

TrustVault:

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

S.E Jacobino, Dr.ir. J.A. Pouwelse
31 Augustus 2022



Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties



Outline

- Introduction
- Problem description
- Building blocks
- TrustVault Architecture & Design
- Evaluation
- Related Work
- Conclusion

Introduction

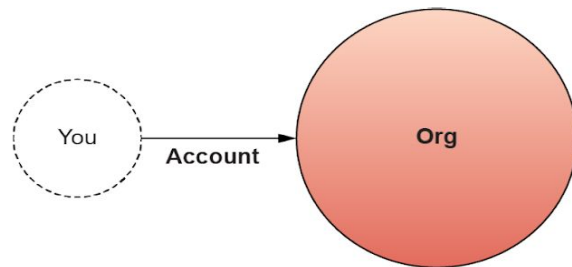
You are *not*
in control.

Introduction

- History of identity on the Internet

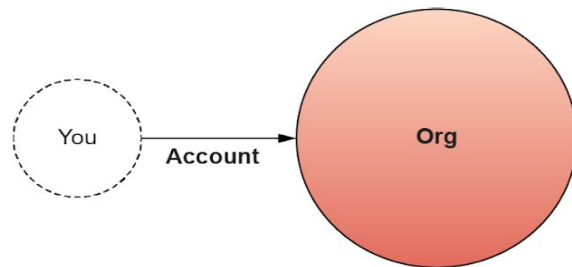
Introduction

Centralized Identity

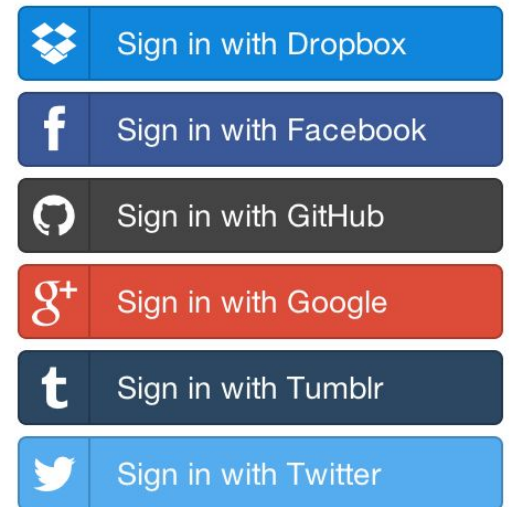
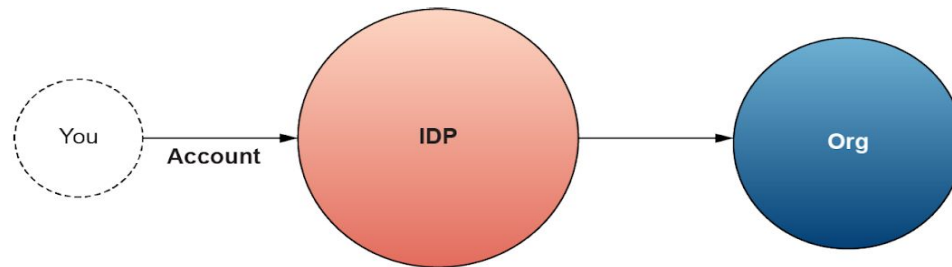


Introduction

Centralized Identity

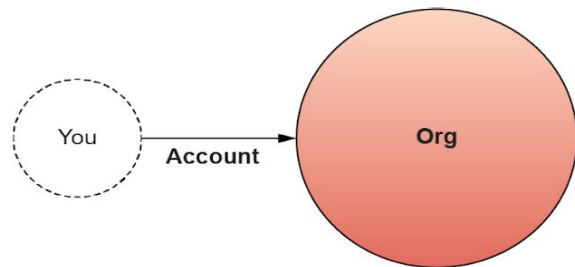


Federated Identity

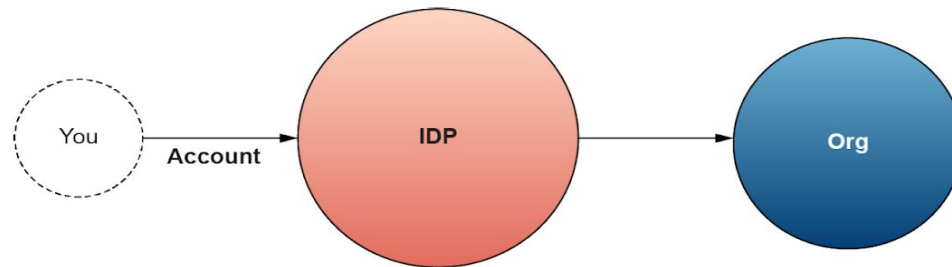


Introduction

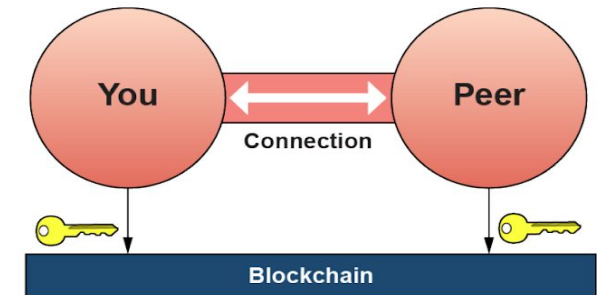
Centralized Identity



Federated Identity



Self-Sovereign Identity



Introduction

- History of identity on the Internet
- Requirements for a digital identity
 - Security: identity information is protected from unintentional disclosure.
 - Control: the identity owner determines who can access their data and under what circumstances.
 - Portability: identity must not be tied to a single service or provider.
- The European Union is aware of the problem

“Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality.”

Ursula von der Leyen, President of the
European Commission

Shaping Europe's digital future

Home Policies Activities News Library Funding Calendar Consultations

Home > Policies > Europe's Digital Decade

Europe's Digital Decade

The EU will pursue a human-centric, sustainable vision for digital society throughout the digital decade to empower citizens and businesses.



Digital Decade
Join the disc
Decade >
Press release

THALES
Building a future we can all trust



EU digital identity



Free

Safe

Voluntary

Linked to national eID

Available across the EU

Keeps you in control of your data

**THE EU DIGITAL ID WALLET IS COMING.
HERE'S WHAT IT MEANS FOR YOU**

<https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade>

<https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/government/magazine/eu-digital-id-wallet-coming-heres-what>

€26M

for European Digital Wallet

Introduction

- History of identity on the Internet
- Requirements for a digital identity
 - Security: identity information is protected from unintentional disclosure.
 - Control: the identity owner determines who can access their data and under what circumstances.
 - Portability: identity must not be tied to a single service or provider.
- The European Union is aware of the problem
- European Self-Sovereign Identity Framework
- Leverage blockchain technology: European Blockchain Services Infrastructure
- EU digital wallet on the app store



What about my data?

Problem description

- Still reliant on Big Tech to store and host our data
- Hard to secure centralised applications
 - Large amount of data
 - Statistical analysis on metadata and interactions
- Not under your full control
 - Access control not enforced or not flexible
 - Censorship
- Not portable
 - Incentive to retain users & data
 - Data coupled to application

Problem description

A system with true data sovereignty requires the following properties:

- Decentralised data storage on device controlled by data owner
- Fine-grained and resolutely enforced access control
 - Decentralised identity
 - Verified authentication
- Data decoupled from applications

Bonus: plug into the societal infrastructure for identity

TrustVault: data wallet with attribute-based access control based on verifiable credentials from EBSI

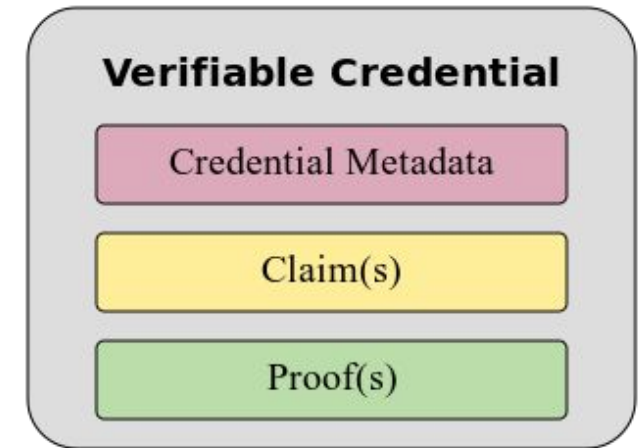
Background

Digital Signatures

- TODO

Self-Sovereign Identity

- Issuers, Holders, Verifiers and a Verifiable Data Registry
- Verifiable Credentials (VC) are the building blocks of SSI
 - Contains claims about the holder and proofs that those claims are true
 - Used to convince others of the validity of claims

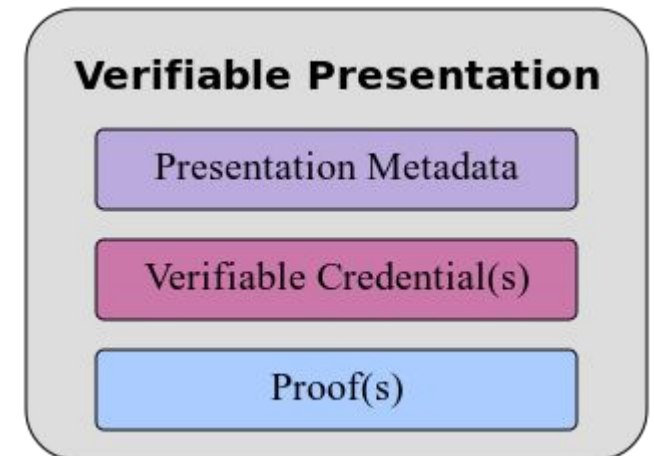
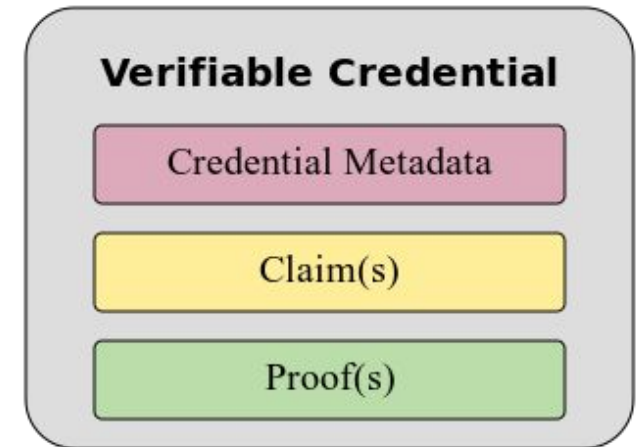


