TrustVault: A privacy-first data wallet for the European Blockchain Services Infrastructure

Sharif Jacobino
Department of Software Technology
Distributed Systems
Faculty of Electrical Engineering, Mathematics & Computer Science
Delft University of Technology

Johan Pouwelse
Department of Software Technology
Distributed Systems
Faculty of Electrical Engineering, Mathematics & Computer Science
Delft University of Technology

I. Introduction

Internet users today have very little control over where and how their data is stored and used online. Big Tech companies store gigabytes of data about you, and know which online services you use [1]. User data is an extremely valuable asset and is the main source of income for these companies. Public and policy trust in Big Tech has been breaking down in recent years (also called the ”techlash”) following major scandals, rampant misinformation campaigns, and a perceived consolidation of power [2]. There are various movements aiming at halting the power of Big Tech and giving back control to the users. These movements are powered by technologies like blockchains and self-sovereign identity which promise to improve the way we interact online services and with each other.

The European Commission wants to improve the way citizens, businesses and public administrations share information and trust each other, and simplify verification processes for cross-border services using blockchain technology [3]. Its proposed solution to reduce our reliance on Big Tech is the European Blockchain Services Infrastructure (EBSI). As at May 2022, there was €57 million in funding for large scale EBSI trials [4]. Each European citizen will have its own digital wallet to interact with EBSI.

This work aims to accelerate the European identity and data self-sovereignty movement by providing a EBSI-certified data wallet with advance data sharing capabilities. Citizens can issue credentials within the EBSI framework and define access policies that are automatically enforced for their data based on these credentials. This fine-grained access control for both read and write operations to the user's data wallet gives the user even more control over their data. Our approach preserves user privacy by enabling selective disclosure of only the credentials necessary to satisfy an access policy.

Using verifiable credentials as a basis for attribute-based access control for personal data storage is a novel concept that extends the notion of self-sovereignty over personal identity to personal data. The question that this work aims to answer is: How can a secure personal data storage be created, that gives granular access control to the owner based on attributes extracted from verifiable credentials on the European Blockchain Services Infrastructure. This research question is divided into the following sub-questions:

- How can access to data in a personal data storage be controlled granularly using policy rules?
- How can self-issued credentials be used as access tokens in a privacy-preserving manner?
- How does a privacy-first data wallet add value to EBSI?

The result of this work is called a proof of concept called TrustVault: A privacy-first data wallet deployed on the TrustChain Super App. TrustVault builds upon the concept of personal data Pods developed by the Solid team [5]. TrustVault is hosted on the user's smartphone rather than in the cloud. TrustVault also consists of a EBSI conformant SSI wallet able to issue and receive credentials to and from the EBSI network. Besides EBSI credentials, credentials from TrustChain's internal SSI framework can also be used as access tokens. In this proof of concept photos can be grouped together with access policy rules on photo and on group level. Peers on the TrustChain network can share photos using the IPv8 peer-to-peer protocol.

In section II related work is discussed. In section III we detail the different components and interactions of TrustVault.

II. Related Work

A. Solid

Solid is a protocol developed at MIT that let's people store their data securely in decentralized data stores called Pods

[6]. Pods are personal web servers that can store any kind data. The Pod owner has granular control over who has access to the data. Solid uses Access Control Lists (ACL) to grant and revoke access to any slice of data contained in a Pod to individuals, organizations, or applications.

B. European Blockchain Services Infrastructure

The European Blockchain Services Infrastructure (EBSI) is a distributed network that runs a public blockchain to host public and private services that want to leverage the benefits of blockchain technology. The main services that EBSI aims to facilitate are:

1) Notarization: using the blockchain to make digital audit trails and automate compliance checks.
2) Diplomas: giving citizens control over their educational credentials and lowering the cost of verifying documents.
3) European Self-Sovereign-Identity Framework (ESSIF): serve as a verifiable registry and communication channel for an SSI framework across Europe.

Most relevant to this work is ESSIF, as it serves as the network used to issue and receive verifiable credentials. TrustVault users can issue credentials to other participants in the network and receive and verify credentials from other participants using EBSI.

C. Attribute-Based Credentials

Attribute-based access control (ABAC) is an access control model that controls access to objects by evaluating rules against attributes of entities [7]. This allows for more precise access control because of the large set of possible combinations of attributes and consequently large set of possible rules for policies, only limited by the available set of attributes.

D. Tribler IPv8

IPv8 is a peer-to-peer communication protocol developed by Tribler for private and authenticated communication. IPv8 abstracts away physical addresses and allows peers to be identified by their public keys[8][9].

III. Design

IV. Evaluation

V. Discussion

VI. Conclussion and Future Work

References

[1] D. Curran. (2018) Are you ready? Here is all the data Facebook and Google have on you. [Online]. Available: https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy

[2] K. Birch, D. Cochrane, and C. Ward, "Data as asset? the measurement, governance, and valuation of digital personal data by big tech," *Big Data & Society*, vol. 8, no. 1, p. 20539517211017308, 2021.

[3] European Commission. (2022) European Blockchain Services Infrastructure. [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

[4] ——. (2022) EBSI Grants. [Online]. Available: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EBSI+Grants

[5] T. Berners-Lee. Solid. [Online]. Available: https://solidproject.org

[6] E. Mansour, A. V. Sambra, S. Hawke, M. Zereba, S. Capadisli, A. Ghanem, A. Aboulnaga, and T. Berners-Lee, "A demonstration of the solid platform for social web applications," in *Proceedings of the 25th International Conference Companion on World Wide Web*, ser. WWW '16 Companion. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2016, p. 223–226. [Online]. Available: https://doi.org/10.1145/2872518.2890529

[7] V. C. Hu, D. R. Kuhn, D. F. Ferraiolo, and J. Voas, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.

[8] Tribler. IPv8. [Online]. Available: https://github.com/Tribler/kotlin-ipv8

[9] ——. IPv8. [Online]. Available: https://github.com/Tribler/py-ipv8