

eldas and SSI interactions

Fabrizio Leoni Head of Product Innovation



My Data 2018, Helsinki August 31st 2018

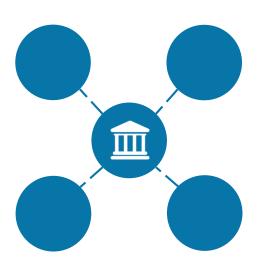
Evolution of trust

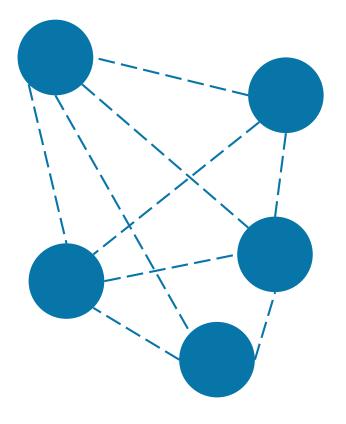
LOCAL

INSTITUTIONAL

DISTRIBUTED

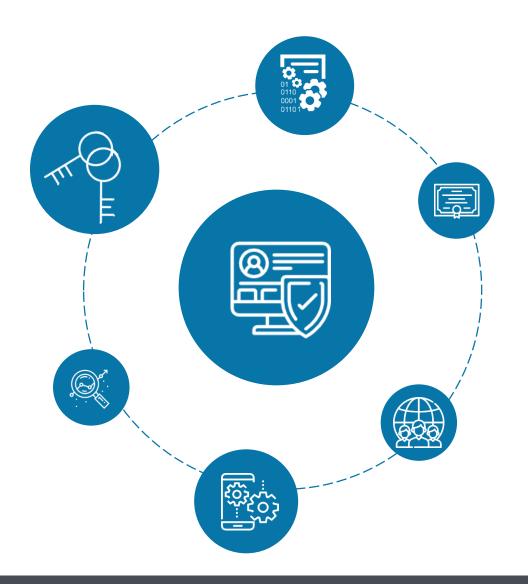






Source: Rachel Botsman, «Who can you trust?», Penguin, 2017.

Trust de facto vs trust de iure





elDAS trust framework





PAPERLESS





UNIQUE DIGITAL MARKET

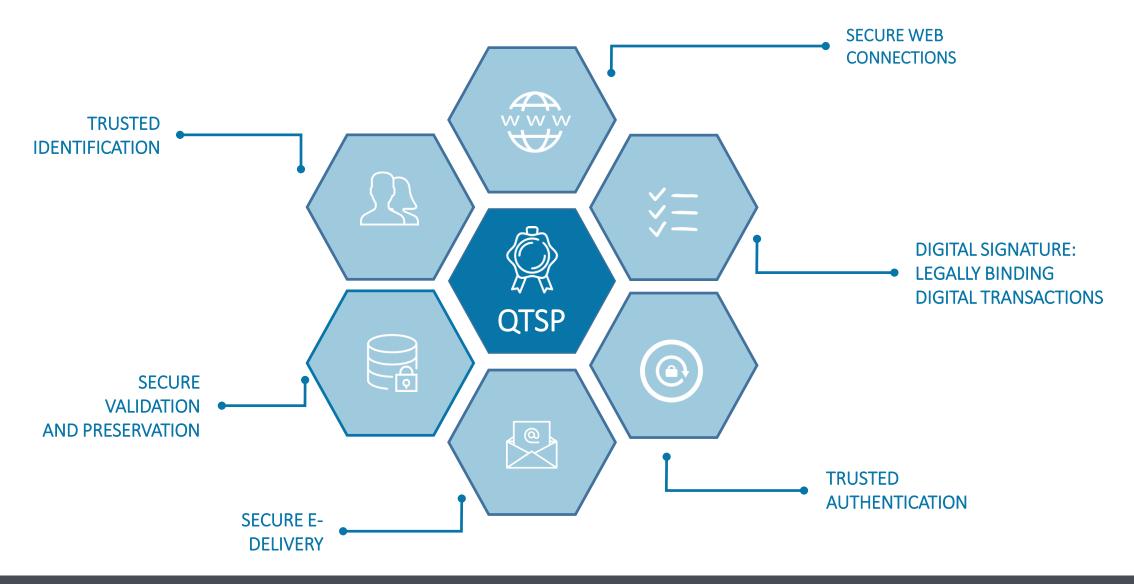
The new European regulation (Regulation 910/2014 electronic Identification Authentication and Signature - eIDAS) is today fully in force: the scope of the regulation is to create a unique digital single market and allow the digital citizens to obtain a whole digital experience. A common and legally binding law is essential for the grow of the digital business. The regulation includes all the aspect of digital life, in order to enable the trusted access to online – pubblic and private – services.



