DIGITAL TECHNOLOGIES ACTING AS A GATEKEEPER TO INFORMATION AND DATA FLOWS

Introducing TANGO

ENCRYPTing Europe towards Secure and Federated Data Use, ENCRYPT Project, Athens, Greece

Anaxagoras Fotopoulos

EXUS AI Labs

17-06-2025

This project has received funding from the European Union's HE research and innovation programme under the grant agreement No. 101070052

TANGO Project Fiche

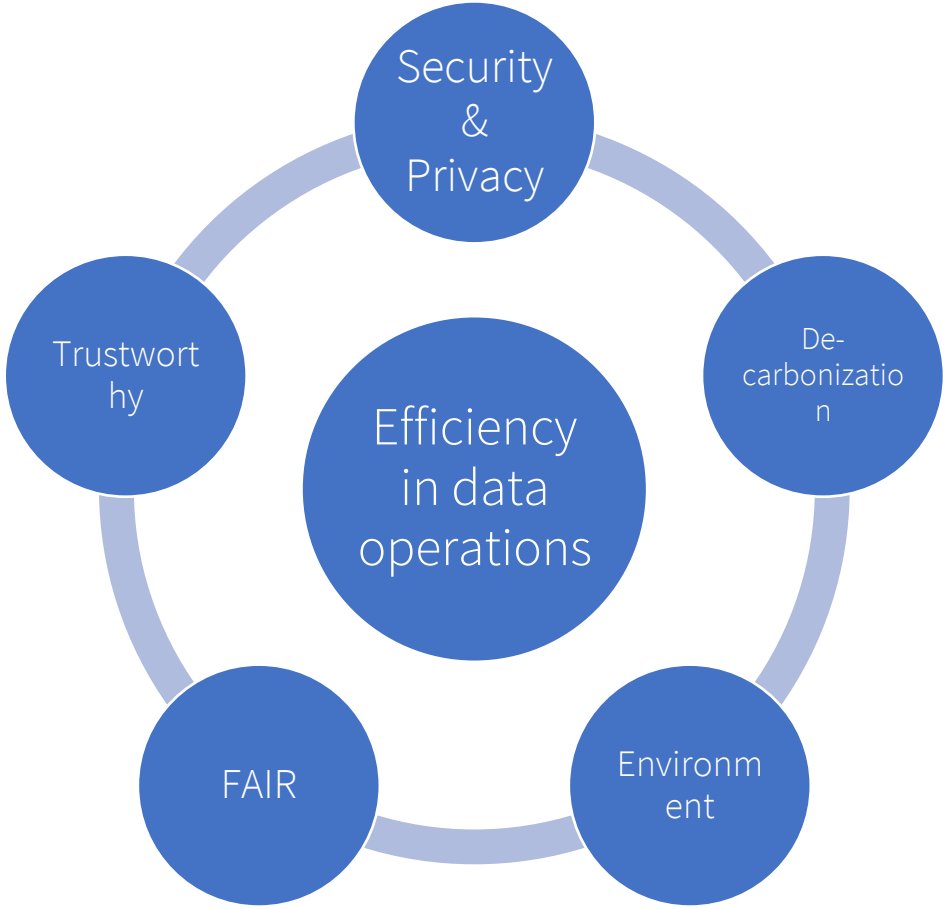
Project Name	• Digital Technologies ActiNg as a Gatekeeper to information and data flOws
Project Consortium	• 37 partners, 14 Countries
Call / Project Type	• Topic: HORIZON-CL4-2021-DATA-01-01 • Project Type: RIA
Total Budget/Max EU Contribution	• €10.444.121
Start Date	• 1 September 2022
Duration	• 36 months (31 August 2025)

GA n. 101070052

Acronym	Country
ATOS	ES
ATOS SP	ES
FSDE	DE
FUJ_LU	LU
INTRA	LU
SQUAD	PT
NORB	SE
DBC	BE
EXUS	EL
LSTECH	ES
SVI	CY
QBE	EL
SQD	BE
XLAB	SI
FN	CY
ANYS	ES
CEA	FR
FHG	DE
VTT	FI
DUT	NL
UMU	ES
KUL	BE
UTH	EL
UPRC	EL
IDSA	DE
EGI	NL
ECO	DE
LIC	BE
IDIADA	ES
ABI	IT
RIAS	PT
FMAKE	BE
CESGA	ES
AHOP	ES
VISA	DE
MET	EL
UOM	UK
UOG	UK

TANGO Motivation

- TANGO aims **at improving the efficiency of data intensive applications while decreasing time and carbon footprint** via innovative solutions for
  - Privacy-preserving and secure data sharing and management
  - Smart contracts
  - AI model training, life-cycle, decentralization
- Applied to **several real-life business problems**
- From a **citizen-centric, secure and trustworthy viewpoint**



DUE TO CLIMATE CHANGE, ENERGY CRISIS, RISE OF PRICES
OPERATORS ARE NOW QUICKLY REALISING THAT THERE IS AN
URGENT NEED TO INCREASE THE ENERGY EFFICIENCY OF DATA CENTRES AND REDUCE THEIR ENVIRONMENTAL IMPACT