Self-Sovereign Identity



Self-Sovereign Identity

- Issuers, Holders, Verifiers and a Verifiable Data Registry
- Verifiable Credentials (VC) are the building blocks of SSI
 - Contains claims about the holder and proofs that those claims are true
 - Used to convince others of the validity of claims
- Verifiable Presentations (VP)
 - Requested by verifiers
 - Contains VCs and proof that the VCs are about you

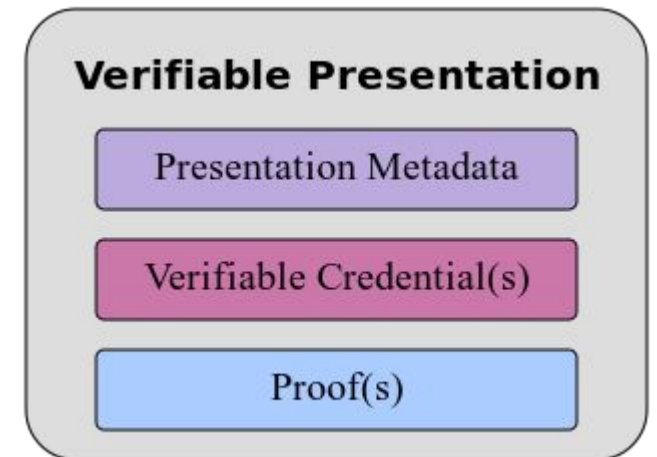
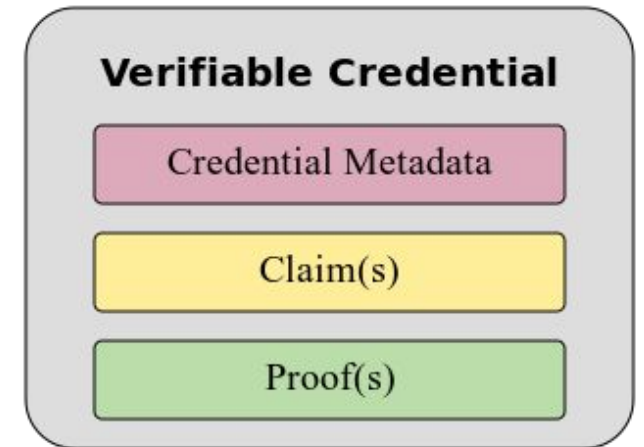


Self-Sovereign Identity

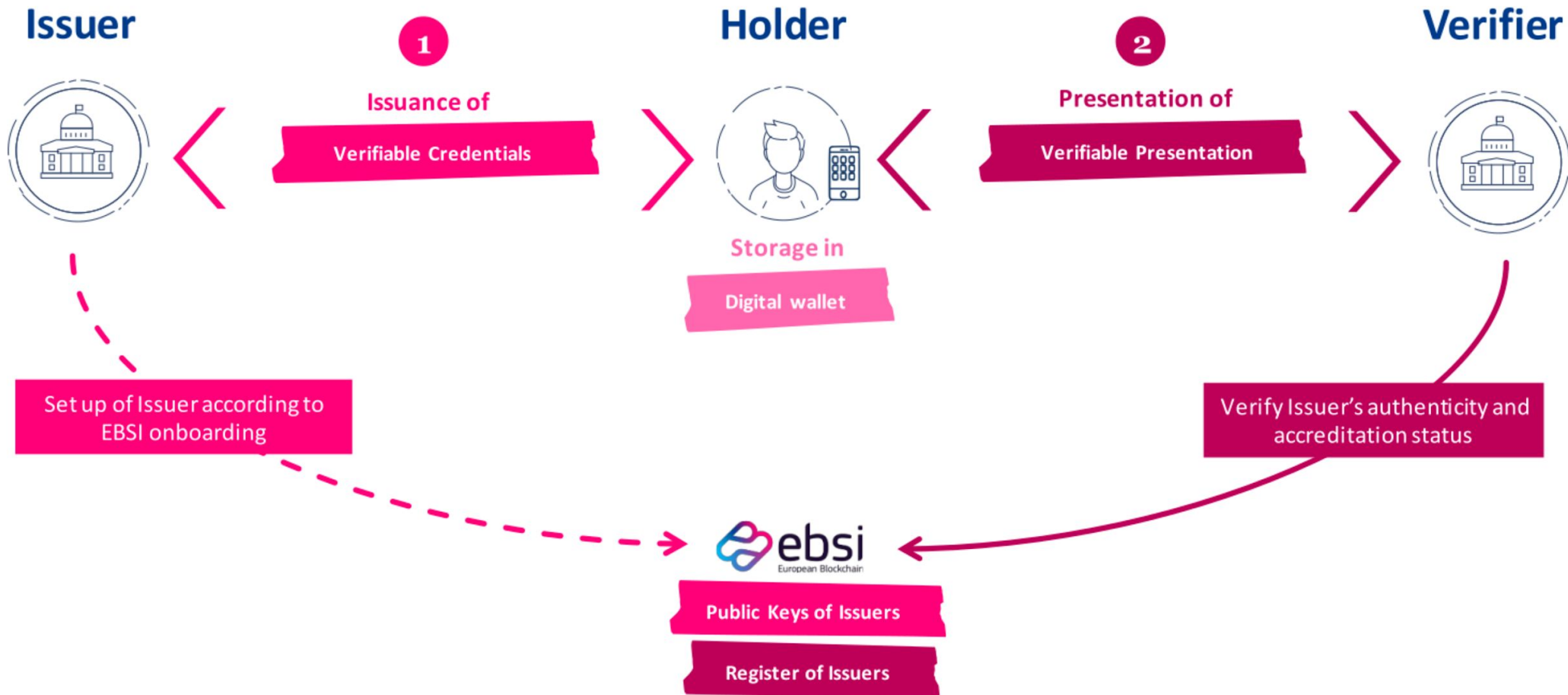


Self-Sovereign Identity

- Issuers, Holders, Verifiers and a Verifiable Data Registry
- Verifiable Credentials (VC) are the building blocks of SSI
 - Contains claims about the holder and proofs that those claims are true
 - Used to convince others of the validity of claims
- Verifiable Presentations (VP)
 - Requested by verifiers
 - Contains VCs and proof that the VCs are about you
- Verifiable Data Registry is the anchor of trust