DIGITAL BY DEFAULT

The today regulation solve the problem of the **DIGITAL FIRST**: the idea that the Pubblic Administration first and the private services later shall adopt a fully digital approach in order to reduce cost and grants a trusted approach to online services. Today we have a coherent legal framework which is made mandatory both from the European Authority and the local Authorities: the Qualified Trust Service Provider (QTSP) enables the trust in the market.

TSP Role in the eIDAS trust framework

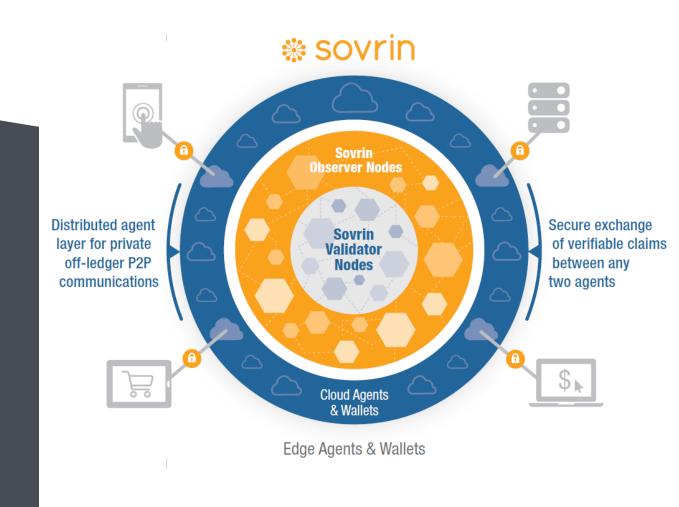


SOVRIN

The Sovrin Network has been designed to establish a global public utility for self-sovereign identity

Sovrin implements Privacy by Design on a global scale, including pairwise pseudonymous identifiers, peer-to-peer private agents, and selective disclosure of personal data using zero-knowledge proof cryptography.

The network is open source and designed to establish trust through transparency, diffusion, and neutrality.





SOVRIN SSI key concepts

TRUST ANCHOR

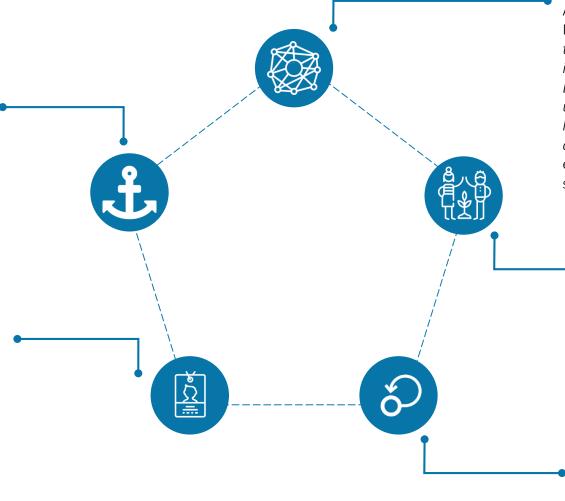
A trust anchor is an identity owner that one or more verifiers consider to be a root of trust for one or more verifiable credentials.