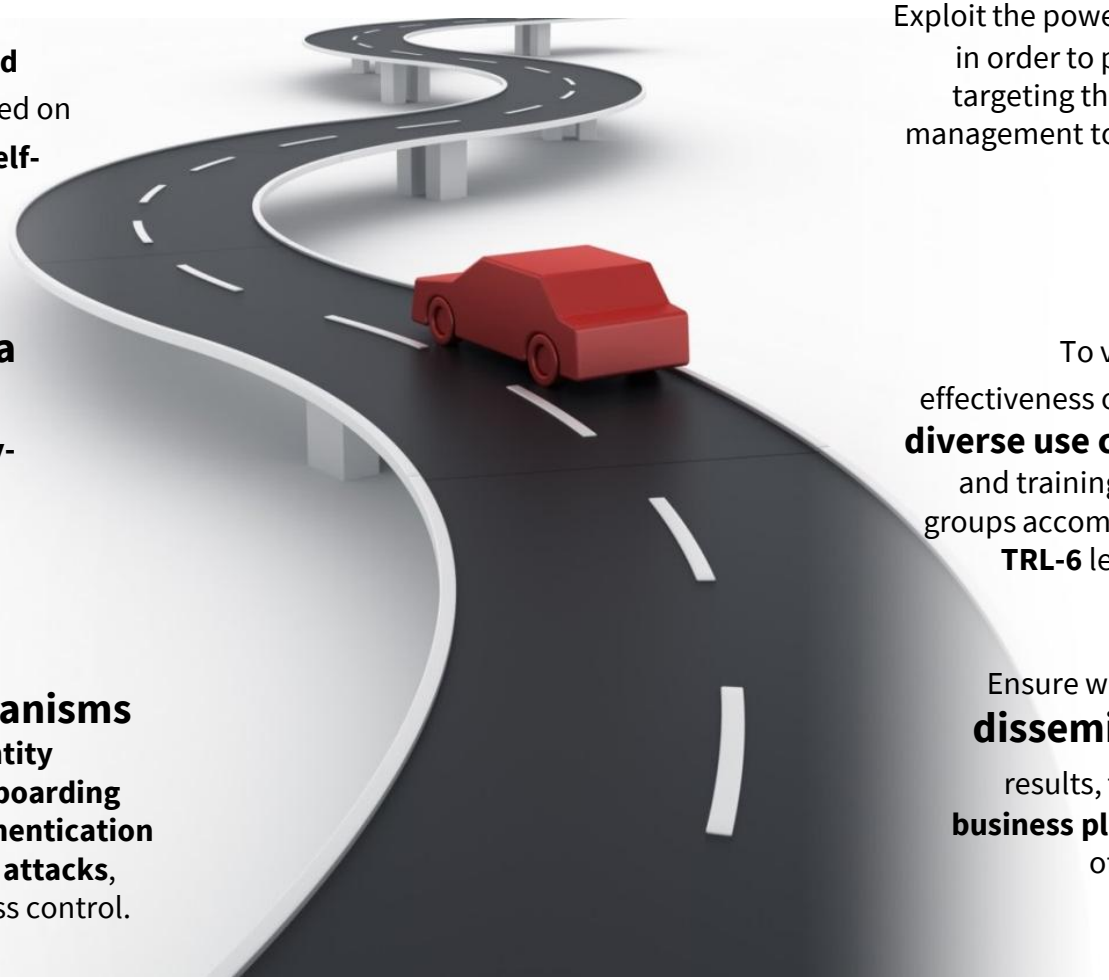
EUROPE (AND THE WORLD) NEED STATE-OF-THE ART
TECHNIQUES AND TOOLS TO REDUCE THE ENERGY CONSUMPTION AND CARBON FOOTPRINT OF DATA INTENSIVE APPLICATIONS

TANGO Objectives

1 Framework for **fair, responsible and green data management, sharing and storage** while maintaining data ownership based on **energy-efficient Smart Contracts, AI, Self-Sovereign Identity, Self-Encryption and Continuous Behavioural Authentication.**

2 A **secure, trusted and audible data management, storage and sharing environment** by developing advanced **energy-efficient Blockchain,** novel **security and privacy-preserving protocols** for **guaranteeing the ownership** of the data throughout the whole data lifecycle.

3 Distributed **trust management mechanisms** that leverage **Self-Sovereign Identity for identity management**, innovative **user and device onboarding approaches** and continuous **behavioural authentication mechanisms**, and **hardening of side-channel attacks**, providing highly secure and user-friendly access control.

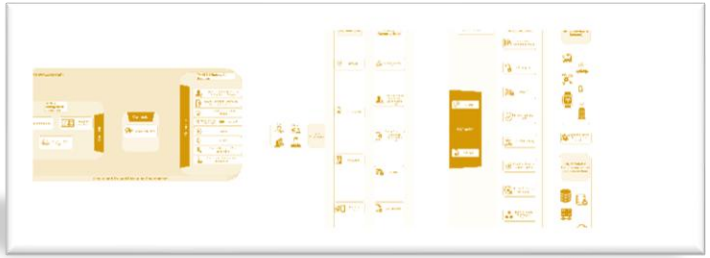


4 Exploit the power of **Artificial Intelligence** in order to produce accurate decision making targeting the data, security and infrastructure management towards **"green" data operations**.

5 To validate and **demonstrate** the effectiveness of the proposed solution in **six (6) diverse use cases** with the active engagement and training of several different stakeholders' groups accomplishing at the end of the project a **TRL-6** level for the entire TANGO platform.

6 Ensure wide **communication and scientific dissemination** of the innovative TANGO results, the **efficient exploitation and business planning,** as well as the contribution of specific project results to relevant **standardisation** bodies.

