

Always be yourself

19 Febrero 2020



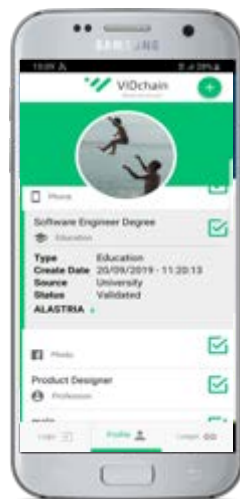
Los nuevos modelos europeos de identidad digital en Blockchain

Santi Casas – CEO
Validated ID

¿Qué hacemos?



Servicio de firma electronica multicanal siguiendo el modelo TSP



Solución de identidad soberana (SSI - self-sovereign identity) para onboarding y KYC



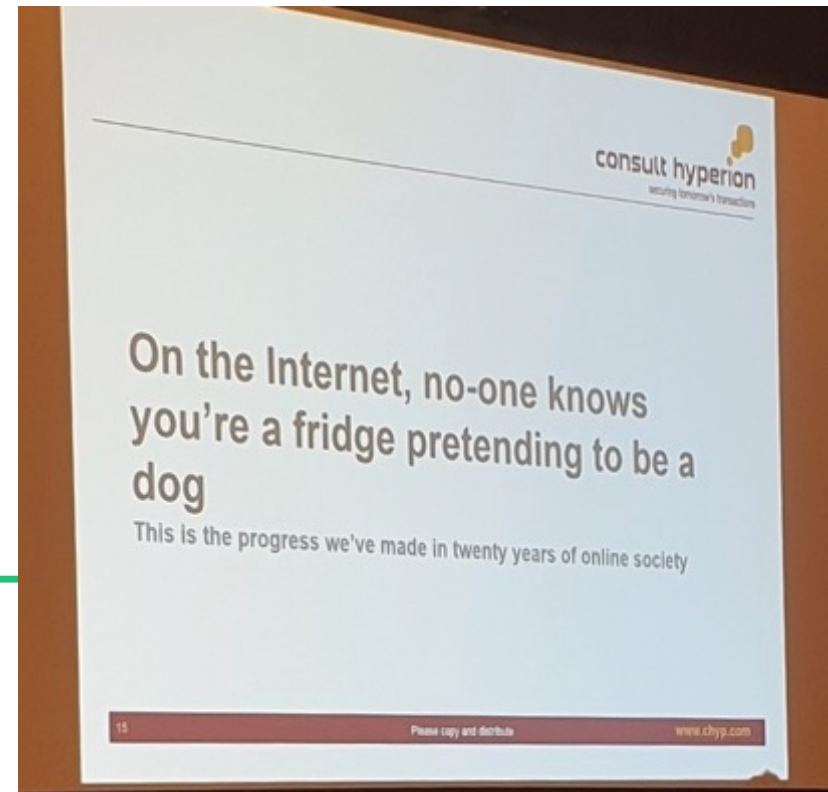
1993

Peter Steiner
THE
NEW YORKER

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

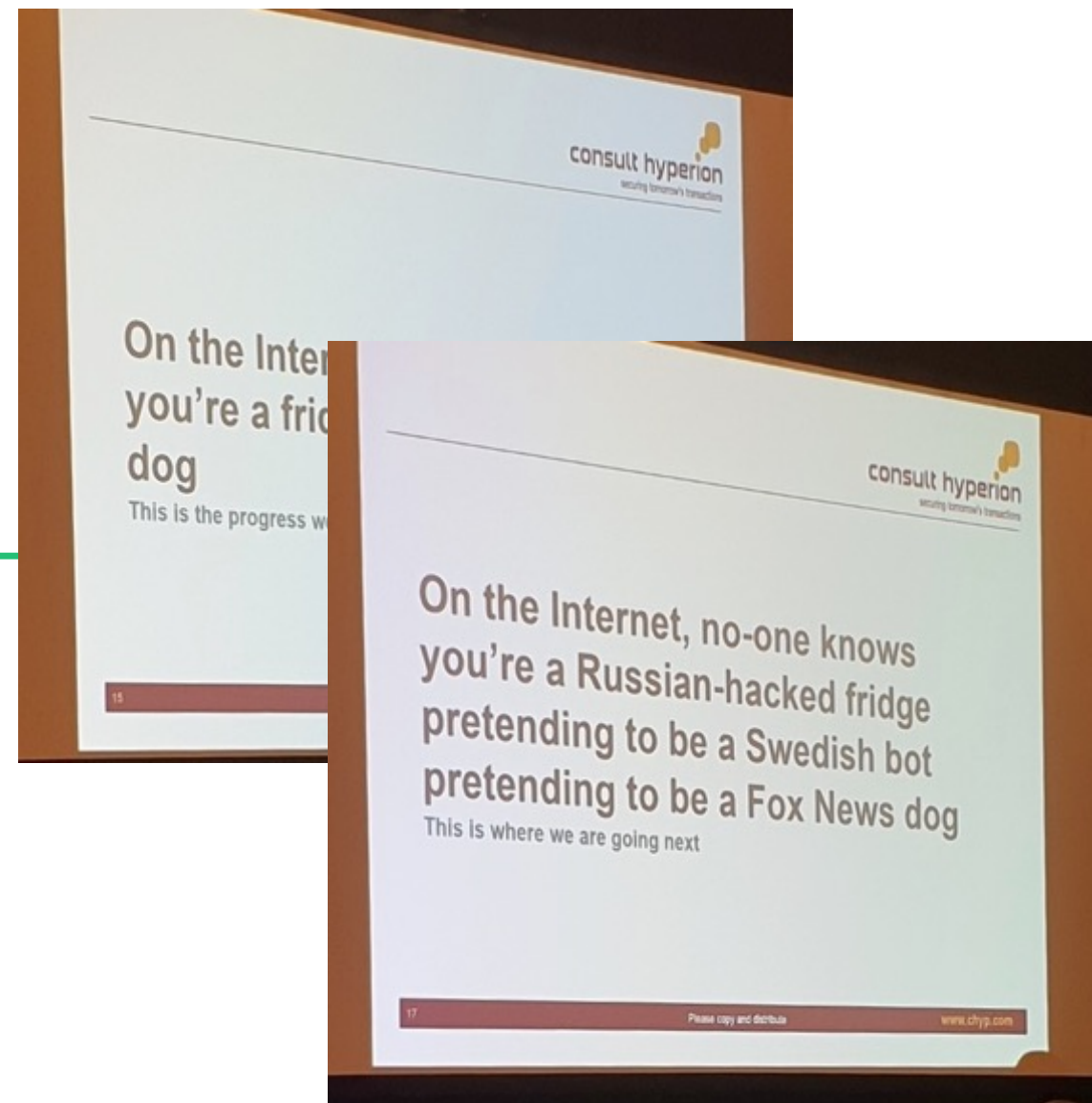


"On the Internet, nobody knows you're a dog."





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



EU - PKI



1999

Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica.

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica

Kim Cameron



2005

Kim Cameron's

Laws of Identity

1 User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

3 Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

2 Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

4 Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

7 Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

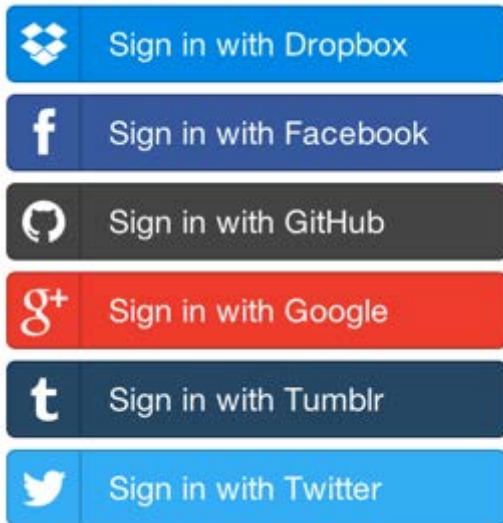
6 Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

