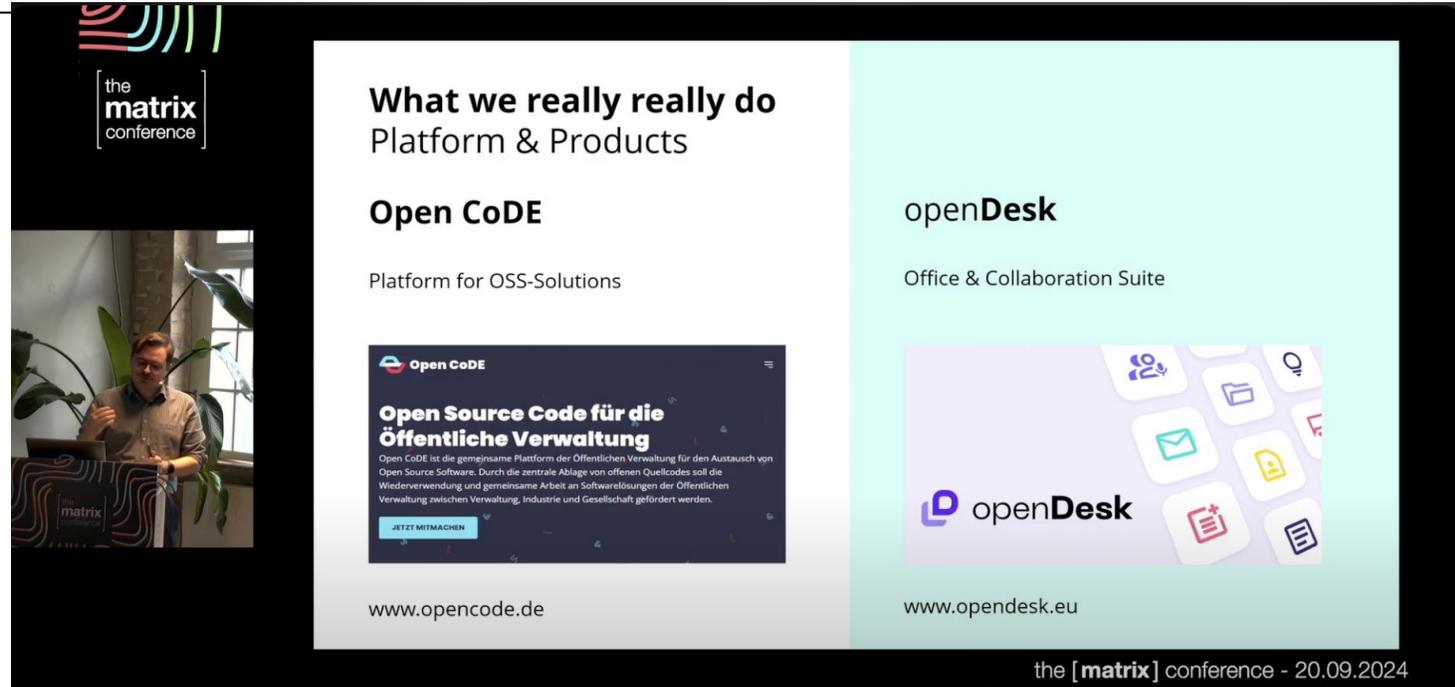
openDesk (Germany)

ZenDiS is the Center for Digital Sovereignty in Germany.

It's led the creation of OpenDesk: an open source Office365 alternative that can be deployed anywhere for German public administration.

openDesk brings 8 vendors together (Element being the chat component) and sustainably funds the upstream projects.

Launched in October 2024.

