Paving the road to self-sovereign identity with blockchain: The Hellenic Distributed Ledger Technology Infrastructure (ELEDGER) & EBSI Conformant wallets

Dr. Konstantinos Votis, Senior Researcher
Head of Blockchain Lab, CERTH/ITI

https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/

CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

ELEDGER

The Commission has decided to award a grant, under the terms and conditions set out in the Special Conditions, the General Conditions and the other Annexes to the Agreement, number 2020-EL-IA-0079.

iti Information Technologies Institute

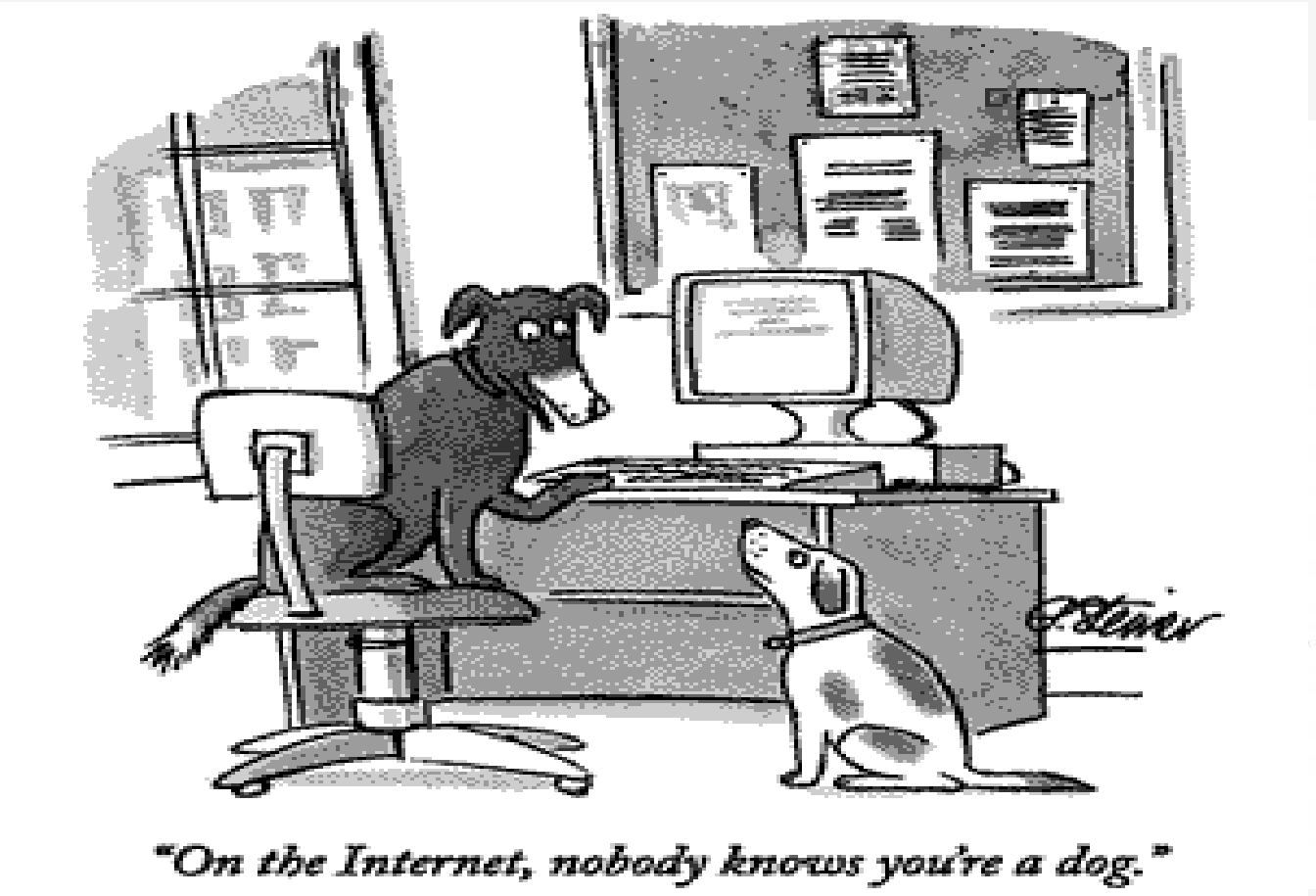
Self-Sovereign Identity (SSI)

Brief Introductory Note

The Digital Identity Problem

…quantity over quality

- Every platform makes users to enroll themselves for accessing the services.
- Reality is that multiple identities stored in proprietary systems refer to the same person.
- These identities are based on user's inputs and their validation may be inaccurate or obsolete.
- Companies perform the same procedure which is vastly costly.



The Digital Identity Problem

…disclosing too much

- There are unnecessary information that users share for a verification.
- Simple questions tend to require more information.
- The answer to the question if a person is adult is simply a yes or no.
- Current identities require the user's date of birth to verify the question revealing the actual age.
- Data disclosure should be minimised to the necessary.

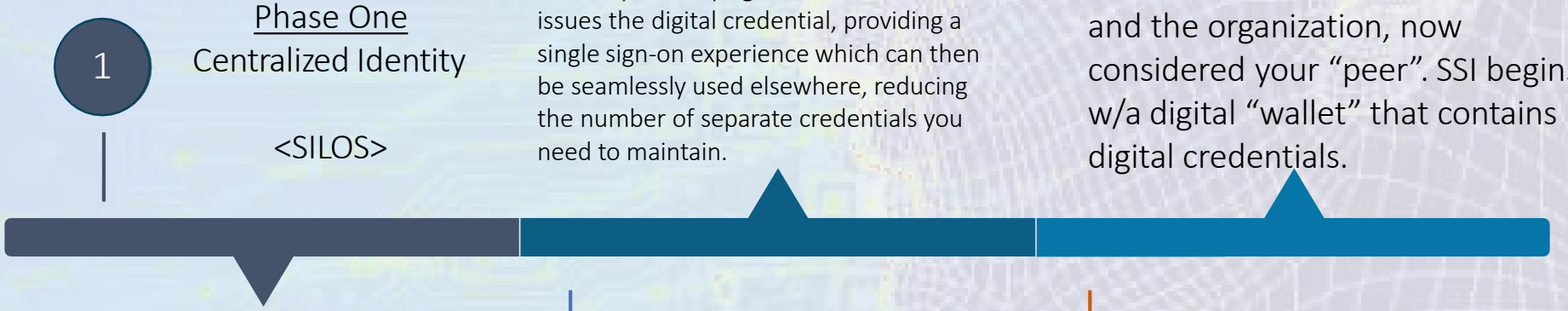
When we think of digital identity we therefore need to see it not as a single thing. It is rather the sum total of all the attributes that exist about us in the digital realm, a constantly growing and evolving collection of data points.

Definition digital identity

EU blockchain observatory report on digital identity and blockchain
https://www.eublockchainforum.eu/sites/default/files/report_identity_v0.9.4.pdf

Identity Evolution

The models for online identity have advanced through three broad stages since the advent of the Internet



1

Phase One
Centralized Identity

<SILOS>

Traditional “siloed” identity is simple: an organization issues to you a digital credential that you use to access a service. Trust between you and the organization is typically established through shared secrets, usually via a username and a password.

2

Phase Two
Federated Identity

<THIRD-PARTY IDP>

The IDP relationship model adds a third-party to act as an “identity provider” between you and the organization or service you’re trying to access. The IDP issues the digital credential, providing a single sign-on experience which can then be seamlessly used elsewhere, reducing the number of separate credentials you need to maintain.

3

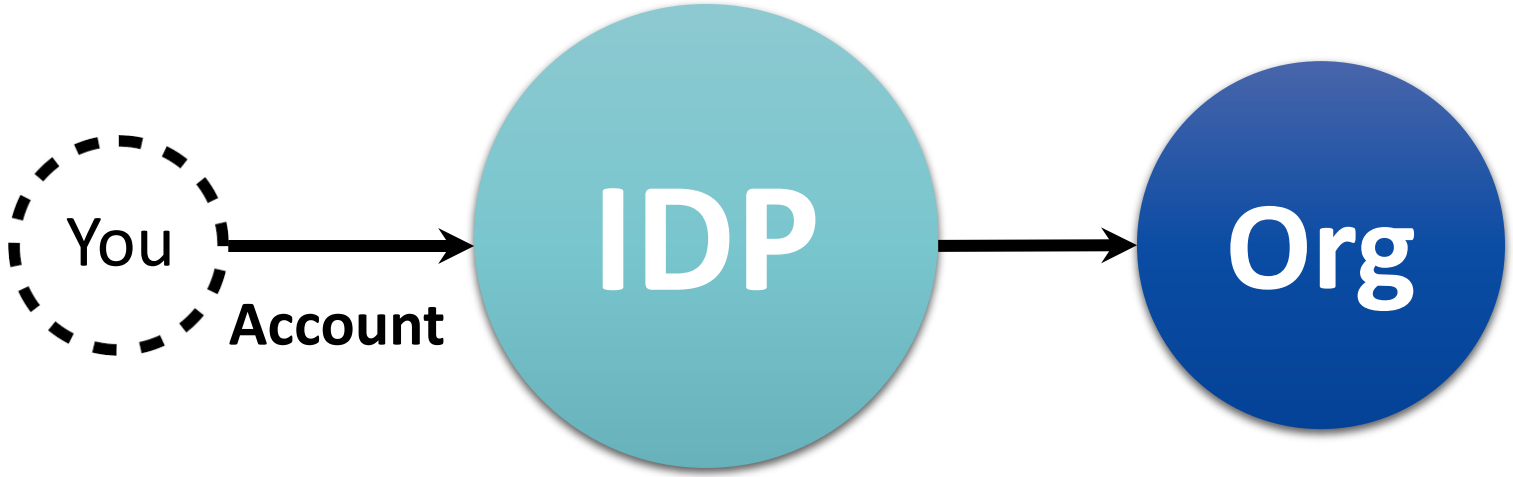
Phase Three
Self-Sovereign Identity

<PEER2PEER>

Self-sovereign identity is a two-party relationship model, with no third party coming between you and the organization, now considered your “peer”. SSI begins w/a digital “wallet” that contains digital credentials.

TINEXTA

Federated Identity Model



Standards:

SAML

OAUTH 2

OpenID Connect

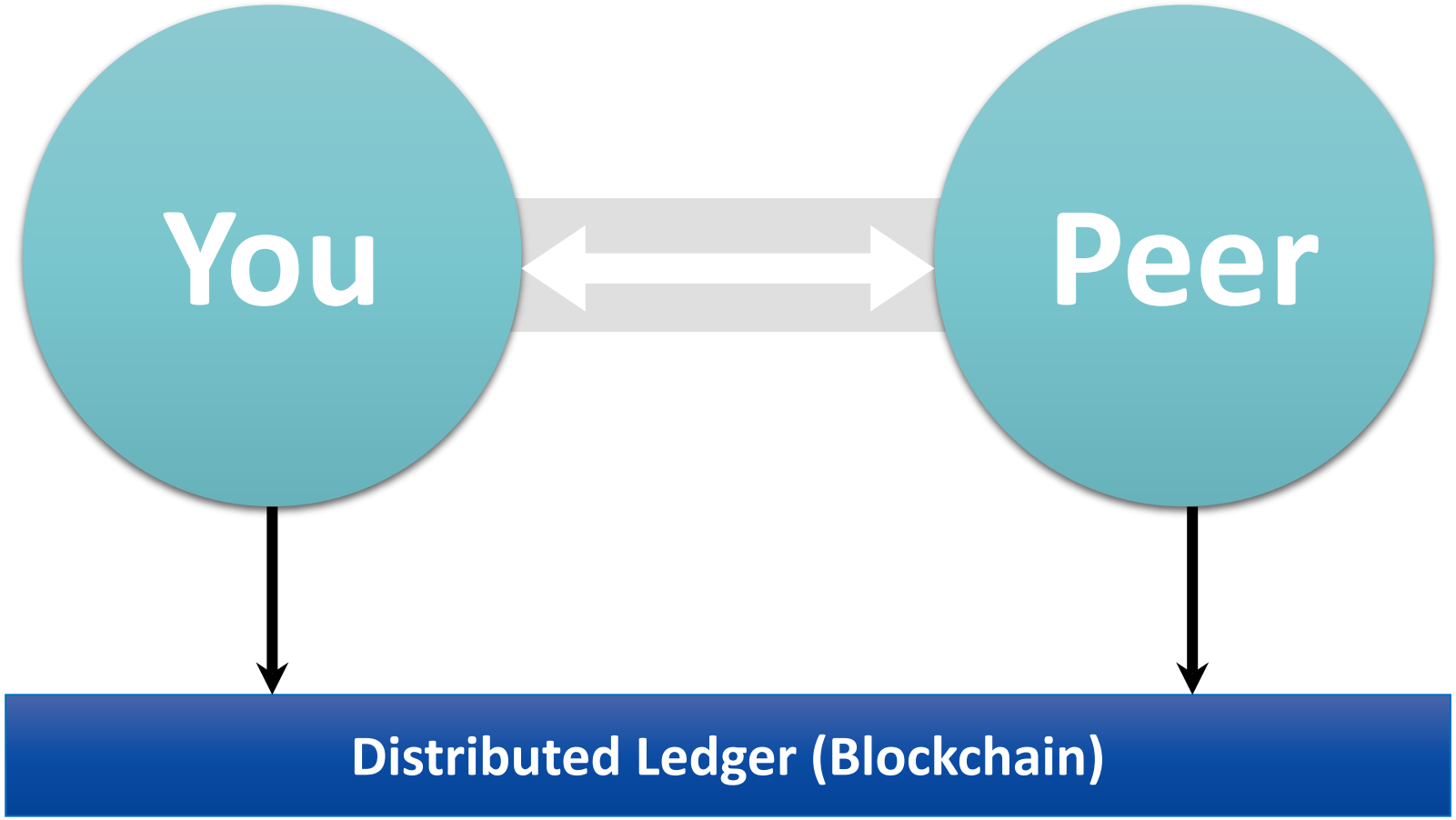
Pain Points

- Registration w/ Username & Password
  - Weak security (low entropy)
  - Password management
- Different login credentials per online service
- **No control** over what data is shared
- Identity (credentials) depend on issuer liveness & permissions
  - Think: Facebook/Google ban your account
- Financial incentive to collect & sell user data:
  - All kinds of privacy violations
- Centralized storage of credentials:
  - Hackers love it
  - No fault-tolerance

‘Self-Sovereign Identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity.’