TANGO Overall Architecture



Dataspace compatible

Builds on the principles of security, trust and interoperability of dataspace initiatives

Adopts the notion of **Connector** and extends it by providing extra privacy, security and AI tools

- Offered as **Services** (on-premise or cloud deployment)
- Or deployed at organization/end-user premises as **containerized** packages

Modular

Highly-modular architecture allowing for **fine-grained configuration** and dynamic enablement of services/technology offerings

- Connector deployed on a **Kubernetes** cluster
- Blueprint files provide configuration options and selection of container images for deployment

Transparent

Front-end applications and User Interfaces allow users to interact with the TANGO ecosystem in a user-friendly and **transparent** way

- **TANGO App Store and Portal** allow users to browse and select technology offerings and discover services

Three Layer Architecture

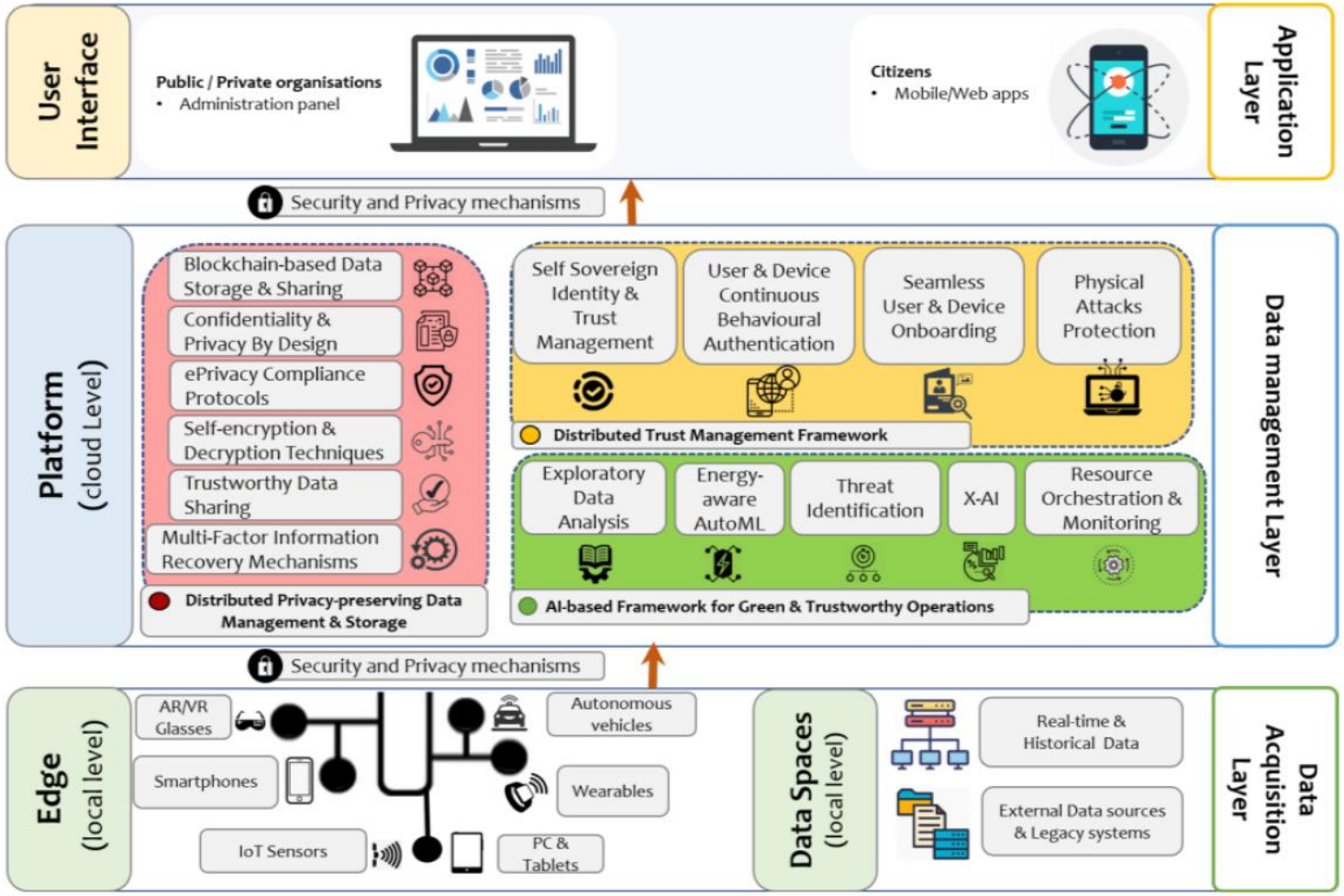
- Trust Layer:
  - all the services and functionalities that facilitate the data exchange and interaction between TANGO participants in a secure and trustworthy manner
  - i.e., Personal Credential Manager, Audit Log, Usage Control, etc.
- Management Layer
  - services and functionalities for fine-grained control, automatic deployment, and orchestration of the TANGO ecosystem
  - i.e., Deployment Orchestrator, Configuration Manager, etc.
- User Layer
  - technology offerings created by the TANGO consortium and all the supporting mechanisms that enable their independent coexistence within the TANGO ecosystem
  - i.e., Device Continuous Behavioural Authentication, User Behaviour Exchange Module, etc.

- Microservices: the three layers are distributed across multiple runtime environments and physical locations.

