

# The State of SSI

Drummond Reed  
Chief Trust Officer, Evernym

Hyperledger Identity Working Group  
25 November 2020

 THE **LINUX** FOUNDATION

 evernym

# Highlights

1. Trust over IP (ToIP) Interoperability Profiles (TIPs)
2. ToIP Human Experience Working Group
3. Lumedic Exchange (ToIP Layer 4 Digital Trust Ecosystem for healthcare)
4. COVID-19 Credential Initiative (CCI) Governance Framework
5. IATA Travel Pass
6. Yale Open Climate Platform
7. W3C DID Core Specification
8. DIF DIDComm V2
9. KERI (Key Event Receipt Infrastructure)



**TRUST**  
Over **IP**  
**FOUNDATION**

The Trust over IP Foundation is defining a complete architecture for Internet-scale digital trust that combines both cryptographic trust at the machine layer and human trust at the business, legal, and social layers.

## Trust over IP Governance Stack

### Ecosystem Governance Frameworks



### Credential Governance Frameworks



### Provider Governance Frameworks



### Utility Governance Frameworks



Layer 4

Layer 3

Layer 2

Layer 1

## Trust over IP Technology Stack

### Application Ecosystems



### Data Exchange Protocols



### DIDComm Peer to Peer Protocol



### Public Utilities





# Trust over IP Foundation Introduces a New Tool for Interoperable Digital Trust

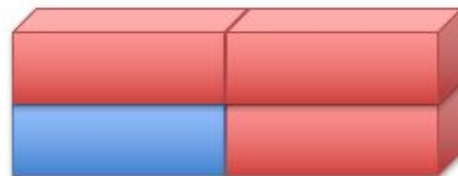
By [trustoverip](#) | October 19, 2020 | [Blog](#)

When the ToIP Foundation launched in May 2020, our mission was to define a new model for achieving trust online—a model that breaks away from the thousands of siloed solutions for secure, privacy-enhancing digital identity and trust that do not work with each other. This lack of interoperability costs billions of dollars per year in complicated and time-consuming integration and hinders adoption by the very customers we are trying to serve.

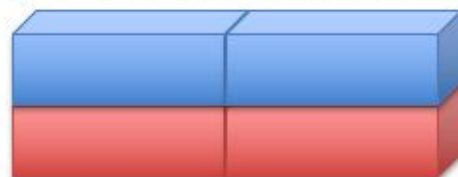
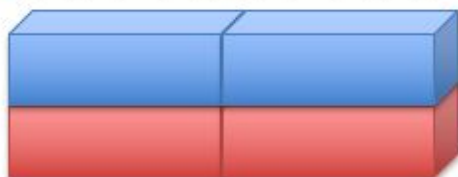
## TIP A

## TIP B

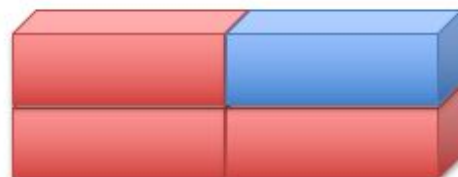
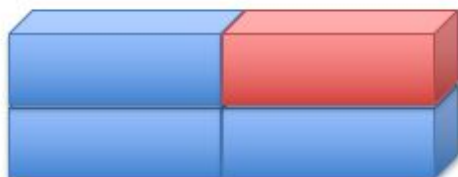
Layer 4



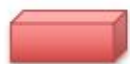
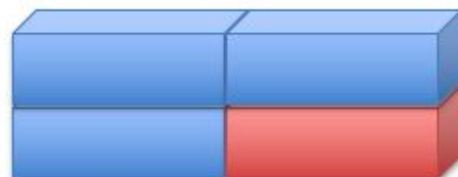
Layer 3



