



Friday 13th November 2020 – at 11:00 a.m.

Online Seminar via Zoom

Egidio Casati
Enrico Talin

eIDAS e tecnologie per la decentralizzazione:

l'esperienza della blockchain Commercio Network

Main-Net 2.1 is live

THE DOCUMENTS BLOCKCHAIN™

Exchange and sign documents on the first eIDAS compliant blockchain in Europe

eSignature

Electronically Sign any
PDF e XML digital
document

eID

Create and manage
Self Sovereign
Identities

eDelivery

Notarized electronic
documents exchange
among parties

eInvoicing

Order-to-cash cross
border supply chain
protocol

Commercio Network

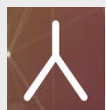
Commercio.network is “The Documents Blockchain”
born to **sign** and **exchange** business **documents** among its participants.



Egidio Casati - About Me

I have a passion for cutting edge technologies with a particular focus on cryptography, online identity and decentralisation, with more than 20 years of experience in the field.

My career focused on Public Key Infrastructure and Digital Signature for the Digital Transformation of the Finance, Lending and Industry sectors.



Founder and CEO at NYM Srl, building solutions for the decentralised web (2019)



Co-Founder of Blank Art Network, a start up, working on digital art on the Blockchain (2018)



Board member of the Commercio Consortium, governing the Commercio.network blockchain, a B2B proof of stake based decentralised network legally binding data exchange (2018)

NAM



eID.AS



Our Mission

"We leverage decentralised technologies to design ideas for a greener, smarter, resilient yet regulation-wise business."

214

✓ All

176

✓ CA

✓

eSignatures

✓

eSeals

✓

Website

112

✓ TSA

12

✓ PresS

18

✓ EDS

15

✓ ValS

✓

eSignatures

✓

eSeals

Status

Granted

Countries



Source: <https://www.eid.as/tsp-map/#/>

eIDAS

○ trust services single market

eIDAS stands for “**e**lectronic **I**dentification, **A**uthentication and trust **S**ervices”, i.e.:

- ID
- eSignatures
- Long Term Archival
- Time Stamping
- Certified Delivery
- Validation Services

eID

AS

2015/1501/EU
eID Interoperability Framework
and Voluntary Recognition of eID

2015/1502/EU
eID Assurance Levels

2015/296/EU
eID Collaboration

2015/1984/EU
eID Notification

eIDAS-Regulation
(EU) No 910/2014
in force

2015/806/EU
Trust Mark

2015/1505/EU
Trusted List

2015/1506/EU
AdES Formats

2016/650/EU
QSCD Security
Assessment

2016/07/01
(EU) No 910/2014
fully applicable

go.eIDAS

EU-wide
eID-Recognition



eID notified schema

Italy - eID	Republic of Italy	Italian eID based on National ID card (CIE)	Italian eID card (Carta di Identità elettronica)	High	NOTIFIED	13 Sep 2019	2019/C 309/09
Italy - SPID	Republic of Italy	SPID – Public System of Digital Identity	SPID eID means provided by: <ul style="list-style-type: none">• Aruba PEC SpA• Namirial SpA• InfoCert SpA• In.Te.S.A. SpA• Poste Italiane SpA• Register.it SpA• Sielte SpA• Telecom Italia Trust Technologies S.r.l.	Low, Substantial, High	NOTIFIED	10 Sep 2018	2018/C 318/02 corrected by 2018/C 344/09

Source: <https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS>

eIDAS Definitions – art. 3 - eID

- (1) '**electronic identification**' means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
- (2) '**electronic identification means**' means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;
- (3) '**person identification data**' means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
- (4) '**electronic identification scheme**' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;
- (5) '**authentication**' means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;

eIDAS Definitions – art. 3 – Trust Service Provider

- (16) **'trust service'** means an electronic service normally provided for remuneration which consists of:
 - (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
 - (b) the creation, verification and validation of certificates for website authentication; or
 - (c) the preservation of electronic signatures, seals or certificates related to those services;
- (17) **'qualified trust service'** means a trust service that meets the applicable requirements laid down in this Regulation;
- (18) **'conformity assessment body'** means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
- (19) **'trust service provider'** means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;
- (20) **'qualified trust service provider'** means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

eIDAS Definitions – art. 3 - eSignature

- (10) '**electronic signature**' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
- (11) '**advanced electronic signature**' means an electronic signature which meets the requirements set out in Article 26;
- (12) '**qualified electronic signature**' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

eIDAS Definitions – art. 3 - eDelivery

- (36) '**electronic registered delivery service**' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations
- (37) '**qualified electronic registered delivery service**' means an electronic registered delivery service which meets the requirements laid down in Article 44;

Main-Net 2.1 is live

THE DOCUMENTS BLOCKCHAIN™

Exchange and sign documents on the first eIDAS compliant blockchain in Europe

eSignature

Electronically Sign any
PDF e XML digital
document

eID

Create and manage
Self Sovereign
Identities

eDelivery

Notarized electronic
documents exchange
among parties

eInvoicing

Order-to-cash cross
border supply chain
protocol

Commercio Network

Commercio.network is “The Documents Blockchain”
born to **sign** and **exchange** business **documents** among its participants.

