InfoCert
TECNOINVESTIMENTI GROUP

sovrin
identity for all

Sovrin for KYC

Commission expert group on electronic identification and remote KYC processes

L. Boldrin
September 28, 2018

Electronic identity know-how

InfoCert role

InfoCert is a provider of the **notified Italian National eID system** - SPID

InfoCert runs an eIDAS **node and a CEF project for connecting banks**

InfoCert provides **trusted digital onboarding services** for most Italian banks, insurance, finance services

InfoCert is a **Founding Steward** of the **SOVRIN** Network

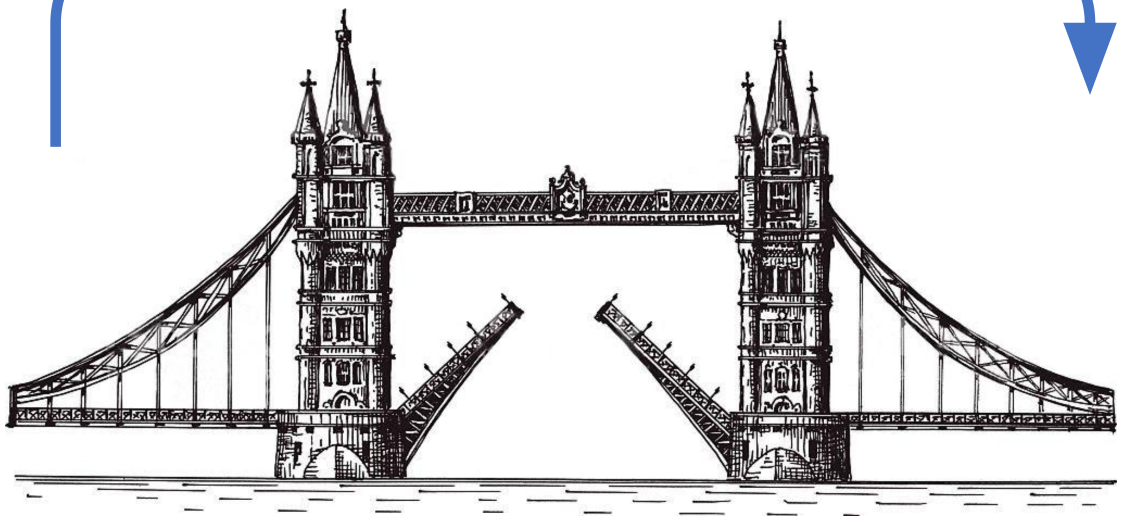
SSI & eIDAS

Regulation and Self Sovrin Identity

trusted identity data and liability framework

National-Sovereign Identity
eIDAS

Centrally defined identity for any person and organization, strongly validated, largely available, with a closed and regulated set of (KYC) data and data providers



