Introduction to Decentralized Online Identities and How to Implement It Wrong

An Analysis on IATA Travel Pass

Pellaeon Lin, Citizen Lab @HITCON 2022

Pellaeon Lin

- Researcher at Citizen Lab, University of Toronto
- Security and privacy of mobile apps
- Past studies
  - TikTok vs Douyin - A Security and Privacy Analysis
  - Unmasked II: An Analysis of Indonesia and the Philippines’ Government-launched COVID-19 Apps
  - Unmasked: COVID-KAYA and the Exposure of Healthcare Worker Data in the Philippines
- Digital security trainer for Civil Society Organizations
- Linux desktop user, FOSS contributor

THE CITIZEN LAB

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

VELUT ARBOR ÆVO

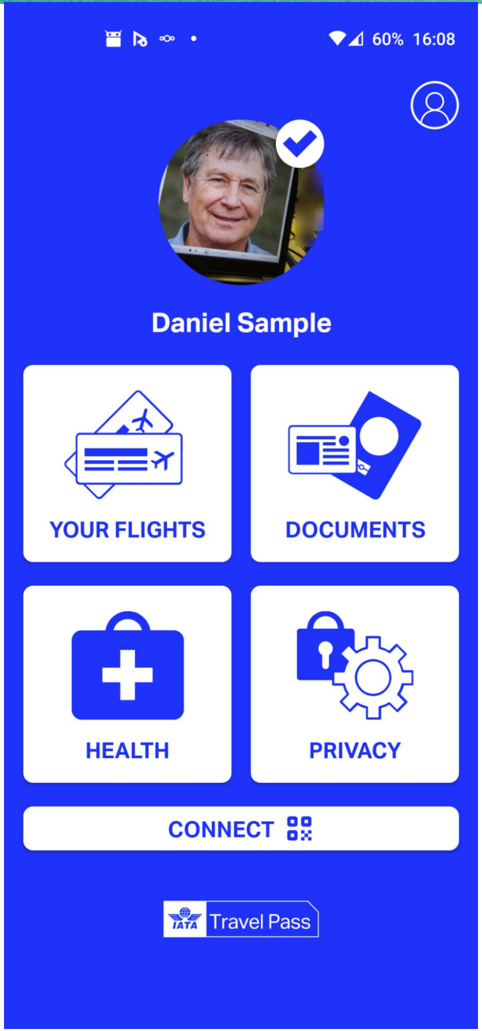
UNIVERSITY OF
TORONTO

Background:
IATA Travel Pass

IATA Travel Pass (ITP)

A global, opt-in app to receive, store, and share digital COVID-19 test certificates for flights

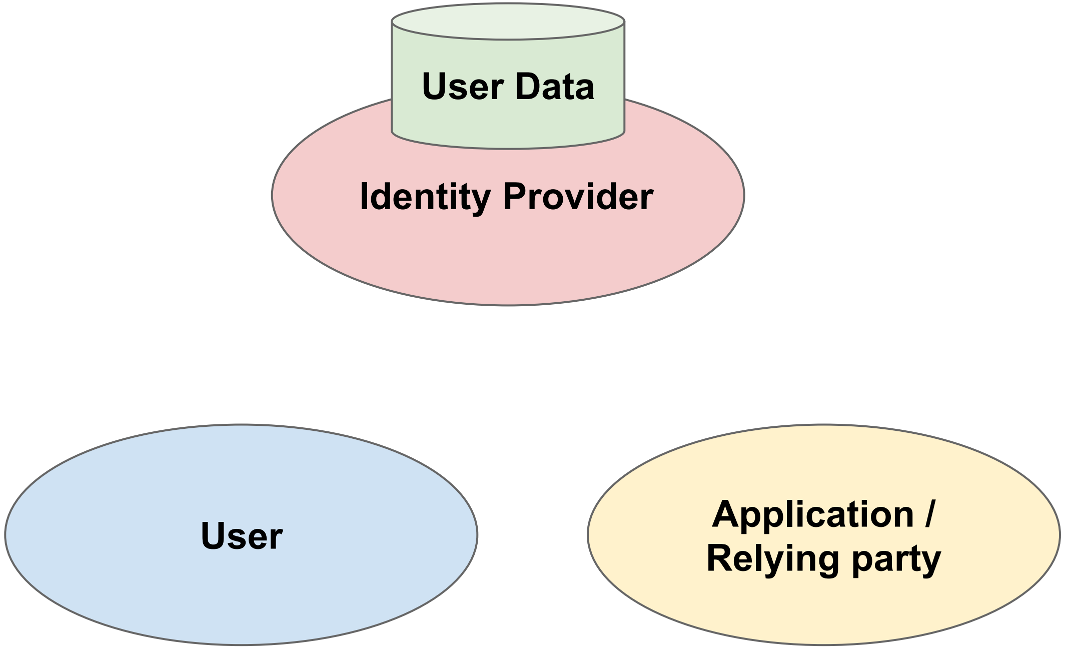
1. User registers on ITP by scanning passport and completing “liveness test”
2. User visits a COVID-19 testing laboratory
3. Lab sends digital test result via ITP
4. Airport staff verifies the digital test result



Self-Sovereign Identity (SSI)

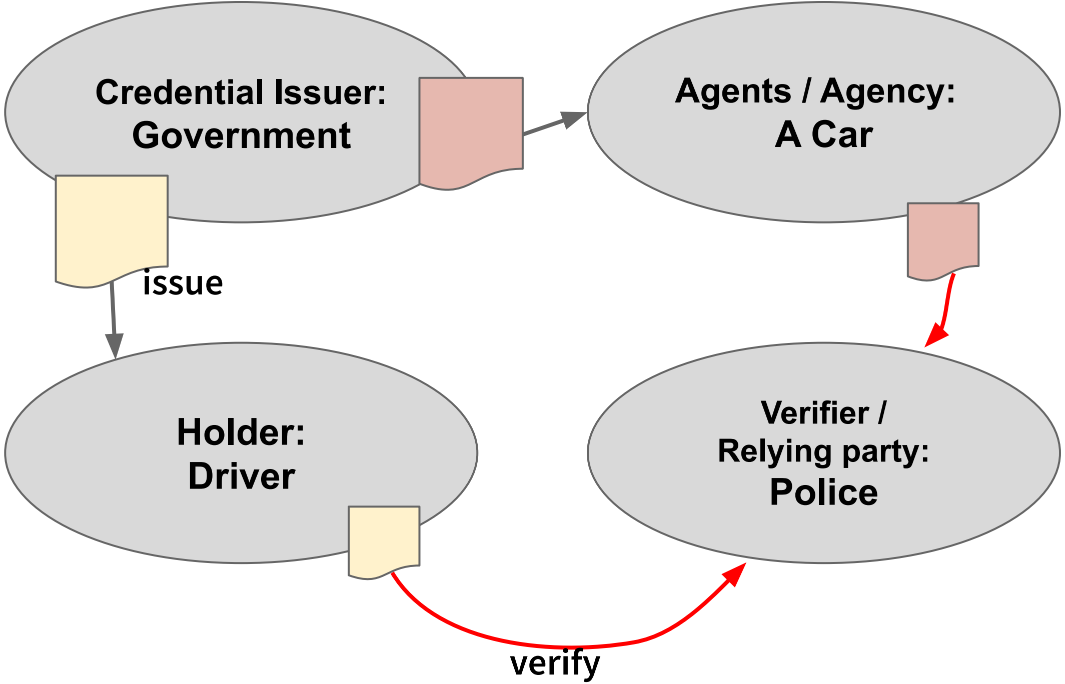
Conventional online identity systems, such as OAuth