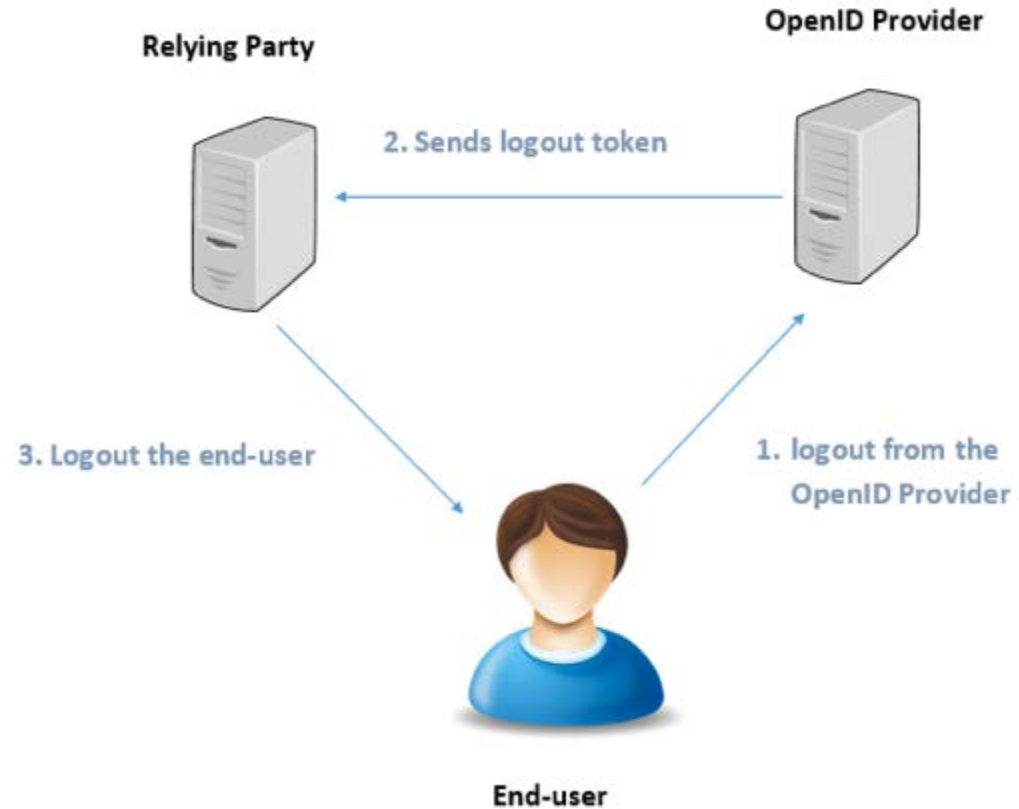


Photo: Alan

OpenID - Oauth



2006



eIDAS



2014



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**

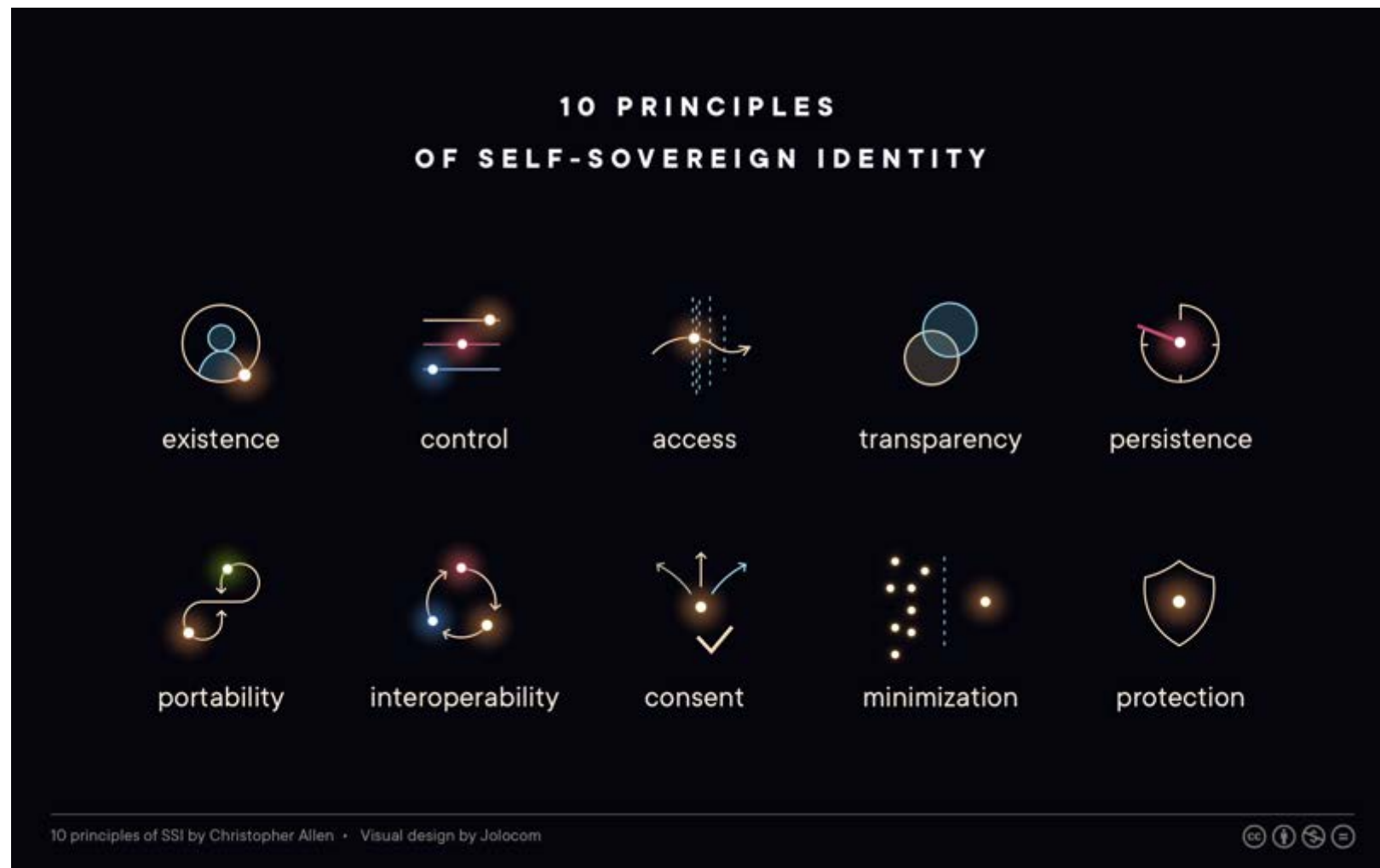
Controller is responsible and liable to ensure and demonstrate compliance

2016

Christopher Allen



2016



A NEW PARADYGM: SELF-SOVEREIGN IDENTITIES



CURRENT IDENTITY MODEL



SELF-SOVEREIGN IDENTITY MODEL

SSI

Me, Myself, & I

Self-sovereign digital identity

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





A GLOBAL IDENTITY APPROACH...