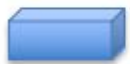
Layer 2



Layer 1

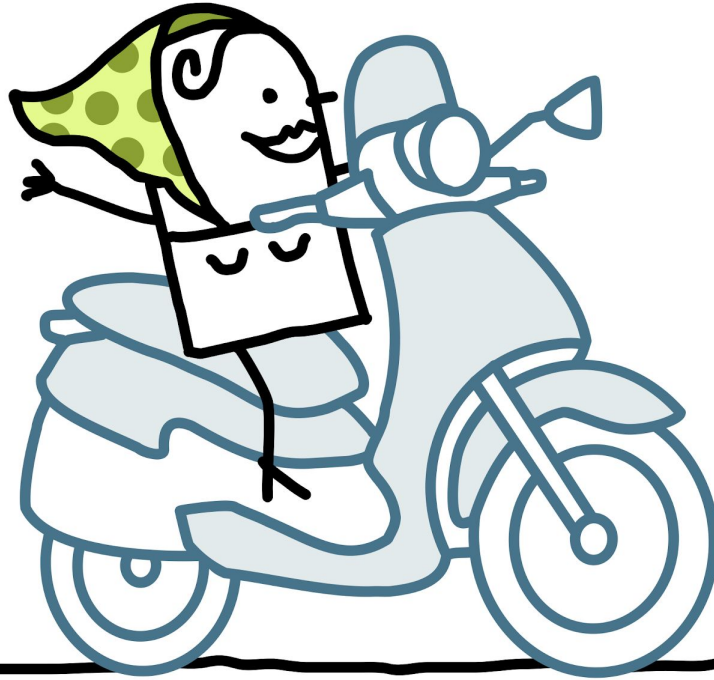


Custom TIP-specific  
component



Standard TSS  
component





# The Human Experience

*(working group)*

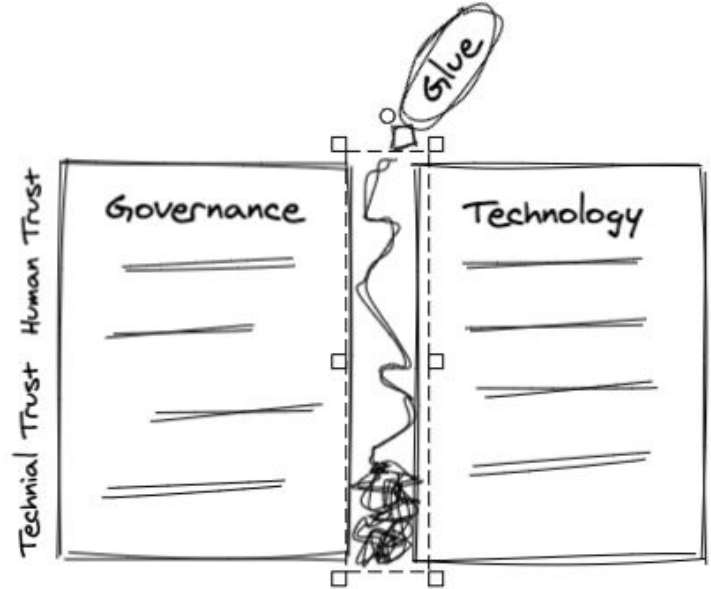
The  
November  
2020  
Roadshow!

# What is HXWG?



*Not your leftover scrabble tiles.*

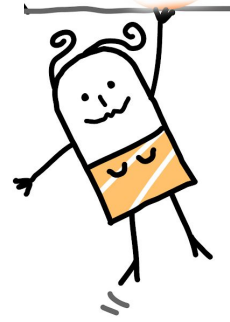
- Put people at the heart of the work of ToIP using human centered design
- Develop strategic and practical resources to improve outcomes
- Develop trust-centric best practices of user experience design
- The glue between the technical and governance stacks





# Anything else we should know?

*Yep. You should know our guiding principles.*



## 1. Inclusive by Design

*We will follow the principles of inclusive design to enable the ToIP community to serve the widest possible community of ecosystem partners.*

## 2. Cross pollination in ToIP

*We will actively seek to inject human experience into ToIP Working Groups and Task Forces*

## 3. Respectful by Design

*We recognize that diversity of participation is not enough to give voice to minority or excluded groups. We will find ways to enable communities to own and control the design process and its outcomes.*

# You seem really cool. Can we join the HXWG?

*Yes! Just wait until we teach you the secret handshake.*

We are looking for:

Social/research scientists

UX/CX experts

Marketing, CRM, communications professionals

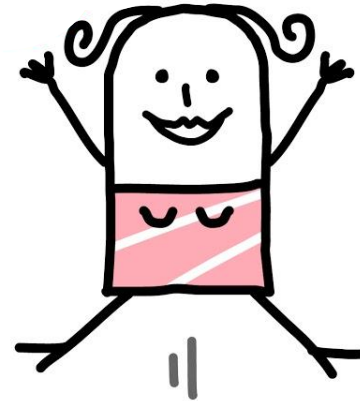
Members of diverse communities

Accessibility designers

Folks who don't identify as "techy"

Folks who identify as "troublemaker techies"

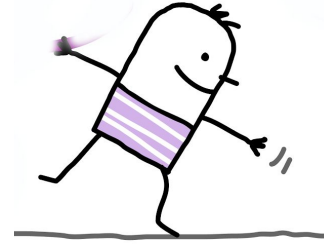
Humans



*If you have difficulty with digital access or a particular disability and want to join this group, please let us know as your input is critical and, we will make your participation possible.*

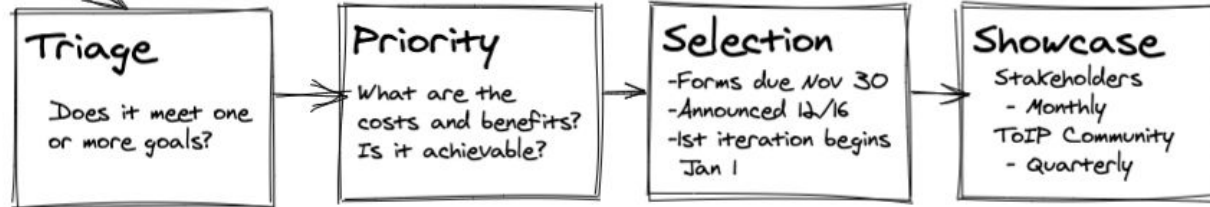
# Got it. So how do we get started?

*We're so glad you asked!*



Fill out this form!

[HXWG Project Request](#)





Home

 Pages Blog

SPACE SHORTCUTS

 File lists Meeting notes

PAGE TREE

▸ Steering Committee

▸ Education and Resources

▸ Concepts &amp; Terminology Working Group

▸ Semantics Working Group

▸ Ecosystem Foundry Working Group

▸ Governance Stack Working Group

▸ Technology Stack Working Group

▸ Utility Foundry Working Group

• Meeting notes

• **Human Experience Working Group**Dashboard / Trust over IP Foundation  Edit Save for later Watching Share

# Human Experience Working Group Charter

Created by David Luchuk, last modified by Drummond Reed just a moment ago

- [1. Introduction](#)
- [2. Scope](#)
- [3. Purpose](#)
- [4. Principles](#)
- [5. Example Deliverables](#)
- [6. HXWG Start-Up Approach](#)
- [7. IPR Licensing](#)
  - [1\) Copyright Policy](#)
  - [2\) Approved Deliverable Patent Licensing.](#)
  - [3\) Source Code.](#)
- [8. Non-Working Group Participant Feedback and Participation](#)

## **NOTE**

- All Trust over IP members are invited to review the proposed charter for this working group below.
- Please make your comments directly on this page ([see this tip about how to make comments directly inline](#)) or submit your comments to [operations@trustoverip.org](mailto:operations@trustoverip.org) or to [dluchuk@contractor.linuxfoundation.org](mailto:dluchuk@contractor.linuxfoundation.org) by **Monday, November 9, 2020**.

