Case Study:

Reopening global travel with verifiable credentials and IATA Travel Pass

Drummond Reed
Chief Trust Officer, Evernym
drummond.reed@evernym.com

evernym

A little about me

- Chief Trust Officer, Evernym
- Co-Author, W3C Decentralized Identifiers (DID) Spec
- Co-Author, *Self-Sovereign Identity*
- Co-Founder, Trust over IP Foundation
- Chair, ToIP Governance Stack WG
- Member, Sovrin Guardianship Task Force
- 25+ years in Internet identity
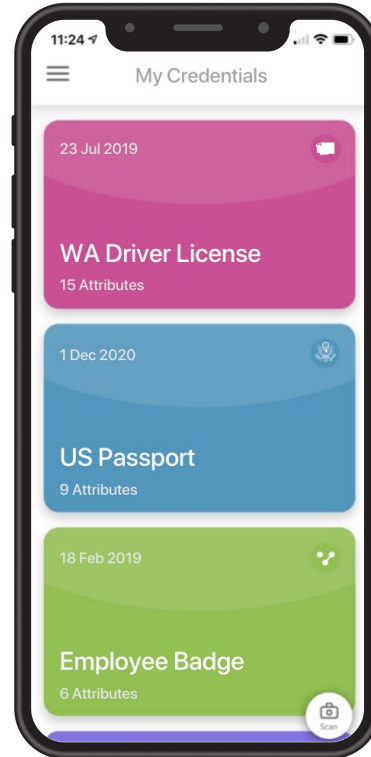- 20+ years in identity standards

You can reach me at **@drummondreed** or **drummond.reed@evernym.com**.

A quick primer
What are **verifiable credentials** and **digital wallets**?

The digital equivalents of the paper documents we use everyday

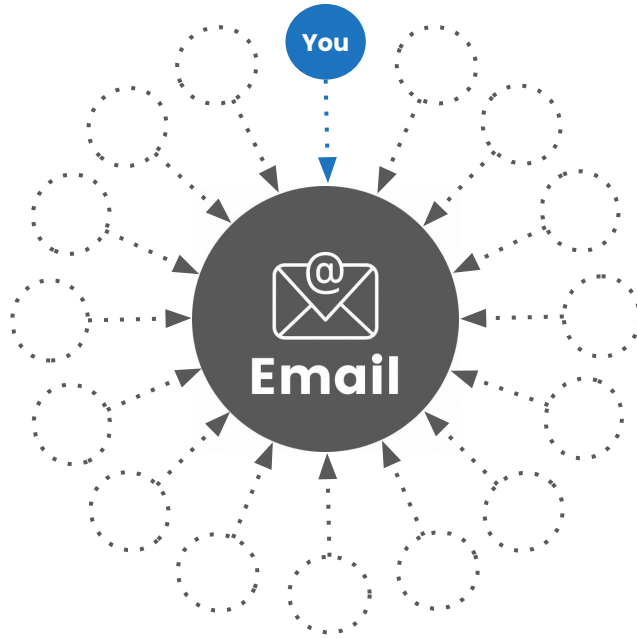# With a few extra benefits
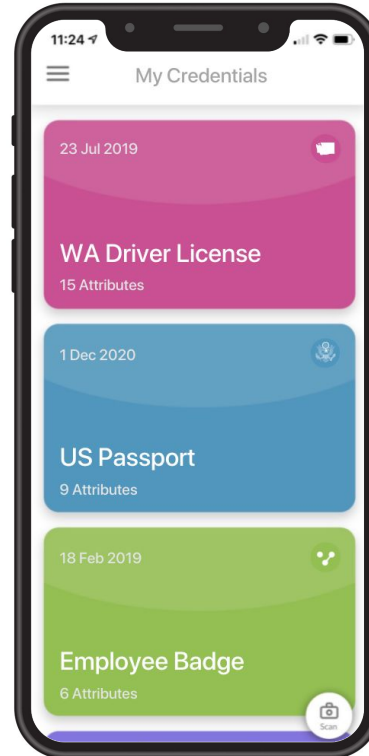
✓ Portable & shareable

✓ Immediately verifiable

✓ Tamper-proof

✓ Secure

✓ Private

✓ Trusted

Verifiable credentials put **you** in the center of your digital world

centralized/federated

decentralized

They are the **next evolution** of digital identity

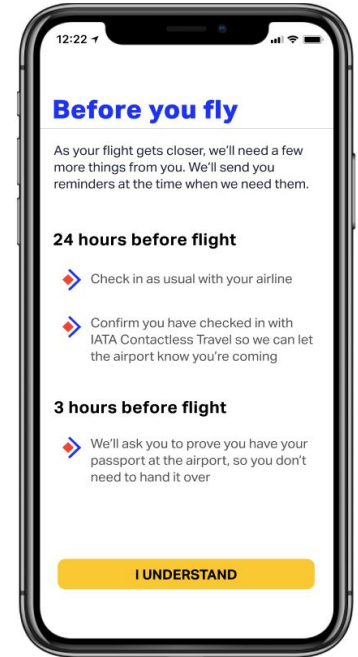| Centralized	Federated	Decentralized
• X.500 • SSL • TLS • HTTPS	• SAML • OpenID • OAuth • UMA	• Blockchains • DIDs • Verifiable Credentials

Verifiable Credentials In Action:
IATA Travel Pass
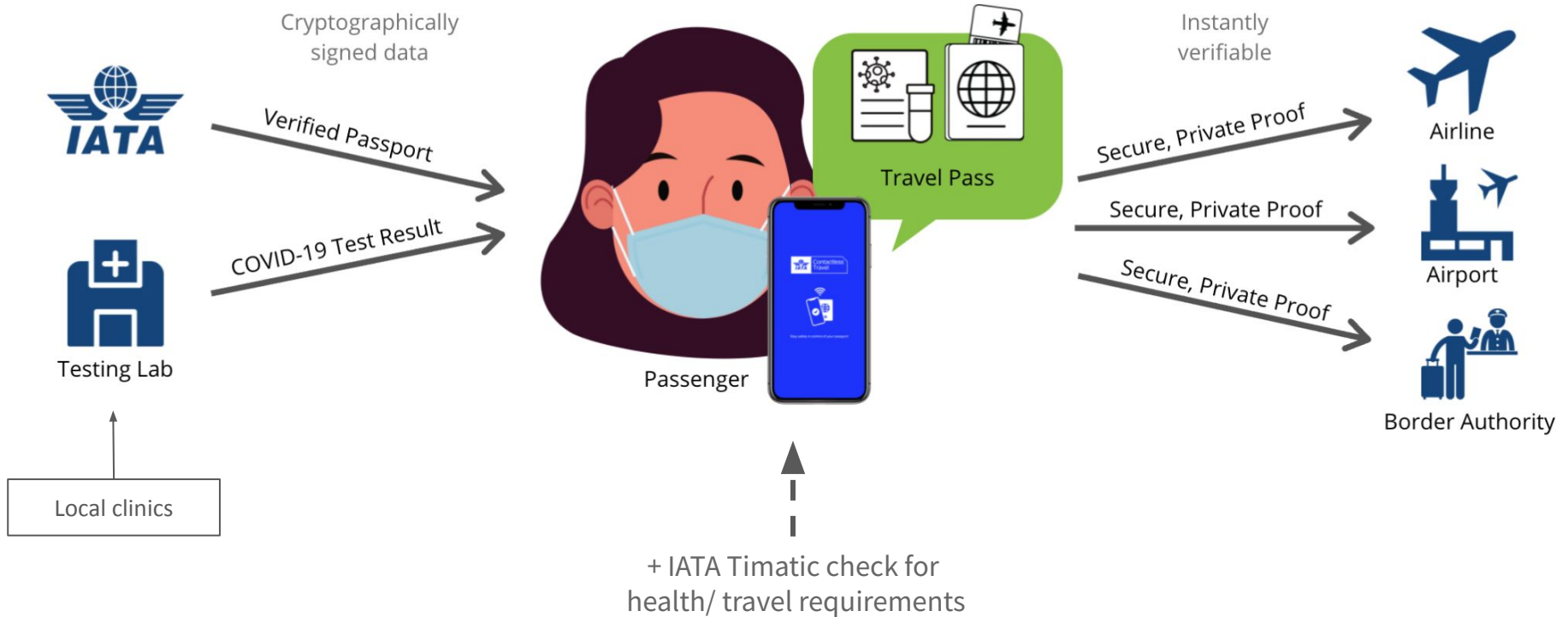
IATA Travel Pass

New standard for secure, contactless passenger journeys

- At-home digital passport verification

- Proof of vaccine or test certificate

- Pre-departure Covid-19 testing

- Provide negative Covid-19 test during online check-in

- Share travel documents with airline, airport & border authorities

In trial with 60+ major airlines and thousands of COVID-19 testing labs.

