# Self-Sovereign Identity
# La nuova identità digitale decentralizzata

This work is licensed under CC BY-NC-SA 4.0. To view a copy of this license, visit
http://creativecommons.org/licenses/by-nc-sa/4.0/

innova

# Identità digitale

- La tecnologia blockchain abilita le transazioni senza intermediari, utilizzando identità anonime (o meglio pseudonime), ma cosa succede quando vogliamo accertare l'identità online delle controparti?

- **Cosa facciamo online? Acquistiamo beni fisici, l'ecommerce è l'applicazione di maggior successo ma.. solo perché gli oggetti devono arrivare a casa!**

- **Aprire conto bancario ?**
- **Iscriversi all'università ?**
- **Acquistare una casa ?**
- **Come aziende, partecipare a gare oppure a processi di acquisizione di beni e servizi?**

- **Soluzione tipica: Scansione e invio di file PDF!**

# Problemi dell'identità digitale

- «Identity is the MOST IMPORTANT thing YOU DON'T OWN»
- Problemi legati a ID e password:
  - Ne usiamo troppe (centinaia di password memorizzate nel "portachiavi")
  - Difficoltà di ricordare le password e schemi di complessità -> stessa password
  - Hacker prendono di mira grandi sistemi per ottenere migliaia di identità:
    - Data breach
    - Il riconoscimento è «a senso unico» -> Phishing
- Identificatori centralizzati
  - Non sono in nostro possesso!
  - Possono essere revocati senza il nostro consenso
  - "esisto solo perchè qualcun altro lo certifica"

# Problemi dell'identità digitale

- Soluzione «comune» è peggio del problema :
  - Login with Facebook
  - Login with Twitter
  - Login with Google

- Portano a **correlazione non voluta (possibilità di associare senza il consenso del soggetto lo stesso ID su più sistemi trasversali)**

- **Soluzione: Autenticazione a due fattori (2FA), es SPID**
  - Una cosa che conosco (password)
  - Una cosa che possiedo (codice su cellulare)

# SSI: la «Teoria del tutto» dell'identità digitale?

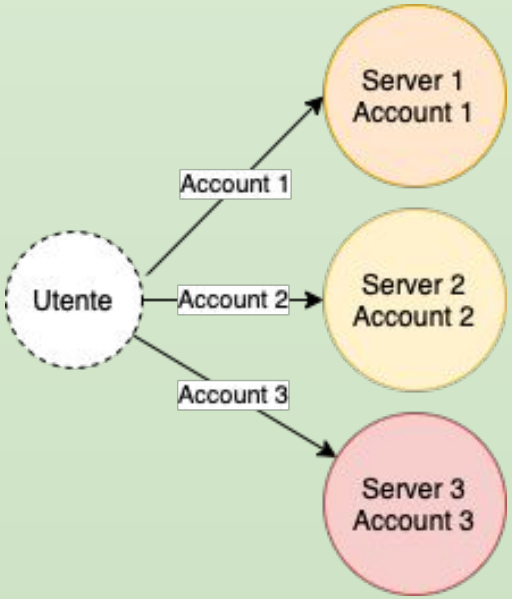
- **Self Sovereign Identity:** Drummond Reed, identity guru of the Sovrin Foundation:

*«Lifetime portable identity for any **person**, **organization**, or **thing** that does not depend on any centralized authority and can **never** be taken away.»*