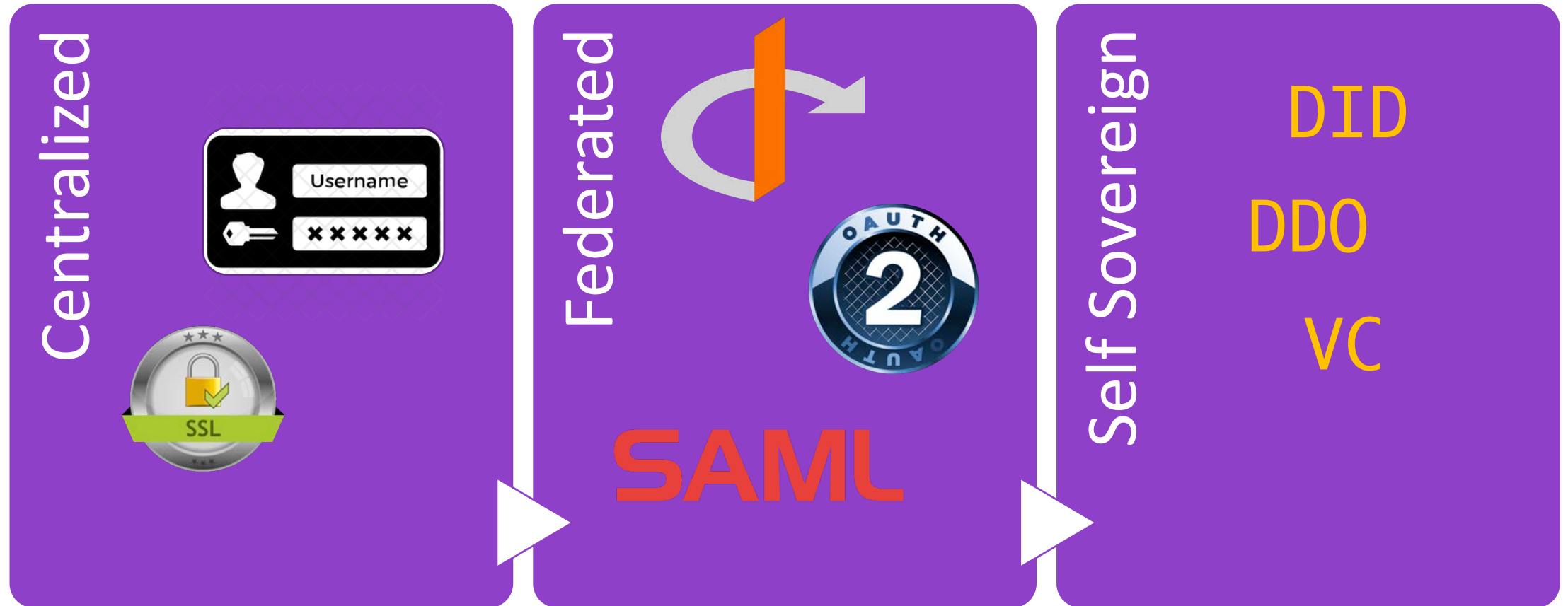


«Self Sovereign Identity»

what's that?

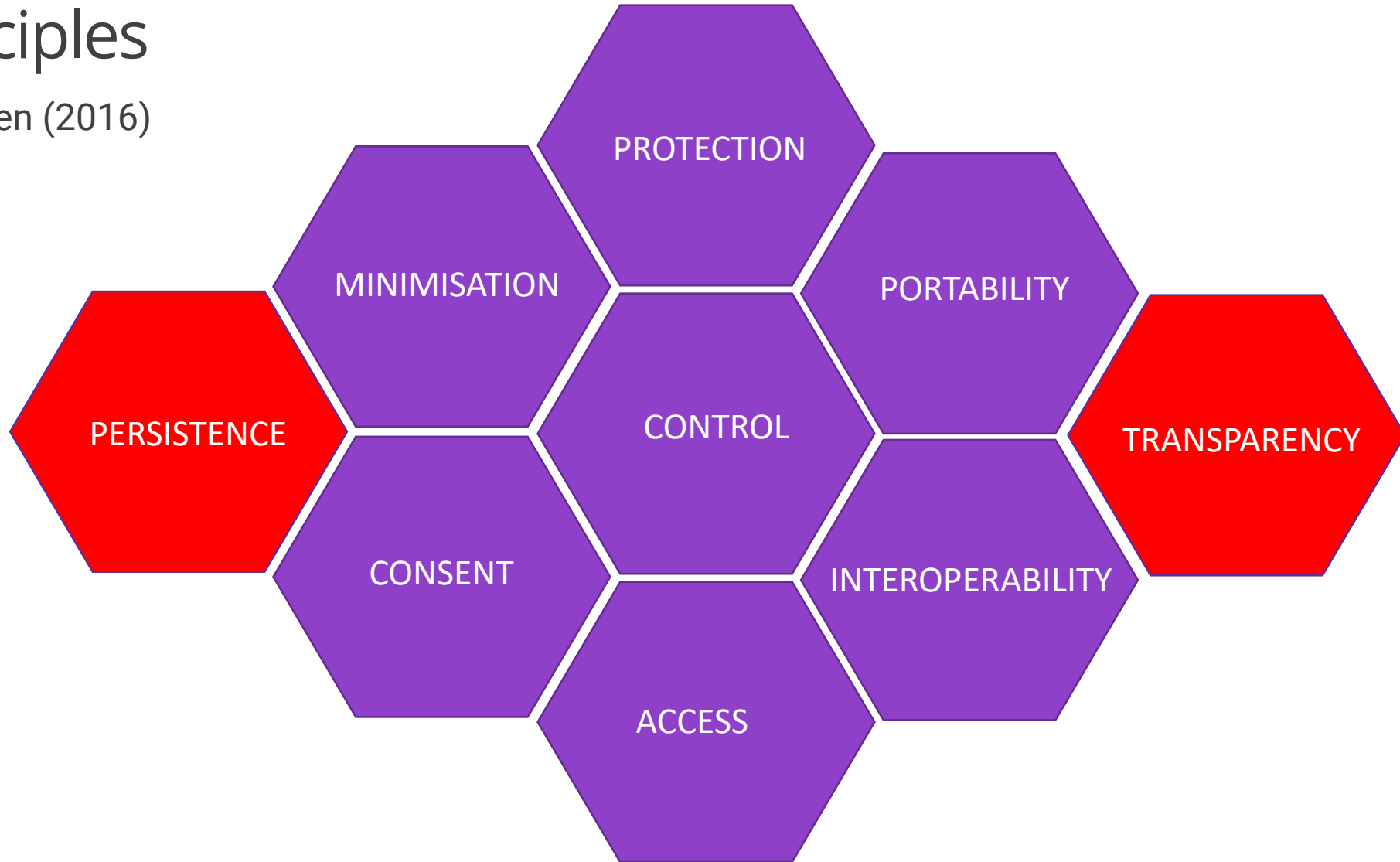
... the digital movement that recognizes an **individual should own and control their identity** without the intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world.

