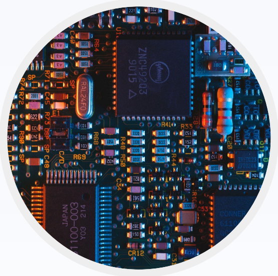
ECSCI

Decentralized Identities and its role in CI protection and information sharing

michele@iota.org
Head of Telco and Infrastructure
Development

More connectivity means more opportunities but also more risks for Critical Infrastructures



IoT monitoring

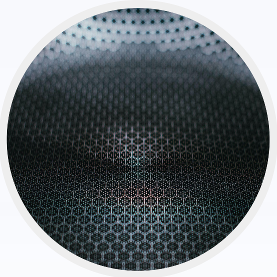
IoT devices are more pervasive, providing more monitoring and actuation capabilities (smart factories, ..)

5G PMR/network slicing

5G and LPWAN bring more connectivity where it was not available before (smart logistics, smart warehouse)

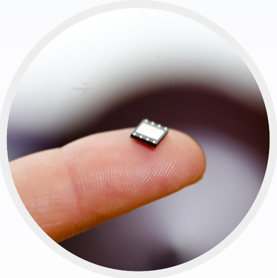
Everything connected

Workers become connected, thus increasing their safety and sites security



E2E Security

Data integrity should be guaranteed and access controlled (critical infrastructures can become target of cyber-physical threats)



Identity management

Access to network infrastructure needs to be controlled and prevent malicious access attempts

Privacy

Data needs to be secured, and their privacy guaranteed

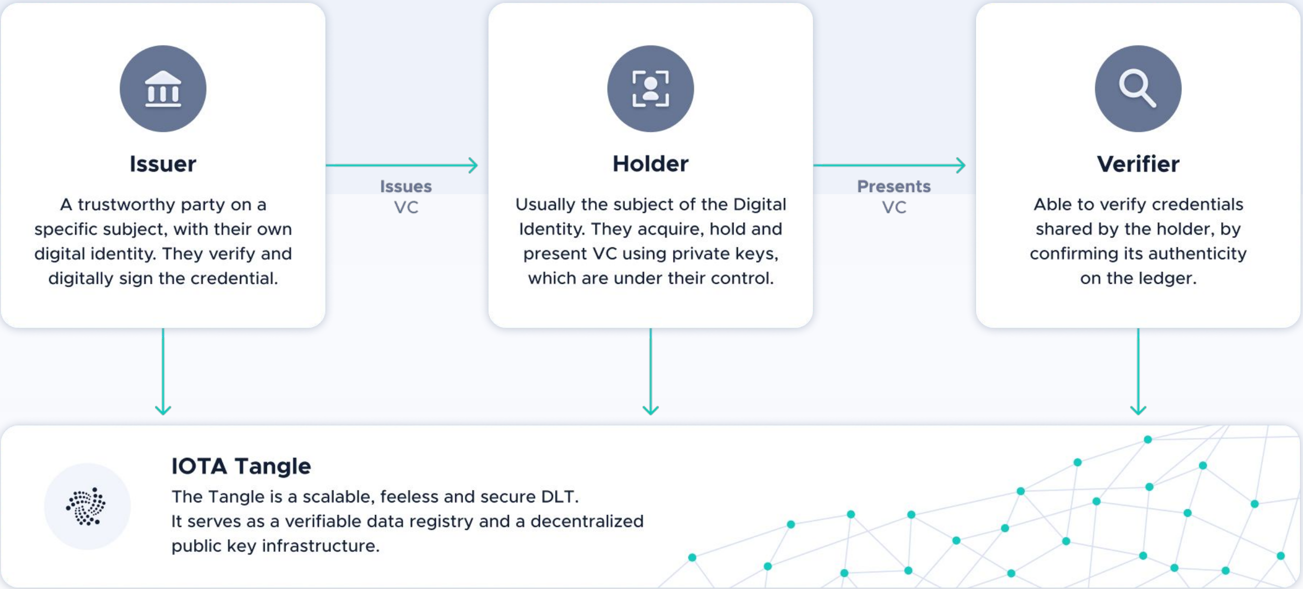
Decentralized Identity

Secure digital identities for humans, organizations and machines

An implementation based on the IOTA Tangle of W3C standards for Decentralized Identifiers and Verifiable Credentials (VC)

IOTA Identity establishes trust and interoperability across organizations, individuals and devices and enables the development of identity solutions in a production ready, open source environment.

It is the only decentralized identity solution that runs on the mainnet of a feeless, permissionless DLT.



Issuer

A trustworthy party on a specific subject, with their own digital identity. They verify and digitally sign the credential.

Holder

Usually the subject of the Digital Identity. They acquire, hold and present VC using private keys, which are under their control.

Verifier

Able to verify credentials shared by the holder, by confirming its authenticity on the ledger.

IOTA Tangle

The Tangle is a scalable, feeless and secure DLT.
It serves as a verifiable data registry and a decentralized public key infrastructure.

Identity for People

Individuals can prove their identity online without relying on centralized services or giving up ownership or control over their personal data.

Identity for Organizations

Onboarding customers with digital identities can reduce regulatory overhead and risk for companies; by having their own digital identity, organizations can improve digital business processes and auditing.

Identity for Devices

Access to and control of devices through digital identities improves data ownership and authentication, increasing security and enabling new business models.

Realizing these opportunities require underlying infrastructure with a unique set of features

Scalability

To cope with growing # of network participants and network traffic.

Feeless transactions

To allow economically viable operations at scale, and on small devices.

Decentralization

To eliminate single points of failure for near 100% uptime.

Security

To keep devices, people, stored data and value protected.

Energy efficiency

To decouple data from value and enable anyone to participate.

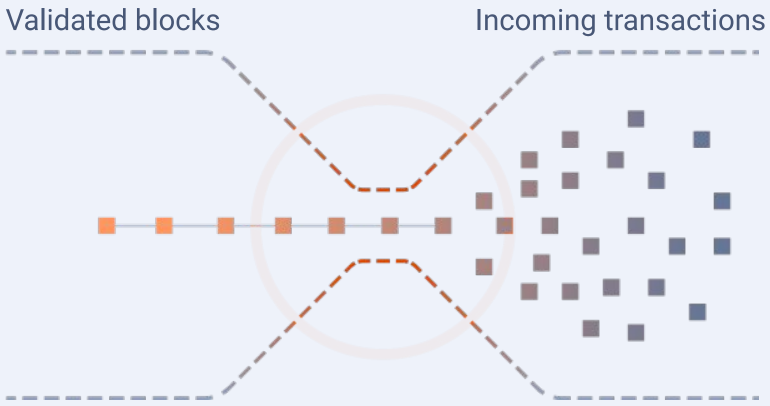
Standardization

To create compatibility for any participant and any type of interaction

The IOTA Tangle is a blockchain without blocks, chains, miners or fees

Blockchains

***Bottleneck** by design*

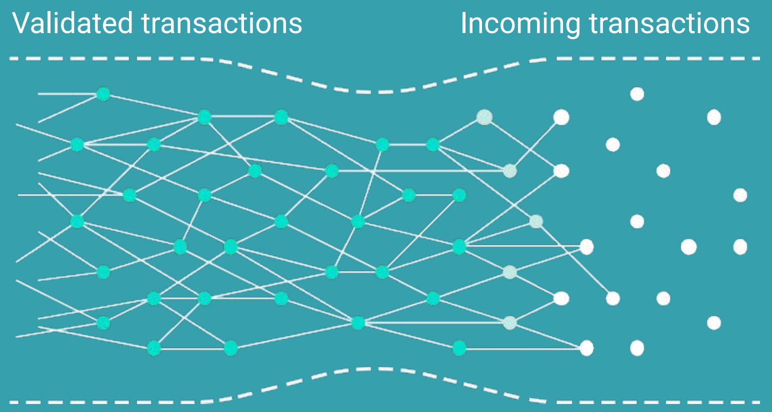


A chain of blocks containing a **limited number of transactions** each

Miners validate new transactions & package them into new blocks, extracting fees

IOTA

***Scalability** by design*



A directed acyclic graph (DAG) of **individual interlinked transactions**

Incoming transactions validate and attach to previous ones, **without transaction fees**

