WIDE

Web3 Identity for
DAOs and Education

Funded by
the European Union

April 9, 2024

2nd International Workshop on Trends in Digital Identity (TDI 2024)

Aggregating Digital Identities through Bridging.

An Integration of Open Authentication Protocols for Web3 Identifiers.

Ben Biedermann

2nd International Workshop on Trends in Digital Identity (TDI 2024)

April 9, 2024

Contents

The Problem

- Self-Sovereign Identity (SSI) protocols require cryptographic key management in addition to Web3 key pairs.
- Only SSI edge wallets allow using verifiable credentials (VCs) in a privacy-preserving way (Reed et al., 2021).
- Web3 is perceived as discrete sector and distinct user experience. In reality, Web3 user journeys intermingle with Web2.
  - A user may authenticate with a dApp using their Web3 identifier, input user and/or KYC information, access and share information on Google Workspace, and manually confirm their Web3 address for receiving payment.
- Global Virtual Asset Service Providers (VASPs) continue to use existing identification rails.

The EUDIW does not help Web3 professionals KYC at VASPs for off-boarding their crypto.

A Proposed Solution

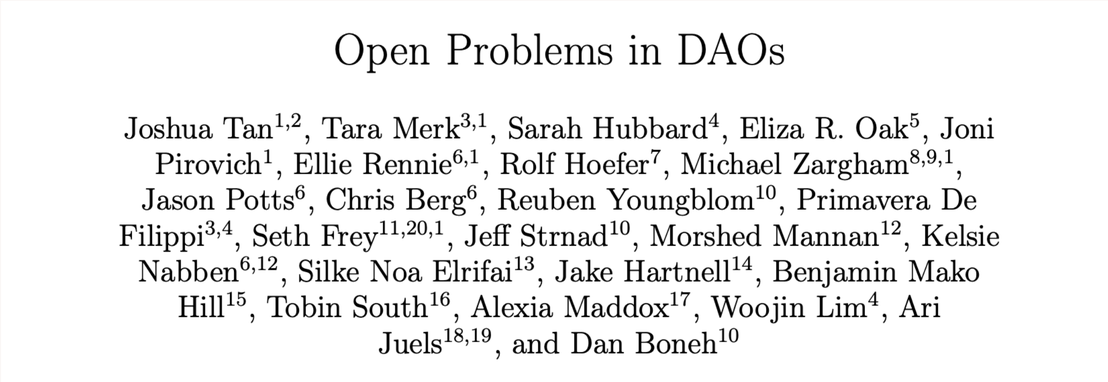
- A wallet-like architecture that aggregates, encrypts, and attests to credentials from various issuers by integrating a multitude of digital identity protocols.
  - Users request their data from a resource server using OAuth 2.0;
  - Request export their data from an EUDIW using verifiable presentations according to OID4VP;
  - Aggregate Web3-specific data by querying the blockchains and subgraphs.
- The data is encrypted and signed by the user with their Web3 public key.
- Encrypted credentials are stored on the server.
- A history of credential uploads and presentations are logged in a smart contract.

How did we get here?

- DAOs rely on blockchain-based automated data storage mechanisms and smart contracts, but risk becoming technocracies.

- “How can plutocracy or sybil attacks be avoided, when common “one-token-one-vote" mechanisms mean that wealthy users can buy a disproportionate number of tokens and subsequently gain a disproportionate amount of voting power?”

