

Decentralized Identity 101

Steven McCown

Anonymome Labs, Chief Architect

Decentralized Identity Foundation, Steering Committee

We have a *security* problem ...

... and a *privacy* problem.

The Security Problem

Report: “Account Takeover in 2022”

- 25B login credentials leaked to the dark web (over time)
- 65% increase over 2020



“98% of orgs have vendor relationships with at least one third-party that has experienced a breach in the last two years.”

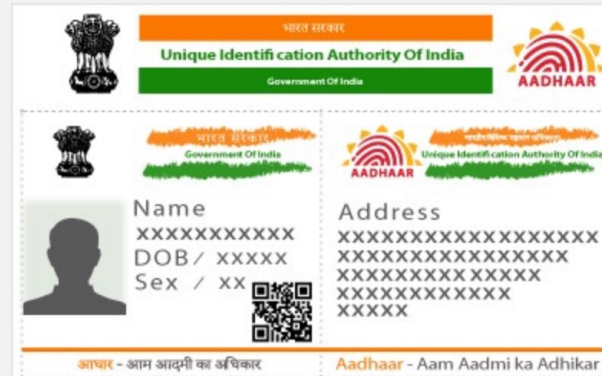
~ Security Scorecard & The Cyentia Institute, 2022

Leads To Privacy Problems



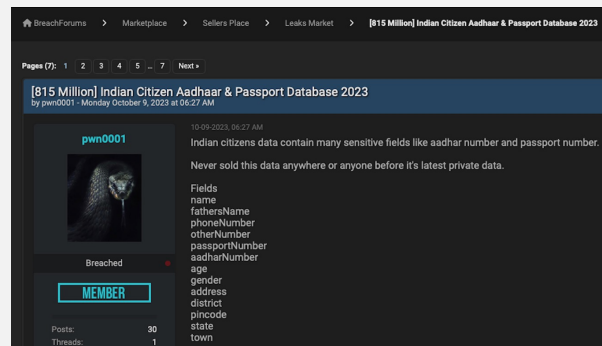
Aadhaar Card Breaches 2023

- 815M cards disclosed
 - Personal data + Biometrics
 - For sale on dark web



2018

- 1.1B cards disclosed
 - Personal data + Photos
 - Anonymous seller on WhatsApp



Uses

- Gov. Services
- Voting
- Passports
- e-KYC
- Payments
- Banking
- Cell phone

“Identities are the true hackers objective.”

~ Garret F. Grajeck, CEO YouAttest, 2023

What is a Digital Identity?

Most of us use the ID of our communication endpoints.



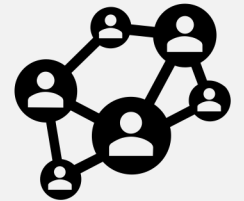
user@example.com



+1 (801) 555-1212



42222222222222



@Handle

Are you:

- *Locked-in* to a provider?
- *Profiled* (AI / algorithms)?
- *Monetized* (sold for ads)?

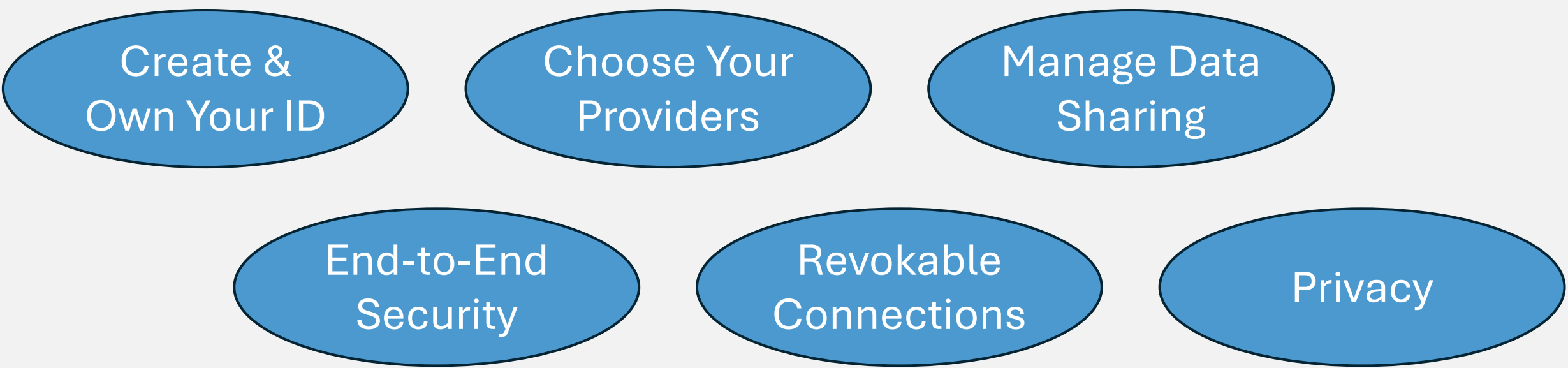
Can you:

- *Upgrade* security?
- *Control* your private data?
- Interoperate with others?

Enter Decentralized Identity...

Why Decentralized Identity?

Puts you in control



Create &
Own Your ID

Choose Your
Providers

Manage Data
Sharing

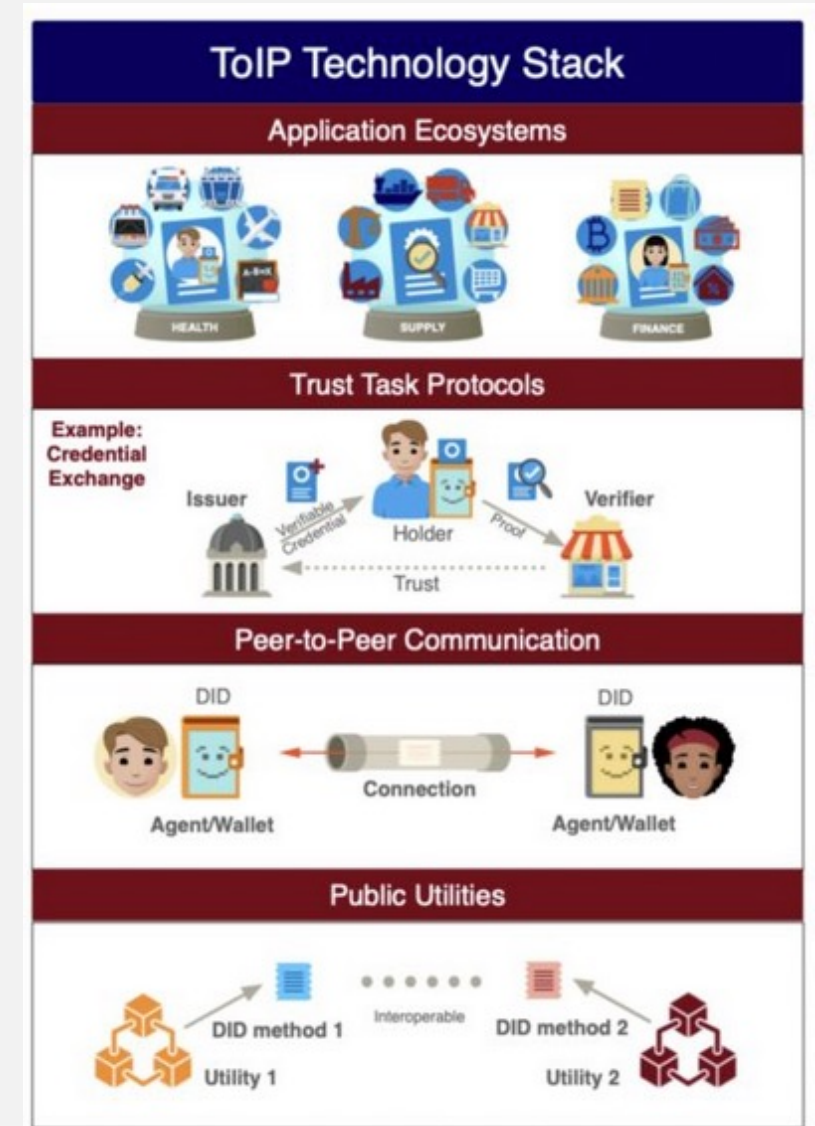
End-to-End
Security

Revokable
Connections

Privacy

What is Decentralized Identity?