- Users entrust their data to the Identity Provider
- Applications request users' permission to obtain their data
- Applications obtain user data from the Identity Provider



Self-Sovereign Identity systems: Metaphor to real world credentials

- Governments issue driver's licences and car plates (credentials)
- Drivers and cars hold credentials
- Police verifies credentials

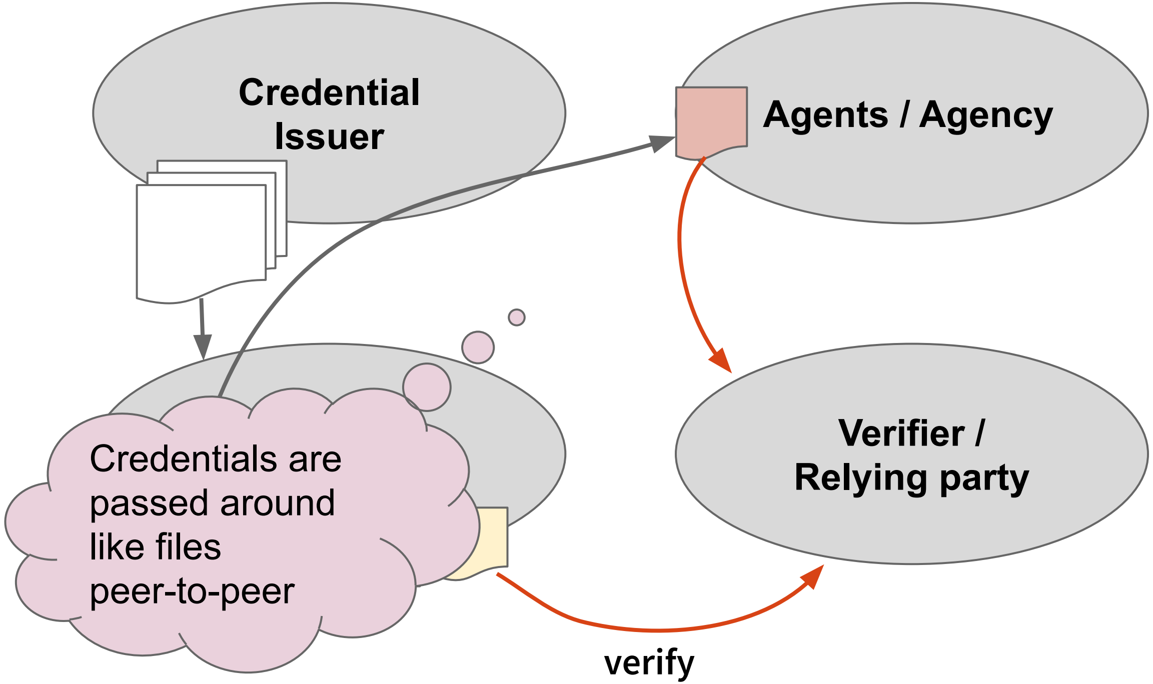


Credential Issuer: Government
Agents / Agency: A Car
issue
Holder: Driver
Verifier / Relying party: Police
verify

SSI is a category of technologies

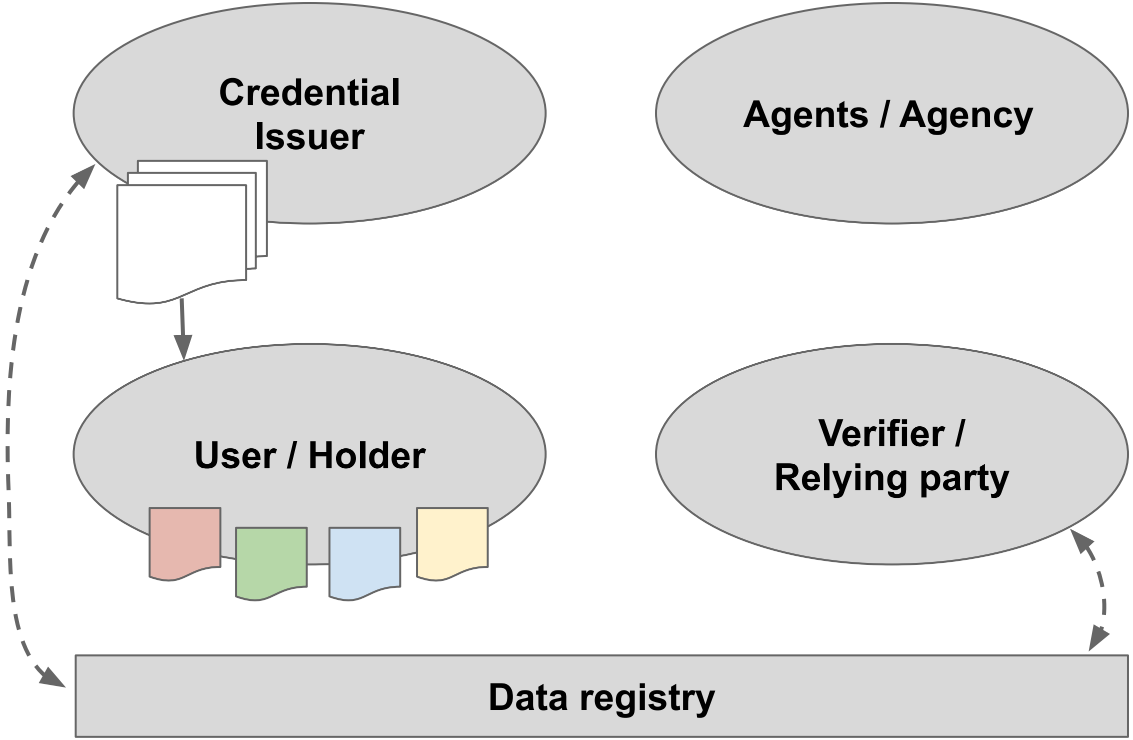
Self-Sovereign Identity systems

- "Credentials" are "certificates", which contain *statements*
- Issuer can issue any credential to any user
- Users can delegate credentials to agents
- Agents are robots / programs that act on behalf of a user
  - Cars
  - Mailboxes
- Verifiers request credentials from users or agents, and verifies the credentials



Self-Sovereign Identity system data registry

- Often, but not necessarily blockchains
- Facilitates peer communication
- Revocation registry
- Does not store private data



