Patrocinen

andornet · Deloitte. · OptimumTIC Gestión integral de la ciberseguridad · S21sec · auren · ÍTACA advanced analytics

ISACA Barcelona Chapter

"SSI - La capa d'identitat que li faltava al món digital?"

Ponent

Santi Casas

CEO a Validated ID

Barcelona 15 de desembre 2020

Suport Institucional

informàTICa · Col·legi Oficial Enginyeria Informàtica Illes Balears · iapp · isms forum spain · atl · UAB Universitat Autònoma de Barcelona · telecos.cat · economistas · NcN · Col·legi de Censors Jurats de Comptes de Catalunya = EL CØL·LEGI · AQPE · Project Management Institute Barcelona, Spain

Validated ID

Always be yourself

ISACA
Barcelona Chapter

SSI: Self-Sovereign Identities

¿La capa de identidad que le faltaba al mundo digital?

Santi Casas
@santicasas

Diciembre 2020

"On the Internet, nobody knows you're a dog."

1993

Peter Steiner

THE NEW YORKER

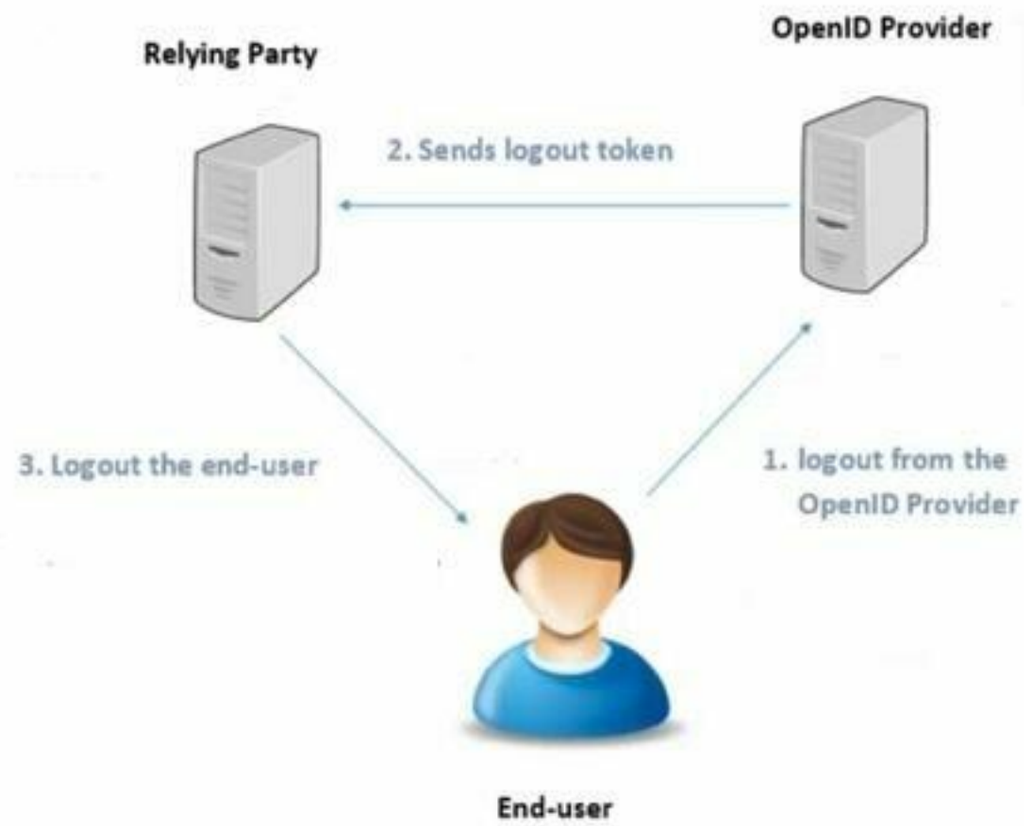
Validated ID

Kim Cameron

2005

OpenID - OAuth

2006



Validated ID

kuppingercole ANALYSTS

GDPR

GDPR – Six Key Principles

- **Personally Identifiable Data** must be processed **fairly** and **lawfully**
- For **specified, explicit** and **legitimate purposes**
- Adequate, **relevant** and **minimum necessary.**
- **Accurate** and **kept up to date**
- Kept no **longer than is necessary**
- **Controller** is **responsible** and **liable** to **ensure and demonstrate compliance**