## **CHARTER - Human Experience Working Group**

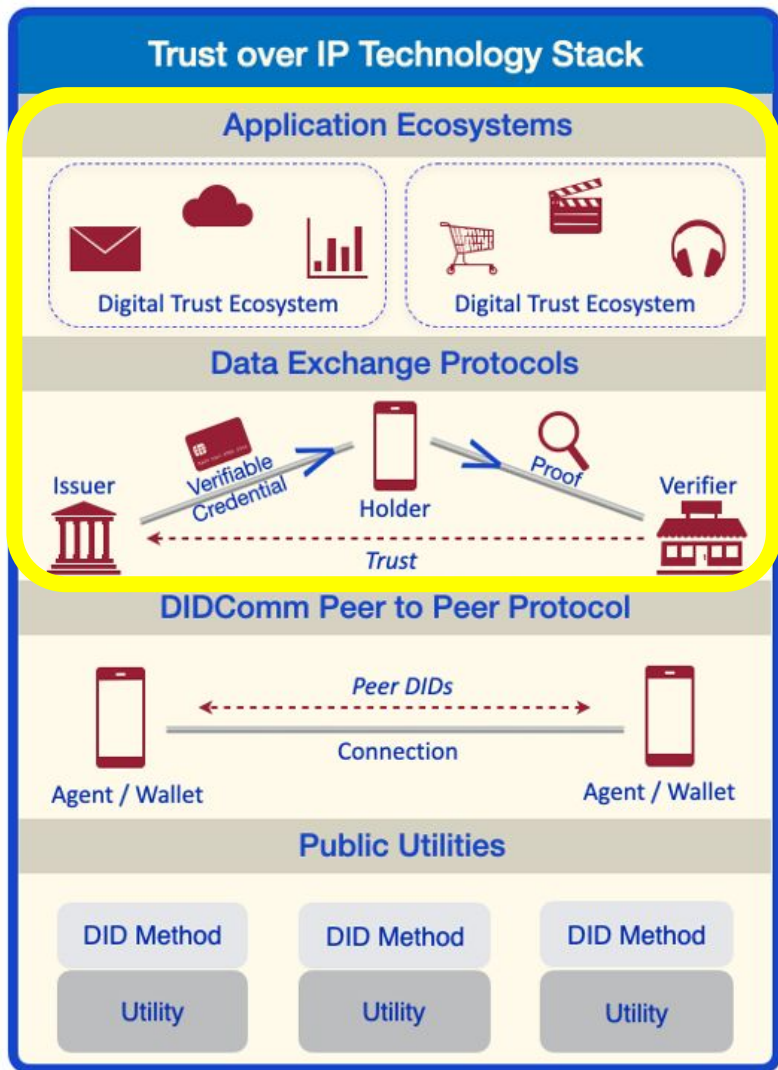
This Working Group Charter establishes the Scope, Principles, Purpose, Activities, Deliverables and intellectual property terms used to develop the materials identified in this Working Group Charter for the Project. Only Project Steering Members, Associates, and Contributors that Joined the Working Group will be bound by its terms and be permitted to participate in this Working Group.

AN OPEN COMMUNITY

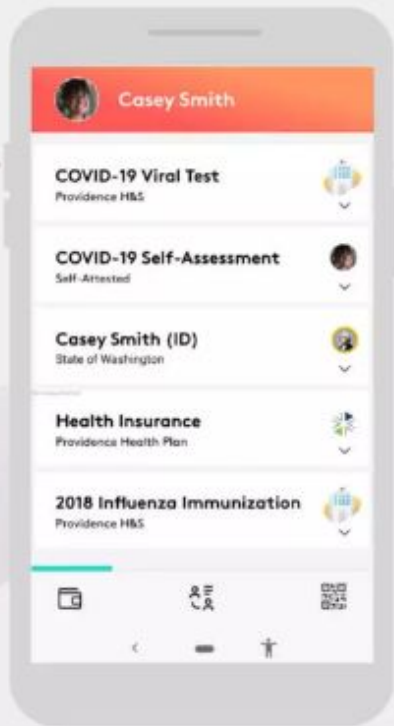
# Lumedic Exchange

The Lumedic Exchange is the community of organizations taking on healthcare interoperability by thinking differently about the role patients play in the exchange of their own personal health information.









PROVIDERS



PAYERS



BUSINESSES



<https://www.lumedic.io/perspectives/introducing-lumedic-connect>



# COVID-19 CREDENTIALS INITIATIVE



Supporting projects that use privacy-preserving Verifiable Credentials (VCs) in order to **mitigate the spread of COVID-19** and strengthen our societies and economies.

