Decentralized Identities for Self-sovereign End-users (DISSENS)

Open Identity Summit 2021

Martin Schanzenbach

1.6.2021

Objectives

- Combination of user-centric, privacy-friendly personal data sharing and payments:
  - Self-sovereign identity system **re:claimID** eliminates need for Web accounts.
  - Privacy-friendly payment system **GNU Taler** suitable for Digital Euro.[1]

[1] David Chaum et al, "How to Issue a CBDC", Swiss National Bank, 2021; `https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03`

Objectives

- Combination of user-centric, privacy-friendly personal data sharing and payments:
  - Self-sovereign identity system **re:claimID** eliminates need for Web accounts.
  - Privacy-friendly payment system **GNU Taler** suitable for Digital Euro.[1]
- Unique benefits over existing solutions:
  - No gatekeepers; no vendor lock-in.
  - Support for non-interactive business processes.
  - Scalability and sustainability.

[1] David Chaum et al, "How to Issue a CBDC", Swiss National Bank, 2021; `https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03`

Objectives

- Combination of user-centric, privacy-friendly personal data sharing and payments:
  - Self-sovereign identity system **re:claimID** eliminates need for Web accounts.
  - Privacy-friendly payment system **GNU Taler** suitable for Digital Euro.[1]
- Unique benefits over existing solutions:
  - No gatekeepers; no vendor lock-in.
  - Support for non-interactive business processes.
  - Scalability and sustainability.
- Integration in a popular e-commerce framework (WooCommerce) as pilot
  - Use of OpenID Connect standard for interoperability.
  - GNU Taler plugin for usable one-click account-less payments.
  - Academic institutions as credential issuers highlighting federation capabilities.

[1] David Chaum et al, "How to Issue a CBDC", Swiss National Bank, 2021;
`https://www.snb.ch/en/mmr/papers/id/working_paper_2021_03`

Requirements and Blockchains

Neither **reclaimID**[2] nor **GNU Taler**[3] are built on top of a blockchain technologies.

[2] https://reclaim.gnunet.org/
[3] https://taler-systems.com/

Requirements and Blockchains

SSI systems and **privacy-friendly payments** do not require a blockchain!

Requirements and Blockchains

- SSI requirements:
  - Public/private-keys.
  - Users, issuers and verifier.
  - Decentralized directory ("verifiable data registry" – W3c DID).

[4] https://medium.com/coinmonks/storing-on-ethereum-analyzing-the-costs-922d41d6b316

Requirements and Blockchains

- SSI requirements:
  - Public/private-keys.
  - Users, issuers and verifier.
  - Decentralized directory ("verifiable data registry" – W3c DID).

- Privacy-friendly payments requirements:
  - Payer privacy/anonymity.
  - Auditable income transparency.

[4] https://medium.com/coinmonks/storing-on-ethereum-analyzing-the-costs-922d41d6b316

Requirements and Blockchains

- SSI requirements:
  - Public/private-keys.
  - Users, issuers and verifier.
  - Decentralized directory ("verifiable data registry" – W3c DID).

  $\Rightarrow$ Blockchains are **notoriously bad** for data storage.

  "Store data permanently on Ethereum is extremely expensive. It has no sense to use Ethereum to store data. It should store only the required data to work properly and delegate the storage to other solutions"[4]
- Privacy-friendly payments requirements:
  - Payer privacy/anonymity.
  - Auditable income transparency.

[4] https://medium.com/coinmonks/storing-on-ethereum-analyzing-the-costs-922d41d6b316

Requirements and Blockchains

- SSI requirements:
  - Public/private-keys.
  - Users, issuers and verifier.
  - Decentralized directory ("verifiable data registry" – W3c DID).

  ⇒ Blockchains are **notoriously bad** for data storage.

  "Store data permanently on Ethereum is extremely expensive. It has no sense to use Ethereum to store data. It should store only the required data to work properly and delegate the storage to other solutions"[4]
- Privacy-friendly payments requirements:
  - Payer privacy/anonymity.
  - Auditable income transparency.

  ⇒ This is exactly what blockchains do **not** provide.

