Introducing Decentralised Identity to Matrix

Wenjing Chu

The Matrix Conference, 09-21, 2024, 17:30–18:15 Berlin, Mitosis LAB

A few words about myself & My Talk

I am an active contributor to the OpenWallet, Trust over IP / LF Decentralised Trust, W3C, and related communities focused on digital identities & trust frameworks, but *a newbie* on Matrix.

This talk will discuss a proposal to introduce the latest *decentralised identity methods and protocols* within *the Matrix architecture* and discuss the benefits of that integration to Matrix users and ecosystem.

Wenjing Chu:
@firegod0:matrix.org
https://www.linkedin.com/in/wenjingchu/

Three things to cover

Why do we need decentralised identity in Matrix? What does it mean to users and the Matrix ecosystem?

A new way: the Trust Spanning Protocol (TSP) to realize universal ***Interoperability of authenticity and privacy*** with decentralised identity.

Seeking feedbacks and a good approach to introduce decentralized identity in Matrix.

Why Decentralised Identity for Matrix

“...the mission to bring secure, interoperable, decentralised communication to the world.”

Matrix Manifesto

“We believe:

People should have full control over their own communication.

People should not be locked into centralised communication silos, but instead be free to pick who they choose to host their communication without limiting who they can reach.

The ability to converse securely and privately is a basic human right.

Communication should be available to everyone as a free and open, unencumbered, standard and global network.”

Why Decentralised Identity for Matrix

Matrix is an open protocol for decentralised, secure communications with a federation architecture.

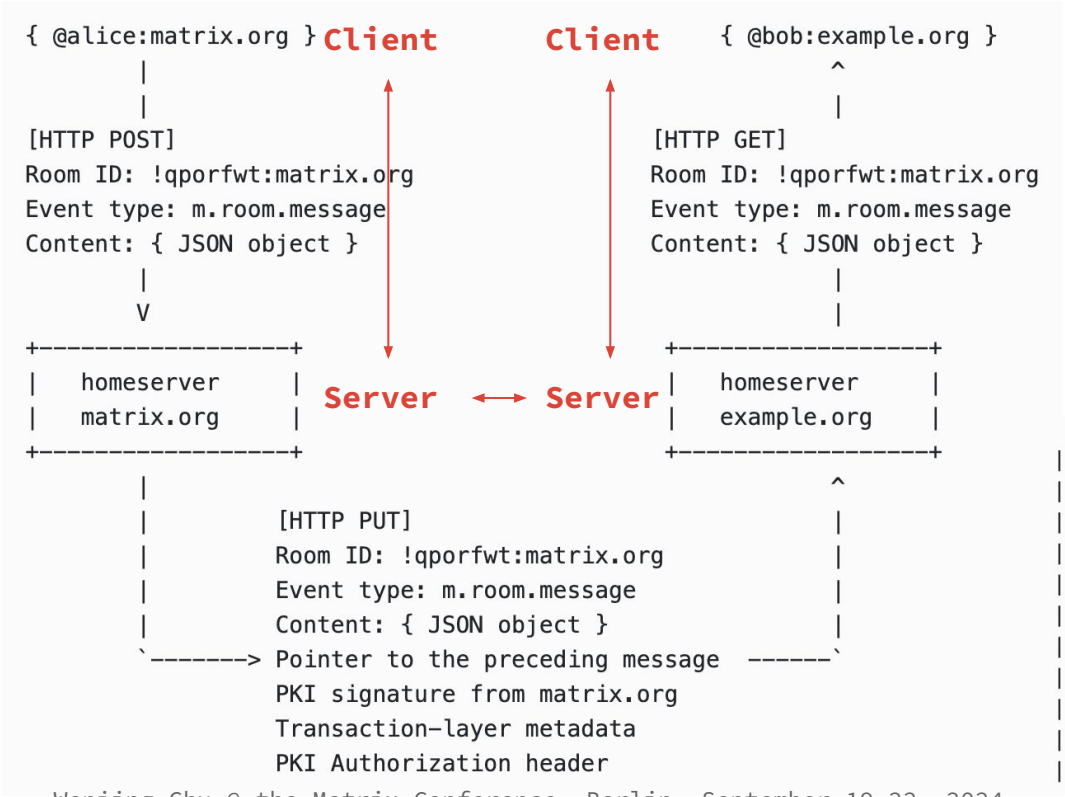
Its digital identity system however is not fully decentralised and is a significant weakness in the overall user experience, authenticity and privacy protection.