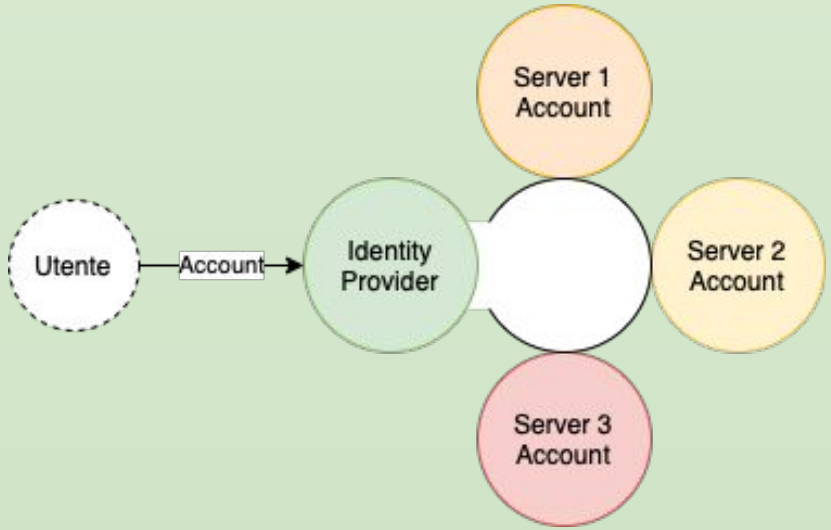
- 10 principi di SSI : Christopher Allen, (W3C Credentials Community Group)
  - Users must have an independent existence
  - Users must **control their identities**
  - Users must have access to their own data
  - Systems and algorithms must be **transparent**
  - Identities must be long-lived
  - Information and services about identity must be **transportable**
  - Identities should be as **widely used** as possible
  - Users must agree to the use of their identity
  - Disclosure of claims must be minimized
  - The **rights of users** must be protected

# Modelli di identità

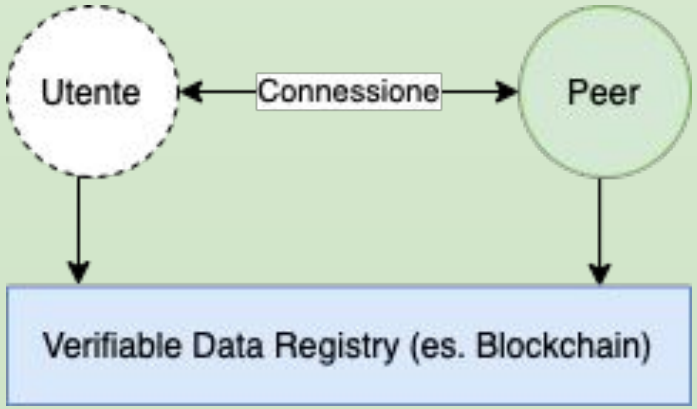
- Centralizzata




- Federata




- Decentralizzata



# DID - Decentralized Identifier

- **I Decentralized Identifiers** sono l'elemento chiave del modello delle Verifiable Credentials
- I DID sono in corso di standardizzazione presso il Web Consortium (W3C). Il modello dei Verifiable Credentials si basa su un'infrastruttura decentralizzata composta da DID e da altri applicativi di controllo
- I DID sono:
  - Un nuovo tipo di identificatore  - es.  «uniform resource locator» (URL)
  - Creati autonomamente dal proprietario in qualunque momento
  - Indipendentemente da qualunque autorità centrale
  - Univoci a livello globale
  - Verificabili mediante la crittografia