  "[Bitcoin is a]boon for surveillance" – Michael Morell, Former CIA director

[4] `https://medium.com/coinmonks/storing-on-ethereum-analyzing-the-costs-922d41d6b316`

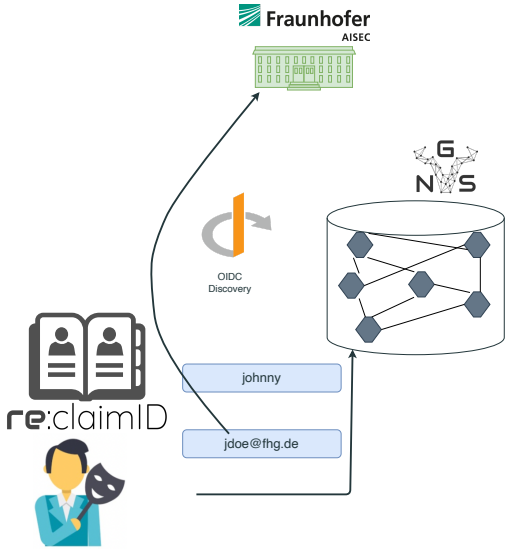
Requirements and Blockchains

Some business processes (billing, fulfillment) happen **after** user interaction.

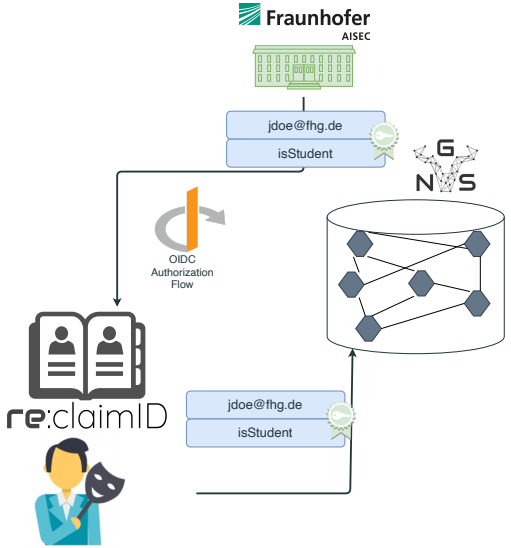
- Persisting information creates liability and requires strong protection.
- Permanent connectivity from user device to service(s) does not scale.
- Exposed endpoints on user devices for data retrieval is a security (and connectivity) nightmare.

$\Rightarrow$ Scalable and secure decentralized storage for user information.