How it works

IATA — Verified Passport → Passenger

Cryptographically signed data

Testing Lab — COVID-19 Test Result → Passenger

Local clinics → Testing Lab

Travel Pass

Passenger

+ IATA Timatic check for health/ travel requirements

Instantly verifiable

Secure, Private Proof → Airline

Secure, Private Proof → Airport

Secure, Private Proof → Border Authority

Features

Travel Pass
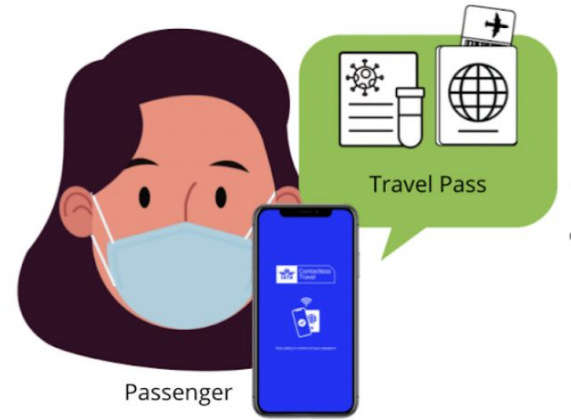
Passenger

Features

- **No central database**
  no data troves to hack

Data only lives on the device

Features

- **No central database**
  no data troves to hack

- **Data moves peer to peer**
  no one can listen in or intercept

*Data moves directly from the
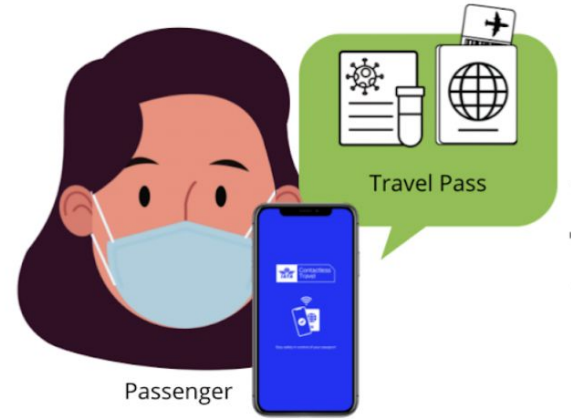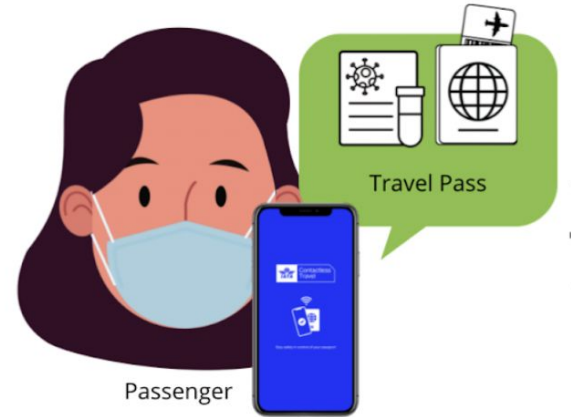passenger to the organisation,
not via a 3rd party*

Features

- **No central database**
  no data troves to hack

- **Data moves peer to peer**
  no one can listen in or intercept

- **Data formatted as 'verifiable credentials'**
  Information exchange is flexible and private

Travel Pass

Passenger

Specific format
- *Can share one attribute at a time*
- *Doesn't leave behind digital breadcrumbs*
- *Can share different credentials with one tap*

Features

- **No central database**
  no data troves to hack

- **Data moves peer to peer**
  no one can listen in or intercept

- **Data formatted as 'verifiable credentials'**
  information exchange is flexible and private

- **Individual is in complete control**
  choose what and with whom you share your data

Travel Pass

Passenger

A digital wallet becomes **useful for *anything***

With a digital wallet, travelers can receive **ANY** data
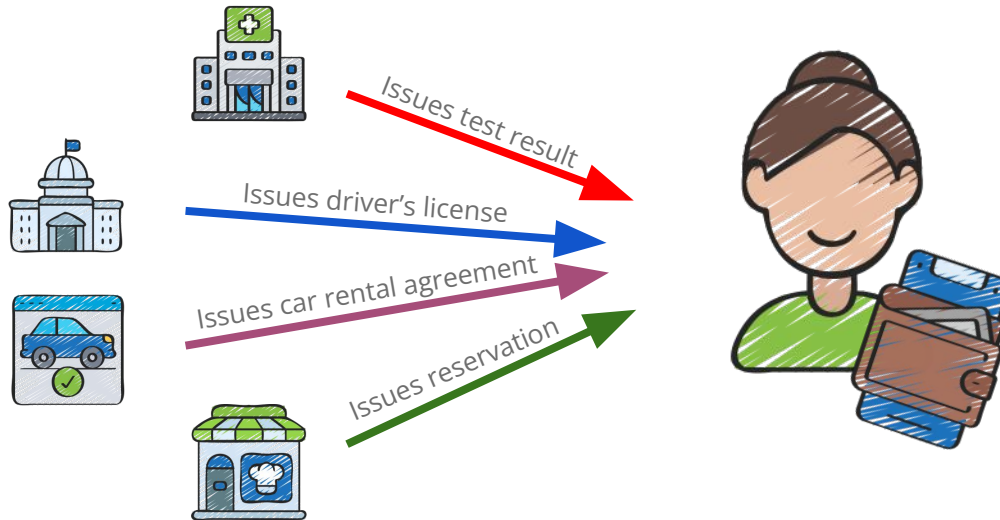
Issues test result

Issues driver's license

Issues car rental agreement

Issues reservation

ISSUERS
E.g., COVID Test Lab, Government,
Car Rental, Restaurant

HOLDER
An Individual / Identity Owner

…and then share it with **ANY** organization

Seamless data sharing by combining attributes from multiple credentials

ISSUERS
E.g., COVID Test Lab, Government,
Car Rental, Restaurant

HOLDER
An Individual / Identity Owner

VERIFIERS
E.g., Airport Lounge, Restaurant,
Car Rental
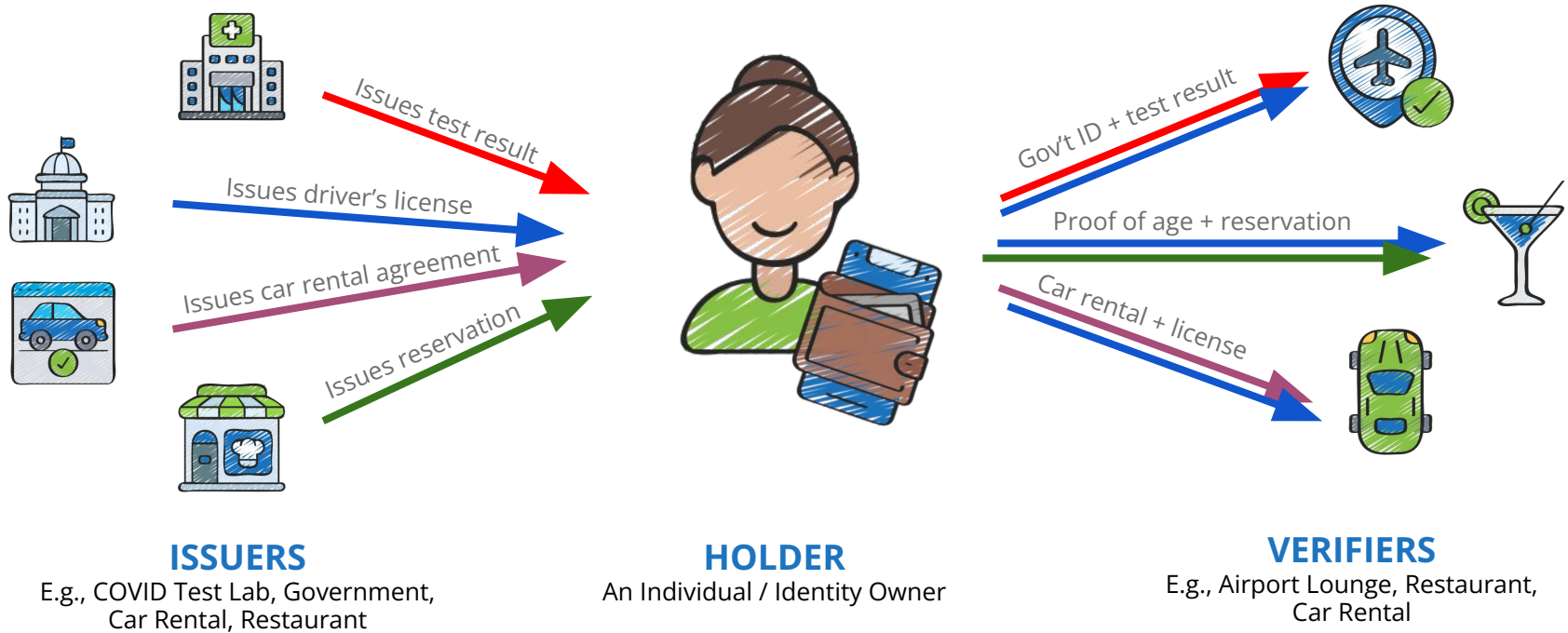
...without having to 'phone home'