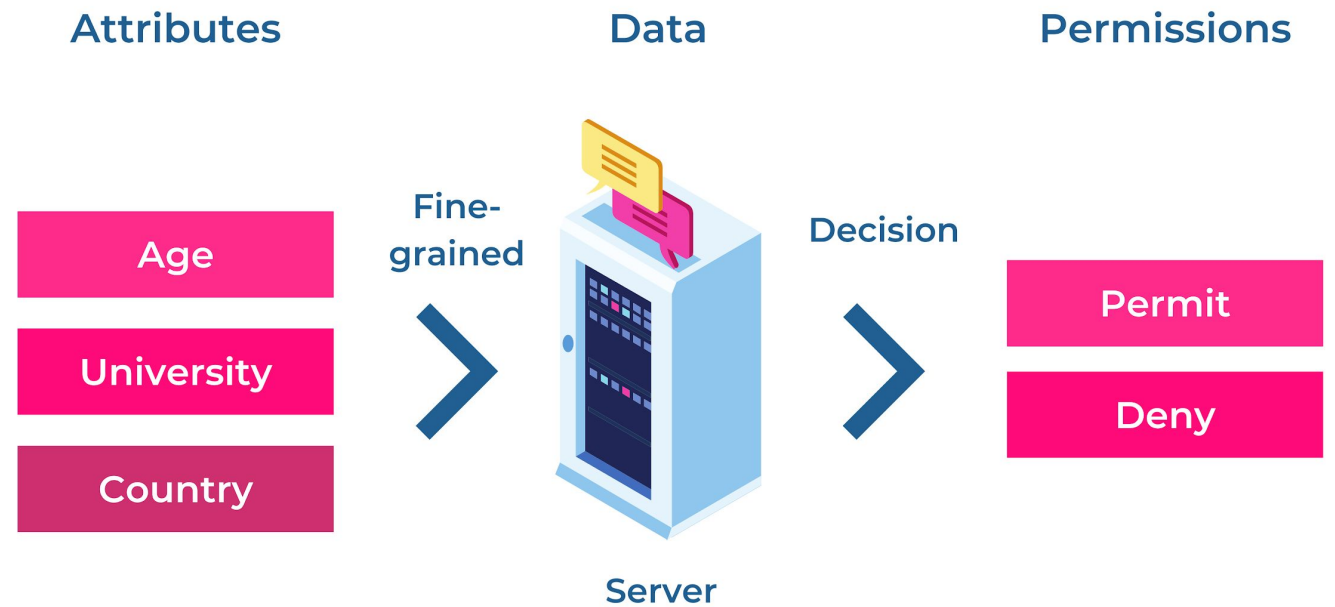


Self-Sovereign Identity

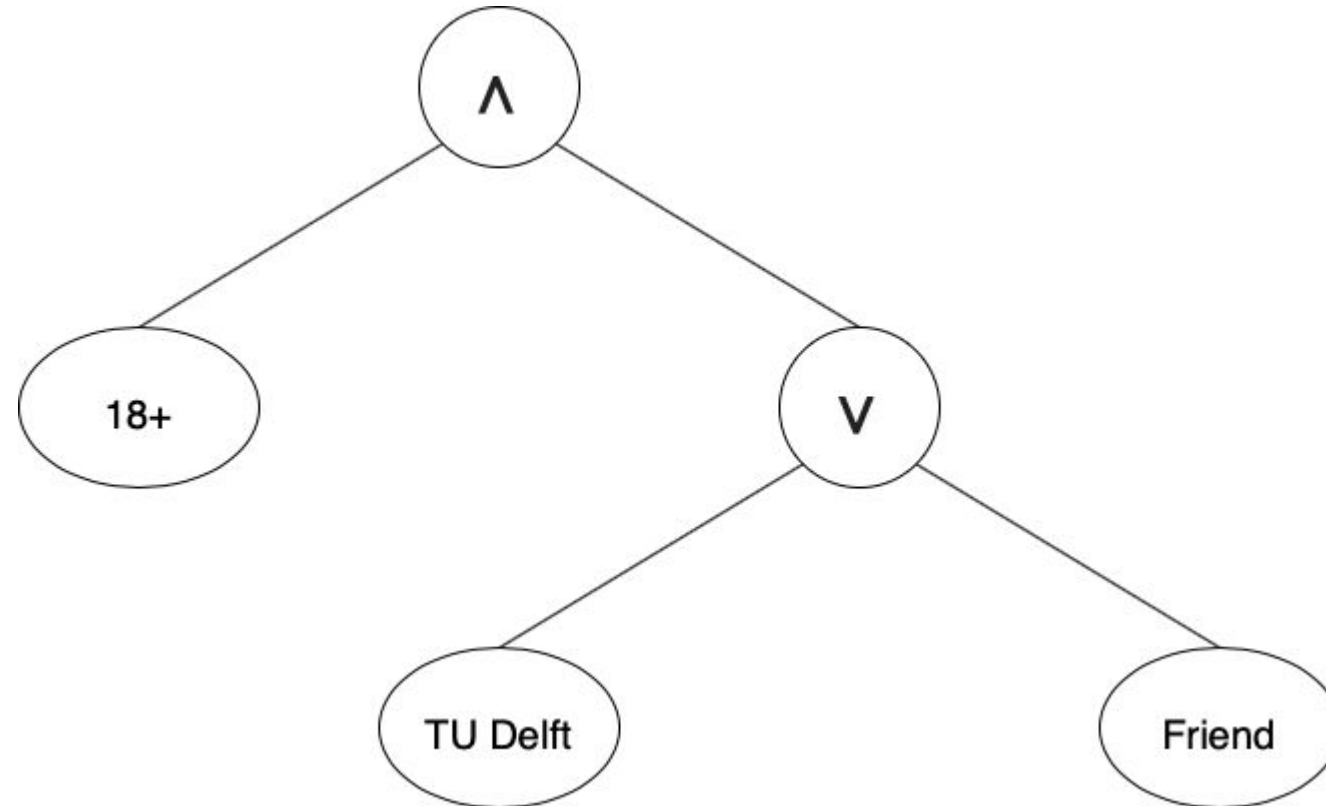


Attribute-Based Access Control

- Control access to resources
- Evaluate set of attributes against predefined rules
- Fine-grained control
- Only limited by available attributes
- Requires verifiable attributes