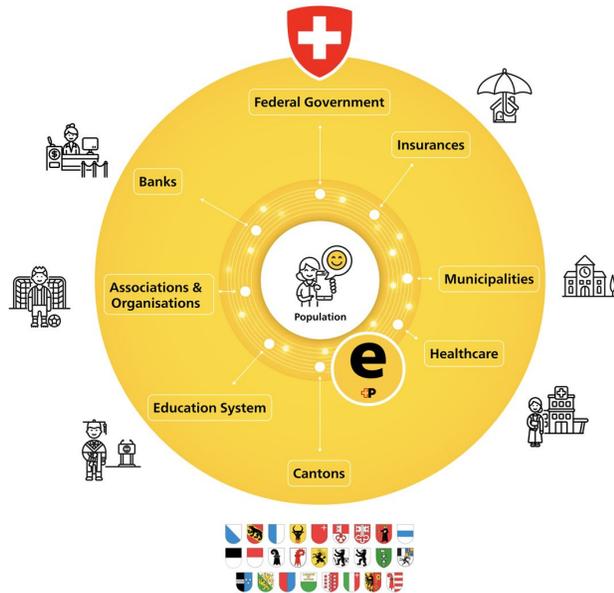


openDesk is now also attracting interest service as role model for other countries, leveraging Matrix as for cross-country federation and collaboration.

Some Matrix Conference Highlights

ePost for Switzerland

ePost is the central communication platform for Switzerland. It connects 9 million citizens with institutions & orgs. A free app as a single point of access to all institutions.



Started in 2021, rolling out as we speak.

Some Matrix Conference Highlights

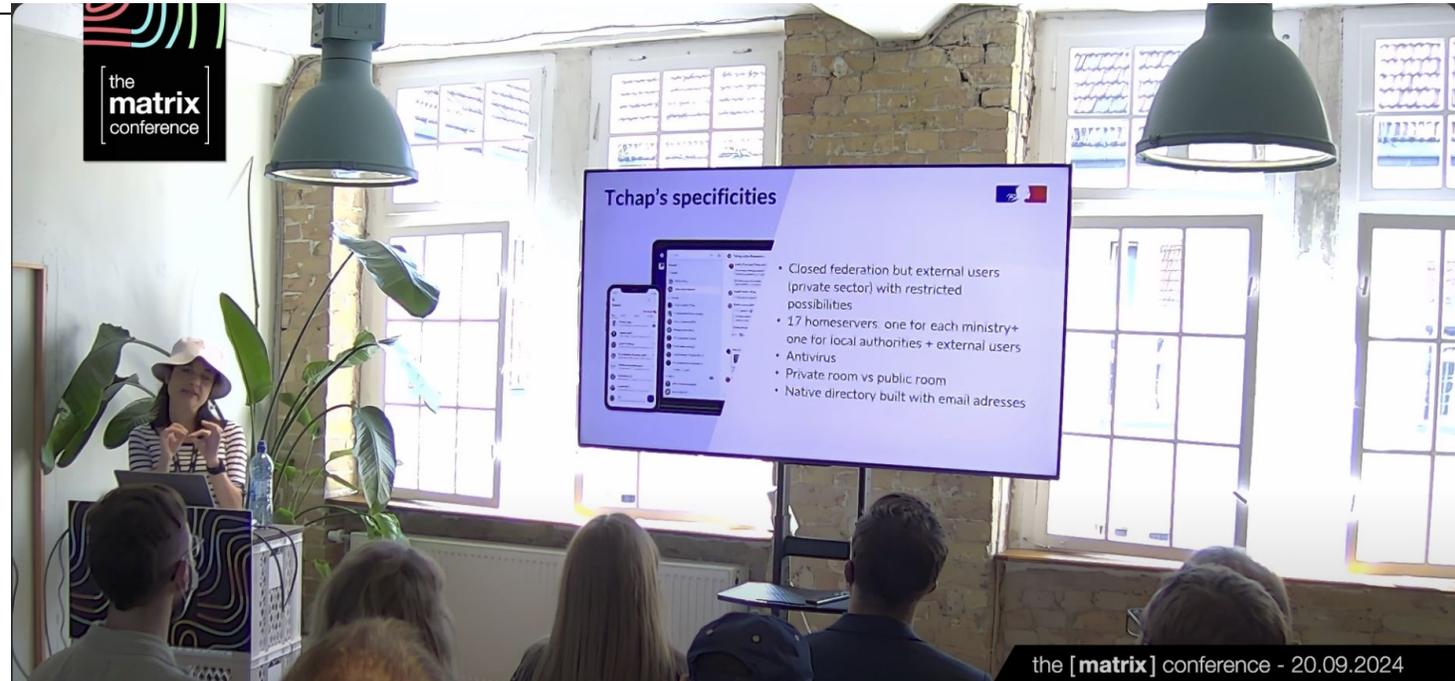
[matrix]

Tchap (France)

A sovereign messenger for the French public sector targeting 5 million civil servants.