Evolution of Online Identity



SSI Principles

Cristopher Allen (2016)



Source: <https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md>

Decentralized Identifier

EXAMPLE 1: A simple example of a Decentralized Identifier (DID)

did:example:123456789abcdefghi

URL Scheme Identifier

DID Method Identifier

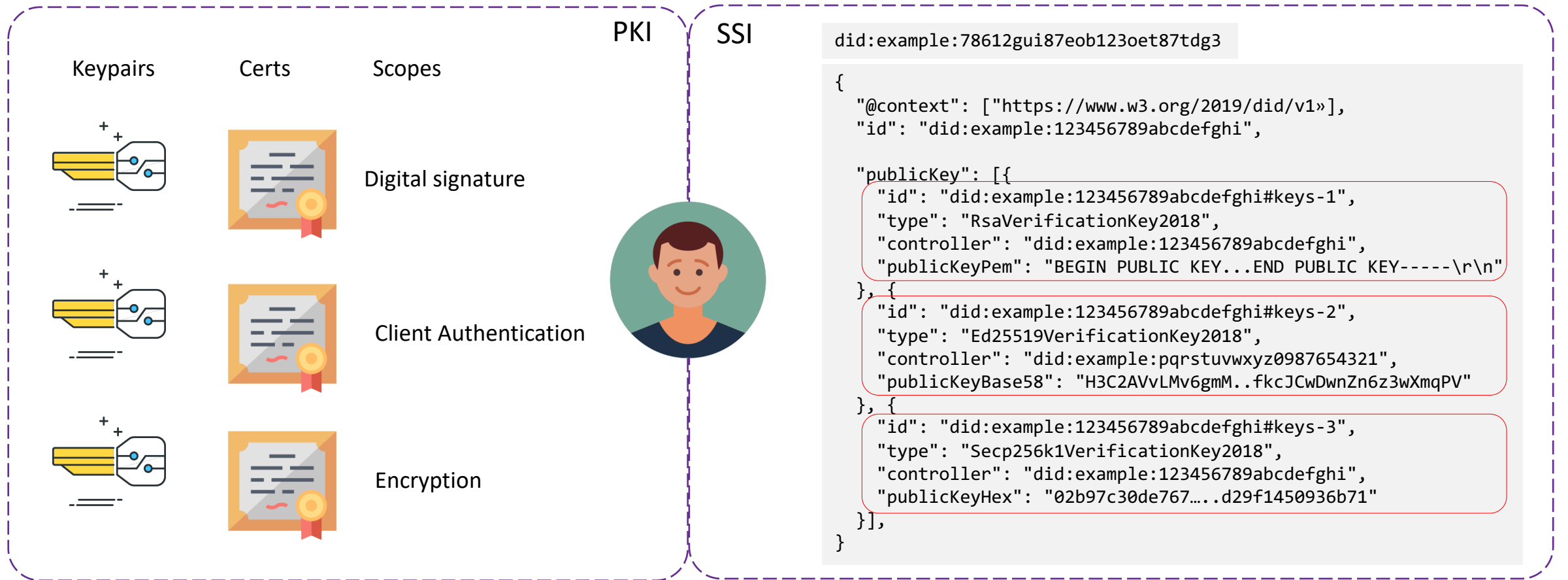
DID Method-specific identifier

did:com:1uzvgy7kkgjhyg27drm7ltrfumtmhuhc67hhtc7

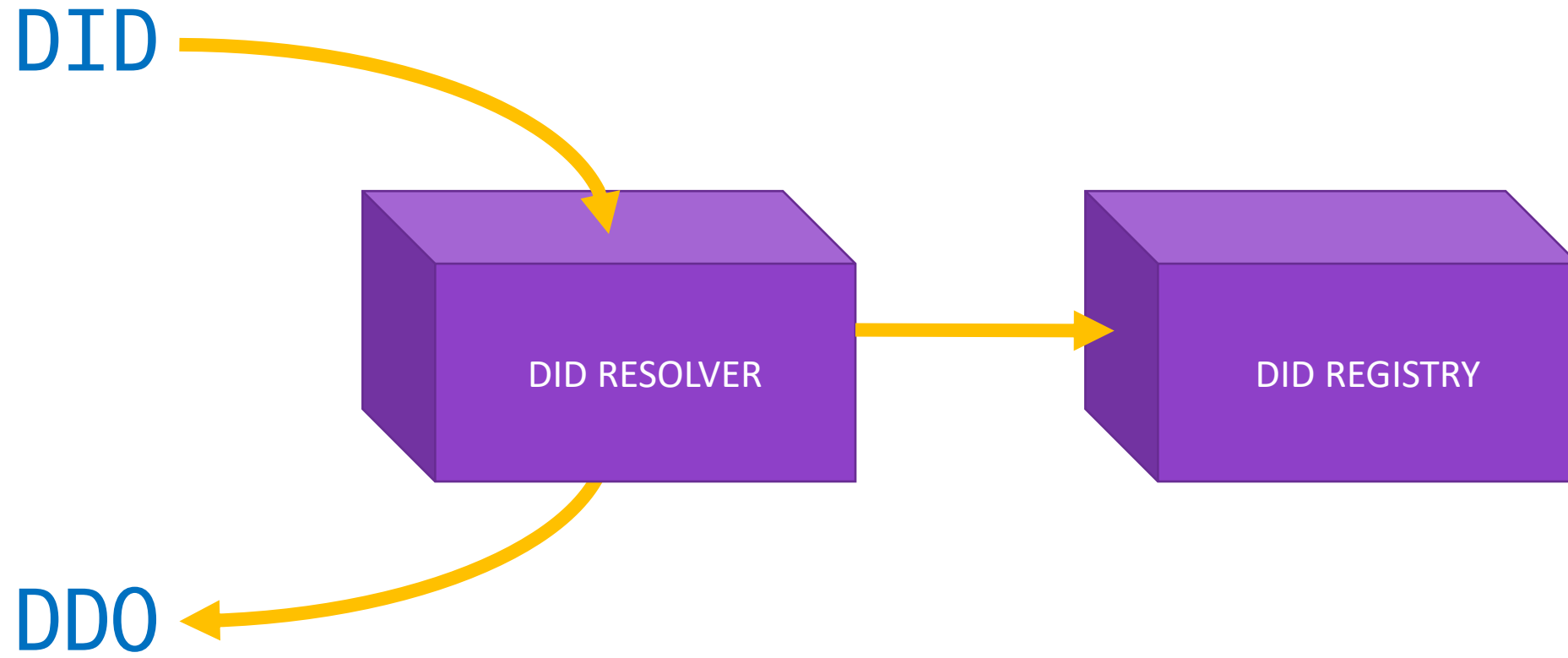
DDO: Did Document

```
{
  "@context": ["https://w3id.org/did/v1", "https://w3id.org/security/v1"],
  "id": "did:example:123456789abcdefghi",
  ...
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }, {
    "id": "did:example:123456789abcdefghi#keys-2",
    "type": "Ed25519VerificationKey2018",
    "owner": "did:example:pqrstuvwxyz0987654321",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }, {
    "id": "did:example:123456789abcdefghi#keys-3",
    "type": "Secp256k1VerificationKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyHex": "02b97c30de767f084ce3080168ee293053ba33b235d7116a3263d29f1450936b71"
  }],
  ...
}
```