Issues test result

Issues driver's license

Issues car rental agreement

Issues reservation

Gov't ID + test result

Proof of age + reservation

Car rental + license

No integration
between issuer and verifier

No intermediaries
accessing your data

19
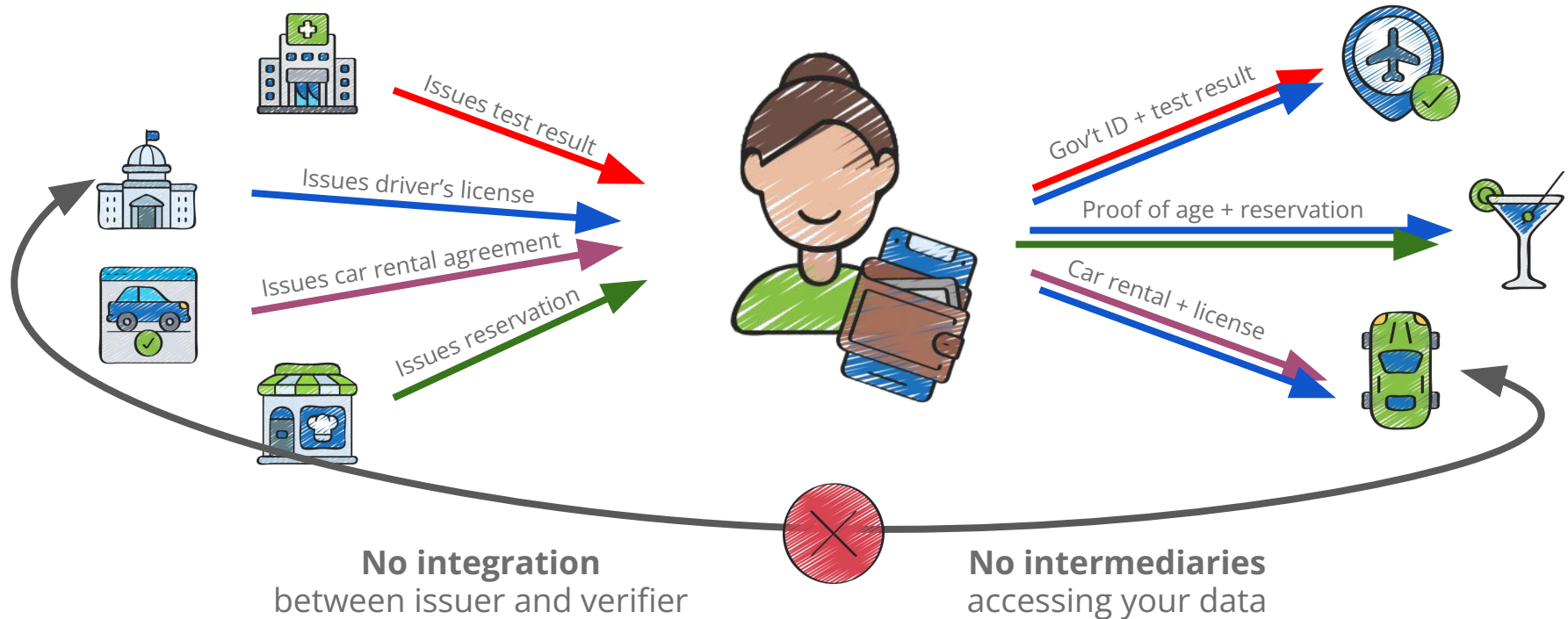
But there's more!

- Travelers can LOG IN to websites with their wallet

- Organizations can send secure, messages to travelers - direct to wallet

Multi Factor Auth & Passwordless Log-In

Secure Peer-to-Peer Messaging

HOTEL
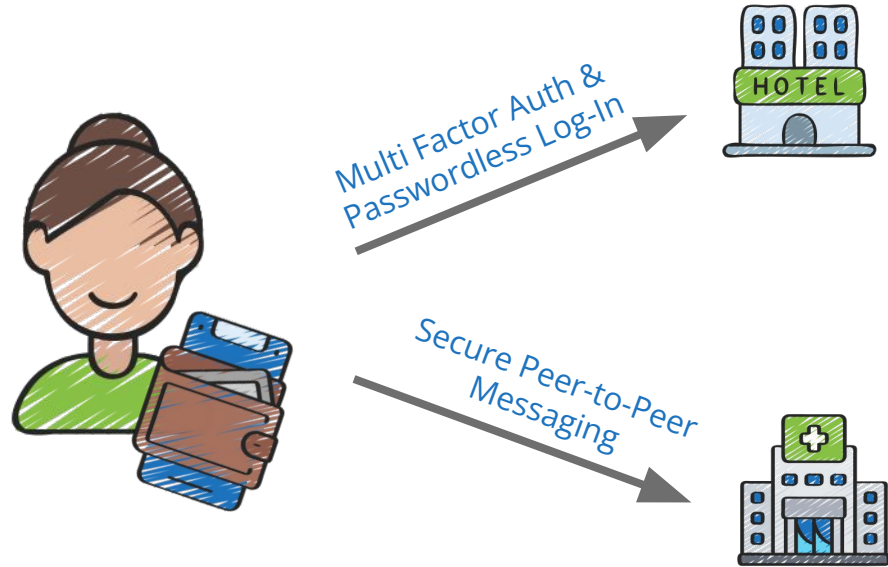
Open ecosystem based on **open standards**