TANGO Main contributions

Technologies for industrial data sharing – Several building blocks for piloting

- Ensuring privacy, security & trustworthiness
- Data & AI toolkit
- Legal and ethical compliance



Technology offerings

Technologies to be part of a data space

Distributed Privacy-preserving Data Management and Storage

Blockchain-based Data Storage and Sharing

Blockchain data-sharing for regulated areas; secure, compliant, and private with consent management.

Ubiquitous Personal Context Vectors

UPCVs use VRNs for secure, personalized service recommendations without storing user history, ensuring privacy across vendors.

CP-ABE

CP-ABE encrypts data with access policies in ciphertext, allowing only users with matching attributes to decrypt.

Trustworthiness Scoring Module

Trustworthiness Scoring and Privacy Risk Modules assess and control data sharing risks on Tango using weighted scores.

Policy-based Access Control

Policy-based access control for granular, GDPR-compliant access, fostering trust via CP-ABE and XACML.

Self-Encryption and Decryption Techniques

Self-encryption module uses file's unique features for personalized, robust encryption, enhancing security by encrypting split chunks.

Distributed Trust Management Framework

SSI Agent

SSI-Agent issues and verifies verifiable credentials, supporting secure, decentralized identity management and data control.

TANGO Wallet

TANGO Wallet manages digital identities with privacy, enabling selective information disclosure while ensuring data integrity.

Seamless Onboarding

Seamless Onboarding for User offers a wizard-like interface for secure, remote identity verification using SSI.

Side-channel attack hardening

Hardening against side-channel attacks uses masking and hiding to protect cryptographic systems from unintended information leaks.

Device Continuous Behavioral Authentication

Device Continuous Behavioral Authentication analyzes device behavior and system logs for real-time authentication, enhancing security.

User Continuous Behavioral Authentication

User Continuous Behavioral Authentication module uses analytics to authenticate users by their behaviors, enhancing security on third-party platforms.

AI-based Framework for Green & Trustworthy Operations

Exploratory Data Analysis Engine

EDAE in TANGO discovers patterns in datasets, preparing them for ML with traditional and AI-driven analysis techniques.

FL– MLOps – AutoML

TANGO integrates Federated Learning, MLOps, and AutoML for decentralized AI training, lifecycle management, and automated model creation.

Dynamic Intelligent Execution on Heterogeneous Systems

TornadoVM in TANGO enables Java hardware acceleration on CPUs, GPUs, FPGAs, and supports Java-Python interoperability.

Privacy Enhancing Component & Privacy Assurance Tool

PEC and PAT in TANGO calculate and mitigate privacy risks, ensure GDPR compliance, and secure data exchange.