  (Tan et al., 2023, pp.48)



Open Problems in DAOs

Joshua Tan[1,2], Tara Merk[3,1], Sarah Hubbard[4], Eliza R. Oak[5], Joni Pirovich[1], Ellie Rennie[6,1], Rolf Hoefer[7], Michael Zargham[8,9,1], Jason Potts[6], Chris Berg[6], Reuben Youngblom[10], Primavera De Filippi[3,4], Seth Frey[11,20,1], Jeff Strnad[10], Morshed Mannan[12], Kelsie Nabben[6,12], Silke Noa Elrifai[13], Jake Hartnell[14], Benjamin Mako Hill[15], Tobin South[16], Alexia Maddox[17], Woojin Lim[4], Ari Juels[18,19], and Dan Boneh[10]

Definitions

Self-Sovereign Identity (SSI)

SSI Practitioners

- Recently, a new identity model known as decentralized identity — popularly called “self-sovereign identity” (SSI) — has emerged. It is important to note that the definition of self-sovereign identity (SSI) is still a work in progress in the industry. (Avellaneda et al., 2019)

- “Self-sovereign identity is a digital identity philosophical perspective that emerged based on providing users with ownership and control of their digital identity information.” (Boysen, 2021)

Observers

- “SSI is still only loosely defined. [...] In essence it is an identity management system which allows individuals to fully own and manage their digital identity.” (Mühle et al., 2018)

- “SSI [...] refers to a new IMS whereby the user should fully own his/her identity data without any intervention from an outside administration.” (Dib & Toumi, 2020)

Critics

- “The conception of a self-sovereign identity or a sovereign individual did not emerge from philosophy, legal theory, or political science texts; instead, it came from blog posts, magazines, and Internet forums of software developers. Such forums defined SSI as a set of ethical principles and an idealistic vision in which individuals become ‘rulers of their own identity’ (Allen, 2016)” (Weigl et al., 2022)

Decentralised Identity

Positive Definition

- “[D]ecentralized alternatives such as Pretty Good Privacy (PGP) crypto systems, which allowed secure signing and encryption [are] based on “webs of trust” among individuals, rather than a central authority.” (Weitzner, 2006)

- “[D]ecentralized systems such as OpenID give complete control over creating the identifier to the user (who just mints a URI). [...] Notably, the identity provider is virtually uninvolved with the nature or quality of assertions others make about the identity holder.” (Weitzner, 2007)

Negative Definition

- “As a distinction to decentralized identity systems, the SSI paradigm has additional requirements that ensure the users’ sovereignty of their identity and the storage-control of the associated confidential data linked to their identity (Naik and Jenkins, 2020).” (Laatikainen et al., 2021)

WIDE

“A Sybil attack attempts to target user reputation features in a peer-to-peer network system through forging multiple identities and acting as several nodes within the system.”
(Reynolds & Irwin, 2017)

“DAOs are organizations whose origins are the web, and whose rules and terms of membership are orchestrated by code-backed protocols, rather than large institutions and ‘middleman’ organizations.” (Sinha et al., 2021)

Semantic Web vs. Web3

ben@wid3.org

The Pragmatic Meaning(s) Decentralised Identity

(Lai et al., 2023)

- **Semantic Web (2006 -)** “enhances data resource access efficiency through data reuse and interlinking between websites, mainly involving P2P technology (D. J. Weitzner, 2007) and Resource Description Framework (RDF)”;

- **Web3 (2014 -)** “Web3 is that it can realize a serverless internet, that is, an internet where users generate content that belongs to the users themselves”.