LAYER 1 / CORE PROTOCOL

IOTA offers everything blockchains offer, and more

Like most Blockchains, the IOTA Tangle is:

Permissionless Anyone can connect to, interact with, and transact on the Tangle

Decentralized No central authority and no single point of failure

Secure Through state-of-the art cryptography and probabilistic consensus

Open source Code and documentation are publicly available

Immutable Transfers of data and value recorded on the Tangle

On top of that, the IOTA Tangle is also:

Scalable Increasing network activity decreases tx settlement times

Parallelized Finality of transactions in seconds

Energy-efficient IOTA is designed to be used by low-power micro and IoT devices

Hybrid Possibility for permissioned networks secured by the Tangle

Feeless If a device sends 0.001 cents, the recipient receives 0.001 cents

LAYER 2 / FRAMEWORKS

Frameworks are an easy, modular way to build on IOTA

Frameworks

Tokenized Assets

Enables deployment of custom assets, stable coins and new currencies on IOTA.

Regulatory compliant securitization and tokenization for global asset exchange.

Streams

Enables sending and accessing data stored on the Tangle in an organized way.

Data aggregation from various sources, access control. Powers oracles.

Smart Contracts

Implemented as a second layer protocol, Smart Contracts are scalable and efficient.

Cheaper and easier to integrate through a flexible fee structure.

Access

Lightweight, highly flexible access control for resource-constrained settings.

Functions can be embedded on the device level and be managed remotely.

Digital Identity (DiD)

Decentralized Identity for humans, devices and organizations.

Users can collect and share verified personal data while keeping ownership.

The Tangle

Core protocol

The Tangle provides the basic functionality and security of the IOTA protocol and defines its key characteristics.

LAYER 2 / FRAMEWORKS

Secure digital identities for humans, organizations and machines

IOTA's self sovereign identity (SSI) allows individuals and devices to collect and share verified personal data.

IOTA Identities removes the need for complicated and expensive data collection and management practices.

Every new interaction is trusted, with the user owning their data and deciding with whom to share it.

Decentralised Identifier or DID or SSI = You/Your identity

Verifiable Credentials or VC's = Any attribute that is associated with your identity

IOTA Identities implements the W3C specification for identity

The identity system underpinning the IOTA Identities builds on the standards proposed by the World Wide Web Consortium (W3C).

A new digital identity can be freely created by any individual, organisation or device.

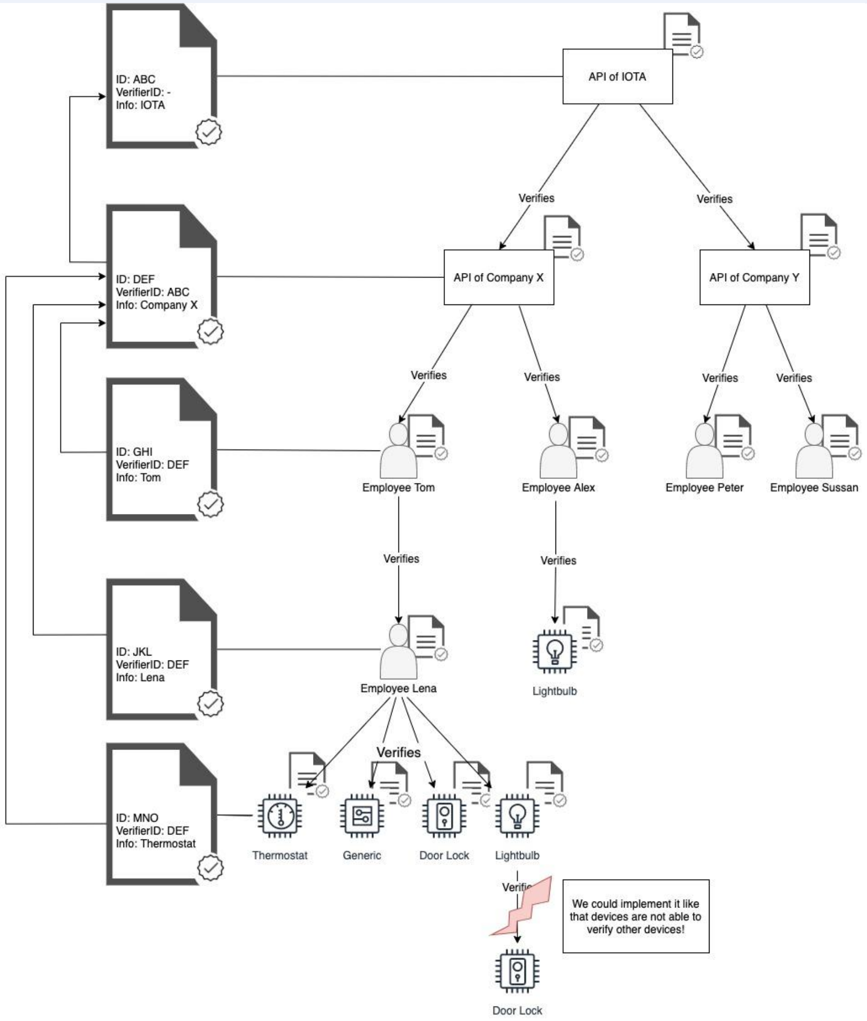
Shareable credentials link identity and its attribute. Anyone verifying a credential can reliably confirm:

- ✔ which authority issued the credential
- ✔ that the credential is being presented is owned by the presenter
- ✔ that the credential is genuine
- ✔ that the credential has not been revoked.

Validating data in a decentralised manner

A combination of public-key cryptography and distributed ledger technology (DLT) to create a feeless framework for generating and validating data.

The IOTA network provides the decentralised, cryptographically-secure trust protocol between authorities, organisations and individuals where this data is anchored.



We could implement it like that devices are not able to verify other devices!

