Case Study:

Reopening global travel with verifiable credentials and IATA Travel Pass

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

<table>
<thead>
<tr>
<th>Centralized</th>
<th>Federated</th>
<th>Decentralized</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.500</td>
<td>SAML</td>
<td>Blockchains</td>
</tr>
<tr>
<td>SSL</td>
<td>OpenID</td>
<td>DIDs</td>
</tr>
<tr>
<td>TLS</td>
<td>OAuth</td>
<td>Verifiable Credentials</td>
</tr>
<tr>
<td>HTTPS</td>
<td>UMA</td>
<td></td>
</tr>
</tbody>
</table>

[Logos of various organizations like IETF, ICANN, Webtrust, Oasis, OpenID, OIX (Open Identity Exchange), W3C, DIF, TRUST Over IP Foundation]
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 Timatic check for health/travel requirements
- Cryptographically signed data
- Verified Passport
- COVID-19 Test Result
- Instantly verifiable
- Secure, Private Proof
- Airline
- Airport
- Border Authority
- Testing Lab
- Passenger

Local clinics
Features

- No central database
  no data troves to hack
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

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
A digital wallet becomes useful for anything
With a digital wallet, travelers can receive **ANY** data

**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’

No integration between issuer and verifier

No intermediaries accessing your data
But there’s more!

- Travelers can LOG IN to websites with their wallet
- Organizations can send secure, messages to travelers - direct to wallet
Open ecosystem based on open standards
How do verifiable credentials work?
The verifiable credential trust triangle

- **Holder**
  - Sign
  - Verify
  - Trust
  - Proof

- **Issuer**
  - Write
  - DID
  - Public Key
  - Verifiable Credential

- **Verifier**
  - Read
  - Proof

**Verifiable Data Registry (e.g., Blockchain)**

- No integration needed!
IATA Travel Pass example

- **Sign**
- **Verify**
- **Write**
- **Read**

- **Traveler (Holder)**
- **Health Authority (Issuer)**
- **Airline (Verifier)**

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

- **Trust**
  - No integration needed!
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**

- **100% Off-Chain**
- **Fully GDPR Compliant**

**Issuer**

**Verifier**

**Holder**

- **Private Pairwise Peer DIDs**
- **Private Pairwise Peer DIDs**

**Trust**

**Verifiable Data Registry (e.g., Blockchain)**

- **Public Key** + other cryptographic metadata
Why blockchains play a very limited role

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.
ZKP-Based VCs

- **Holder**
  - ZKP-Encoded Credential
  - Zero-Knowledge Proof
- **Issuer**
  - Link Secret
  - Trust
- **Verifier**
  - Selective disclosure + non-correlatable digital signatures and proofs

**Private DIDs**

**Public DIDs**

**Verifiable Data Registry (e.g., Blockchain)**

- DID
  - Public Key + other cryptographic metadata
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
- Issued to highly trackable public DIDs
- Do not use zero-knowledge proofs (ZKPs)
- Do not use privacy-preserving protocols

Privacy Preserving VCs
- Issued to privacy-preserving identifiers
- Use zero-knowledge proofs (ZKPs)
- Use privacy-preserving protocols
The Special Role Of Governance Frameworks
How can verifiers know all the issuers?
The governance trust diamond

Issuer

Bank

Verifiable Credential

Trust

Governance Authority (Issuer)

Mastercard

Governance Framework

Cardholder

Verifier

Holder

Issuer Holder

Wallet

Proof

Bank

Merchant

Mastercard
The governance trust diamond

1. **Issuer**
   - Holder
   - Publishes
   - Governance Authority (Issuer)

2. **Health Authority**
3. **Traveler**
   - Verifier
   - Proof
   - Verifiable Credential

4. **Airline**
   - IATA
   - Governance Framework

- The diagram shows the relationships and trust models among issuers, holders, verifiers, and airlines in a governance framework.
How can we standardize DIDs and VCs for universal interoperability?
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