— **Christopher Allen**

Self-Sovereign Identity (SSI) Model



10 PRINCIPLES OF SELF-SOVEREIGN IDENTITY

existence

control

access

transparency

persistence

portability

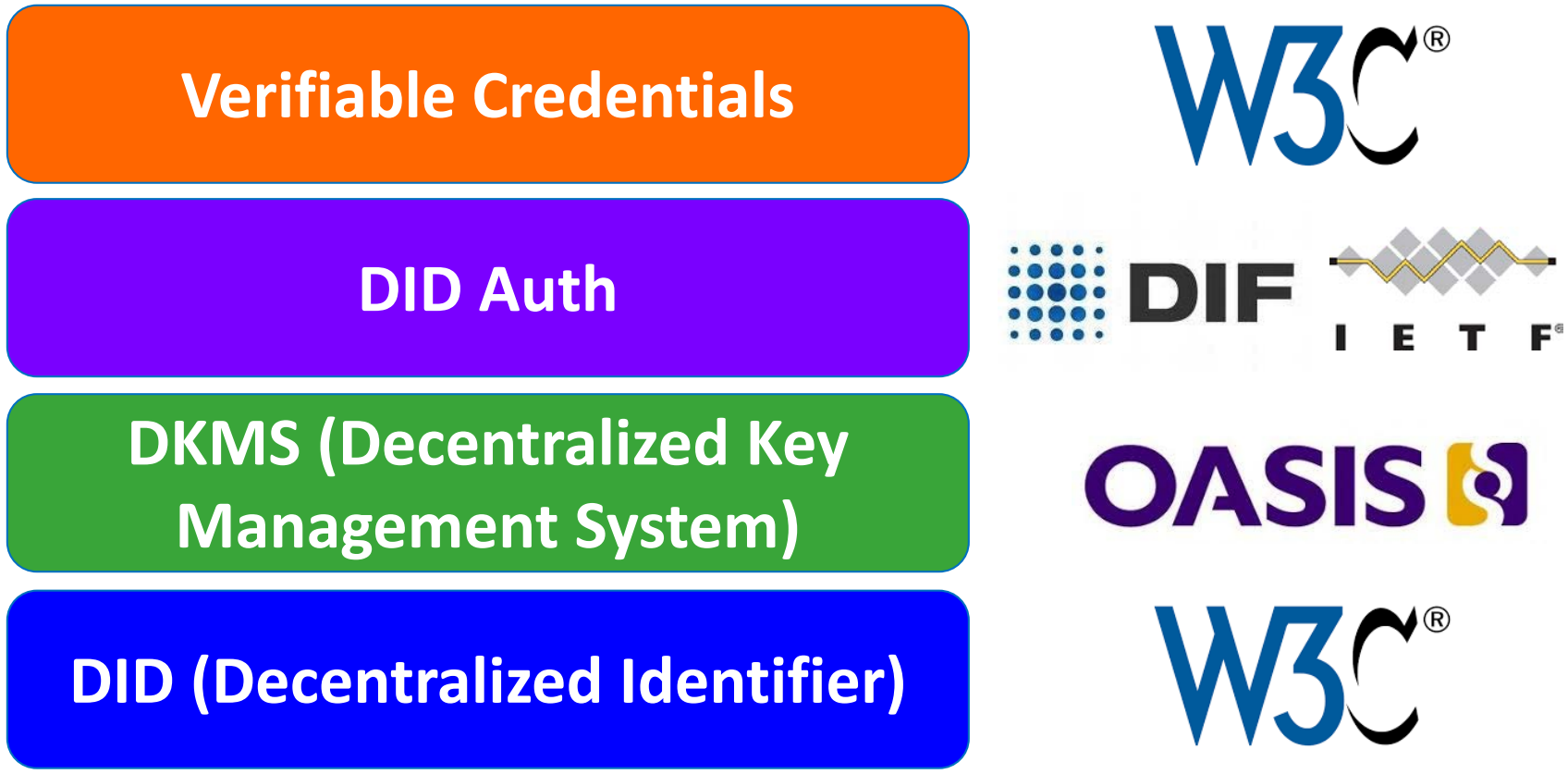
interoperability

consent

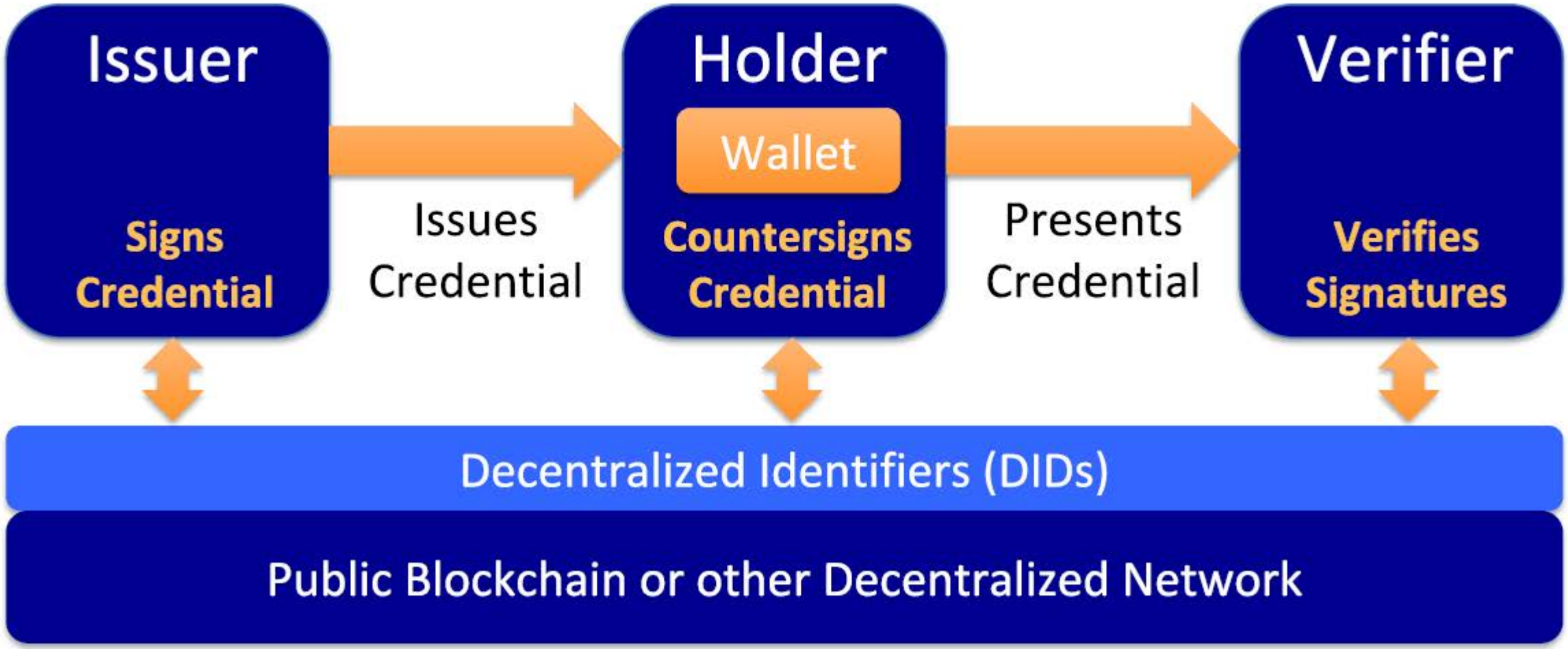
minimization

protection

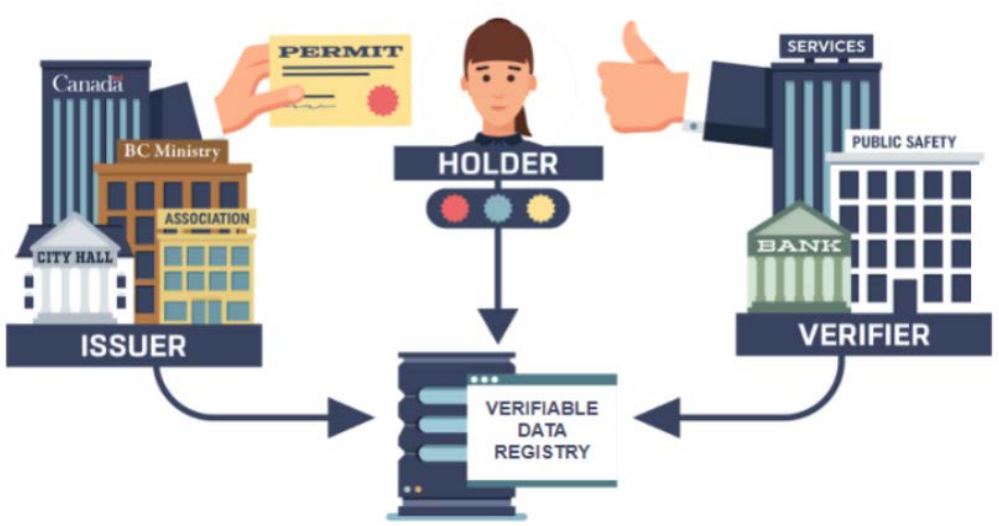
Standards

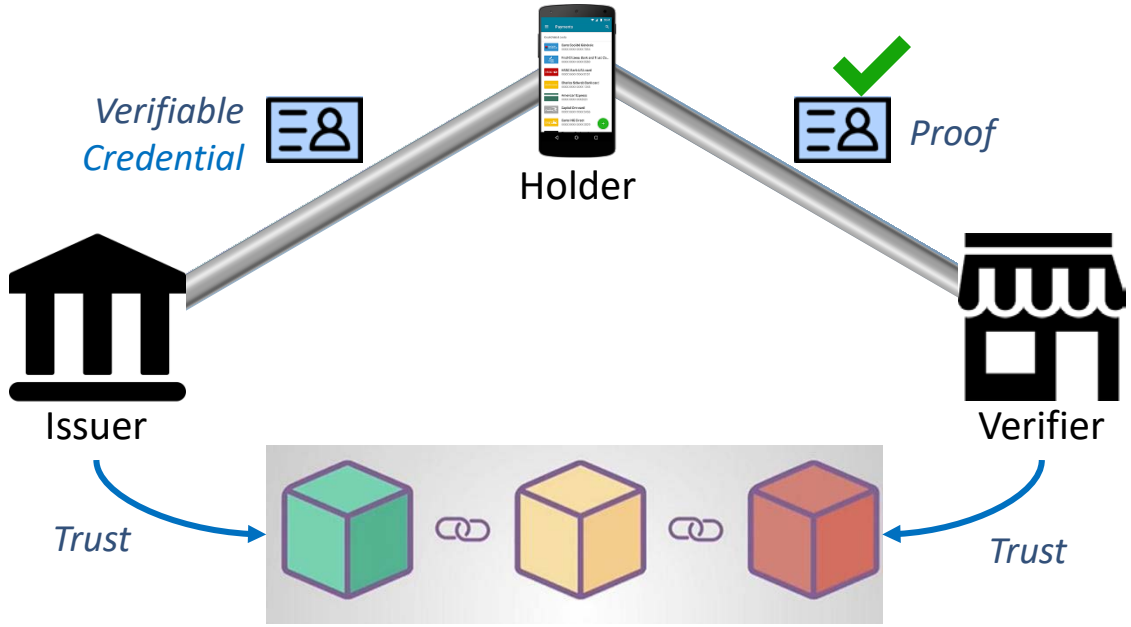

Verifiable Credentials
DID Auth
DKMS (Decentralized Key Management System)
DID (Decentralized Identifier)
W3C®
DIF
IETF
OASIS
W3C®

SSI Architecture: Overview



From Physical to Digital Credentials





Blockchain technology
as a secure root of trust

EBSI & EBSI use cases

EBSI, European Blockchain Service Infrastructure

European Commission

EBSI use cases

Overview of functionalities

European Self-Sovereign Identity

Implement a generic Self-Sovereign Identity capability, allowing users to create and control their own identity without relying on centralized authorities.