This means the verifiers will trust verifiable credentials issued by that trust anchor.

A trust Hub is a special type of trust anchor whose role is to serve as a root of trust for other trust anchors.

ELECTRONIC IDENTITY (eID)

A set of information that can uniquely identify the owner. The **trust level** required may change according to the purpose of legal accountability required by the single use case. References of the identity may also lay in public and accessible Web resources.



DID

A decentralized identifier as defined by the "DID Data Model and Generic Syntax" specification: DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document contains at least three things: cryptographic material, authentication suites, and service endpoints. DIDs enable interoperable and decentralized the self-sovereign identity.

STEWARD

An organizations which runs a node of the SOVRIN network: it shall meet the Steward Qualifications and agree to the Steward Obligations of the SOVRIN Trust Framework. The qualified organization can run either a **validator** or an **observer** node.

SELF-SOVEREIGN IDENTITY

An identity system that provides digital identities for digital Owners (person, natural or legal, and/or Things): the owner can manage his/her identity without the need of a centralized Authority. The Private key grant the sole control of the identity.

InfoCert role in the SOVRIN network

InfoCert can give an identity to each wallet, in order to grant the compliance with existing identification laws



InfoCert enables the use of advanced authentication mechanism each time a service on the ledger is called in action

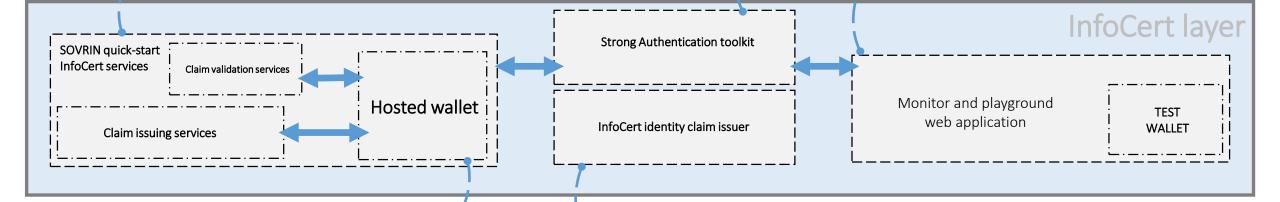
The source of the data shall be certified and checked by a trusted party as InfoCert. Issuing

FOUNDING STEWARD InfoCert runs a Sovrin node and offer integration services to enable the access to the Network for citizens and institutions

InfoCert role as a SSI TSP- if it makes sense...

- Hosted or backup wallet: repository of claims and keys of the customer
- Claim issuing services: service to issue claims toward a customer wallet
- Claim validation services: service to validate claim as received by a customer wallet
- Infrastructure management

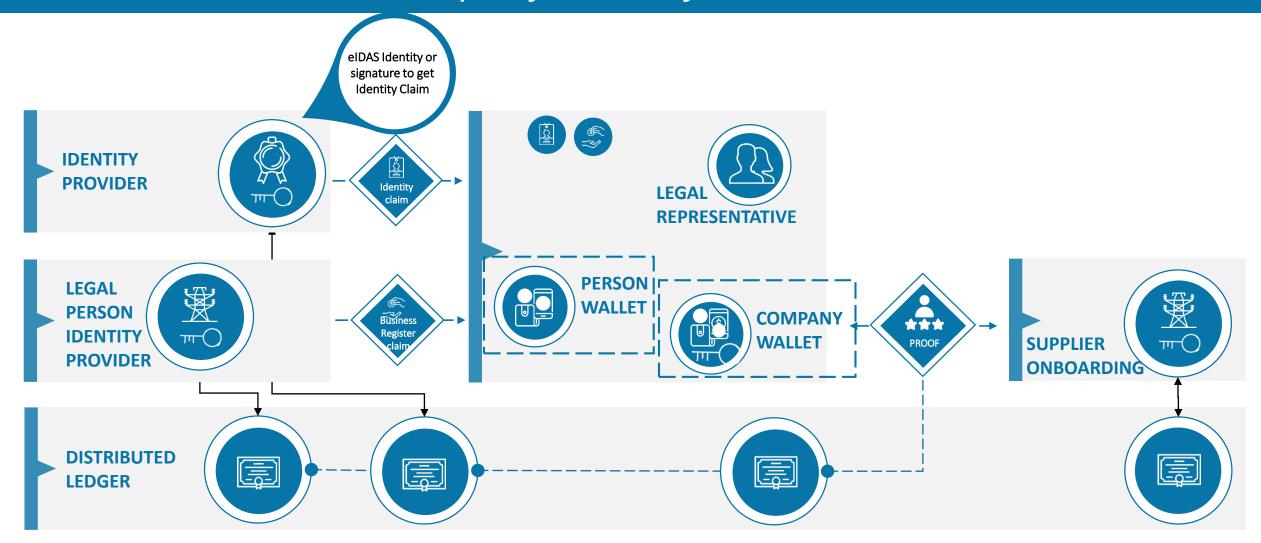
- Services for customer / supervisor strong authentication
 - A web application to navigate into the ledger, also used as a playground for operators; includes a test wallet



