Hubs and Agents Notes
Adrian Gropper - July 25

I completely agree with the Hubs and Agents paper. Here are some of the protocol implications.

The phrase I would like to focus on is:
"In keeping with the hub's focus on data management, hubs are not deeply trusted or deeply informed about their owner's behavior. They don't take actions on the owner's behalf, and they don't hold keys."

Is the *"owner"* above the data subject, a service provider, or both? The data subject would be Alice, the person that controls her agent. The service provider would be any entity other than the data subject including a storage service or a lab that generates data about the subject. It seems desirable to support both kinds of owners.

The principle of *"not deeply trusted or informed"* conforms to the GDPR framing of a data processor vs. data controller. This is valuable because service providers as owners can avoid the privacy costs and risks associated with the data controller role. When the owner is the subject, the issue of trusted or informed is moot.

The principle of hubs being potentially redundant and their architecture transparent to the subject is also valuable. This begins to drive the relationship between a DID service endpoint pointing to hubs vs. agents. If the agent endpoint of a data subject is responsible for tracking the redundant hubs, life is easy. If the hubs themselves or their contents can be replicated independently of the agent, then the protocols get more complex. Content addressable storage a la IPFS could manage some of this complexity, but beyond that, adding a permissions function to the hub splits control between the hub and agent and complexity grows.

In line with the Hubs and Agents paper, the simplest way to structure the protocols is to delegate the evaluation of Bob's credentials to the agent and issue a token to Bob for presentation to the hub. In this scenario, Bob presents credentials and the information request to Alice's DID service endpoint and, if approved, Bob receives a token and the address of a hub to present it. There is no particular reason for the hub to have a DID or a service endpoint in Alice's DID. Let's call this Plan A.

Plan A puts all privacy-related issues in the agent. Service providers can still own or rent hubs but they need to register them with Alice's agent as part of the subject registration step. Alice's DID can be used to authenticate to the service provider and also implicitly leave behind her agent as a DID service endpoint. The service provider may not know anything about Bob or Bob's credentials until such time that Bob brings a bearer token signed by Alice's agent. This reduces the service provider's liability as well as their computing costs. This also extends Alice's self-sovereign technology beyond SSI to include her self-sovereign agent.