Authenticated media & shipping spec features

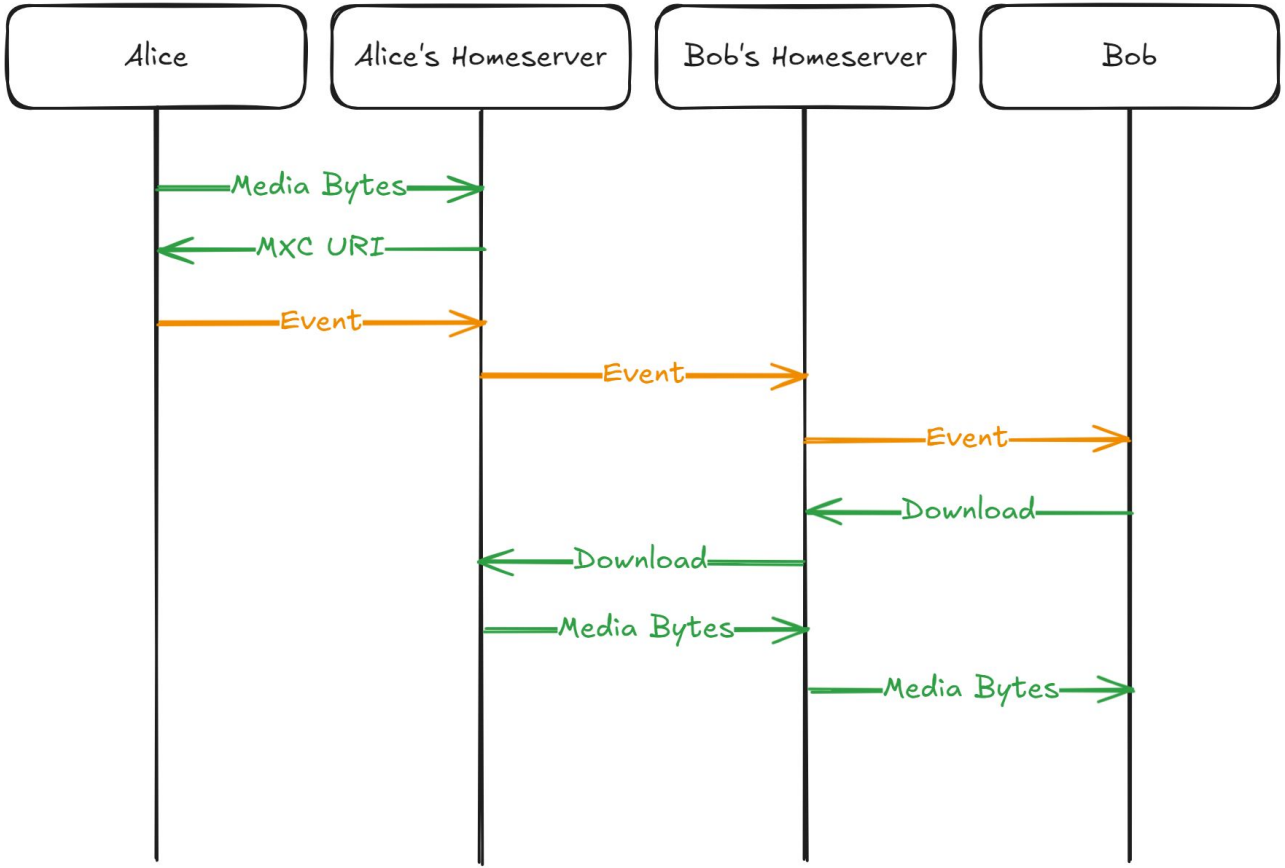
Matrix Conference - September 21, 2024

Travis Ralston
T&S / Director of Standards Development - matrix.org
@travis:t2l.io | travisr@matrix.org