- Centralized
- Federated
- Decentralised

Why Decentralised Identity for Matrix

Matrix manifesto goals	Secure?	Interoperable?	Private?	Choice?	Reach?
Centralized	Yes & no	No	No	No	Yes, but
Federated	Yes & no	Yes, but	No	Yes, but	Yes, but
Decentralised	Yes, and getting better	Yes with open protocol	Yes with open protocol	Yes	Yes with open protocol

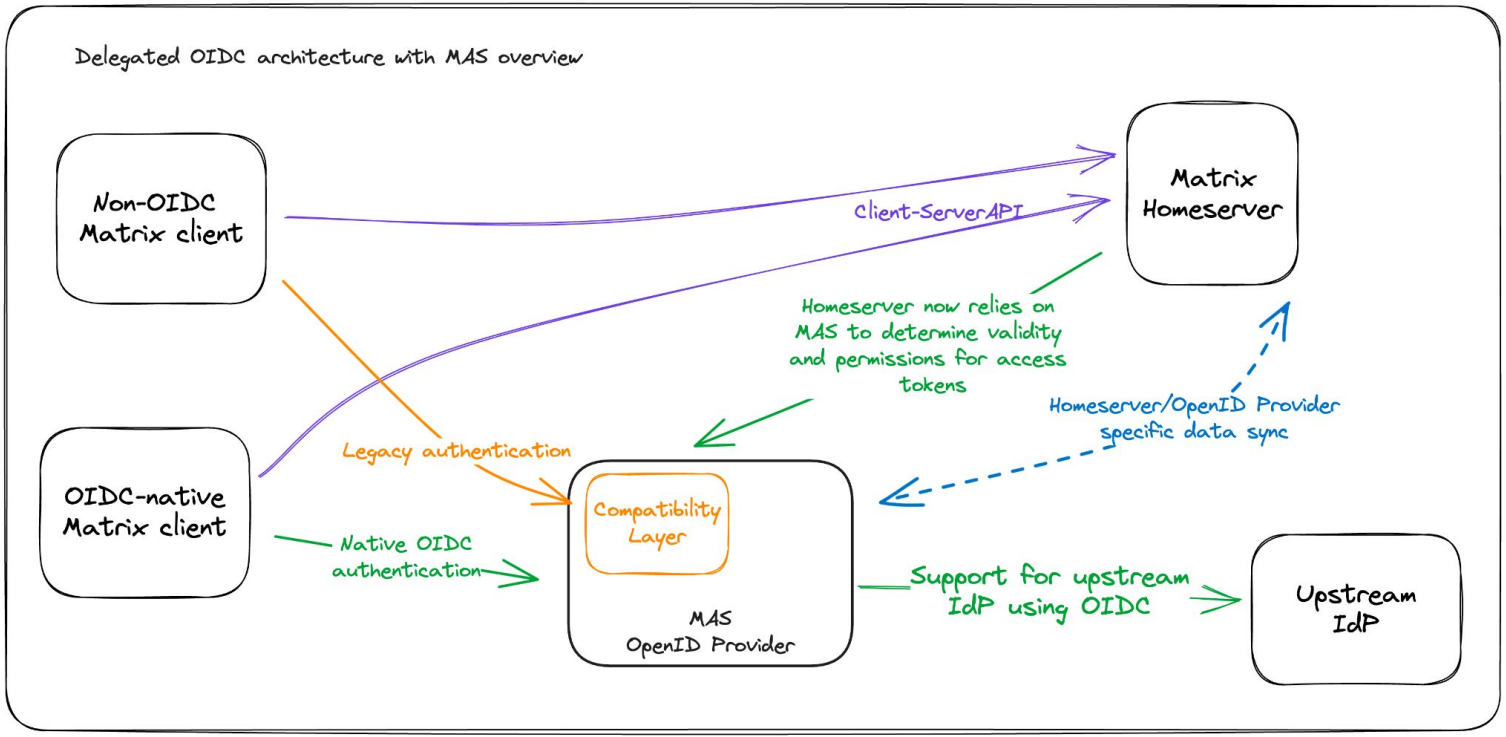
What does decentralised identity Support mean?