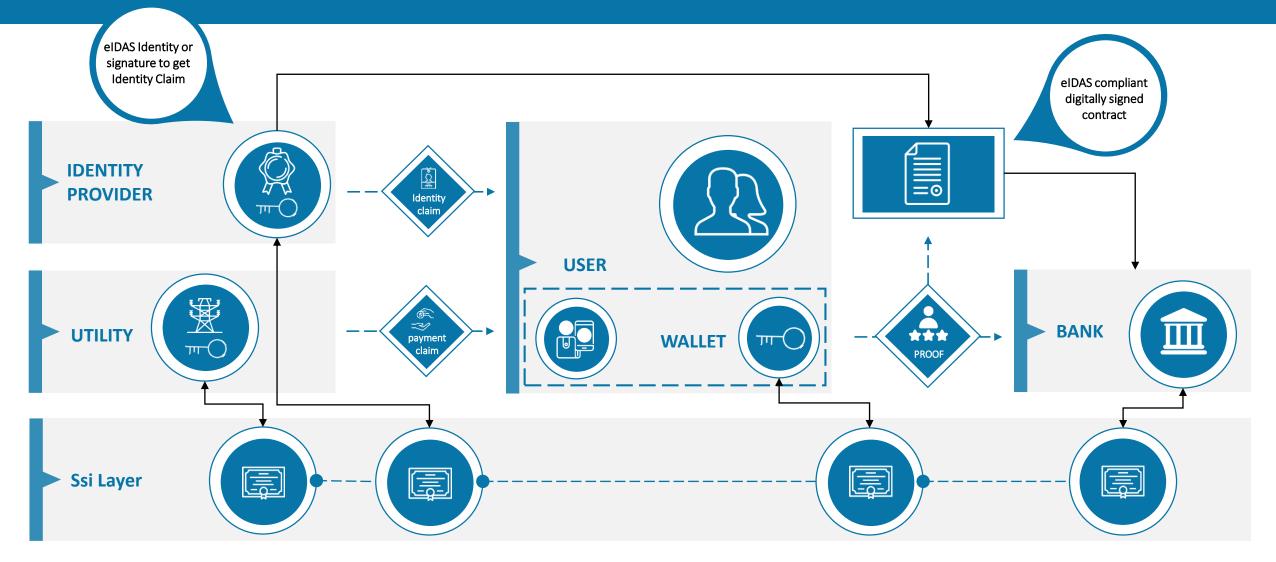
- App for access to the wallet
- Integrates infoCert authentication services

 Issuer of claims proving identity attributes

SOVRIN & eIDAS: Company Identity



SOVRIN & eIDAS – Personal Loan use Case





Thank you

fabrizio.leoni@infocert.it