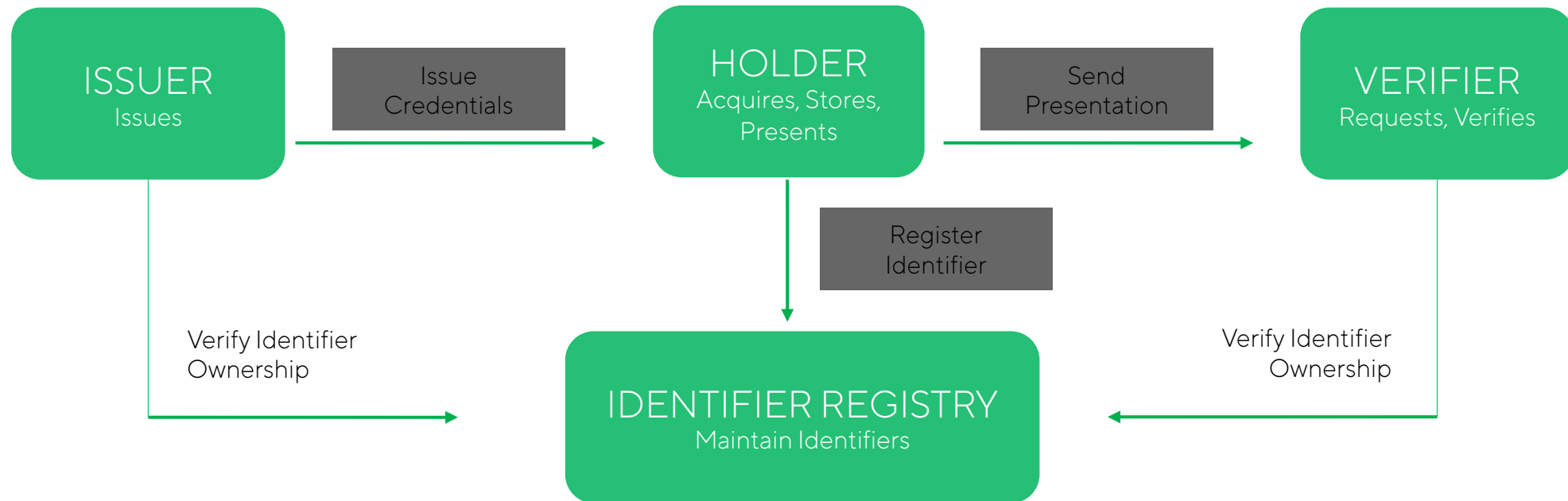


AND ANOTHER GLOBAL IDENTITY APPROACH...

SSI IS CONTRIBUTING TO EU'S VALUES & PROTECTION OF ITS CITIZENS



International SSI Standardization Forums



Emerging Open Standards

VERIFIABLE CREDENTIALS

DID AUTH

DKMS
(Decentralized Key Management System)

DID
(Decentralized Identifier)

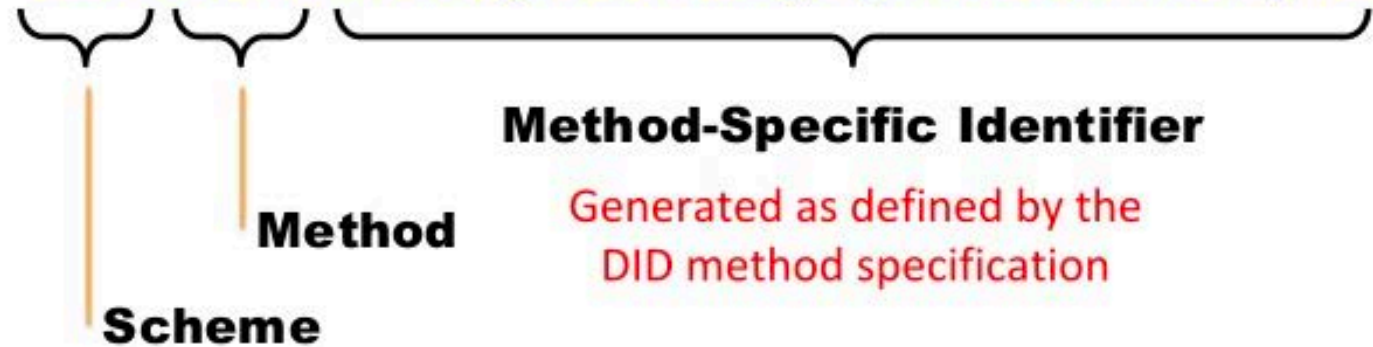


DID

DID Syntax (W3C)