Use case: European Self-Sovereign Identity

Overview of core functionalities

Registration

Users can request their own self-sovereign identity (i.e. users control what is shared with whom)

Issuers can request their registration

Authentication

Users can authenticate using a strong authentication online (i.e. national eID)

Verification

Users can:

- Request / obtain / present verifiable claims and credentials
- Request verifiable consent / mandate

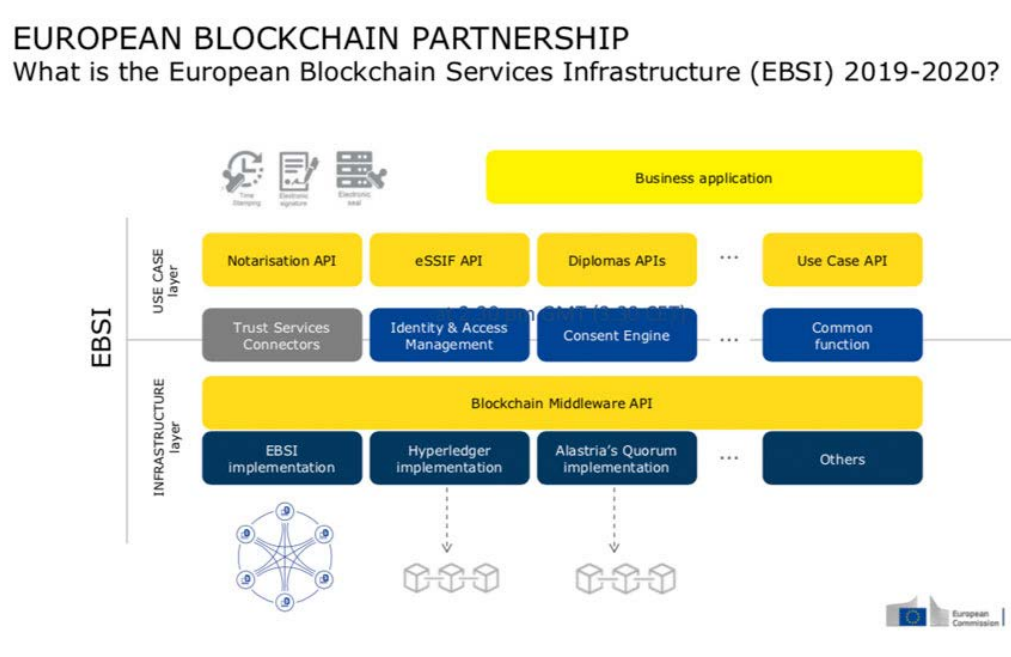
Issuers can:

- Verify identifications
- Suspend / revoke credentials

European Blockchain Services Infrastructure

…investing in Blockchain

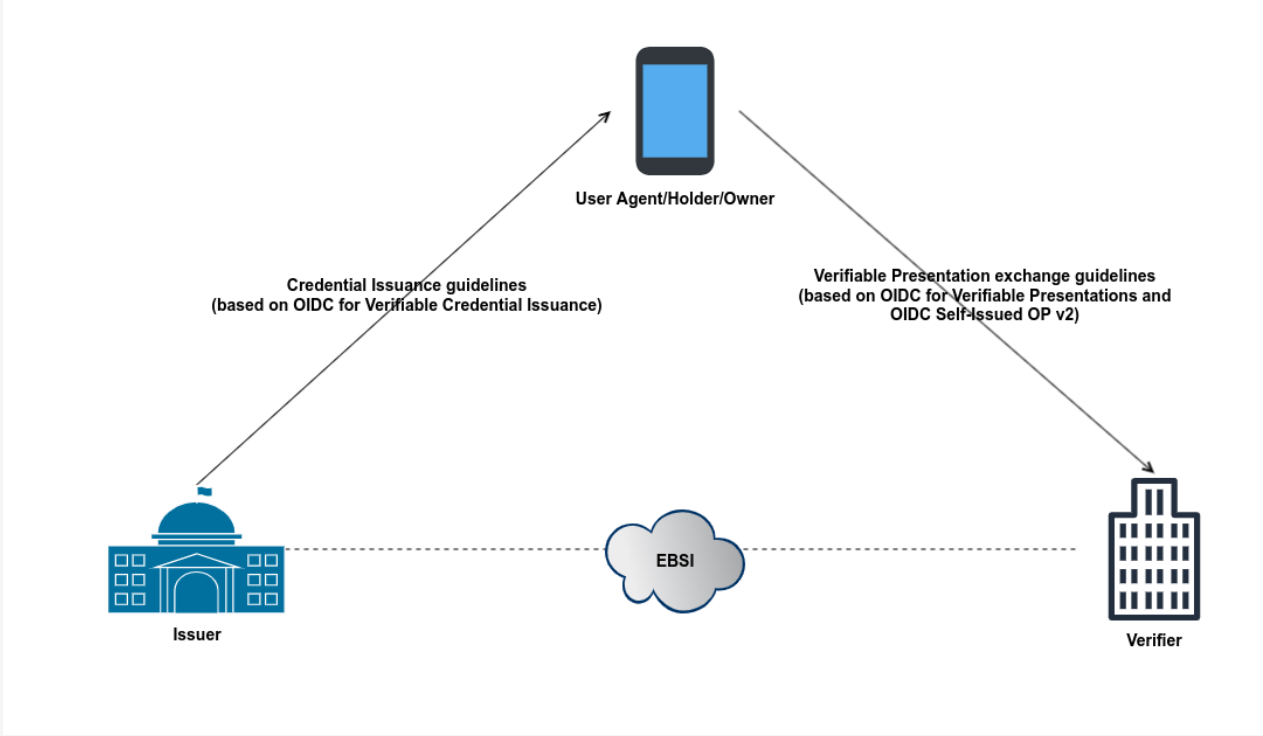
eLedger Connected European Facility Project



2 official EBSI installations (GRNET, CERTH)

EBSI conformant wallet & identities

- EBSI requires the use of Decentralised Identifiers (DIDs) as the cornerstone of self-sovereign identity (SSI).
- Promoting the use of openness with open standards use from W3C. Specifically, Credential Issuance is compliant with OIDC 4 Verifiable Credential Issuance.
- Identities are a core component in every service.



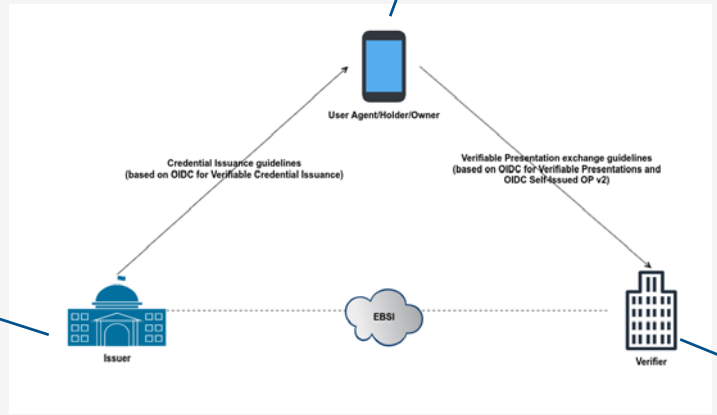
EBSI Verifiable Credentials – OpenID Connect

On January 23, CERTH's digital wallet had its compliance report published on EBSI.

SSI roles forming a triangle

Identity owner: The person who controls the digital identity. They decide what information to share and whom accesses them.

Issuer: any entity that creates and issues digital credentials. They are responsible for verifying the identity and publish a digital credential.



Verifier: any entity that verifies the authenticity of the document presented by the identity owner.

Comparing contemporary digital identities with SSI

Access

Access can phase barriers for marginalized communities since they are based on traditional identity systems. **SSI** aims to create a system that is inclusive and accessible to all individuals, regardless of their background or circumstances.

Trust

Individuals put their trust on third parties to manage identities and underlying data. On the other hand, **SSI** have individuals to verify their identities using trusted credentials.

Privacy

Personal information are shared with third-parties. **SSI** allows individuals to control the information to share and with whom.

Security

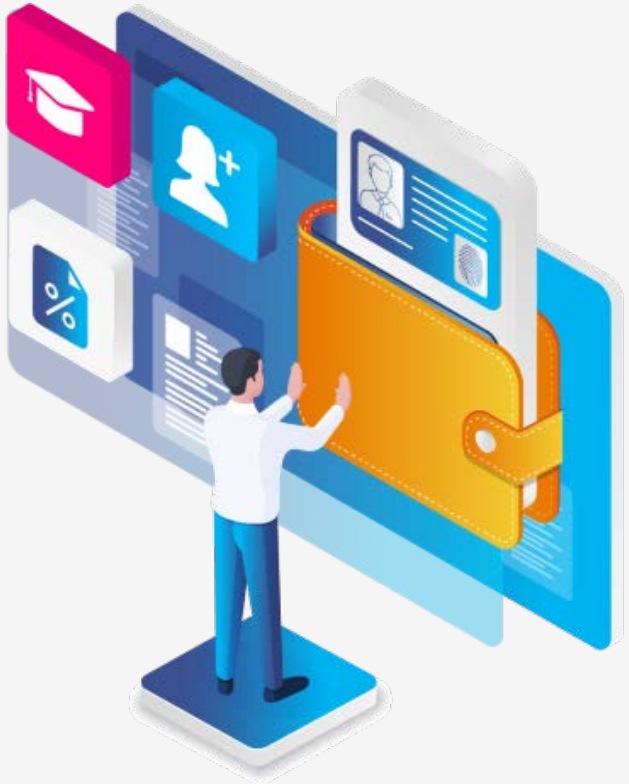
Traditionally, centralised entities are a point for attacks (hacks, data breaches). **SSI** uses cryptographic technology to secure digital identities and prevent unauthorized access.

Interoperability

Contemporary systems' identities are in siloes and are not transferable. **SSI** is based on standardisation for usability across platforms.

EBSI conformant wallet requirements

- Support for the EBSI network
- Compliance with EBSI standards
- Secure storage of private keys
- User control over data
- Interoperability
- Compliance with data protection regulations



Openness, security, and cross-border applicability are essential.

CERTH/ITI Self-Sovereign Identity (SSI)

Solution Overview & Use Cases

On January 23, CERTH's digital wallet had its compliance report published on EBSI.

Technologies

Self-Sovereign Identities → Security, Controllability and Portability of an identity → No Central Authority

SSI Decentralized Identifiers (DIDs) - unique global identifiers, cryptographically verifiable

SSI Verifiable Credentials (VCs) - Machine-readable digital credentials, cryptographically verifiable, tamper-proof, no need for the issuer to mediate the presentation and verification of the VC

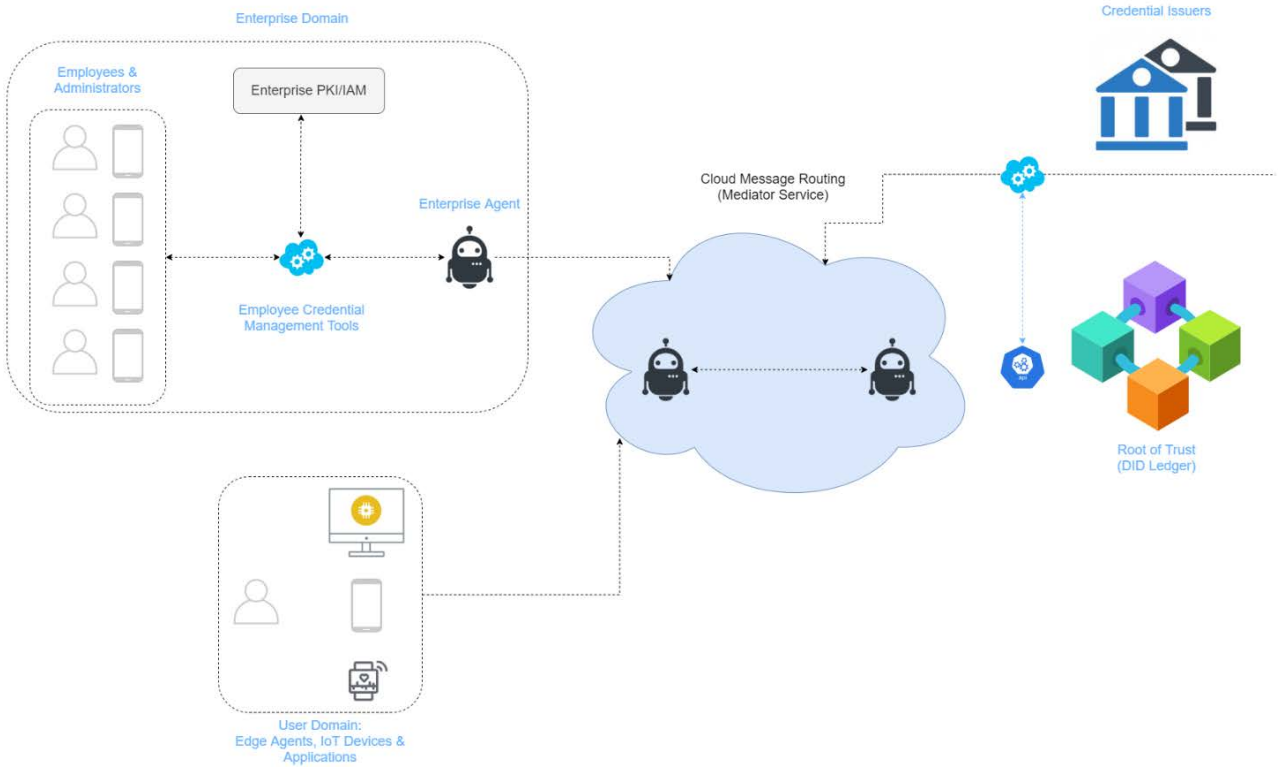
SSI Zero-knowledge Proofs (ZKP) - prove the truthfulness or possession of a claim to a verifier without conveying any further information about the claim itself or revealing the actual claim

Hyperledger Aries (HLA) - Shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials.

Hyperledger Indy (HLI) - Interoperable distributed ledger for purpose-built for privacy-preserving digital identities.