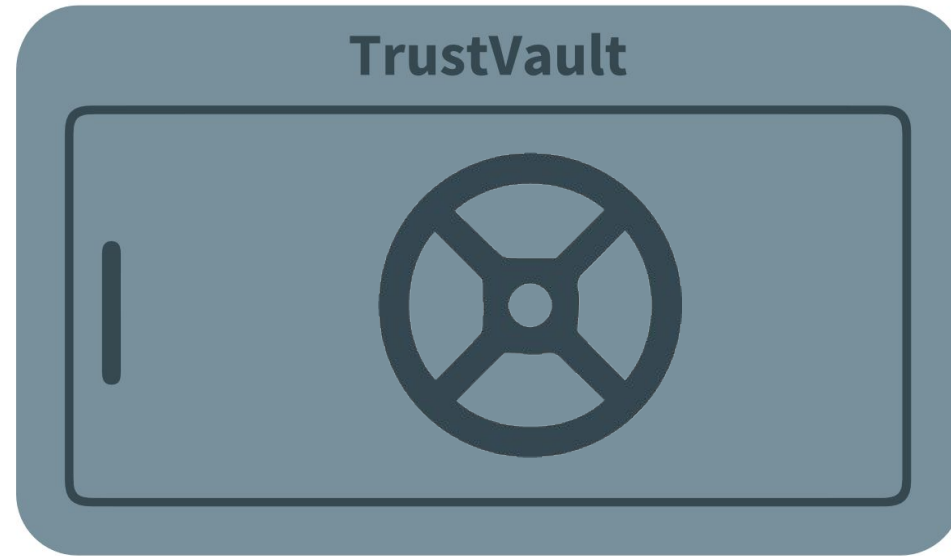


Attribute-Based Access Control

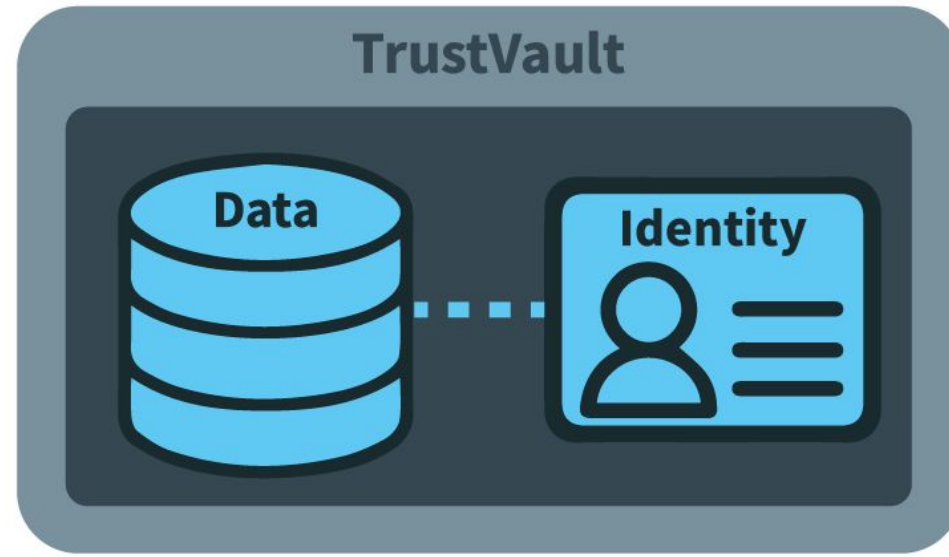


Architecture and Design

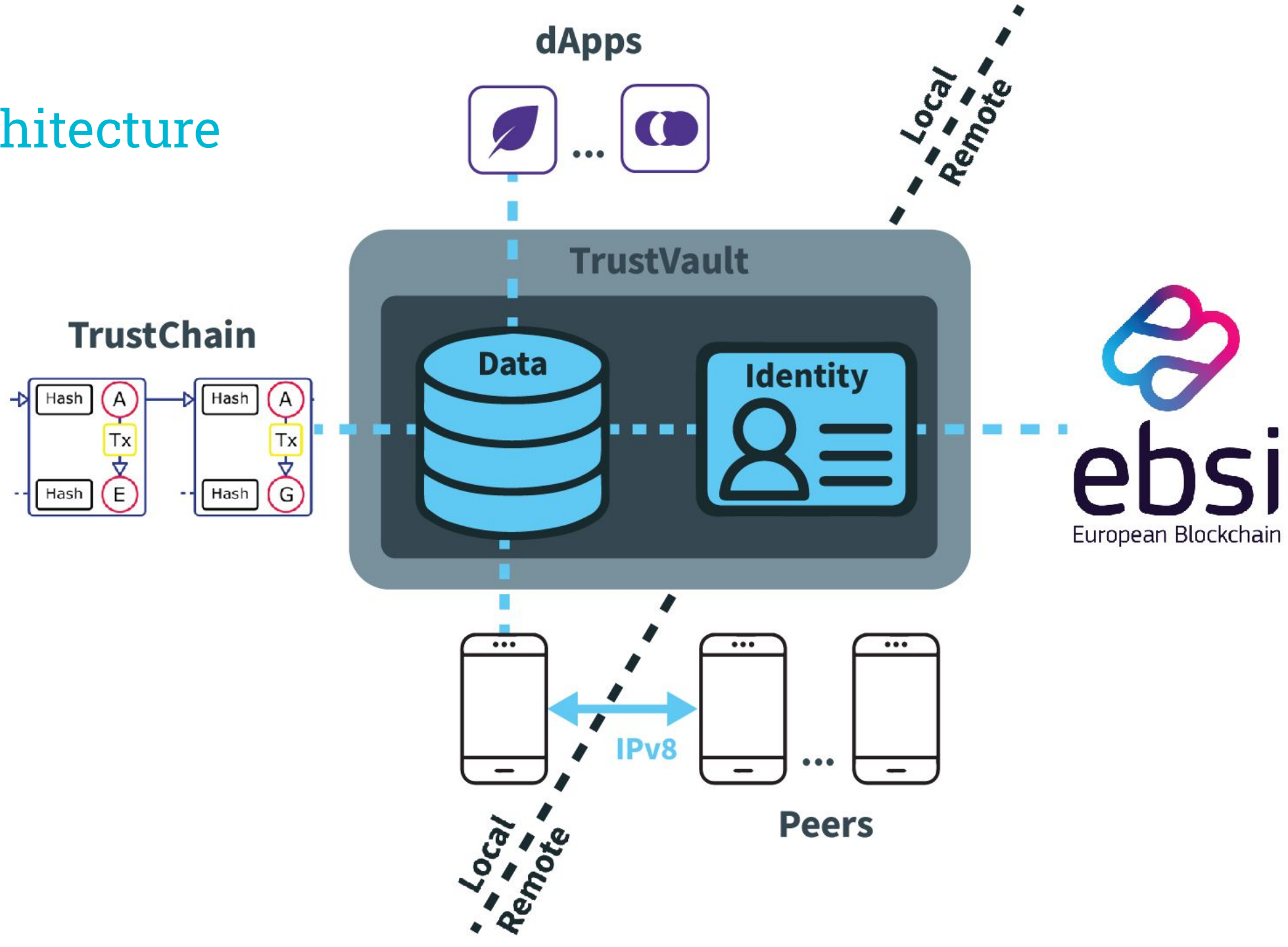
Architecture



Architecture

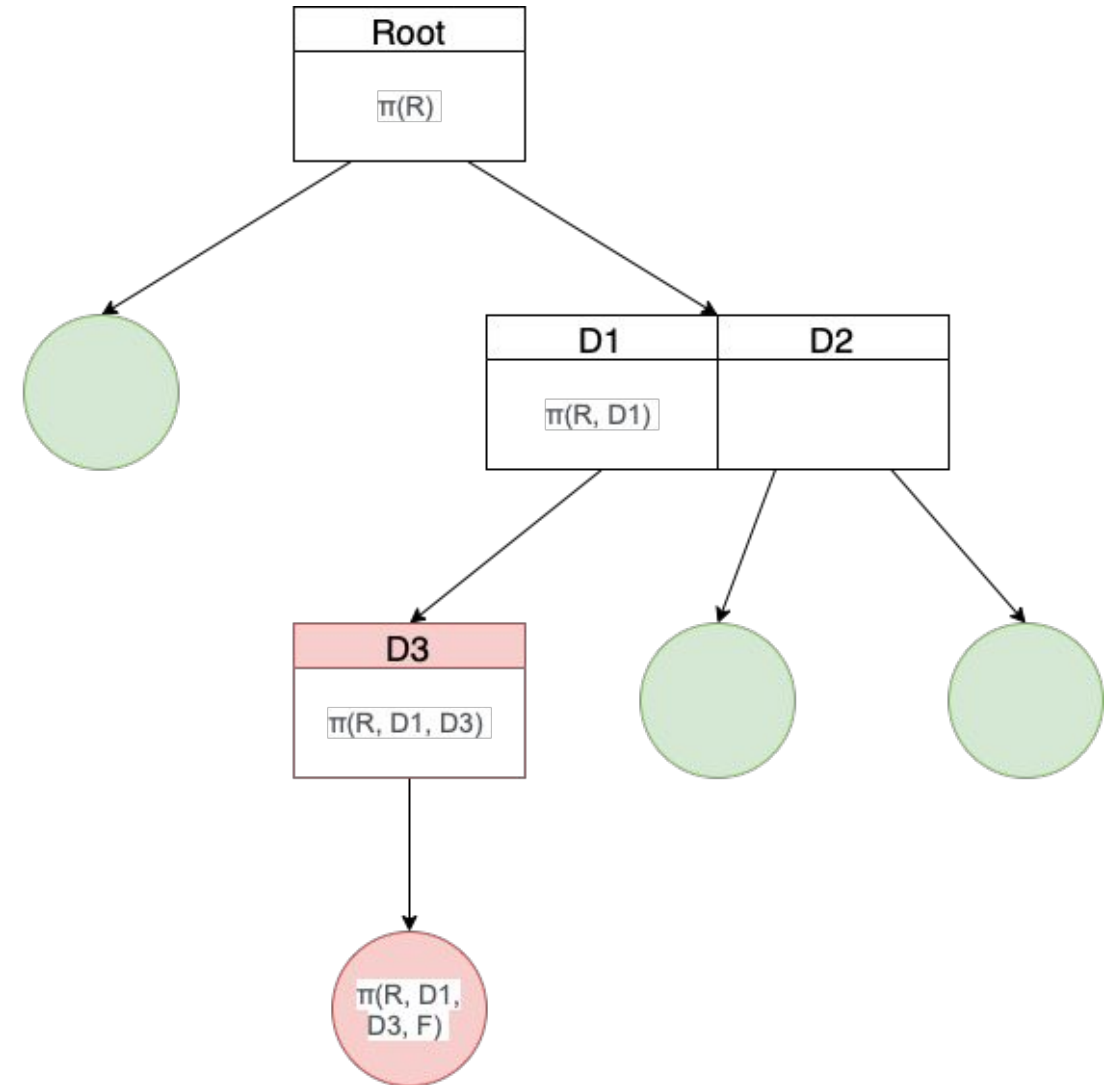


Architecture



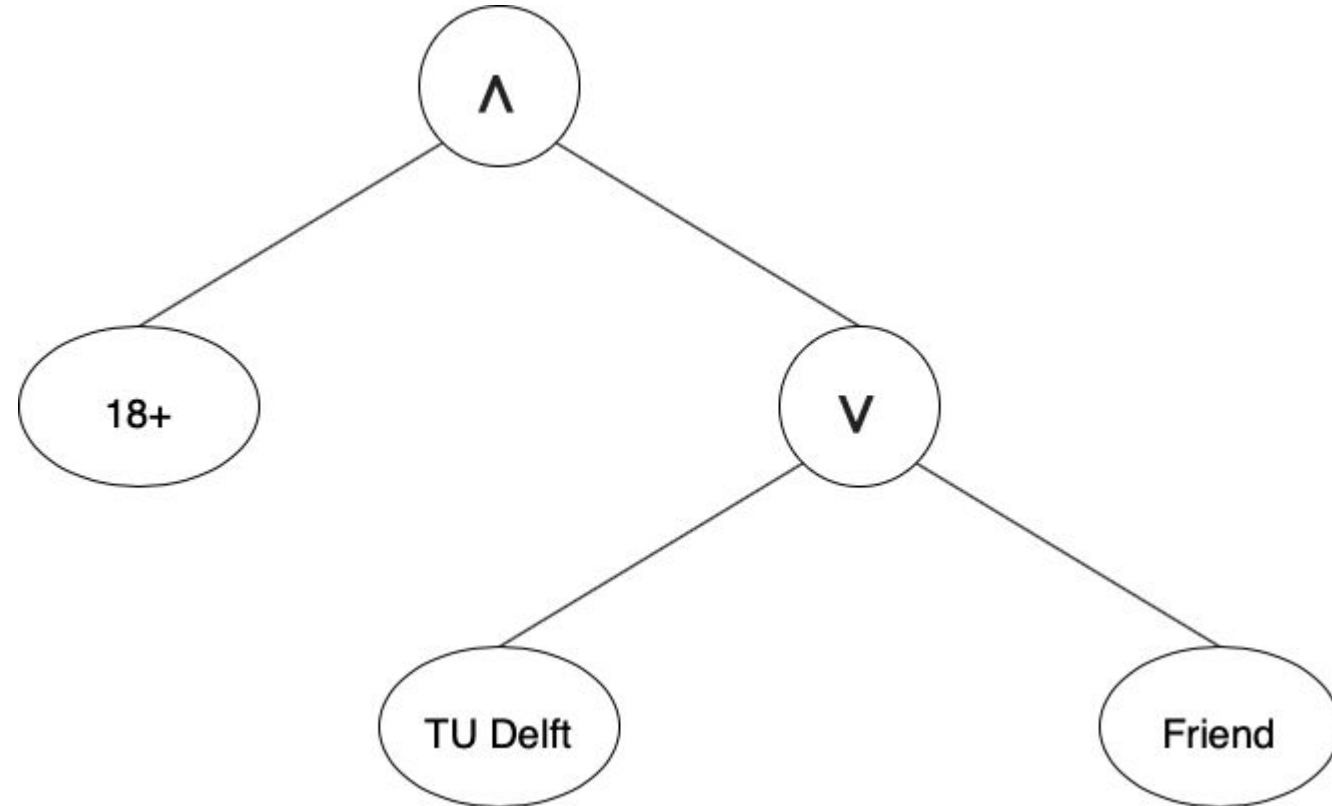
Access Control

- Files and folders have associated access policy file
- Local policy $\pi(f)$
- Global $\Pi(f) = \pi(f) \wedge \Pi(P(f))$
- Every policy along the root path
- Minimal restrictions on the root folder
- Increasingly specific policies for sub-folders