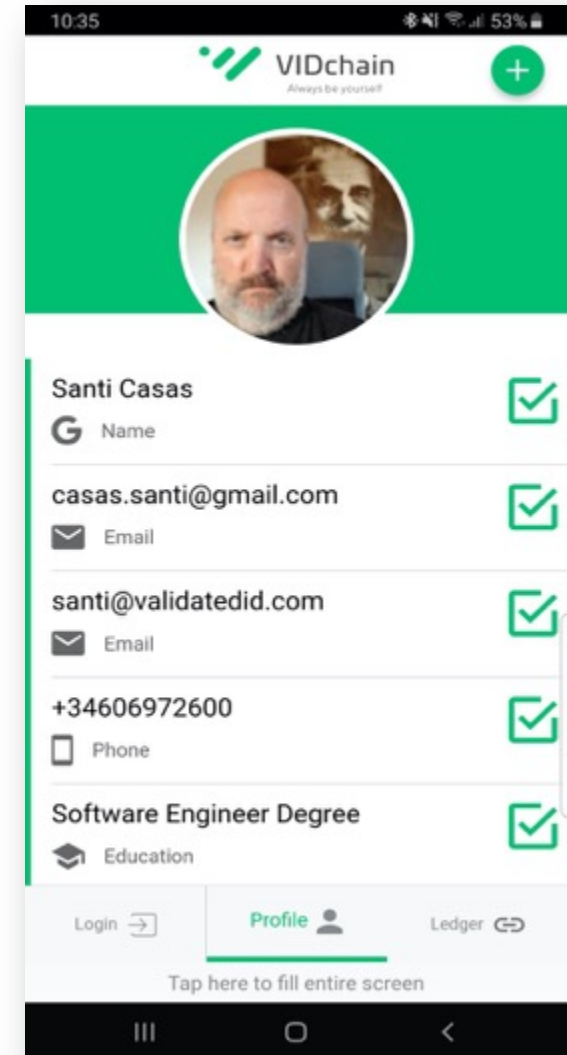
Your address

`did:sov:3k9dg356wdcj5gf2k9bw8kfg7a`



W3C® Verifiable Credentials

About you



Zero-knowledge proof (ZKP)

Minimum disclosure



Graphic: <https://www.youtube.com/watch?v=QDwXt00Xk>

<https://www.youtube.com/watch?v=QDwXt00Xk>
https://www.ibm.com/identity_mixer/
https://www.ibm.com/identity_mixer/ if you want to take back control of your personal data TED Talk