Solution Benefits & Overview

- It is a set of services that allow implementing Self-Sovereign Identity systems in order to establish digital trust
- It allows entities to share data between each other in a trustworthy, standardized and privacy-preserving way
- Using these services, the entities are able to:
  - Obtain secure wallets for controlling and managing their DIDs and VCs
  - Create and use private communication channels based on DIDs for information exchange
  - Issue, prove and verify VCs

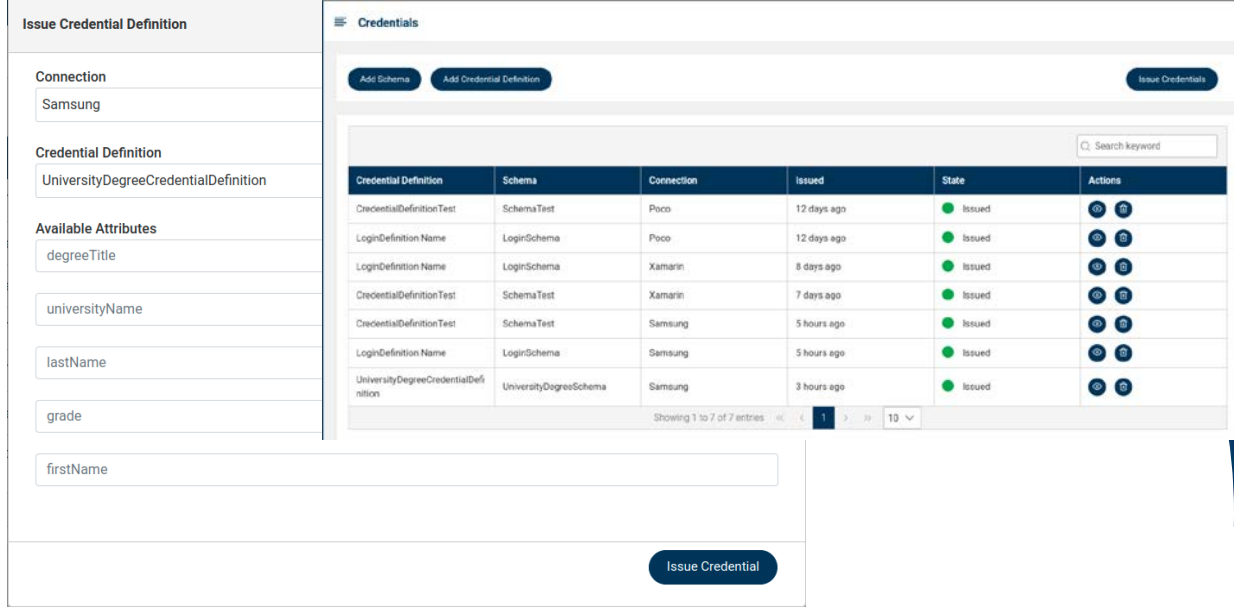


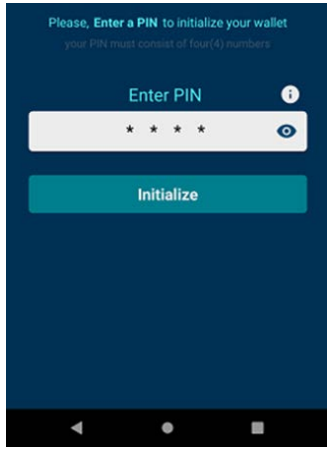
Solution Components

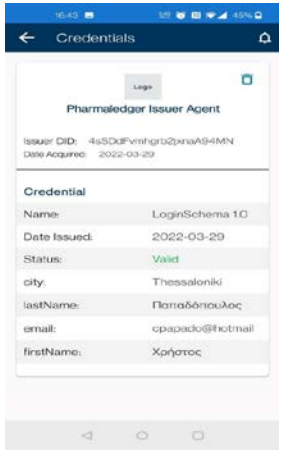
- Credential Issuer Platform:
  - Issue, revoke & verify credentials
- Credential Holder (Web & Mobile Wallet):
  - Receive, prove & verify credentials

Ancillary Services:

- Mediator Service
  - Cloud messaging mix network (similar to Tor).
- Verifiable Credentials Verification Service (VCVS):
  - Bridge between credentials & OAuth 2.0 & OpenID Connect as a service







Transparent Management of Public Accounts

OVERVIEW

Problem statement

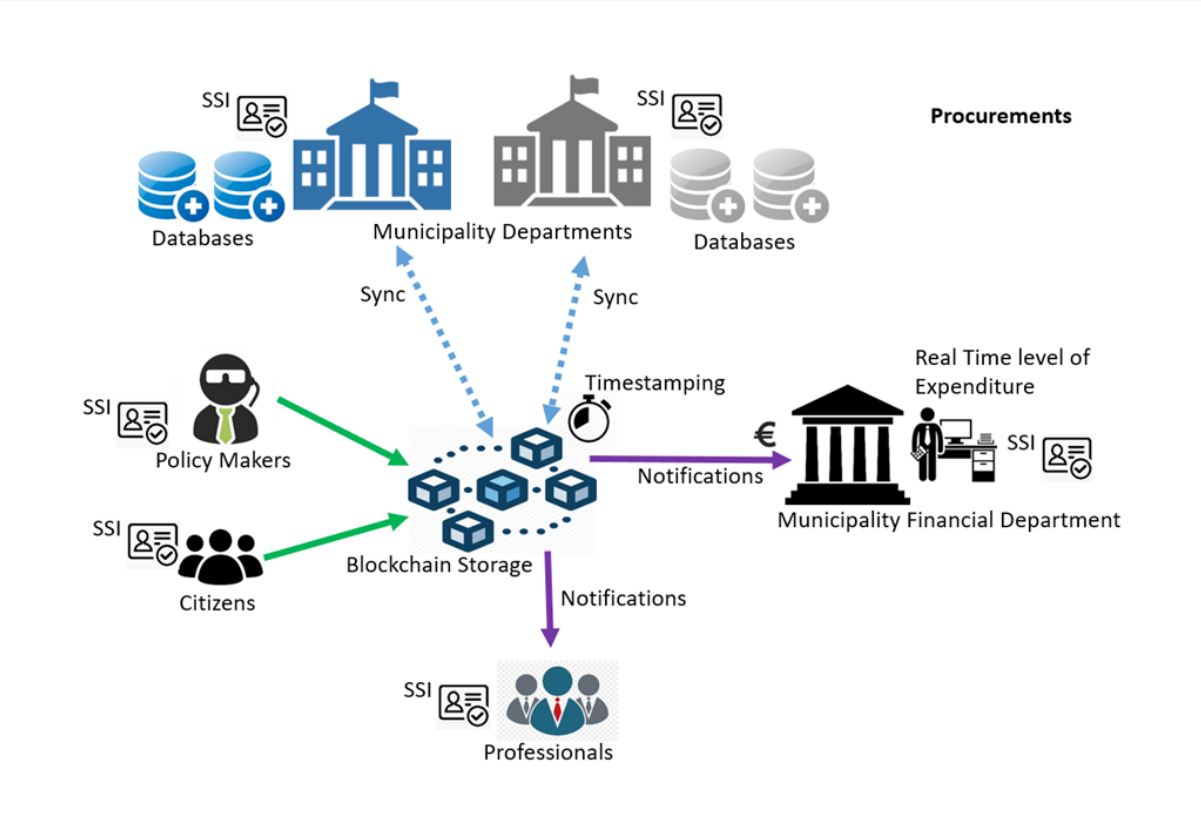
- **Time-consuming** and **error-prone work** involved around procurements
- **Fragmented process**, limited use of technology, communication silos among civil servants and departments
- **Lack of transparency** about timeline, procedures, requirements and fund allocation
- **Limited citizen participation** in decision making processes

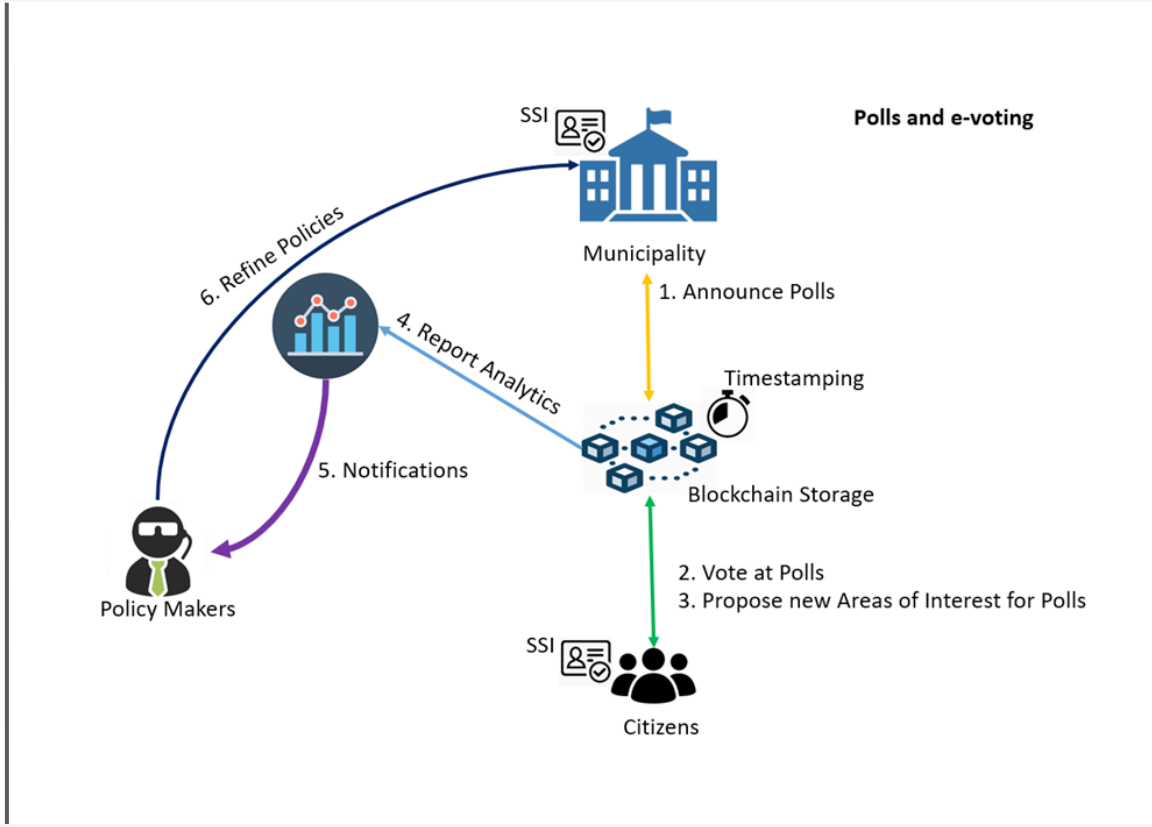
CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS

MUNICIPALITY OF KATERINI

Transparent Management of Public Accounts

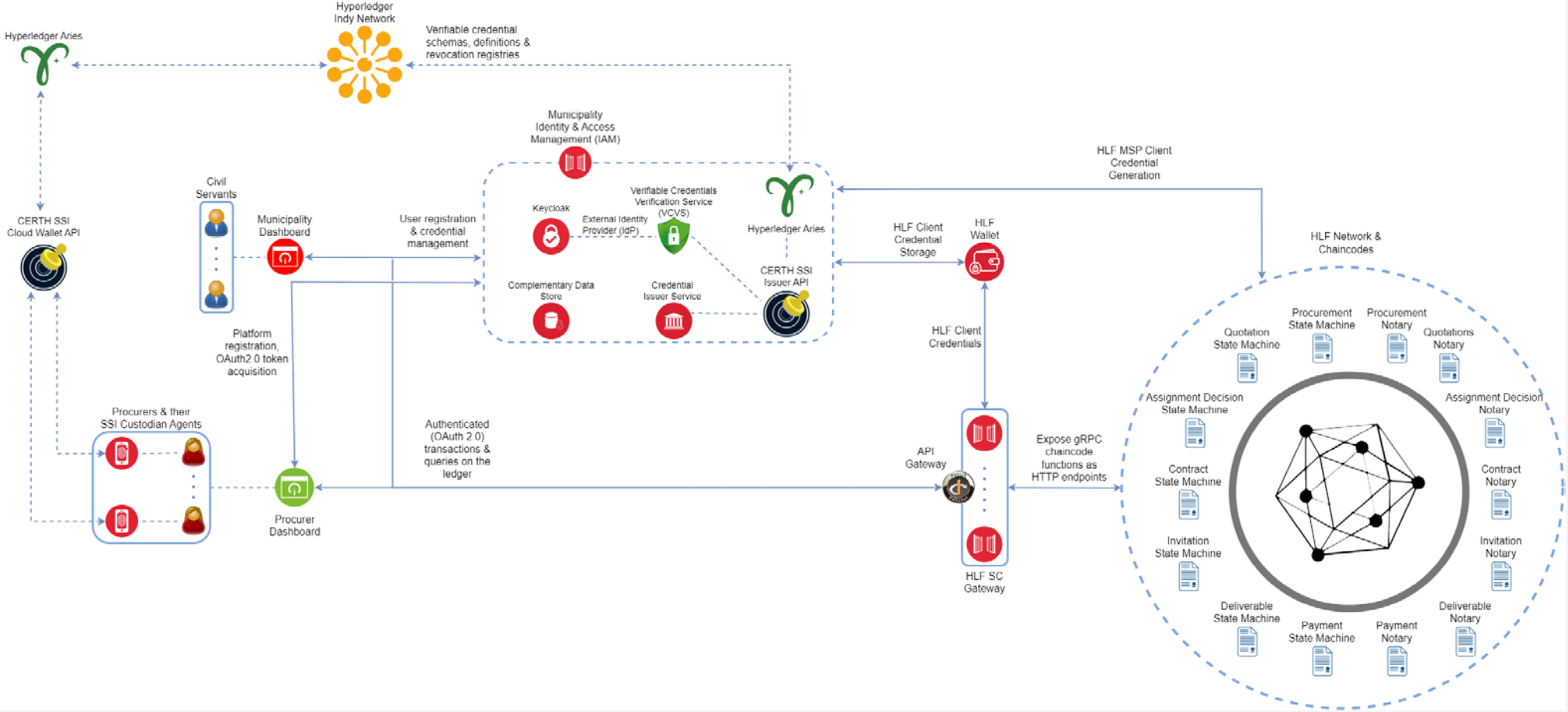
ACTORS





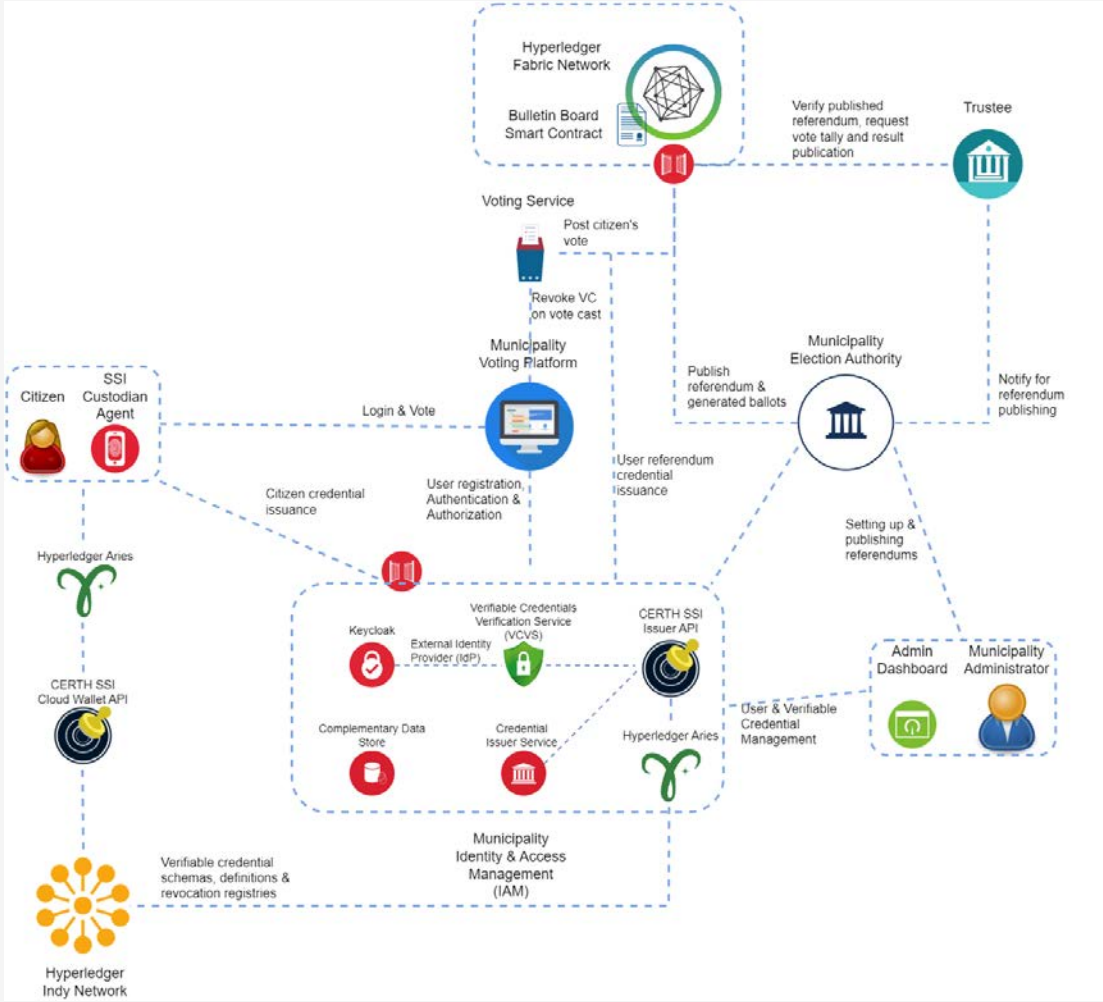
Transparent Management of Public Accounts

PROCUREMENTS



Transparent Management of Public Accounts

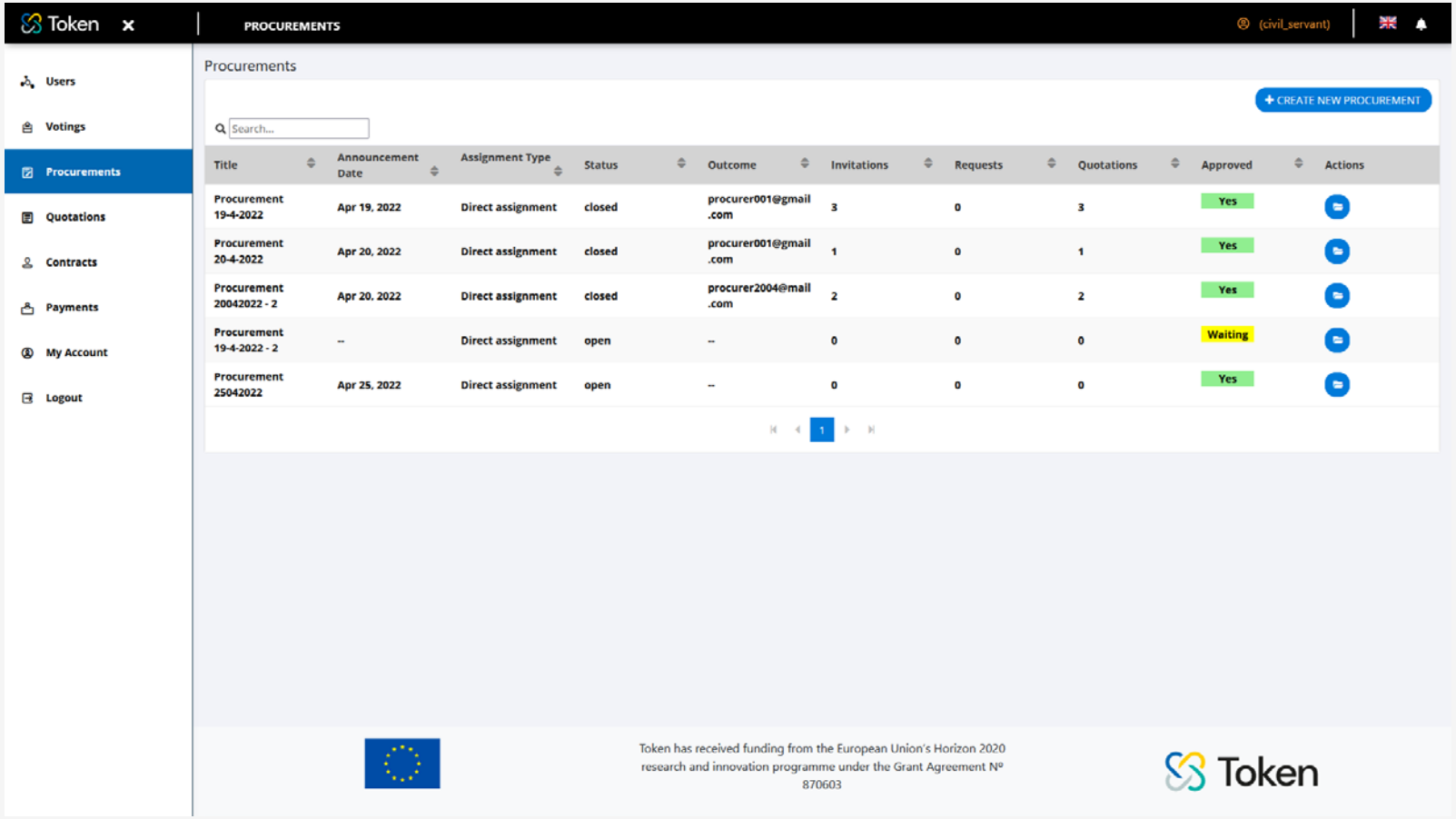
E-VOTING



Transparent Management of Public Accounts

VIEWS

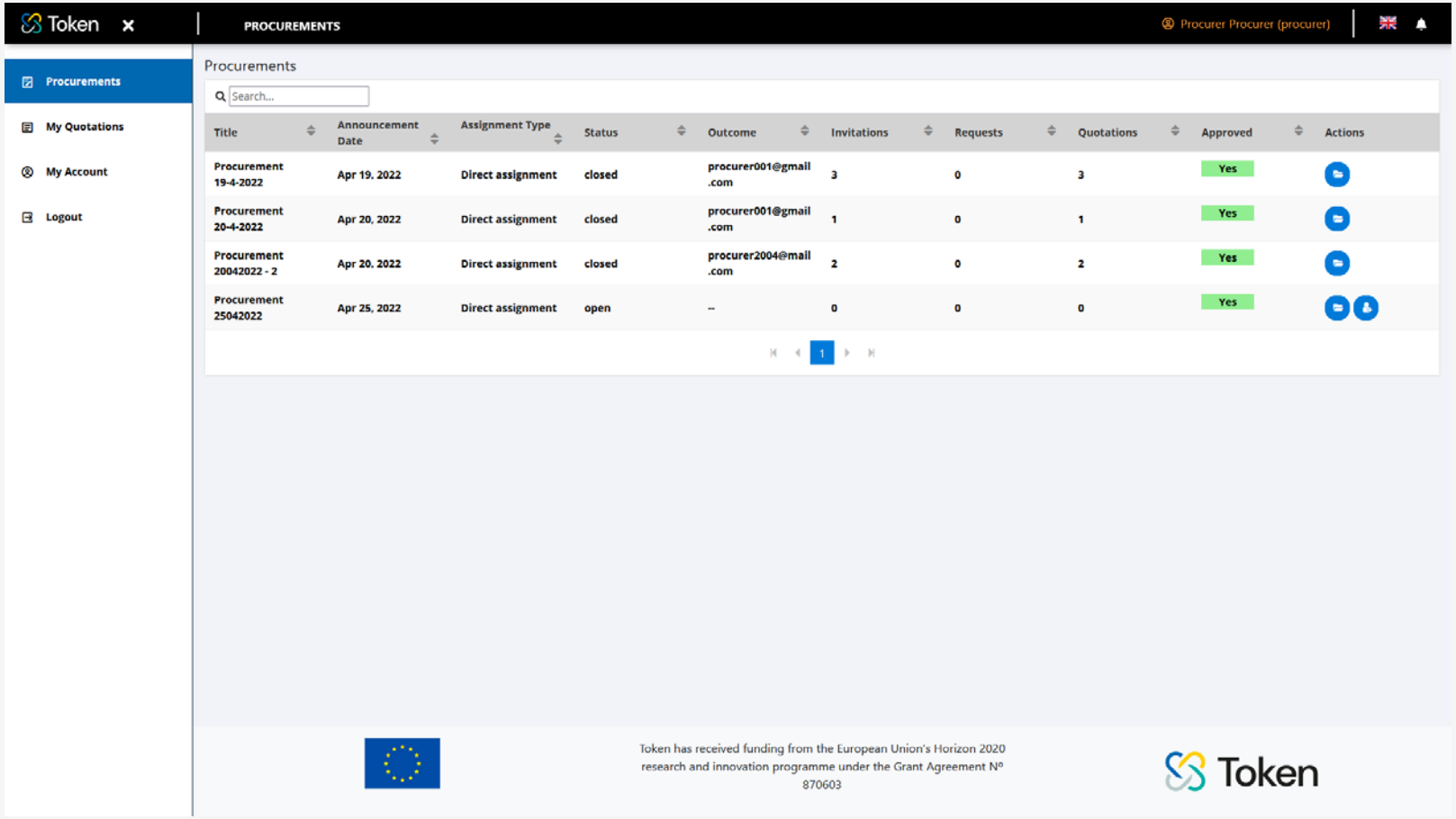
(Civil Servant – Procurement Process)



Transparent Management of Public Accounts

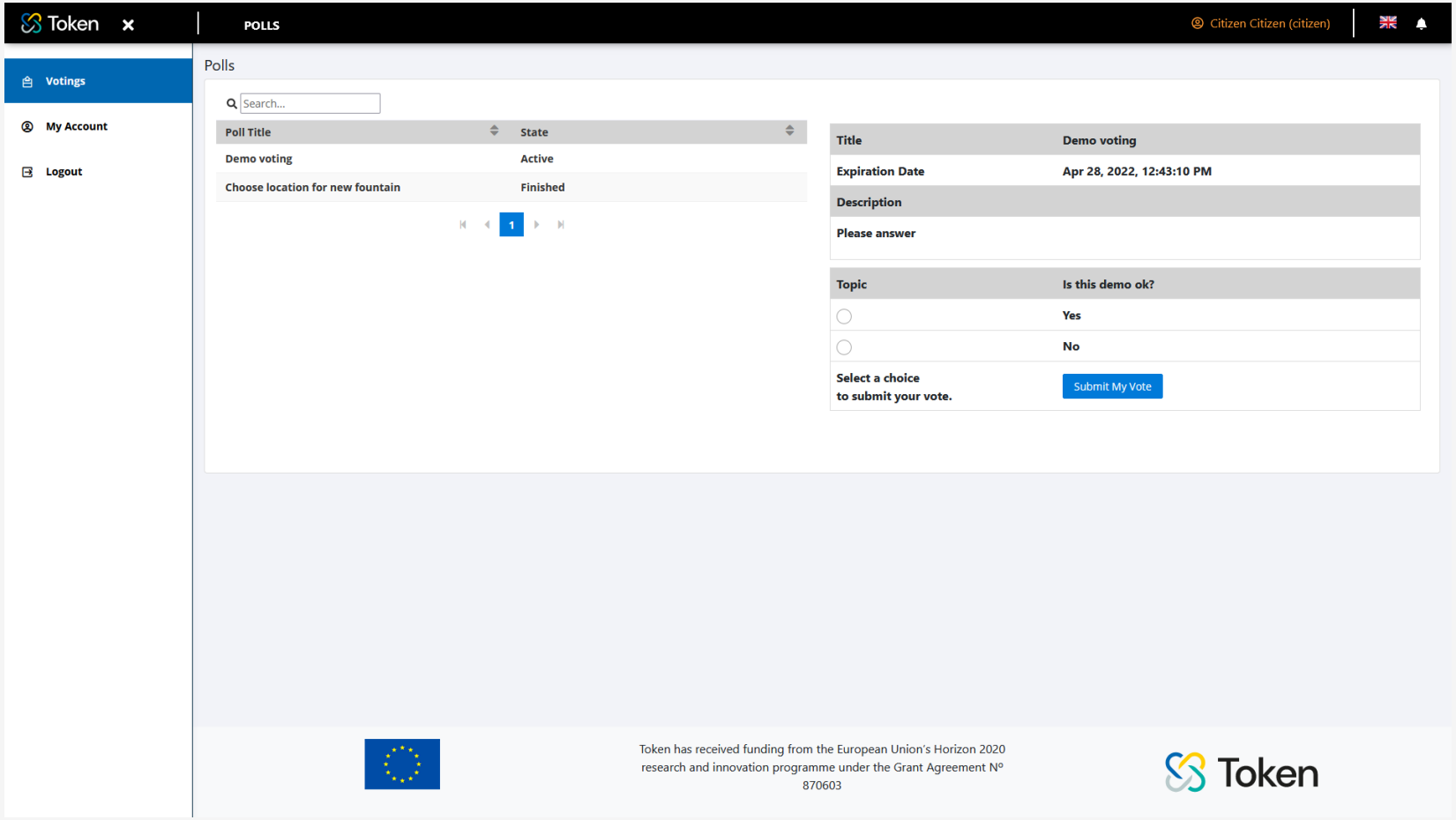
VIEWS

(Procurer – Procurement Process)