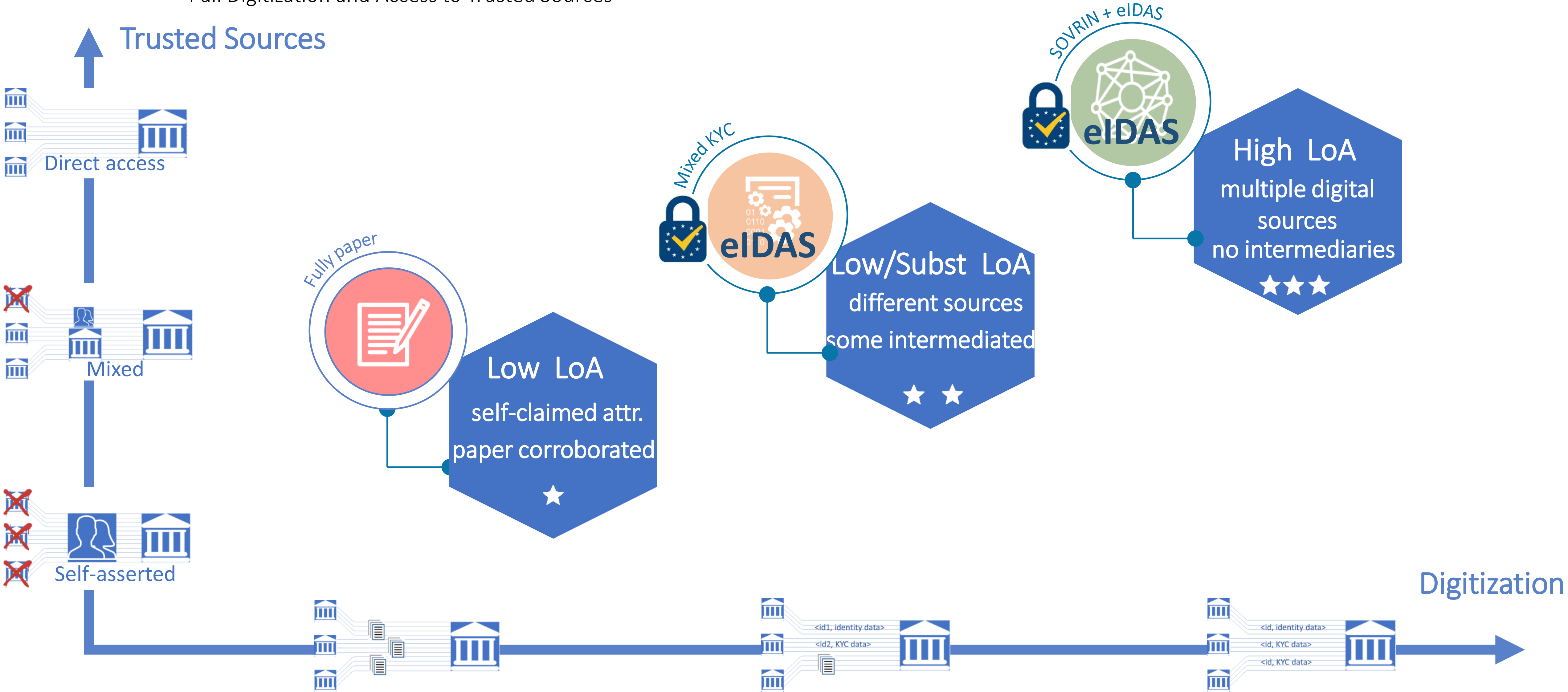
Lifetime portable identity (identifier!) for persons and organizations that does not depend on any centralized authority and offers support for unlimited (KYC) data and data providers