Decentralised Identity for the Semantic Web

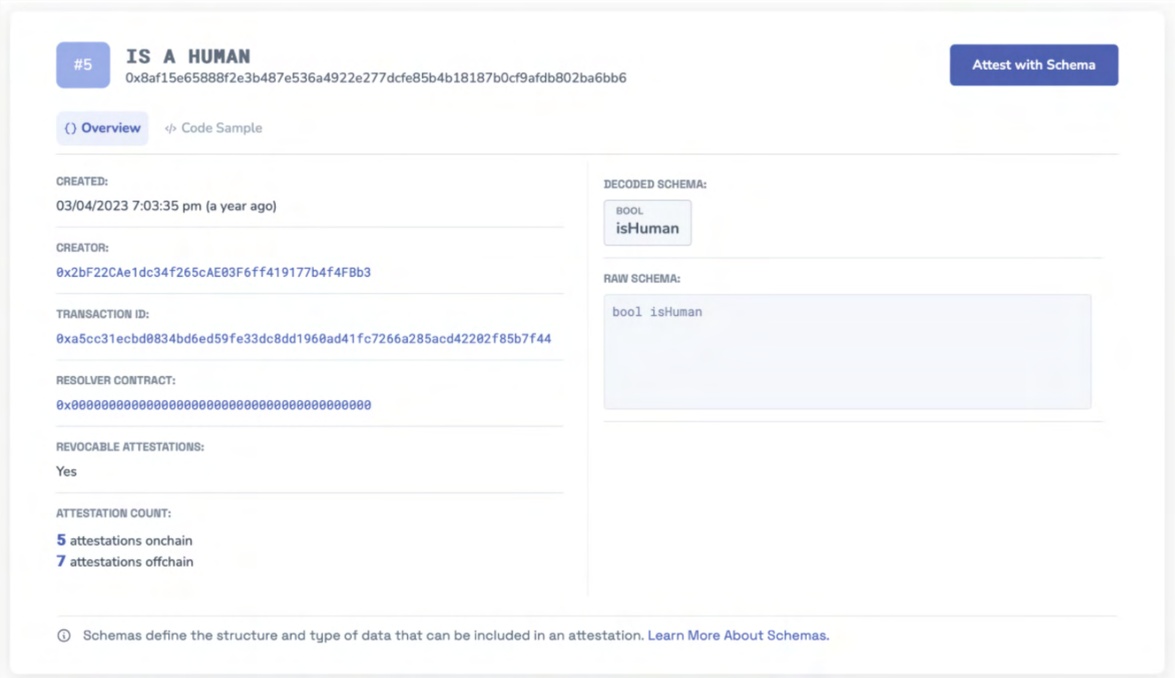
(Miller et al., 2007)

- OIDC-based “decentralised identifiers”.
- MicroID was referred to as *decentralised* because it is generated through client-server interactions and does not rely on centralised PKIs.
- It is not *decentralised* in the Web3-meaning of decentralisation, as it requires OAuth and a conventional server architecture.

```
The hash is generated as follows (note: the line break in the third
example is included only for the sake of readability):

sha1(
     sha1(xmpp:stpeter@jabber.org)
     +
     sha1(https://www.xmpp.net/)
    )

sha1(
     afa6353518f818af2f036da336c3097dedc00dee
     +
     3115de01ebfa34a34314060b5f30038b0fa359f8
    )

sha1(
afa6353518f818af2f036da336c3097dedc00dee
3115de01ebfa34a34314060b5f30038b0fa359f8
    )

6196ea6709be2a4cbdf2bc0cfaeac491f2fb8921

Thus the issued MicroID is:

xmpp+https:sha1:6196ea6709be2a4cbdf2bc0cfaeac491f2fb8921
```

Decentralised Identity for Web3

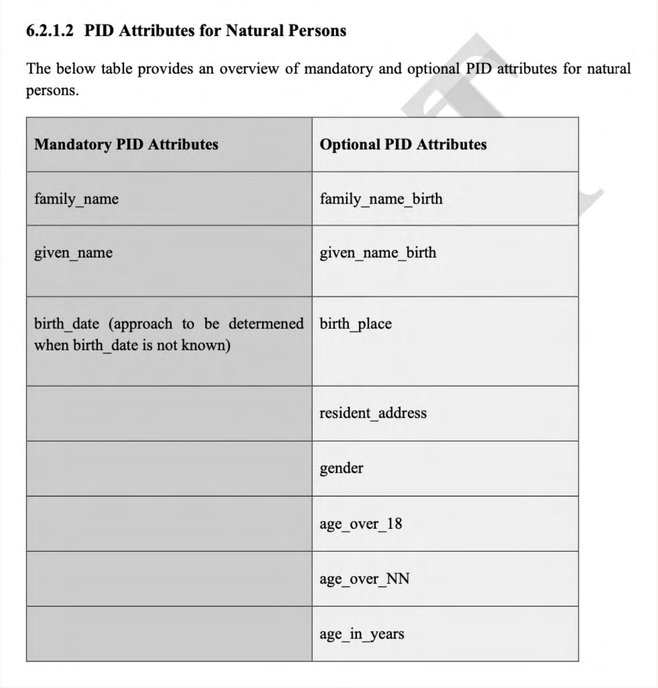
- Today, decentralised identity focuses on Web3 attestations for long-lived and pseudonymous identifiers on public-permissionless blockchains.
- Permissionless schema registries allow for the registration of schemas and their issuance to EVM-compatible public keys.