Benefits: For People and Devices

Secure/Trusted

- Validated by DLT
- No passwords as cryptographically signed
  - No account creation barriers
  - Prevents log in fraud
- No reliance on a single entity/company

Open

- Anyone who chooses to can participate in the network
- Anyone who chooses to can make use of a private network
- Any data can be validated using the technology

The ENSURESEC Consortium

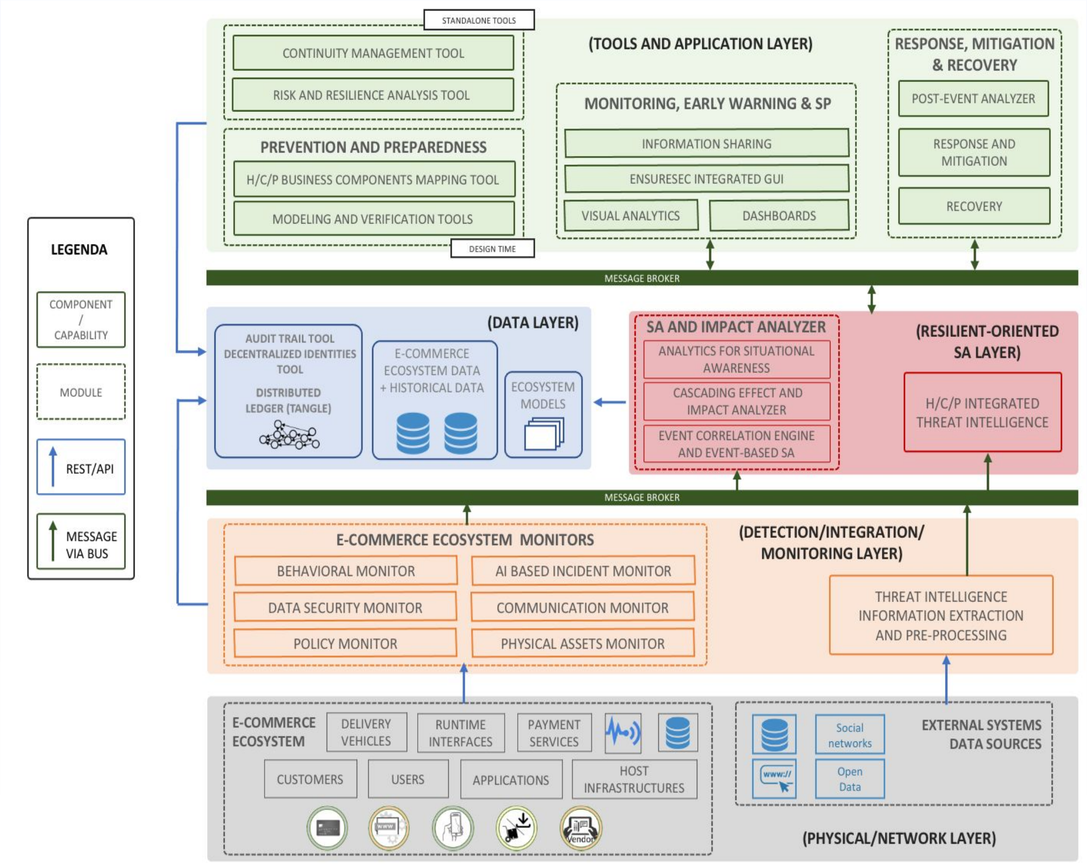
No.	Participant Organisation Name	Acronym	Type	Country
1	INOV INESC Inovação	INOV	RTO	PT
2	Sonae MC Serviços Partilhados	SONAE	LE	PT
3	G4S Telematix	G4S	LE	GR
4	Caixabank S.A.	CXB	LE	ES
5	Atos Spain S.A.	ATOS	LE	ES
6	Engineering	ENG	LE	IT
7	Milsped Group	MSPED	LE	RS
8	Tofarmakeiomou	TOFAR	SME	GR
9	Relational Romania Srl	REL	SME	RO
10	Itti Sp. Z O.O.	ITTI	SME	PO
11	G & N Silensec Ltd	SIL	SME	CY
12	Search-Lab Sec. Eval. Analysis and Research	SLAB	SME	HU
13	Internet of Things Applications and Multi-Layer Development	ITML	SME	CY
14	IOTA Stiftung	IOTA	OTH	DE
15	Lithuanian Cybercrime Center of Excellence	L3CE	NGO	LT
16	Commissariat à L'énergie Atomique et aux Énergies Alternatives	CEA	RTO	FR
17	Fraunhofer - Gesellshaft Zur Forderung der Angewandten Forschung	FRA	RTO	DE
18	Abi Lab Centro Di Ricerca e Innov. per la Banca	ABI	RTO	IT
19	Software Imagination & Vision Srl	SIMAVI	LE	RO
20	Inst. of Communication and Computer Systems	ICCS	RTO	GR
21	Katholieke Universiteit Leuven	KUL	UNIV	BE
22	University of Greenwich	UOG	UNIV	UK

Project Coordinator: INOV; **Technical Manager:** CEA

Objectives

- **E-commerce** is the primary pillar of the **EU Digital Single Market** and as such is **critical for the future and autonomy** of the EU. In order to provide **better access to digital goods and services**, there is the need to establish **trust and security** among e-commerce actors. This is particularly challenging in e-commerce ecosystems due to the **large attack surface** that needs to be addressed and the limited visibility of the entities involved in the value chain.
- ENSURESEC aims at developing a **solution** to provide **e-commerce infrastructures** and ecosystems with through-life **protection** against **cyber, cyber-physical and physical threats, including cascading effects.**
- The goal is to develop a **security toolkit** that addresses the **whole span of the e-commerce ecosystem**, with its various forms of payment and delivery (**virtual, online and physical**) through the implementation of **different modules** that ensure that operations are **protected by design**, as well as provide **continuous monitoring, response, recovery and mitigation measures at run-time.**
- The project will also **create security awareness** among SMEs and their clients, while **promoting trust** in the e-commerce ecosystem, through the creation of dedicated content and the implementation of **tools for training and educating e-commerce** stakeholders on cyber security and improve the resilience of the ecosystem.
- Finally, the solution will be **demonstrated and validated** in a relevant environment by the end of the project, by applying the ENSURESEC concepts in **three different use cases**, each composed of **two scenarios**.

The Role of DID in ENSURESEC


STANDALONE TOOLS
CONTINUITY MANAGEMENT TOOL
RISK AND RESILIENCE ANALYSIS TOOL
(TOOLS AND APPLICATION LAYER)
RESPONSE, MITIGATION & RECOVERY
POST-EVENT ANALYZER
RESPONSE AND MITIGATION
RECOVERY
MONITORING, EARLY WARNING & SP
INFORMATION SHARING
ENSURESEC INTEGRATED GUI
VISUAL ANALYTICS
DASHBOARDS
PREVENTION AND PREPAREDNESS
H/C/P BUSINESS COMPONENTS MAPPING TOOL
MODELING AND VERIFICATION TOOLS
DESIGN TIME
MESSAGE BROKER
LEGENDA
COMPONENT / CAPABILITY
MODULE
REST/API
MESSAGE VIA BUS
(DATA LAYER)
AUDIT TRAIL TOOL DECENTRALIZED IDENTITIES TOOL
DISTRIBUTED LEDGER (TANGLE)
E-COMMERCE ECOSYSTEM DATA + HISTORICAL DATA
ECOSYSTEM MODELS
SA AND IMPACT ANALYZER
ANALYTICS FOR SITUATIONAL AWARENESS
CASCADING EFFECT AND IMPACT ANALYZER
EVENT CORRELATION ENGINE AND EVENT-BASED SA
(RESILIENT-ORIENTED SA LAYER)
H/C/P INTEGRATED THREAT INTELLIGENCE
MESSAGE BROKER
E-COMMERCE ECOSYSTEM MONITORS
BEHAVIORAL MONITOR
AI BASED INCIDENT MONITOR
DATA SECURITY MONITOR
COMMUNICATION MONITOR
POLICY MONITOR
PHYSICAL ASSETS MONITOR
(DETECTION/INTEGRATION/ MONITORING LAYER)
THREAT INTELLIGENCE INFORMATION EXTRACTION AND PRE-PROCESSING
E-COMMERCE ECOSYSTEM
DELIVERY VEHICLES
RUNTIME INTERFACES
PAYMENT SERVICES
CUSTOMERS
USERS
APPLICATIONS
HOST INFRASTRUCTURES
Vendor
Social networks
Open Data
www://
EXTERNAL SYSTEMS DATA SOURCES
(PHYSICAL/NETWORK LAYER)

- In a complex scenario like the one of e-commerce with multiple stakeholders and assets interacting at the same time, the need of a trusted and neutral infrastructure is paramount.