Self-Sovereign Identity
Sovrin

access to disparate trusted data issuers

Portable KYC

Full Digitization and Access to Trusted Sources



Trusted Sources

Direct access

Mixed

Self-asserted

Fully paper

Low LoA
self-claimed attr.
paper corroborated
★

Mixed KYC

eIDAS

Low/Subst LoA
different sources
some intermediated
★ ★

SOVRIN + eIDAS

eIDAS

High LoA
multiple digital sources
no intermediaries
★★★

Digitization

<id1, identity data>
<id2, KYC data>

<id, identity data>
<id, KYC data>
<id, KYC data>

Sovrin Decentralized Identity

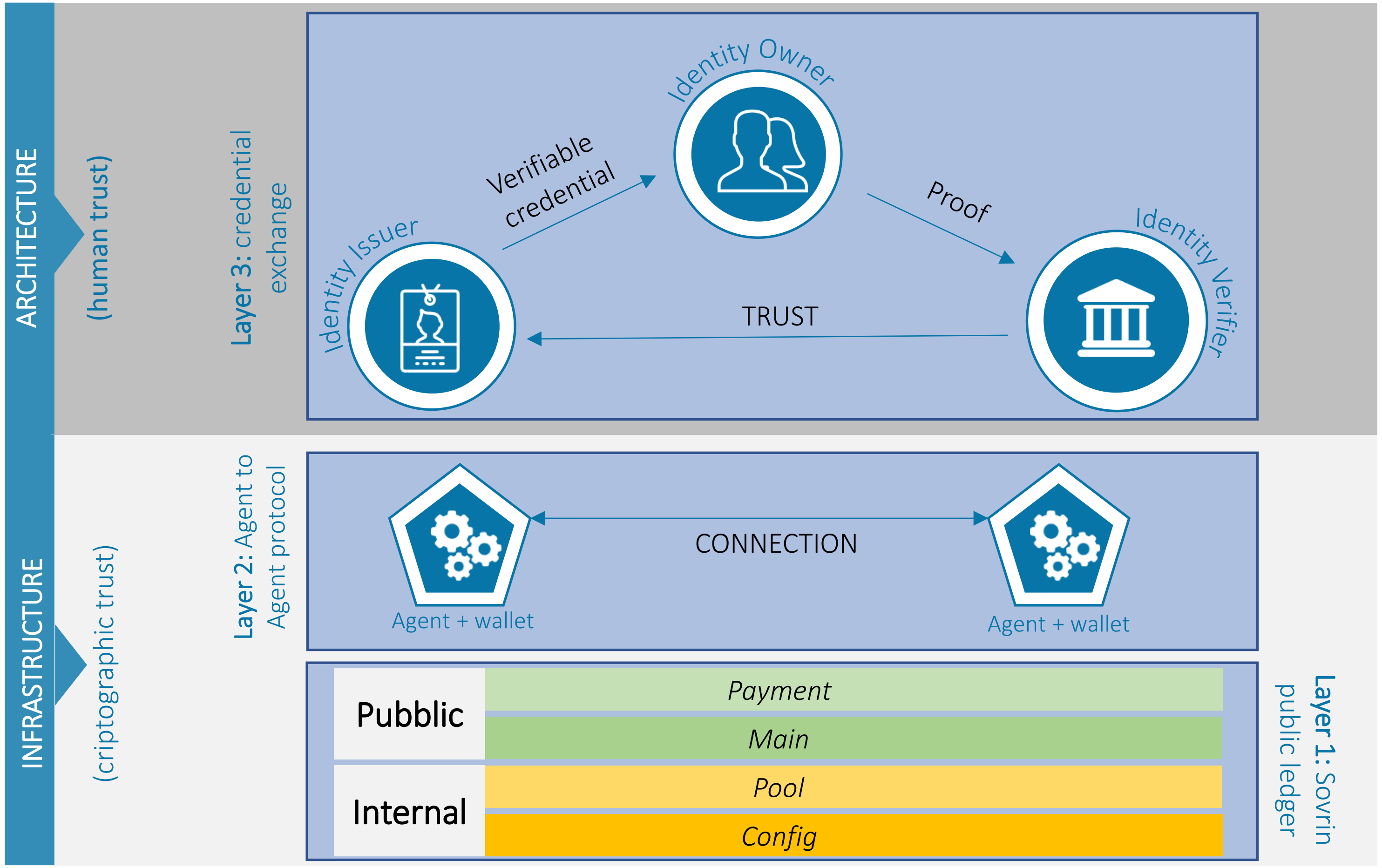
Cryptographic Trust and Preservation of Privacy

A global public utility for self-sovereign identity, designed for the governance, scalability, and privacy requirements

Structured in 3 layers

Provides a level playing field for:

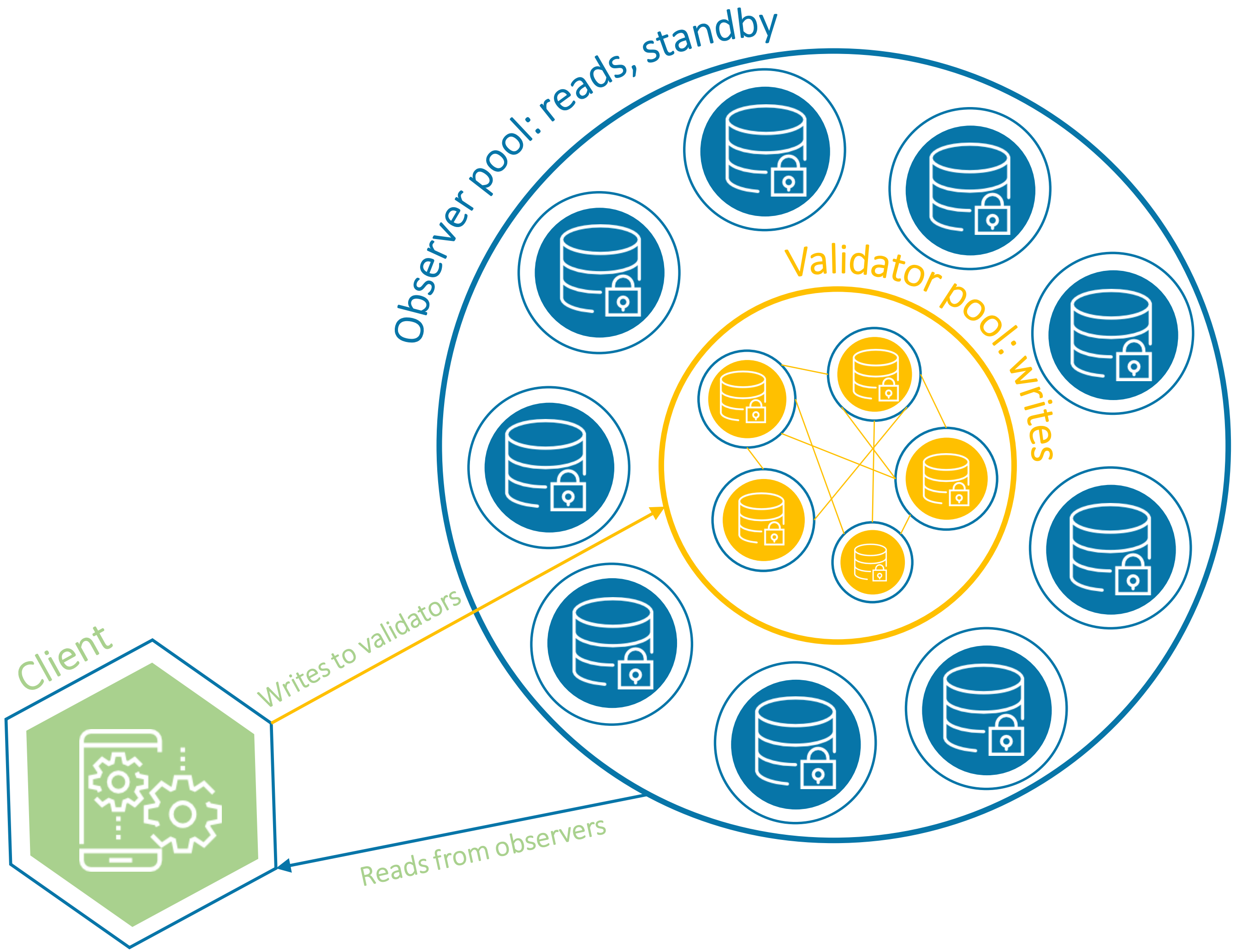
- technical competition /innovation (layer 2)
- Trusted content offerings (layer 3)



A Governed Ledger

The Global Layer Zero for All Public Information

- It operates like the Domain Name System
- On a Public permissioned blockchain
- It uses standardized components (W3C, OASIS, DIF)
  HYPERLEDGER Indy
- It includes identifiers, templates, revocation
- it is governed by no-profit Sovrin Foundation
  - board of trustees includes representatives from NGOs, universities, and standard-savvy people
- It is run by Stewards – carefully selected and monitored
  - Financial institutions, Certification authorities, Tech companies, Law firms, NGOs, Universities
  - The network includes eIDAS operator



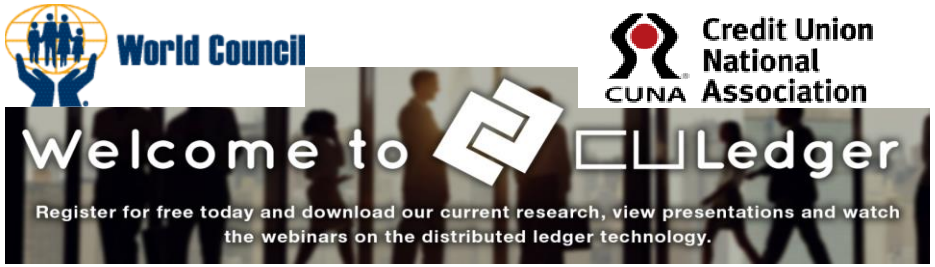
Use cases

The future is now

Finicity

workday

IBM



World Council

Credit Union National Association
CUNA

Welcome to CULedger

Register for free today and download our current research, view presentations and watch the webinars on the distributed ledger technology.