© KuppingerCole 10/18/2017

2016

Christopher Allen

2016

CURRENT MODEL OF IDENTITY

SELF-SOVEREIGN IDENTITY

Also known as: DECENTRALIZED IDENTITY

Validated ID

SSI - Self-Sovereign Identity:

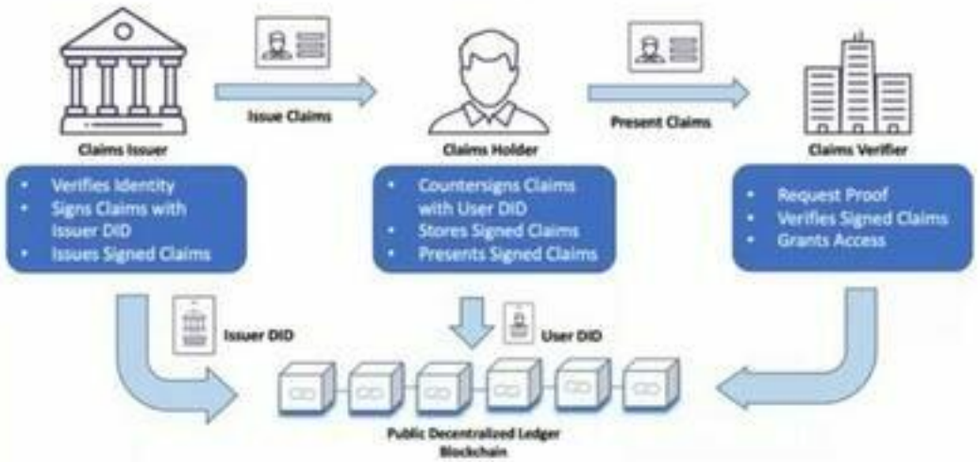
The missing trustful and universal identity layer for the digital world

- User-centric. Authentic user control.
- Based on decentralized identity data issued by third parties:
  - Identity
  - Education / Career
  - Health
  - Financial

- Blockchain/DLT used to avoid a central authority.
- Standardized to be universal by W3C, DIF, ISO ...
- Controlled by the user through a wallet app in their smartphone.
- Better model for GDPR compliance.

STAKEHOLDERS

W3C
sovrin identity for all
DIF
Microsoft
INATBA
European Commission
IBM
HYPERLEDGER