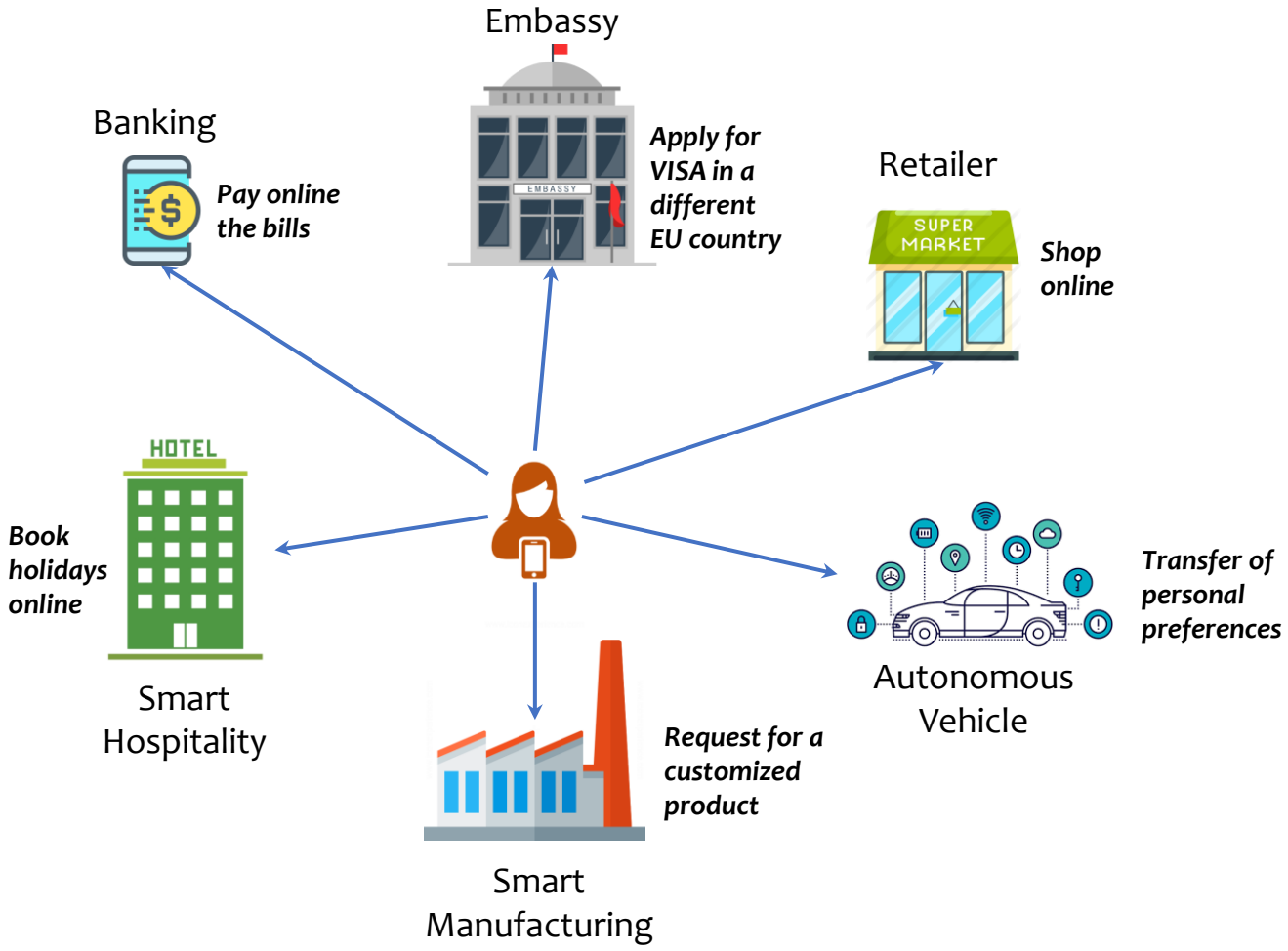
X-AI for Privacy and Trust Enhancement

XAI component provides explainability for AI models using LIME, Grad-CAM, LRP to visualize predictions and biases.

Infrastructure Management based on AI

RENOPS in TANGO forecasts renewable energy availability for efficient, cost-effective computing infrastructure management.

6 pilots in different sectors

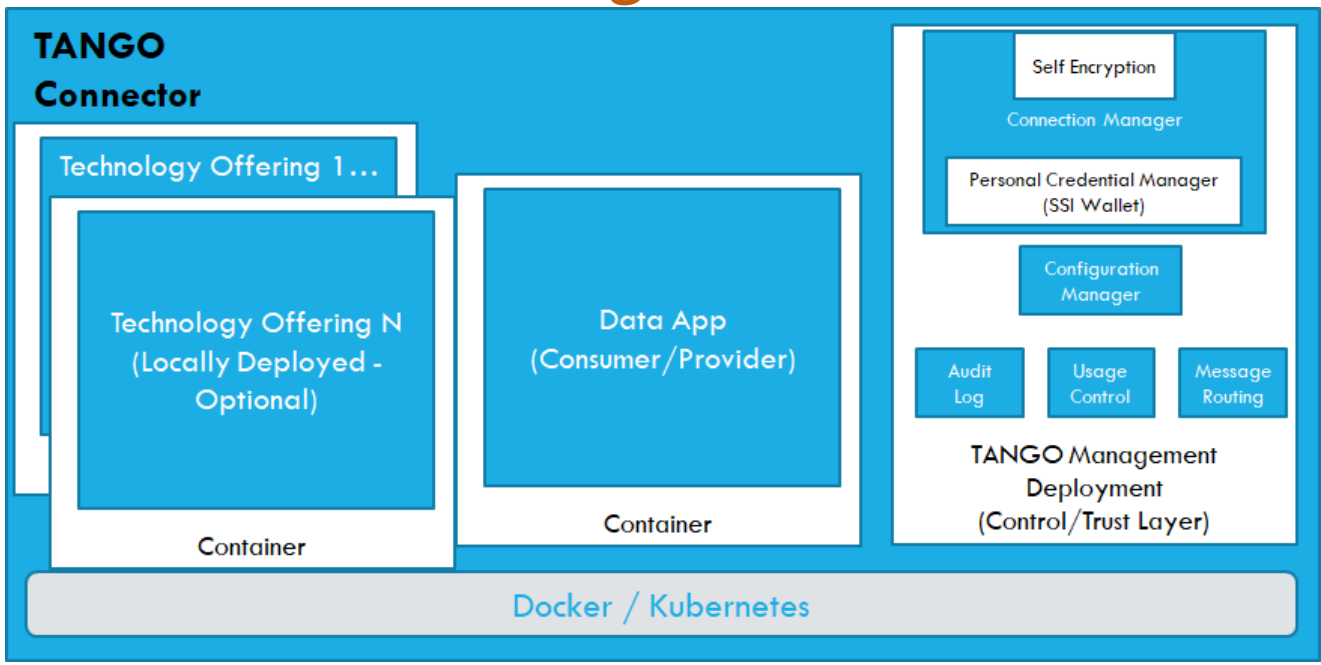


TANGO Connector

Management System

- Multiple data transfer and configuration endpoints.
- The TANGO Connector facilitates communication with other Connectors and their associated services;
- Only data that is intended to be shared with other TANGO entities is made public.
- Both internal and external communication are based on secure protocols such as HTTPS,
- The adoption of the IDS Communication Protocol is also considered

Encapsulation of management and trust ensuring services



TANGO Connector

Connection Manager

- Personal Credential Manager (SSI Wallet)
  - Mobile Wallet for Person(s)
  - Agent for devices
- Responsible for TANGO's ecosystem's authentication with the other Connectors.
  - It interacts with the corresponding modules of the other Connectors (SSI Wallets/SSI Agents) for the exchange of Decentralized Identifiers (DIDs) and with the Verifiable Credential Manager
- Decentralization of Identity Management and Authentication Processes
- Stores the Verifiable Credentials
- Digital tokens as proof of specific attributes using Zero-Knowledge Proof Techniques

TANGO's SSI solution → *expand the current functionalities of the Eclipse connector* (which integrates the principles of IDSA) concerning identity management.