Classic X509 vs DDO (smart certificate)



DID Resolver, the DNS of SSI



DID Method and Method Registry

- DID scheme definition
- DID string generation
- DID Operations:
 - Create (register)
 - Read (resolve)
 - Update (replace)
 - Delete (revoke)
- Security Considerations
- Privacy Considerations

W3C Working Group

DID Specification Registries

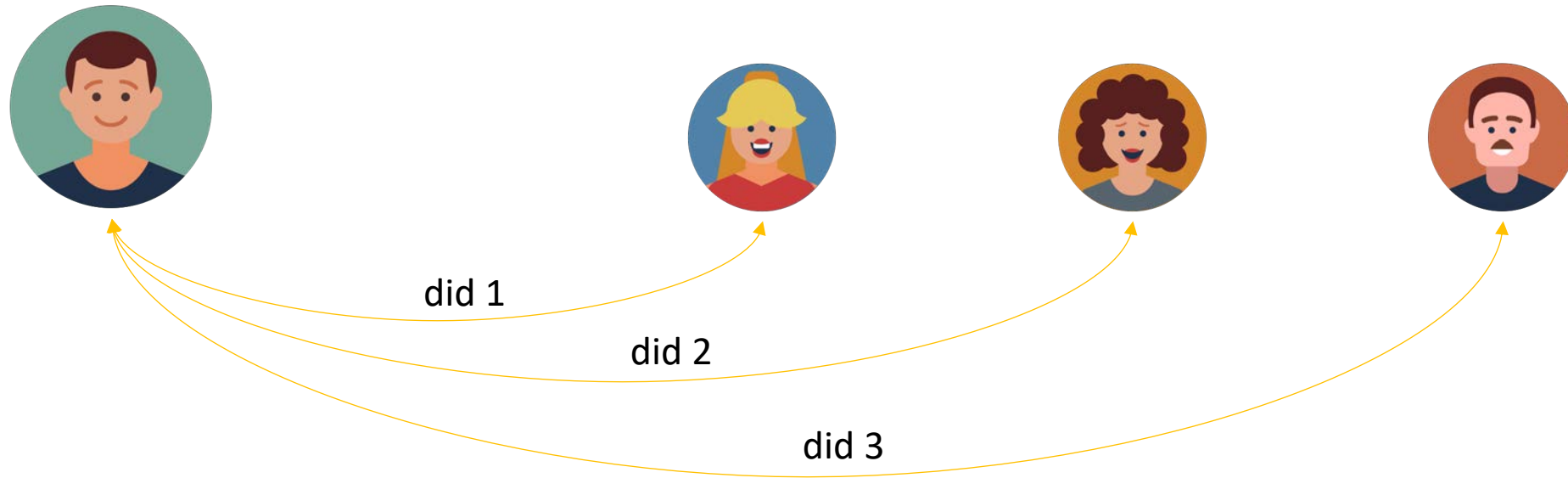
The interoperability registry for Decentralized Identifiers