Transparent Management of Public Accounts

VIEWS
(Citizen – Evoting Process)

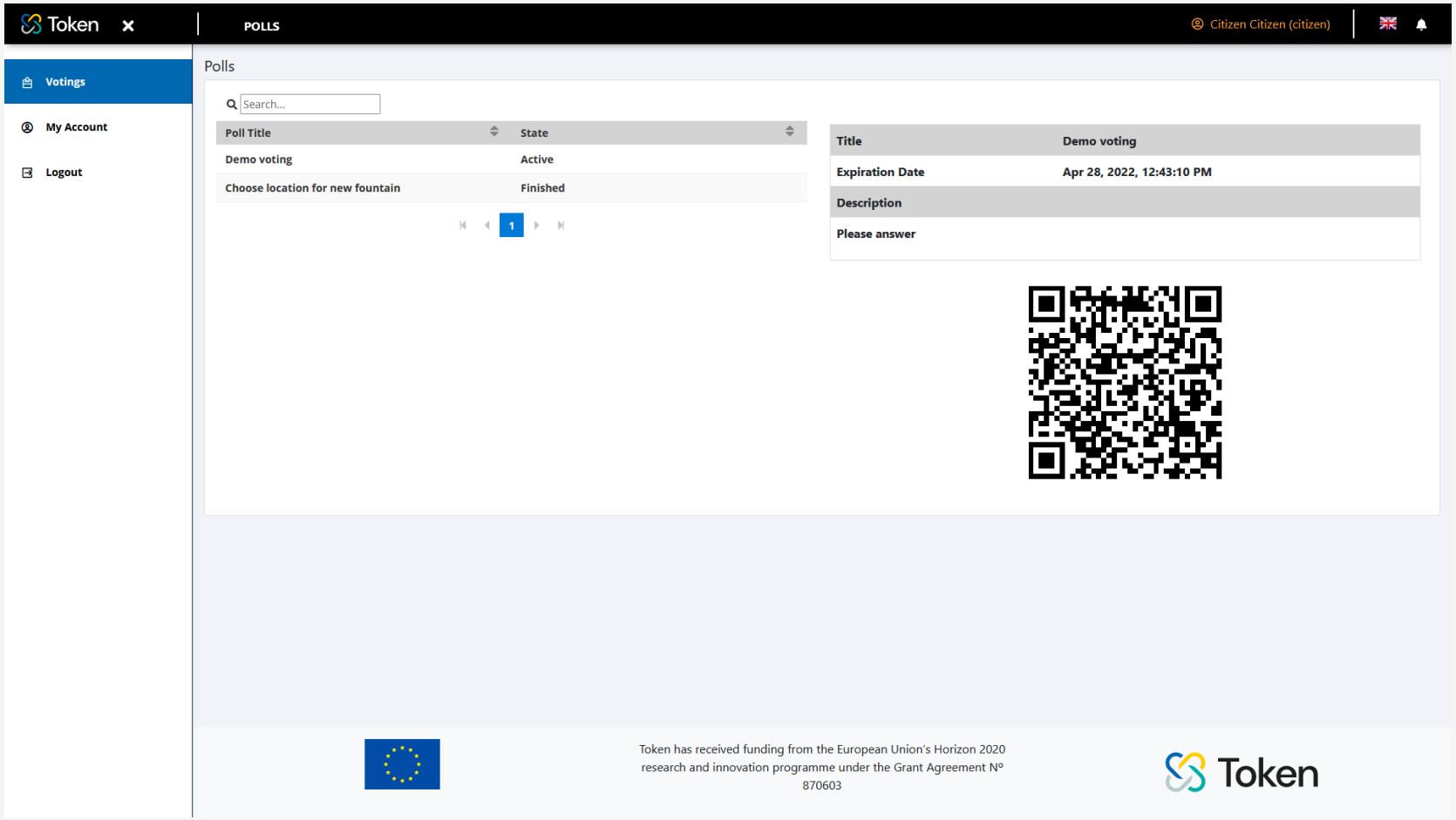


Token has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement Nº 870603

Token

Transparent Management of Public Accounts

VIEWS (Citizen – Evoting Process)

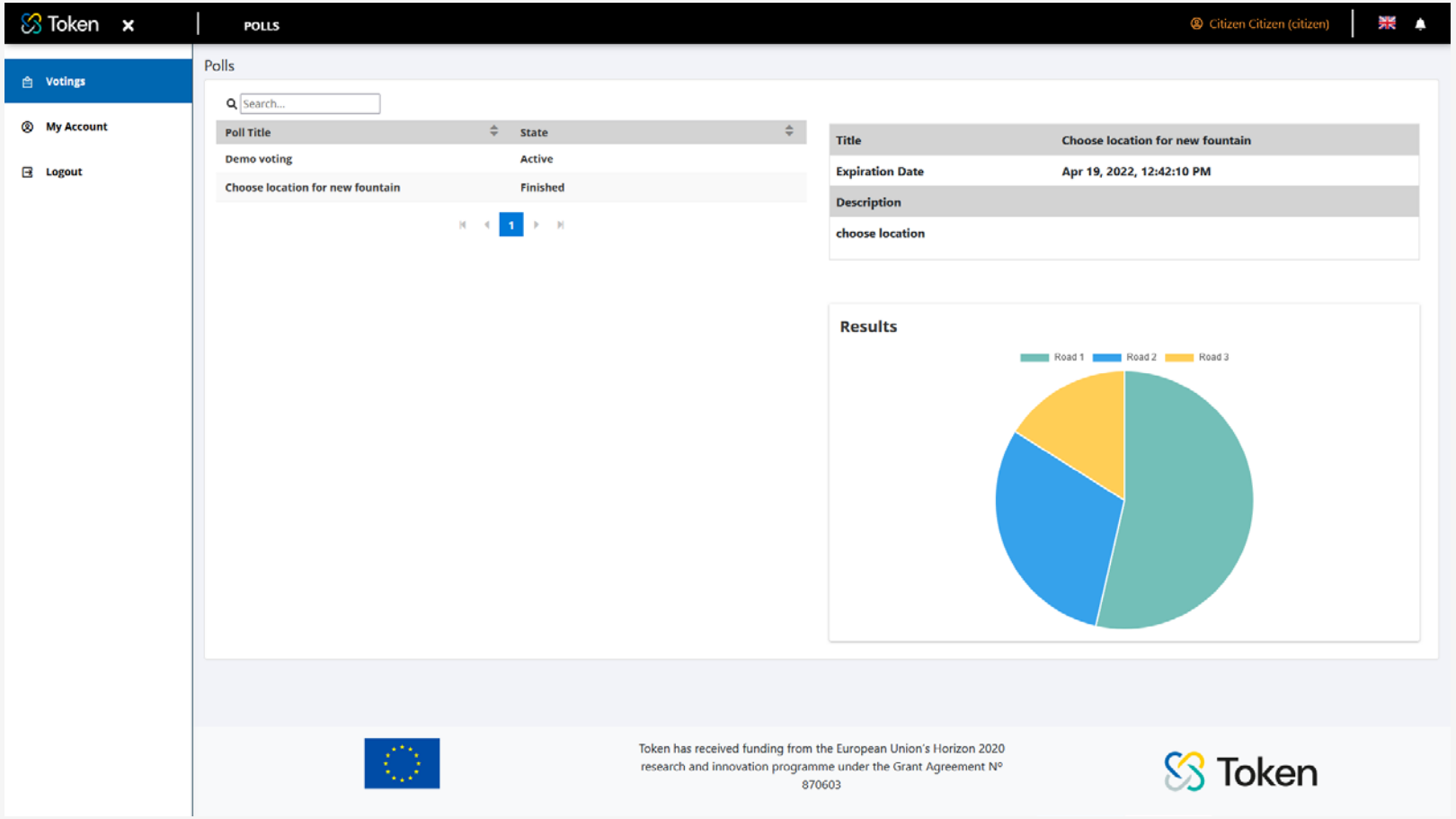


Token has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement Nº 870603

Token

Transparent Management of Public Accounts

VIEWS
(Citizen – Evoting Process)



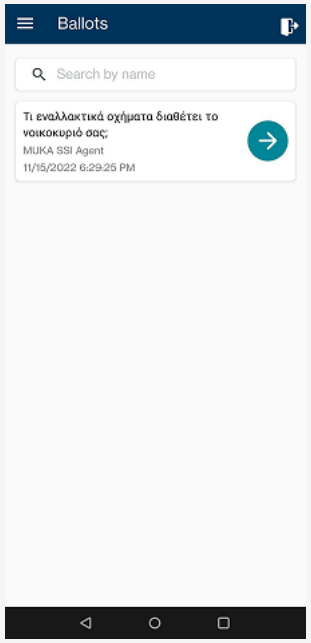
Token has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement N° 870603

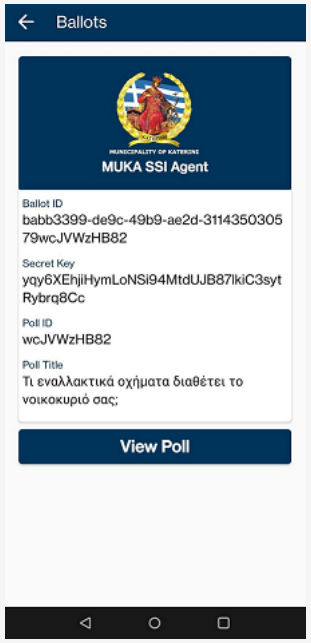
Token

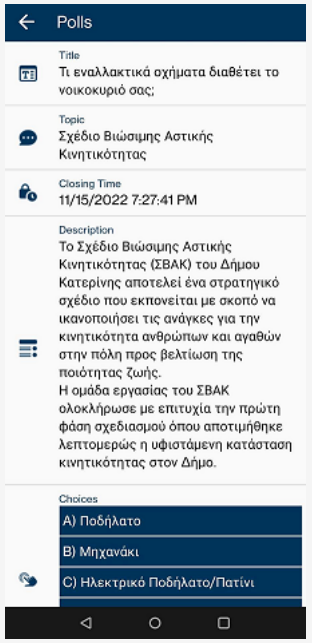
Transparent Management of Public Accounts

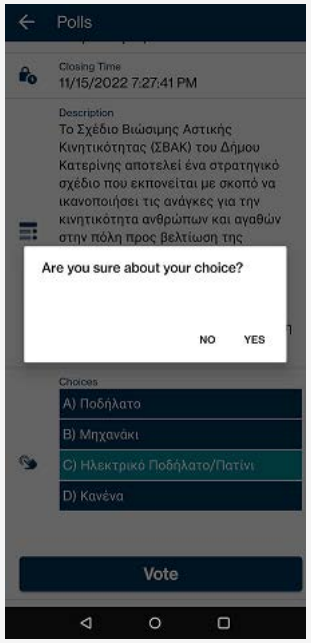
MOBILE APPLICATION

(Citizen – Evoting Process through Mobile Application)