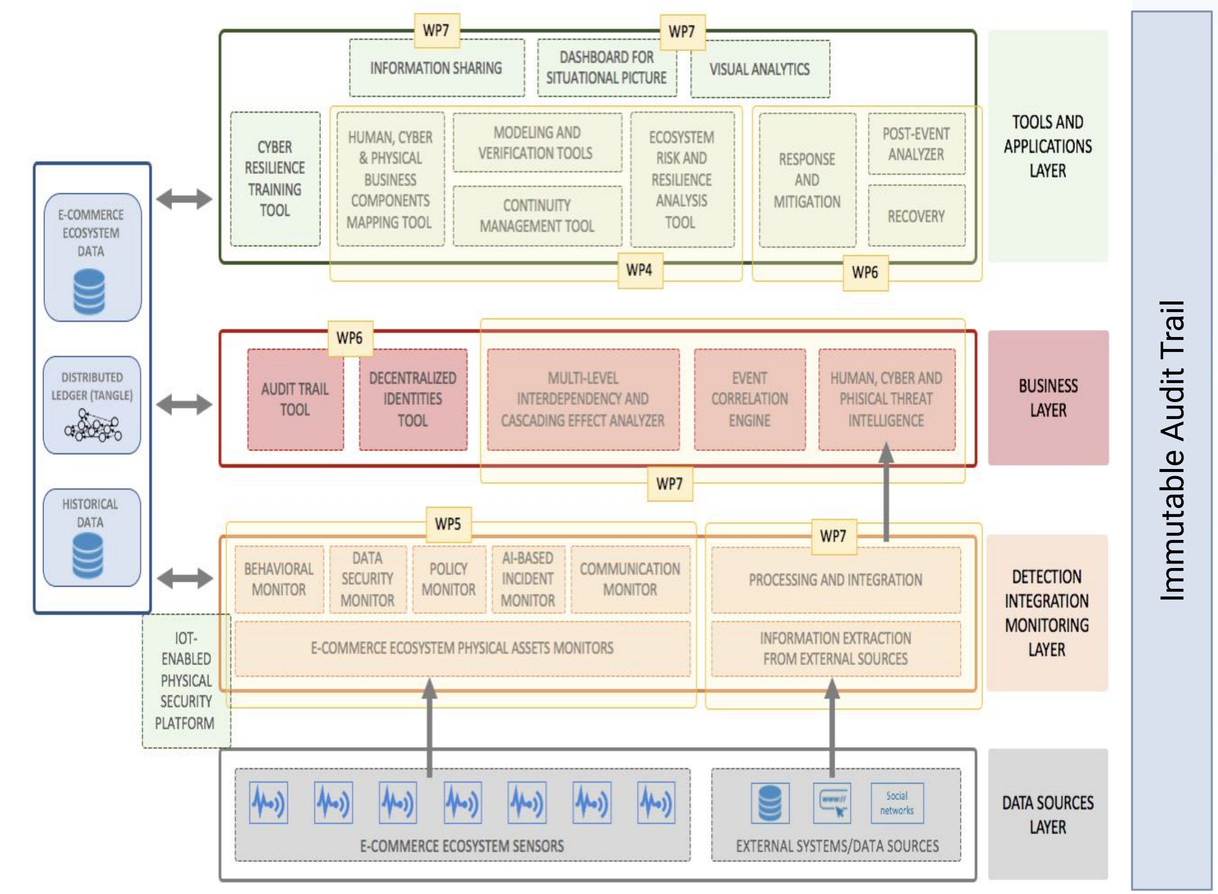
- IOTA has provided the technology and the expertise to build an immutable decentralized audit trail infrastructure.

Tools: Audit Trail Log

An immutable trail of e-commerce events

Primary use case

- Guarantee authenticity and immutability of data collected by tools
- Guarantee immutability and auditability events, mitigation strategies, etc


WP7
WP7
INFORMATION SHARING
DASHBOARD FOR SITUATIONAL PICTURE
VISUAL ANALYTICS
CYBER RESILIENCE TRAINING TOOL
HUMAN, CYBER & PHYSICAL BUSINESS COMPONENTS MAPPING TOOL
MODELING AND VERIFICATION TOOLS
CONTINUITY MANAGEMENT TOOL
ECOSYSTEM RISK AND RESILIENCE ANALYSIS TOOL
RESPONSE AND MITIGATION
POST-EVENT ANALYZER
RECOVERY
WP4
WP6
TOOLS AND APPLICATIONS LAYER
E-COMMERCE ECOSYSTEM DATA
DISTRIBUTED LEDGER (TANGLE)
HISTORICAL DATA
WP6
AUDIT TRAIL TOOL
DECENTRALIZED IDENTITIES TOOL
MULTI-LEVEL INTERDEPENDENCY AND CASCADING EFFECT ANALYZER
EVENT CORRELATION ENGINE
HUMAN, CYBER AND PHISICAL THREAT INTELLIGENCE
WP7
BUSINESS LAYER
WP5
WP7
BEHAVIORAL MONITOR
DATA SECURITY MONITOR
POLICY MONITOR
AI-BASED INCIDENT MONITOR
COMMUNICATION MONITOR
PROCESSING AND INTEGRATION
E-COMMERCE ECOSYSTEM PHYSICAL ASSETS MONITORS
INFORMATION EXTRACTION FROM EXTERNAL SOURCES
IOT-ENABLED PHYSICAL SECURITY PLATFORM
DETECTION INTEGRATION MONITORING LAYER
Social networks
E-COMMERCE ECOSYSTEM SENSORS
EXTERNAL SYSTEMS/DATA SOURCES
DATA SOURCES LAYER
Immutable Audit Trail

Tools: Decentralized Digital Identities

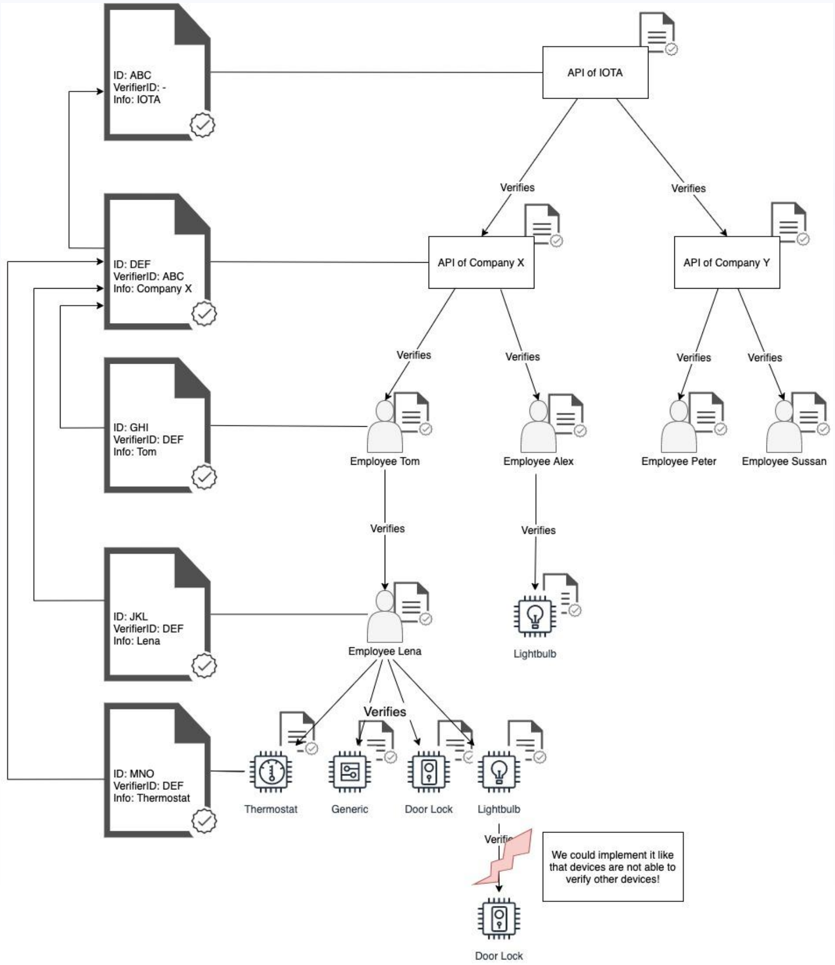
A trusted and decentralized identity management system

