DIZME «THIS IS ME»

The key to digital identity

Nicole Mazzoni

InfoCert
TINEXTA GROUP

Camerfirma
AN INFOCERT COMPANY

LUXTRUST®
Enabling a digital world

Sixtema
TINEXTA GROUP

*"We enable companies to **innovate** the **customer interactions and operational processes** leveraging our portfolio of **trust-based business solutions** and services."*

10
Offices
(2 in Latam)

500
Employees

80 MLN
Turnover

17
Patents

INFOCERT AS A TRUST ENABLER FOR YOUR DIGITAL TRANSACTIONS...

- Provide Trust for Digital Transactions

- Leverage Digital Identity to unlock innovation in business processes

- Bring technology standards into regulatory frameworks

- Cover all Trusted building blocks to deploy end-to-end digital transaction solutions

   Self Sovereign paradigm positioning

- Interoperability is made possible thanks to the dual role of InfoCert, which acts not only as Founding Steward of the Sovrin Network (as well as DIZME Governance Authority) but also as a QTSP in accordance with eIDAS regulation

www.infocert.digital
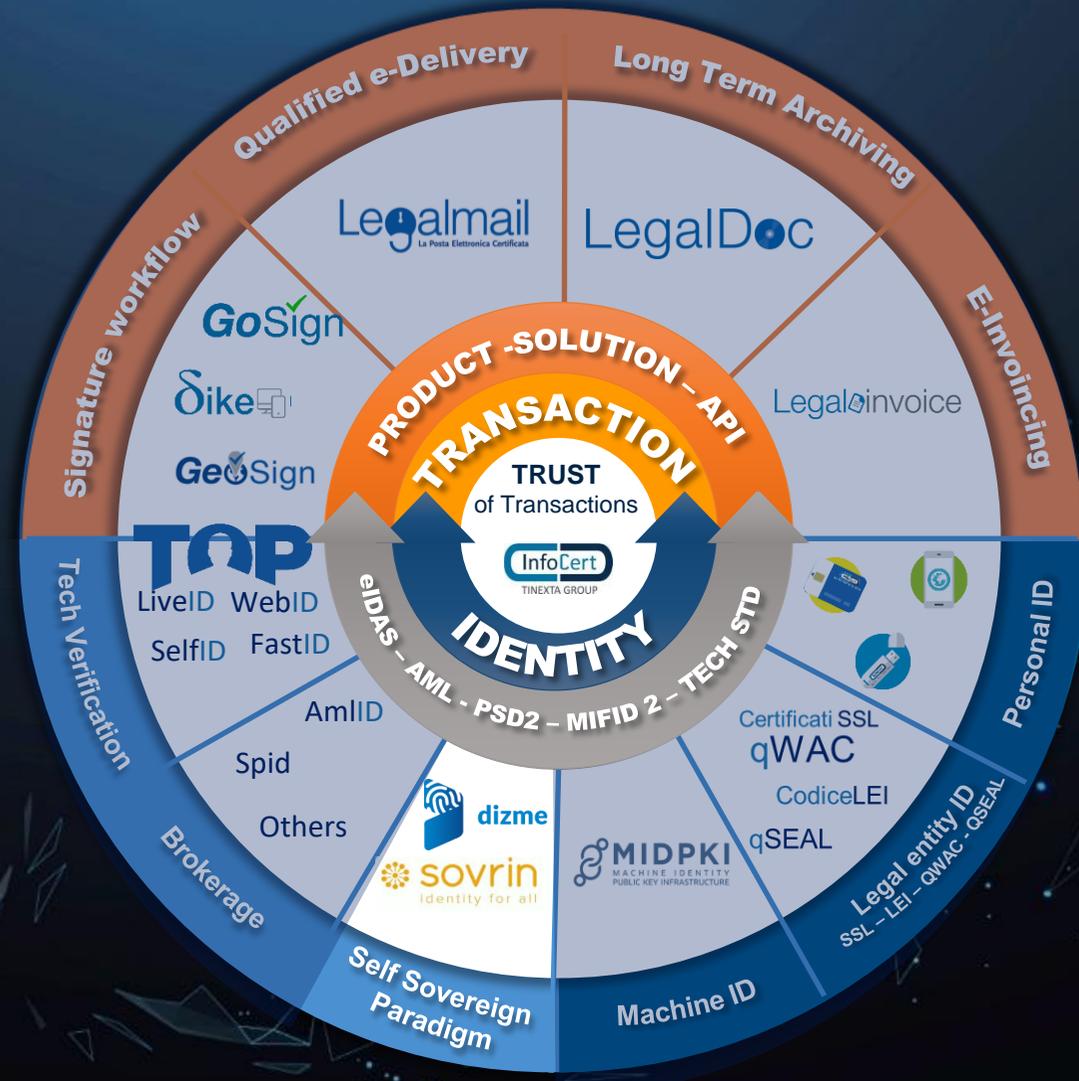
SELF SOVEREIGN IDENTITY 10 PRINCIPLES