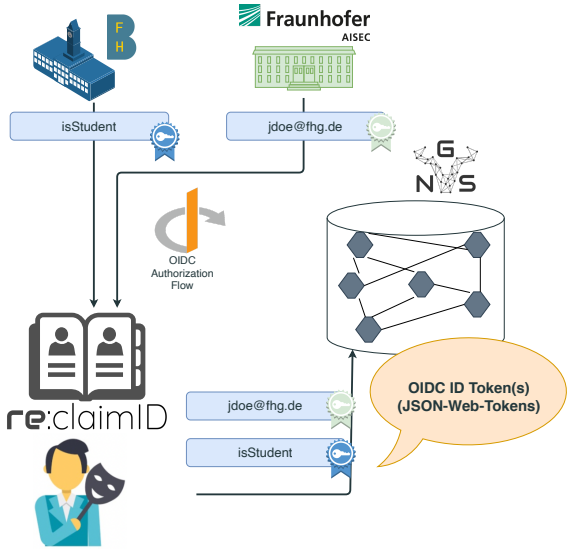
Identity and personal data management



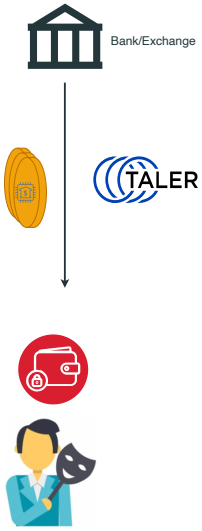
Third-party credentials I



Third-party credentials II

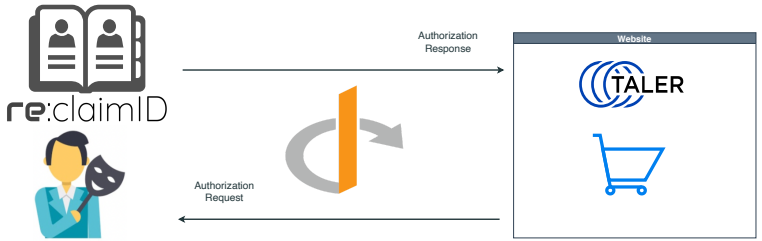


Coin withdrawal



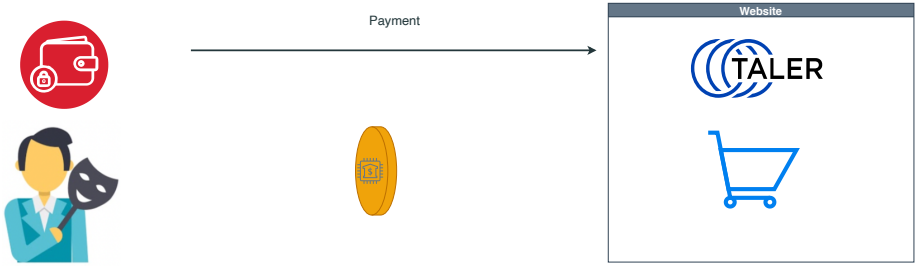
Login and authorization

Login and authorization

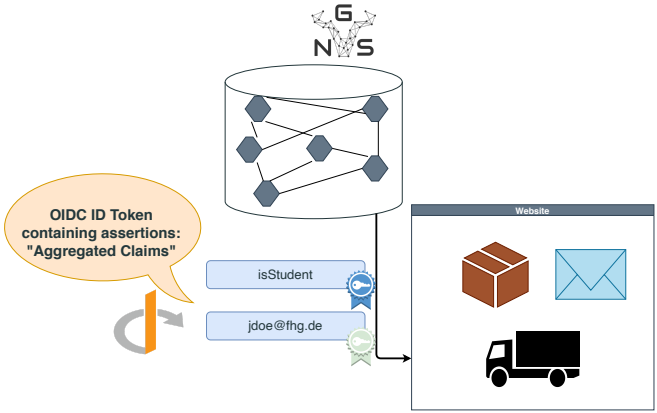


Payment

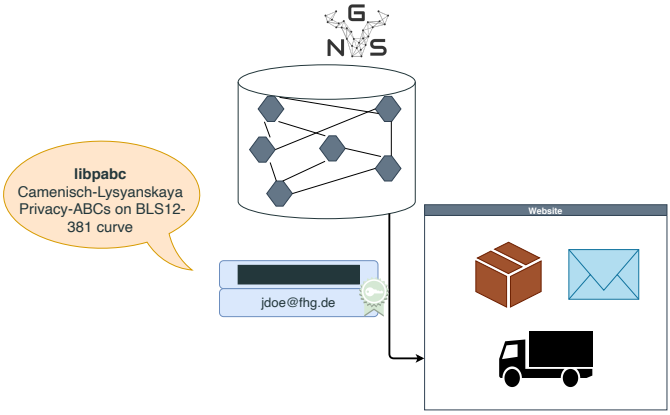
- Payer anonymity.
- Payee accountability.



“Offline” attribute retrieval



Selective disclosure of credentials



Future Work

- Continuous integration of/into emerging standards (DID/SIOP).
- Improvement of underlying P2P architecture.
- Integration of advanced trust management mechanisms.

Questions?

https://reclaim-identity.io

https://taler.net

https://gnunet.org

schanzen@aisec.fraunhofer.de
6665 201E A925 7CC6 8FDE 77E8 8433 5131 EA3D ABF0
– or –
schanzen@gnunet.org
3D11 063C 10F9 8D14 BD24 D147 0B09 98EF 86F5 9B6A

References

1. Martin Schanzenbach. *Towards Self-sovereign, Decentralized Personal Data Sharing and Identity Management*. **Technische Universität München (Dissertation)**, 2020
2. Martin Schanzenbach, Georg Bramm, Julian Schütte. *reclaimID: Secure, Self-Sovereign Identities Using Name Systems and Attribute-Based Encryption*. **17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom)**, 2018
3. Matthias Wachs, Martin Schanzenbach and Christian Grothoff. *A Censorship-Resistant, Privacy-Enhancing and Fully Decentralized Name System*. **13th Intern ational Conference on Cryptology and Network Security**, 2014.