- Decentralized Identity
 - An approach to allow individuals and enterprises to **manage their own data** instead of using a central authority.
- DI Goals
 - **Common Standards** allow individual/businesses to control which applications and services can have access to specific types of data.
- **Increasing adoption**
 - In transportation, supply chain, banking/finance, health care, travel, farming and mining.



What's a DID?

DIDs are:

- URIs ... like web addresses
- Controlled by each Holder

Types:

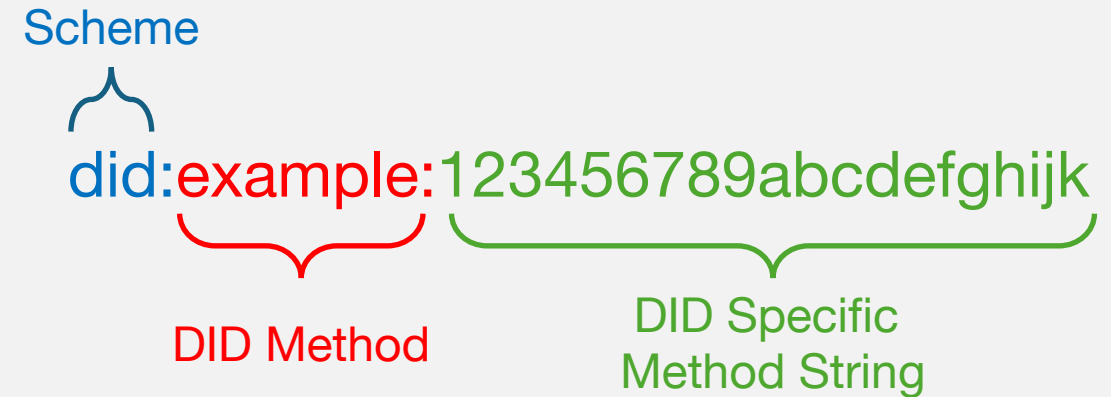
- Based in *Verifiable Data Registry*
- Peer DIDs (between 2 Holders)

Functions

- Resolved by *DID Methods*
- Point to *DID Docs*

DID Providers

- Lots ... and they're all interoperable



What's a DIDDoc?

Set of data needed to:

- Communicate
 - Service endpoints (where to communicate)
 - Basic protocols (how to communicate)
- Security
 - Cryptographic material (e.g., keys)
 - Signed
- Extensibility
 - Data necessary to support Verifiable Credentials

```
{
  "@context": "https://w3id.org/did-resolution/v1",
  "didResolutionMetadata": {
    "contentType": "application/did+json",
    "retrieved": "2024-05-23T21:42:24Z",
    "did": {
      "didString": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN",
      "methodSpecificId": "PslysXP2Ae6GBfxNhNQNKN",
      "method": "cheqd"
    }
  },
  "didDocument": {
    "@context": [
      "https://www.w3.org/ns/did/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
    ],
    "id": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN",
    "verificationMethod": [
      {
        "id": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN#key1",
        "type": "Ed25519VerificationKey2020",
        "controller": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN",
        "publicKeyMultibase": "z6Mkta7joRuvDh7UnoESdgpr9dDUMh5LvdoECDi3WGrJoscA"
      }
    ],
    "authentication": [
      "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN#key1"
    ],
    "service": [
      {
        "id": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN#website",
        "type": "LinkedDomains",
        "serviceEndpoint": [
          "https://www.cheqd.io"
        ]
      },
      {
        "id": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN#non-fungible-image",
        "type": "LinkedDomains",
        "serviceEndpoint": [
          "https://gateway.ipfs.io/ipfs/bafybeihetj2ng3d74k7t754atv2s5dk76pcqtvx1s6dntef3xa6rax25xe"
        ]
      },
      {
        "id": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN#twitter",
        "type": "LinkedDomains",
        "serviceEndpoint": [
          "https://twitter.com/cheqd_io"
        ]
      },
      {
        "id": "did:cheqd:mainnet:PslysXP2Ae6GBfxNhNQNKN#linkedin",
        "type": "LinkedDomains",
        "serviceEndpoint": [
          "https://www.linkedin.com/company/cheqd-identity/"
        ]
      }
    ]
  },
  "didDocumentMetadata": {
    "created": "2022-04-05T11:49:19Z",
    "versionId": "4fa8e367-c70e-533e-babf-3732d9761061"
  }
}
```

What's a Verifiable Data Registry?