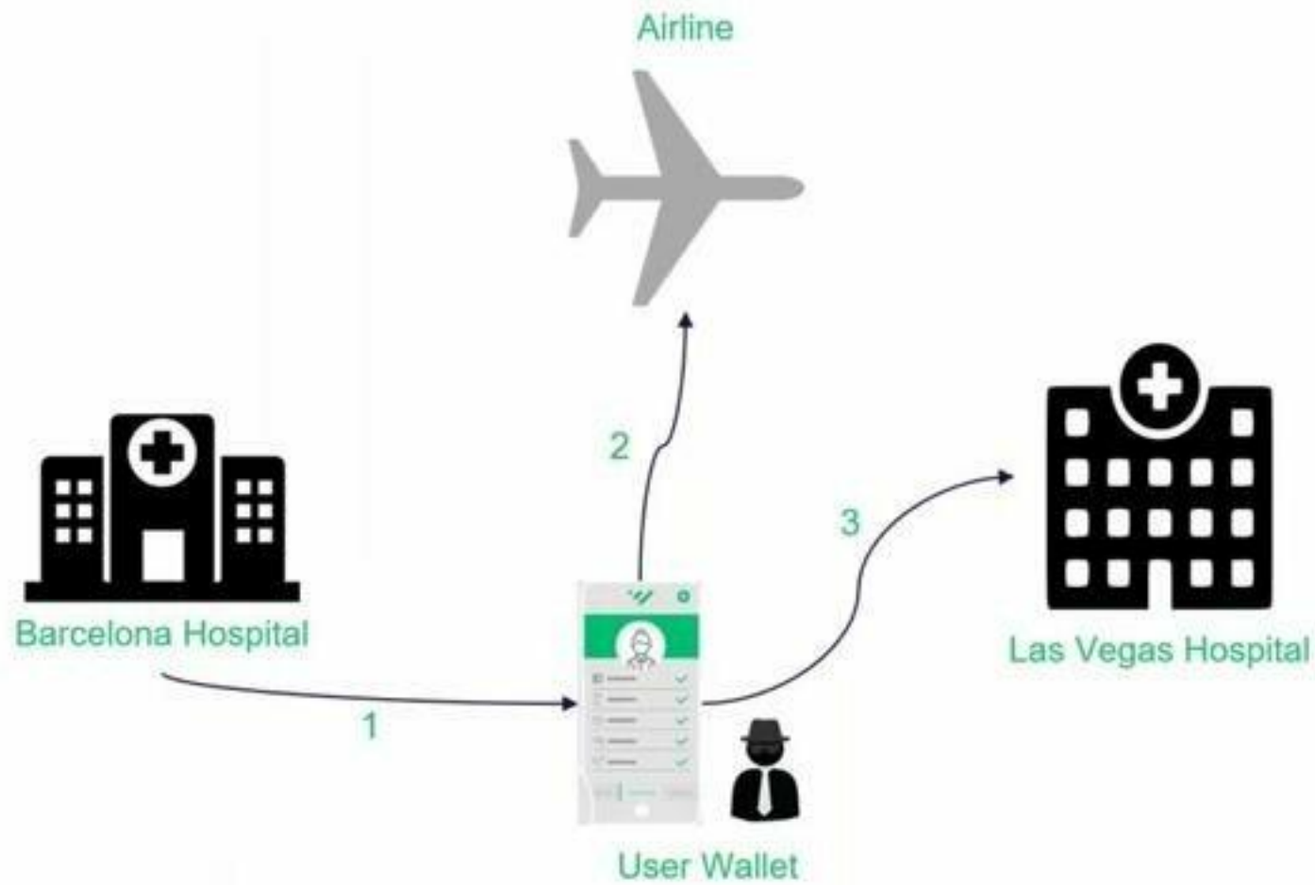


SSI traction is boosting the SSI universal model the same way that email boosted