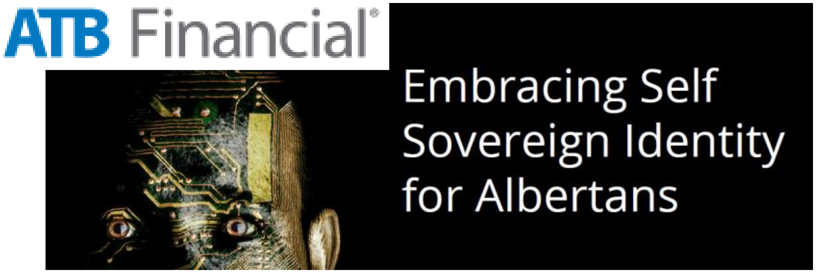
BRITISH COLUMBIA

Verifiable Organizations Network

absa

IC
InfoCamere

Decentralized Business Identites



ATB Financial

Embracing Self Sovereign Identity for Albertans

op

tieto

Trusted Digital Identity For Doctors

NHS

POST OFFICE

Portable KYC Practices main pains

What need to be fixed

Digitisation of KYC content

- Different sources normally provide data on different (proprietary) identifiers:
  - IBAN for banks, PointOfDelivery for utilities, fiscal code for public administrations, LEI for finance,…
  - This is key for information assembly
- There are competing standards (formats, protocols) and no common templates
- Privacy loss via disclosure of unnecessary information to the KYC consumer
- Privacy loss via disclosing KYC consumers to KYC issuers

Trusted sources & KYC validation

- Recognize sources as trustworthy and liable for the data they provide, as in the paper world
- Enable sources of KYC data (facilitate, incentivize)
- Guaranteeing freshness / non-expiration of information
- Disintermediate: if information is intermediated, the assurance level is jeopardized