Primary use case

- Guarantee authenticity of audit trail data and manage access
- Auditors

Secondary use cases

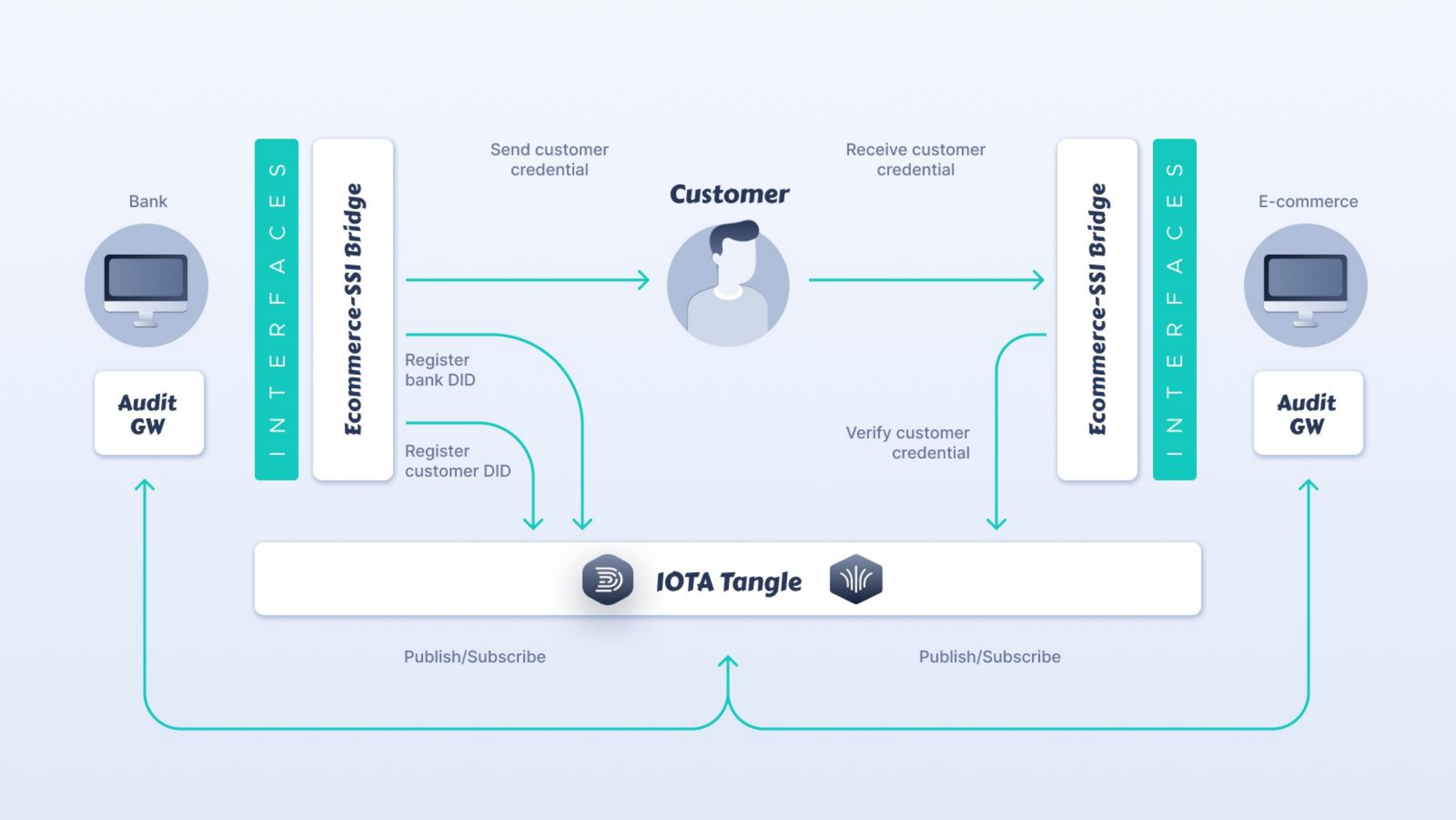
- Guarantee integrity of organizations to customers communication (anti-phishing)
- Guarantee correct and secure delivery
- Help to minimise customers personal data



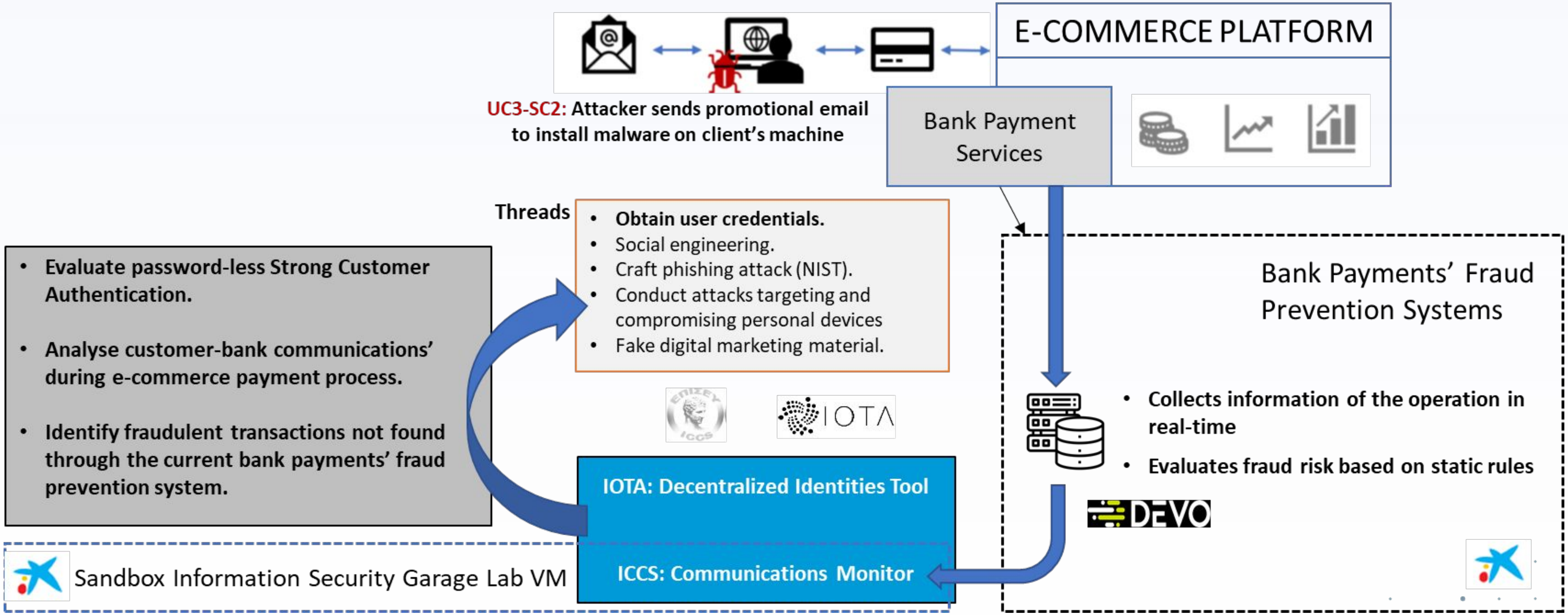
We could implement it like that devices are not able to verify other devices!