# CCI Governance Framework

- › The COVID-19 Credentials Initiative Governance Framework (CCI GF) V2 has been completed, and is almost ready for public release.
- › Individuals from around the world created the CCI GF V2, including strong contributions from India, East Asia, N. America and Europe.
- › The CCI GF has been presented to a few organizations, including [HIMSS](#).
- › CCI will take actions to expand awareness, and use/adoption of the GF.
- › Principles, policies and guidance for verifiable credentials in COVID-19 related use-cases
  - › Protect Individuals
  - › Reduce utilization friction
  - › Alignment with jurisdictional regulatory compliance
  - › Shape best practices

Meeting notes

PAGE TREE

- > Steering Committee
- > Education and Resources
- > Concepts & Terminology Working
- > Semantics Working Group
- ▼ Ecosystem Foundry Working Grc
  - Ecosystem Working Group File
  - > EFWG Meeting Page
  - > EFWG Concepts and Workflow
  - > Ecosystem White Paper Task F
  - Ecosystem Governance Stack
  - ▼ **CCI GF Task Force**
    - > CCI GF V1 Documents - All A
    - Human Trafficking Ecosystem
    - Internet of Education (IoE) Eco
    - > Patient Identity Task Force
    - Sovrin Ecosystem Governance
    - > Internet of Research Ecosyster

[Dashboard](#) / [Trust over IP Foundation](#) / [Ecosystem Foundry Working Group](#)

# CCI GF Task Force

Created by Chris Raczkowski, last modified by Paul Knowles on Oct 06, 2020

## Industry sector: [Health Care](#)

- [Objectives](#)
- [Background/Context](#)
- [Organizers](#)
- [Membership and Joining](#)
- [Deliverables](#)
- [Intellectual Property Rights \(Copyright, Patent, Source Code\)](#)
- [Milestones](#)
- [Meeting Schedule](#)
- [Mailing List and Communications](#)

This page describes the COVID-19 Credentials Initiative Governance Framework Task Force (the "**CCI GF TF**"). It was created by Sankarshan Mukhopadhyay and Chris Raczkowski.

## Objectives

1. To develop and make available a set of documents which include (but are not limited to) a governance framework (a "**GF**") for verifiable digital credentials related to COVID-19 emergency response,
2. To with the establishment of an appropriate governance authority (a "**GA**") for the GF,
3. To help enable the development of tools, methods and systems which promote adoption of the GF by many organizations globally.

**IATA  
GLOBAL  
MEDIA DAYS**



# IATA Travel Pass

**Nick Careen**

Senior Vice President, Airport,  
Passenger, Cargo & Security

#IATAMediaDays 23 and 25 November 2020





# Re-opening borders safely

## Issue

Governments need to be confident that they are mitigating the risk of importing COVID-19 to re-open borders without quarantine and restart aviation.

## Solution

Testing has been proven to be the safest and most effective method to achieve this. And passengers are willing to get tested to travel.

## Confidence

But both passengers and governments need to have confidence in each passenger's verified COVID-19 status.



# The challenges

## **Passengers**

Need accurate information on test requirements, where they can get tested or vaccinated, and the means to securely convey test information to airlines and border authorities

## **Airlines**

Need to have the ability to provide accurate information to their passengers on test requirements and verify that a passenger meets the requirements for travel

## **Governments**

Need to be able to verify the authenticity of tests and the identity of those presenting the test certificates

## **Laboratories**

Need to be able to issue certificates that will be recognized by governments

# IATA Travel Pass

## Developed for everyone



### Registry of Health Requirements

powered by Timatic

- Enables passengers to find accurate information on travel, testing (and eventually vaccine) requirements for their journey

### Registry of testing / vaccination centers

- Enables passengers to find testing centres and labs at their departure location which meet the standards for testing/vaccination requirements of their destination

### Lab App

- Enables authorized labs and test centers to securely send test results or vaccination certificates to passengers

