PSEUDONYMITY IS NOT ENOUGH

Monero 'misses out' on Decentralised Identity

Contents

1. Background and Objective
2. Systematisation of Identity Solutions
3. DID:XMR - a Proposal

BACKGROUND AND OBJECTIVE

Research Background and Positioning

Which implications do technological policies have on digital identity by private public partnerships for Monero?

"Social technology [...] allows for a 'technisation' [of] new administrative [...] power between authority and subject" (Leibetseder, 2011, p.15).

Bentham (1778), p.38

Peripherality Unites Monero and Small Jurisdictions

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
26	Monero XMR	$136.40	▼0.15%	▲1.69%	▼1.14%	$2,495,226,477	$35,370,522 259,156 XMR	18,293,441 XMR
27	Ethereum Classic ETC	$15.34	▼0.17%	▲0.71%	▲1.73%	$2,171,078,491	$82,632,122 5,385,266 ETC	141,500,510 ETC
28	Stellar XLM	$0.07966	▼0.45%	▲2.84%	▼3.46%	$2,142,886,791	$34,986,347 439,327,433 XLM	26,901,614,149 XLM
29	Bitcoin Cash BCH	$106.69	▼0.24%	▼1.21%	▲2.76%	$2,072,226,639	$63,905,155 599,112 BCH	19,422,444 BCH

Coinmarketcap (2023)

Local productions' dependence on innovations and technologies of the centre polarises, thus, manifests peripherality (Komninos and Sefertzi, 1998, p.47, cf. Sefertzi (1996)).

Large Networks' Claim on Sovereignty

- large distributed ledgers already have did:methods (W3C, 2023)
  - Bitcoin (did:btcr)
  - Ethereum (did:ethr)
  - Solana (did:sol)
- identities persisted on the public ledgers threaten privacy
- IPFS was introduced for institutional identity data storage
- Hyperledger Foundation (2020) marketed un-linkable credentials
  - Ed25519-based cryptography
  - Pedersen commitments
  - decoupled session identification from holder binding

EXISTING IDENTITY SOLUTIONS
a Systematisation

Governmental Identity Schemes are those really exerting Technological Sovereignty.

ePassport

International Standards Organisation

European Commission eIDAS Trusted List

National Identity Schemes-A Prudent Approach

"[T]he transferability of MRTD chip's signature on the challenge [proves] [t]he MRTD chip was indeed at a certain date and time. [S]uch proves (sic!) can be misused to track persons" - BSI, 2015, TR-30111-1, p.22.

"Commands for installing, updating, and using the eSign Application are out of scope of this specification" (BSI, 2015, TR-30111-3, p.69).

Mobile Driving Licence - a paradigm shift

MAC provides better privacy to the mdoc holder because it does not require the mdoc to produce a potentially non-repudiable signature over mdoc reader-provided data.

"Security requirements regarding storage of credential information, including the mdoc private key are out of scope for this document."

ISO/IEC 18013-5:2021, p.53

```
[
{
      -1:1,
      -2:h'98f50a4ff6c05861c8860d13a638ea56c3f5ad7590bbfbf054e1c7b4d91
   d6280',
      -3:h'f01400b089867804b8e9fc96c3932161f1934f4223069170d924b7e03bf
   822bb',
      1:2,
      2:'peregrin.took@tuckborough.example'
    },
{
      1:2,
      -1:1,
      2:'peregrin.took@tuckborough.example',
      -2:h'98f50a4ff6c05861c8860d13a638ea56c3f5ad7590bbfbf054e1c7b4d91
   d6280',
      -3:h'f01400b089867804b8e9fc96c3932161f1934f4223069170d924b7e03bf
   822bb',
      -4:h'02d1f7e6f26c43d4868d87ceb2353161740aacf1f7163647984b522a848
   df1c3'
    }
]
```

IETF (2022),RFC-9053(8152), COSE, pp.117

SD-JWT Privacy & Security Considerations

5.1.3. Holder Public Key Claim

If the Issuer wants to enable Holder Binding, it MAY include a public key associated with the Holder, or a reference thereto.

It is out of the scope of this document to describe how the Holder key pair is established. For example, the Holder MAY provide a key pair to the Issuer, the Issuer MAY create the key pair for the Holder, or Holder and Issuer MAY use pre-established key material.

"Colluding Issuer/Verifier or Verifier/Verifier pairs multiple sessions to the same user on the basis of unique values encoded in the SD-JWT (Issuer signature, salts, digests, etc.)."

IETF (2023), SD-JWT, Section 9.4

Private Keys & Personal Identifiers (PIDs)

"PID attestation MUST include all the information (as an attribute or as any other signed value) required to perform verification of the holder binding by a Relying Party" (European Commission, 2023, p.24).