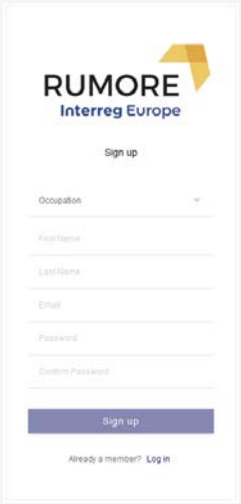






Track&Trace @Agrifood

…investing in Blockchain Research and Development



Producer

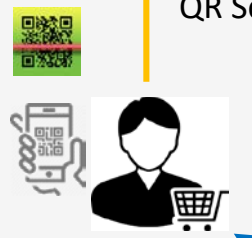
Rice production

Silos

Auditors' Check

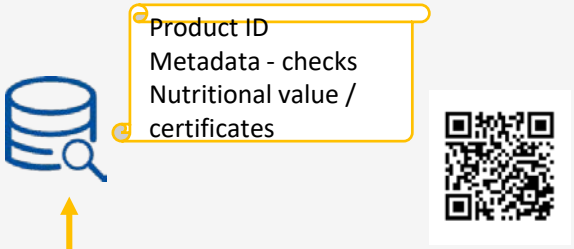
Verify Delivery

Sale

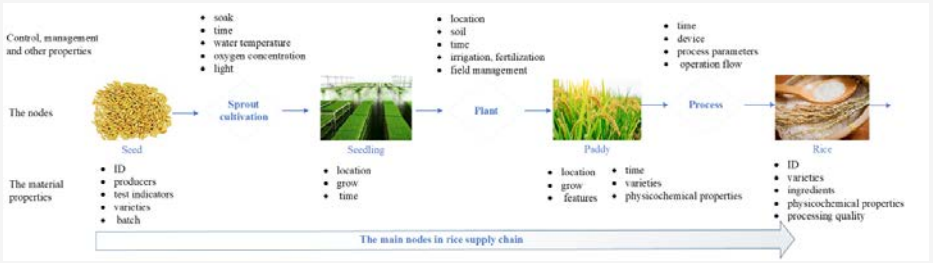


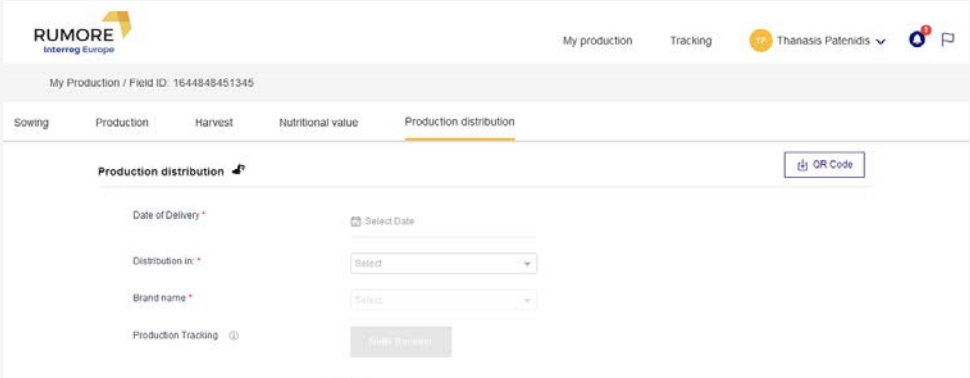
Customer

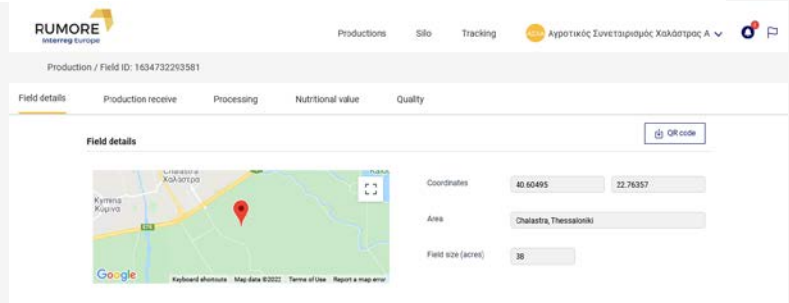
QR Scan for the information of each product