Verifiable Credentials

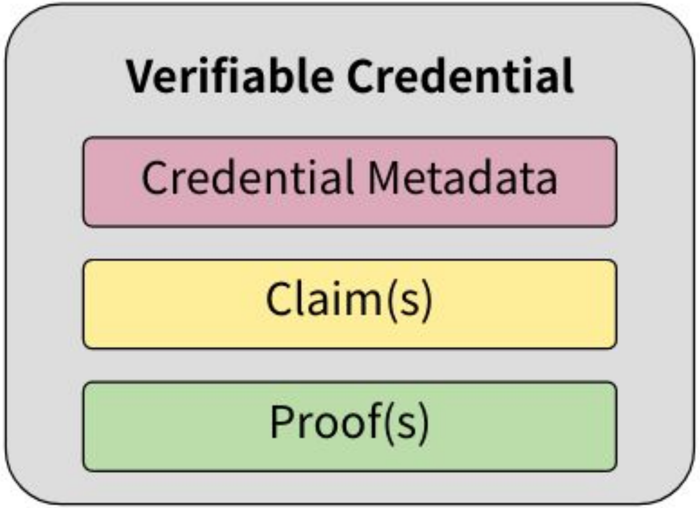
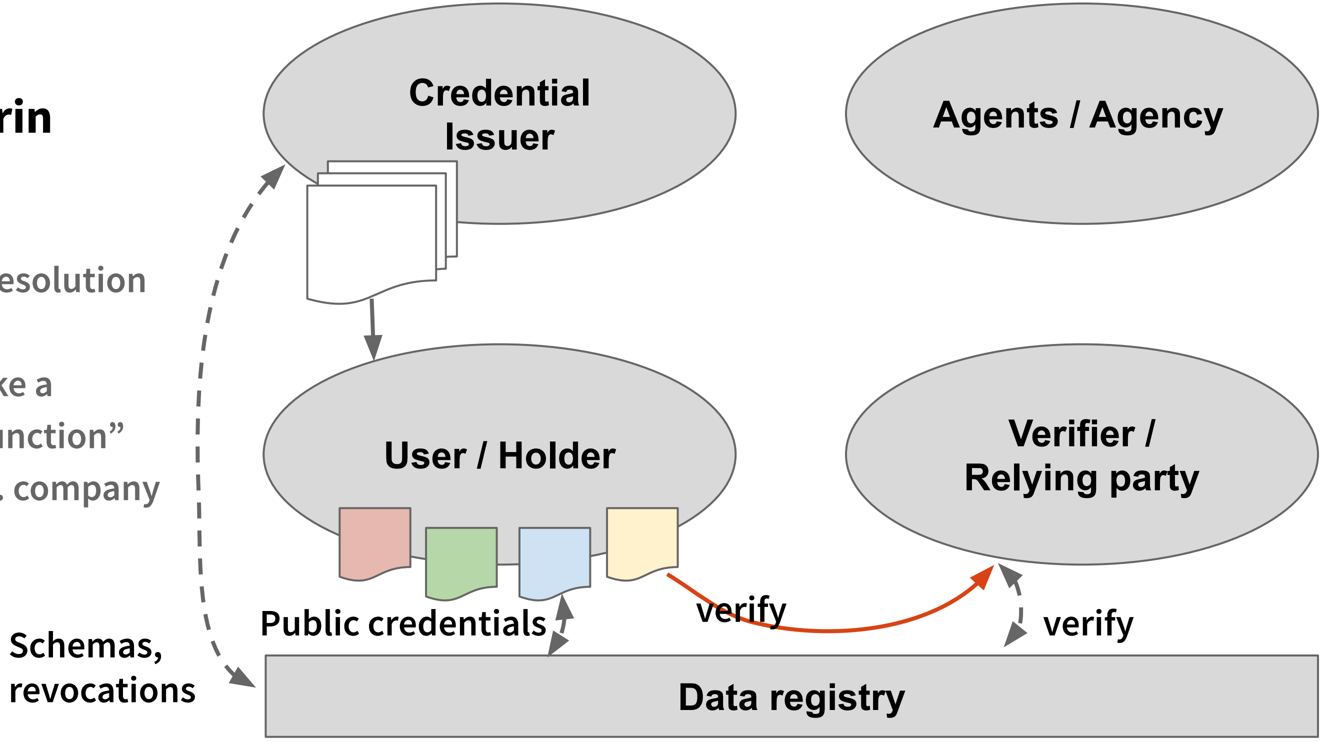


Figure 5 Basic components of a verifiable credential.

```
{
  "@context": [
       "https://www.w3.org/2018/credentials/v1",
       "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "AlumniCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
       "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
       "alumniOf": {
       "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
       "name": [{
       "value": "Example University",
       "lang": "en"
       }, {
       "value": "Exemple d'Université",
       "lang": "fr"
       }]
       }
  },
  "proof": {
       "type": "RsaSignature2018",
       "created": "2017-06-18T21:19:10Z",
       "proofPurpose": "assertionMethod",
       "verificationMethod":
"https://example.edu/issuers/565049#key-1",
       "jws":
"eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..T
CYt5XsITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy
7UJiN5mgRxD-WUcX16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS2
45-kronKb78cPN25DGlcTwLtj
       PAYuNzVBAh4vGHSrQyHUdBBPM"
  }
```

What goes on the Sovrin blockchain?

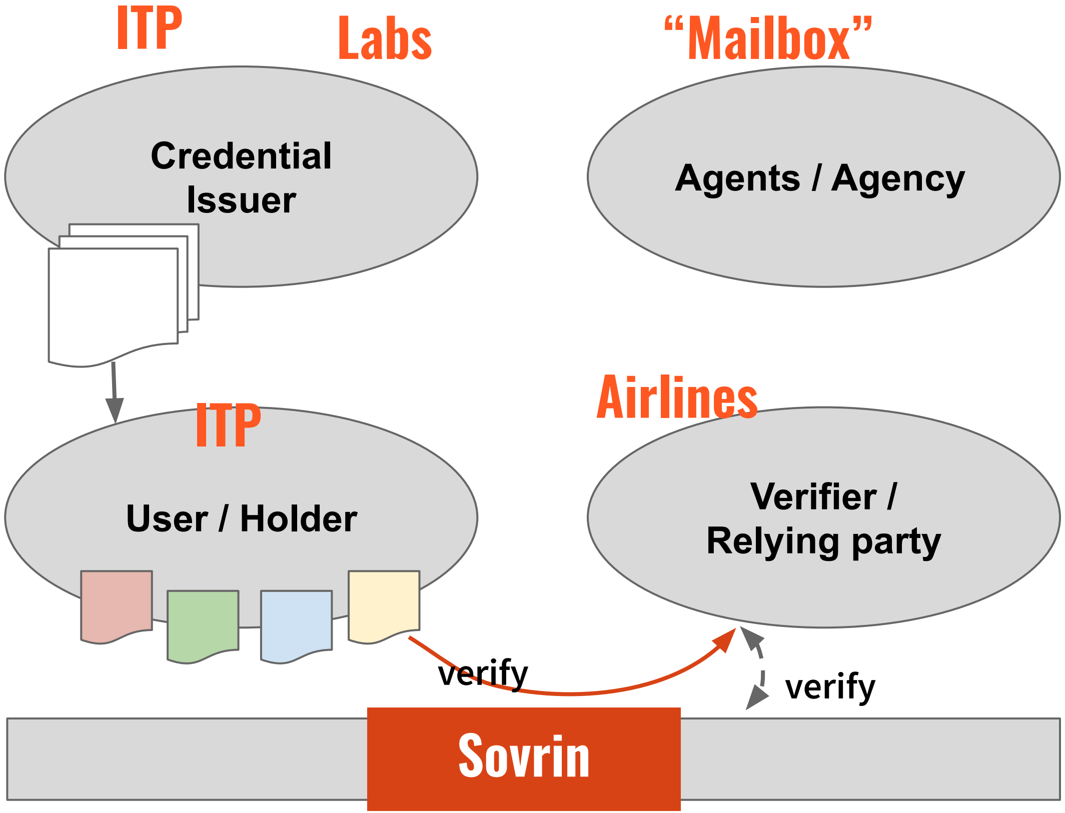
- Name and public key resolution
- Credential schemas
- Revocation registry: like a “compound hashing function”
- Public credentials, e.g. company registration
- Other