# Verifiable Credentials vs Credenziali cartacee

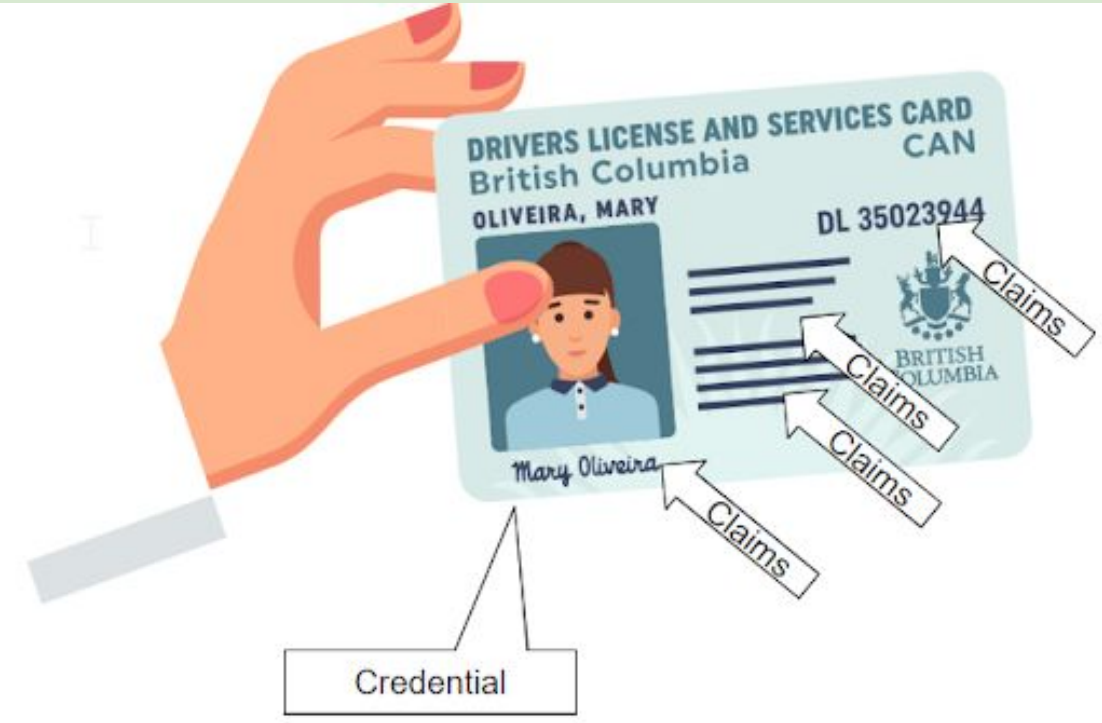
- **Verifiable Credentials W3C Rec. v1.1 09/11/2021**
  (patente, passaporto, certificazioni, singolo claim, …)

  - Chi ha emesso le credenziali;
  - Che le credenziali sono state emesse all'entità che le sta presentando;
  - Che le credenziali non sono state revocate (ove ammesso per scelta progettuale);
  - Che le credenziali e i singoli claim non sono stati alterati verifica eseguibile automaticamente;
  - Possono essere collegate digitalmente ad un DID;

- **Credenziali cartacee**
  (patente, passaporto, certificazioni, …)

  - Chi ha emesso le credenziali;
  - Chi possiede le credenziali;
  - Che il contenuto delle credenziali non è stato contraffatto (richiede conoscenze tecniche per l'operatore)

# Relazione tra “Credenziale” e “Claim”




Con le Verifiable Credentials,
**non è possibile rubare l’identità di un'altra persona solo perché si possiedono sue informazioni personali** (per es. nome, indirizzo, telefono, username, password, pin etc.).

**Un claim è una singola unità** informativa all’interno di una credenziale (per es. nella Carta d'Identità, la data di nascita e l’indirizzo sono claim distinti).