Solution: Self Sovereign Identity

Portable KYC

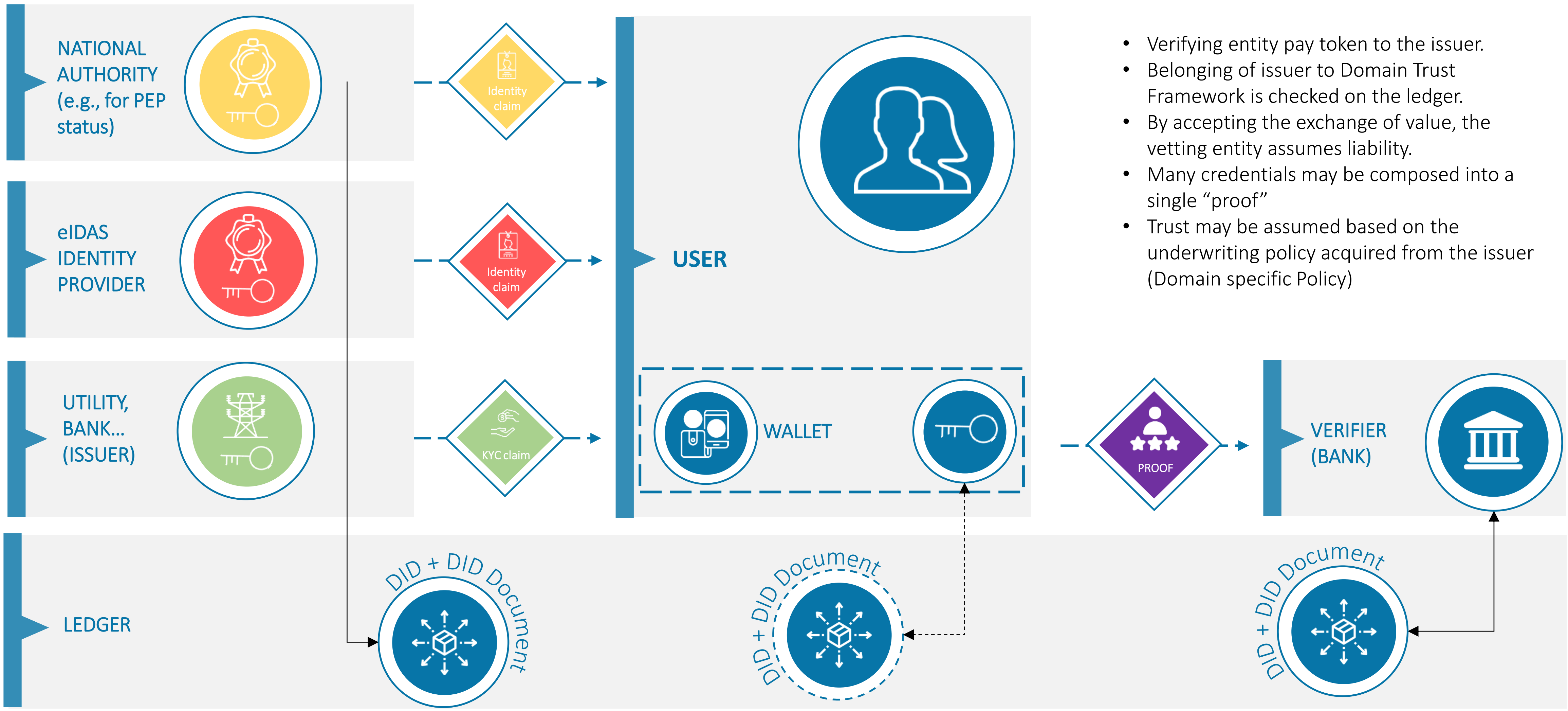
	feature	Traditional PKI	Online Identity	SSI
Digitisation of KYC content	Common Identifiers	Identifier owned by CA	Identifier owned by IdP (john.doe@gmail.com)	DID + master identity owned by user
	Privacy loss: Data Minimisation	No	Yes, delegated to IdP	Yes, through ZKP
	Privacy loss: undisclosed KYC consumer	Certificates are in the hands of the user	Data is siloed at IdPs	Credentials are in the hands of the user
Trusted sources & KYC validation	Recognise the source	Sources are identified (via identity certificates) Trust needs a separate channel	Sources are identified (via TLS certificates) Trust needs a separate channel	Sources are identified Trust is supported by the ledger
	Facilitate and Incentivise	Off-line incentives	Off-line incentives	Supports value exchange via token
	Freshness	Yes, but requires access to several CRLs	Yes, info freshness is granted by issuer	Yes, revocation is handled on the ledger
	Public Templates	No	No	Yes (on the ledger)
	Disintermediate	Yes	Yes, but issuer must run high-available service	Yes