IATA Travel Pass

ITP using SSI

- Labs issue COVID test results to ITP
- ITP issues “digital passport” to itself
- Mailbox receive messages when ITP is not online
- ITP sends test results and digital passport to Airlines to verify
- Sovrin blockchain as data registry



IATA Travel Pass (ITP) User Flow

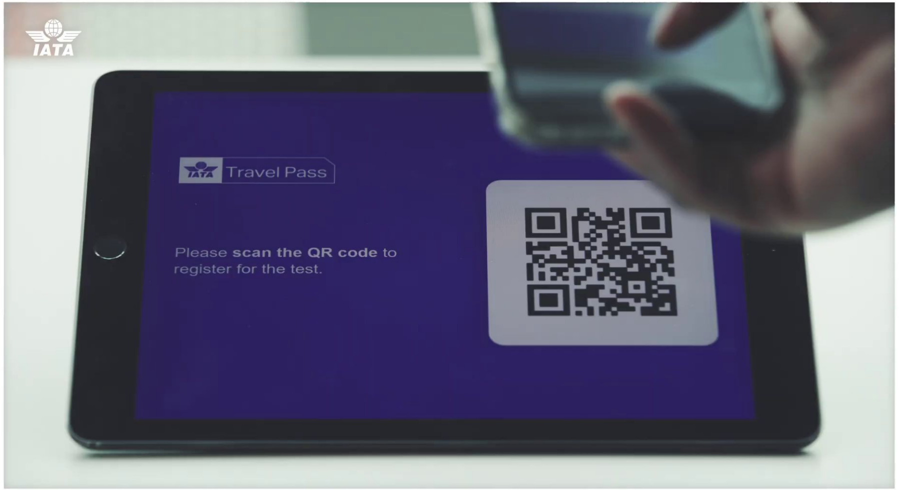
1. User registers on ITP by scanning passport and completing "liveness test"
2. User visits a COVID-19 testing laboratory
3. Lab sends digital test result via ITP
4. Airport staff verifies the digital test result

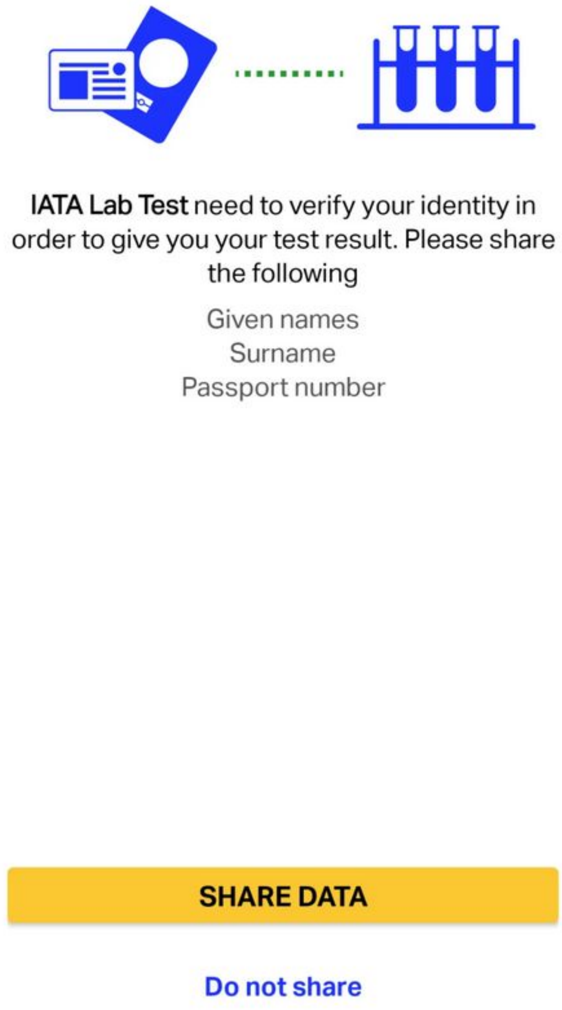
Technical Flow

1. ITP generates a self-asserted VC to represent the passport
2. ITP establishes an Aries connection with the lab
3. A VC denoting the test result is sent by the lab via the Aries connection to ITP
4. Airport staff establishes another connection with ITP, then
    a. Requests VC of a particular schema
    b. ITP sends over the VC
    c. Airport staff verifies the VC

Aries invitation:

To build an Aries *connection* between the lab and the user





IATA Lab Test need to verify your identity in order to give you your test result. Please share the following

Given names
Surname
Passport number

```
/invitation",
id>",

raduate credential",



1.0",
1.0"


,

ssage>"


egQDRm7EL"]
```

Sovrin, an SSI system

Sovrin = Verifiable Credentials (W3C standard)
+ **Aries protocol** (Hyperledger standard)
+ **Decentralized Identifiers** (W3C standard)
+ **Sovrin blockchain** (Hyperledger Indy instance)

Data format: Verifiable Credentials

- W3C standard

Data exchange protocol: Aries

- A high-level protocol defining the flows for onboarding users, messaging, issuing VCs, requesting proofs, encryption, etc
- Similar level as OAuth
- Transport: usually HTTP(S)
- Parties establish Aries *connections* with each other
- Aries *connection* denotes a communication relationship between parties
- *Connections* are peer-to-peer, but can be relayed by *agents*