Part of La Suite Numerique, with other open source workplace tools.

Working on federating with openDesk and other public sector deployments.



Started in 2018:

- 470,000 accounts
- 280,000 monthly active users
- 6.5 million messages sent per month
- 17 homeservers

Some Matrix Conference Highlights

[matrix]

NI²CE (NATO)

NI²CE messenger for low-side communication (i.e. WhatsApp / Signal replacement) from NATO Innovation Hub inside Allied Command Transformation.

NI²CE in NATO (start)

ACT Priorities: Digital Transformation - NI²CE Messenger: Communication is KEY

Purpose: Provide a safe enough alternative for commercial instant messaging on private devices

Features: instant messaging, location sharing, voice messages (basically anything you would want from a modern messaging app)

Benefits: Safe instant messaging without data leaks and increased resilience

Stakeholders: HQ SACT, ACO, NMI, JFC Norfolk, (possibly the whole NATO Enterprise)

NI²CE Messenger
NATO Interoperable Instant Communication Environment Messenger

The NATO Interoperable Instant Communication Environment (NI²CE) Messenger is a **proof of concept** project with the following objectives:

- Use post quantum proof encryption schemes
- Demonstrate the usability of the Matrix protocol and the compatible end-user applications for the NATO Enterprise and NATO missions and capture additional user requirements
- Analyze and certify the use of bridges to connect Matrix to the NS environment and JChat

NI²CE allows for secure & safe communication across NATO bodies on private devices, supporting the digital transformation of the Alliance

A messenger for NATO and its members
Jeroen Franssen

the [matrix] conference - 20.09.2024

Started in 2022:

- Thousands of users
- Multiple homeservers
- Using Element Server Suite

An aerial photograph of a dense forest at sunrise. The sun is low on the horizon, creating a warm, golden glow that filters through the trees. A road or path winds through the forest in the lower right quadrant. The overall atmosphere is serene and forward-looking.

What comes next?

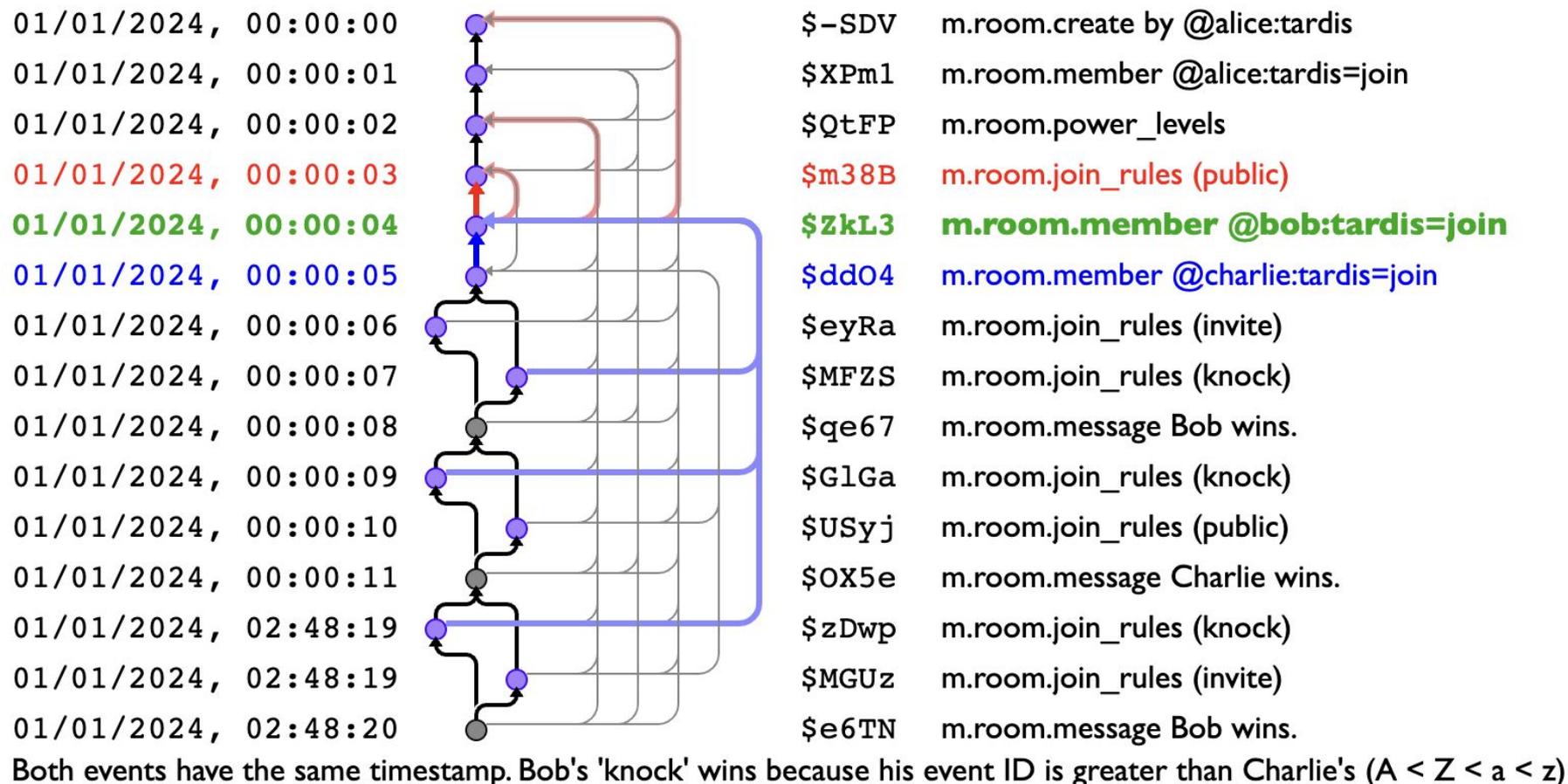
Building for the next 10 years...