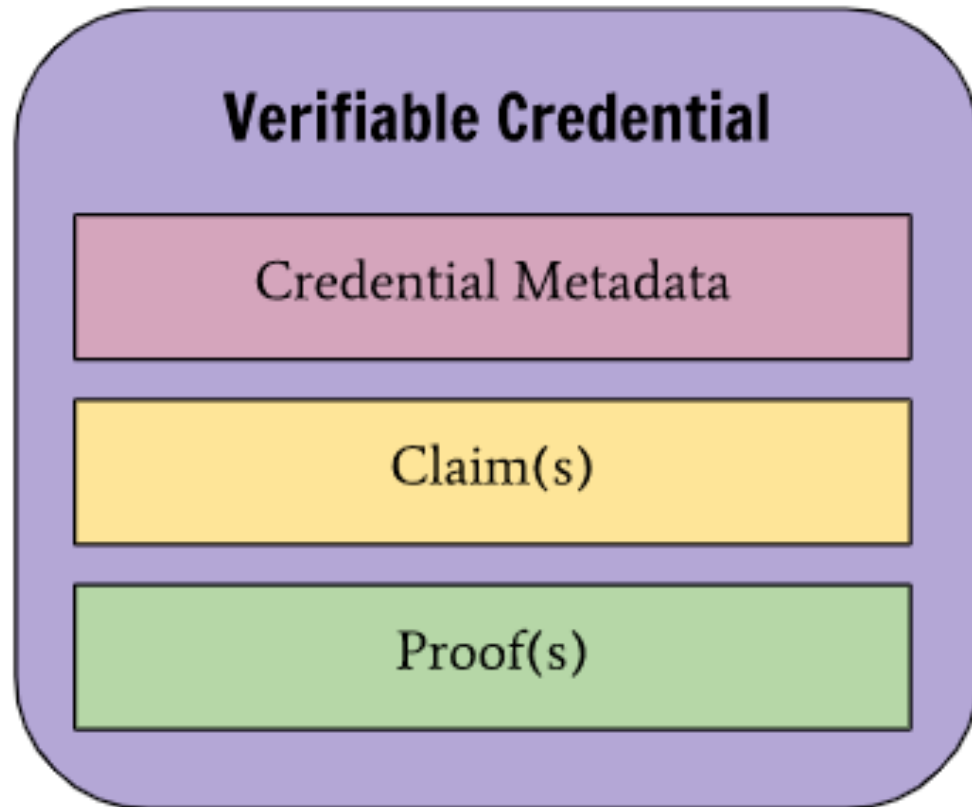
COM DID Method

Public DID and Pairwise DID

- Like any type of globally unique identifier, DIDs may be used for correlation.
- DID controllers can mitigate this privacy risk by using pairwise unique DIDs, i.e., by sharing a different private DID for every relationship.

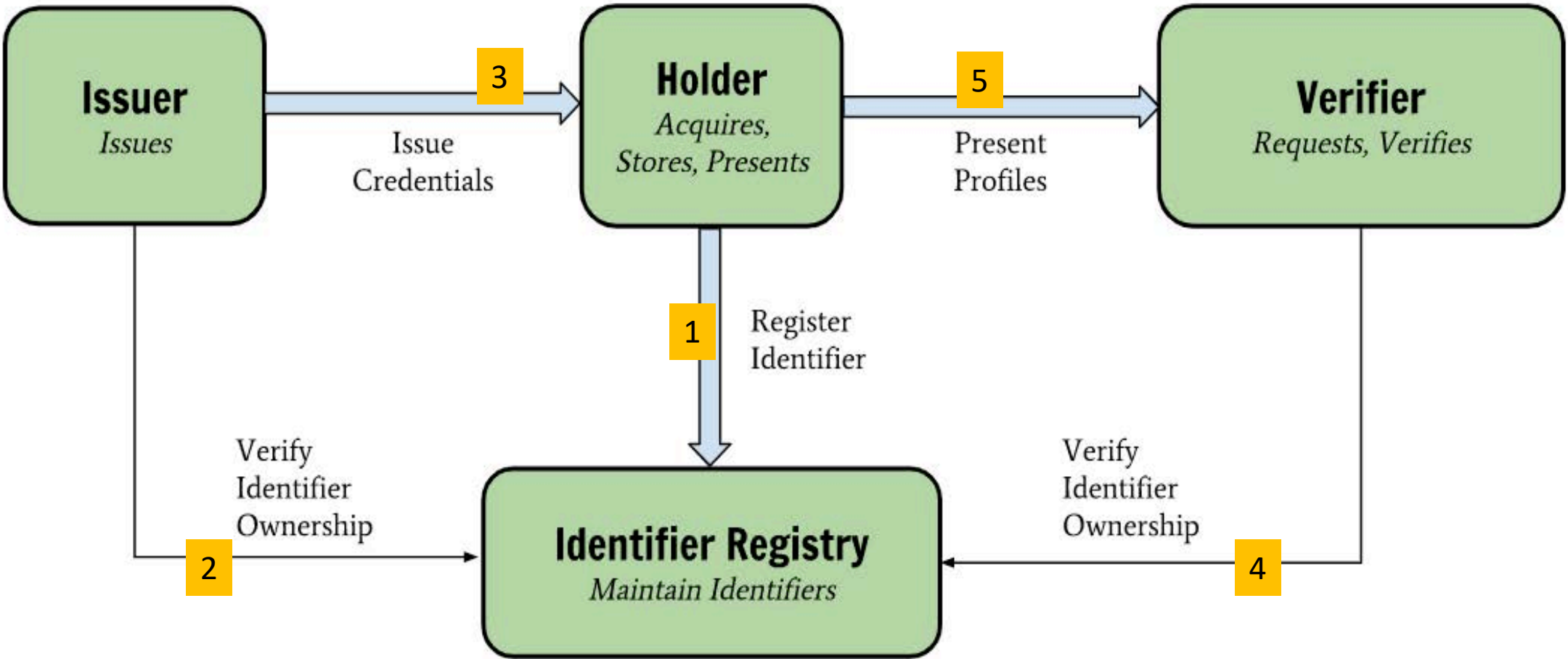


Verifiable Credential



- A credential is a set of one or more claims made by the same entity.
- A verifiable credential is a set of tamper-evident claims and metadata that cryptographically prove who issued it.