Addressing and Naming: Decentralized Identifiers

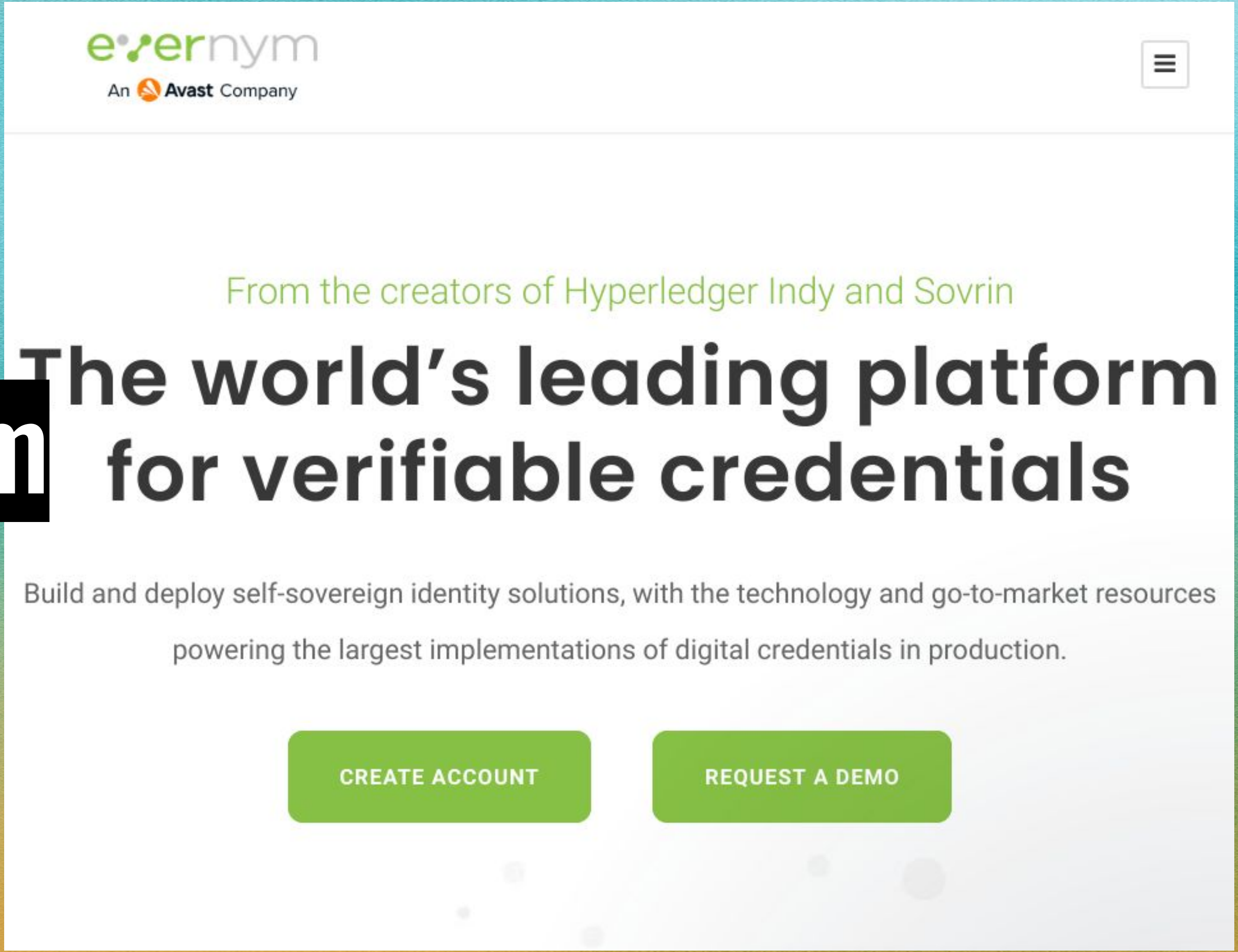
- Example: `did:sov:DNeU2RvXbosNfv5zcm9rwv`
- W3C Recommended Standard
- Purpose: resolve an identifier to a object or document, akin to DNS
- `sov` is the “method” of resolution
- DID standard does not actually specify any resolution mechanism, instead it’s up to the implementers
- “No practical interoperability” - Mozilla
- “Agree to disagree” - me
- Standard does make recommendations on security, privacy and architecture

Proof Mechanism: Sovrin Blockchain

- All transactions are public
- Only authorized nodes can write to it
- VC verification does not need central authority
- Distributed zero-knowledge revocation check
    - Does not need central authority to track revocations
    - Blockchain nodes could not know what is being checked
- Selective disclosure and verification
    - E.g. only showing the “age” field in driving license

How ITP Implements It Wrong

Evernym



From the creators of Hyperledger Indy and Sovrin

The world's leading platform for verifiable credentials

Build and deploy self-sovereign identity solutions, with the technology and go-to-market resources powering the largest implementations of digital credentials in production.

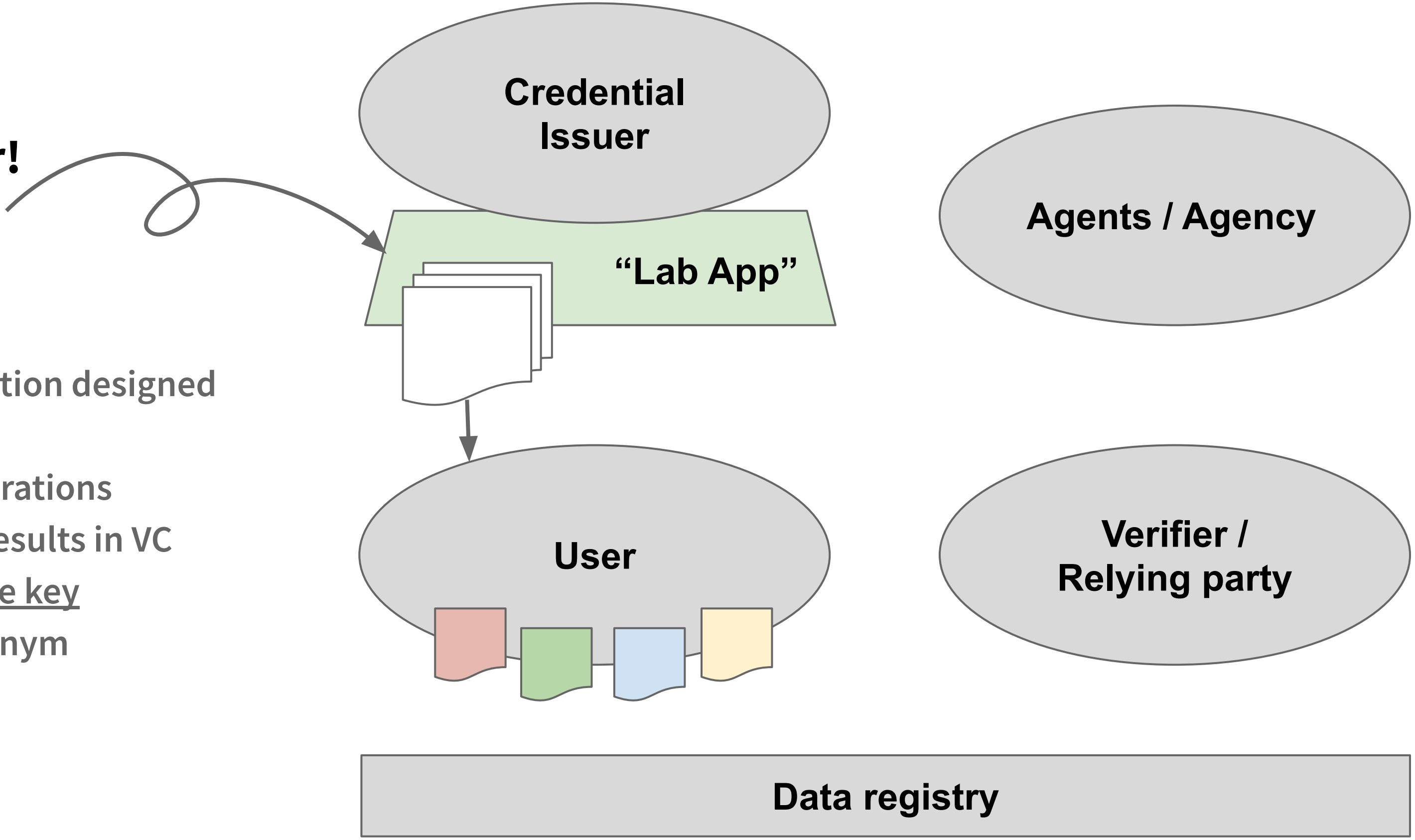
Blockchain is too complex!