an international standard that is real today

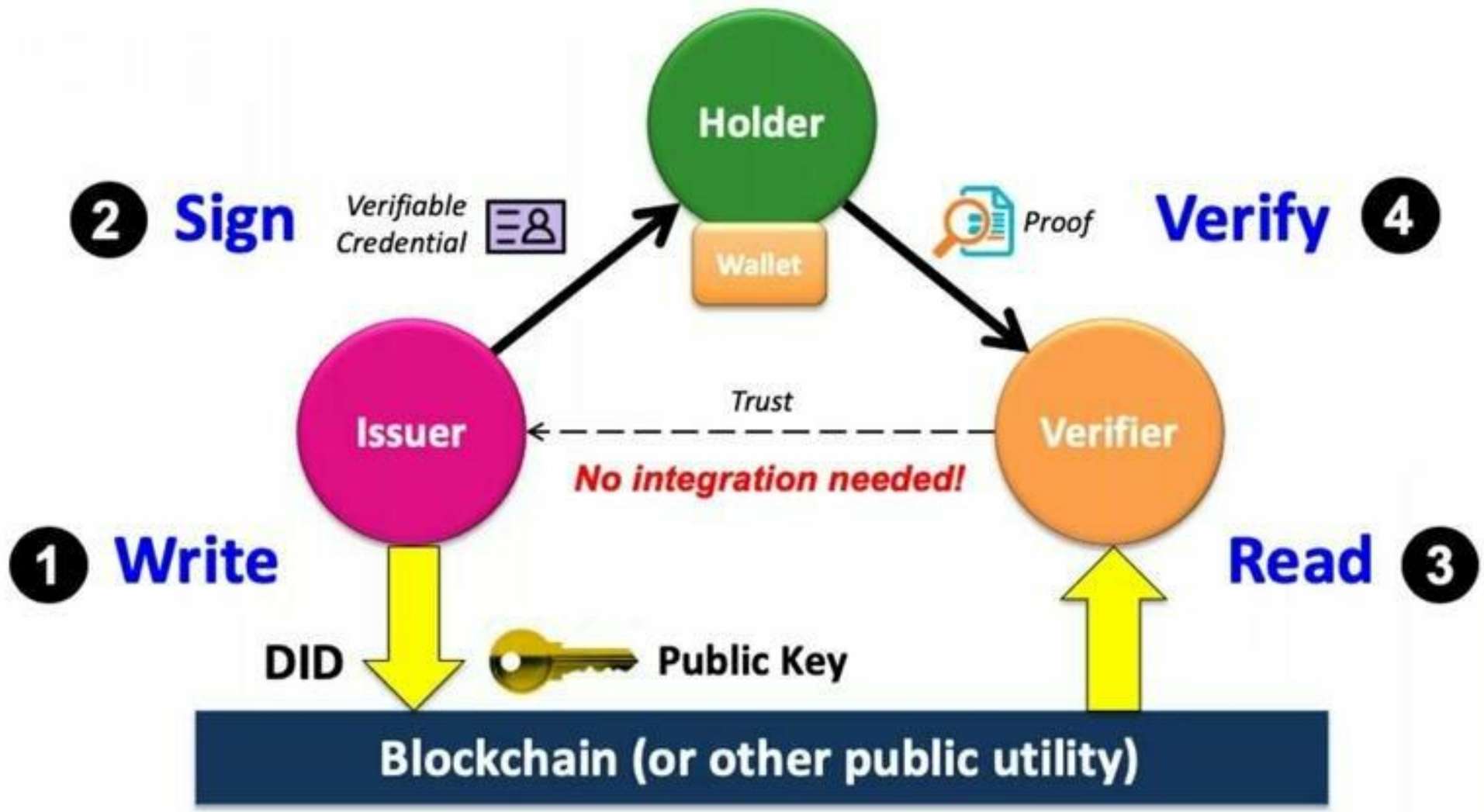
SSI - Self-Sovereign Identity:

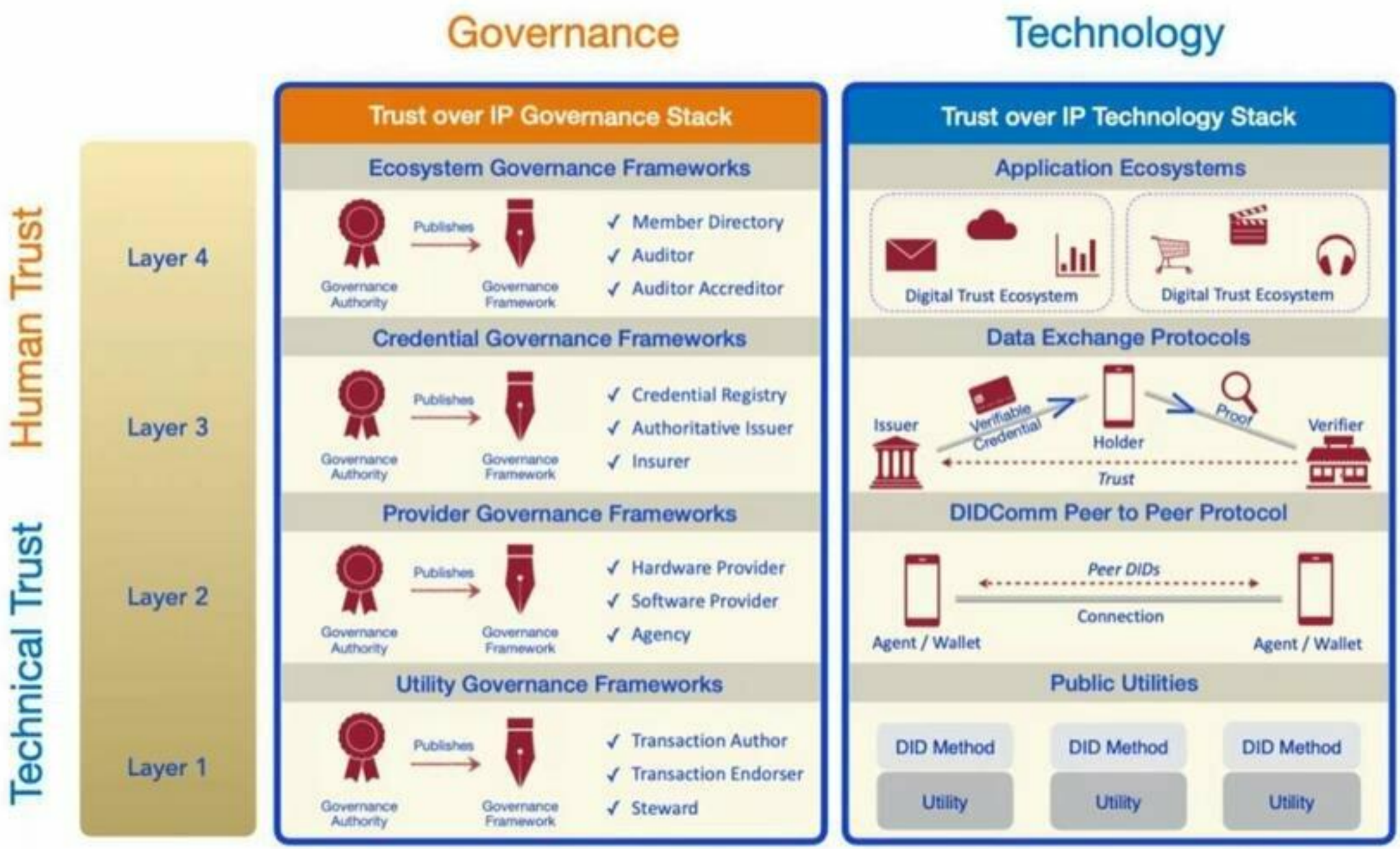
Healthcare example

1. **Barcelona Hospital** issues **health VCs** (verifiable credentials) about the users based on their **EHR** (electronic health records), including COVID related credentials.
2. To be allowed **to travel to Las Vegas**, the users **must present their COVID credentials** to verify the government and airline requirements.
3. In **Las Vegas**, the user feels sick and go to a hospital. They **can present whatever health credentials the hospital needs** to make a good diagnosis and get a properly prescribed treatment.



Validated ID is member of the **CCI** (COVID Credentials Initiative)


Holder
Wallet
2 Sign
Verifiable Credential
Proof
Verify 4
Issuer
Trust
Verifier
No integration needed!
1 Write
Read 3
DID
Public Key
Blockchain (or other public utility)


Governance
Technology
Human Trust
Technical Trust
Layer 4
Layer 3
Layer 2
Layer 1
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
Trust over IP Technology Stack
Application Ecosystems
Digital Trust Ecosystem
Digital Trust Ecosystem
Data Exchange Protocols
Issuer
Verifiable Credential
Holder
Proof
Verifier
Trust
DIDComm Peer to Peer Protocol
Peer DIDs
Connection
Agent / Wallet
Agent / Wallet
Public Utilities
DID Method
DID Method
DID Method
Utility
Utility
Utility

TRUST Over IP FOUNDATION

Considerations, Requirements

Feedback Cycle

Capabilities, Components

W3C

IETF

OASIS
Open standards. Open source.

HYPERLEDGER

OpenID

DIF

Validated ID

Decentralised Identity: What's at Stake?

Authors

Kai Wagner (Jolocom)
Xavier Vila Pueyo (Validated ID)
Nathan Vandy (Blockchain Helix)
Daniel Bachenheimer (Accenture)
Dominik Beron (Danube Tech)

Contributors and Reviewers

Michelle Leech (Tendermint)
Catarina Veloso (Trust Fractal)
Oliver Naegele (Blockchain Helix)
Wim Stalmans (Infrachain)
Edilson Osorio Junior (OriginalMy)
Hervé Bonazzi (Archipels)
Joachim Lohkamp (Bundesverband Blockchain)
Gerrit Steinfort (IBM)
Emilyan Enev (ReCheck)

Gustavo Prieto (University of Turin) — INATBA AAB
Roberto Garcia (Universitat de Lleida) — INATBA AAB

1

https://inatba.org/wp-content/uploads/2020/11/2020-11-INATBA-Decentralised-Identity-001.pdf