Ethereum Attestation Service (2024)

~~De~~Centralisation?

- Logging data that is encrypted using user-controlled public keys persistently on public-permissionless ledgers is risky and does not conform with GDPR (European Parliament, 2016).
- DIDs rely on resolving a DDO (Sporny et al., 2022), which is a hurdle to serverless dApps that have a minimal backend at most.
- Users have to rely on the EUDIW supporting VPs for Web3.
- The EUDIW does not offer pseudonymous privacy-preserving attestations of sensitive credentials because the PID is always transmitted.



6.2.1.2 PID Attributes for Natural Persons

The below table provides an overview of mandatory and optional PID attributes for natural persons.

Mandatory PID Attributes	Optional PID Attributes
family_name	family_name_birth
given_name	given_name_birth
birth_date (approach to be determened when birth_date is not known)	birth_place
	resident_address
	gender
	age_over_18
	age_over_NN
	age_in_years

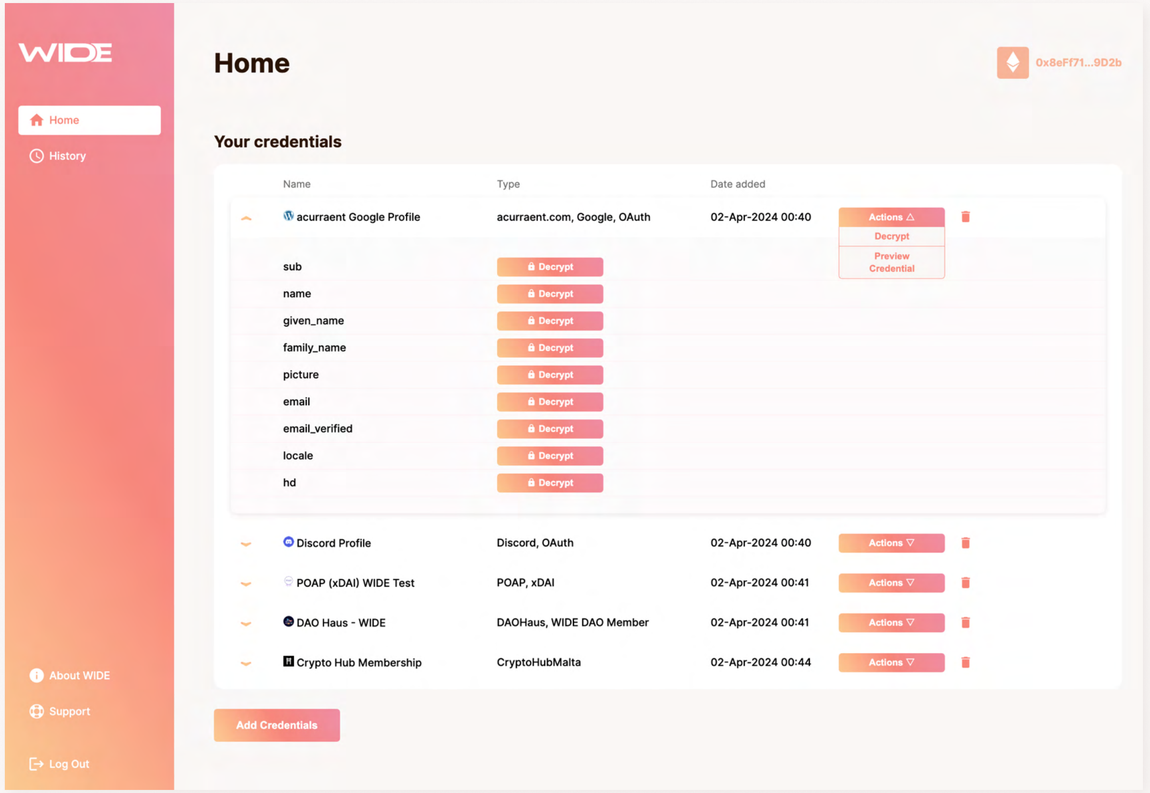
eIDAS Expert Group (2023)