# SSI in pratica

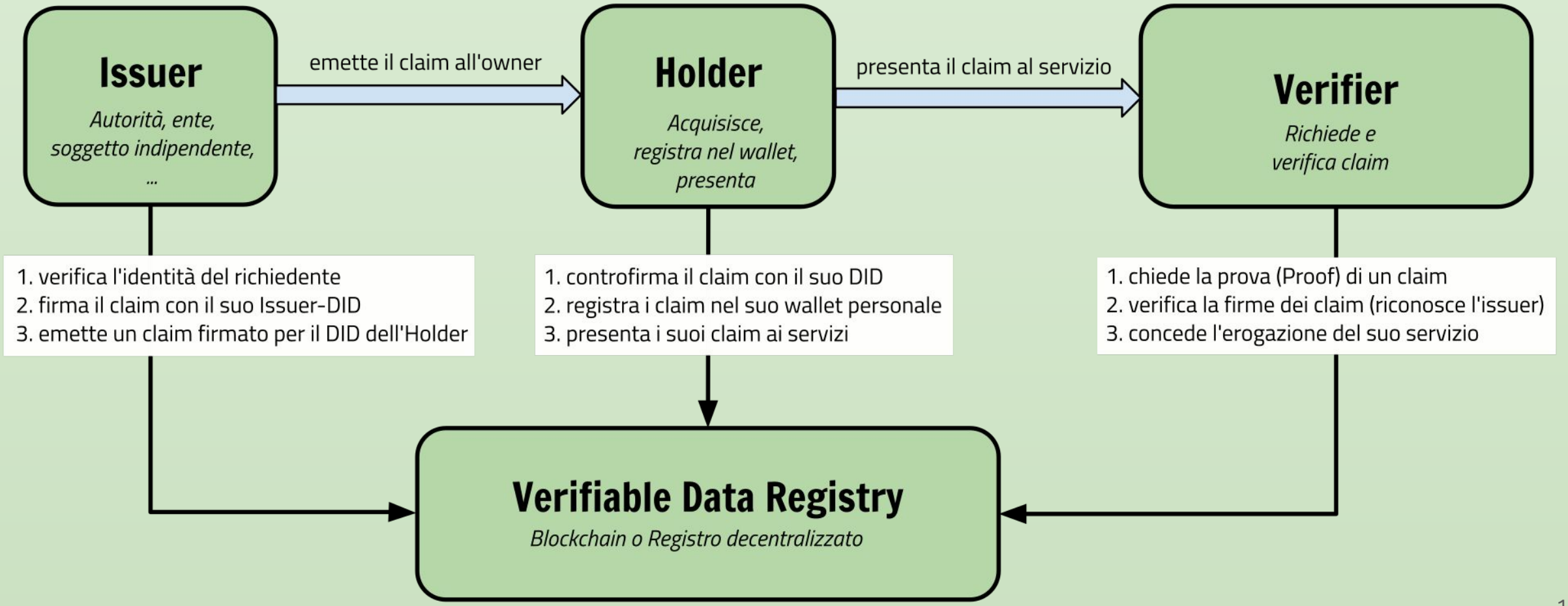

**Nel mondo fisico** presentiamo credenziali che vengono verificate e giudicate attendibili da parte di altre persone.

**portafogli**

**Nel mondo digitale** per ottenere servizi abbiamo bisogno di standard comprensibili alle macchine per verificare le credenziali di un soggetto: DID, Verifiable Credentials, ...

**wallet/agent**

# Modello Issuer, Holder, Verifier



# Vantaggi notevoli

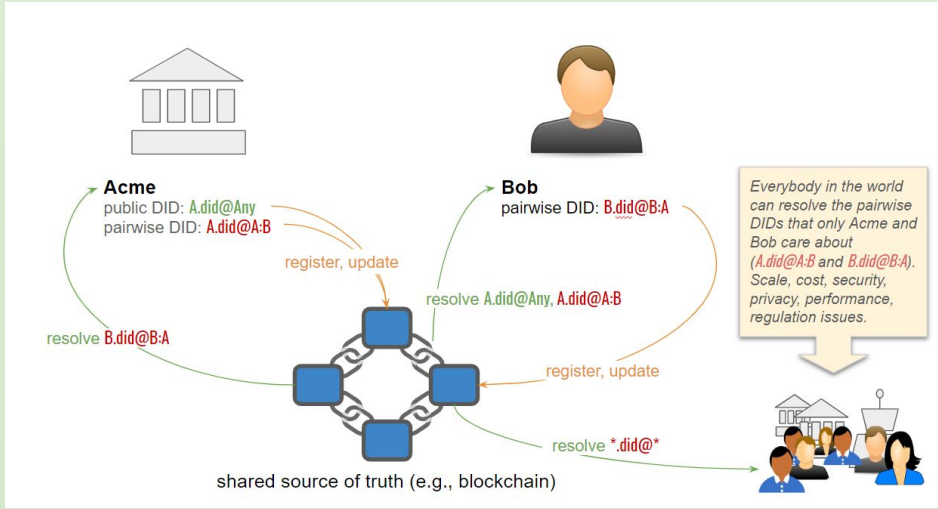
- Ridare in mano alle persone il potere di controllo sui propri dati personali
- Decorrelazione delle attività utente
- Possibilità di agganciare qualsiasi Credenziale Verificabile ad un DID
- Verifica asimmetrica delle credenziali anche offline
- Human-Machine readable / automazione
- Liste di revoca CRL opzionali secondo le scelte progettuali;
  vale a dire che una volta che genero e pubblico un mio DID, se lo schema in cui pubblico il mio identificatore non prevede l'uso di liste revoca (condizione non modificabile) nessuno potrà mai togliermi il mio identificatore ossia la mia identità digitale (non censurabile).