Vendor A → Open standards → App Provider B

App Provider B → Open standards → Digital Platform C

App Provider B → Open standards → Vendor D

App Provider B → Open standards → Open Source Tool E

Vendor A

App Provider B

Digital Platform C

Vendor D

Open Source Tool E

W3C

GOOD HEALTH PASS

TRUST Over IP FOUNDATION
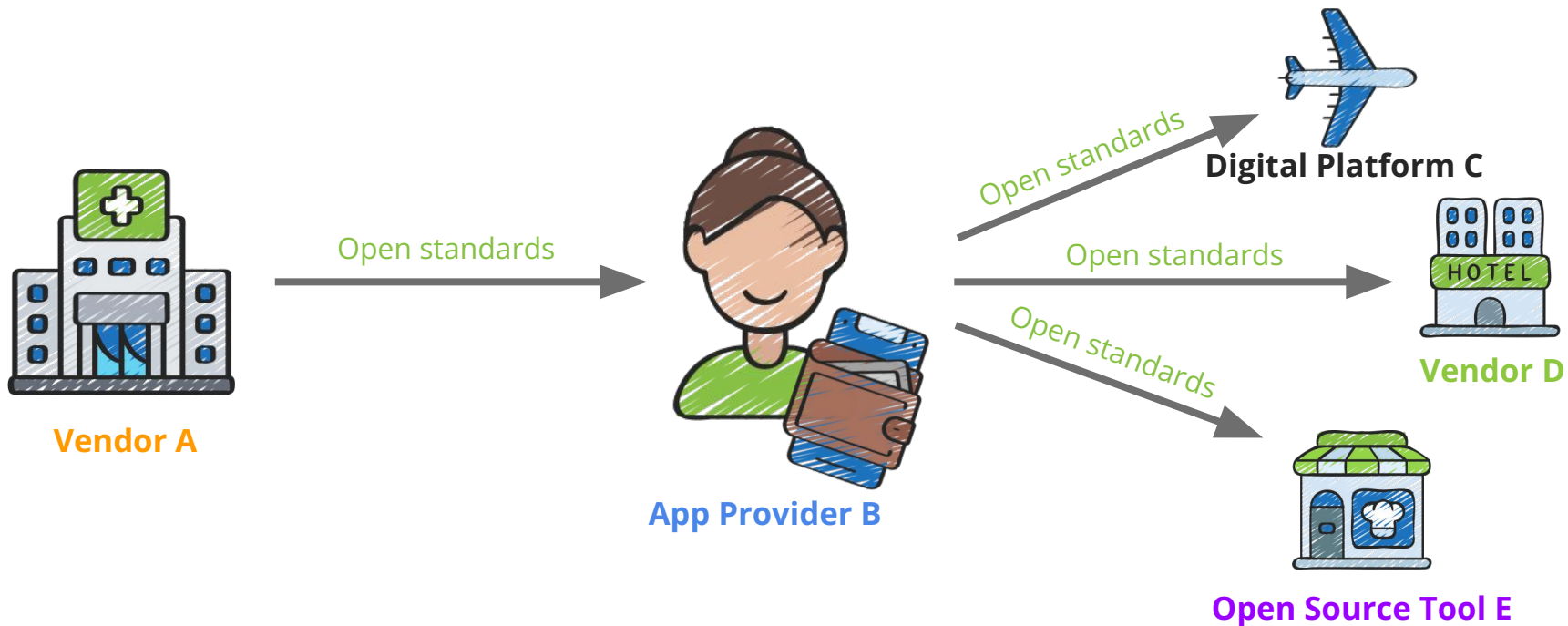
How do **verifiable credentials** work?

The verifiable credential trust triangle

Sign

Verify

Holder

Wallet

Verifiable Credential

Proof

Trust

Issuer

Verifier

✗ No integration needed!

Write

Read

DID

Public Key
+ other cryptographic metadata

Verifiable Data Registry (e.g., Blockchain)

23
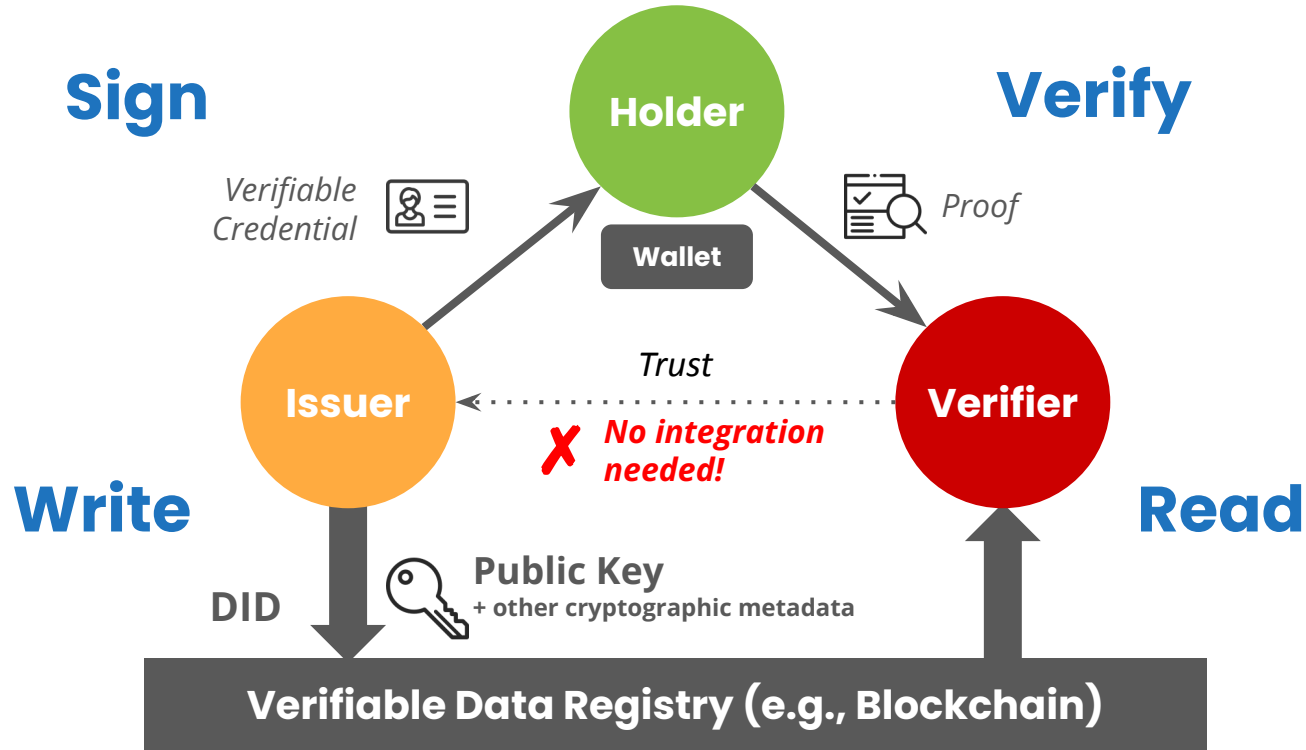
IATA Travel Pass example

Sign

Verify

Traveler (Holder)

IATA Travel Pass

Proof

Wallet

Health Authority (Issuer)

Trust

Airline (Verifier)

✗ *No integration needed!*

Write

Read

DID

Public Key
+ other cryptographic metadata
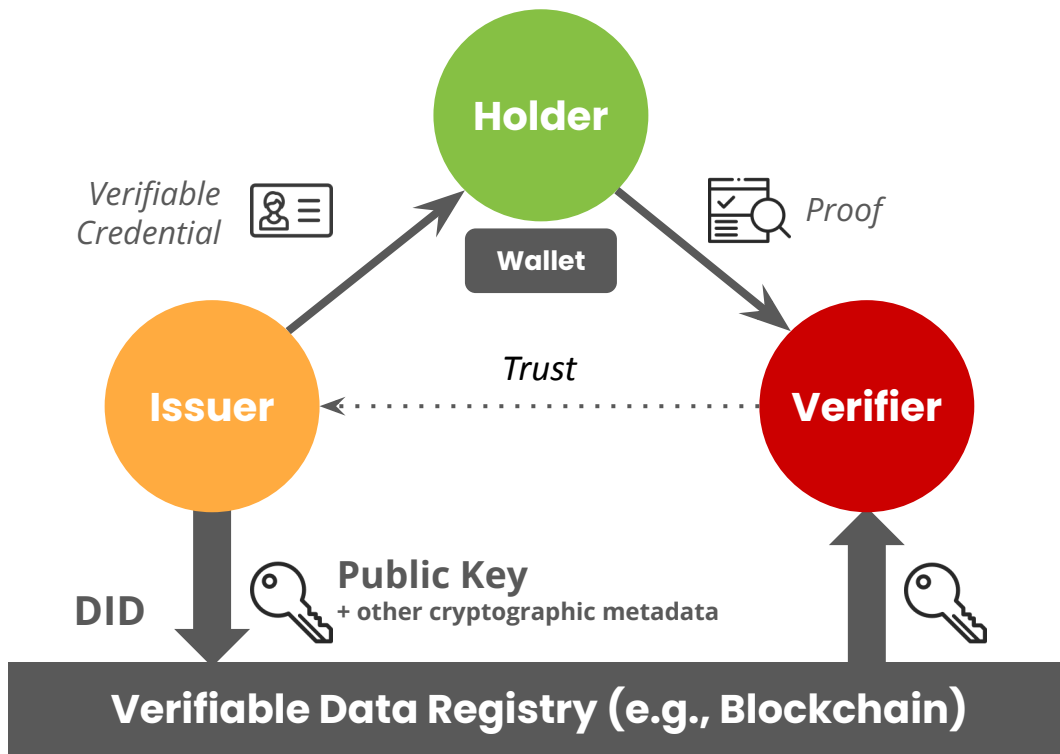
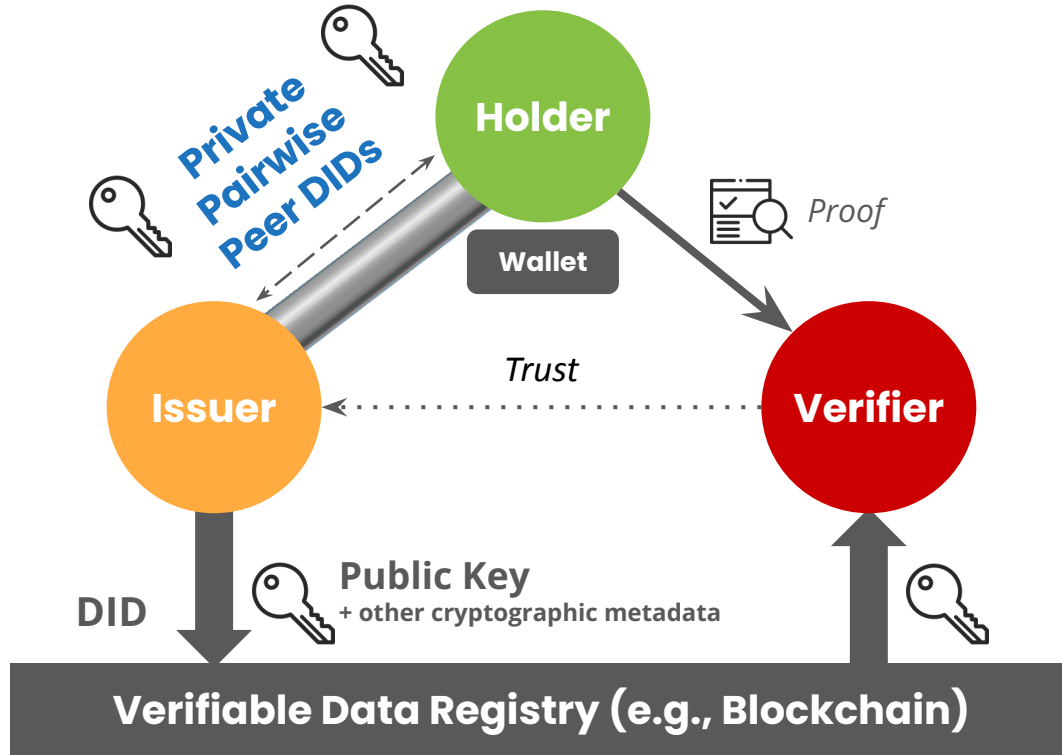**Verifiable Data Registry (e.g., Blockchain)**