W3C https://www.w3.org/TR/did-core/

DID

Your address

DID Syntax (W3C)

did:sov:3k9dg356wdcj5gf2k9bw8kfg7a

Method-Specific Identifier

Generated as defined by the DID method specification

Method

Scheme

CC BY SA

Best of all: there is
no central registration authority—
every DID is registered directly by
you on a public or private
blockchain or distributed network

CC BY SA

In summary, a DID is…

CC BY SA

In summary, a DID is…

1. A permanent (persistent) identifier
   - It never needs to change
2. A resolvable identifier
   - You can look it up to get metadata
3. A cryptographically-verifiable identifier
   - You can prove ownership using cryptography
4. A decentralized identifier
   - No centralized registration authority is required

CC BY SA

A DID Method spec defines…

1. The syntax of the method-specific identifier
2. Any method-specific elements of a DID document
3. The CRUD (Create, Read, Update, Delete) operations on DIDs and DID documents for the target system

CC BY SA

Some DID Method Specs

Method	DID prefix
Sovrin	did:sov:
Bitcoin Reference	did:btcr:
Ethereum uPort	did:uport:
Blockstack	did:stack:
Veres One	did:v1:
IPFS	did:ipld:

The standard elements of a DID doc

1. **DID** (for self-description)
2. **Set of public keys** (for verification)
3. **Set of auth methods** (for authentication)
4. **Set of service endpoints** (for interaction)
5. **Timestamp** (for audit history)
6. **Signature** (for integrity)

DID Specification Links

W3C Version	https://w3c-ccg.github.io/did-spec/
Issues List	https://github.com/w3c-ccg/did-spec/issues/
Discussion Forums	https://www.w3.org/community/credentials/ http://forum.sovrin.org/c/technical/did