- Add a wrapper!

Users lose their private keys!

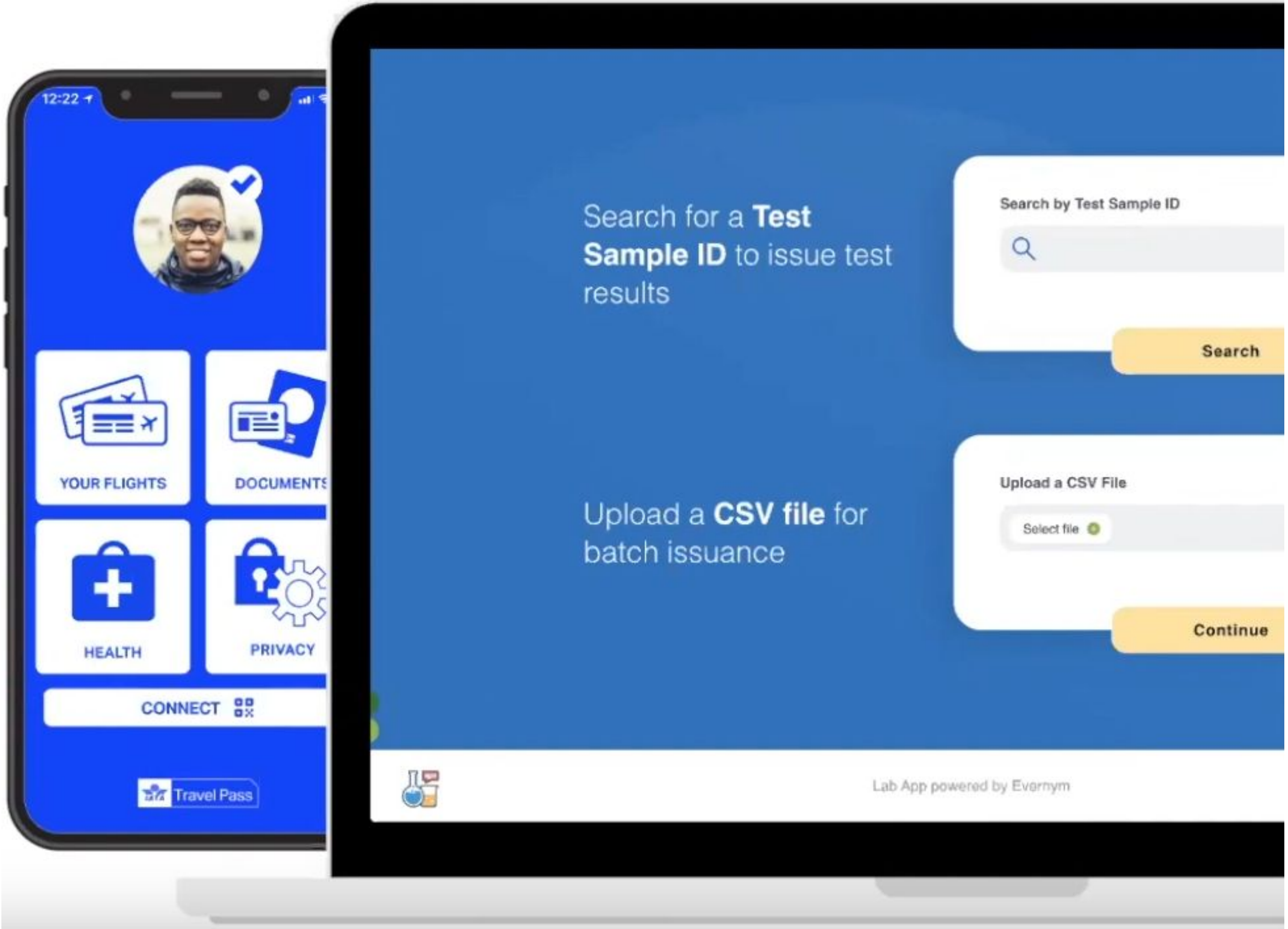
- Let’s manage keys for them!

Add a wrapper!
“Lab App”



- Web-based application designed for lab staff
- Receives Lab registrations
- Issues COVID test results in VC
- Manages lab private key
- An instance of Evernym *Verity Flow*

Evernym Verity Flow as “Lab App”



Search for a **Test Sample ID** to issue test results

Upload a **CSV file** for batch issuance

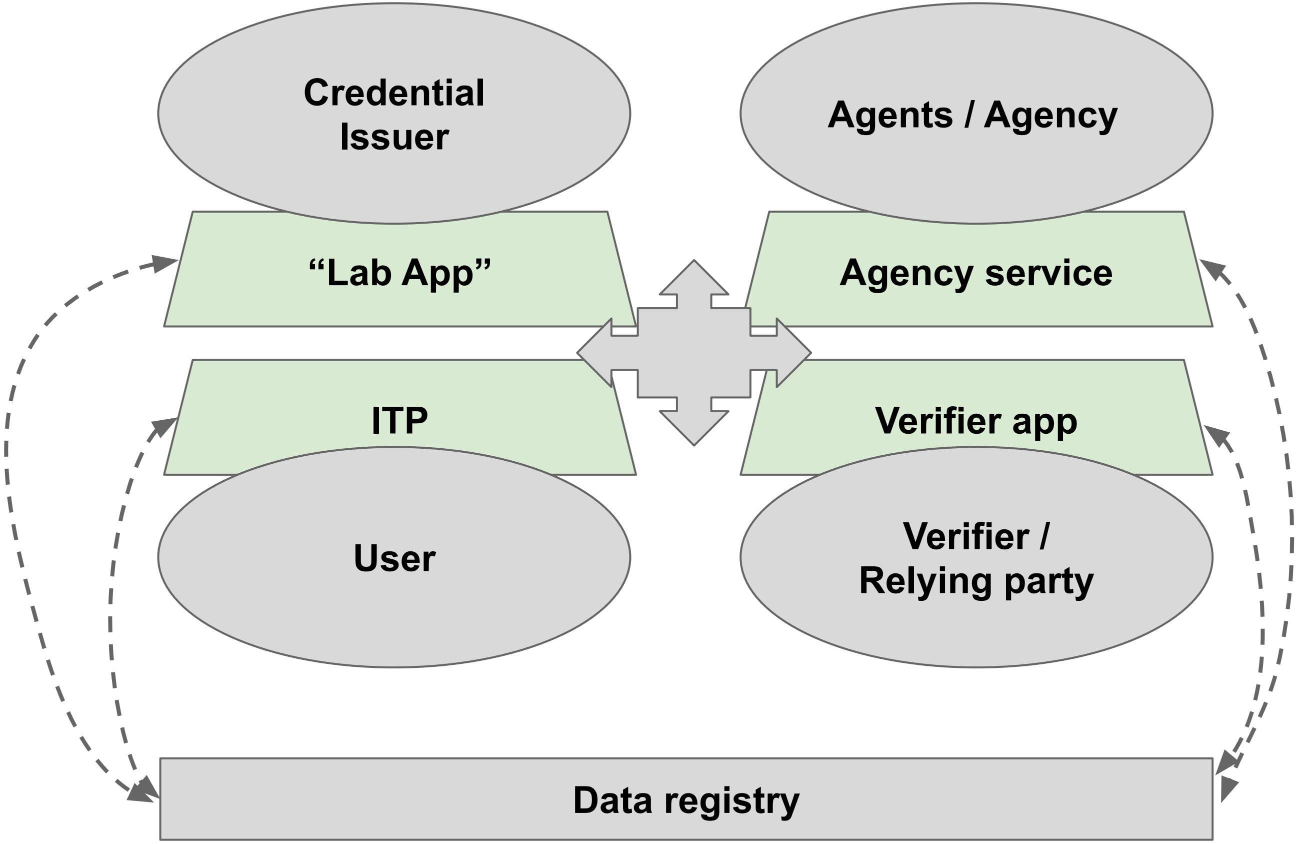
Verifying COVID-19 Test Results

- Evernym provides an “Airline App”
- IATA: “Airline App” is not used by any airlines
- IATA provided no further details other than that
  “Verifiers are using the Verifiable Credentials technology provided by Evernym to authenticate and validate the data received.”