24
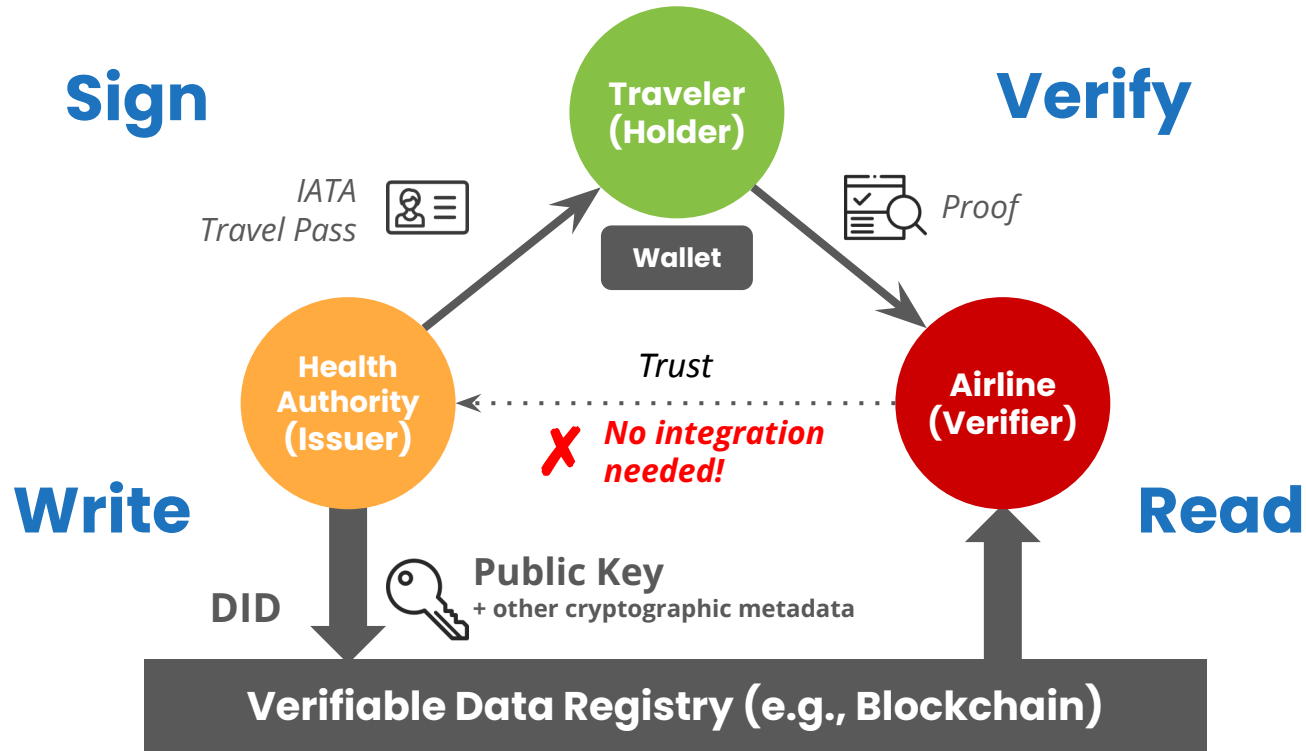
The Special Role Of
Privacy By Design

With DIDs and Verifiable Credentials, we have the opportunity to implement **Privacy by Design** at Internet scale

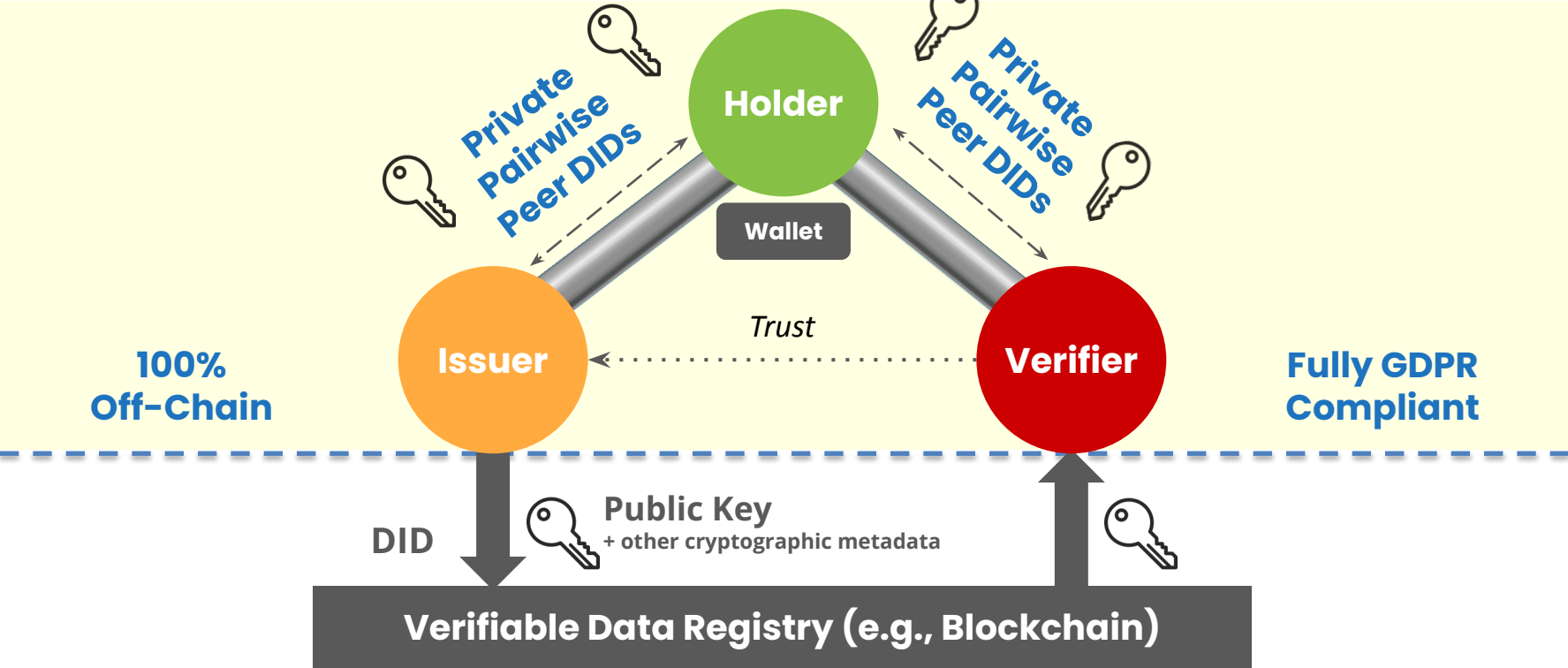# Every connection is **secure** and **private**