Verifiable Credential



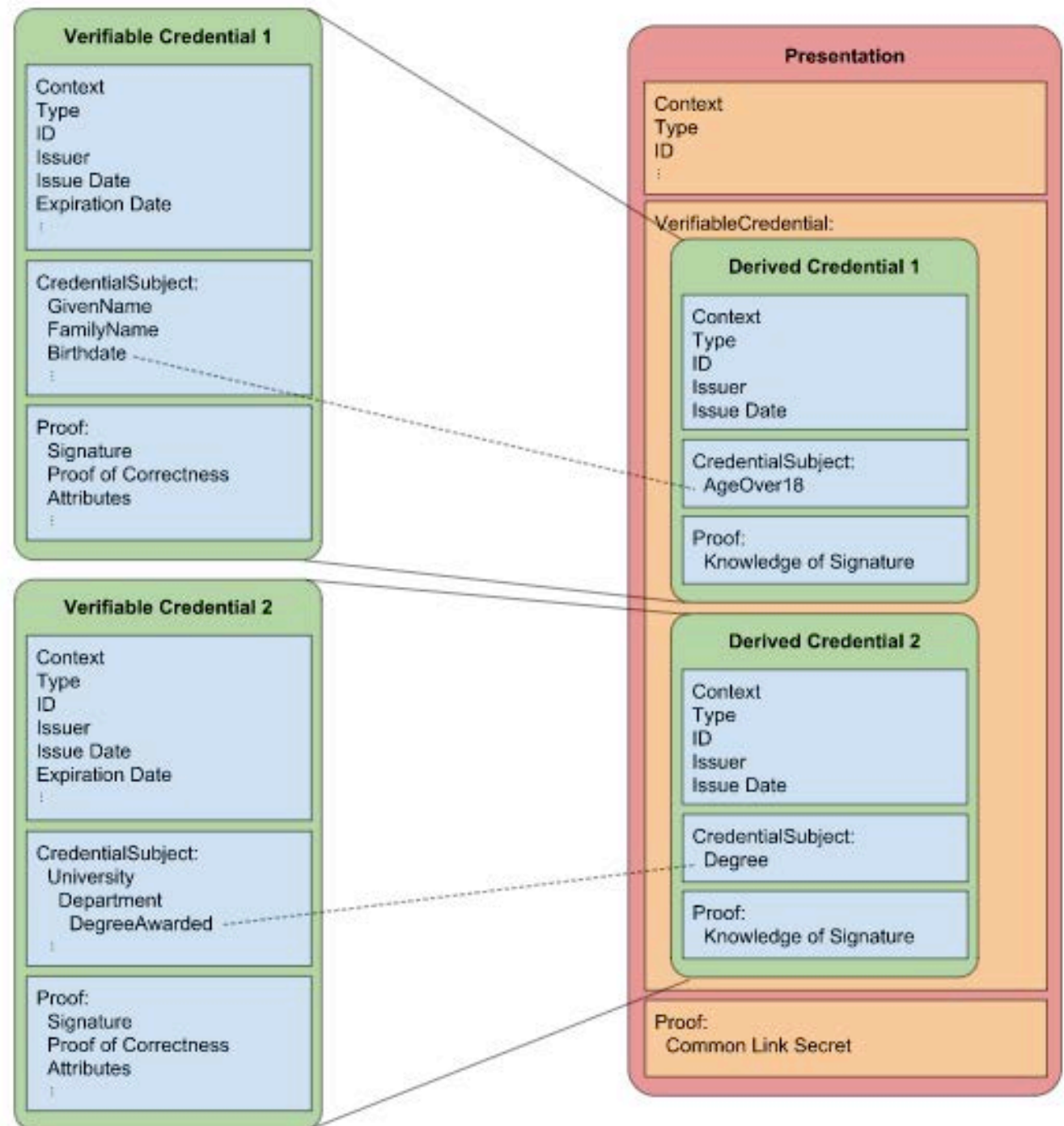
Claim Types (K. Cameron 2008)

<https://www.identityblog.com/wp-content/images/2009/06/UserCentricIdentityMetasystem.pdf>

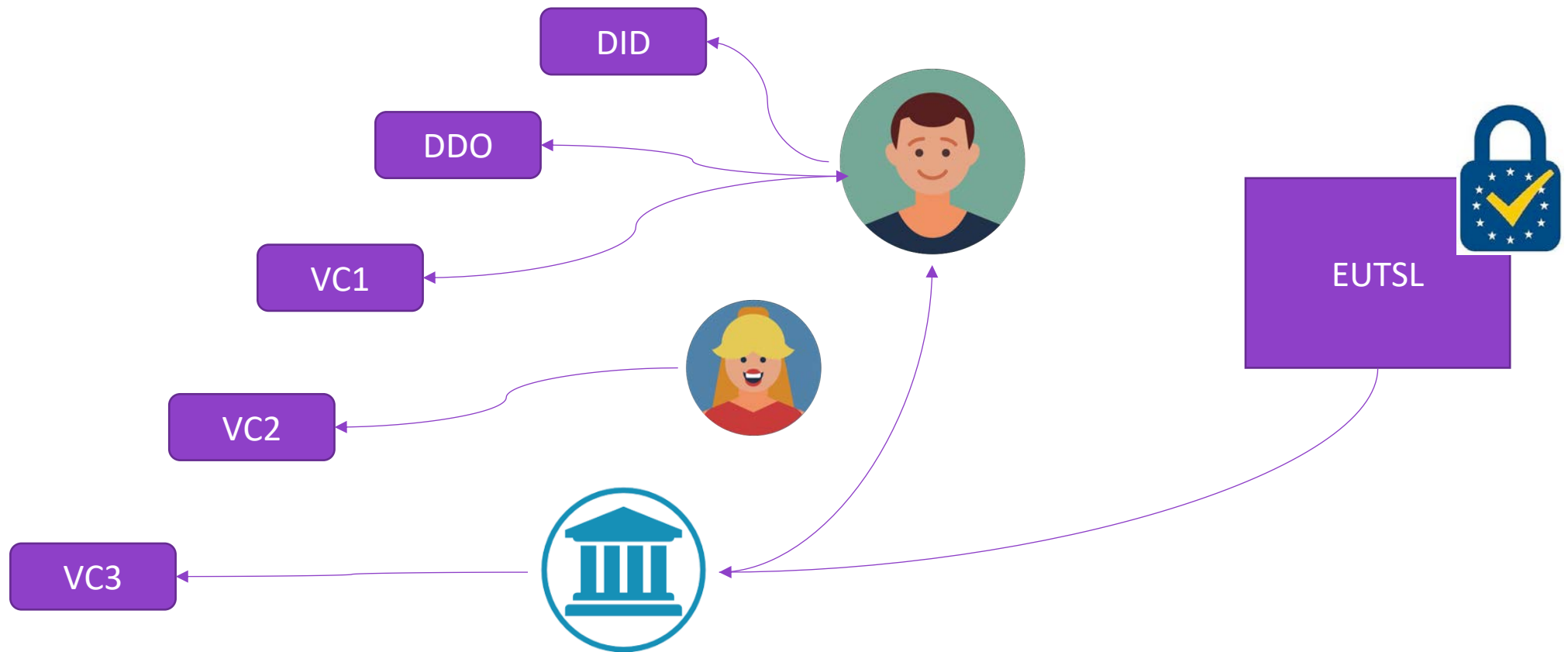
Type of Claim	Description	Example
Static	What we have traditionally called “properties” and “attributes” of the subject – static within some window of time	National identifiers and employee numbers Date of Birth Name Address
Relationship	Subject is in some relationship with another subject (and open-ended model with multiple sources and viewpoints)	Member of arbitrary group Member of assigned role Relationship to another subject (e.g. Personal Assistant or Parent) Mandate (e.g. trustee) Acting-as / On-behalf-of relationships
Derived	Claims that convey minimum necessary information by deriving it from facts but not releasing the facts	Over 21 or Under 16 University Student Person in Drug Trial Unmarried Female in 20's
Capability	Authentication and authorization both based on claims transformation. Capabilities are determined by relying party within a defined scope	Can-read-calendar Can-access-write-operation Denied-update-in-given-scope
Contextual	Factors useful in evaluating the security presentation.	Authentication technology, location, time