Recentralisation

- WIDE creates an untrusted server architecture (Dong et al., 2011) with client-sided claim encryption.
- VCs are encrypted by the user with an EVM-compatible cryptographic key pair.
- The WIDE bridging server signs ciphers in hexadecimal format and logs identifier-specific signatures on a public-permissionless ledger.
- **Thus, WIDE offers non-economic on-chain attestations and sybil resistance by allowing users to prudently correlate their identifiers. Relying parties then verify probabilistically that a public key represents a unique human (Siddarth et al., 2020).**

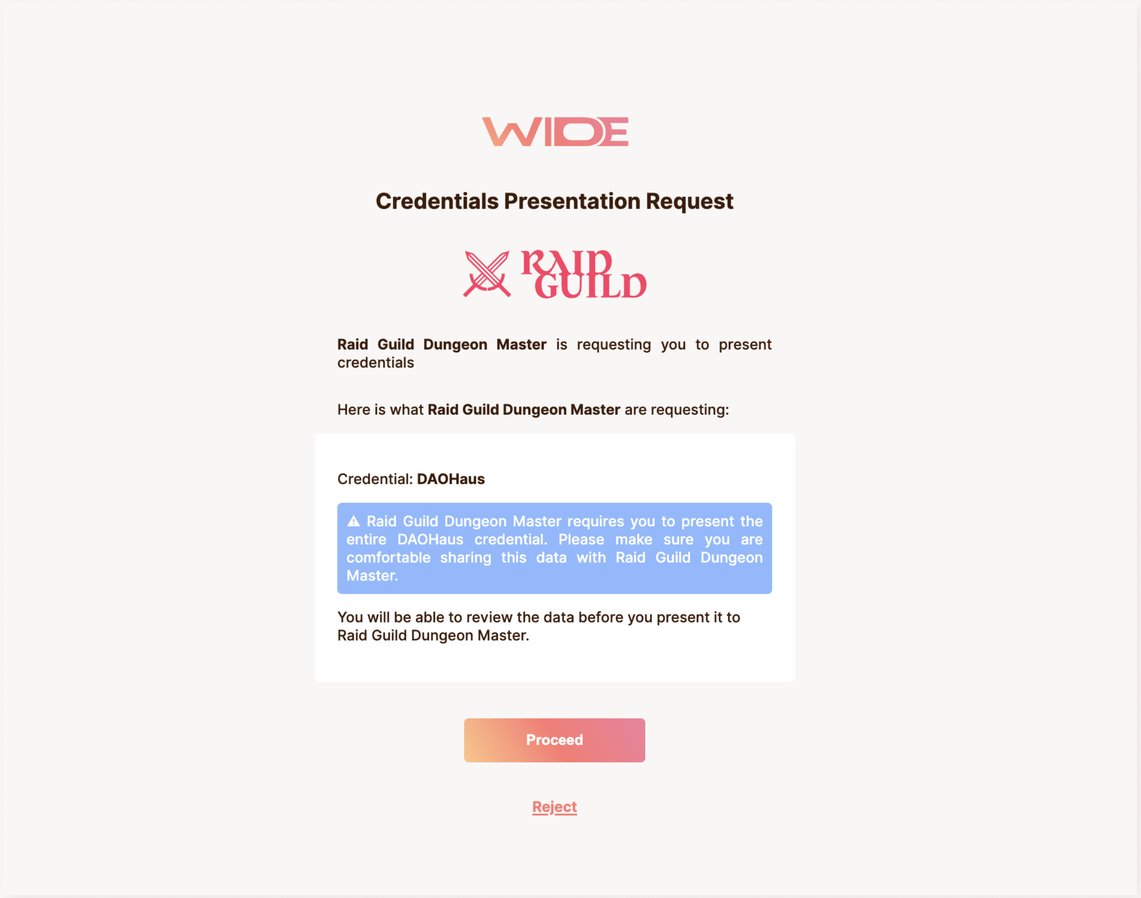
Claim Onboarding

1. Alice connects an EVM-compatible Web3 wallet to the digital identity bridge.
2. The digital identity bridge verifies Alice is the owner of a secret key through signed message verification (Chang et al., 2021).
3. Alice imports a credential import through a verifiable presentation, POAP, or OAuth2.0.
4. Alice encrypts and hashes the credential and sends both to the bridging server.
5. The bridging server tags the encrypted credentials of Alice through issuer metadata and stores the ciphers.
6. The bridging server signs over Alice's wallet, the hash and the cipher and logs the signature to Optimism.