State Res v3

- State resolution is how Matrix replicates state (key/value data - e.g. room membership and permissions) between servers.
- This is a Hard Problem in a decentralised world.
- We're currently on State Res v2 (MSC1442), which aimed for both correctness and minimal network overhead.
- Generally works, but over the years we've found some scenarios where state can still "reset" (i.e. resolves to an unexpected result)
- Currently in the final stages of analysing these and proposing a provably correct v3!

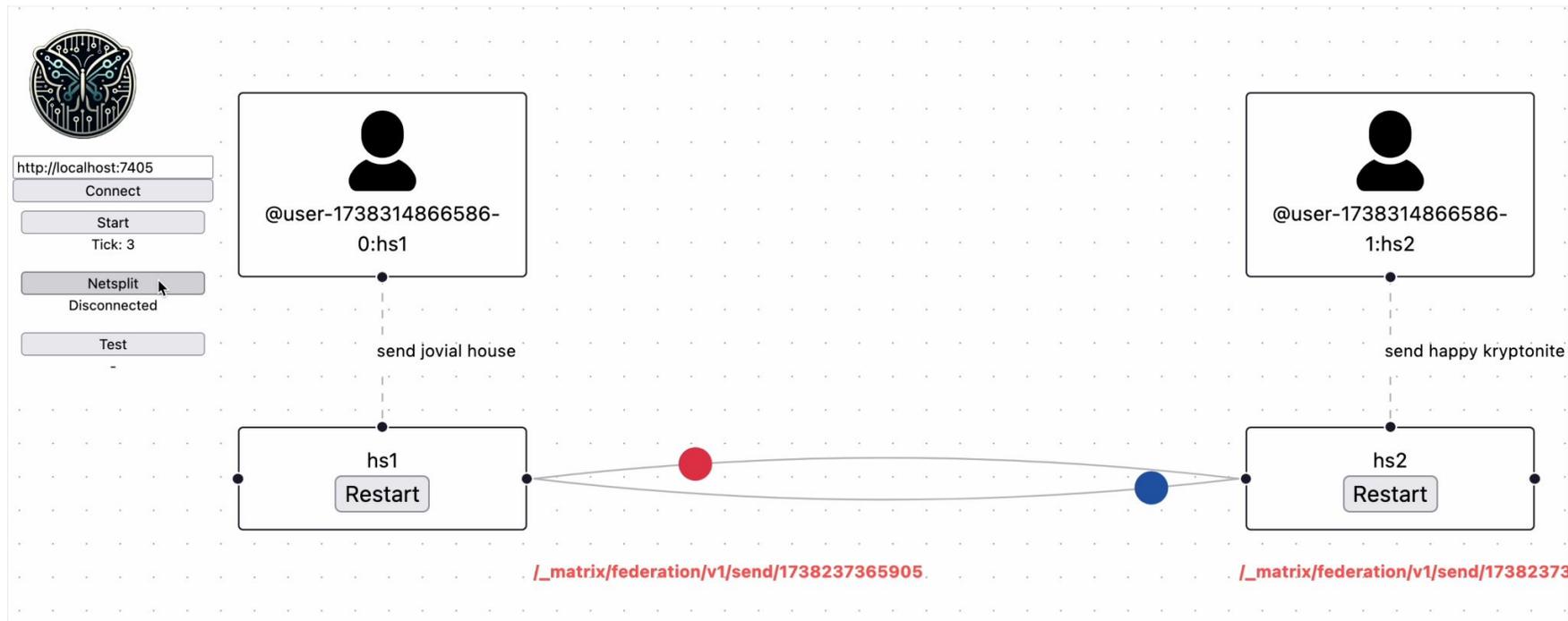
State Res v3: TARDIS

- Time Agnostic Room DAG Inspection Service
- Time-travelling debugger for state resolution!



State Res v3: Introducing Chaos

- Chaos is a partition/fault tolerance testing tool for homeservers.
- It causes netsplits and restarts servers, checking for convergence by ensuring all homeservers see the same member list.
- See Kegan's talk in the devroom (K.4.201 at 14:00 CET) for more.



MLS (Messaging Layer Security: RFC 9420) [matrix]

- Defines efficient key exchange across a set of devices.
- Requires a central entity to sequence commits (e.g. group changes)
- Lots of investigation over the years on if/how to use it in Matrix:
 - DMLS (MSC2883): Each server maintains its own MLS tree, and they get merged together. Means you may have to store key material for future merges, and diverges from normal MLS semantics.
 - RFC 9420 MLS for Matrix (MSC4224): Each conversation has a hub server which sequences commits; State resolution operates as it does today.