SSI Principles places **control** and **ownership** of identity in the hands of the users themselves.

DIZME adopts these principles because it's based on the **Sovrin schema.**

Existence Users must have an independent existence.

Control Users must control their identities.

Access Users must have access to their own data

Transparency Systems and algorithms must be transparent.

Persistence Identities must be long-lived.

Portability Information about identity must be transportable

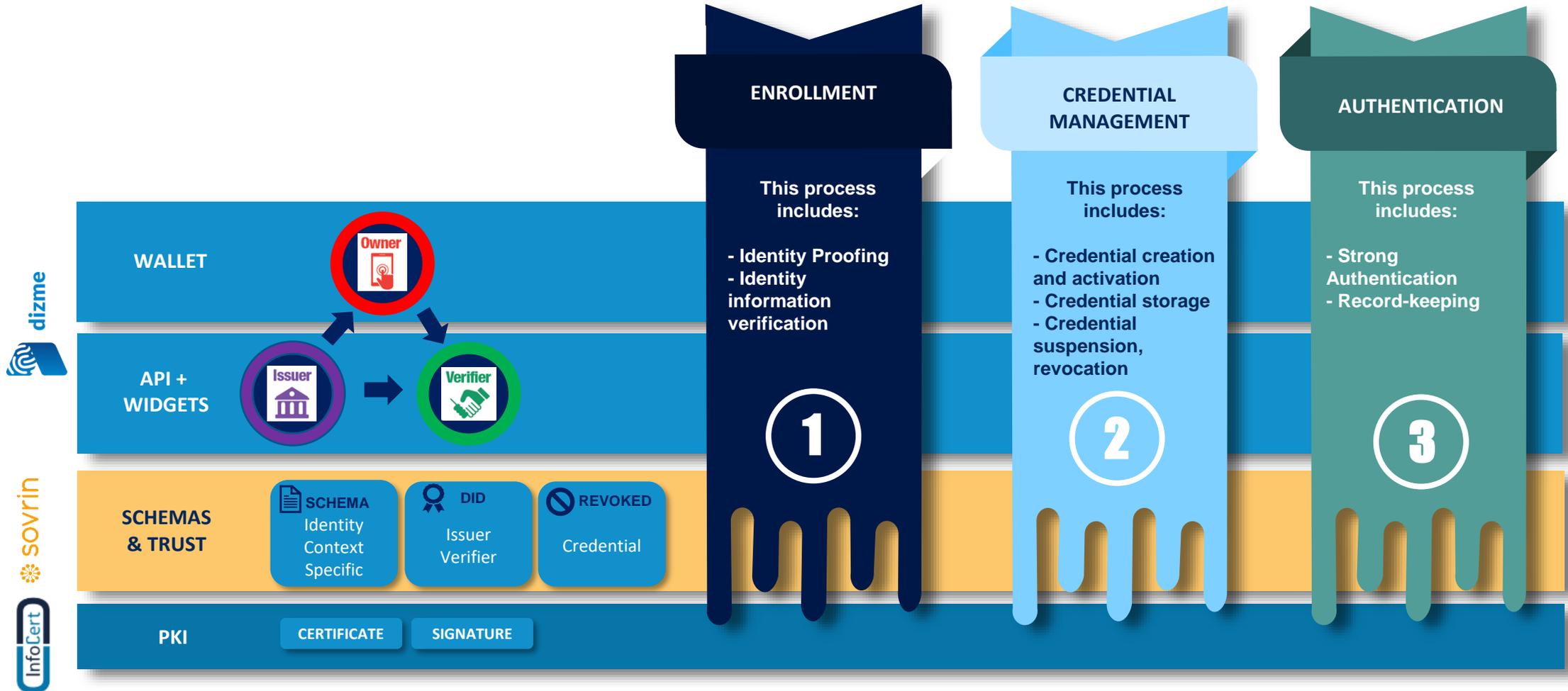**Interoperability** Identities should be as widely usable as possible.