The Infrastructure building blocks

We listened to the industry in order to accelerate adoption



Malware protection and Fraud prevention



UC3-SC2: Attacker sends promotional email to install malware on client's machine

- **Obtain user credentials.**
- Social engineering.
- Craft phishing attack (NIST).
- Conduct attacks targeting and compromising personal devices
- Fake digital marketing material.

- **Evaluate password-less Strong Customer Authentication.**
- **Analyse customer-bank communications' during e-commerce payment process.**
- **Identify fraudulent transactions not found through the current bank payments' fraud prevention system.**

- **Collects information of the operation in real-time**
- **Evaluates fraud risk based on static rules**

IOTA: Decentralized Identities Tool

ICCS: Communications Monitor

Sandbox Information Security Garage Lab VM

SSI Bridge for e-commerce

Reduce risks and increases security of e-commerce

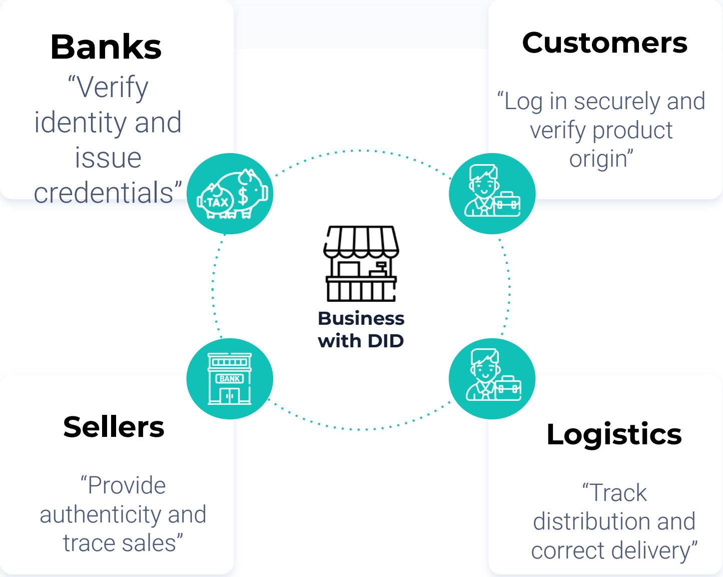
What it is

Prevention of frauds and of other cyber-physical threats in e-commerce requires a combination of secure verifiable identities of involved actors.

Use Case: Age and benefits verification, VIP deliveries, seller on-boarding.

SSI Bridge

The SSI Bridge allows e-commerce ecosystem actors including sellers, buyers and payment providers (banks) to register decentralized identities and issue verifiable credentials. Identities and credentials can be created and verified for both individuals and products.



Banks
"Verify identity and issue credentials"

Customers
"Log in securely and verify product origin"

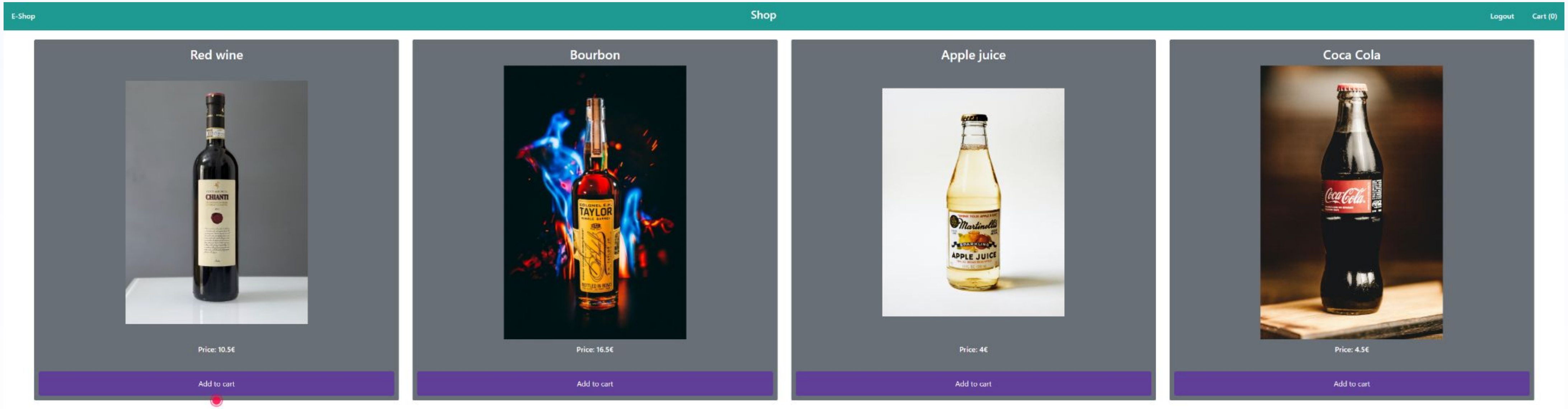
Business with DID

Sellers
"Provide authenticity and trace sales"

Logistics
"Track distribution and correct delivery"

› Find more information here

Age verification via SSI Bridge and verifiable credential demonstration


E-Shop

Shop

Logout Cart (0)

Red wine

Price: 10.5€

Add to cart

Bourbon

Price: 16.5€

Add to cart

Apple juice

Price: 4€

Add to cart

Coca Cola

Price: 4.5€

Add to cart

This demo was produced for Ensuresec project by the IOTA Foundation and in collaboration with Caixa Bank.

POWERED BY IOTA

CaixaBank

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883242.

Verifiable Transport Credentials

Flexible people movement across transport modes

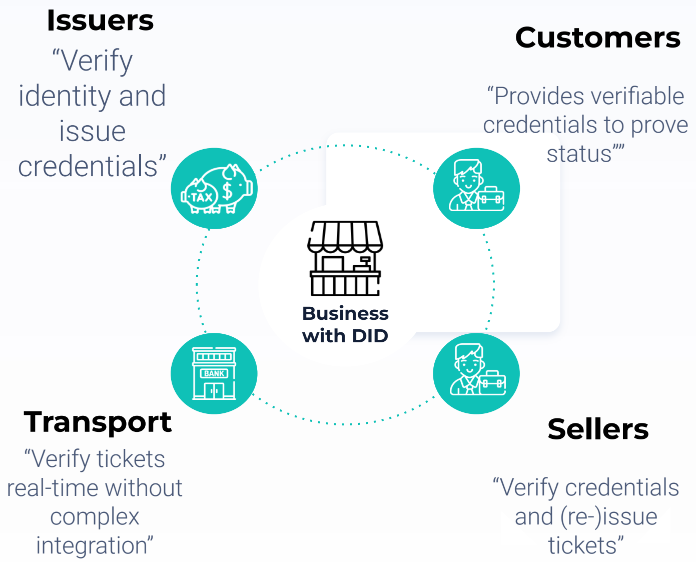
What it is

Mobility as a Service requires a number of different transport documents, that is difficult to (re-)issue in case of disruption and to verify without complex integration or aggregators fees; it is also difficult to verify eligibility for special transport conditions.