CC BY SA

https://www.w3.org/TR/vc-data-model/

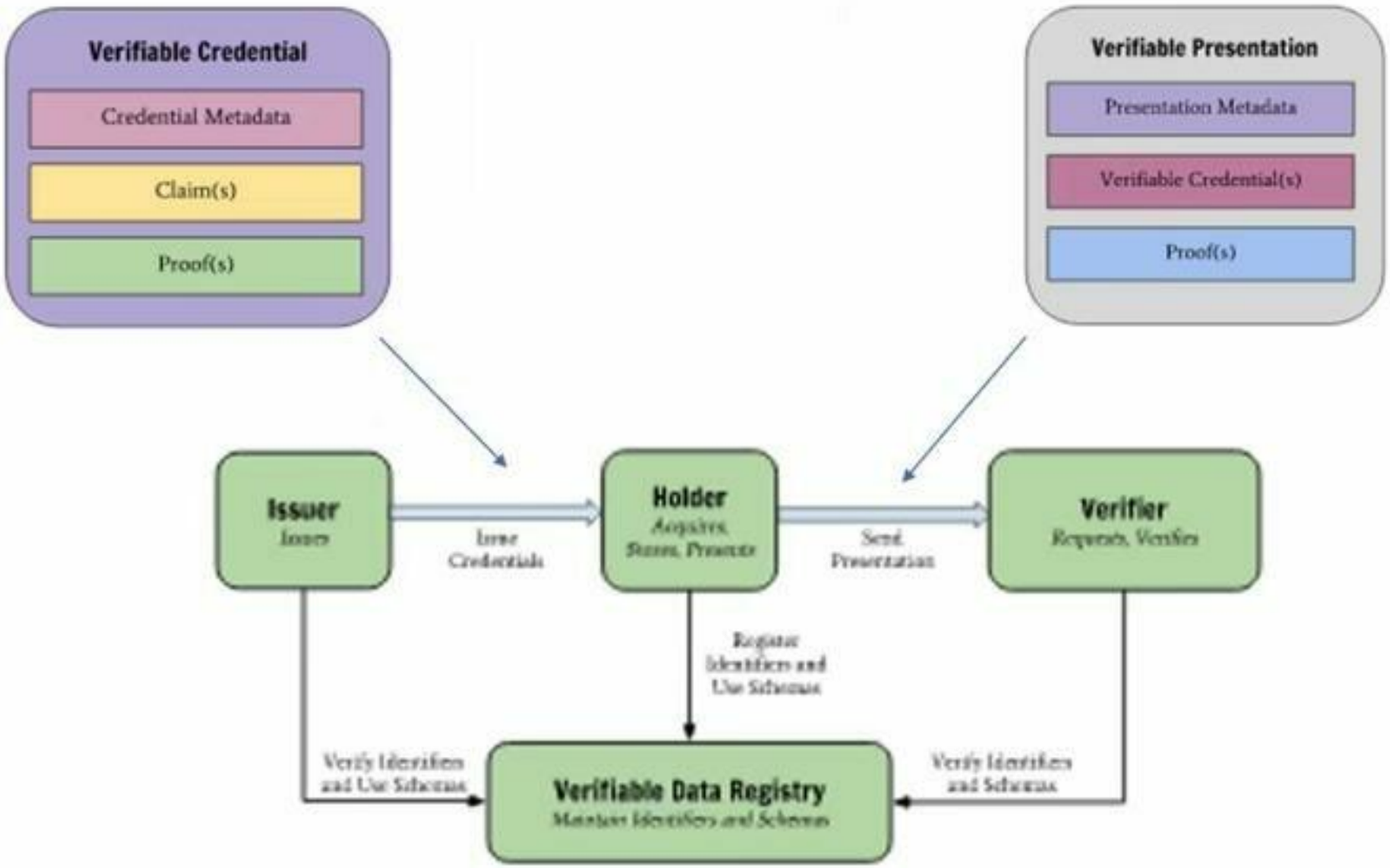
Verifiable Credentials

About you

Verifiable Credentials are:

- All digital, under the true owner's control
- High scalability
- Much harder to fake
- Near impossible to impersonate true owner
- Eliminates need for any treasure troves of data
- Enables minimum disclosure
- Enables Zero-Knowledge Proofs
- Data alone is useless

CC BY SA



https://www.w3.org/TR/vc-data-model/

Zero-knowledge proof (ZKP)

Minimum disclosure

Zero-Knowledge Proofs

If your personal data is never collected, it cannot be stolen.

– **Maria Dubovitskaya** Cryptographer, Research Staff Member, IBM Zurich Research Laboratory, Ph.D. in cryptography and privacy from ETH Zurich

SSIMeetup.org

ZKP Identity-Related Landscape

Identity Verification, Authentication

MIRACL, VelixID, STRĀTUMN, val:ID, Microsoft UProve, everynym, sovrin, clearme, sedicii, lifeID, IBM, nuggets, KRIPTAN, QEDit, PEER MOUNTAIN, NuID, civic

Players

uport
ethereum
did:uport:XXX

ERC-725 ALLIANCE
ethereum
did:erc725:XXX

sovrin
identity for all
HYPERLEDGER INDY
HYPERLEDGER ARIES
did:sovrin:XXX

VIDchain
Always be yourself
Ledger Agnostic
did:xxx:XXX

VIDchain ecosystem

SSI Momentum

Gartner

"**Decentralized identity** is making a debut in 2021, and will disrupt traditional methods of access for many providers, as it will be used for **25%** of all bring your own identity (BYOI) logins **by 2023**"

June **2020**: **SSI** successfully trialed for **KYC in UK** regulatory sandbox

FCA FINANCIAL CONDUCT AUTHORITY

Forbes randstad SAP cornerstone

New Network Will Build An **"Internet of Careers"**: Using Blockchain To Control Your Own Career Credentials

The ACE is a collaboration to create the world's first **truly decentralized, multi-sector digital credential** ecosystem

ESSIF

"The **European Council** calls for the development of an **EU-wide framework** for secure public electronic identification (**e-ID**), including interoperable **digital signatures**, to provide **people with control over their online identity and data** as well as to enable access to public, private and cross-border digital services. It invites the Commission to come forward with a proposal for a **"European Digital Identification' initiative by mid-2021**."

Ursula von der Leyer

State of the Union 2020

This includes **control over our personal data** which still have far too rarely today. Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, **we have no idea what happens to our data** in reality. That is why the **Commission will soon propose a secure European e-identity.**

* Decentralized identity and SSI are synonymous.