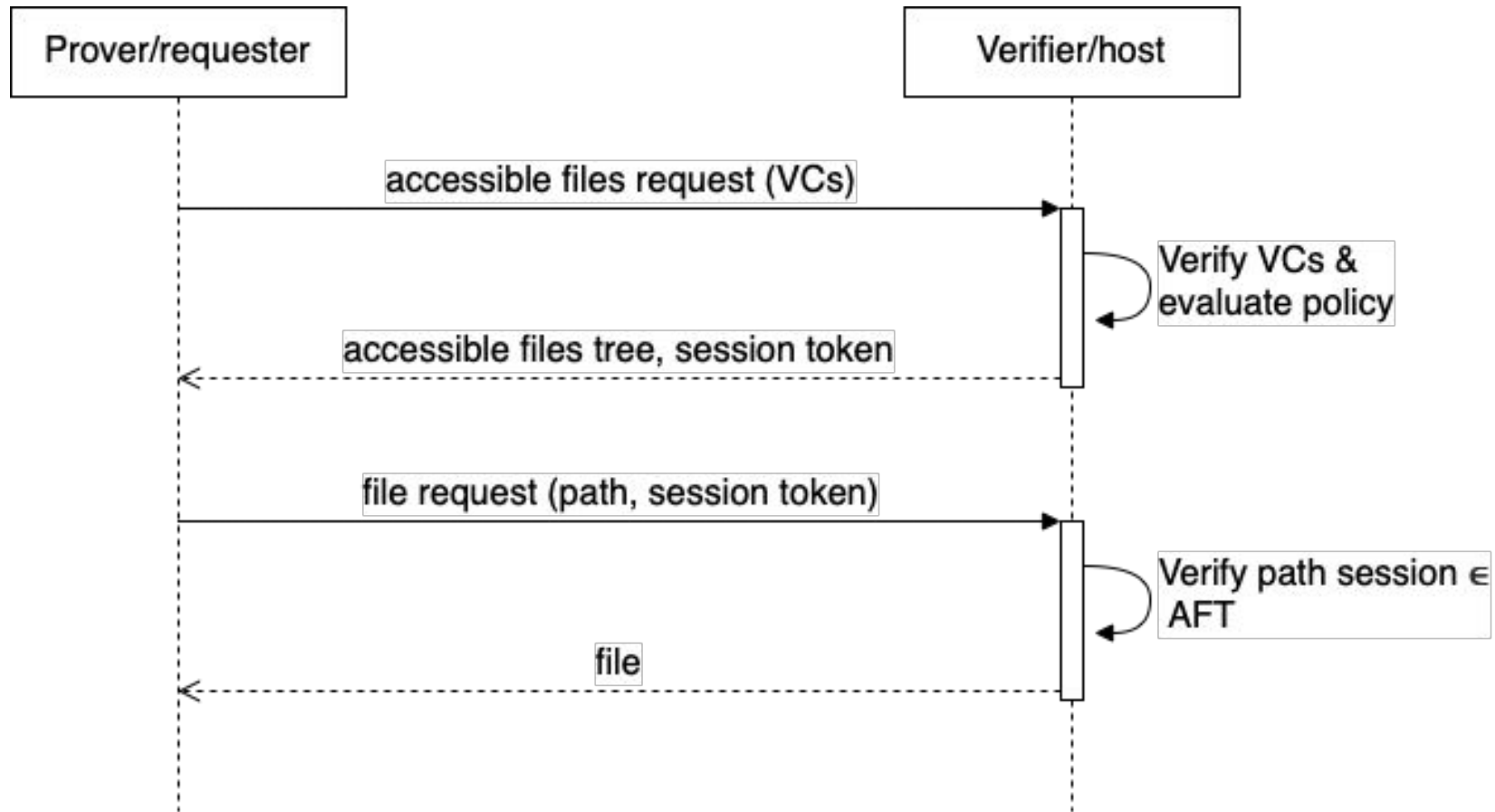


Access Control

- Access policies are boolean expression trees
- Attribute rules at the leaves
- Triplets in the form of *(attribute, operator, value)*



Access Control

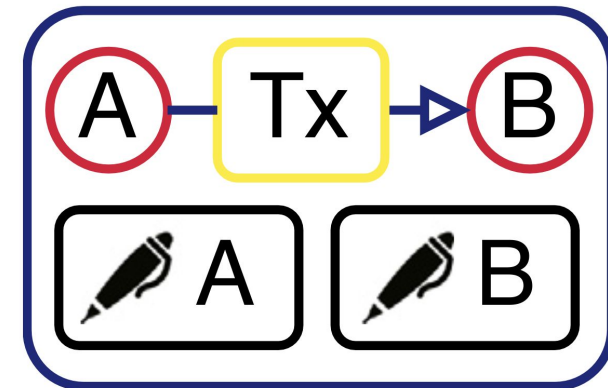


Self-issued credentials

- Access policy based on the issuer of a credential
- Similar to follow/friend request in traditional social networks
- Attributes that give context about the relationship

Tamper-proof access log

- Keep record of accessibleFilesRequests on-chain
- Bloom filter that contains all accessible files
- Transaction with session key and bloom filter sent to requester
- Both sender and recipient sign transactions in TrustChain
- Timestamped, tamper-proof and irrefutable record



Bloom filter

- TODO

Data protection

- Data protected at rest
 - AES Counter mode encryption
 - Password required to unlock data vault
- End-to-end encryption using IPv8

Evaluation

Privacy +

- Self-hosted data
- Fine-grained access control on folder and file level
 - Mistakes in defining policies may end in unintentional disclosure
- Data minimisation: requesting only the minimum of information necessary
- Selective disclosure for the requester

Privacy -

- Peer identification by public key
 - Curious verifier can aggregate enough correlatable information over time
 - Not solved by having multiple DIDs
 - Network-Level Anonymity implemented in Python, not in Kotlin
- No private transactions on TrustChain
 - On-chain access logs are public for anyone to see