sovrin

InfoCert
TECNOINVESTIMENTI GROUP

Re-usable KYC Proof

A set of credential in the User’s wallet serve as a verifiable proof

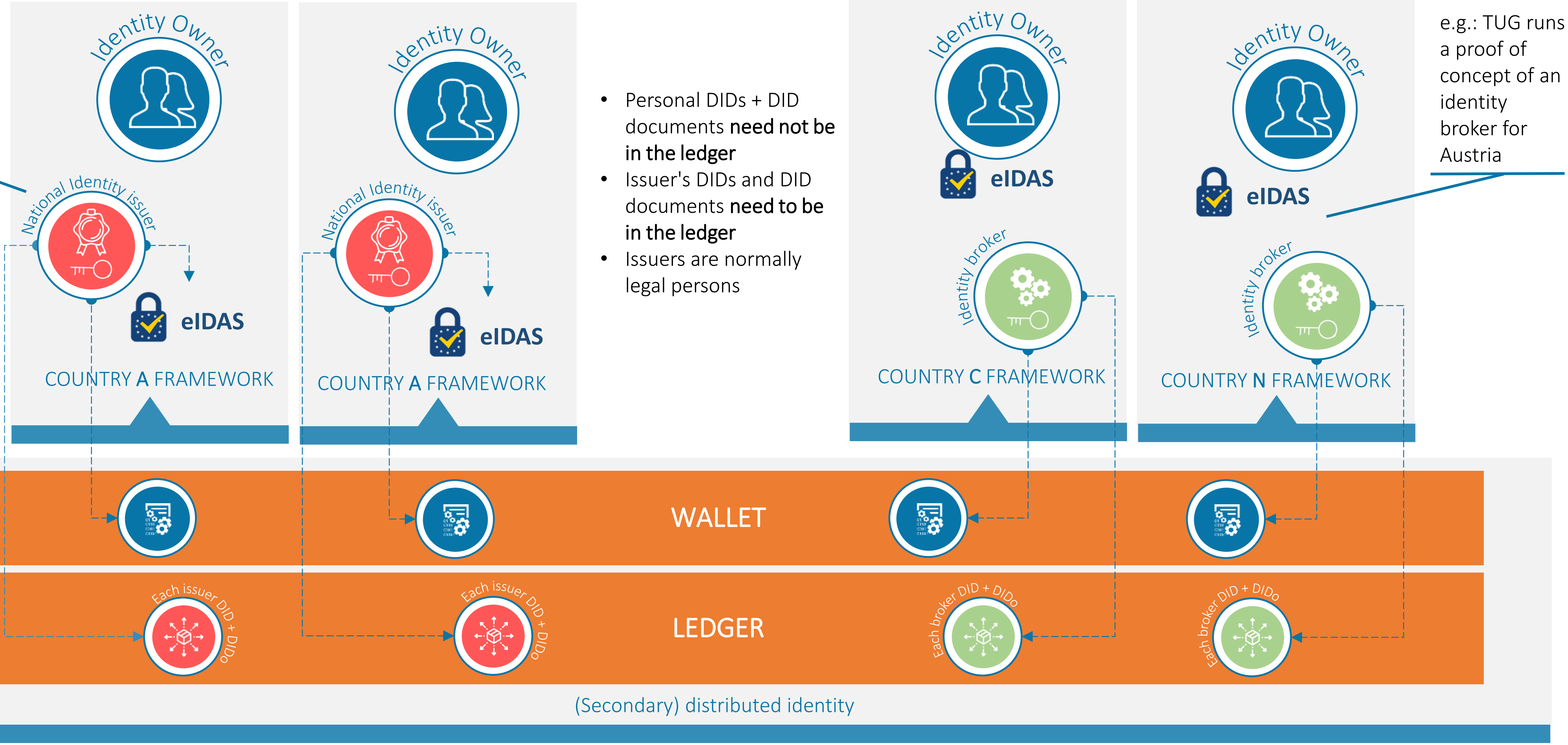


- Verifying entity pay token to the issuer.
- Belonging of issuer to Domain Trust Framework is checked on the ledger.
- By accepting the exchange of value, the vetting entity assumes liability.
- Many credentials may be composed into a single “proof”
- Trust may be assumed based on the underwriting policy acquired from the issuer (Domain specific Policy)

