PERSONAL DATA VAULTS

The TrustChain Super App offers a great platform to host decentralized applications built on top of the IPv8 peer to peer networking protocol and the TrustChain pair-wise ledger. Currently off-chain storage is managed by each application with separate local databases. This means that while data is stored within the ecosystem of the Super App, each application's data can only be used within that application. This restricts applications from sharing off-chain data and limits the potential of creating a truly all-in-one app experience. This traditional approach means that if you make an information rich application that integrates data from external sources, you have copies of the same data in different locations. Users that want to update or delete their data has to do so in multiple locations. A trivial solution seems to be a single data storage, managed by the user, structured in a way that makes it generally accessible.

Our proposal is to implement Personal Data Vaults (PDV) within the Super App. The data vault serves as a secure storage for personal data that can be accessed by multiple applications. PDVs allow users to have more control over their personal data by controlling what is shared with each application [2], even services outside of the Super App ecosystem. Data management is simplified by having to update or delete in a single place. This perfectly complements the Self-Sovereign Identity framework on the platform. To make PDVs more useful, stored data will be structured as Linked Data. An essential part of the Semantic Web, Linked Data structures form a Web of Data that connects data from different domains such as people, companies, books, songs, essentially any named category. The Web of Data opens up new possibilities for domain-specific applications as it enables access to more data sources [1].

The goal of this project is to set a template for social applications that are able to access, aggregate and use data from the PDV's of different users according to the access control rules set by each user. We take inspiration from the Solid platform [3]. Solid deploys personal online datastores (pods), which are essentially data vaults with a access control mechanism that defines how social web applications can read from and write to the pods.

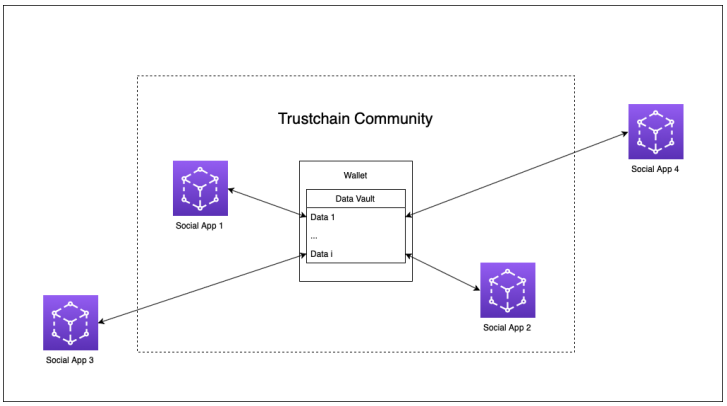

Figure 0.1: Personal Data Vault accessible from within the Super App and from outside.

ACCESS CONTROL

Attribute-based access control (ABAC) will be used to manage access to data in PDVs. Different data items will have different access policies defined as a set of attributes that the user must posses.These attributes are presented as verifiable credential that will be matched against the access policy of the requested data. The verifiable credential is constructed from attestations contained in the user's wallet. To comply with the access policy in 0.2, the user must present a credential that contains 18+ attestation and either a TU Delft student attestation or a "friend" attestation. The first two credentials are not issued by the controller of the PDV but can still be used in the access policy. The "friend" credential is a self-issued credential by the controller of the PDV that has an analogous function to accepting a follow request on social media.

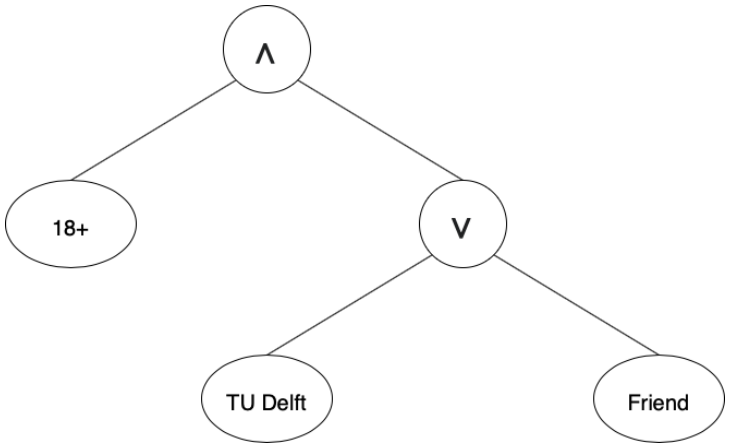

Figure 0.2: Example access policy.

Using the Trustchain wallet for access control allows to use the existing DID infrastructures and protocol including the revocation mechanism.

SCALABILITY

Because PDVs are hosted on personal smartphones, there is a limited capacity for handling incoming requests for data in the PDV. A possibility would be to allow external hosting of PDVs. In that case a PDV can be hosted on an external server, either private or by a service provider, and accessed from any device. This means that a user can have multiple (backups) PDVs and can switch between them seamlessly.