# SSI: gli «attori»

- Il **World Wide Web Consortium (W3C)** si occupa di standardizzare la gestione delle identità digitali decentralizzate.

- La **Decentralized Identity Foundation** ha l'obiettivo di realizzare il nuovo **ecosistema open** per identità decentralizzate https://identity.foundation/
- DIF rappresenta un insieme diversificato e internazionale di organizzazioni che lavorano insieme per creare un ecosistema aperto di identità decentralizzata accessibile a tutti.
- Il network Sovrin: https://sovrin.org/

# Trusted Issuer




- Una società o un ente pubblico userà **sempre** un DID pubblico
- Chiunque emette verifiable credentials dovrebbe avere un DID pubblico.
- Un possessore di credenziali può potenzialmente presentarle a chiunque, quindi il verificatore deve conoscere l'identità dell'issuer per verificare la chiave pubblica, l'eventuale revoca e quindi  per decidere se si può «fidare».
- Ci serve un «elenco telefonico» globale per i DID: ad es. una **BLOCKCHAIN**

# Casi d’uso a breve termine

- Authentication and authorization
- In-person verification
- Proof of training
- E-procurement

# Casi d'uso concreti di SSI

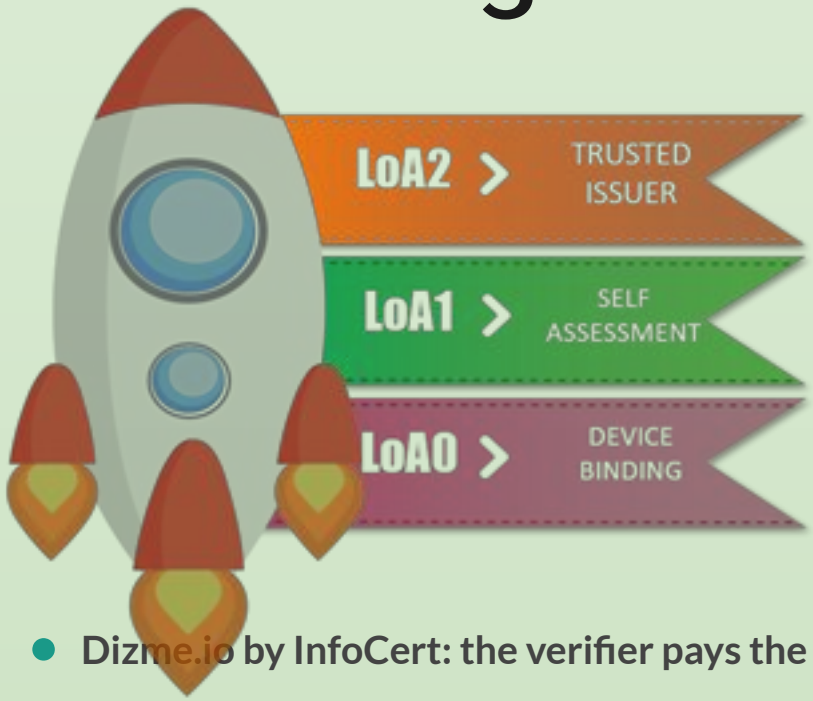
- **Riutilizzo di procedure KYC**: "proprietà transitiva della fiducia":

  **"se mi fido di qualcuno, posso utilizzare le credenziali verificabili che emette":**

  - **https://email-verification.vonx.io: procedura per l'emissione della credenziale che attesta il «controllo di un indirizzo mail»**
  - **https://iiwbook.vonx.io: consente l'autenticazione al sito con la credenziale emessa**

- **Solvibilità / centrale rischi / AML**

# Validità legale di SSI




**LoA2 - è il livello più alto di sicurezza**

L'utente in possesso del LoA1 deve rivolgersi ad un ISSUER certificato e abilitato a riconoscerlo per rilasciargli tale livello di sicurezza. Necessita di una modalità di riconoscimento forte (es. de visu, da remoto, ...)

