Agents, Identity Hubs, and Secure Data Hubs

A naive, likely flawed, but hopefully neutral introduction

About this presentation

- There are 3 proposed self-sovereign approaches, solving some subset of problems like the following:
  - Data/credential storage
  - Key management
  - Credential exchange protocols
- Approaches
  - Aries Agents
  - DIF Identity Hubs
  - Digital Bazaar Secure Data Hubs
- We'll also briefly mention other technologies like Solid Pods and IPFS

About this presentation, continued

- We'll attempt a neutral overview
  - How? I knew little, but wanted to learn more. I like/dislike aspects of all of them :)
  - I tried to make sense out of specs, and here we are
- This is an educational session only
  - Goal: Get CCG up-to-speed in different approaches to these critical "after DID" problems
  - Foundation for subsequent discussions in the SSI communities
  - Goal is to set foundation for interoperability
- Experts in each have been invited to give feedback
  - On the slide deck
  - During this presentation to provide clarifications, answers to Q&A

Flow of this presentation

- High level context
  - Alignment work so far, what problems are they trying to solve
- Brief intro to each
- Q&A, Discussion
  - Some Discussion Points called out
- Resources for further reading
- This conversation will continue...

High level context

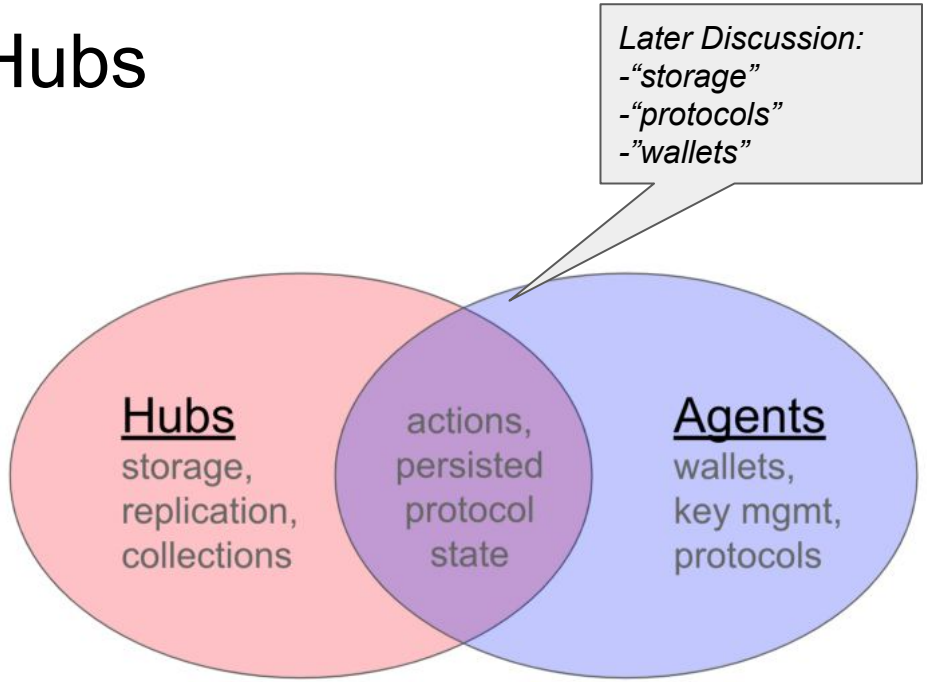
Alignment work done so far, problems they are solving

Agents and Identity Hubs: current alignment efforts

- DIF Identity Hubs
  - “Services that help an identity owner manage data and interact through it”
- Aries/Sovrin Agents
  - ”Pieces of software that hold delegated keys, exchange digital credentials, and otherwise do an identity owner’s bidding”
- Work has already been done to align them, effort started at IIW
- Led by Daniel Hardman, Daniel Buchner, and Sam Curren
- Output is this Medium post: https://medium.com/decentralized-identity/rhythm-and-melody-how-hubs-and-agents-rock-together-ac2dd6bf8cf4
  - Basis of comparison to follow