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



ZKP Identity-Related Landscape

Identity Verification, Authentication



Players



did:uport:XXX



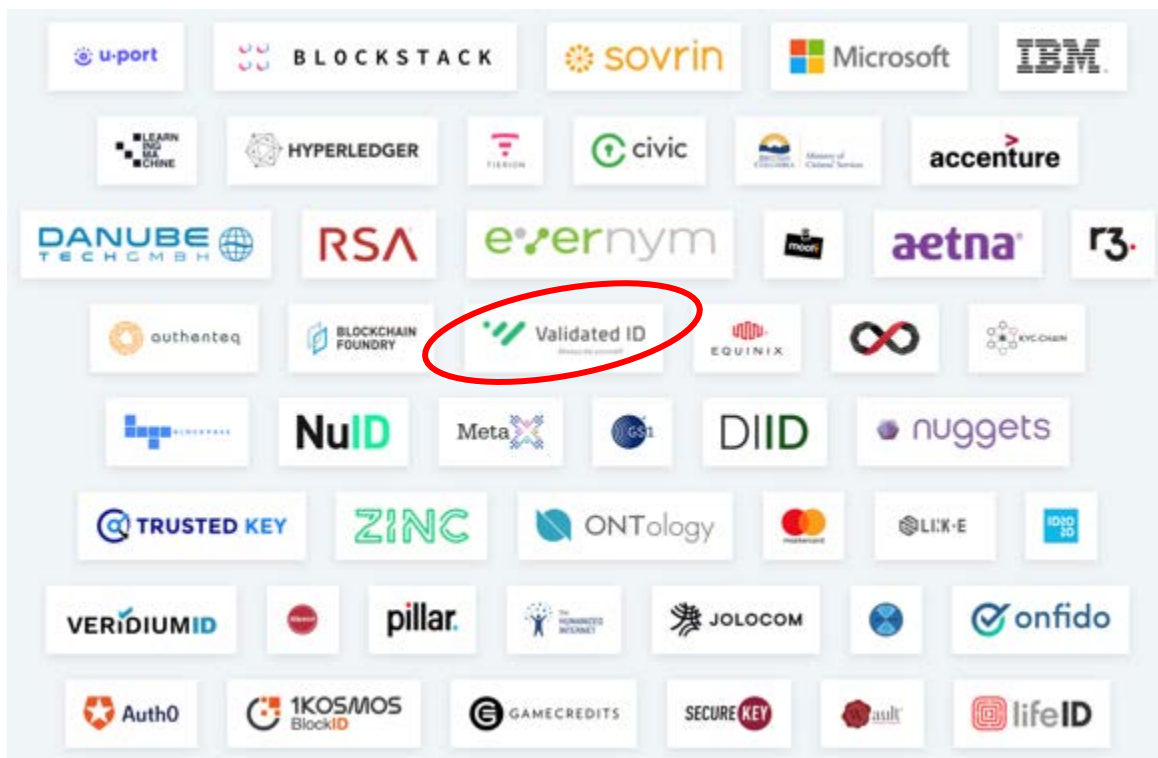
did:erc725:XXX



did:sovrin:XXX

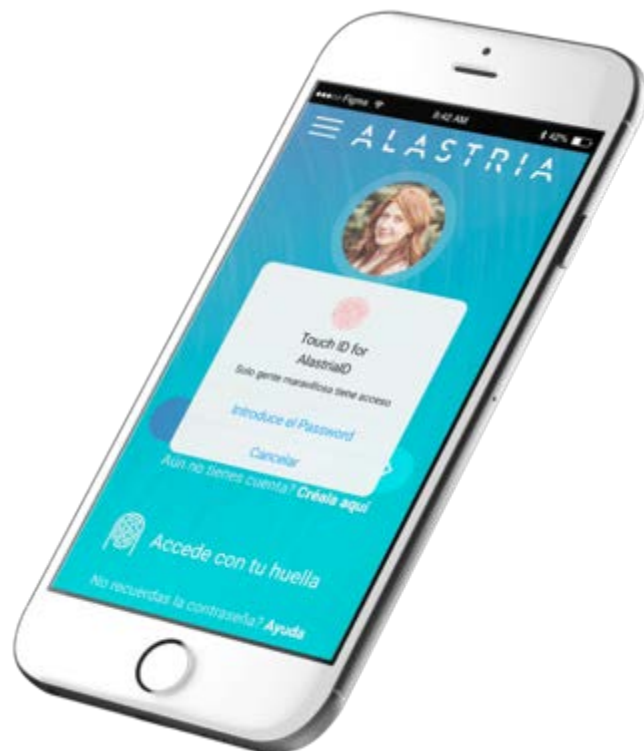


did:xxx:XXX



<https://identity.foundation/>





ALASTRIA ID

Un modelo de identidad digital de **fuerza legal** para una **Blockchain Permissionada**.

ALASTRIA ID tiene como objeto hacer de este nuevo contexto digital un espacio en el que los **miembros del consorcio** puedan desplegar sus productos