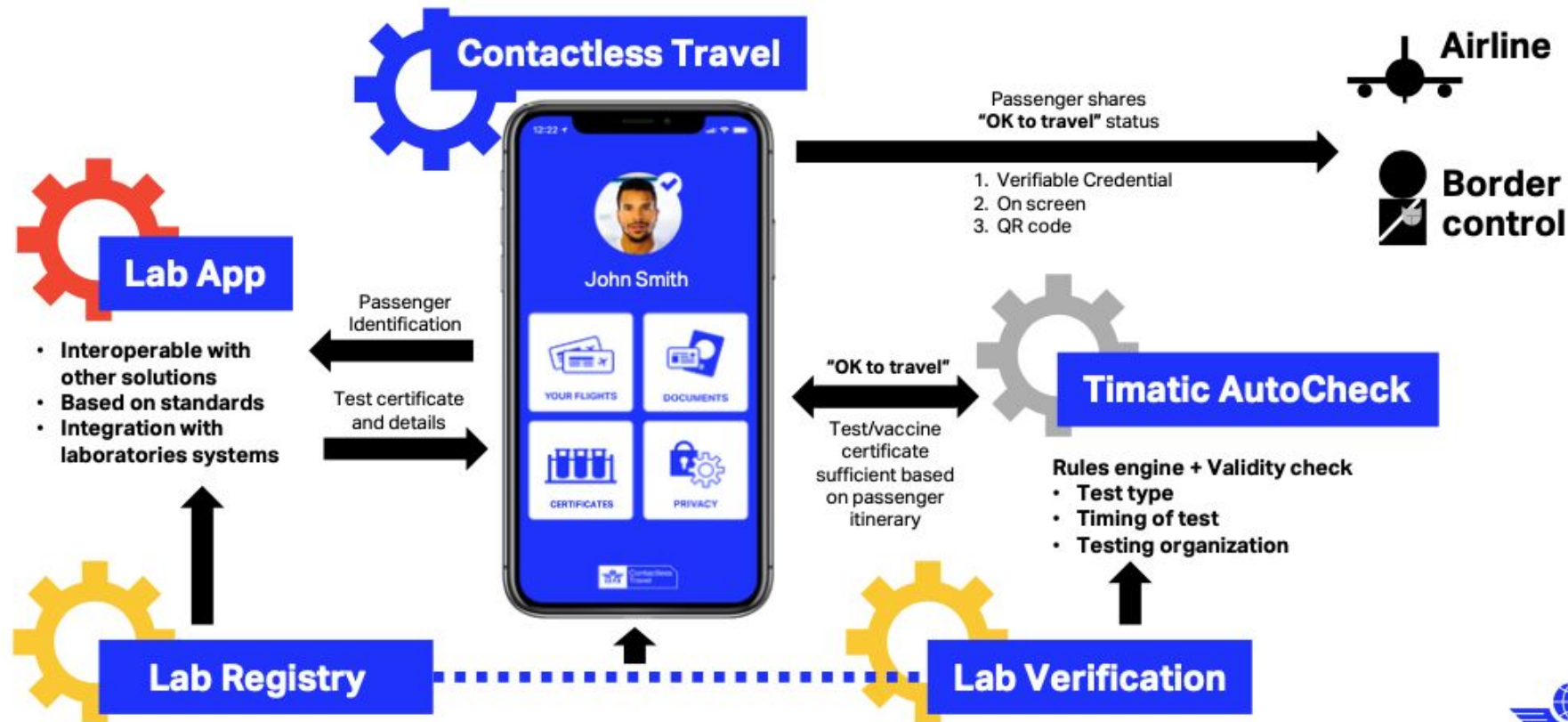
### Contactless Travel App

- Enables passengers to (1) create a 'digital passport', (2) verify their test/vaccination meets the regulations & (3) shares test or vaccination certificates with authorities to facilitate travel.
- Can be used by travelers to manage travel documentation digitally and seamlessly throughout the travel experience.



# How the modules combine as an integrated service

## Overview





# High level data privacy and security

'Decentralized Technology' means there is **no** central database holding passenger information

## Rights

Passengers have the sole right share to their data

Users can delete their data anytime on their app

## Compliance

Country regulations on access to passengers' data will be respected (eg France & Germany)

# IATA Travel Pass principles

## Modular and interoperable with:

- Other COVID-19 solutions
- Existing airline and industry solutions



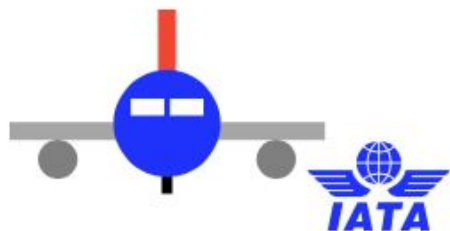
## Based on standards:

- ICAO DTC
- W3C – Digital Comms
- One ID initiative



## Solution for everyone:

- IATA is a trusted industry body
- Industry expertise
- Favors a collective solution





Yale openlab.

open. projects team

join

# Open Climate

*an open source project leveraging blockchain for a global,  
transparent and integrated climate accounting system*



# Exploring the use of blockchain for global climate accounting

The open climate project is an open source initiative exploring the application of blockchain and other emerging technologies, such as IoT (Internet of Things), big data and machine learning, to the challenge of helping the world keep a transparent accounting system as we strive to achieve the climate targets set in the 2015 Paris Agreement (PA)—i.e. maintaining anthropogenic warming below 1.50C. The project is currently incubated at the Yale Open Innovation Lab (openlab) and combines multiple other project components incubated and developed by a growing network of collaborators.