 - RFC 9420 MLS mode Matrix (MSC4256): Commits sequence via hub; MLS is used to store state; Message senders are device public keys, not mxids.
 - Linearized Matrix (MSC3995): All traffic goes through a hub; Matrix state events are synchronised with MLS state by the hub.
 - MIMI: IETF WG - All traffic goes through a hub; MLS is used to store state; Has its own event format.
- Any progress on this by the core team is blocked on funding.

Post Quantum Encryption

- Last FOSDEM we teased poljar's PQXDH PR #120 for vodozemac
- Adds Kyber for post-quantum key exchange to the Double Ratchet, following Signal's example.
- Further progress by the core team is blocked on funding.
- MLS meanwhile is experimenting with PQ - e.g. <https://cryspen.com/post/pq-mls/>
- Further progress by the core team there is blocked on funding too...

matrix-rust-sdk evolution

- Aim: to be a core flagship SDK
- Persistent Event Cache!
- Offline support!
- Lazy-loading from the event cache!
- Threads! (coming soon)
- Spaces! (coming later)
- More bindings!
 - React Native
 - WASM
 - Ruby

A world without matrix-js-sdk?

- WASM bindings for matrix-rust-sdk pave the way to matrix-rust-sdk one day replacing matrix-js-sdk, letting it be used on iOS & Android.
- matrix-rust-sdk compiles to WASM already
- Uniffi support for WASM is all that's missing - Mozilla and Filament currently working on this.
- Don't want to have to maintain wasm-bindgen bindings as well as the existing uniffi bindings used for Swift, Kotlin etc.
- What if we cheated and didn't bind the API at all...?
- See Timo Kandra's talk in the devroom (K.4.201 @ 13:30 CET) for more!