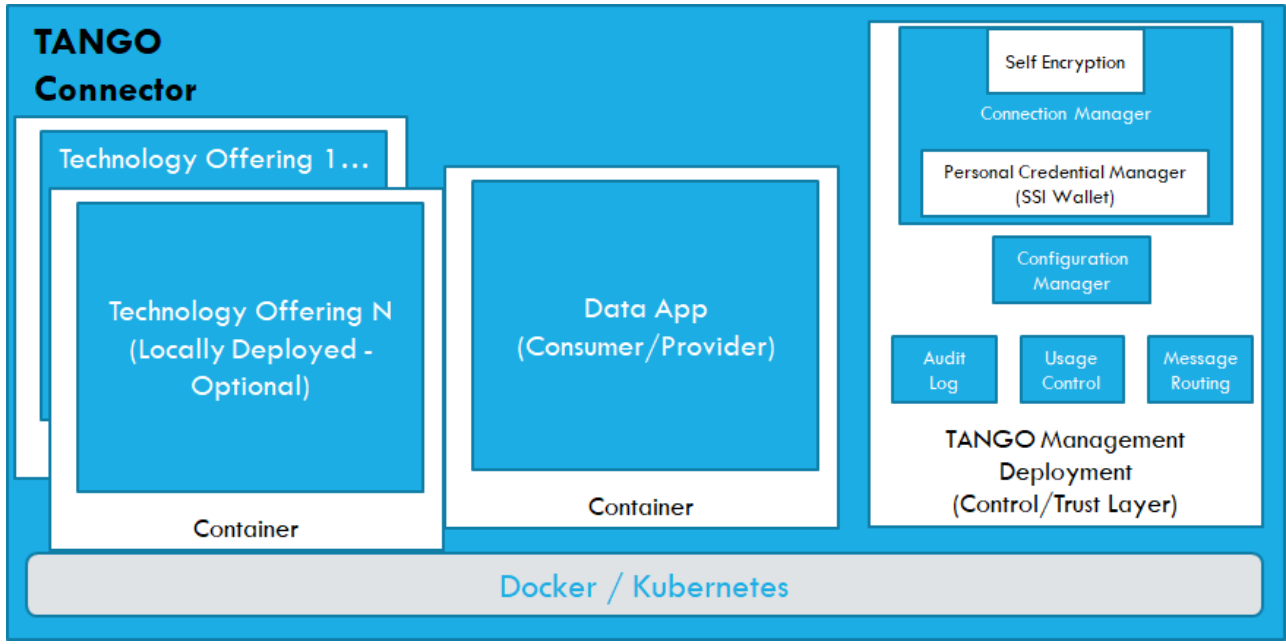
Managing and storing key pairs and

- the private keys of the entity associated with the Connector.
- provides the interfaces for gaining access to and managing cryptography keys, as SSI and other ecosystem operations require the use of public-key cryptography to manage digital signatures and the encryption and security of sensitive data.

TANGO Connector

Connection Manager

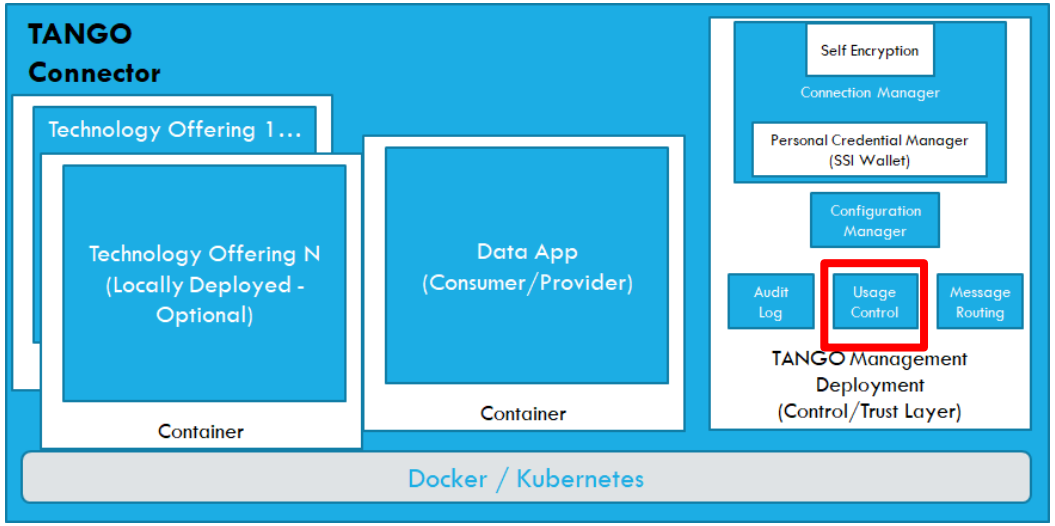
- Self-Encryption Module
  - encrypts data that will be exchanged between TANGO Connectors.
- Self-encryption ensures that data is encrypted prior to leaving the client's environment
- The self-encryption module communicates directly with the *Personal Credential Manager*, which stores the encryption/decryption keys.
- Relation with *the Attribute-Based Encryption tool* for encrypting the data according to an attribute-based policy defined by the data owner and decrypting them using the keys associated with the identity attributes of the Connector