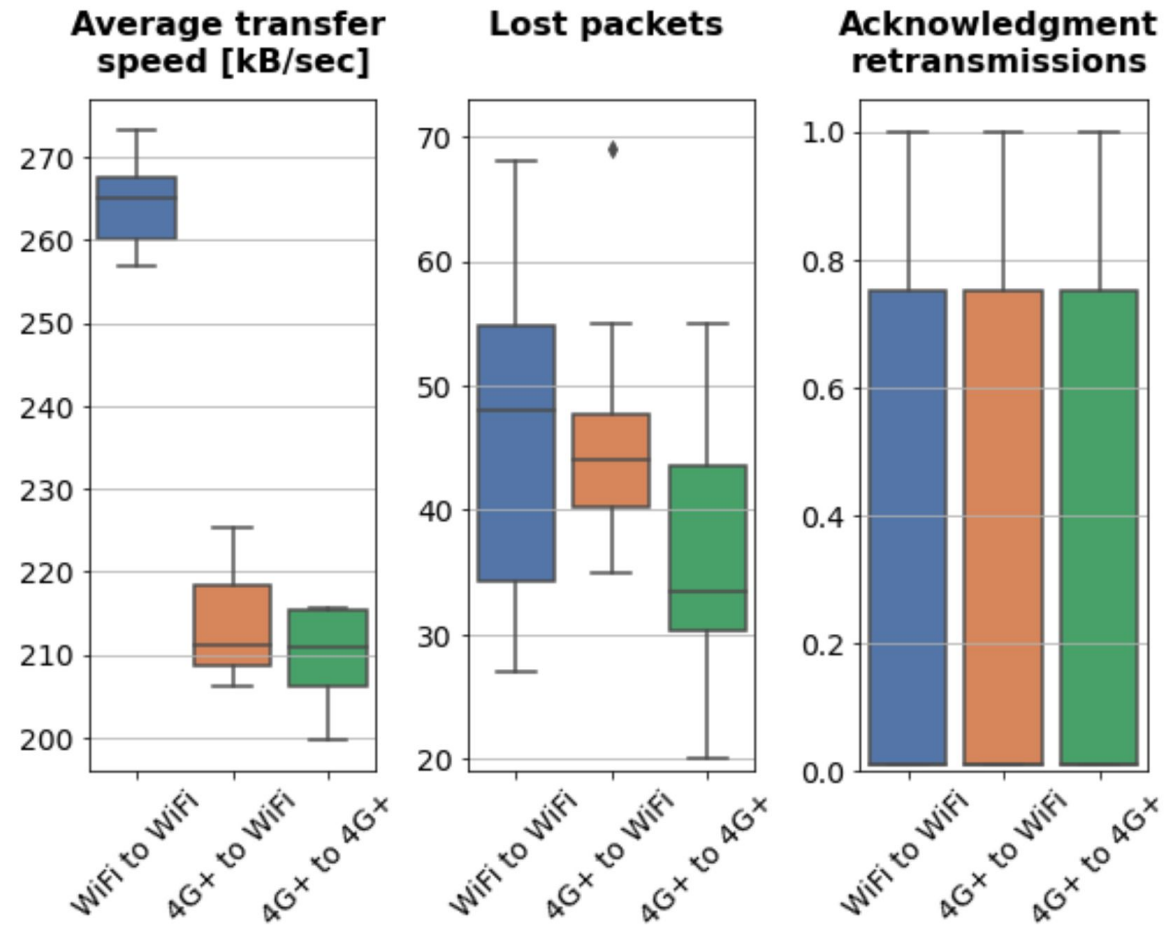
Security +

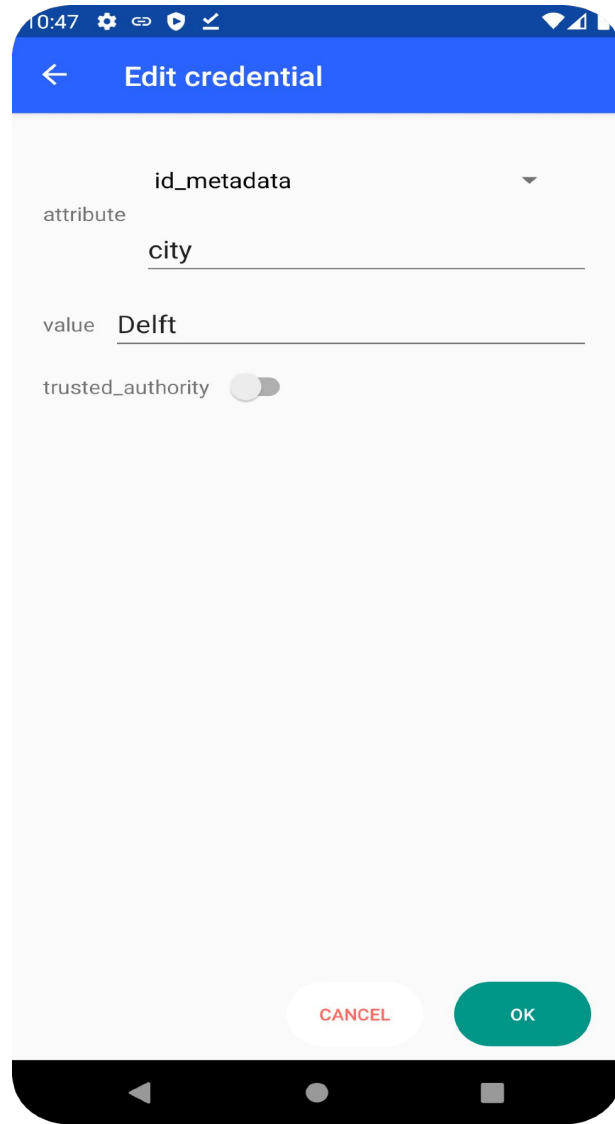
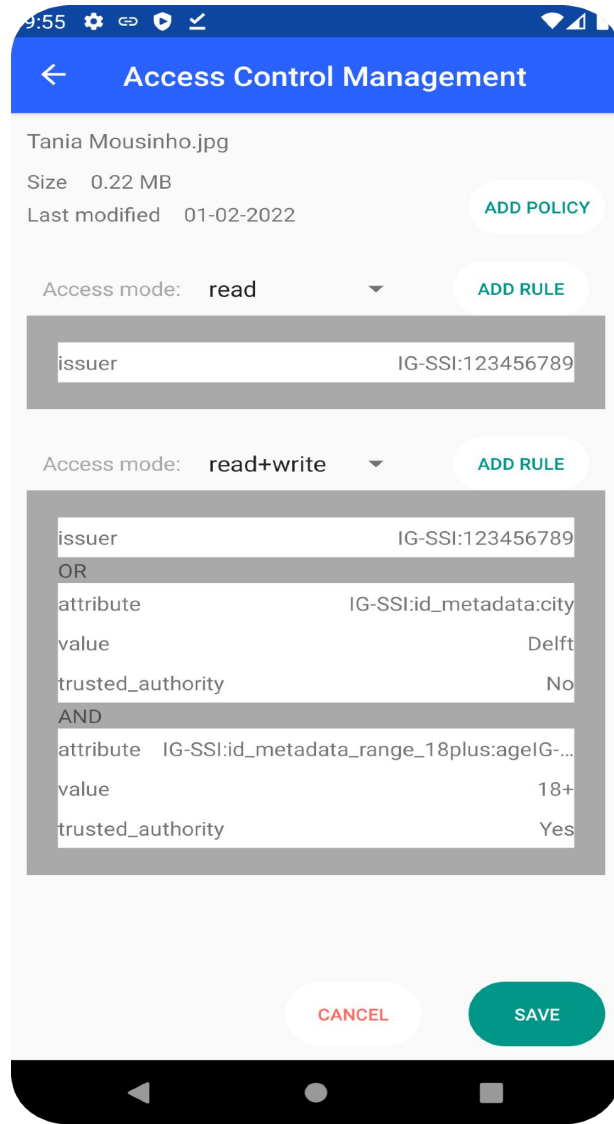
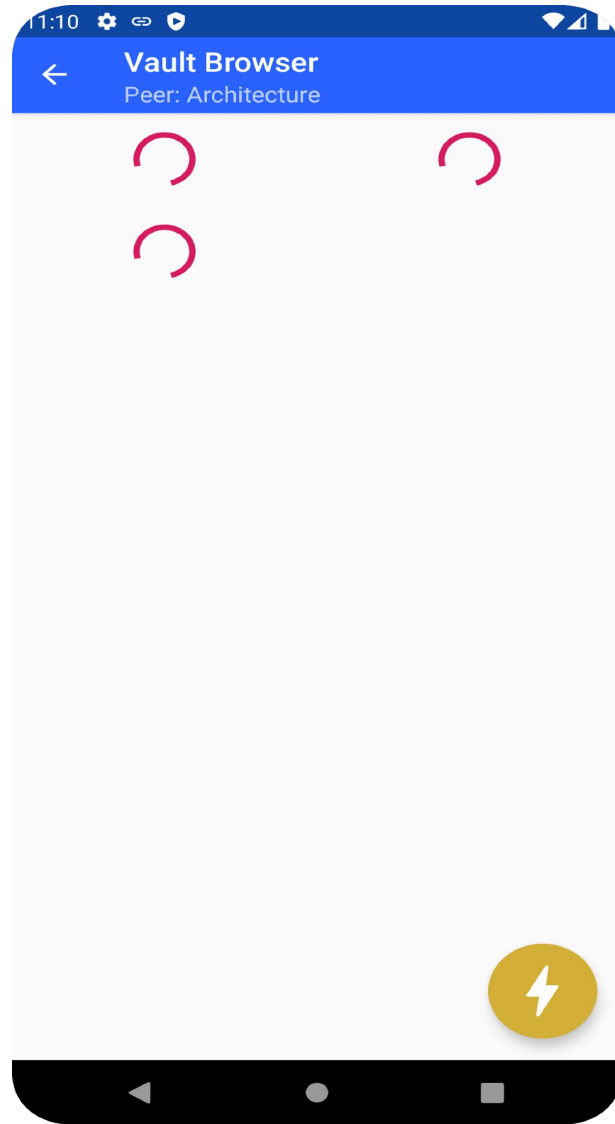
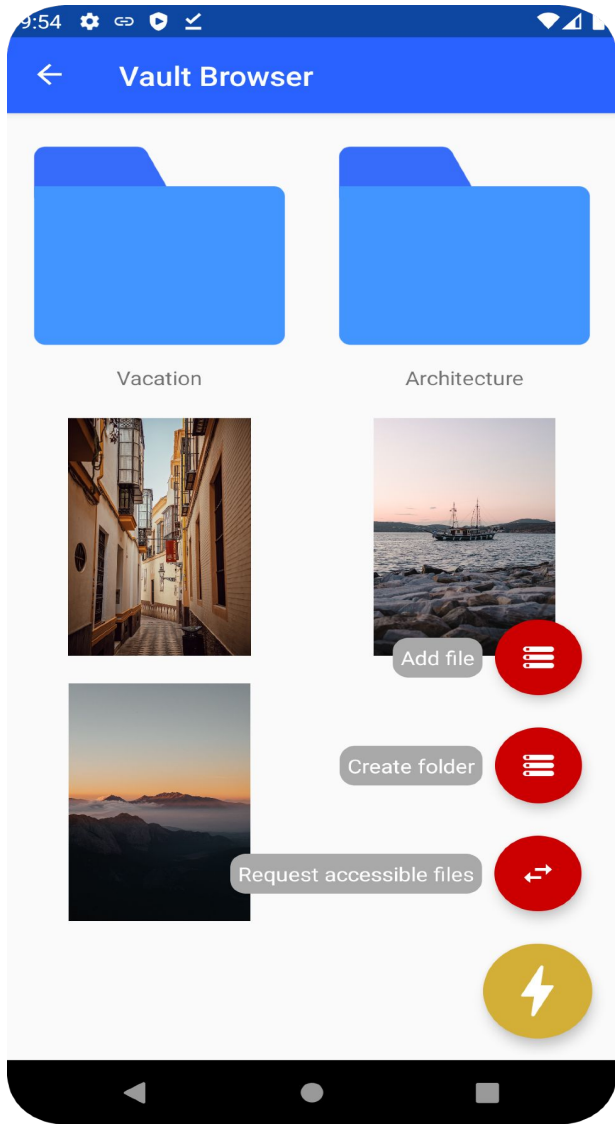
- Android internal file storage shielded from outside access
- Encryption at rest prevents unauthorised access even with physical access
- End-to-end encryption with message authentication
- IPv8 maintains p2p connection with changing physical addresses
- EBSI accreditation process for Trusted Issuers
 - Malicious, compromised or incompetent issuers could issue false credentials

Security -

- EBSI Verifiable Data Registry not convincing in requirement of accuracy
 - Hosted API layer between user and blockchain that can corrupt read/writes
 - Single point of failure
- No redundancy
 - Mobile devices can go out of service
 - Data loss if there is no back-up