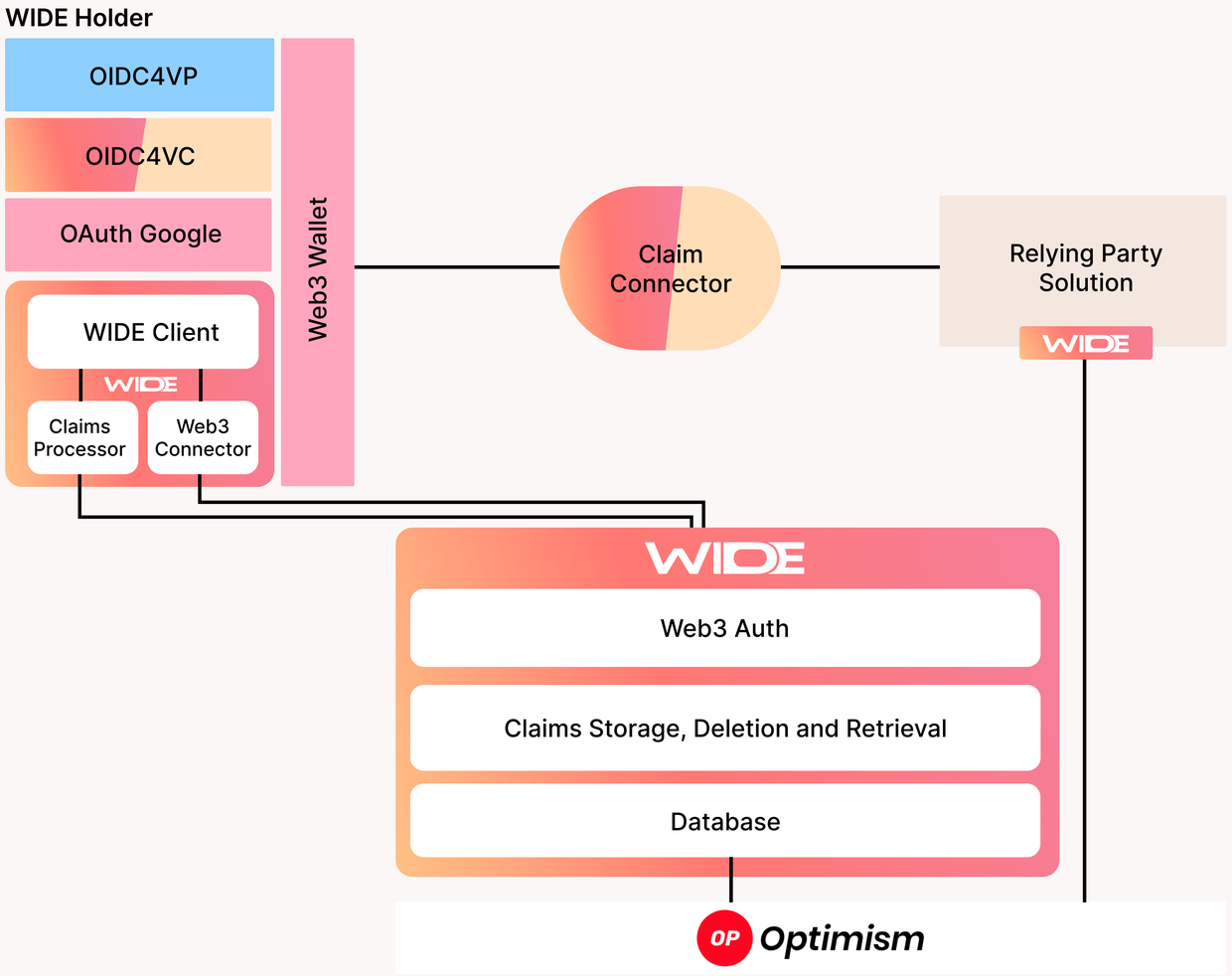


Presentation

1. Bob request for plain text claims and blinded claims are needed from Alice.
2. Bob is sending the presentation configuration to the bridging server.
3. Alice is redirected to the digital identity bridge and connects their wallet.
4. Alice is presented with the request from Bob by the digital identity bridge and accepts the request.
5. Alice downloads the appropriate ciphers with a random token and decrypts them.
6. Alice signs a consent message, the data and sends it with the token to Bob.
7. The digital identity bridge redirects Alice to Bob.
8. The bridging server logs the identity interaction with Bob on Optimism.



Simplified WIDE Solution Map



Key

- Component developed by WIDE
- External 3rd Party library
- 3rd Party Provider
- 3rd Party Dependencies that are not yet provided

! For a detailed architecture, please browse our documentation on GitHub.

Our Partners

WIDE

University

L-Università ta' Malta

Local Communities

CRYPTO HUB MALTA

DAOs

RAID GUILD

NGI TRUST CHAIN

Funded by the European Union

References

Allen, C. (2016). The Path to Self-Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Avellaneda, O., Bachmann, A., Barbir, A., Brenan, J., Dingle, P., Duffy, K. H., Maler, E., Reed, D., & Sporny, M. (2019). Decentralized Identity: Where Did It Come From and Where Is It Going? IEEE Communications Standards Magazine, 3(4), 10–13. https://doi.org/10.1109/MCOMSTD.2019.9031542

Boysen, A. (2021). Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. Frontiers in Blockchain, 4. https://doi.org/10.3389/fbloc.2021.624258

Chang, W., Gregory Rocco, Millegan, B., Johnson, N., & Terbu, O. (2021). ERC-4361: Sign-In with Ethereum [DRAFT] (Version 4361) [Ethereum Improvement Proposals]. https://eips.ethereum.org/EIPS/eip-4361

Consensys Software Inc. (2023, December 23). MetaMask developer documentation. eth_getEncryptionPublicKey. https://web.archive.org/web/20231218223550/https://docs.metamask.io/wallet/reference/eth_getencryptionpublickey/

Dib, O., & Toumi, K. (2020). Decentralized Identity Systems: Architecture, Challenges, Solutions and Future Directions (SSRN Scholarly Paper 3785452). https://papers.ssrn.com/abstract=3785452