Decentralized Ledger



Centralized Ledger



Blockchain

A Verifiable Data Registry (VDR) is used to securely store and lookup DIDs and DIDDocs.

Ideally, a VDR is:

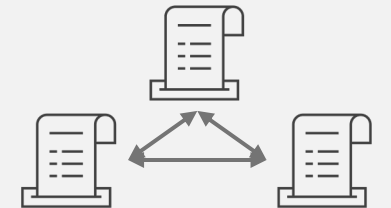
- Immutable
- Decentralized
- Privacy preserving
- Secure



Secure Cloud Storage



Websites



Transaction Receipts

What's a DID Method?

Process that:

- Accepts a DID
- Returns a DID Doc
- Verifies a DID Doc's authenticity
- Accesses stored data on a Verifiable Data Registry (VDR)

Choosing a DID Method

- Many to choose from
- Trust level (subjective)
- Some are more / less 'secure' than others
- All are interoperable



DID Method	DID Prefix
Cheqd	did:cheqd:....
WebVH Platform	did:webvh:...
Keri	did:webs:...
Polygon	did:polygonid:...
Bitcoin	did:btcr:...
Ethereum	did:ethr:...
Peer DID	did:peer:..

How To Resolve DIDs?

Universal Resolver

- Similar to DNS lookup
- DID Docs have a cryptographic verification method

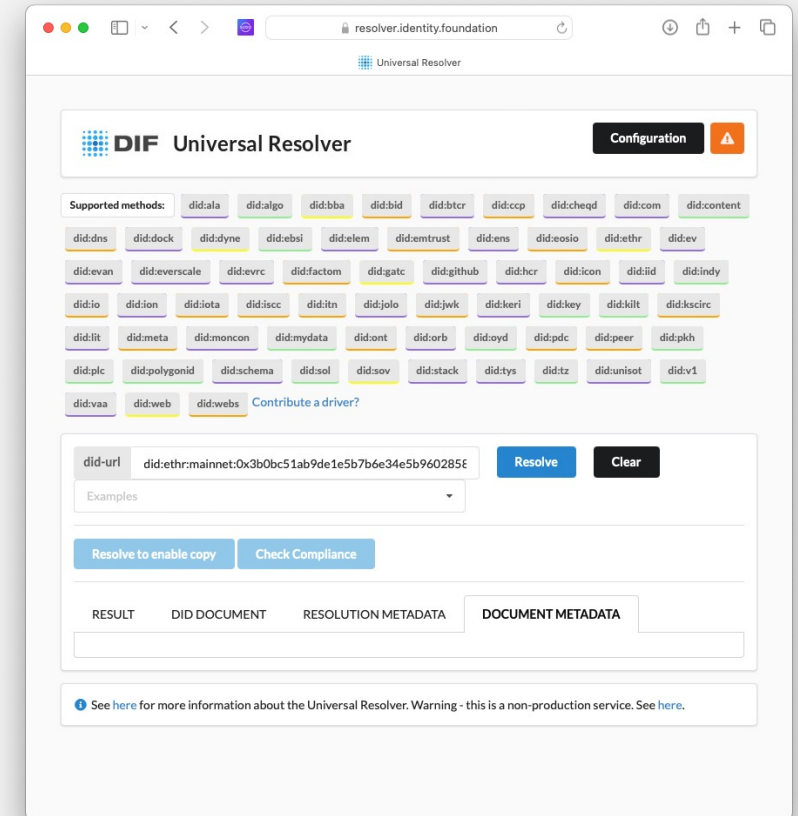
DIF Universal Resolver

- Live: (<https://resolver.identity.foundation>)
- Source: (<https://github.com/decentralized-identity/universal-resolver>)

Cheqd Universal Resolver

- Docs: (<https://docs.cheqd.io/identity/advanced/did-resolver>)
- Source: (<https://github.com/cheqd/did-resolver>)

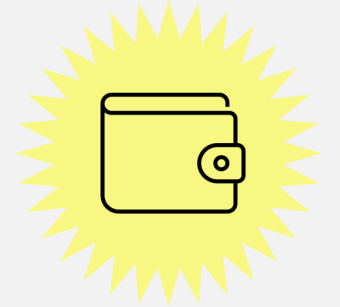
Want to host your own?