**LoA1 - è il livello medio di sicurezza**

All'utente viene richiesto di catturare la foto del proprio volto (selfie) e la foto fronte retro del proprio documento di identità e di validare i dati anagrafici che il sistema estrae automaticamente dalle foto scattate.

**LoA0 - è il livello più basso di sicurezza**

L'utente inserisce il proprio indirizzo email e il proprio numero di cellulare e li verifica inserendo le OTP che l'utente riceverà singolarmente sui rispettivi canali.

Abilitante al rilascio di firme qualificate

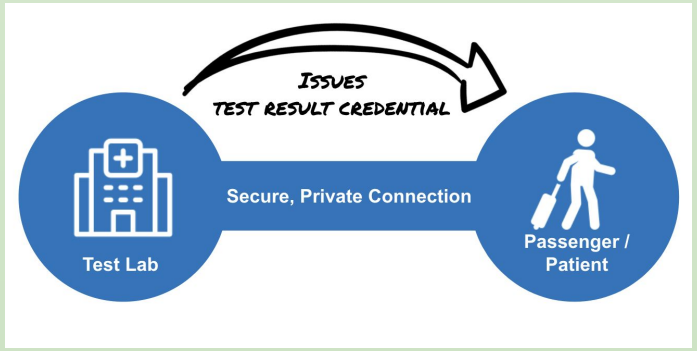
Abilitante al rilascio di firme avanzate

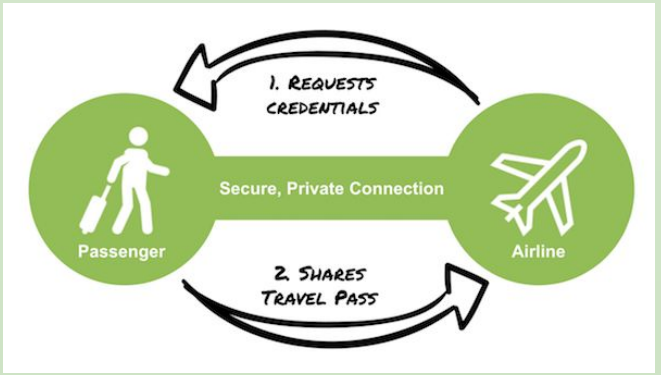
Abilitante al rilascio di firme elettroniche semplici

- **Dizme.io by InfoCert: the verifier pays the issuer, pagamento in crediti DIZ scambiabili con Algo**
- **eIDAS Bridge: le credenziali verificabili sono firmate con una firma digitale attualmente valida per il regolamento eIDAS**
- **Poste Italiane: demo Wallet SSI, ricevo la mia credenziale di identità con autenticazione SPID**

# Casi d'uso di SSI

- **IATA Travel Pass**
- A digital credential solution that enables airlines, governments, and other organizations to instantly verify travel and health documents (such as COVID-19 test results) in a highly secure and privacy-preserving manner.




# EBSI: European Blockchain Services Infrastructure

- Prodotto dell'**European Blockchain Partnership**
- Sfruttare la **blockchain** per la realizzazione di **servizi cross-border** destinati a**:**
    - Amministrazioni
    - Business
    - Cittadini
- **7 Casi d'uso principali**:
    - Diploma Management
    - Document Traceability
    - Trust Data Sharing
    - SME Financing
    - European Social Security Pass (ESSP)
    - Asylum Process Management
    - **Self-Sovereign Identity (ESSIF)**