<https://openlab.yale.edu/open-climate>

PLATFORM  
STACK LAYOUT



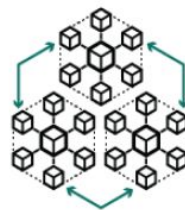
& CORE  
FUNCTIONALITY

FRONT END  
PORTAL



Front end

**BLOCKCHAIN  
LAYERS &  
INTEROPERABLE  
ECOSYSTEMS**



This technological section involves the core protocols allowing different blockchain ecosystems (eg. public and private) to adopt and participate under a common smart contract (eg. paris agreement), communicating specific record entries and states, allowing nested governance and consensus layers and yet maintain a distinct identification within the network of networks.



Smart contracts



Ledger records



Node network



Decentralised IDs



Interoperability (IBC)



# Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations



W3C Working Draft 08 November 2020

**This version:**

<https://www.w3.org/TR/2020/WD-did-core-20201108/>

**Latest published version:**

<https://www.w3.org/TR/did-core/>

**Latest editor's draft:**

<https://w3c.github.io/did-core/>

**Previous version:**

<https://www.w3.org/TR/2020/WD-did-core-20201108/>

**Editors:**

[Drummond Reed](#) (Evernym)

[Manu Sporny](#) (Digital Bazaar)

[Markus Sabadello](#) (Danube Tech)



## 1. Purpose and Scope

### 1.1 Overview

### 1.2 Specific Requirements

### 1.3 Ramifications

#### 1.3.1 Message-Based, Asynchronous, and Simplex

#### 1.3.2 Message-Level Security, Reciprocal Authentication

### 1.4 Processing Model

## 2. Message Structure

### 2.1 Message Headers

### 2.2 DID Rotation

#### 2.2.1 JWT Details

#### 2.2.2 Example Message Rotating DID

#### 2.2.3 Rotation Limitations

# DIDComm Messaging

Specification Status: Editor's Draft

Latest published version: [identity.foundation/didcomm-messaging/docs/spec](https://identity.foundation/didcomm-messaging/docs/spec)

Editors:

Contributors: Daniel Hardman

Participate:

[GitHub repo](#)

[File a bug](#)

[Commit history](#)

Testing: 4

---

## § 1. Purpose and Scope

The purpose of DIDComm is to provide a secure, private communication methodology built atop the decentralized design of [DIDs](#).



KERI is a new approach to decentralized identifiers and decentralized key management that promises significant benefits for SSI (self-sovereign identity) and ToIP (Trust over IP) infrastructure



## Trust over IP Governance Stack

### Ecosystem Governance Frameworks



### Credential Governance Frameworks



### Provider Governance Frameworks



### Utility Governance Frameworks



Layer 4

Layer 3

Layer 2

Layer 1

## Trust over IP Technology Stack

### Application Ecosystems



### Data Exchange Protocols



### DIDComm Peer to Peer Protocol



### Public Utilities

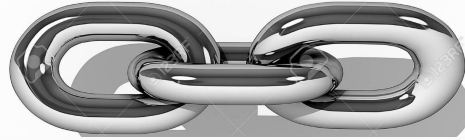


Although the full technical architecture of KERI goes very deep (140 pages), the seven main features and benefits are not hard to explain

Caveat: all of this depends on one fundamental concept:  
**public and private keys**