Every connection is **secure** and **private**

Every connection is **secure** and **private**
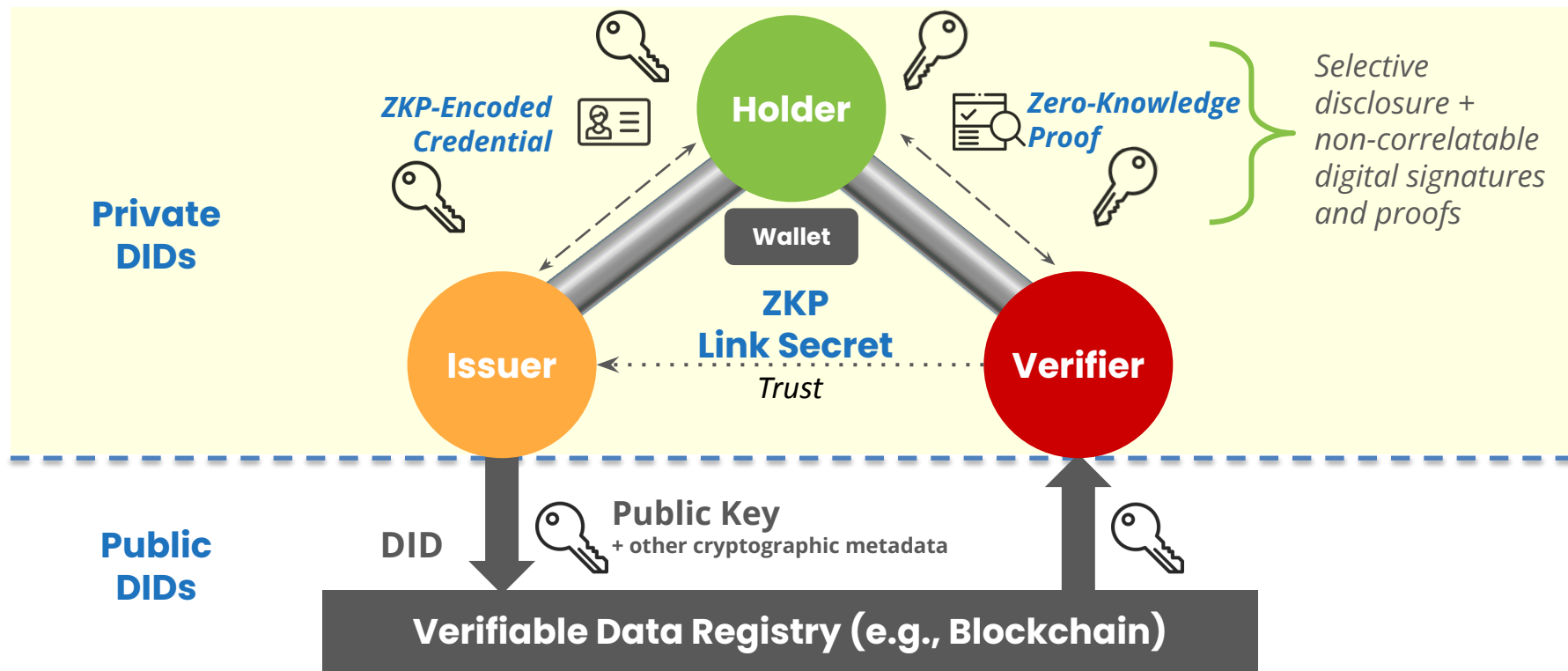

Holder

Wallet

Private Pairwise Peer DIDs

Private Pairwise Peer DIDs

100% Off-Chain

Issuer

Trust

Verifier

Fully GDPR Compliant

DID

Public Key
+ other cryptographic metadata

Verifiable Data Registry (e.g., Blockchain)

Why blockchains play a very limited role

Private Pairwise Peer DIDs

Private Pairwise Peer DIDs

Holder

Wallet

Trust

Issuer

Verifier

100% Off-Chain

Fully GDPR Compliant

DID

Public Key + other cryptographic metadata

Verifiable Data Registry (e.g., Blockchain)
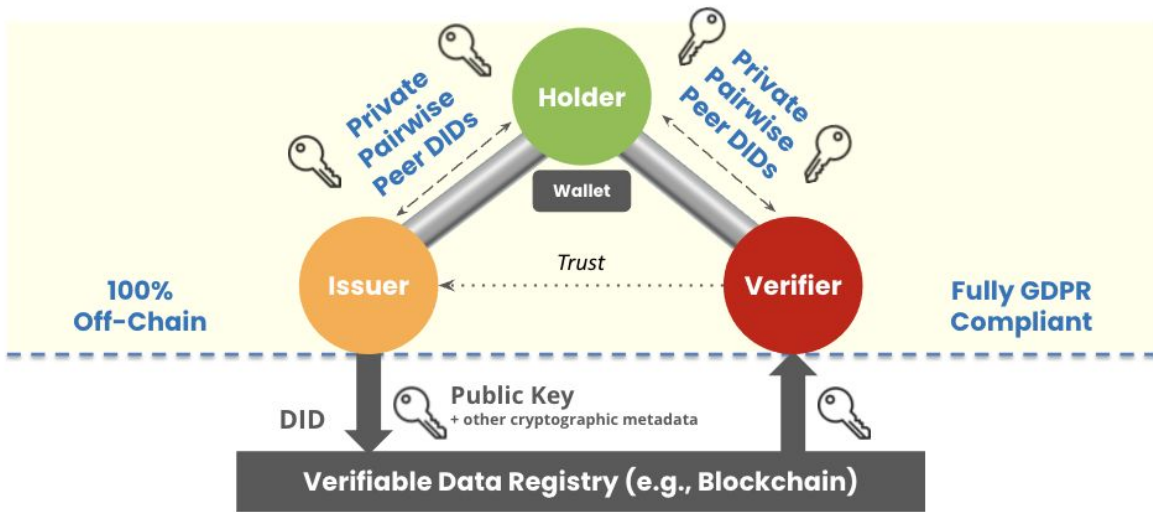
But public blockchains are **not needed**—and for privacy reasons are **not wanted**—for this higher layer of direct peer-to-peer connections

Public blockchains serve as excellent verifiable data registries for **public DIDs** at this layer
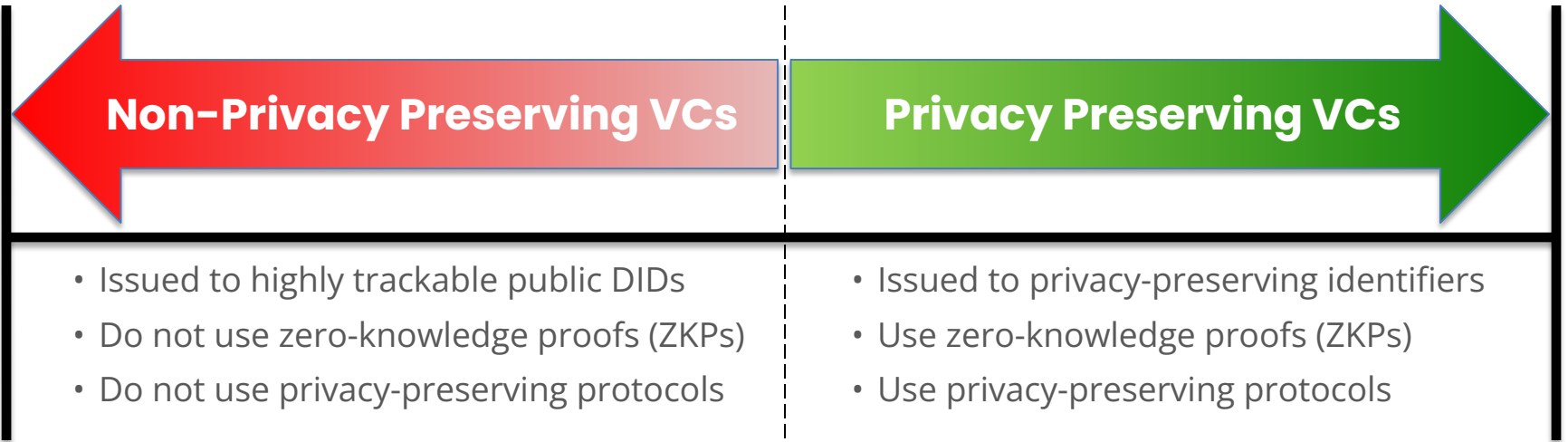
30