Performance





Related Work

Related Work

- TODO

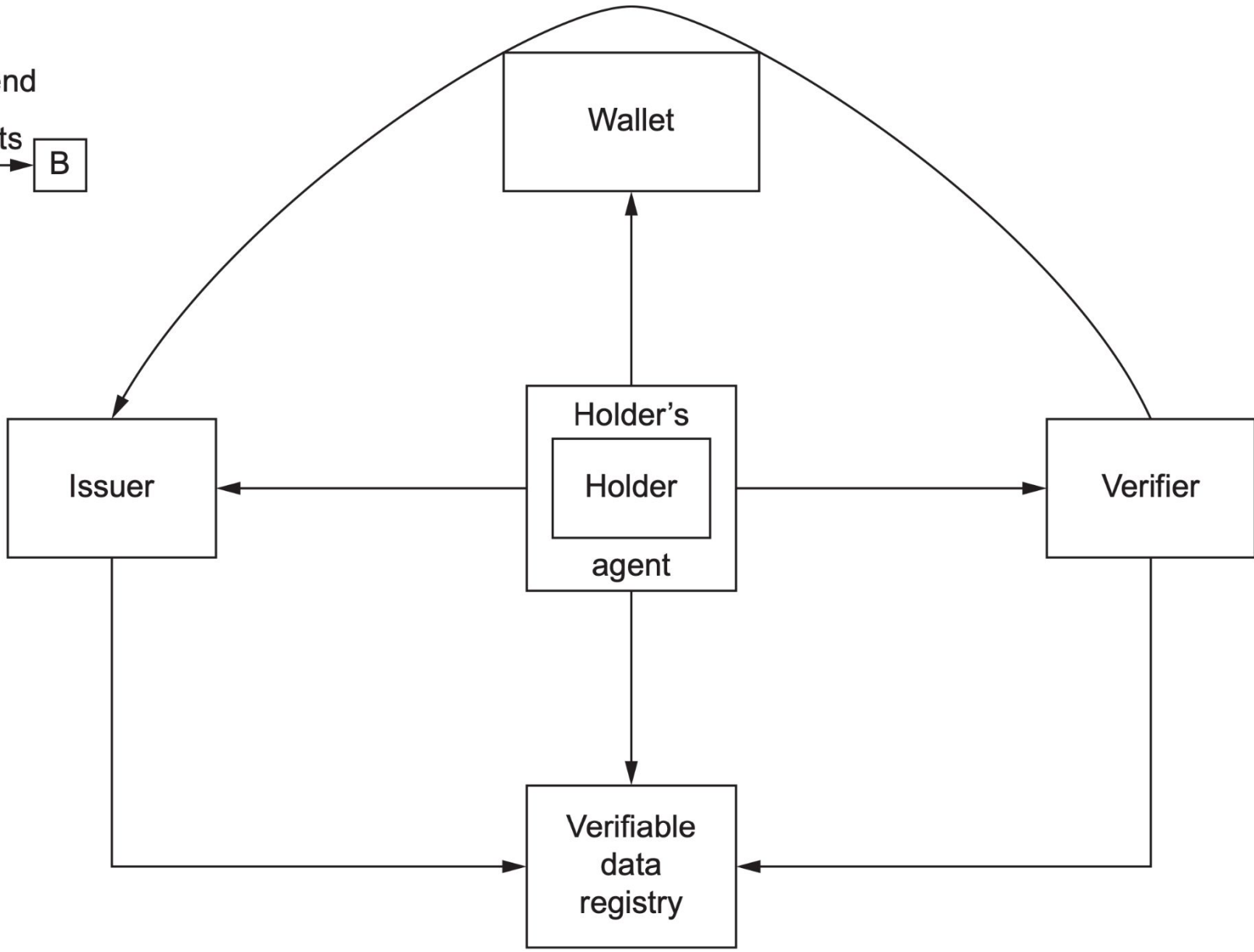
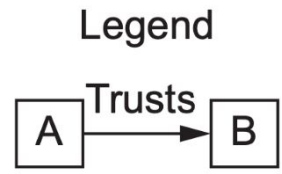
Conclusion

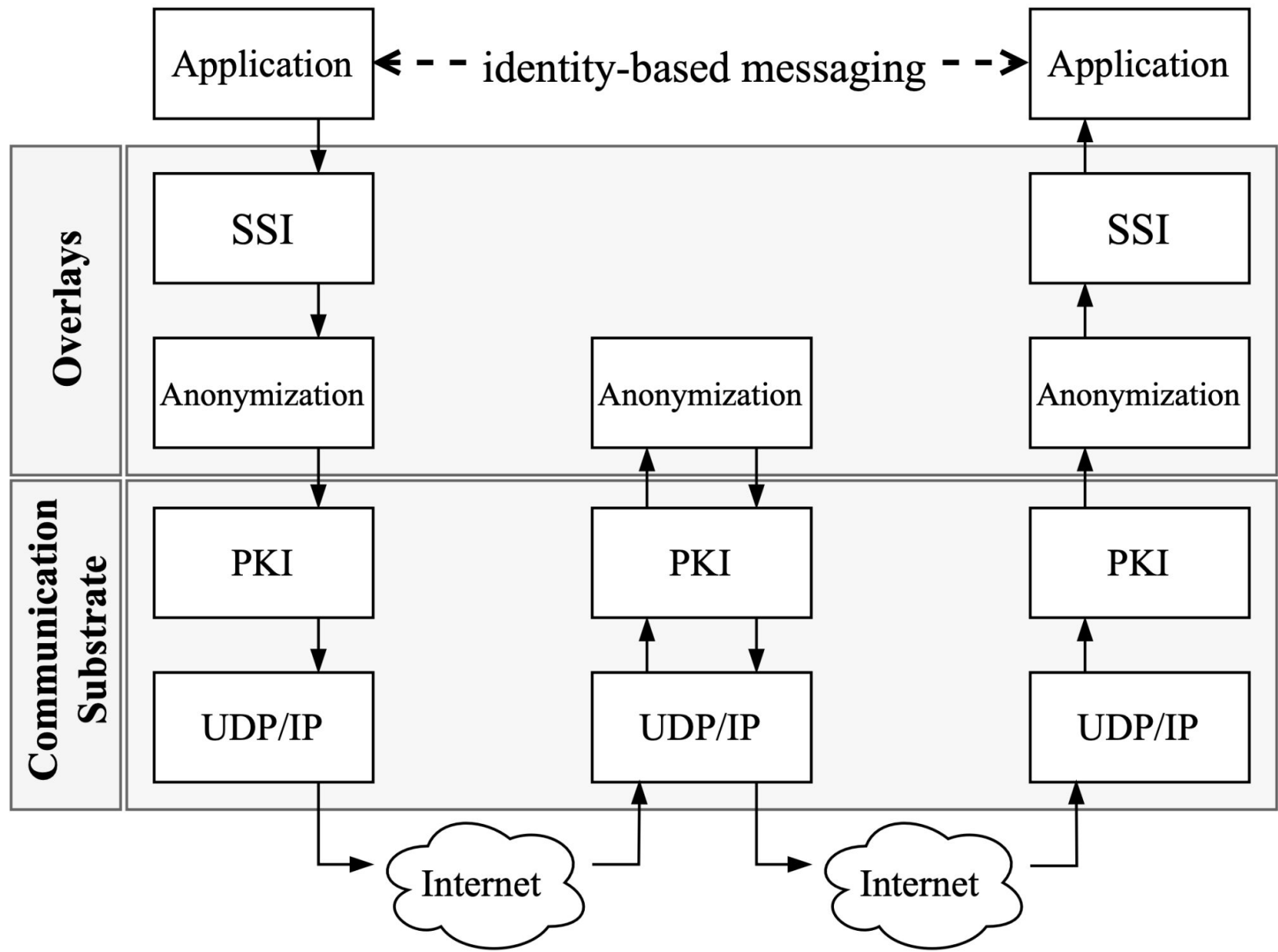
Conclusion

- TrustVault users are sovereign over identity and data
 - Secure, under user control and portable
- User data is stored locally, with fine-grained access control
- Build upon upcoming European Digital Identity Wallet
- EBSI is viable way of giving control to citizens
- Alternative for Big Tech
- Fair, competitive and transparent

Thanks for joining

Sharif Jacobino





```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/citizenship/v1"
  ],
  "id": "https://issuer.oidp.uscis.gov/credentials/83627465",
  "type": [
    "PermanentResidentCard",
    "VerifiableCredential"
  ],
  "description": "Government of Example Permanent Resident Card.",
  "identifier": "83627465",
  "name": "Permanent Resident Card",
  "credentialSubject": {
    "id": "did:example:b34ca6cd37bbf23",
    "type": [
      "Person",
      "PermanentResident"
    ],
    "familyName": "SMITH",
    "gender": "Male",
    "givenName": "JOHN"
  },
  "expirationDate": "2029-12-03T12:19:52Z",
  "issuanceDate": "2019-12-03T12:19:52Z",
  "issuer": "did:example:489398593",
  "proof": {
    "type": "BbsBlsSignatureProof2020",
    "created": "2020-04-26T04:21:07Z",
    "verificationMethod": "did:example:489398593#test",
    "proofPurpose": "assertionMethod",
    "proof":
"G0/i24loDTTgUtMCGM/jivlD260k93d9ek2FxB/L2NQMZANjKd13r+8yDIRqD5hB1HjIc1gY3Y/lwexZNUa+BA laXBQZa8iXhY
LK8kUvQHdYZmkBwL3Whyqptl2hkgNIIdCnpqoBH+L9DmIZH9iGwrzYJ6rx/AAAAdIu4GCCrIhQ1Vb/B0lHYaer1eTC+Sukw3ypVmN
kAU/oDTR4EcEsFcUbiM9ThFKytMZ/uGC28463I/9Bb1JAL3F23JgUHe5eJzScg7Nu2hDHpkSk04/NaExd0cA/Sle9qeo0bCi6trw
uP2+F6tptRavAAAACUiVcbDWp07LE8hMFmAfr0+DrWd7S0T2opAk6Qhe0TdnUfZI05gpCDEvXGnZ2pmnGYqcLnAjth/gwhAEfTST
nFGHyhzkZJD0NSjihxQD0x45pYSaIqiF0uM4iGLh79G5xU2Av+PBqbG4ASU1kzXa8N2cE6F7osL5LYKvm+yeGl2gDktCRwrcansu
LpVFJcFpIy4x2GUD3tkZFGKYpEm2Sc00bNzfYozLdKj4erTr17SjoHwYyHwiofPmb2PRcrknpYVJaxyrvVM9sn9gwEoI4dLJRbT6
'
    "revealStatements": [ 0, 1, 2, 4, 5, 6, 8, 9, 15, 16, 17, 18, 19, 20, 21, 22, 23 ],
    "totalStatements": 24,
    "nonce": "M/e44JTNSsfhnykE0yoD8eaYIdJARbpDIWFhu+TWwc70J5iwPHa8Q6bYQd1YjjxpV4c="
  }
}
```

```
{
  "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "EBSI Natural Person Verifiable ID",
  "description": "Schema of an EBSI Verifiable ID for a natural person participating in the educational use cases ",
  "type": "object",
  "allOf": [
    {
      "$ref": "https://api.preprod.ebsi.eu/trusted-schemas-registry/v1/schemas/0x28d76954924d1c4747a4f1f9e3e9edc9ca965efbf8ff20e4339c2bf2323a5773"
    },
    {
      "properties": {
        "credentialSubject": {
          "description": "Defines additional properties on credentialSubject to describe IDs that do not have a substantial level of assurance.",
          "type": "object",
          "properties": {
            "id": {
              "description": "Defines a unique identifier of the credential subject",
              "type": "string"
            },
            "identifier": {
              "description": "Defines an alternative identifier for the person ",
              "type": "array",
              "items": {
                "$ref": "#/definitions/identifier"
              }
            },
            "familyName": {
              "description": "Defines current family name(s) of the credential subject",
              "type": "string"
            },
            "firstName": {
              "description": "Defines current first name(s) of the credential subject",
              "type": "string"
            },
            "dateOfBirth": {
              "description": "Defines date of birth of the credential subject",
              "type": "string",
              "format": "date"
            },
            "personalIdentifier": {
              "description": "Defines the unique national identifier of the credential subject (constructed by the sending Member State in accordance with the te",
              "type": "string"
            },
            "nameAndFamilyNameAtBirth": {
              "description": "Defines the first and the family name(s) of the credential subject at the time of their birth",
              "type": "string"
            }
          }
        }
      }
    }
  ]
}
```