Storing DIDs and Other Crypto Stuff

Storing our DIDs, keys, credentials, etc.

Not just marketing hype ... we really do need a wallet



What's a wallet?

- **Basic:** it's a *secure data store* for cryptographic DI data
- **Advanced:** Basic + *secure hardware element*
- **More Advanced:** Advanced + *DI protocols*
- **Super Advanced:** More Advanced + *UI / UX*

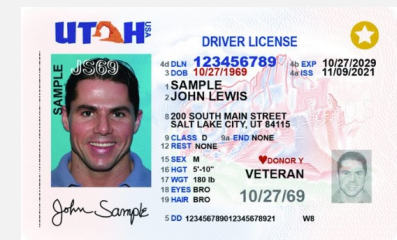
What's it really?

- An app, application, service, etc.
- Providers: governments, banks, schools, comms providers, etc.

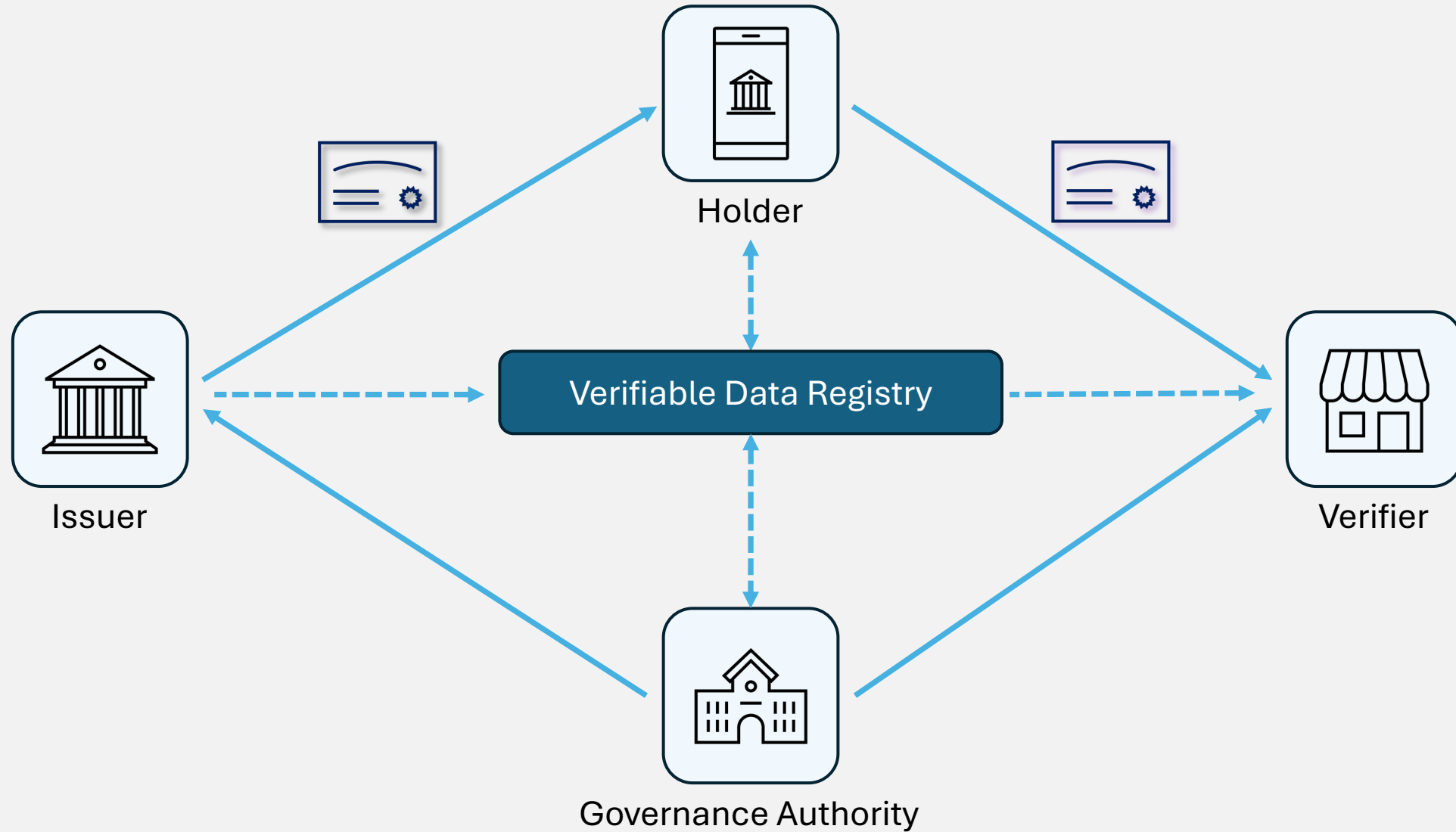
Verifiable Credentials

Verifiable Credentials

- Can have the same data as physical credentials