ZKP-Based VCs

Holder Authentication & Biometrics

Based on the issuer policies, verifiers can choose from one or more of the following:

- Peer DID channel authentication

- ZKP link secret proof (cryptographic binding)

- Wallet biometric proof

- Wallet liveness detection proof

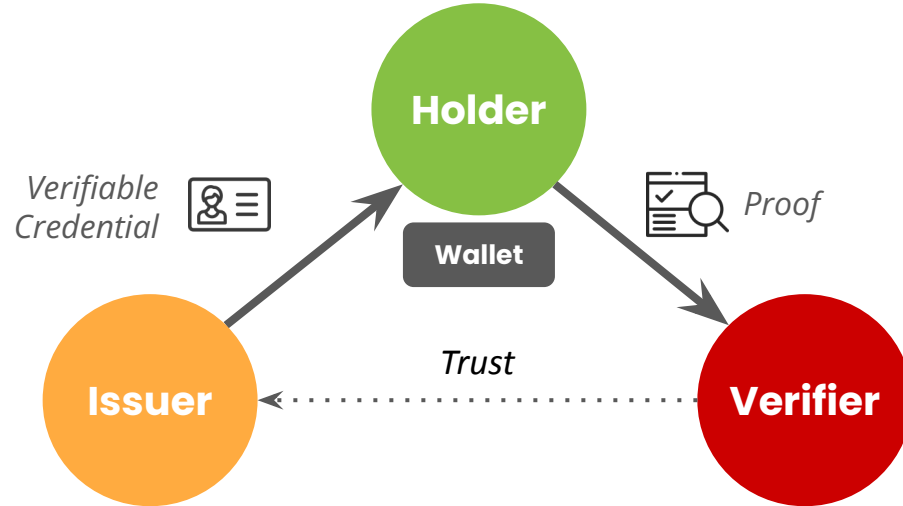- OOB (Out of Band) identity verification

The VC "**Spectrum of Privacy**"

Non-Privacy Preserving VCs	Privacy Preserving VCs
• Issued to highly trackable public DIDs	• Issued to privacy-preserving identifiers
• Do not use zero-knowledge proofs (ZKPs)	• Use zero-knowledge proofs (ZKPs)
• Do not use privacy-preserving protocols	• Use privacy-preserving protocols

33

The Special Role Of
Governance Frameworks

How can verifiers know all the issuers?

The governance trust diamond
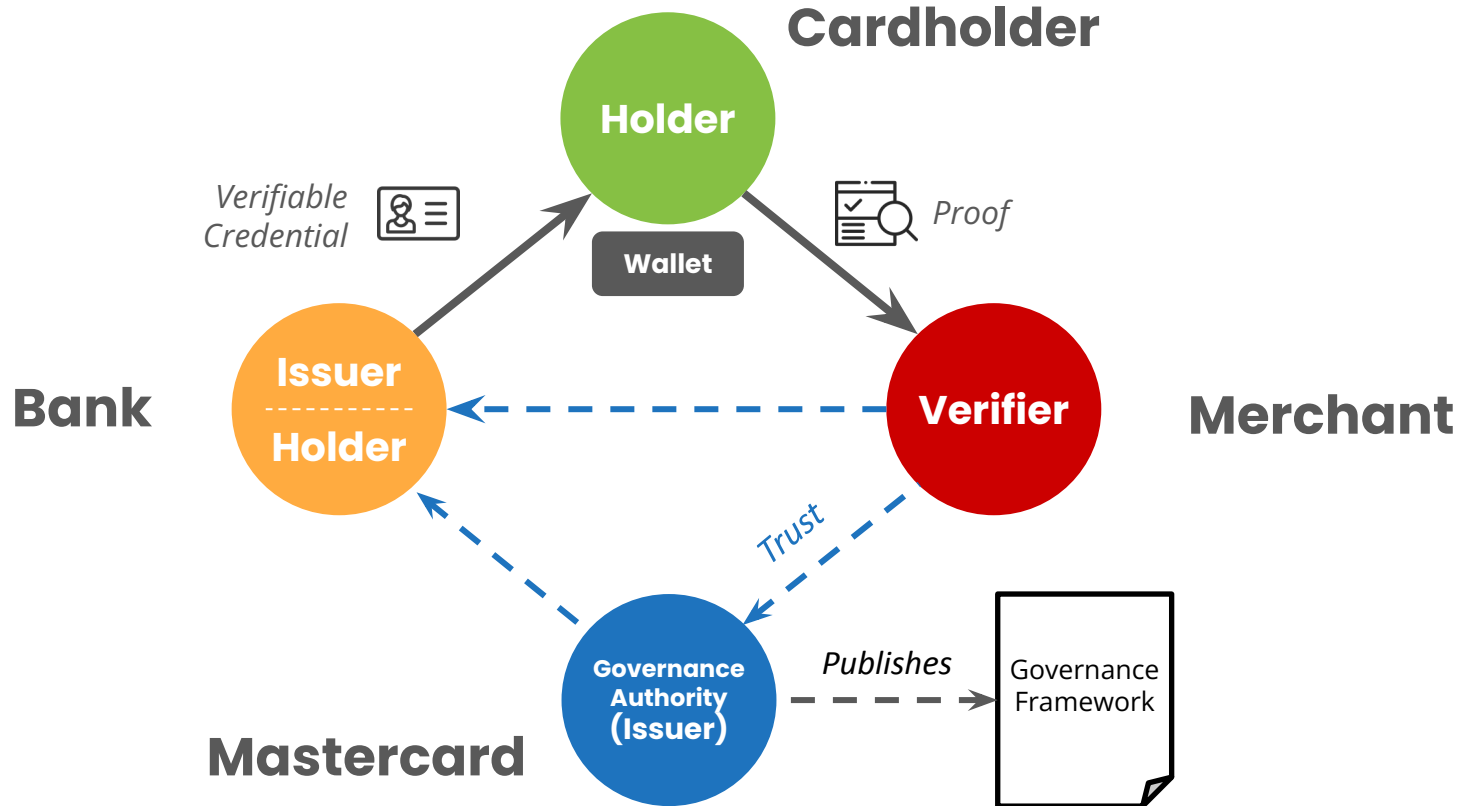
The governance trust diamond