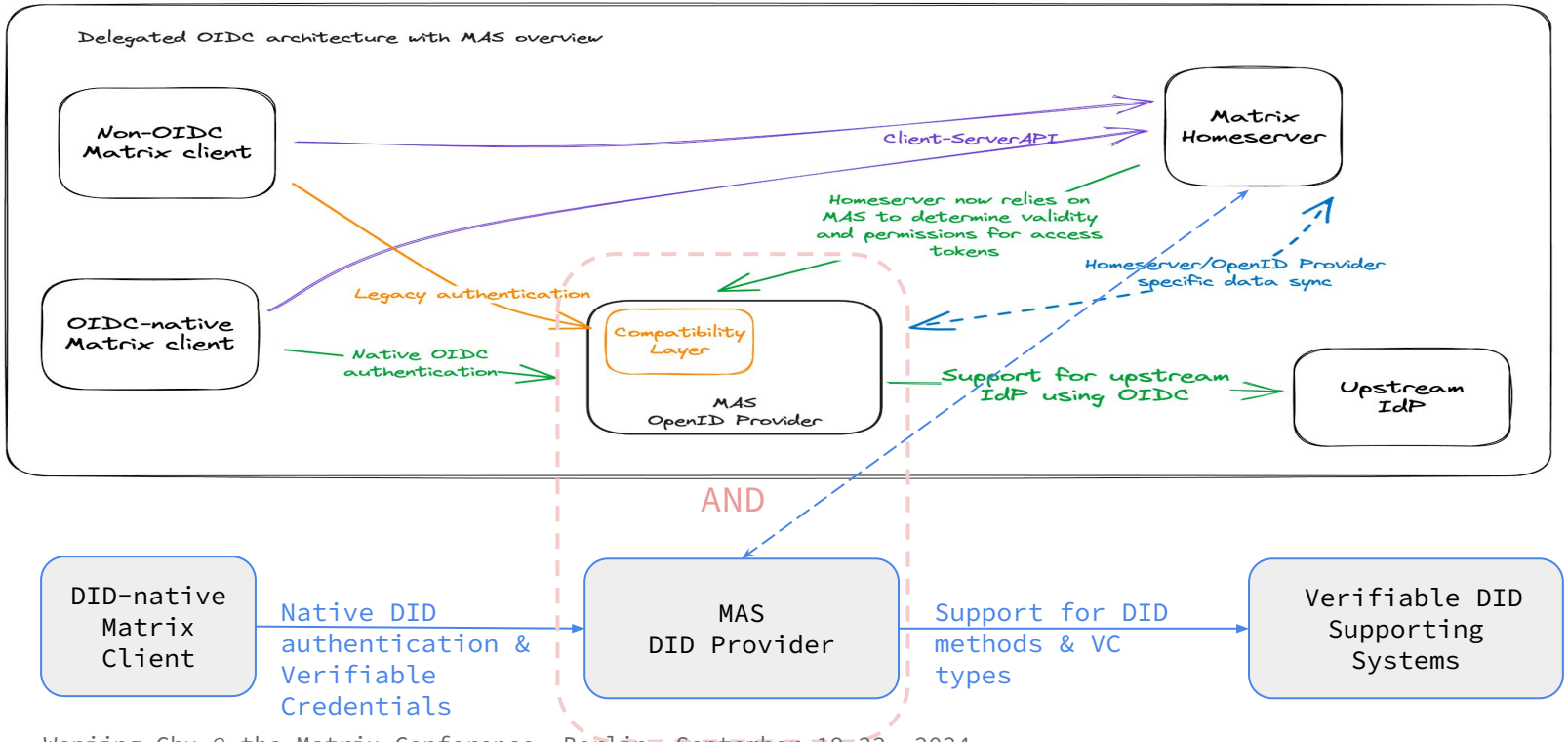

```
.................................
|          Shared Data          |
| State:                        |
|   Room ID: !qporfwt:matrix.org|
|   Servers: matrix.org, example.org |
|   Members:                    |
|    - @alice:matrix.org        |
|    - @bob:example.org         |
| Messages:                     |
|   - @alice:matrix.org         |
|     Content: { JSON object }  |
|...............................|
```

What does decentralised identity Support mean?