- May incorporate biometrics
- Electronic issuable and presentable
- Cryptographic verification
- Selective disclosure*
- Privacy preserving*



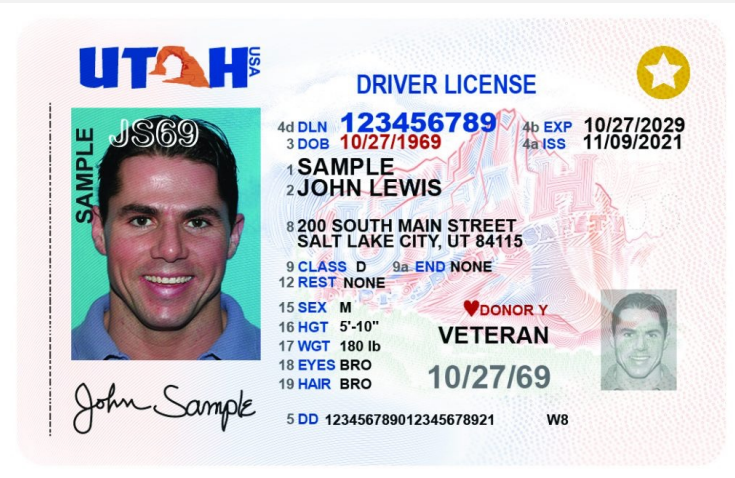
Verifiable Credentials



SEDI: Selective Disclosure

Utah Legislation: SB0260

- (e) the state-endorsed digital identity enables an individual to:
(i) selectively disclose elements of the individual's identity; and

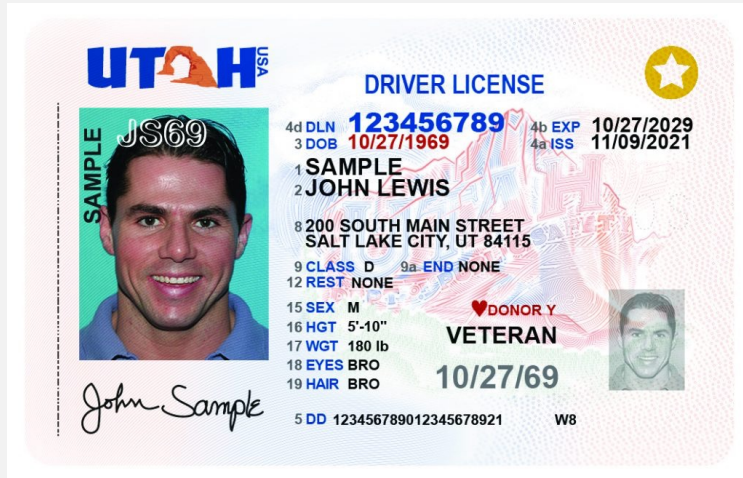


Only give what you choose

SEDI: Asserting with Zero Correlation

Utah Legislation: S.B 0260

(ii) verify that the individual's age satisfies an age requirement without revealing the individual's age or date of birth.