Credential (Verifiable) Presentation

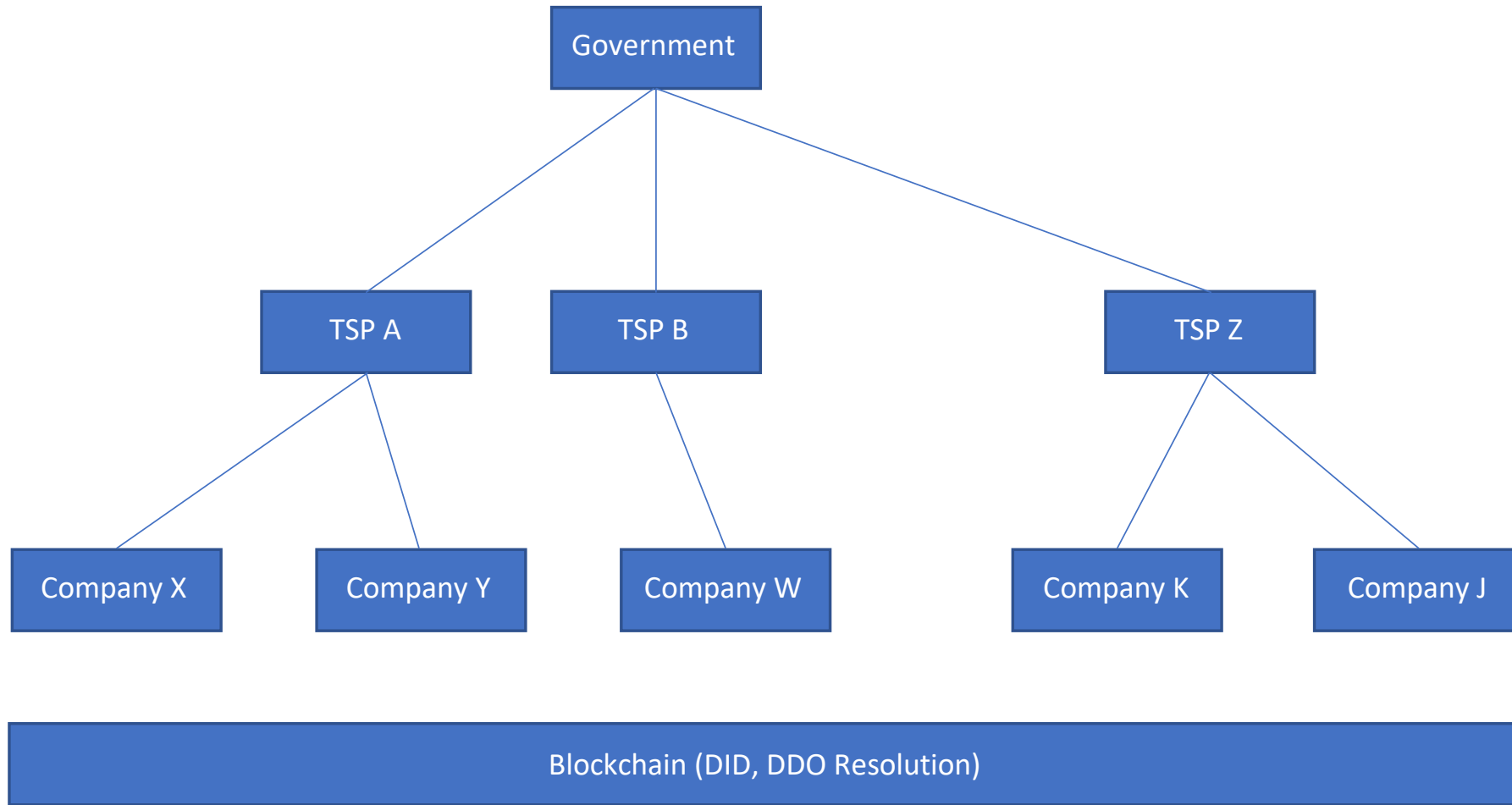
PRESENTATION COMBINES
CREDENTIALS PROVIDING
PROOF AND ZERO
KNOWLEDGE PROOFS