EBSI: European Blockchain Service Infrastructure

Iniciativa conjunta de la Comisión Europea y del European Blockchain Partnership

Ofrecer servicios sobre Blockchain para los ciudadanos de los Estados Miembros y, en un futuro, la empresa privada

Publicada V1 para los Estados Miembros el 12 de febrero de 2020, release pública finales de marzo 2020

Apertura plataforma finales 2020

4 Casos de Uso:

Los principios de EBSI:

- **PÚBLICA PERMISIONADA**: la identidad de los nodos participantes será conocida
- **DESCENTRALIZADA**: cada estado miembro se hará cargo de su propios nodos
- **ESCALABLE**: soporte para alto rendimiento y alto número de nodos
- **ABIERTA**: en código abierto y con licencia de uso libre
- **SOSTENIBLE**: eficiente en términos de energía
- **INTEROPERABLE**: basado en estándares existentes y corriendo diferentes ledgers (HL Besu y HL Fabric)

ESSIF: European Self-Sovereign Identity Framework

Servicio de SSI para los ciudadanos de los estados miembros

Montado sobre blockchain HL Besu con la generación de un identificador único (DID) para cada par de claves: did:ebsi:0xabcdefgh001

Permite la generación de DIDs y el intercambio de credenciales verificables: verifiable ID (credencial de identidad firmada con claves eIDAS) y otros como diplomas.

Se ofrece un wallet de identidad para gestionar el DID y las VCs

Implementado el caso de uso de “El viaje de Eva” para emitir su Verifiable ID, Bachelor Diploma y Master Diploma.

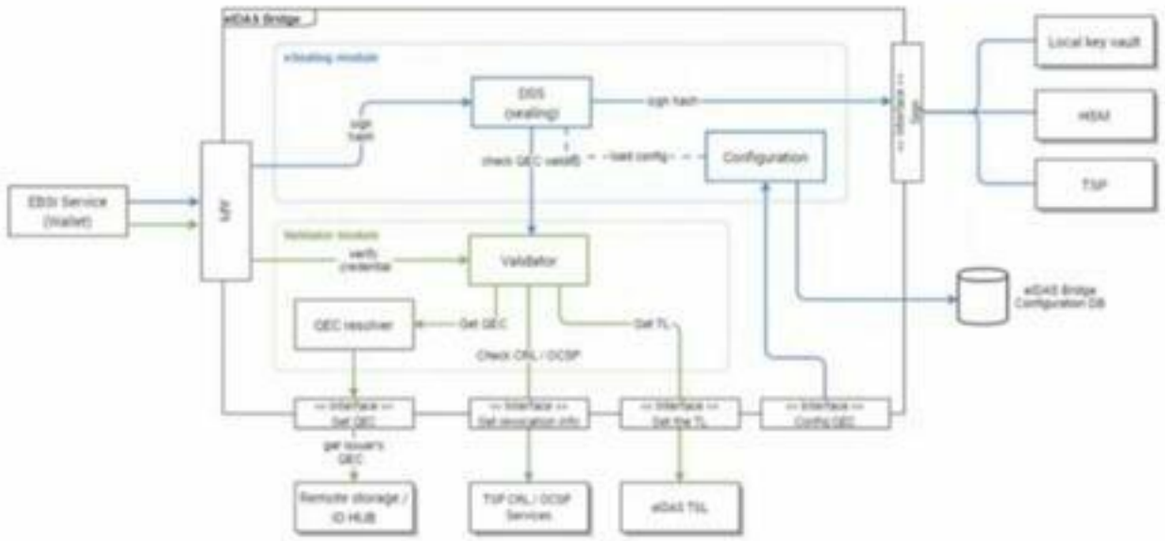
eIDAS bridge: conectando SSI con eIDAS

eIDAS es una regulación europea que establece un marco de confianza sobre las firmas electrónicas (Electronic IDentification for Authentication and Trust Services) permitiendo transacciones seguras transfronterizas para establecer el Mercado Único Digital (Digital Single Market)

eIDAS-bridge es un componente dentro del proyecto ESSIF que enlaza el marco de confianza eIDAS dentro de la plataforma de SSI de EBSI

Vinculando las Verifiable Credentials con las reglas de eIDAS eID (identificación) y eiDAS eSeals (sello)

Una Credencial Verificable firmada con claves y certifucadis eIDAS adoptaría el nivel de confianza (LoA) equivalente.



Validated ID

Santi Casas
@santicasas

Thank you!