

Migrating the gematik TI-Messenger spec from Matrix 1.3 to 1.11

Johannes Marbach | Matrix Conference 2024

Agenda

1. Intro

2. Moving TIM from Matrix 1.3 to 1.11

3. Summary & outlook

1. Intro

Intro – Who am I?

- Systems Architect at gematik 
 - Freelance Engineer at Unomed 
 - Previously Engineering Manager at Element 
 - Matrix enthusiast
-
- Matrix – <https://matrix.to/#/@johannes-marbach-gematik:matrix.org>
<https://matrix.to/#/@h3nn3s:matrix.org>
 - GitHub – <https://github.com/Johennes/>
 - Mastodon – @h3nn3s@fosstodon.org
 - LinkedIn – <https://www.linkedin.com/in/johannesmarbach/>

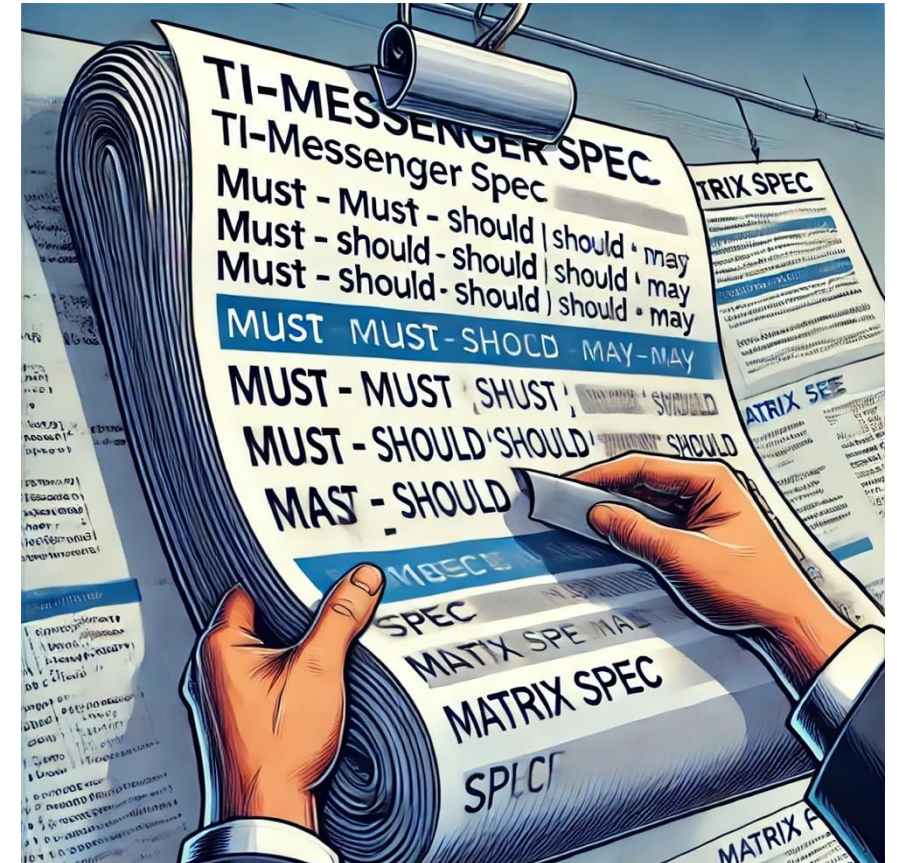


Intro – What is gematik?

- National Agency for Digital Medicine in Germany
- Shareholders include
 - Ministry of Health
 - Representatives of health insurances / physicians / pharmacists
 - etc.
- Responsible for Telematics Infrastructure (TI)
 - Secure digital healthcare network for exchanging sensitive medical data
- Duties: Specification, certification, monitoring, etc.

Intro – What is the TI-Messenger (TIM)?

- Secure messaging service for medical communication
- Open market model
 - gematik specifies & certifies
 - Other companies implement & operate
- Based on Matrix
- Latest release (June 2024) builds on Matrix 1.3



2. Moving TIM from Matrix 1.3 to 1.11

Why is a Matrix version update needed (and complicated)?