"A PID Provider may issue a PID set to the EUDI Wallet" with level of assurance (LoA) **high** (European Commission, 2023, p.21).

Mandatory eIDAS Attributes	Optional eIDAS Attributes	Possible additional optional attributes
Current Family Name	Family Name at Birth	Nationality/Citizenship*
Current First Names	First Names at Birth	Optional attributes used at national level, e.g., tax number, social security number etc.
Date of Birth	Place of Birth	
Unique Identifier	Current Address	
	Gender	

cf. European Commission, 2023, p.22-23

DID:XMR
privacy preserving authenticity

Properties of DID:XMR

- Monero's dual key pair setup mimics the security of governmental IDs (Koe et al., 2020)
  - Pedersen commitments ensure privacy preserving key rotation
  - Sub-accounts promise to minimise the identity management overhead
- DID:XMR integrates two cryptographic operations into one DID method
  - authentication and ID presentation are decoupled, but integrated
  - interoperability without reliance on Anonymous Credentials
  - permissioned disclosure of auditable key rotation
- simple, did:btcr-based DID method
  - transaction hash-based identifiers are well known
  - no need for server-sided verifiable data registries

Verifier/ Issuer
Key Management

References

Bentham, J. (1778). Panopticon; Or, The Inspection-House. In: Bowring, J. (ed.), The Works of Jeremy Bentham. Volume 4.

Bundesamt für Informationssicherheit (BSI). (2015). Technical Guideline TR-03110. Version 2.20. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03110/TR-03110_node.html. Retrieved: 2023-06-20.

Coinmarketcap. (2023). Today's Cryptocurrency Prices by Market Cap. coinmarketcap.com. Retrieved: 2023-06-18.

European Commission. (2023). eIDAS Dashboard. EU/EEA Trusted List Browser. eidas.ec.europa.eu/efda/tl-browser/#/screen/home. Retrieved: 2023-06-20.

European Commission. (2023). The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework. The European Digital Identity Wallet Architecture and Reference Framework. Version 1.0.0. digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework. Retrieved: 2023-06-20.

Hyperledger Foundation. (2020). Aries Request for Comment (RFC): 0559. Privacy-Preserving Proof of Uniqueness github.com/hyperledger/aries-rfcs/blob/main/concepts/0559-pppu/README.md. Retrieved: 2023-06-20.

International Engineering Taskforce (IETF). (2020). Request for Comments (RFC): 8949. Concise Binary Object Representation (CBOR). rfc-editor.org/rfc/rfc8949.html. Retrieved: 2023-06-20.

International Engineering Taskforce (IETF). (2022). Request for Comments (RFC): 9053. CBOR Object Signing and Encryption (COSE). rfc-editor.org/rfc/rfc9053. Retrieved: 2023-06-20.

International Engineering Taskforce (IETF). (2023). Draft. Selective Disclosure for JWTs (SD-JWT). ietf.org/archive/id/draft-ietf-oauth-selective-disclosure-jwt-04.html. Retrieved: 2023-06-20.

International Standards Organisation (ISO). (2021). ISO/IEC 18013-5:2021. Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application.

International Standards Organisation (ISO). (2023). ISO name and logo. iso.org/iso-name-and-logo.html. Retrieved: 2023-06-20.

Koe, et al. (2020). Zero to Monero. A Technical Guide to a Private Digital Currency. Version 2.0.0. getmonero.org/library/Zero-to-Monero-2-0-0.pdf. Retrieved: 2023-06-20.

Komninos, N. and Sefertzi, E. (1998). Neo-industrialisation and Peripherality Evidence from Regions of Northern Greece. In: Geoforum. Pergamon. Volume 29. Issue 1. p. 37-49.

Leibetseder, B. (2011). A Critical Review on The Concept of Social Technology. In: Social Technologies. Volume 1. Issue 1. p. 7-24.

The Monero Project. (2023). Monero Symbol. getmonero.org/press-kit/symbols/monero-symbol-480.png. Retrieved: 2023-06-20.

Wikimedia Commons. (2008). International symbol for biometric passports // gold. commons.wikimedia.org/wiki/File:EPassport_logo_gold.svg. Retrieved: 2023-06-20.

World Wide Web Consortium (W3C). (2023). DID Specification Registries. The interoperability registry for Decentralized Identifiers. w3c.github.io/did-spec-registries/#did-methods. Retrieved: 2023-06-20.

BEN BIEDERMANN

Independent Researcher

bb@dvctvs.wtf

t.me/benedictiner

CC BY-NC-SA