Nutritional value identity

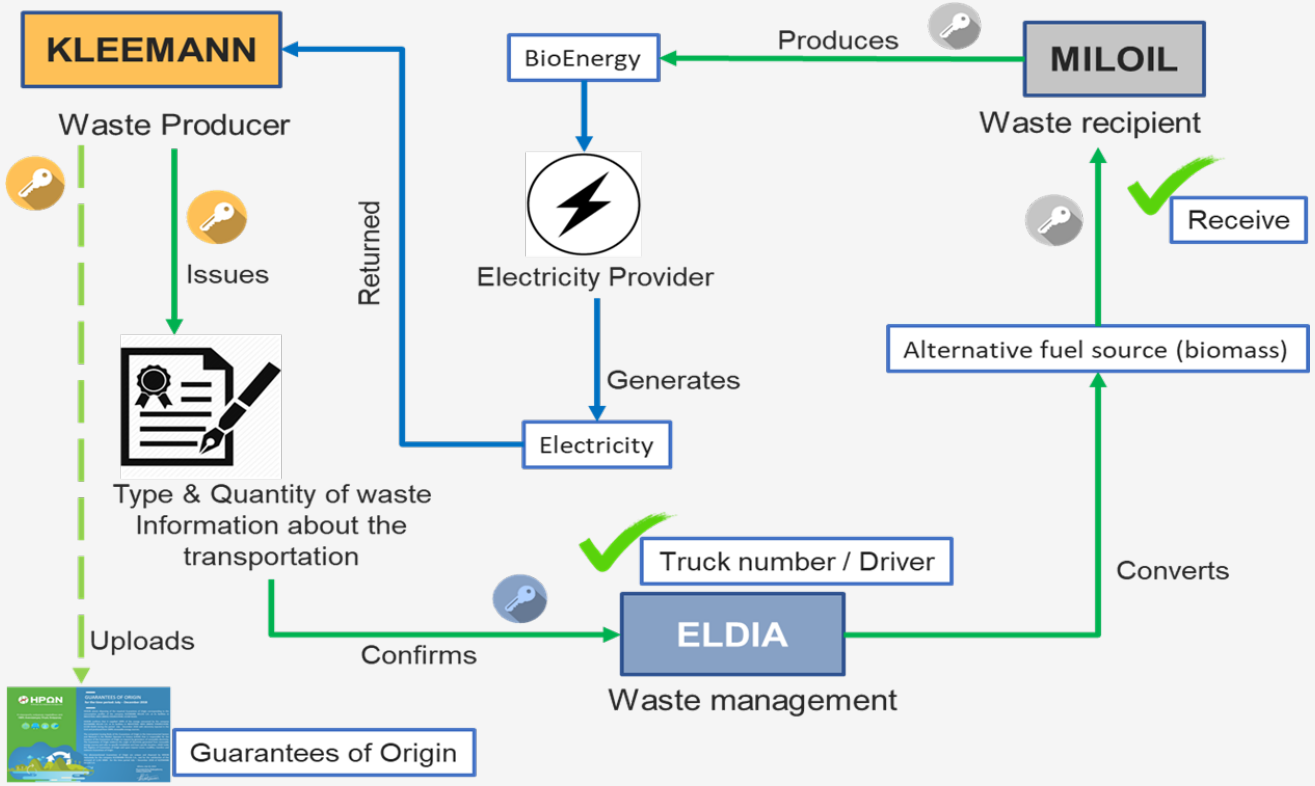


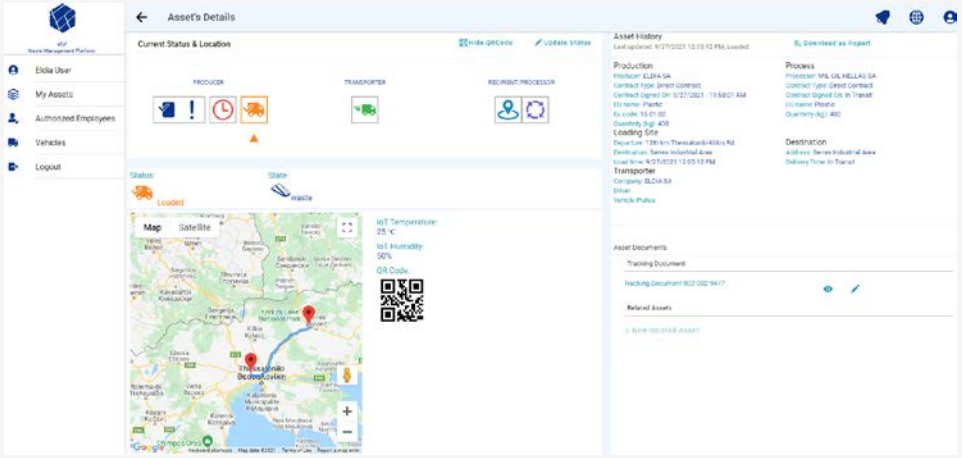


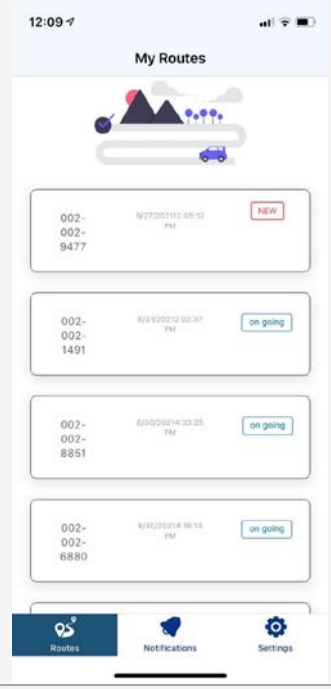


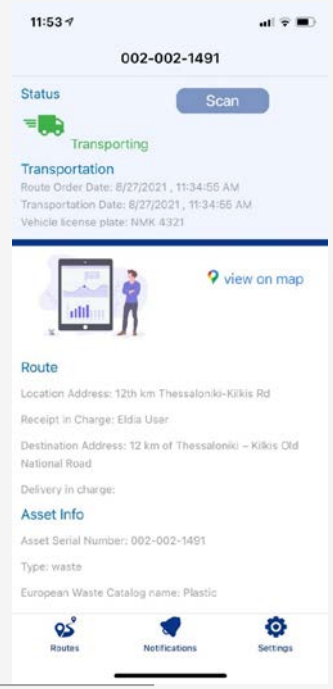
Track&Trace Waste Assets

…investing in Blockchain Research and Development



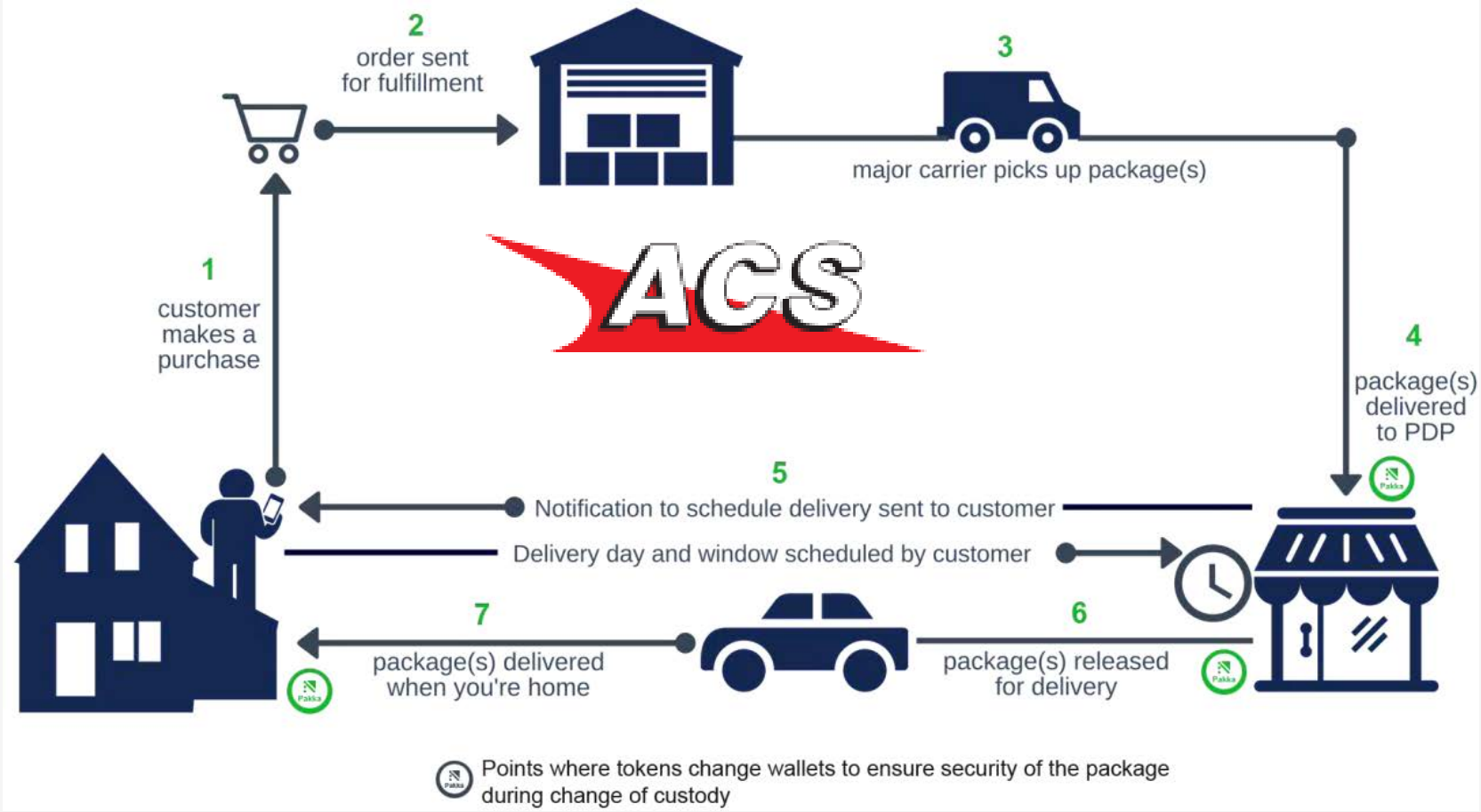






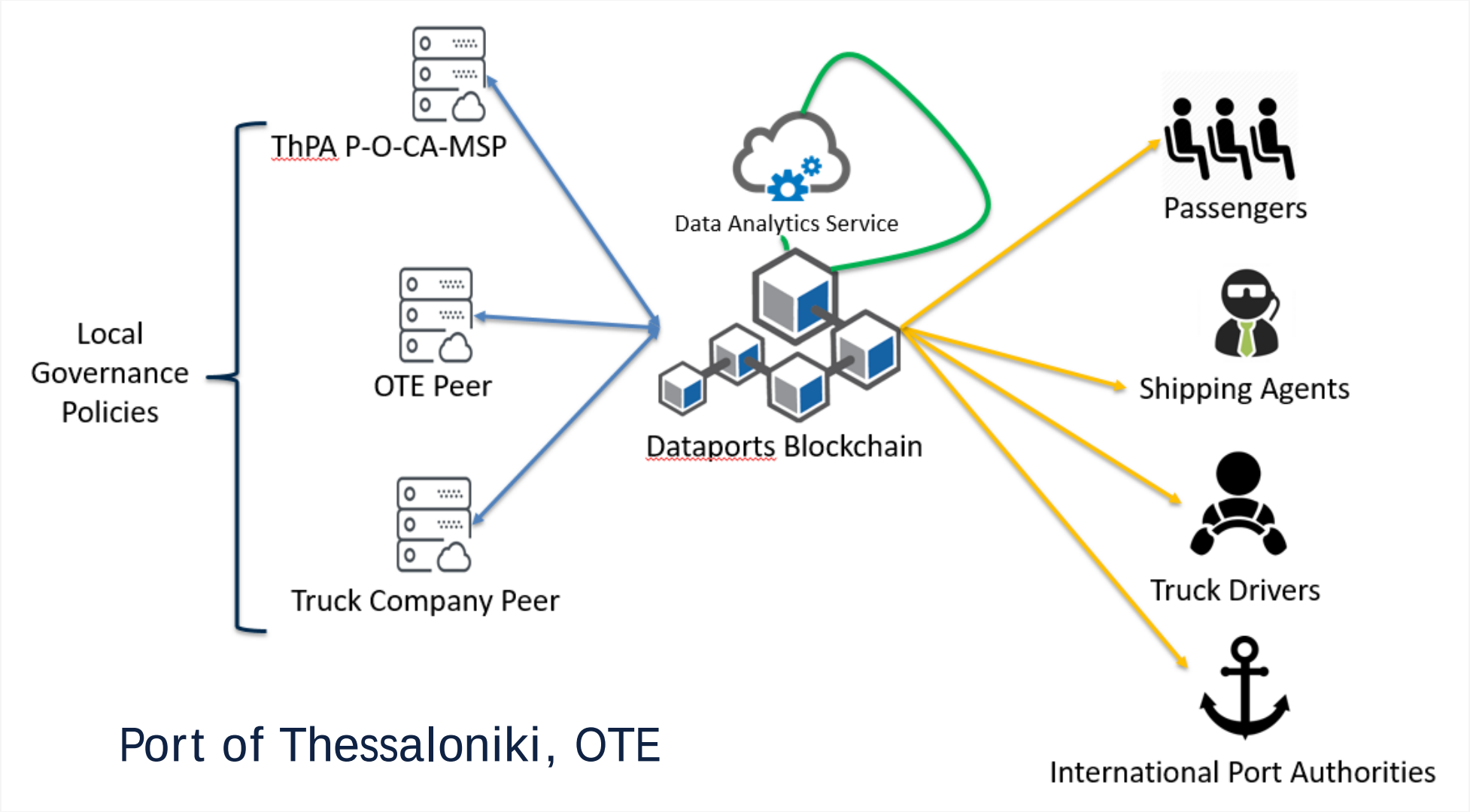
Digital identity & Blockchain in Freight

…investing in Blockchain Courier Platform



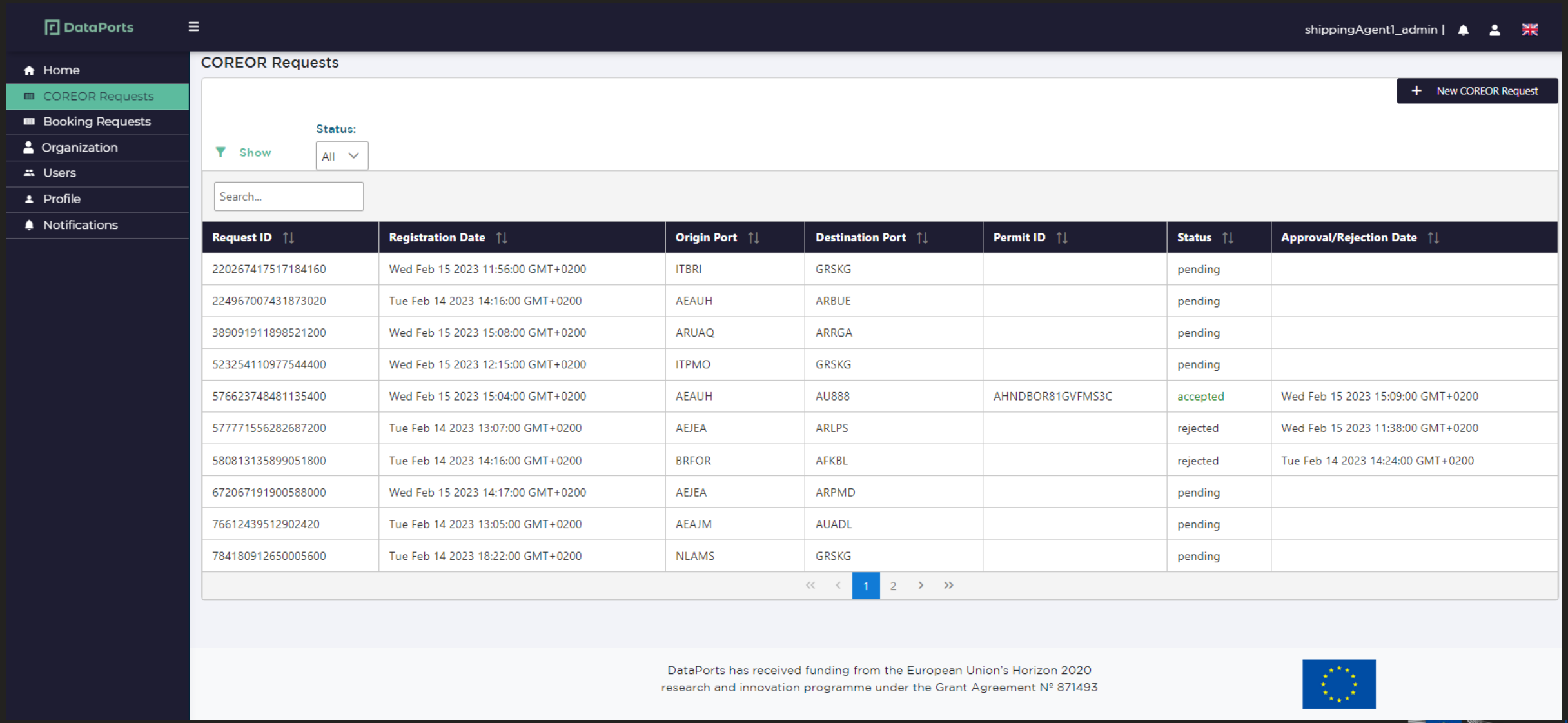
Digital identity & Blockchain in Transport

…investing in Blockchain Research and Development



Port of Thessaloniki, OTE

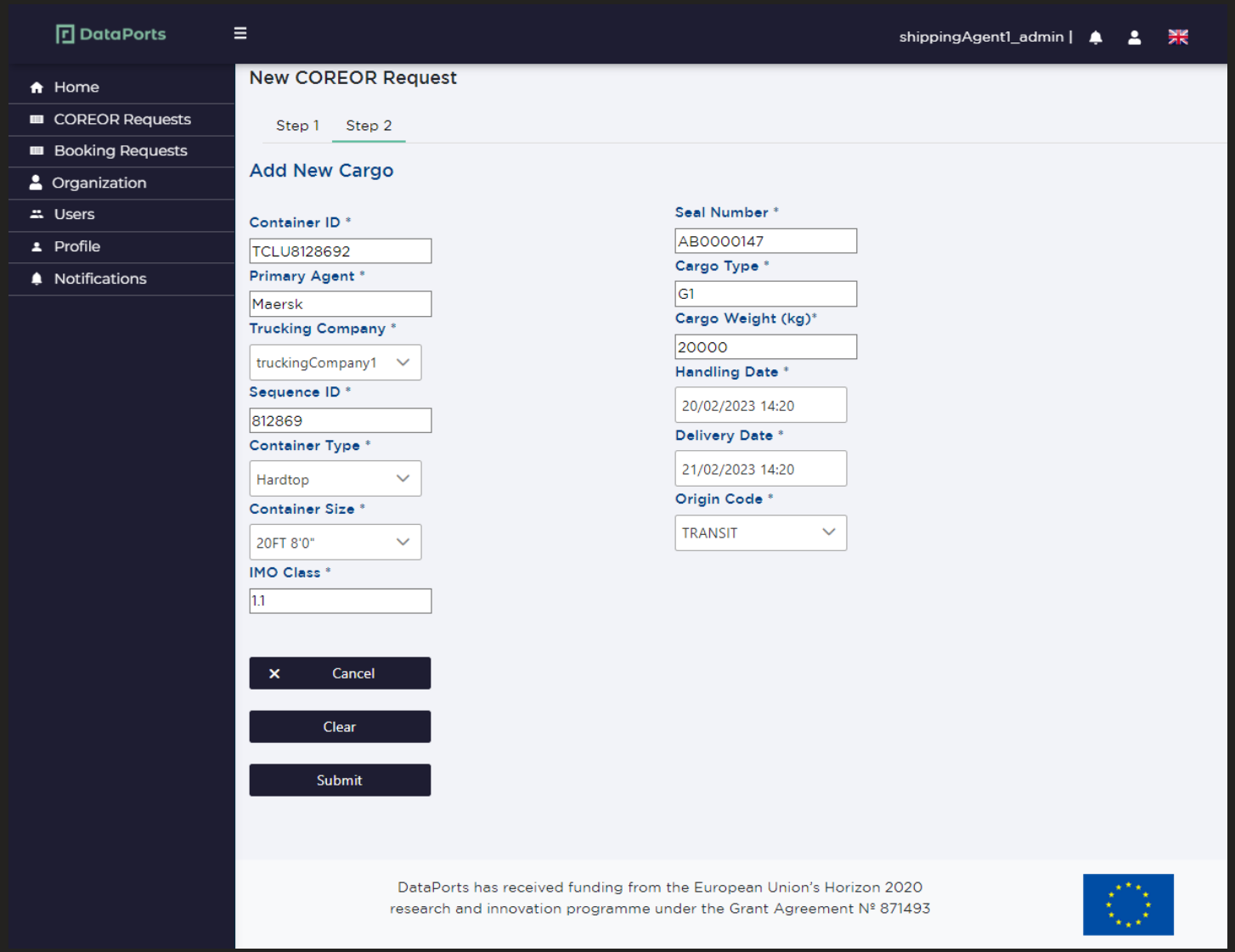
Container Pick-Up application (COREOR requests)



DataPorts has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement Nº 871493

European Commission

Container Pick-Up application (new COREOR request)

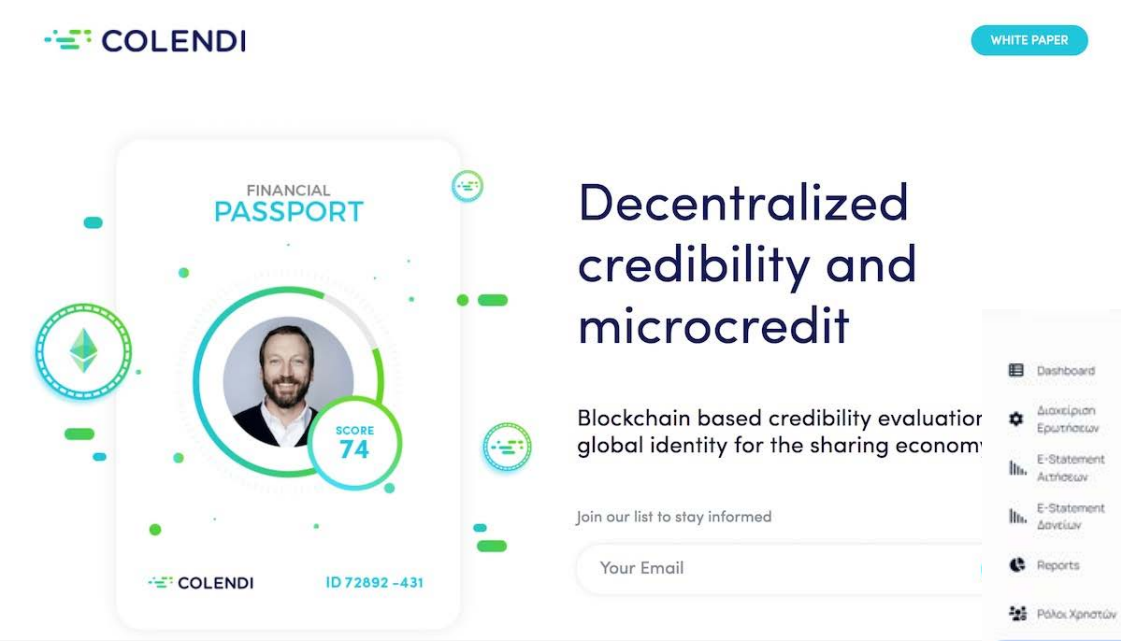


European Commission

Blockchain in Microfinancing

…investing in Fintech

BLOCKCHAIN BASED CREDIT SCORING WEB APPLICATION FOR MICROFINANCING / loans to tokens….



SSI-Enabled Passwordless Login

- *Login Page*
- *Click on “Mobile App” button*
- *Scan QR-code with Mobile App*
- *Logged-in user redirected to the platform*

Thank you

Information Technologies Institute
Centre for Research & Technology Hellas

Dr. Konstantinos Votis
Senior Researcher
Head of Blockchain Lab, ITI
EU Blockchain Observatory and Forum Member
kvotis@iti.gr

ELEDGER

The Commission has decided to award a grant, under the terms and conditions set out in the Special Conditions, the General Conditions and the other Annexes to the Agreement, number 2020-EL-IA-0079.