y servicios de forma que las transacciones de esos productos y servicios sobre la "Red ALASTRIA", puedan tener **validez legal**.



ALASTRIA ID: ¿CÓMO FUNCIONA?



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)



Notarisation of Documents for Auditing Purposes



Certification of Diplomas



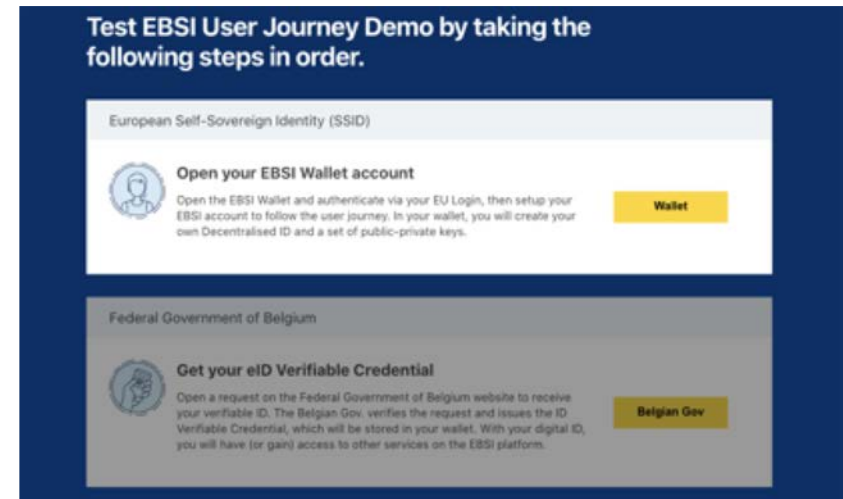
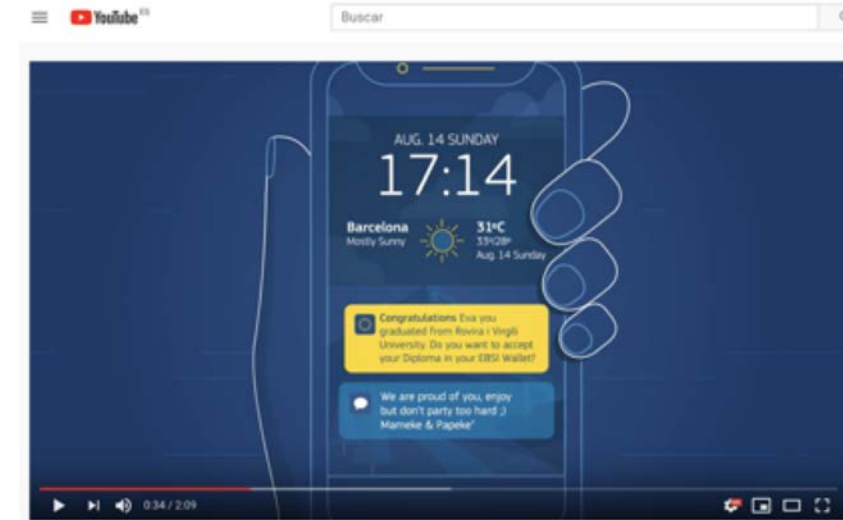
EU Self-Sovereign Identity Framework



Trusted Data Sharing

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:ebis:0xabcdefg001
- 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.