1.Summary of the report

This report certifies the conformance of Web Wallet 0.2.0 distributed by walt.id to the EBSI specifications v1.0.0 on 01/03/2022. The results and details of the tests can be found hereunder:

Test ID	Timestamp	Results
ONBOARD_01_A	2022-02-15 16:02:00	Successful
ONBOARD_02_A	2022-02-15 16:02:00	Successful
ONBOARD_051	N/A	N/A
ONBOARD_052	2022-02-15 16:02:00	Successful
ONBOARD_061	2022-02-15 16:02:00	Successful
ONBOARD_062	N/A	N/A
ONBOARD_063	N/A	N/A
ISSUE_011	2022-02-15 16:02:00	Successful
ISSUE_021	2022-02-15 16:02:00	Successful
ISSUE_031	2022-02-15 16:02:00	Successful
VERIFY_011	2022-02-15 16:02:00	Successful
VERIFY_031	2022-02-15 16:02:00	Successful
ISSUE_041	N/A	N/A
ISSUE_051	N/A	N/A
ISSUE_052	N/A	N/A
ISSUE_061	N/A	N/A
ISSUE_062	N/A	N/A
ISSUE_065	N/A	N/A
VERIFY_041	N/A	N/A
VERIFY_051	N/A	N/A
VERIFY_061	N/A	N/A
VERIFY_064	N/A	N/A

2.Detailed results

ISSUE_011 - Requests Verifiable Attestation (VA)

ISSUE_011

2022-02-15 11:02:00

```
{"logNumber":18,"body":{"state":"teststate","code":"202f157ab816626a4826"},"conformance":"286dc8c9-15ce-4f4b-a32b-8ce5a5b7c4f5","date":"2022-02-15T10:50:47.000Z","service":"conformance","url":"/conformance/v1/issuer-mock/authorize?scope=openid&claims=%7B%22credentials%22%3A%5B%7B%22type%22%3A%22https%3A%5C%2F%5C%2Fapi.preprod.ebsi.eu%5C%2Ftrusted-schemas-registry%5C%2Fv1%5C%2Fschemas%5C%2F0x14b05b9213dbe7d343ec1fe1d3c8c739a3f3dc5a59bae55eb38fa0c295124f49%23%22%7D%5D%7D&response_type=code&redirect_uri=http%3A%2F%2Fblank&state=teststate&nonce=testnonce&client_id=http%3A%2F%2Fblank","type":"response","method":"GET","status":200}
```

2022-02-15 11:02:00

```
{"logNumber":26,"body":{"state":"teststate","code":"b4afa21fba719bff0d03"},"conformance":"286dc8c9-15ce-4f4b-a32b-8ce5a5b7c4f5","date":"2022-02-15T10:55:44.000Z","service":"conformance","url":"/conformance/v1/issuer-mock/authorize?scope=openid&claims=%7B%22credentials%22%3A%5B%7B%22type%22%3A%22https%3A%5C%2F%5C%2Fapi.preprod.ebsi.eu%5C%2Ftrusted-schemas-registry%5C%2Fv1%5C%2Fschemas%5C%2F0x14b05b9213dbe7d343ec1fe1d3c8c739a3f3dc5a59bae55eb38fa0c295124f49%23%22%7D%5D%7D&response_type=code&redirect_uri=http%3A%2F%2Fblank&state=teststate&nonce=testnonce&client_id=http%3A%2F%2Fblank","type":"response","method":"GET","status":200}
```

2022-02-15 11:02:00

```
{"logNumber":34,"body":{"state":"teststate","code":"2131761da6cfb1fb4608"},"conformance":"286dc8c9-15ce-4f4b-a32b-8ce5a5b7c4f5","date":"2022-02-15T10:58:40.000Z","service":"conformance","url":"/conformance/v1/issuer-mock/authorize?scope=openid&claims=%7B%22credentials%22%3A%5B%7B%22type%22%3A%22https%3A%5C%2F%5C%2Fapi.preprod.ebsi.eu%5C%2Ftrusted-schemas-registry%5C%2Fv1%5C%2Fschemas%5C%2F0x14b05b9213dbe7d343ec1fe1d3c8c739a3f3dc5a59bae55eb38fa0c295124f49%23%22%7D%5D%7D&response_type=code&redirect_uri=http%3A%2F%2Fblank&state=teststate&nonce=testnonce&client_id=http%3A%2F%2Fblank","type":"response","method":"GET","status":200}
```

2022-02-15 12:02:00

```
{"logNumber":42,"body":{"state":"teststate","code":"823703526ef2c2a0c890"},"conformance":"286dc8c9-15ce-4f4b-a32b-8ce5a5b7c4f5","date":"2022-02-15T11:07:59.000Z","service":"conformance","url":"/conformance/v1/issuer-mock/authorize?scope=openid&claims=%7B%22credentials%22%3A%5B%7B%22type%22%3A%22https%3A%5C%2F%5C%2Fapi.preprod.ebsi.eu%5C%2Ftrusted-schemas-registry%5C%2Fv1%5C%2Fschemas%5C%2F0x14b05b9213dbe7d343ec1fe1d3c8c739a3f3dc5a59bae55eb38fa0c295124f49%23%22%7D%5D%7D&response_type=code&redirect_uri=http%3A%2F%2Fblank&state=teststate&nonce=testnonce&client_id=http%3A%2F%2Fblank","type":"response","method":"GET","status":200}
```

insertDidDocument

Call to build an unsigned transaction to insert a new DID Document.

Parameters:

- **from**: Ethereum address of the signer
- **identifier**: DID identifier (hexadecimal)
- **hashAlgorithmId**: ID of the hash algorithm used to hash the DID Document
- **hashValue**: hash of the canonicalized DID Document
- **didVersionInfo**: stringified JSON DID Document (hex-encoded)
- **timestampData**: data to be added to the timestamp (stringified JSON encoded in hexadecimal)
- **didVersionMetadata**: DID Document metadata (stringified JSON encoded in hexadecimal)

- Create a JSON-LD format DID Document compliant with W3C format (<https://www.w3.org/TR/did-core/>) and following ESSIF Model.
- Canonise the JSON-LD with URNDA2012 (using <https://github.com/digitalbazaar/rdf-canonize-native>)
- Encode in Base64url

Your request status changed to: **Waiting for customer** 13/Apr/22 4:01 PM



13/Apr/22 4:01 PM

Dear [Sharif Jacobino](#)

Could you please provide more information and logs?

Thank you

Best Regards

EBSI Support Office

DETAILS

Subject

Issue with the website

User

Wallet provider

Company name/Organisation

TU Delft

Description

We have been going through the wallet conformance testing steps but some api's (e.g. did-registry/v2/identifiers/{did}) has been timing out since last week, preventing us from advancing with the test program.

Request created

12/Apr/22 1:50 PM



Sharif Jacobino Just now

Hi, thanks for looking at the issue. The api's in question seem to be working again.

However, the users-onboarding/v1/authentication-responses api now returns an error it did not before without any change on my side
{"title":"invalid_signature: Signature invalid for JWT","status":400,"type":"about:blank"}

. Has there been any change there?

Your request status changed to: **Waiting for customer** 2 days ago 12:30 PM



2 days ago 12:30 PM

Dear [Sharif Jacobino](#)

We fixed the issue. Could you please re-try WCT ?

Best Regards

EBSI Support office

Your request status changed to: **Waiting for support** 6 days ago 9:45 AM



Sharif Jacobino 6 days ago 9:45 AM

Simply trying out and api call on Swagger (<https://api.conformance.intebesi.xyz/docs/?urls.primaryName=DID%20Registry%20API#/DID%20Documents/get-did-registry-v2-identifier>) or doing a curl request (curl -X 'GET' \ 'https://api.conformance.intebesi.xyz/did-registry/v2/identifiers/did%3Aebsi%3AzsVGDm5zxnNgdEMenHm5yJ8' \ -H 'accept: application/did+ld+json') times out.