Consent Users must agree to the use of their identity.

Minimization Disclosure of claims must be minimized

Protection The rights of users must be protected

The Path to Self-Sovereign Identity April 25, 2016 (Cristopher Allen)

PLATFORM CAPABILITIES

DIZME's Domain Specific Framework brings SSI to the real world

dizme

WALLET

Owner

API + WIDGETS

Issuer → Verifier

sovrin

SCHEMAS & TRUST

📄 **SCHEMA**
Identity Context Specific

🏅 **DID**
Issuer Verifier

🚫 **REVOKED**
Credential

InfoCert

PKI

CERTIFICATE   SIGNATURE

ENROLLMENT

This process includes:

- Identity Proofing
- Identity information verification

①

CREDENTIAL MANAGEMENT

This process includes:

- Credential creation and activation
- Credential storage
- Credential suspension, revocation

②

AUTHENTICATION

This process includes:

- Strong Authentication
- Record-keeping

③

BITGRAIL CASE STUDY

The bankruptsy of a crypto-currencies exchanger

Customer

Follwing the failure of the crypto-currencies exchange platform, the **bankruptcy curatorship** should have been recognize the creditors.
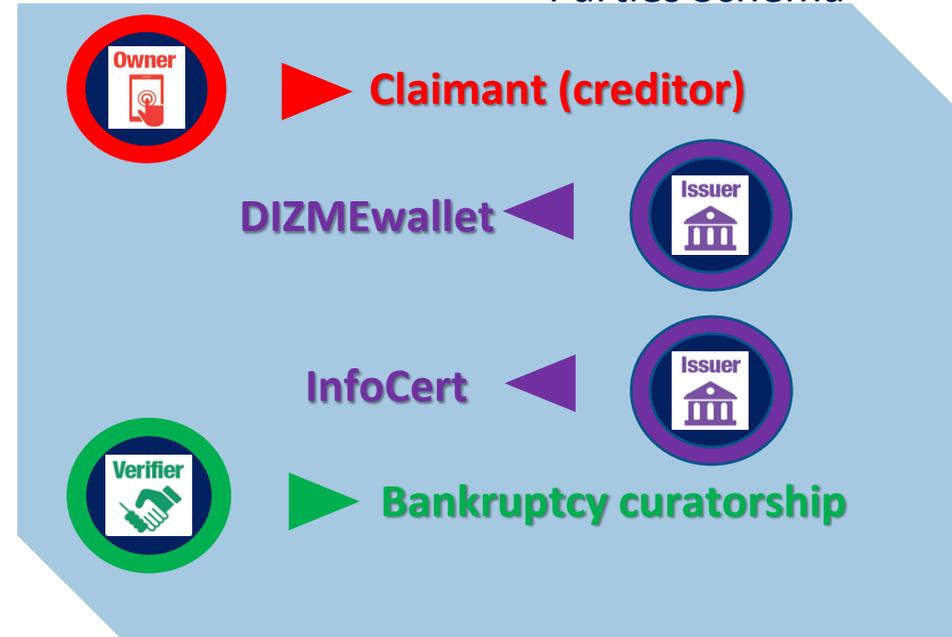
Need

According to the italian bankruptsy law, the claimant must be **correctly identified.**

Subjects

The approximately 80.000 subscribers all round the world should have been called to partecipate to the italian backruptcy procedure.