Dong, C., Russello, G., & Dulay, N. (2011). Shared and searchable encrypted data for untrusted servers. Journal of Computer Security, 19(3), 367–397. https://doi.org/10.3233/JCS-2010-0415

eIDAS Expert Group. (2023). The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework. European Commission. https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases/tag/v1.2.0

Ethereum Attestation Service. (2024). EAS Schema #5. Is a Human. 0×8af1...a6bb6. https://easscan.org/schema/view/0×8af15e65888f2e3b487e536a4922e277dcfe85b4b1 8187b0cf9afdb802ba6bb6

Hardt, D. (2012). The OAuth 2.0 Authorization Framework (Issue RFC 6749). Internet Engineering Task Force. https://doi.org/10.17487/RFC6749

Lai, Y., Yang, J., Liu, M., Li, Y., & Li, S. (2023). Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. Blockchains, 1(2), Article 2. https://doi.org/10.3390/blockchains1020008

Laatikainen, G., Kolehmainen, T., & Abrahamsson, P. (2021). Self-Sovereign Identity Ecosystems: Benefits and Challenges. In E. Parmiggiani, A. Kempton, & P. Mikalef (Eds.), Proceedings of the 12th Scandinavian Conference on Information Systems (Vol. 1). Association for Information Systems.

Miller, J., Saint-Andre, P., & Stutzman, F. (2007). MicroID (Internet Draft draft-miller-microid-01). Internet Engineering Task Force. https://datatracker.ietf.org/doc/draft-miller-microid-00

References

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. Computer Science Review, 30, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Naik, N., & Jenkins, P. (2020). Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 90–95. https://doi.org/10.1109/MobileCloud48802.2020.00021

Reed, D., Joosten, R., van Deventer, R. (2021). The basic building blocks of ssi, in: Preuschkat, A., Reed, D. (Eds.), Self-Sovereign Identity. Decentralized Digital Identity and Verifiable Credentials, volume 1, Manning. pp. 21–38. Section: An Introduction to SSI.)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Reynolds, P., & Irwin, A. S. M. (2017). Tracking digital footprints: Anonymity within the bitcoin system. Journal of Money Laundering Control, 20(2), 172–189. https://doi.org/10.1108/JMLC-07-2016-0027

Siddarth, D., Ivliev, S., Siri, S., & Berman, P. (2020). Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-Resistance in Proof of Personhood Protocols. Frontiers in Blockchain, 3. https://www.frontiersin.org/articles/10.3389/fbloc.2020.590171

Sinha, U., Bianchi, S., Macleod, I., & Imanol Uribe. (2021). DAOs. COMS 6998 Final Project.

Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O., & Allen, C. (2022). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/

Tan, J. Z., Merk, T., Hubbard, S., Oak, E. R., Pirovich, J., Rennie, E., Hoefer, R., Zargham, M., Potts, J., Berg, C., Youngblom, R., De Filippi, P., Frey, S., Strnad, J., Mannan, M., Nabben, K., Elrifai, S. N., Hartnell, J., Hill, B. M., … Boneh, D. (2023, October 29). Open Problems in DAOs. arXiv.Org. https://arxiv.org/abs/2310.19201v1

Unique Identification Authority of India. (2022). Download Aadhaar. Government of India. https://uidai.gov.in/en/my-aadhaar/get-aadhaar.html

Weigl, L., Barbereau, T., Rieger, A., & Fridgen, G. (2022). The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. University of Luxembourg.

Weitzner, D. J. (2006). In Search of Manageable Identity Systems. IEEE Internet Computing, 10(6), 84–86. https://doi.org/10.1109/MIC.2006.127

Weitzner, D. J. (2007). Whose name is it, anyway? decentralized identity systems on the web, IEEE Internet Computing 11. 72–76. doi:10.1109/MIC.2007.95

WIDE

Thank you for your attention!

Do you have any questions?

ben@wid3.org

Follow WIDE