Missing Mainstream features (clients)

- Extensible profiles (MSC4133 - **now passed MSC!!**)
- Custom Emoji (MSC1256 or MSC1951 or MSC3892 or...)
- Threads 2.0
- Sharing E2EE history on join (MSC3061)
- Finishing E2EE Search
- Voice rooms (for Discord folks)
- Safety tooling (“As a user, i want to hide invite spam”)

Missing Mainstream features (server)

[matrix]

- User discovery
 - Federated identity?
 - “Interoperable privacy preserving user identity and discovery for E2EE messaging” - Google in MIMI ⇒ [draft-interop-mimi-discovery-requirements](#)
- Improved room / space discovery
- Small server performance:
 - Finishing Faster Room Joins (MSC3902)
 - Better than Full Mesh Federation
 - Efficient state storage
 - State Res v3
- Guest access that doesn't suck.

Trust & Safety

- Abuse is increasing, but so are countermeasures.
- Authenticated Media landed, stopping abuse of Matrix as a CDN
- Account Suspension landed, allowing more robust counterabuse.
- abuse@matrix.org team expanded at end of 2024 to keep up with reports (improvements in communication expected this year).
- Additional serverside automated abuse detection landed
- Mjolnir is being actively maintained and improved with new protections
- Draupnir released 2.0
- T&S Working Group forming within The Governing Board.

Matrix 3.0?

- Lots of options being thrown around.
 - “Make it safe” - focus entirely on fixing Matrix’s trust & safety tooling?
 - What if we then used decentralised reputation & identity to prove whether information came from humans or are AI slop?
 - MLS + Matrix - hand over cryptographic group membership to MLS?
 - Converge with MIMI?
 - P2P Matrix?
- Place your bets!

The Foundation is key.

- The Matrix.org Foundation has been operating independently since Robin joined as Managing Director in August 2023.
- The fact that the Foundation exists to neutrally protect and preserve Matrix irrespective of commercial entities is a huge deal.
- Responsibilities include:
 - Ensuring key components (e.g. E2EE) are implemented as FOSS and audited.
 - Publishing the spec, and everything else at <https://matrix.org>
 - Running the matrix.org homeserver and other common infra
 - Trust & Safety for Matrix
 - Evangelizing Matrix
- The Foundation will nurture the next 10 years of Matrix, and beyond...
- **...if it has funding.**

Funding Members

AUTOMATTIC



element



FUTUREWEI
Technologies



fairkom

Famedly

iNDIE HOSTERS

X-WIKI



ERCOM
Cyber Solutions byThales

gematik

For Matrix to prevail, **we need your support.**

[matrix]

- The Foundation now runs entirely independently, with Robin Riley as MD!
- The Governing Board was elected in May 2024!
- Fundraising **right now** to support core spec work, trust & safety work, bridging improvements, running the matrix.org infrastructure and governance work - target £900K.
- **To support, join the Foundation:** <https://matrix.org/membership/>
- Meanwhile, **PLEASE** buy Matrix solutions from vendors who fund upstream maintenance and development. Otherwise there will be no upstreams.



Introducing The Matrix Governing Board

[matrix]

- The GB is an advisory board, bringing a representative set of perspectives that will help keep the Foundation on track and accountable.
- Elected in May 2024
- 24 representatives of various stakeholders, spanning 11 orgs
 - Members of the Foundation (including individuals)
 - Representatives of the ecosystem and other supporting foundations (Associate members)
 - Spec Core Team
 - Guardians
 - Robin, the Foundation's Managing Director

We need help!!

FRIENDS DON'T LET FRIENDS USE PROPRIETARY CHAT SERVICES



<https://matrix.org/membership/>

- If you benefit commercially from Matrix - **PLEASE** financially support the upstream project.
- Run a server (or pay your upstream project for one!)
- Build bridges and bots to your services!
- Build your cool new project on Matrix!
- Follow [@matrix@mastodon.matrix.org](https://mstdn.social/@matrix) & spread the word!

[matrix]

Thank you!

[m] @matthew:matrix.org

 matthew@matrix.org

 <https://matrix.org>



[@matrix@mastodon.matrix.org](https://matrix.org/@matrix@mastodon.matrix.org)

 [@matrix.org](https://matrix.org)