Actual architecture…

All of the apps and services are provided by the same company

An Avast Company

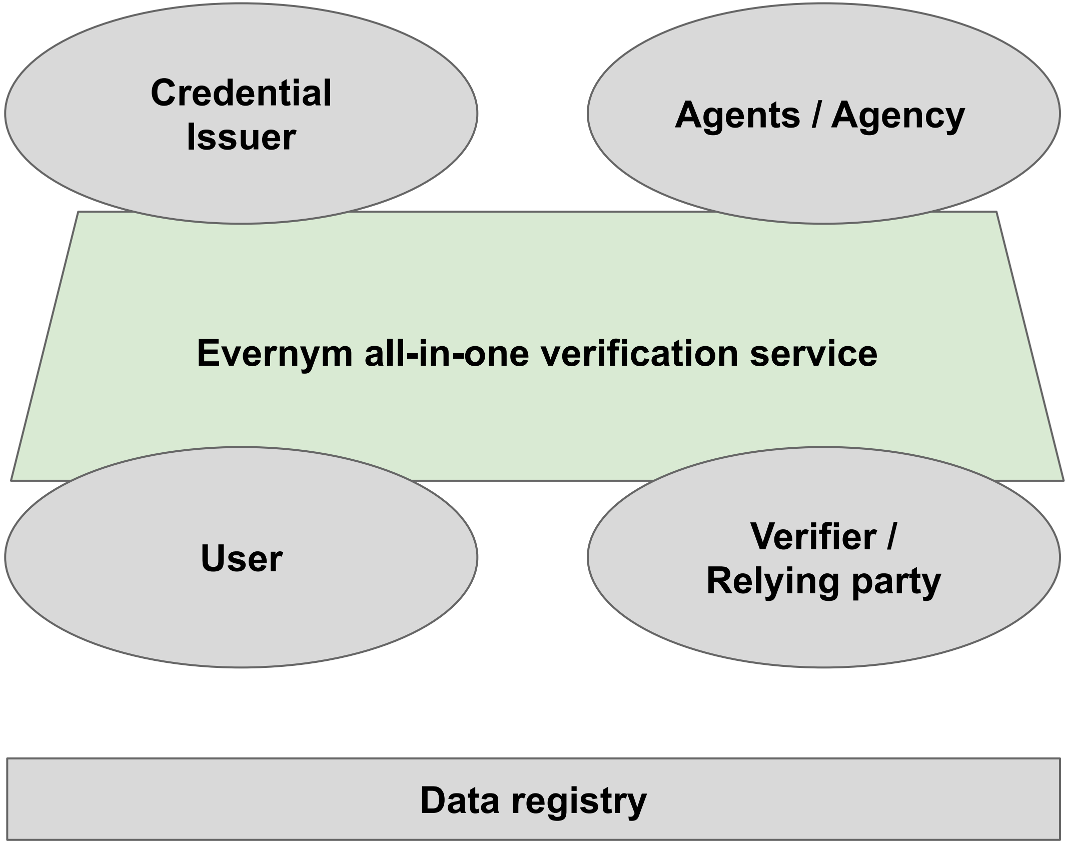


evernym
An Avast Company
還有球證、旁證，再加上主辦單位，協辦所有單位
全都是我的人，你怎麼和我鬥？

TL;DR

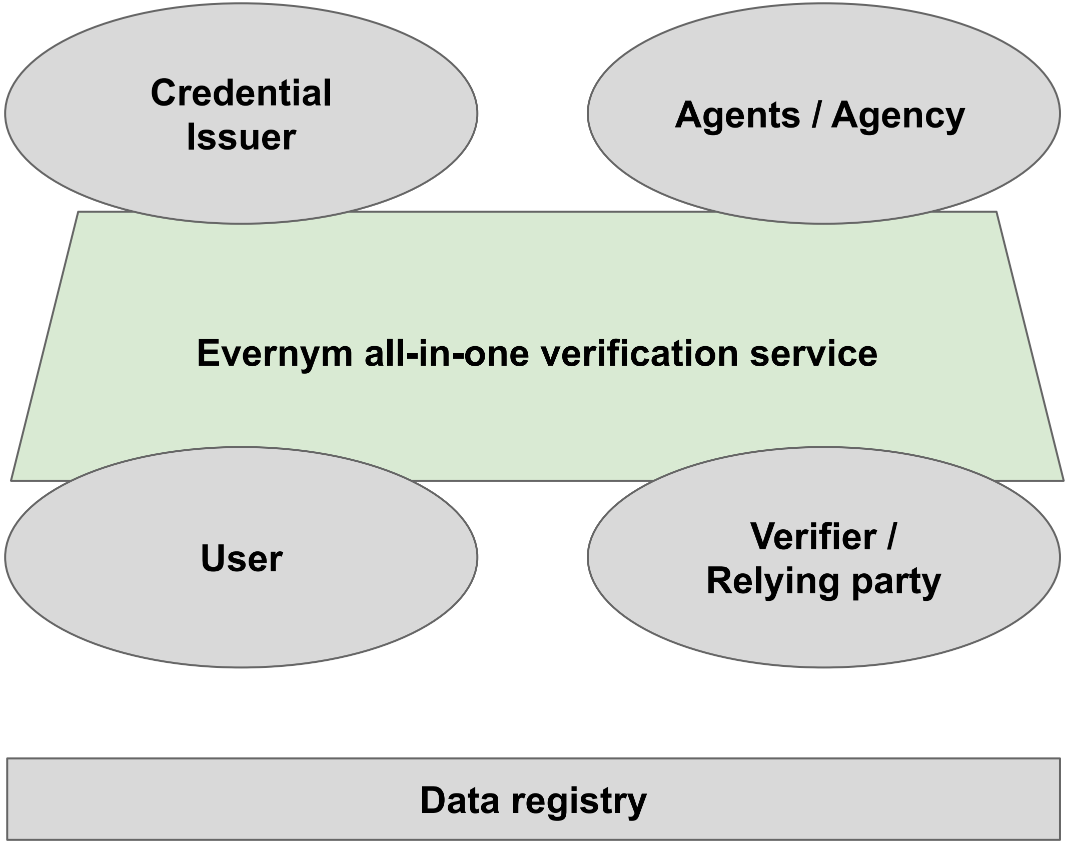
Players, judges, hosts, co-hosts are all my people.
How can you beat me?