I'm 21+

Here's (just) my ticket

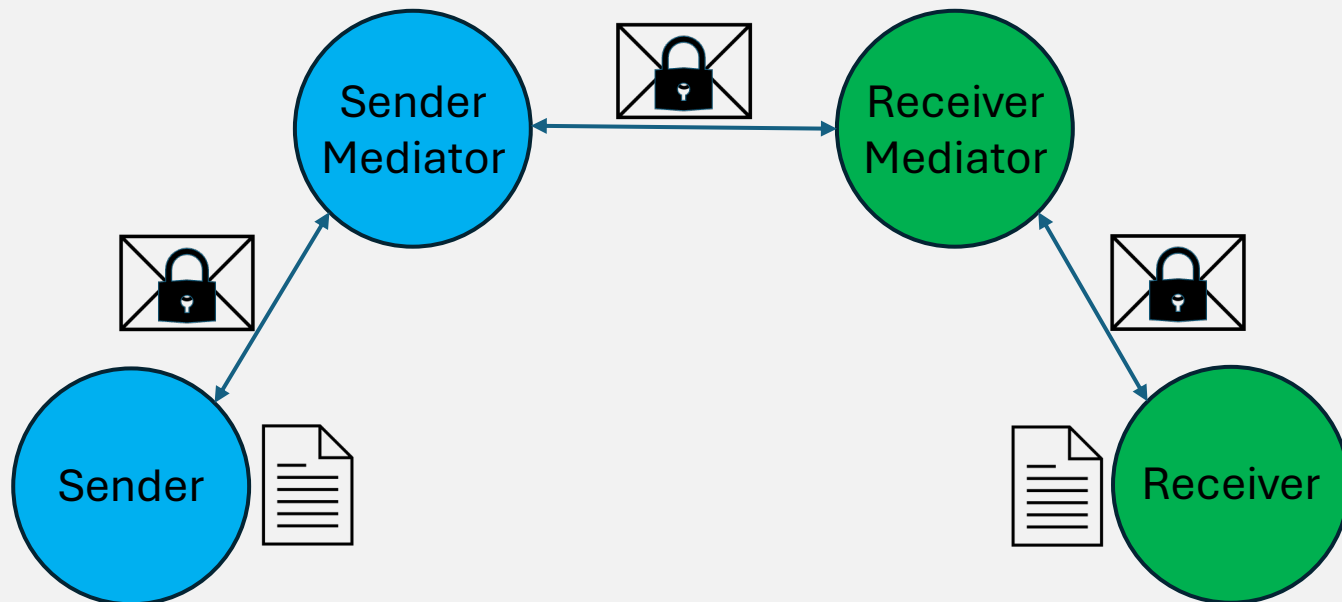


I'm a Veteran



DID Communication

DIDComm: *a DID-based cryptographic communication protocol.*



Plaintext Message

```
{
  "id": "1234567890",
  "type": "<message-type-uri>",
  "from": "did:example:alice",
  "to": ["did:example:bob"],
  "created_time": 1516269022,
  "expires_time": 1516385931,
  "body": {
    "message_type_specific_attribute": "and its value",
    "another_attribute": "and its value"
  }
}
```

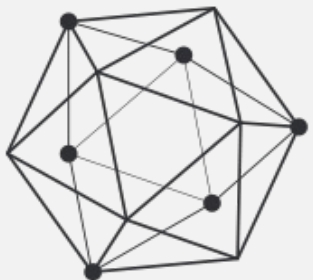
Encrypted Message

```
{
  "ciphertext": "WCufCs2lMZfkxQ0JCK92lPtLFgwWk_FtRWOMj52bQI...",
  "protected": "eyJlcGsiOnsia3R5IjoIRUMiLCJjcnYiOiJQLTI1NiI...",
  "recipients": [
    {
      "encrypted_key": "ZIL6Leligq1Xps_229nlo1xB_tGx0EVoE...",
      "header": {
        "kid": "did:example:bob#key-p256-1"
      }
    }
  ],
  "tag": "nIpa3EQ29hgCkA2cBPde2HpKXK4_bvmL2x7h39rtVEc",
  "iv": "mLqi1bZLz7VwqtVVFSDiLg"
}
```


Interoperability: Enhance Existing Systems

- OpenID + DIDComm
 - Launch DIDComm connection from an OpenID verification
 - How:
 - Add a DID (with a DIDComm service endpoint) to an OID4VC exchange
 - Ideally, both parties exchange DIDComm capable DIDs
 - Initiate secure messaging over DIDComm connection
 - Benefits
 - Enhance existing systems with new DI features and capabilities

Decentralized Identity Standards Groups



HYPERLEDGER



Thank You!

Steve McCown

~ Email:

smccown@Anonyome.com

~ LinkedIn:

<https://www.linkedin.com/in/mccown>

~ Discord: @mccown