- Matrix 1.3 was released June 2022
- Subsequent versions contain fixes, new features and security improvements
- Evaluate new features for medical context (use case & security)
- Prevent incompatibilities
 - Matrix: Features can be removed after being deprecated for ≥ 1 version
 - 🧡 TIM: Additional requirements to guarantee compatibility
- Speed up migration (glacial speed, certification valid for 3 years)
 - Matrix: Servers MUST implement / clients SHOULD NOT use deprecated features
 - 🚚 TIM: Servers MUST implement / clients MUST NOT use

The Matrix changelog (it's amazing)

- Sections for different protocol parts
- Change categories
 - Breaking changes
 - Deprecations
 - Removals
 - New endpoints
 - Backwards-compatible changes
 - Clarification
- Linkified
- Support rooms: [#matrix-spec:matrix.org](#) / [#sct-office:matrix.org](#)

4.6. Room Versions




Backwards Compatible Changes

- Add room version 11 as per [MSC3820](#). ([#1604](#))

Deprecations & removals

- Remove `keyId` from `/_matrix/key/v2/server/{keyId}` ([#1350](#))
 - Compatibility problem (e.g. still used by Synapse until end of 2022)
 - 🤝 Servers MUST still implement `/{keyId}` (Synapse already does this)
- Deprecate query string authentication ([#1808](#))
 - 🚚 Clients MUST use `Authorization` header
- Deprecate unauthenticated media endpoints ([#1858](#))
 - 🚚 Clients MUST use new authenticated endpoints if available







New endpoints

- Authenticated media (#1858)
 -  Inherit with restrictions (no freeze)
- Asynchronous media uploads (#1499)
 -  Inherit without modification
- Logging in another client (#1530)
 -  Forbidden (no use case / potential security threat)
- Most new features don't land in this category





Backwards compatible changes

- In many cases inherited in TIM without changes
- Exception: New features are often backwards compatible
 - New relation types (e.g. `m.replace`, [#1211](#))
 - New parameters on existing endpoints (e.g. erasure requests, [#1730](#))
 - New but optional endpoints (e.g. server support discovery, [#1733](#))
 - Room versions (e.g. room version 11, [#1604](#))
- Compatibility not always exact
 - Updated scope of transaction IDs ([#1526](#))
 - Technically breaking but deemed backwards compatible for *public* ecosystem
 - Deemed uncritical for TIM due to entropy of transaction IDs in open source SDKs

Backwards compatible changes (continued)

- Event replacements (#1211)
 -  Allowed but history MUST be displayed
- Threads (#1254)
 -  Forbidden (no clear use case / difficult to get right UX-wise / possible interplay with notification issues)
- Event annotations (#1475, #1531)
 -  Allowed but length MUST be limited to one Unicode character (unencrypted)
- Room versions 10 & 11 (#1397, #1604)
 - MUST support room versions 9 () , 10 and 11 ()
 -  Room creation / upgrade only with 9 and 10

Clarifications

- Generally just inherited without changes, but some exceptions
- Add missing secrets, third-party invites and room tagging modules ([#1860](#))
 -  Secrets allowed /  Third-party invites forbidden /  Room tagging allowed
- Removal of `dont_notify` and `coalesce` push rule actions ([#1501](#))
 - Actions were NOOPs but technically a removal without deprecation
 -  Clarified upstream that servers MUST gracefully ignore actions ([#1890](#))

3. Summary & outlook

Summary & outlook

- Matrix changelogs have been invaluable in updating the TI-M spec
- Classification not always perfect but we need to dissect the entire changelog anyway
- Being able to upstream spec improvements makes our lives easier

- In future we'd like to:
 - Keep up with Matrix releases as closely as *possible* (updating ~ once a year)
 - Conduct some of the process on GitHub to get feedback earlier
 - Upstream some of our custom extensions (e.g. invite filtering)

Questions?