Reusable electronic Identity

Electronic recycle

e.g: INFOCERT tests creation of SSI identities in parallel with SPID identites

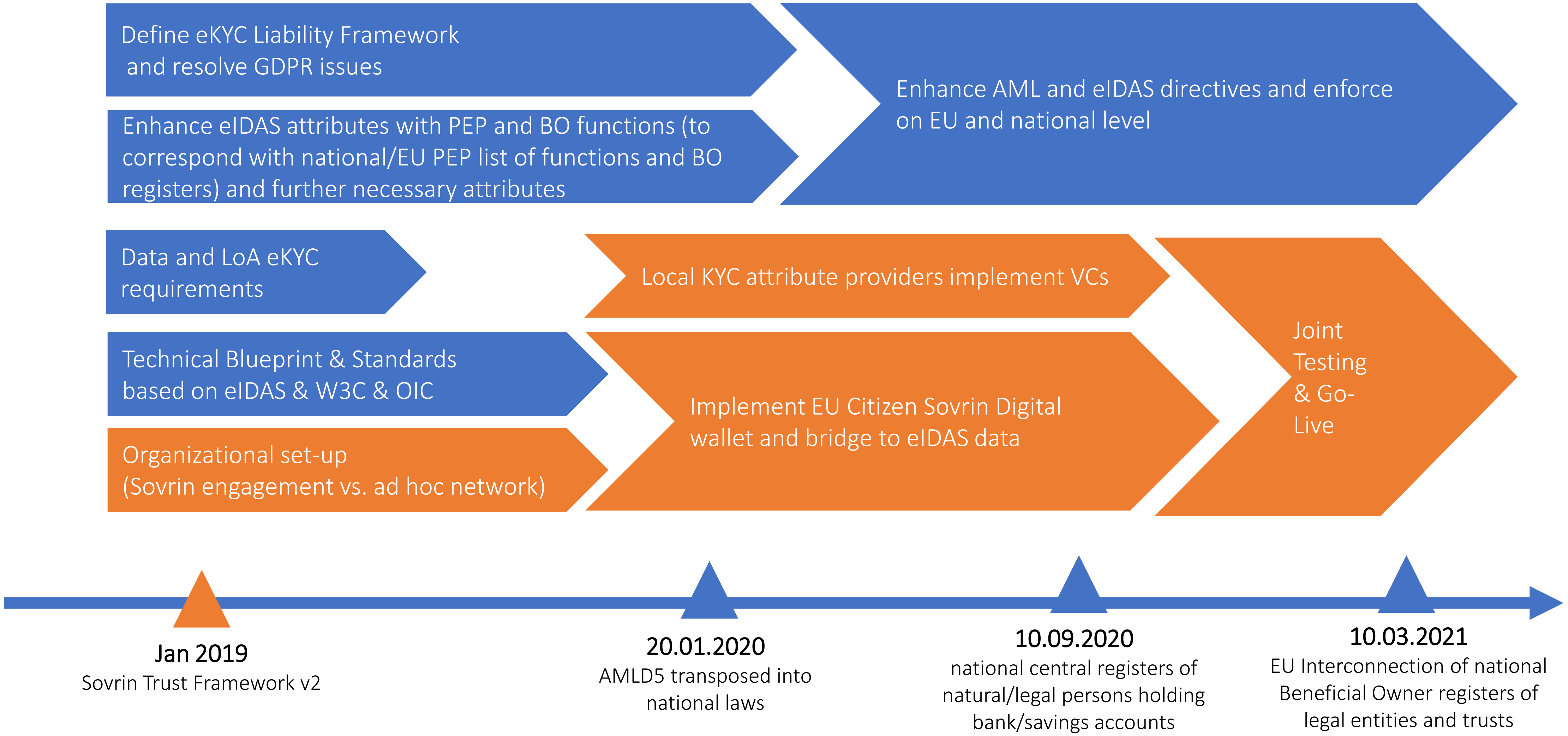


- Personal DIDs + DID documents **need not be in the ledger**
- Issuer's DIDs and DID documents **need to be in the ledger**
- Issuers are normally legal persons

e.g.: TUG runs a proof of concept of an identity broker for Austria

AML5 SOVRIN + eIDAS roadmap

A proposal



Define eKYC Liability Framework and resolve GDPR issues

Enhance eIDAS attributes with PEP and BO functions (to correspond with national/EU PEP list of functions and BO registers) and further necessary attributes

Enhance AML and eIDAS directives and enforce on EU and national level

Data and LoA eKYC requirements

Local KYC attribute providers implement VCs

Technical Blueprint & Standards based on eIDAS & W3C & OIC

Organizational set-up (Sovrin engagement vs. ad hoc network)

Implement EU Citizen Sovrin Digital wallet and bridge to eIDAS data

Joint Testing & Go-Live

Jan 2019
Sovrin Trust Framework v2

20.01.2020
AMLD5 transposed into national laws

10.09.2020
national central registers of natural/legal persons holding bank/savings accounts

10.03.2021
EU Interconnection of national Beneficial Owner registers of legal entities and trusts

sovrin

Thank you

InfoCert
TECNOINVESTIMENTI GROUP

WWW.INFOCERT.IT