Tickets as Verifiable Credentials

IOTA Identities and Verifiable Credentials allow customers to prove their eligibility to specific travel conditions (i.e., red carpet) and to receive tickets that transport providers can verify instantly.

› Find more information here



Issuers
"Verify identity and issue credentials"
Customers
"Provides verifiable credentials to prove status""
Business with DID
Transport
"Verify tickets real-time without complex integration"
Sellers
"Verify credentials and (re-)issue tickets"

ITS Norway	deepblue consulting & research	Cerema	HERØYA INDUSTRIPARK
enav	IKEM	ROSAS	IOTA FOUNDATION
Information Sharing Company	SINTEF	TU Delft	APPLIED AUTONOMY
Statens vegvesen Norwegian Public Roads Administration	TechnoSky	CERTX	SEA Milan Airports
FS TECHNOLOGY			

Multi-modal transport logistics

Flexible goods movement across transport modes

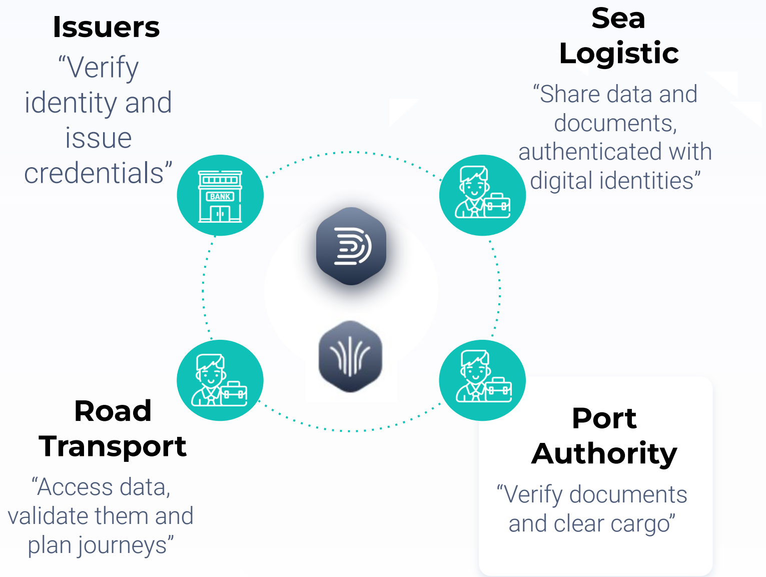
What it is

Multi-modal transport and just in time supply chains require sharing a number of different transport documents, V2X data that is difficult to achieve without guaranteeing their security, confidentiality and ownership.

V2X secure communication infrastructure

IOTA Identities and ledgers allow logistic providers to share relevant transport information, while guaranteeing their integrity and avoiding malicious and unauthorised accesses

› Find more information here



Issuers

"Verify identity and issue credentials"

Sea Logistic

"Share data and documents, authenticated with digital identities"

Road Transport

"Access data, validate them and plan journeys"

Port Authority

"Verify documents and clear cargo"

ITS Norway	deepblue consulting & research	République Française Cerema	HERØYA INDUSTRIPARK www.heroya-industripark.no
enav	IKEM	ROSAS	IOTA FOUNDATION
Information Sharing Company	SINTEF	TUDelft	APPLIED AUTONOMY
Statens vegvesen Norwegian Public Roads Administration	TechnoSky	CERTX	SEA Milan Airports
TECHNOLOGY GRUPPO FERROVIE DELLO STATO ITALIANE			

Personal Digital Twins

Creating new privacy-preserving monitoring and alerting systems

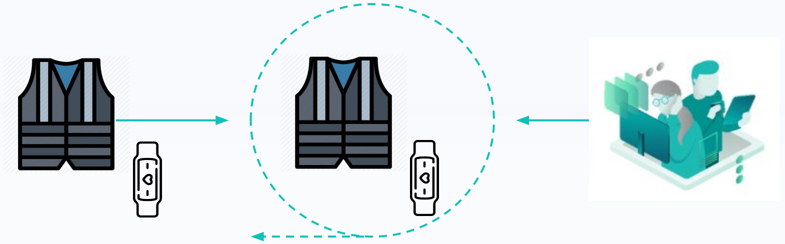
What it is

Increasing safety of workers requires monitoring data from trusted devices and generation and sharing of information in a privacy-preserving way.

Personal Devices Identity

IOTA Identity for wearables allows for tamper-proof credentials validation and immutable registration of key events in the lifespan of a worker. This improves the person health and safety monitoring, while improving control and data management. Sensors IDs can be combined with the owner's personal ID to enable personalised incident responses in case of emergency.

› Find more information here



Smart garment

Reports information in real time

Edge Digital Twin

Analyses behavior and generates credentials locally

Using ZKP information can be shared without revealing secrets

Employee and HSE

Takes decisions and produce privacy-preserving audits

LAYER 3 / MORE SOLUTIONS

Trusted Smart Meters

Cross-ecosystems trusted prosumers

What it is

Certified energy prosumers smart meters can enable peer-to-peer energy tradings with benefits for local communities and RES producers and consumers.

Local Markets rely on authenticity of energy data, while avoiding platform lock-in.

Smart Meters Identity and VCs

IOTA Identity for smart meters allows for tamper-proof credentials validation to certify devices, track and reward RES production, prevent cloning and malicious participants in local energy marketplaces.

› Find more information here

IOT HARDWARE

Original Prototype being tested at NTNU Jan 2021

Edge Intelligent Grid Devices
are connected to each participating energy assets

DLT INTEGRATION

A scalable, feeless and energy efficient **Distributed Ledger Technology (DLT)** *provides transparent, auditable and automated market trading and clearing mechanisms.*

SOFTWARE PLATFORM

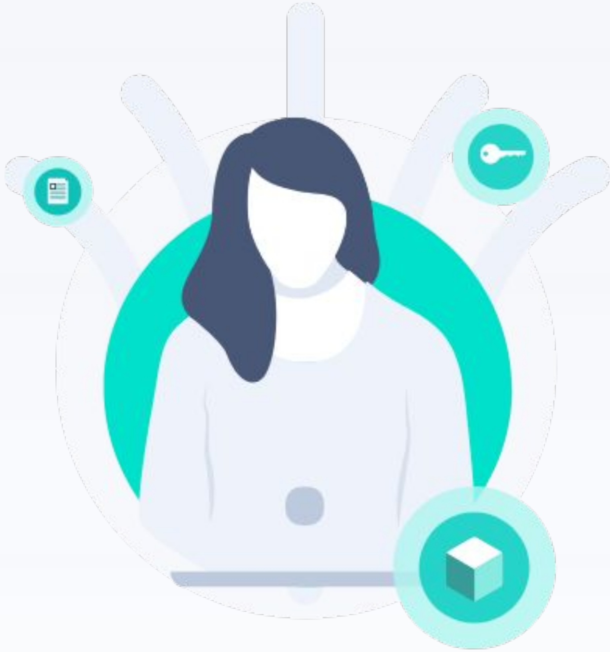
Beta Web Interface for the management of devices