TANGO Connector

Usage Control

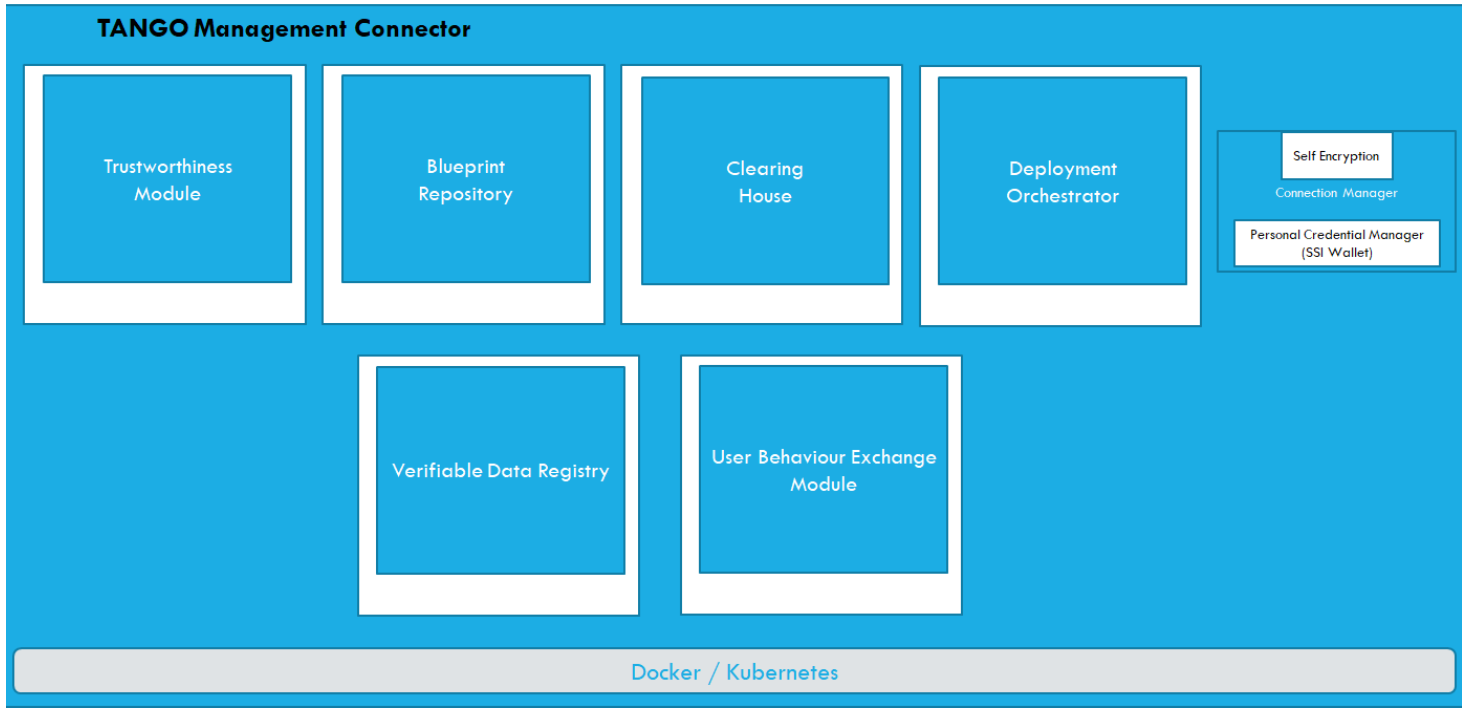
- XACML (eXtensible Access Control Markup Language) Standard to define policies and set ABAC (Attribute-Based Access Control) rules.
  - Policy Enforcement Point (PEP)
  - Policy Decision Point (PDP) Policy Information Point (PIP)
  - and Policy Administration Point (PAP).
- IDS Reference Model extends the access control model for the enforcement of usage rules by leveraging the aforementioned components
  - to monitor, intercept and assess the existing information of the packets
  - but also additional information (e.g. metadata: involved stakeholders, owner, consumer, key dates, issued date, expiration date, term of the rules, for how long the rule is valid, nature and value of the rule: a legal agreement or a contract) concerning the data flows.
- Data usage control in the TANGO architecture
  - follows the concept of the IDS Contract
  - leverages the concept of sticky policies to enforce Data Usage Control Policies
- Sticky policies include attributes related to user roles, resource properties and specify the conditions and the constraints that must be met so that a policy can be enforced.



TANGO Management Connector

A Special TANGO Connector

- contains all the necessary services and modules for the trustworthy management of the TANGO ecosystem and its transactions.
- a container management system that hosts the TANGO Management and Trust Services
  - for handling administrative and orchestration operations in the ecosystem, such as storing and managing repositories of configuration files, deploying TANGO connectors and configuring them in order to perform use-case specific operations, performing access control and enforcing usage control.
  - establish trust relationships within the ecosystem
  - handle authentication and identity management as well as evaluation of the trustworthiness of entities and monitoring transactions between them.
- interacts with and configures the TANGO Connectors.



TANGO Management Connector

Connection Manager
same module the TANGO Connector's Connection Manager

Deployment Orchestrator
a control-plane component to ensure the efficient, consistent deployment of various software components and services within the data space environment.