Public key— **MUST**  
be shared



Cryptographic  
binding



Private key— **MUST**  
**NOT** be shared

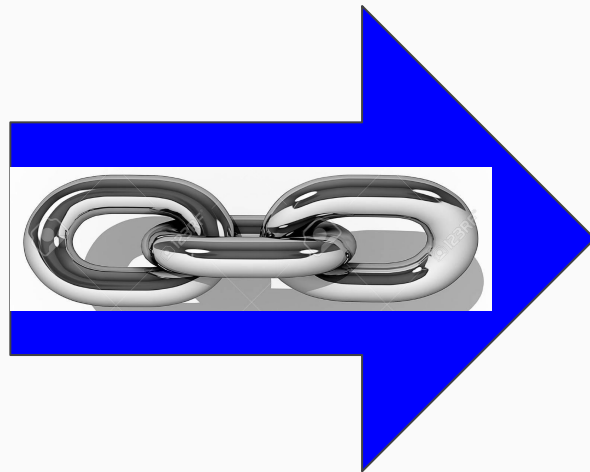
# #1: Self-Certifying Identifiers

A self-certifying identifier (SCID)  
is a identifier that can be  
proven to be the one and only  
identifier tied to a public key  
using cryptography alone\*

\* No blockchain needed



Public key

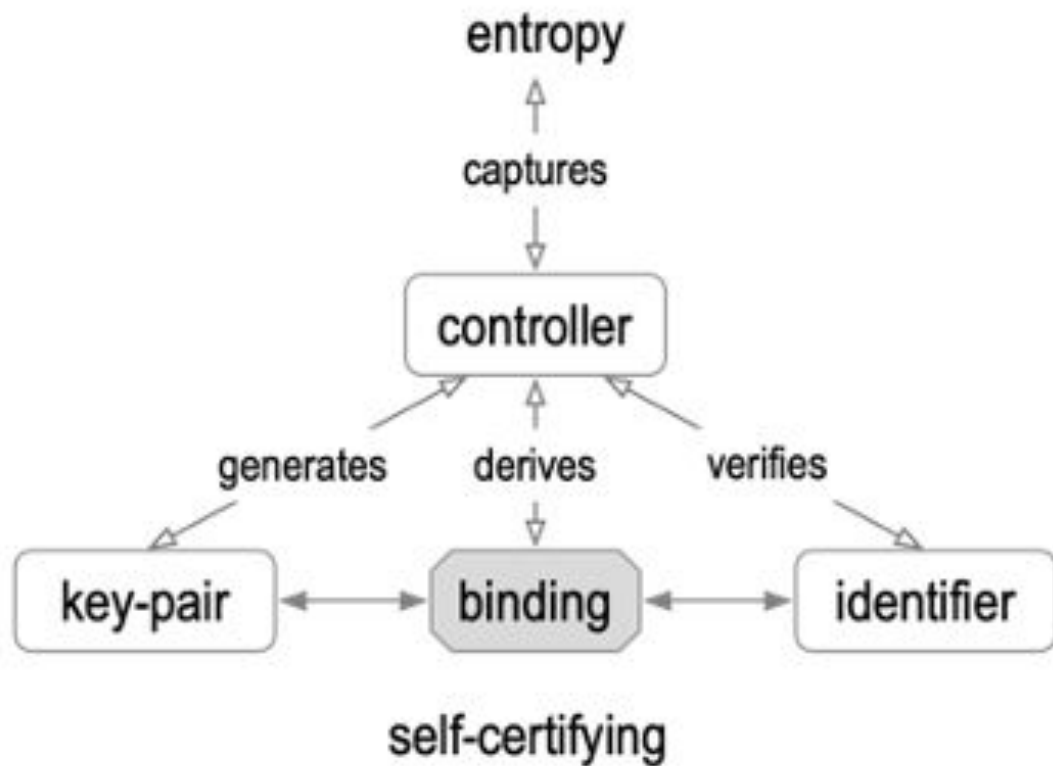


Cryptographic  
binding

keri : 21tD  
AKCERh95u  
GgKbJNHyp

Self-certifying  
identifier





## Benefit #1

You can prove you control a KERI identifier without needing to rely on **ANYONE** outside your control (even a blockchain)

For the other 6 benefits  
(and more about KERI):

<https://keri.one>

<https://identity.foundation/working-groups/identifiers-discovery.html>

Thank you!

May your keys be with you!

[drummond.reed@evernym.com](mailto:drummond.reed@evernym.com)  
[@drummondreed](https://twitter.com/drummondreed)