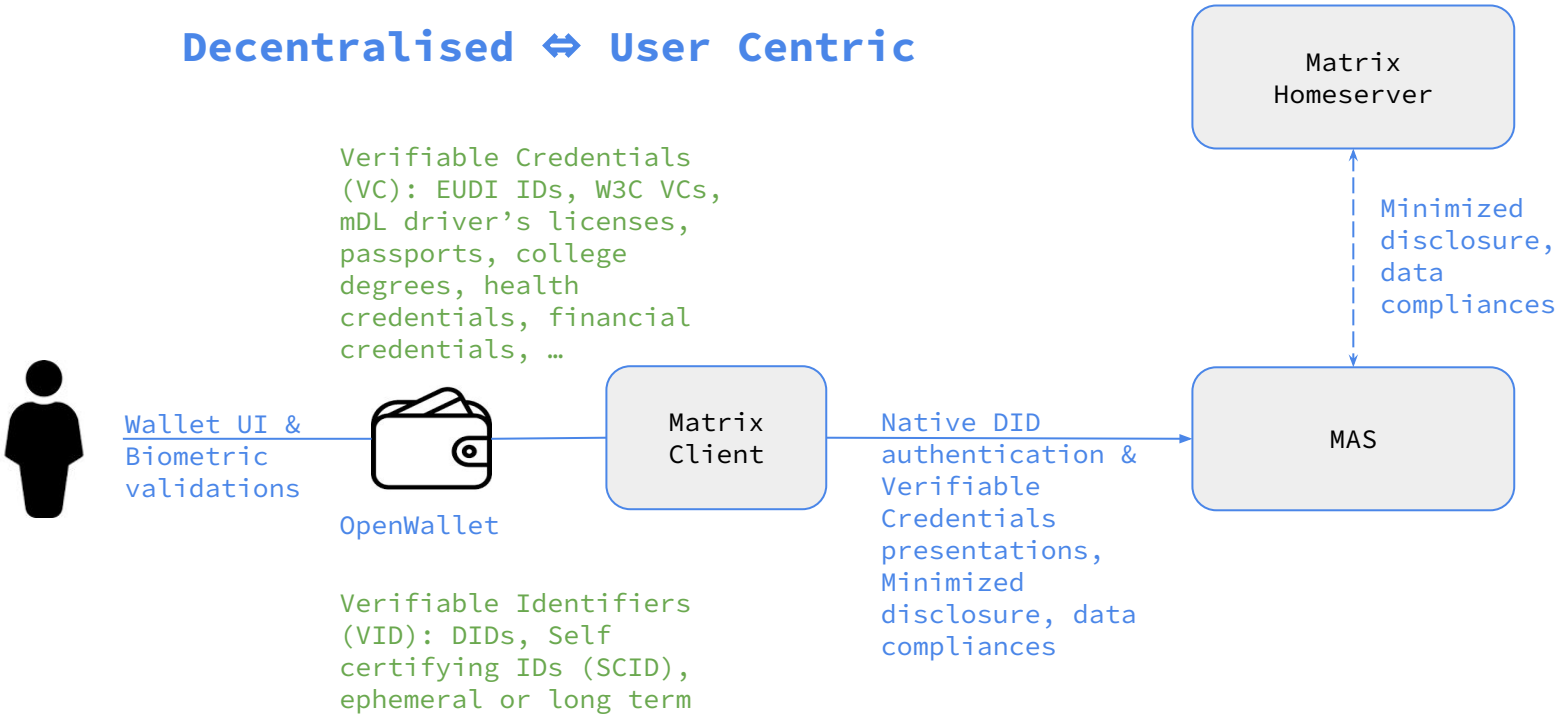
https://github.com/matrix-org/matrix-spec-proposals/pull/3861



