🔖 omigroup / **omigroup**   Public

`<>` Code   ⊙ Issues 38   ⑂ Pull requests   💬 **Discussions**   ▦ Projects 2   ⋯

Open Questions About Homeserver/Wallet Privacy #14

mrmetaverse started this conversation in **General**

mrmetaverse on Apr 20, 2021   Maintainer

Hey all, I wanted to add some interesting questions that have cropped up in the #OMI-Open-Inventory channel on Discord.

Shaw: "I would like to see a zero knowledge scenario.
User syncs data with server A to local storage.
User goes to server B and gives permissioned access to data in local storage
Server B makes a hash of what is being claimed and sends it to server A for comparison
Server A confirms or denies it-- on denial the user can resync their local storage and try again
This way no user data ever flows between servers, in fact it isn't possible."

Robert: _"I'd love a more detailed proposal for this. I like the idea, but I'm not so sure that we can get adoption of zero knowledge APIs. Currently my thoughts are that a trusted home server is your protected data storage. You grant permission to other servers/applications to access partial views of that data. Scopes would be pretty granular.

Things like friends list access could even require a separate more serious permission method. Like, I would only want to give that permission to a browser extension / native app. It's more my client rather than an a third party application that gets access to a scoped view of my data.

This is a bigger discussion that we need to have as a group though. Who do we want to implement homeservers? Who do we want to integrate this into their app? What data do they need? What level of privacy can we build in without making it such that nobody will adopt it because it doesn't fit with their existing application's architecture?

You've also mentioned doing most of this work client-side. I'd love a view into what that would look like. I like this idea a lot, but need to see how it compares with a primarily homeserver-based implementation.

I'm super curious about this and have a bunch of questions. How does my wallet receive messages when I'm offline? Where does it store data? How does it sync between devices? Do we need a homeserver for this implementation? Is a homeserver just used for storage of encrypted data?"_

↑ 2

1 comment

Oldest | Newest | Top

jorgenbuilder　on Aug 27, 2021

Software canisters on the Internet Computer blockchain might be a good medium for home servers.

↑ 1

0 replies

Category

💬 **General**

Labels

None yet

2 participants