After a phase of defining the requirements together with the customer, the project **went live** in **January 2020** and, until the first hearing next June, the claimants can take advantage of the service and obtain their DIZME credentials

Parties Schema

Owner ▶ **Claimant (creditor)**

DIZMEwallet ◀ Issuer

InfoCert ◀ Issuer

Verifier ▶ **Bankruptcy curatorship**

Sept-2019 → Jan-2020 → Jun-2020

Requirements collections and development *Claimants identitfication and credentials enrollment*

Go-live

First hearing

HIGH LEVEL USER JOURNEY

The procedure set up for the curatorship aims to transform all applicants from a simple subscription email (no trust in the identification process) to correctly identified subjects according to security level agreed with the customer (curatorship)

1 Sign-up

2 Identification

3 Credential enrollment

4 Sign-in

The claimant goes to the prepared website (www.fallimentobitgra il.it) and begins the registration procedure
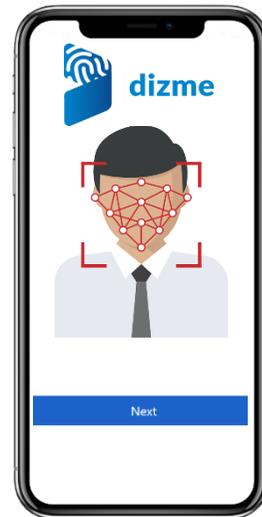
Data and documents collection:
- Liveness detection
- Face matching
- Document recognition

Identity and documents checks;
Credential enrollment

Connects to the curatorship platform and spends his credentials and shares his data, depending on the Level of Security required by the Verifier

DIZME ONBOARDING FOR L0 LEVEL

Contact information verification

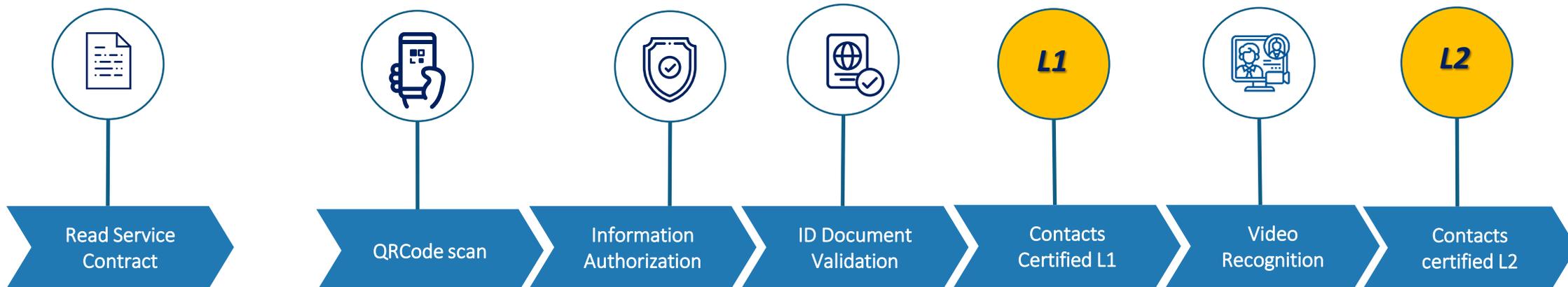| Download APP DIZME | Registration | Send Verification Code | Certification Mobile Number | Certification Email | Contacts Certified |

Document checking e face matching

| Liveness Detection | Country Selection | ID Document Definition | ID Document Capture | Face Matching | Contacts Certified |

USER JOURNEY L1 and L2 PROCESS

Identity verification and enrollment

| Read Service Contract | | QRCode scan | Information Authorization | ID Document Validation | Contacts Certified L1 | Video Recognition | Contacts certified L2 |

PROJECT'S ORIGINALITY AND IT'S OTHERS APPLICATIONS

SSI

eIDAS

GDPR

dizme

For the first time, blockchain technology was used to satisfy a need in the procedural system.
But its applications are innumerable

People can **apply for a loan** by sharing their credit scoring

or ask for an **insurance** by sharing their driving history records. Prove their age online or

share clinical data wherever needed in a secure and reliable way**.**
Enriching eIDs with attributes leads to rewards and triggers a virtuous circle by attracting more users into the network.
Data verifications and transfer happens instantaneously and in full respect of EU privacy policies.