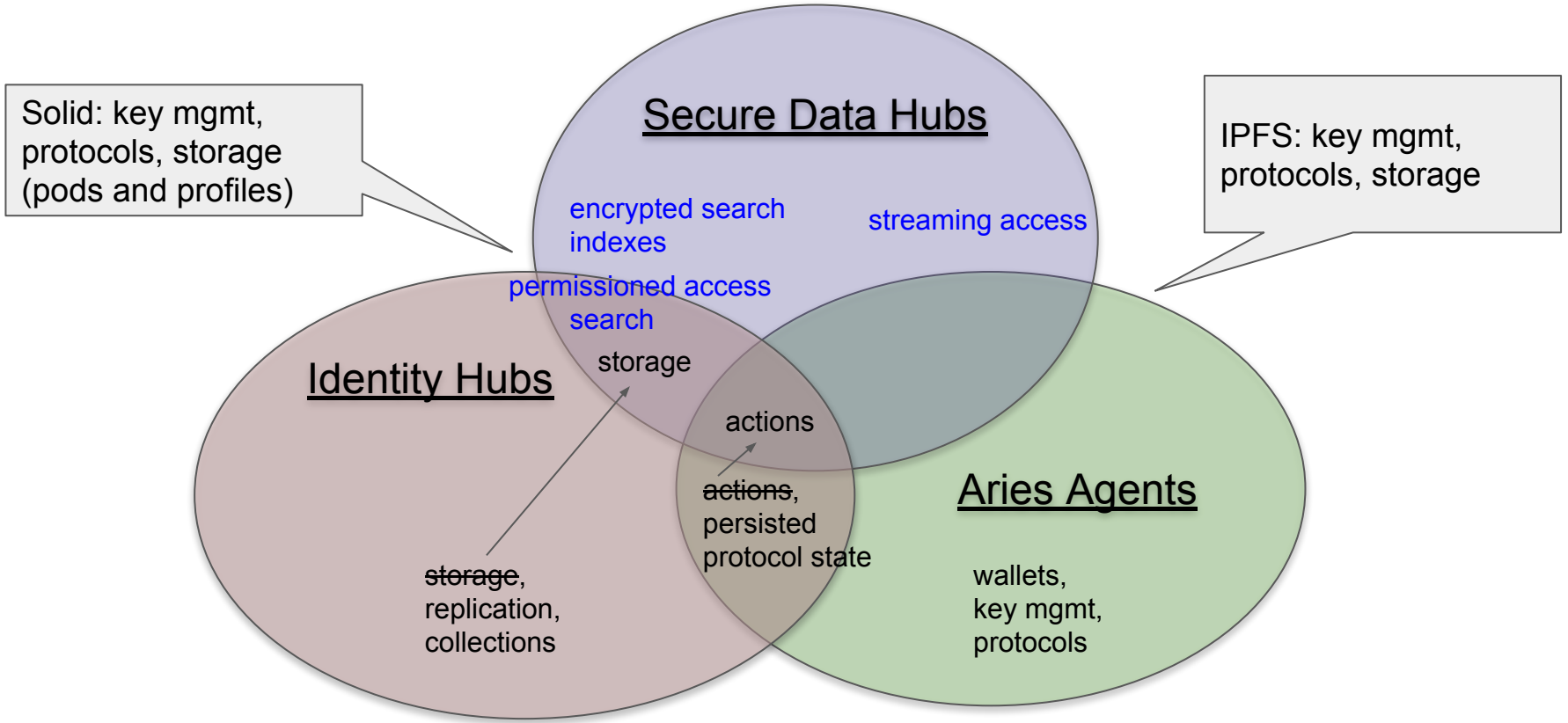
Aries Agents and Identity Hubs

- Identity Hubs
  - Data-oriented
  - Focus is data management; does not take action on user's behalf
- Aries Agents
  - Flow-oriented
  - Takes actions on owner's behalf
  - Protocols reference: https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0003-protocols/README.md.



Source: https://medium.com/decentralized-identity/rhythm-and-melody-how-hubs-and-agents-rock-together-ac2dd6bf8cf4

Aries Agents, Identity Hubs, and Secure Data Hubs



Brief introduction to each

DIF Identity Hubs: Quick Overview

- Allow secure storage and sharing of data
- Hub is a datastore containing semantic data objects at well-known locations
- Requirements
  - Syncing data between instances
  - Serialization
- Operations modeled as commits (like git, but strategy-agnostic)
- “Collections” for search and indexing
- Uses SSI stack
  - DID Auth for Authentication
  - Universal Resolver
- API
  - Write Request & Response
  - Object Read Request & Response
  - Commit Read Request & Response
- Hybrid ACL/OCAP Model (see Identity Hub Permissions and Capability-Based Access Control)
- Hub request is JWE (Description)