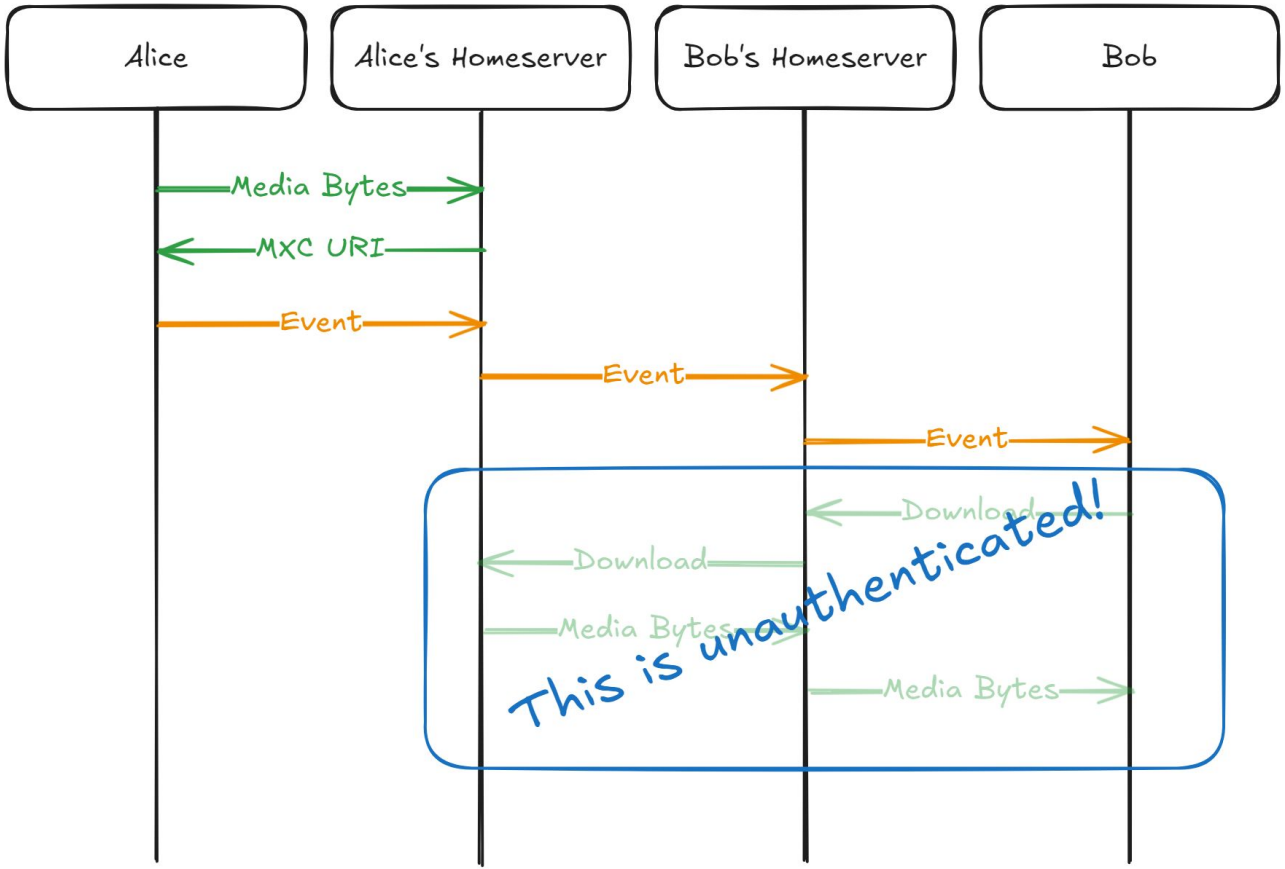
Media in Matrix

- Images, avatars, videos, files, etc are all “media”.
- Media can be large, so it’s pointed to rather than included inline.
- Clients upload media to get an MXC URI they can use in events.
- Media is pulled while events are pushed: Events are sent to servers (and their clients) first, then clients ask their servers to download media.
- The endpoints used to download media have been historically unauthenticated.
- Unauthenticated access means potential for abuse, which is not great.

Media in Matrix



Media in Matrix



Matrix Spec Changes

- Markdown documents which further the specification.
- Should be published in draft status when still exploring solutions. MSCs are great places to coordinate *unstable* implementation.
- Doesn’t have to fit a template, but the template does help.
- Lots of review and experimentation until acceptance.
- Final Comment Period (FCP) called by Spec Core Team (SCT) when proposal meets checklist+template criteria. Some key details being:
  - Evidence of the MSC working
  - Alternatives are discussed and dismissed
  - Clear proposal text

Options for authenticated media

matrix

1. Reuse existing access token and request signing (X-Matrix)
2. Time-limited URLs
3. Pre-signed URLs
4. Cookies
5. Some combination of the above (eg: hmac(access_token, url, expiration))

The MSC will need to propose a singular option, but can be hard to pick early on. Experimentation and evaluating each individually can help.

Reusing existing authentication

matrix

👍 **Clients and servers already know how to use these.**

👍 Easy for mobile clients and bots to account for.

👎 Web/desktop clients might need Service Workers or similar.

👎 Breaks copy/pasted links (a feature in the MSC).

👎 Bridges need to implement a proxy mechanism.