# ESSIF: European Self Sovereign Identity Framework

- **Obiettivo**: Implementazione di un modello SSI Europeo
- **In Scope**:
  - facilitare **interazione cross-border** con SSI
  - **interoperabilità** tra i progetti SSI nazionali
  - **integrare/allineare «building blocks»** esistenti (eIDAS, e-delivery, once-only) con SSI
  - concettualizzare e costruire un **layer di identità** dentro **EBSI**
  - preservare i **valori** europei/democratici nell'implementazione di SSI
  - stimolare la **trasformazione** SSI dei **servizi pubblici**
  - stimolare lo sviluppo e la **standardizzazione** di SSI a livello globale
- **Out of scope**:
  - Interpretazione dei dati (semantica), standardizzazioni e business logic.
  - realizzazione di un SSI wallet per i cittadini europei.
- DEMO: https://app.intebsi.xyz/demo

# eSSIF-Lab: European SSI Framework Lab

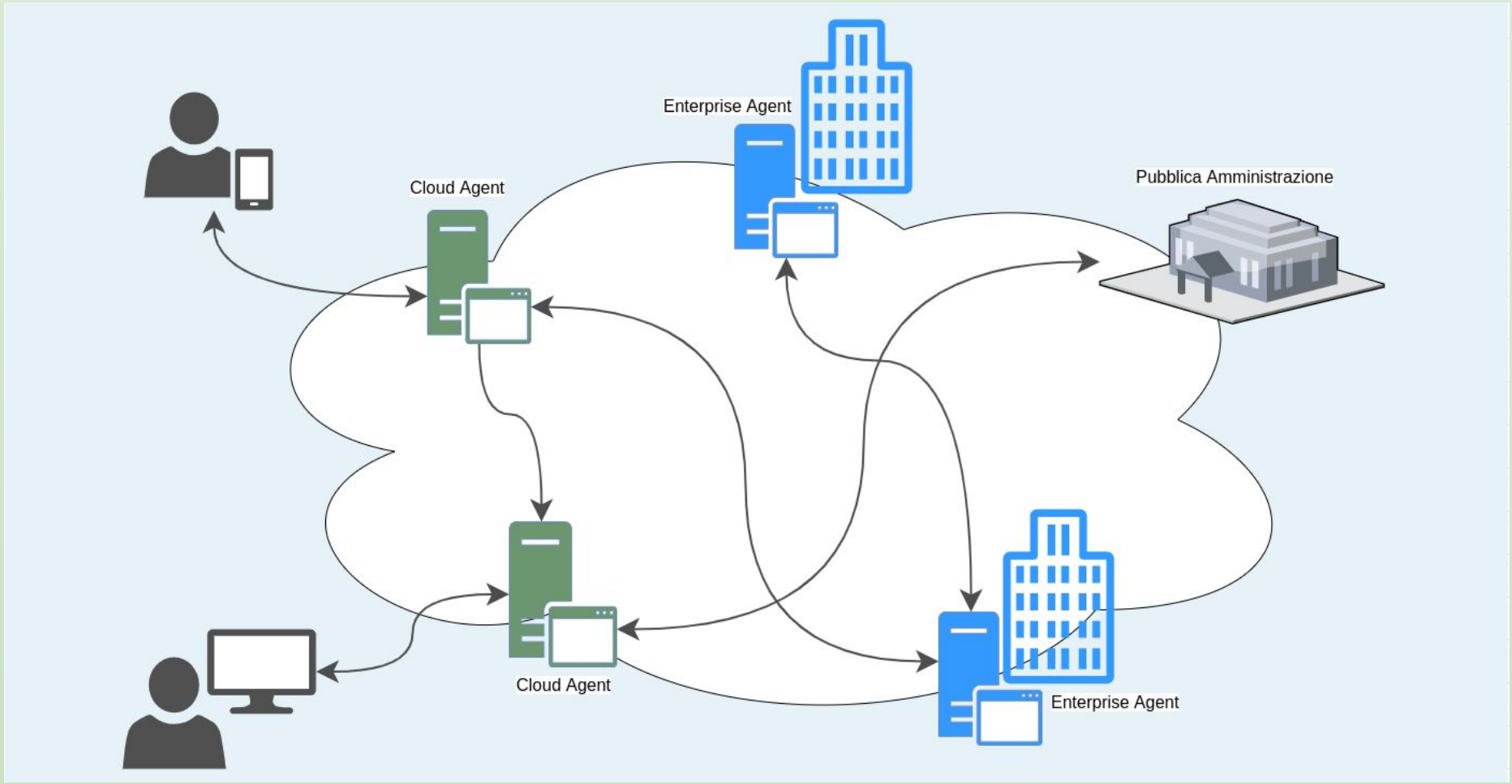
- **ecosistema** di **organizzazioni**

- **obiettivi**:
  - supporto ai **cittadini** Europei e non
  - supporto a **business** e **enti governativi** Europei e non
  - design e sviluppo di un'**infrastruttura SSI**
  - creazione di **community di supporto** all'adozione di soluzioni SSI

- **strumenti:**
  - Infrastructure-oriented call
  - Business-oriented call 1, 2

# Scenari futuri / Gli Agent

Cloud agent e Enterprise agent



# Scenari futuri / Casi d'uso

- Business Logic
- Supply chain
- Blockchain identity
- Machine-2-Machine / Real-time credentialing - IoT
- Data agreement, consent receipts, GDPR compliance
- Delegation of authority with transparency and control

# Conclusioni

## Sfide da affrontare

Necessaria la standardizzazione delle api e dei meccanismi di risoluzione degli identificatori fra i vari attori dell'ecosistema, per garantire l'interoperabilità delle soluzioni.