Secure Data Hubs: Quick Overview

- Highly focused on storage (can be building block for Identity Hubs / Solid Pods)
- Always encrypted storage (encrypted in transit and at rest)
- Structured Data and Metadata (JSON-only or can do JSON-LD semantics)
- Authorization Method Agnostic (OAuth, zcaps, ACLs)
- Streams
  - For large files > 1 MB (by default, but size is configurable)
  - Described using structured docs, with hashlinks to sharded encrypted content
- Indexing: privacy-aware document searching via encrypted search schemes
- API
  - Discover service endpoints
  - CRUD Data Hubs, Documents, Streams, and Encrypted Indexes
  - Query/Search Encrypted Documents
- JSON (today), CBOR (future)
- JWE (today), CWE (future)

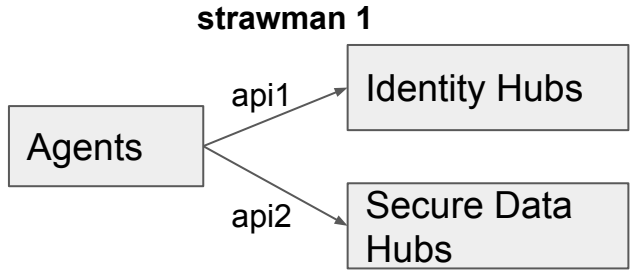
Agents: Quick Introduction

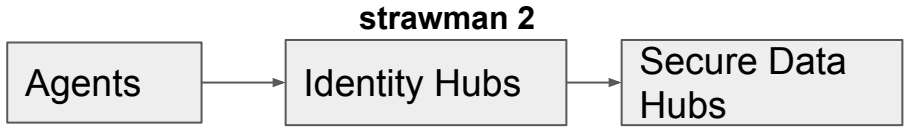
- Responsibilities
  - Acts as a fiduciary on behalf of an identity owner
    - or, for agents of things like IoT devices, pets, and similar things, a single controller
  - Holds cryptographic keys that uniquely embody its delegated authorization
  - Interacts using interoperable DID Comm protocols
- Examples
  - A mobile app that Alice uses to manage credentials and to connect to others is an agent for Alice.
  - A cloud-based service that Alice uses to expose a stable endpoint where other agents can talk to her is an agent for Alice.
  - A server run by Faber College, allowing it to issue credentials to its students, is an agent for Faber.

Q&A and Discussion

Discussion points

- Opinion: Agents easiest to tease apart
- But how do they all fit together?
  - See oversimplified strawman 1 and 2 (not actual proposals)
  - Better approach: Tease apart goals/responsibilities of each approach
- But...
  - Fuzzy terminology/concepts (e.g. “wallet”)
  - Further refinement of SSI Stack
- Reconciling the hub approaches
  - ACLs/OCAP
  - Commit-oriented





References and Further Reading below

- Data Hubs: https://msporny.github.io/data-hubs/
- Identity Hubs
  - https://github.com/decentralized-identity/identity-hub/blob/master/explainer.md
  - https://github.com/decentralized-identity/identity-hub/blob/master/docs/authentication.md
- Agents
  - Concepts: https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0004-agents
  - Protocols: https://github.com/hyperledger/aries-rfcs/blob/master/concepts/0003-protocols/README.md
- Analysis/Comparisons
  - Identity Hubs Capabilities Perspective (RWOT5 paper) https://www.dropbox.com/s/1nn9h14cyf2lh0s/identity-hubs-capabilities-perspective.pdf?dl=0
  - Agents vs Hubs: https://medium.com/decentralized-identity/rhythm-and-melody-how-hubs-and-agents-rock-together-ac2dd6bf8cf4
  - DIF Self-sovereign Identity Stack: https://medium.com/decentralized-identity/the-self-sovereign-identity-stack-8a2cc95f2d45

Backup Slides

Solid

- Concepts: Resources and Containers
- Reading/Writing
  - Linked Data Platform
  - CRUD operations on resources and containers
  - REST, WebSockets APIs
- Profile: Keys
- Pod: Personal data store
- Authentication
  - Solid "...requires *cross-domain*, de-centralized authentication mechanisms not tied to any particular identity provider or certificate authority"
  - WebID-TLS
  - WebID-OIDC
- Authorization/Access Control
  - Web Access Control

Source: https://github.com/solid/solid-spec