Time-based/pre-signed URLs

matrix

👍 Existing concepts from industry.

👍 Trivial for client developers to reason about, if designed well.

👎 Possibly requires extra round-trips to get the URL for a piece of media.

👎 Allows copy/pasted links to work, sometimes.

👎 Bridges need to implement a proxy mechanism.

Cookies

matrix

👍 Existing concept from industry.

👍 Web clients in particular can use this without doing much/anything.

👍 Most HTTP libraries and mobile SDKs support cookies.

👎 Possibly requires extra round-trips to get a cookie.

👎 Confuses users when copy/pasted links work for them but not friends.

👎 Not all environments like third-party cookies.

👎 Bridges need to implement a proxy mechanism.

?verify=hmac(...)&expiration=...

matrix

👍 Existing concept from industry.

👍 All clients can support this trivially.

👍 Pre-calculated values could avoid redundant HTTP calls.

👎 Servers may log query string.

👎 Using the user's access token in the HMAC is a risk.

👎 Bridges need to implement a proxy mechanism.

Design considerations

- Bridges will need to proxy media regardless of feature design.
- New endpoints for downloads are required.
  - We can split Client-Server and Federation while we're here.
- The protocol generally prefers to have only a few unique concepts.
- All developers will be impacted by the change.
- Needs to support CDNs/redirects.
- A transition period may be required.

MSC3916's implementation

matrix

- All the options are roughly equal, so need to pick one to prove out.
- MSC3916 initially picked reusing existing concepts back in 2022.
- T&S weighed the alternatives, and started prototyping out MSC3916 unmodified in early 2024.
- Identified web clients as least likely to support the change nicely.
  - Service Workers could be used with minimal overhead.
- Alternatives had (theoretically) similar impact on other types of clients.
- Synapse and MMR used to ensure federation can work.
  - Ended up being beneficial: Python/Twisted doesn't support multipart requests very well.
- Multiple iterations of implementation and MSC editing, we had a proposal ready for FCP in ~July 2024 🎉

Rollout

The rollout plan was included in MSC3916 to document backwards compatibility:

- Servers should *stop* serving media on old endpoints within 1 spec release.
- Media uploaded before that should remain accessible on the old endpoints indefinitely. This is to avoid breaking URLs in the wild.
- Servers should consider their “local ecosystem” before doing this.
- The matrix.org homeserver plans to do this relatively quickly.
- Error codes exist, helping monitor ecosystem progress.

The above became known as a ‘media freeze’, and was documented in Matrix 1.11’s release and matrix.org’s sunset post too.

Rollout (matrix.org)

- Millions of users would be impacted by the change. Some users will be on old clients, but we can try to support them as best we can.
- With a stable MSC, developers can start relying on the ‘final’ design for authenticated media.
- beta.matrix.org was configured to mimic the freeze.
- matrix.org monitored the ratio of requests to new vs old endpoints.
- Some clients, including Element Web, encountered bugs with their implementations close to the original planned freeze date.
- Freeze date was pushed out by a week to allow those clients a bit of time for releases to reach users.
- Most users on matrix.org didn’t notice the change.

(Early) Retrospective

- More implementations would have been good for the MSC.
  - Condu(wu)it, Dendrite, etc didn't get support until late in the rollout.
  - Multiple clients became aware of the feature *after* matrix.org's freeze.
  - Service workers don't work in private browsers, seemingly.
    - https://github.com/matrix-org/matrix-spec/issues/1949
- Possibly a longer rollout on matrix.org?
- MSC3916 didn't have guest access requirements specified (oops).
  - Fixed: https://github.com/matrix-org/matrix-spec-proposals/pull/4189
- We forgot about widgets (again, sorry). See MSC4039.
- Alternatives weren't detailed out in the MSC.
  - Specifically, "why not cookies?".
- Not all developers hang out in #matrix-client-developers:matrix.org or #matrix-homeserver-developers:matrix.org.

Next steps

- Synapse (and MMR) to enable media freeze by default Soon.
- Unauthenticated (deprecated) endpoints should be removed from the spec, but not Synapse or MMR - they'll continue existing for a long while.
- Update MSC3916 with more details about the alternatives, likely from the authenticated media v2 work.
- Deleting media when the associated events are redacted.
  - https://github.com/matrix-org/matrix-spec-proposals/pull/3911
- Help fix authenticated media for private browsers with a v2.
  - Rollout TBD.

Thanks

Travis Ralston
T&S / Director of Standards Development - matrix.org
@travis:t2l.io | travisr@matrix.org