## Livelli di governance e tecnologici

Queste nuove tecnologie si caratterizzano non solo per la decentralizzazione dell'identità digitale e nel ridare alle persone il potere di controllo sui propri dati personali ma anche per la possibilità di pensare a nuovi meccanismi di automazione e organizzazione delle relazioni tra i partecipanti.
A completamento delle nuove opportunità fornite dalle tecnologie blockchain, permetteranno lo sviluppo di nuovi modelli e logiche di governance, questa volta con accordi, scambi e transazioni "human-machine readable" potenzialmente vincolanti dal punto di vista legale.

Trust Over IP Foundation
CC BY 4.0

Human Trust

Technical Trust

Layer 4

Layer 3

Layer 2

Layer 1

# Governance

## Trust over IP Governance Stack

### Ecosystem Governance Frameworks

Governance Authority → Publishes → Governance Framework

- ✓ Member Directory
- ✓ Auditor
- ✓ Auditor Accreditor

### Credential Governance Frameworks

Governance Authority → Publishes → Governance Framework

- ✓ Credential Registry
- ✓ Authoritative Issuer
- ✓ Insurer

### Provider Governance Frameworks

Governance Authority → Publishes → Governance Framework

- ✓ Hardware Provider
- ✓ Software Provider
- ✓ Agency

### Utility Governance Frameworks

Governance Authority → Publishes → Governance Framework

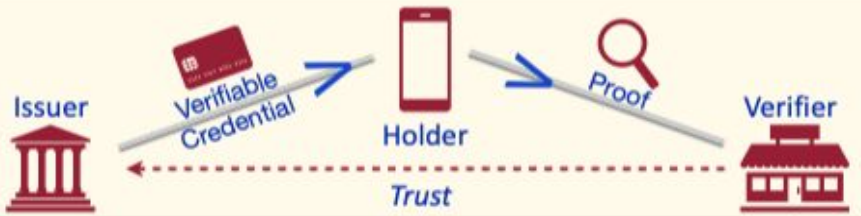
- ✓ Transaction Author
- ✓ Transaction Endorser
- ✓ Steward

# Technology

## Trust over IP Technology Stack

### Application Ecosystems


### Data Exchange Protocols




### DIDComm Peer to Peer Protocol


### Public Utilities

| DID Method | DID Method | DID Method |
|---|---|---|
| Utility | Utility | Utility |

# Grazie per l'attenzione
# Q&A

This work is licensed under CC BY-NC-SA 4.0. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/4.0/

innova