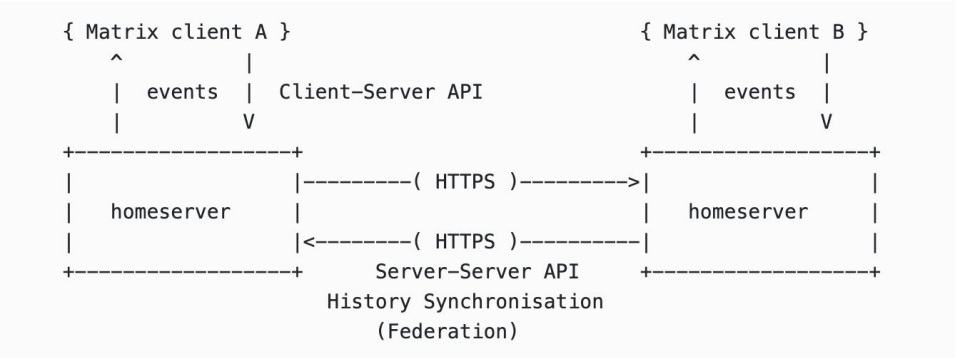
What does decentralised identity Support mean?

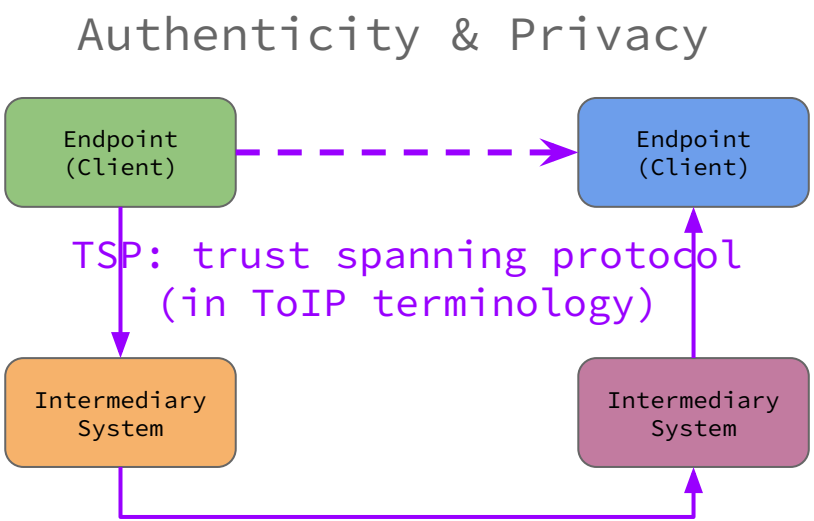


What does decentralised identity Support mean?



Interoperability of Authenticity and Privacy





*Authenticity: Who says What
*Privacy: Confidentiality and Metadata Privacy
*A good architectural match. To learn more about TSP,
Spec: https://trustoverip.github.io/tswg-tsp-specification/
Code: https://github.com/openwallet-foundation-labs/tsp

Interoperability of Authenticity and Privacy

- User centric: Users manage their identities and associated data with the help of a digital wallet
- Stronger authenticity
  - End to end, user to user
  - Dynamic incremental credentials to match application's needs beyond messaging (e.g. tickets, qualifications, money & assets, legal, AI labeling, digital content/media)
- Stronger privacy
  - Data minimization and user control, selective disclosure, ZKP
  - Metadata privacy, reduce tracking and correlations
  - E2E encryption with non-repudiation
- Enable rich applications, make Matrix a general purpose platform for open and better nextgen Internet

Introducing Decentralised Identity to Matrix ?

- Some of great ideas already discussed, e.g.
  - Decentralized identity SPEC-458: https://github.com/matrix-org/matrix-spec/issues/203
  - Non-interactive E2EE Account Verification #1778 https://github.com/matrix-org/matrix-spec/issues/1778
  - Decentralised user accounts #246, Portable accounts: https://github.com/matrix-org/matrix-spec/issues/246
- And that’s only scratching the surface . . .

Introducing Decentralised Identity to Matrix ?

- Is this a good idea for Matrix users and Matrix ecosystem?
- What is the right way to approach this ?
  - Early experimentations ?
  - Spec processes ?
  - Any interests in EUDI, mDL, VC, OpenWallet etc.?
  - Any interests in exploring applications beyond messaging ?
  - AI content authenticity ? Agents ?
  - Super apps ?
- Open discussions

Thanks

Wenjing Chu:
@firegod0:matrix.org
https://www.linkedin.com/in/wenjingchu/