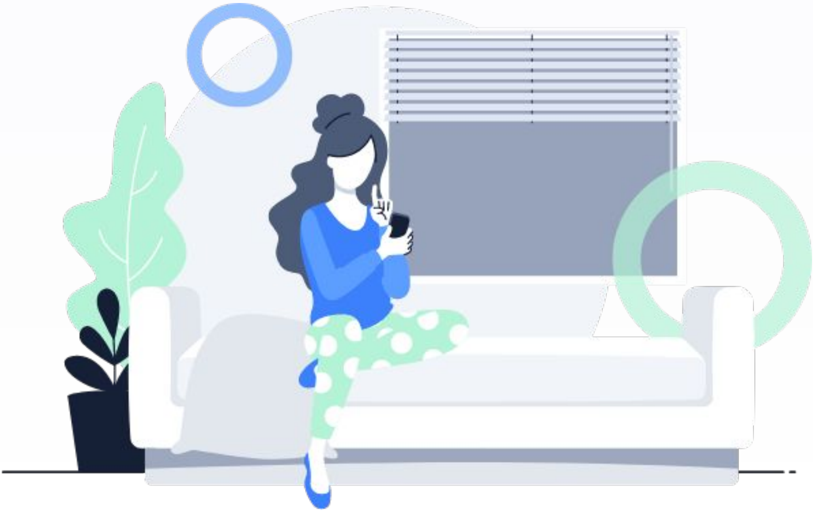
Modular P2P Energy Platform
allow Community System Operators

+CITYXCHANGE

IOTA Audit Trail Gateway

This service enables users to create immutable encrypted data channels and share them with others. Data in channels are stored on the IOTA Tangle. A channel is implemented as an IOTA Stream and can handle different subscribers. By requesting a subscription to a channel, a subscriber can request Read, Write, and ReadAndWrite access to the channel. This request must be authorized by the creator (author) of the channel. After a subscriber is authorized, it is then able to write and/or read to and/or from the channel. In addition to subscribers, the author can always read and write messages in the channel. Authors and subscribers have their own IOTA Identity (through the SSI Bridge). All this workflow is managed with simple REST APIs.





IOTA Self Sovereign Identity Bridge

This service enables users to create Self-Sovereign Identities, linking Decentralized Identifiers (DIDs) to people, organizations, or devices. Each identity is represented by a unique public key immutably stored on the ledger. Identities and public keys are used to anchor off-chain verifiable credentials, which are certificates containing identity attributes signed by an Issuer identity (using its private key).

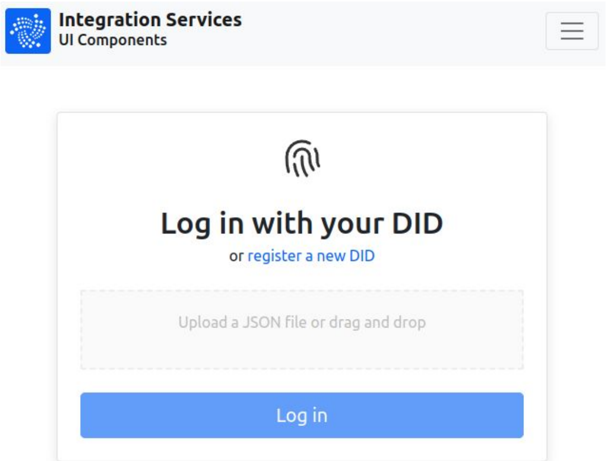
The Issuer itself is an entity with its own decentralized identity. The Bridge allows an identified trust root to verify users' identity. Verified identities can then propagate this verification to other entities (organizations, individuals, or objects) using a network of trust approach. Identity can be used with the Audit Trail Service or as stand-alone. The entire workflow is managed with simple REST APIs.

LAYER 3 / PRODUCTS

What we have built

Integration Services

- Simple REST API’s
- Documentation - https://wiki.iota.org/integration-services/welcome
- Deployed locally or as a managed service
- Modular UI (WIP)



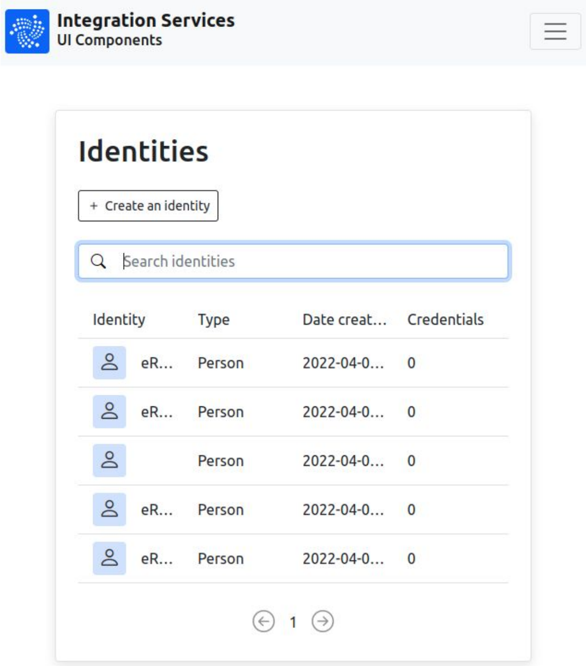
Integration Services
UI Components

Log in with your DID

or register a new DID

Upload a JSON file or drag and drop

Log in



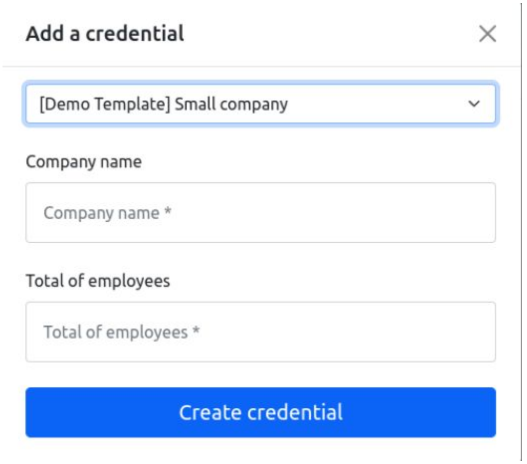
Integration Services
UI Components

Identities

+ Create an identity

Search identities

Identity	Type	Date creat...	Credentials
eR...	Person	2022-04-0...	0
eR...	Person	2022-04-0...	0
	Person	2022-04-0...	0
eR...	Person	2022-04-0...	0
eR...	Person	2022-04-0...	0



Add a credential

[Demo Template] Small company

Company name: Company name *

Total of employees: Total of employees *

Create credential

We don’t build alone

Become an active part of our growing ecosystem

DELL Technologies
ZEBRA
EVRYTHNG
I N A T B A
ClimateCHECK
TRADE MARK EAST AFRICA
IOT1 ACADEMY
zühlke
ENERGINET
+CITYxCHANGE
EDAG GRUPPE MOTION TECHNOLOGIES
ENSURESEC
Tech Mahindra
ENGIE Lab
THE LINUX FOUNDATION
RWTH AACHEN UNIVERSITY
NTNU
JAGUAR
LAND ROVER
EDAG
CLIMATE CHAIN COALITION
BiiLabs
FIWARE
sopra steria
MOBI
Austin CityUP
OMG
Climate-KIC
tmforum
CHAMBER OF DIGITAL COMMERCE
ECLIPSE FOUNDATION
ST life.augmented
ECLASS
peerOS
data.austintexas.gov
CONSTRUCTION BLOCKCHAIN CONSORTIUM

The IOTA Foundation was founded and incorporated in Germany in 2017 to research, develop, and grow the IOTA protocol. By now, the foundation counts over 150 employees distributed across more than 25 nations.

Thriving Community

350+ corporate patents

550+ peer reviewed research papers

180,000+ community members

Mature Network

1,000+ TPS on a feeless DAG protocol

390,000+ active addresses with value*

$173bn value transacted*

*as of April 2020

Thank you!!

michele@iota.org

Head of Telco and Infrastructure Development

Github Twitter Discord LinkedIn Website