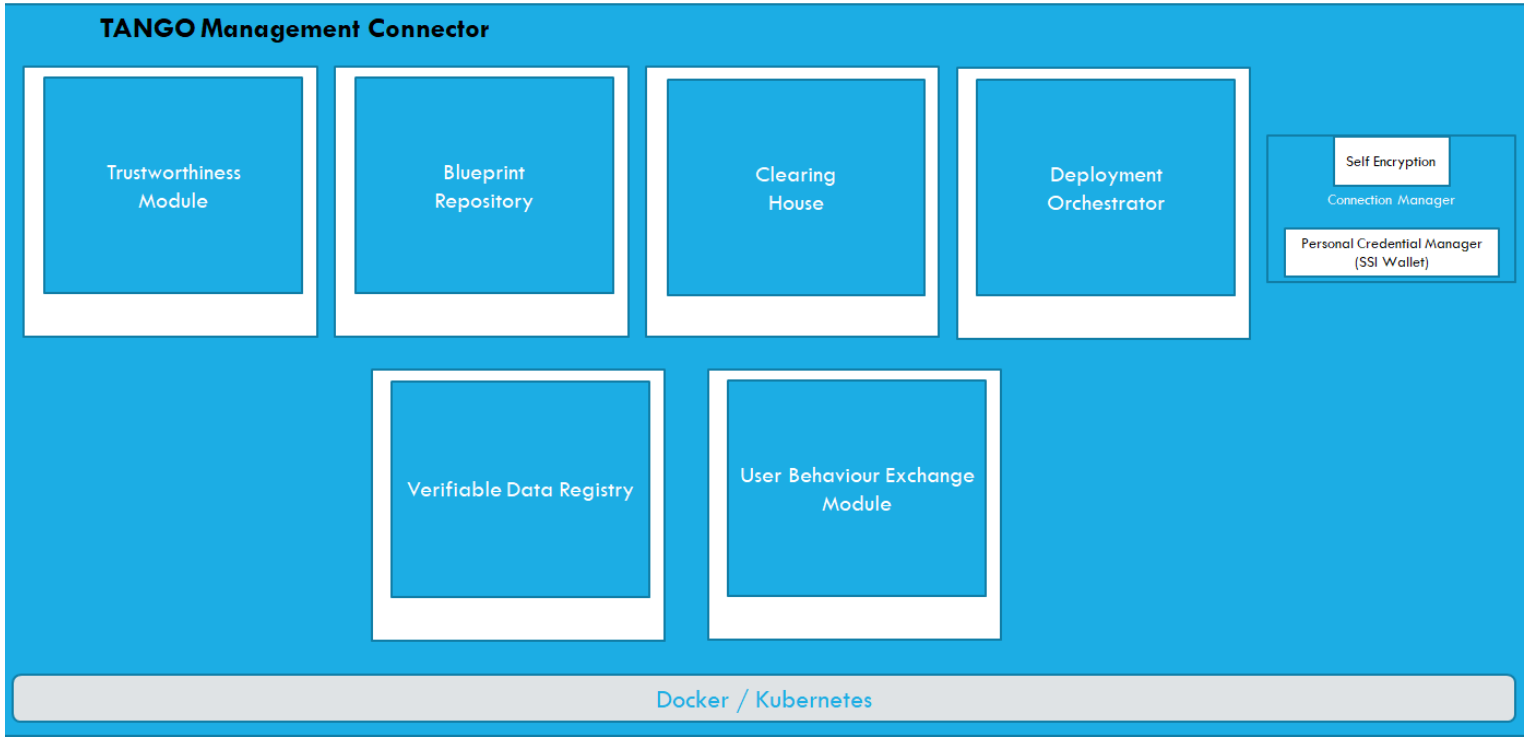
Blueprint Repository
a centralized storage or version control system

Clearing House
enables various functionalities related with the monitoring and recording every transaction that occurs in the TANGO ecosystem

Verifiable Data Registry
facilitates the creation, verification, and discovery of decentralized identifiers (DIDs) and DID documents. Both Centralized and Decentralized Approaches

Trustworthiness Module
assigns scores of trustworthiness to the participating entities / *input:* the attributes of each entity from its Verifiable Credentials /*output:* a calculated score of trustworthiness./ validates the Verifiable Credentials.

User Behavior Exchange Module
records user actions in privacy-preserving manner, in the format of Volatile Random Number (VRN) collections.



And what about sustainability in data operations?

- **The right choice**: Selecting lightweight options fit for purpose.
  - Blockchain: Very expensive in terms of energy. Only used when needed and for legally binding scenarios. Mainly identifiers stored in blockchain.
  - AI: Trying to minimise the footprint: Federated learning (less data movement), lightweight AutoML, MLOps and XAI.
  - Reduction in energy consumption in application execution for a single node (TornadoVM).
  - Openness: To add future green technology offerings into the architecture
- TANGO forecasts **renewable energy availability**
  - For efficient, cost-effective computing infrastructure management.
  - Enabling via RENOPS smart scheduling of heavyweight workloads (e.g., AI training, energy consumption in data centres) when and where renewable energy is available.
- **Evaluation**:
  - Assessing the energy efficiency of the TANGO Platform and several of its components.
  - Reports describing the performance improvement in terms of efficiency/energy consumption between existing solutions and the TANGO approaches.
  - Best practices and lessons learned.

DIGITAL TECHNOLOGIES ACTING AS A GATEKEEPER TO INFORMATION AND DATA FLOWS

Thank you!

https://tango-project.eu/

Anaxagoras Fotopoulos - EXUS AI Labs

a.fotopoulos@exus.ai

Follow us:

@tangoproject_eu

https://www.linkedin.com/company/tango-project-eu/

https://mastodon.uno/@tangoproject_eu

https://www.youtube.com/@tango-project

This project has received funding from the European Union's HE research and innovation programme under the grant agreement No. 101070052