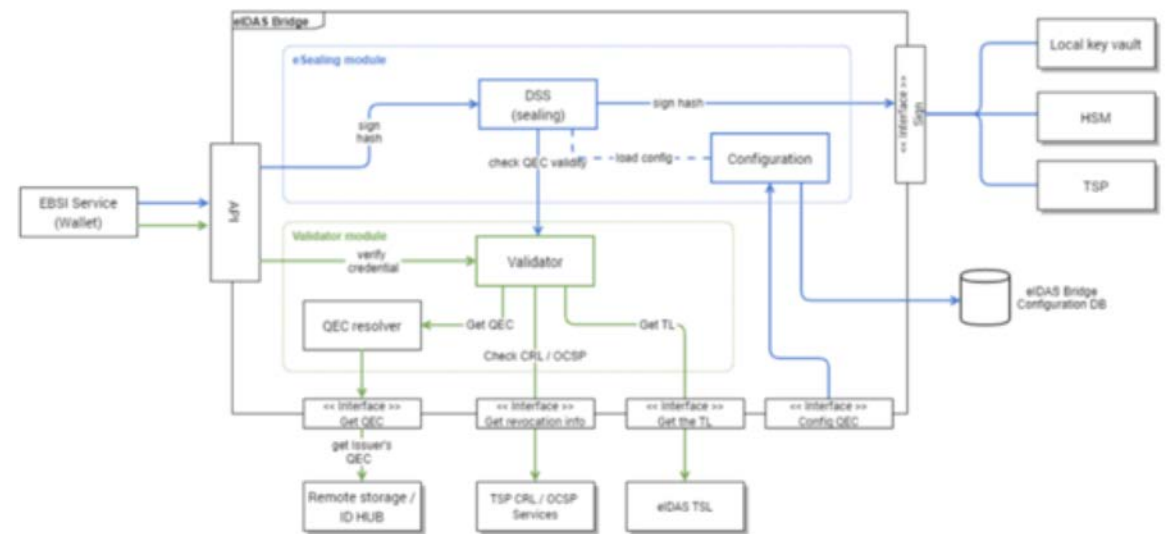


Eva's User Journey



eIDAS bridge: conectando SSI con eIDAS

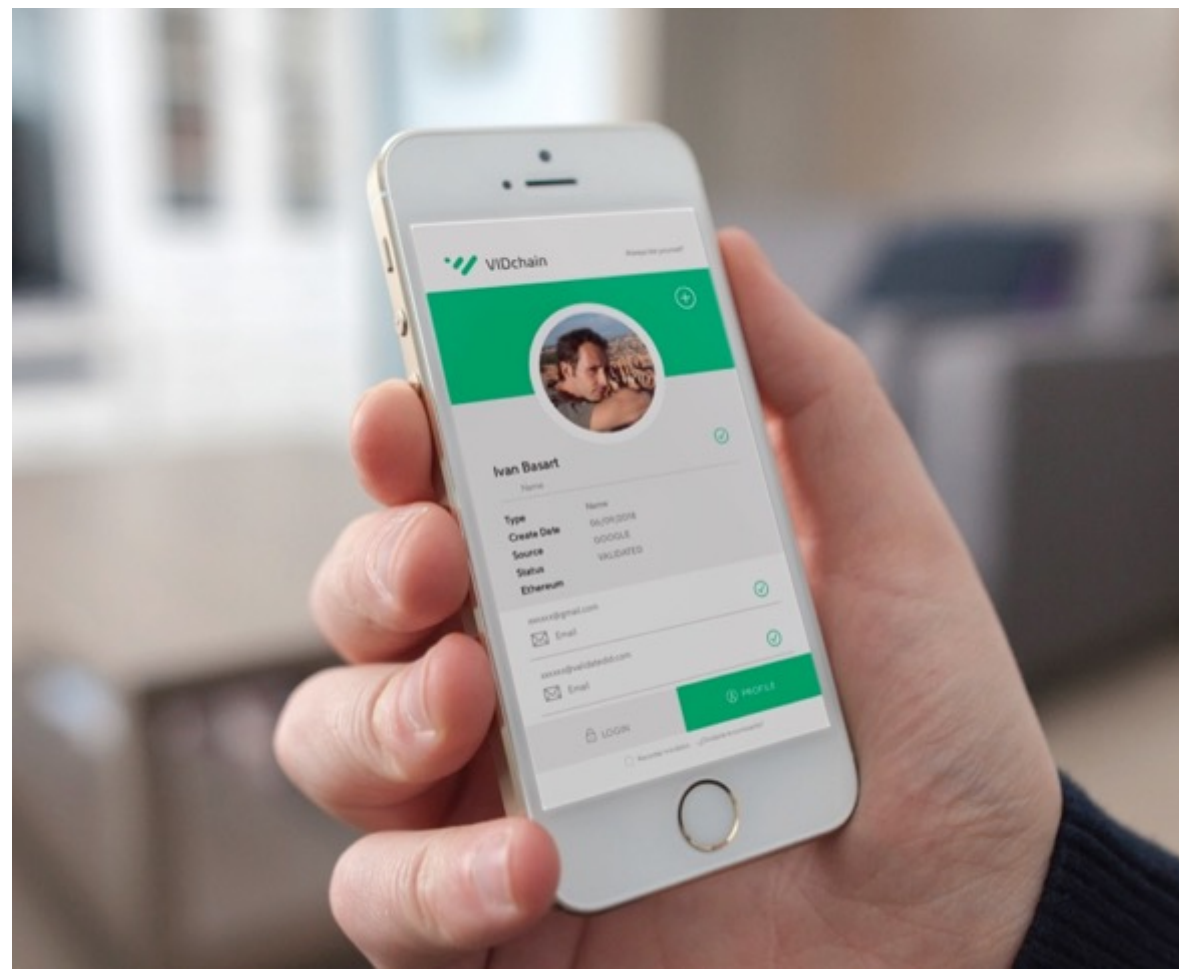
- eIDAS es una regulación europea que establece un marco de confianza sobre las firmas electrónicas (Electronic IDentification for Authentication and Trust Services) permitiendo transacciones seguras transfronterizas para establecer el Mercado Único Digital (Digital Single Market)
- eIDAS-bridge es un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