This would be no different to…



Blockchain does not enhance trustworthiness of the system at all…

Impossible to know if Evernym actually verifies information using the blockchain



Before

- Health authorities select certified test labs
- Labs issue test results
- Verifiers verify test results by:
  - Visual inspection
  - PKI-based digital signatures

⇨ Results might be forged

⇨ But there is separation of power

After

- Labs delegate Evernym to issue test results
- Verifiers delegate Evernym to verify test results
- Evernym claims to use blockchain to verify
- Evernym holds the labs’ private keys

⇨ Results might be forged

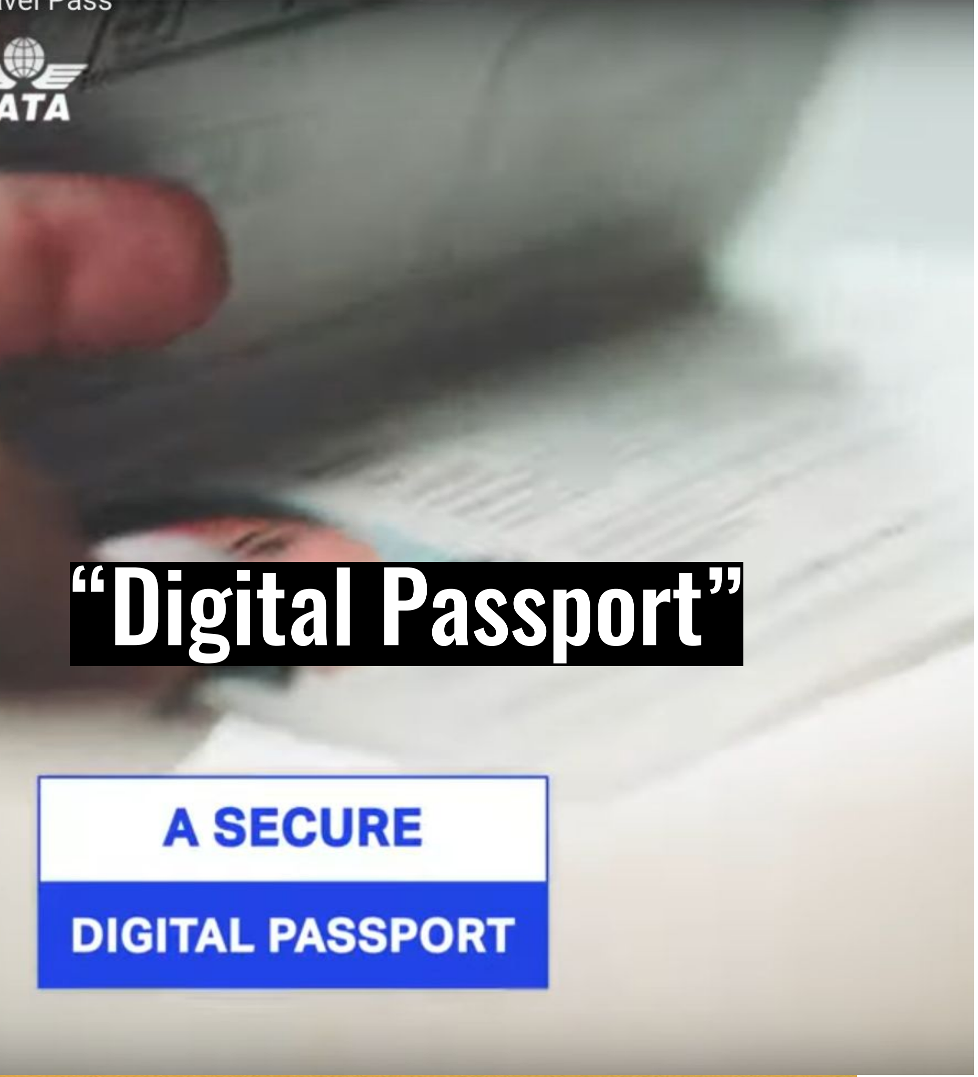
⇨ Evernym controls everything

IATA Travel Pass: Other Issues

Liveness test

- Static face photo
  - Bypassed with AI-generated photo
- Video: requests user to tilt their head
  - Uses Google Firebase ML Kit
  - Bypassed with function hooking (Frida)
- Entirely client side
  - “Business decision” according to IATA

“Digital Passport”



- Optical scanning of MRZ (Machine Readable Zone)
  - Bypassed by choosing to “manually enter”
- NFC chip scanning
  - Passport data is signed but not verified
  - Faked by function hooking (Frida)
- Entirely client side
  - “Business decision” according to IATA

Impact

- Theoretically, Evernym can forge COVID-19 test results
- ITP is even less trustworthy than paper system
- Arbitrary Digital Passports can be created
  - Fortunately Digital Passports are not used for identity verification
  - Merely a convenient way of sharing passport data

Why Should We Care About SSI / ITP ?

Potential Widespread Adoption of SSI

- OrgBook, a company registry of British Columbia, Canada
- Future: EU's European Self-Sovereign Identity Framework (ESSIF)
  - Guidelines and experimental implementations of digital identity systems
  - Part of European Blockchain Services Infrastructure (EBSI)
- Future: Canada's Pan-Canadian Trust Framework
  - Guidelines to implement digital identity systems
- Other small-scale private identity systems
  - Member cards, professional certificates, etc
  - Provided by SSI solution vendors like Evernym

SSI Theoretical Advantages

- Users can keep their own data
- Peer-to-peer data sharing
- Selective disclosure of information
- Decentralized and private revocation checks

SSI Disadvantages

- SSI systems are new, often there is only one vendor
    - Which creates trust issues
- Users always lose their private keys
- Highly complex, which prompts the need for vendors

Conclusion

Lessons Learned

- Don’t trust a system just because it says it uses blockchain
- Don’t let the players be the judge -
  Separate the credential (certificate) issuer and verifier entities

My Opinions

- SSI is highly complex, in early adoption phase
- There is not enough scrutiny on SSI and its implementations
- A complex system has a high bar to implementation and integration
    - Which prompts the need to seek and delegate power to vendors
    - Which heightens the bar for competing vendors, which may lead to monopolies
- **Therefore, citizens should not trust SSI for public use (yet)**
- SSI technology remains a promising alternative to current centralized online identity systems
- However, we must make sure that the SSI market is competitive
- Or else we might end up with worse solutions

FAQ

- Am I required to use ITP?
  - No, it is opt-in and only available on select flights
- Can I pass border control with forged ITP Digital Passport?
  - Likely no, ITP is only used by airlines, not border control
- Does SSI require the use of distributed ledgers (DLT)?
  - No, DID spec and Verifiable Credential spec does not rely on DLT
  - You can even use PKI
- Did you find vulnerabilities in SSI or Sovrin?
  - No, but I found trust issues
  - The problems are not inherent to the Sovrin specification
  - I.e. this is an implementation issue

Thank you!

- **Full report on this topic:** https://citizenlab.ca/2022/04/privacy-and-security-analysis-of-the-iata-travel-pass-android-app/
- **Other cool research from Citizen Lab:** https://citizenlab.ca/

- **Find me at the CSCS booth!**
- **pellaeon@citizenlab.ca**