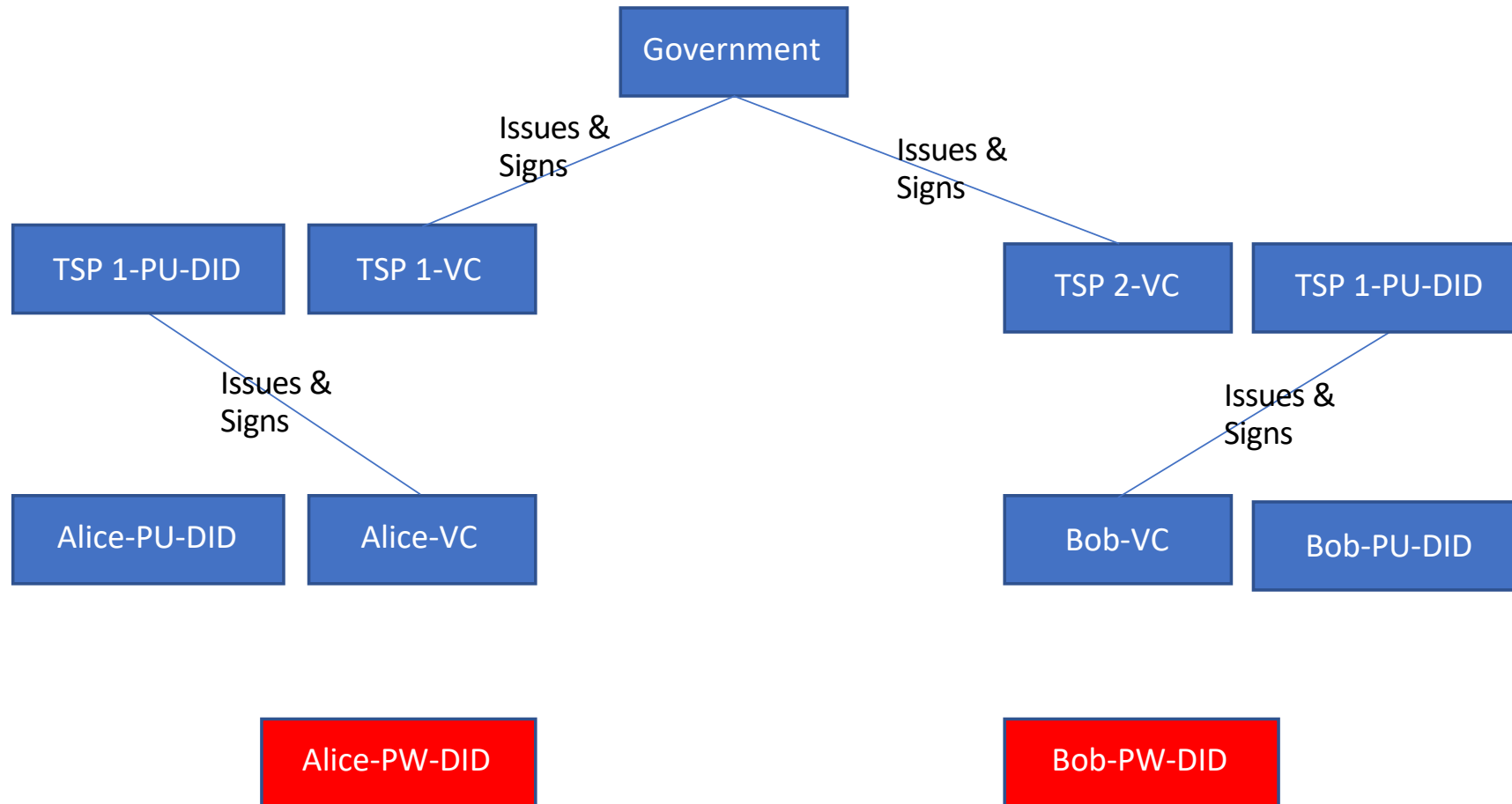
Trusted Issuer



Commercio Network Trust Model



Commercio Network Pairwise DID



Commercio Network Implementatio of a TRUST NETWORK

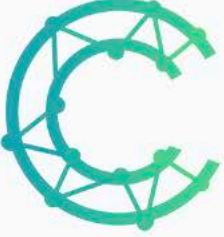
How we envisioned eID, eDelivery and eSignature in a Decentralised Scenario

- [eID – Create Identity](#)
- [eDelivery - Share Doc](#)
- [eSignature - DoSign](#)

	Dart/Flutter	Kotlin/Java	C#/Dot.net	GoLang
Sacco	Repo ↗	Repo ↗	Repo ↗	Repo ↗
CommercioSDK	Repo ↗	Repo ↗	Repo ↗	Later
(Commercio Application SDK)	Docs ↗	Docs ↗	Later	Later

Use AMADEO Boilerplate to TEST Commercio Network in TESTNET


<https://github.com/commercionetwork>





Commercio.network


The Documents Blockchain


<http://commercio.network> info@commerc.io



 **Repositories** 32

 Packages

 People 6

 Teams 3

 Projects

 **Amadeo** 

Commercio Account

Electronically Sign any PDF e XML digital document so no-one can deny having digitally signed the document

[Commercio Account](#)

Commercio Id

Grasp the self sovereign identity and pairwise user connections

[Commercio Id](#)

Commercio Docs

Send a document and prove its paternity, non repudial and integrity

[Commercio Docs](#)

Commercio Sign

Electronically sign any PDF and XML digital document so no-one can deny having digitally signed the document

[Commercio Sign](#)

Commercio Mint

Mint and Burn 1€ a stable coin called Commercio Cash Credit CCC that can be used to pay trasaction fees

[Commercio Mint](#)

NAM

EGIDIO CASATI

egidio.casati@nymlab.it

+39 3459277339

<https://www.nymlab.it>

Thank You