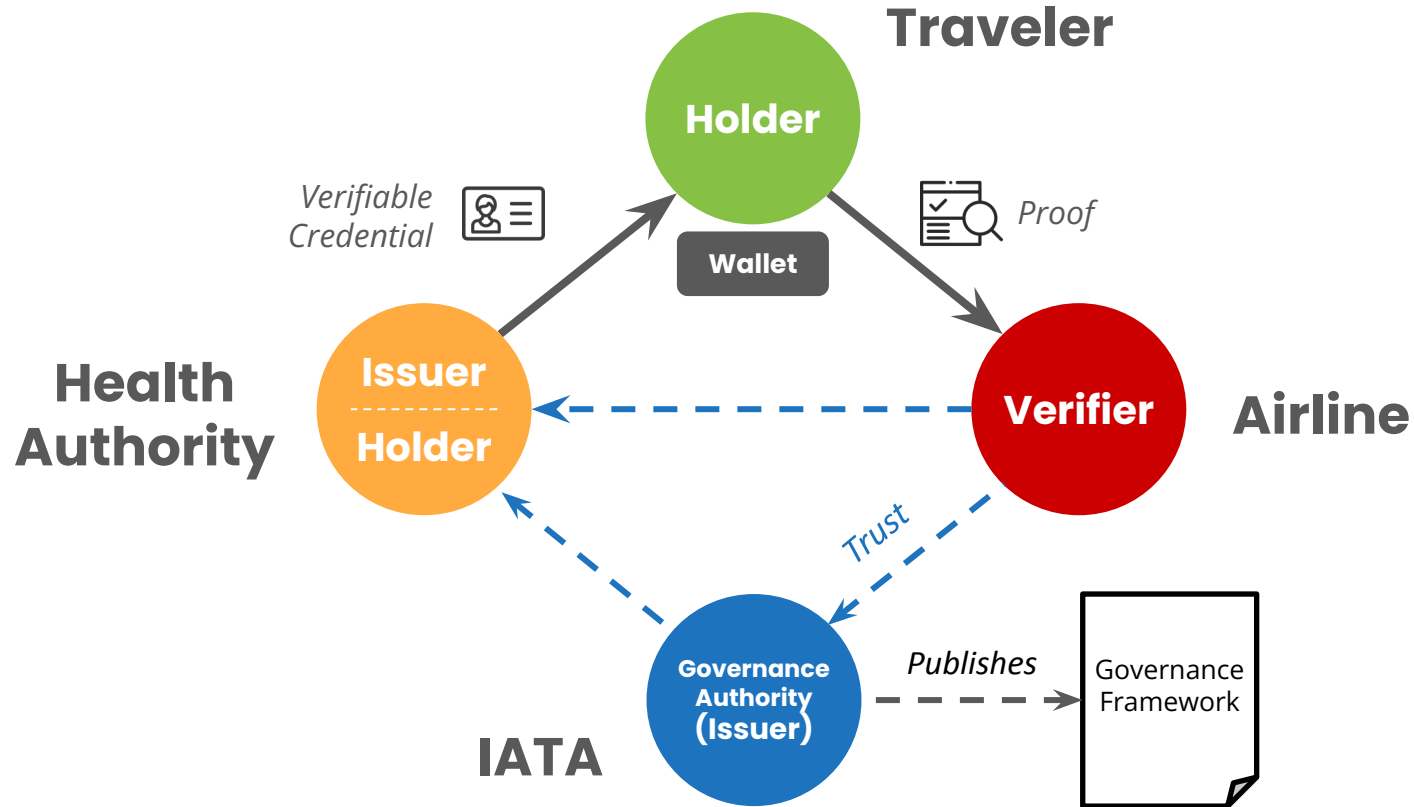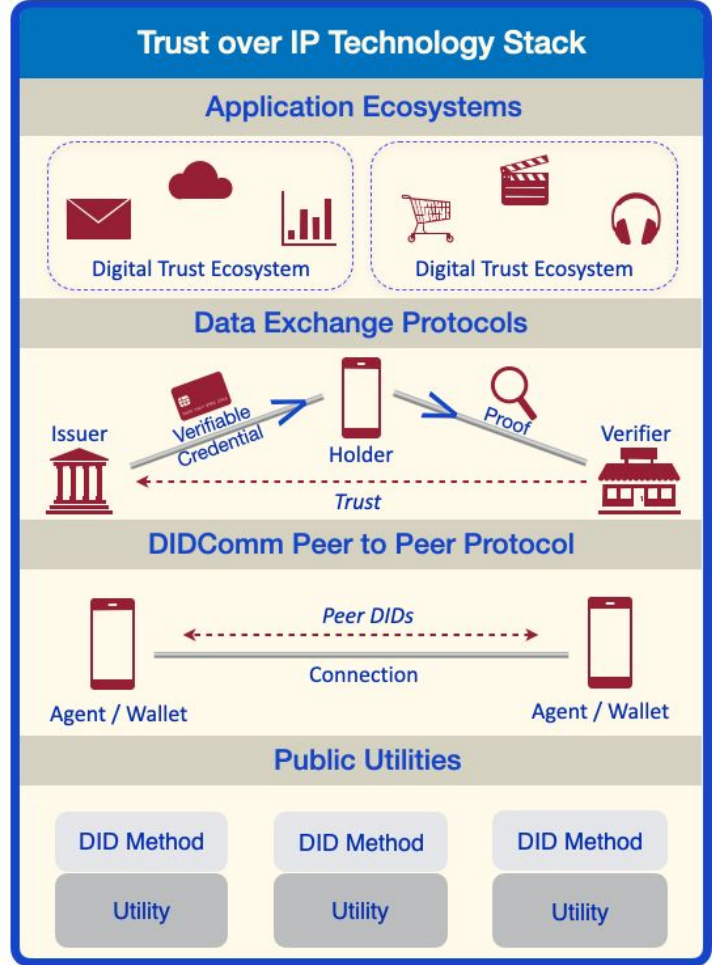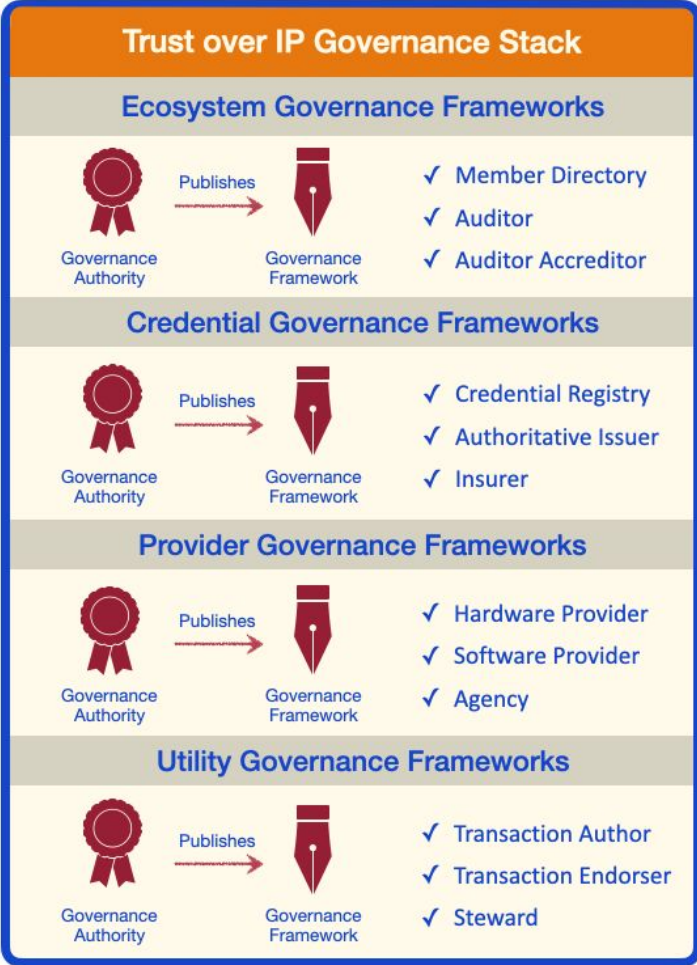How can we standardize
DIDs and VCs for
universal interoperability?

Trust over IP Governance Stack

Trust over IP Technology Stack

Layer 4

Ecosystem Governance Frameworks

Governance Authority → Publishes → Governance Framework

✓ Member Directory
✓ Auditor
✓ Auditor Accreditor

Application Ecosystems

Digital Trust Ecosystem

Digital Trust Ecosystem

Layer 3

Credential Governance Frameworks

Governance Authority → Publishes → Governance Framework

✓ Credential Registry
✓ Authoritative Issuer
✓ Insurer

Data Exchange Protocols

Issuer — Verifiable Credential → Holder — Proof → Verifier

Trust

Layer 2

Provider Governance Frameworks

Governance Authority → Publishes → Governance Framework

✓ Hardware Provider
✓ Software Provider
✓ Agency

DIDComm Peer to Peer Protocol

Agent / Wallet — Peer DIDs / Connection — Agent / Wallet

Layer 1

Utility Governance Frameworks

Governance Authority → Publishes → Governance Framework

✓ Transaction Author
✓ Transaction Endorser
✓ Steward

Public Utilities
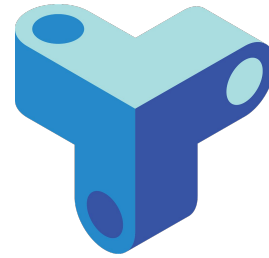
DID Method / Utility

DID Method / Utility

DID Method / Utility

Defining a complete architecture for Internet-scale digital trust that combines cryptographic verifiability at the machine layers with human accountability at the business, legal, and social layers

trustoverip.org

Questions?

drummond.reed@evernym.com
@drummondreed