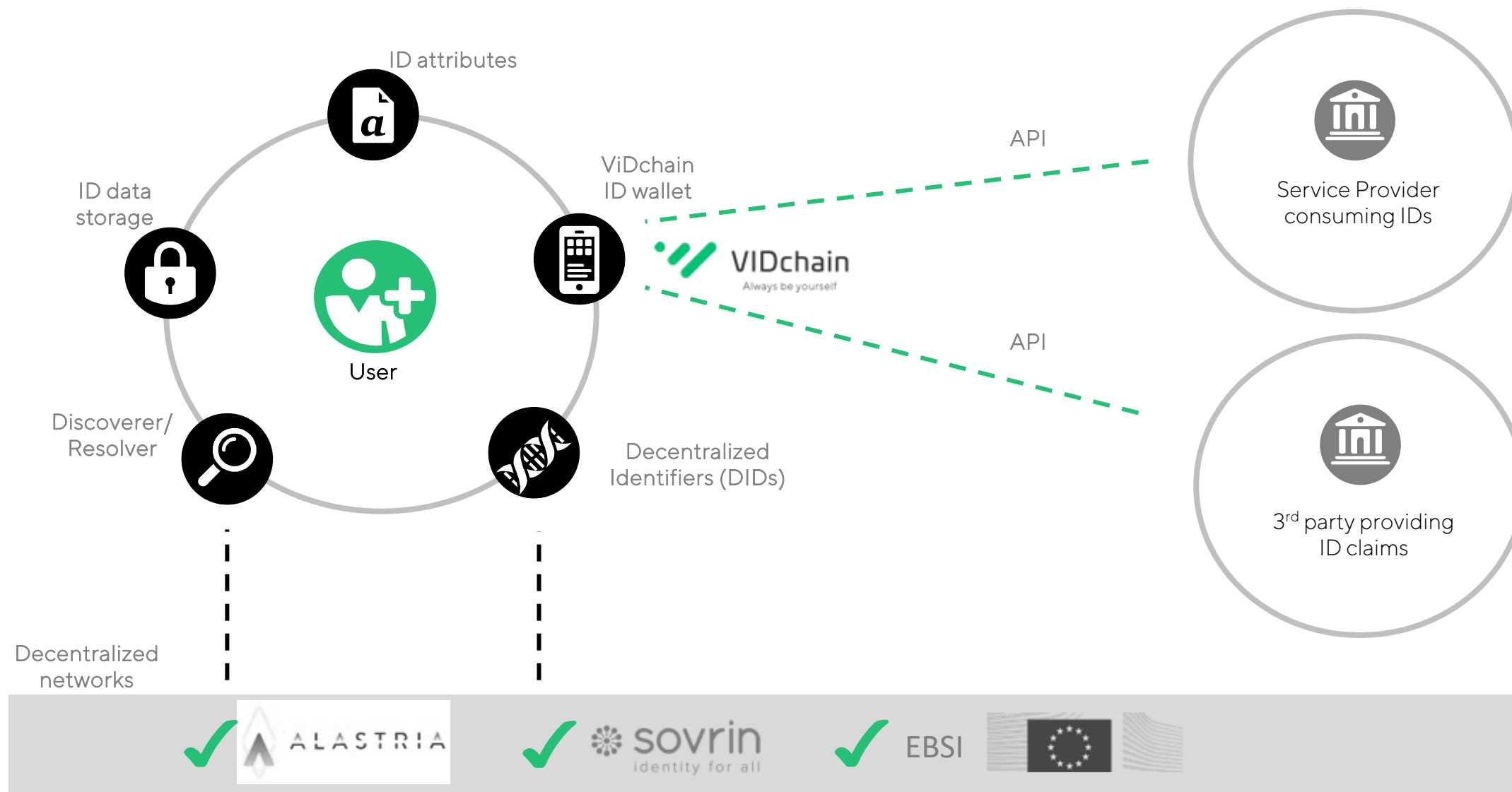




With ViDchain we offer a decentralized Self-Sovereign Identity service based on Blockchain for digital identity verification processes.

This solution ensures GDPR compliance and improves procedures such as customer onboarding, AML, and KYC.





1. Validated ID is the first Sovrin Steward in Spain
2. Validated ID is developing the ESSIF reference wallet in EBSI project.



Gracias

www.validatedid.com
info@validatedid.com

