tango-project.eu

TANGO

DIGITAL TECHNOLOGIES ACTING AS A GATEKEEPER TO INFORMATION AND DATA FLOWS

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

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

White Paper*:*

Ensuring Data Sovereignty: TANGO Platform Solution for Secure and Trusted Data Flows Across Europe – T8.6

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

Document Information

This section provides overall information about contributors and reviewers to the document along its iterative production.

List of Contributors	
Partner	Name
ANYSOL	Dolores Ordóñez
ECO	Ladan Raeisian
ECO	Lauresha Toska
ECO	Nelia Zinatullina
ECO	Peter Koller
EGI	Ilaria Fava
EGI	Renato Santana
EGI	Valeria Ardizzone
DBC	Ioannis Drivas
KUL	Alexandra Papageorgiou

Special thanks to Cáit Kinsella (ECO) for the thorough (external) review of this white paper.

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

Table of Contents

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

List of Acronyms

Acronyms that are used in the document, in alphabetical order.

Abbreviation / acronym	Description
DID	Decentralised Identifiers
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
IDSA	International Data Space Association
IIC	Industrial Internet Consortium
JWT-VC	JSON Web Tokens – Verifiable Credentials
LDP-VCs	Linked Data Proof – Verifiable Credentials
SIMPL	Smart middleware platform
TANGO	Digital Technologies ActiNg as Gatekeepers to information flOws
T8.6	Task 8.6, part of WP8
WPx	Work Package X

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

1 Introduction

1.1 Purpose and Structure of the Document

This second TANGO Project white paper focuses on the distributed trust framework that underpins the TANGO platform. It presents the key components that enable trustworthy data sharing and identity and access management as well as security and privacy mechanisms within TANGO's distributed infrastructure. Additionally, the paper outlines a set of policies and recommendations that are aligned with the TANGO platform's architectural principles.

Building on the conclusions of the first white paper (A TANGO Project White Paper on Distributed Infrastructures, Secure Data Exchange & Data Spaces[1]), this document draws on several public deliverables previously submitted by the TANGO consortium. These include:

- D2.3 – System Requirements and Specifications, Platform Architecture and Privacy, Ethical, Social and Legal Impact Assessment (final version)
- D3.1 – Distributed Privacy-Preserving Data Management and Storage (intermediate version)
- D3.2 – Distributed Privacy-Preserving Data Management and Storage (final version)
- D4.2 – Distributed Trust Management Framework (final version)

Following this introduction, the next two chapters explore the TANGO distributed trust management framework and associated policies and recommendations. The white paper concludes with a summary of key discussions and findings.

Unless otherwise stated, all figures and tables included in this white paper are sourced directly from the above deliverables.

1.2 TANGO: Infrastructure and Data Ecosystems

Effective data sharing across domains requires robust and interoperable infrastructure. This subchapter explores the key components and layers of interoperability essential for the TANGO platform, including cloud services, APIs and data integration tools. Interoperability, defined as the ability of systems, applications and organisations to access, exchange and interpret shared data, is fundamental to building resilient data ecosystems.

As outlined in Blueprint 2.0 of the Data Space Support Centre[2], effectively implementing data interoperability can enhance collaboration, drive innovation and improve decision-making across various sectors. Currently, various data space deployments are working on defining a common interoperability framework that will be linked to the development of SIMPL.

1.2.1 Infrastructure Considerations

The infrastructure supporting data ecosystems must be designed to facilitate interoperability. The TANGO platform and the components previously defined are part of the key elements:

[1] https://tango-project.eu/sites/default/files/uploads/A%20First%20TANGO%20White%20Paper%20-%20T8-6%20-%20FINAL%20%281%29.pdf
[2] https://dssc.eu/space/BVE2/1071251457/Data+Spaces+Blueprint+v2.0+-+Home

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

- **Cloud Services**: Scalable cloud solutions enable flexible data storage and processing, allowing disparate systems to communicate effectively.
- **APIs (Application Programming Interfaces)**: Well-defined APIs are essential for enabling various applications to communicate with one another, facilitating data exchange and interaction.
- **Data Integration Tools**: These tools help in merging data from different sources, ensuring that data can be aggregated and analysed uniformly.

1.2.2 Data Interoperability

Data interoperability comprises several layers, including:

- **Technical interoperability:**

  This relates to the hardware and software standards that enable data exchange. It includes using common protocols and formats to ensure that different systems can understand the data shared between them. The European Commission has launched SIMPL[3] as the middleware that will facilitate data space interoperability.

  The deployment of the different common European Data Spaces includes the definition of an architecture that will enable the implementation of cross-sectoral use cases, thus ensuring that data can flow from one sector to another without any technical issues.

- **Semantic interoperability:**

  This aspect focuses on the meaning of the data being exchanged. It ensures that data is interpreted consistently across different systems. Standard vocabularies and ontologies play a crucial role in achieving semantic interoperability. Semantic interoperability is very complex at a general level, but even more at sector level, as is the case with the tourism sector.

  The lack of a common semantic ontology complicates data sharing. Although there are some initiatives to working on this issue, they do not yet cover the whole ecosystem. FIWARE is working on defining data models to contribute to this semantic interoperability.

- **Governance interoperability:**

  This encompasses the policies and agreements between institutions to facilitate data sharing. Trust and shared governance are essential for effective collaboration. This governance should be secured by a neutral authority that will ensure compliance with the rules. Each sector is defining its own governance scheme based on the Rule and Role book methodology set by SITRA[4].

1.2.3 Used Data Models and Formats

In the pursuit of seamless data interoperability, various data models and formats are utilised:

- **Data Models:** Common data models such as Entity-Relationship Models (ER Models), Unified Modelling Language (UML) and others provide structured frameworks for organising data. These models help standardise how data is represented and structured, promoting more straightforward data exchanges. FIWARE's adoption of

[3] https://digital-strategy.ec.europa.eu/en/policies/simpl
[4] https://www.sitra.fi/en/publications/rulebook-for-a-fair-data-economy/

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

standardized data models enables semantic interoperability. These domain-specific models can be adapted to different contexts, facilitating consistent understanding and utilisation of data.

- **Data Formats:** Formats such as JSON (JavaScript Object Notation), XML (Extensible Markup Language) and CSV (Comma-Separated Values) are widely adopted for data representation. Choosing appropriate data formats is key to ensuring compatibility among various systems.
- **Standards**: Various standards, like those set by the World Wide Web Consortium (W3C), International Organisation for Standardisation (ISO) and industry-specific frameworks, guide data exchange practices. Compliance with these standards is vital for achieving effective interoperability. By leveraging the NGSI-LD standard[5] for linked data management, the FIWARE Context Broker[6] (Orion Context Broker) allows for efficient context data management and dynamic updates. This enhances the integration of diverse data sources in data spaces, supporting richer and more interconnected exchanges.

[5] https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.05.01_60/gs_cim009v010501p.pdf
[6] https://www.fiware.org/2020/12/11/fiware-context-broker-the-engine-for-future-energy-systems/

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

2 TANGO Distributed Trust Management Framework

This chapter provides an overview of the TANGO trust management framework and its core standards and technologies, TANGO highlighting those developed within the project and those that were selected from existing technologies or software.

2.1 Secure and Trustworthy Data Sharing

Within the TANGO framework, WP3 (Distributed Privacy-Preserving Data Management and Storage) focuses on ensuring secure data storage and distribution to support use case applications and other components within the TANGO ecosystem. The primary objectives of this WP include:

- Establishing a decentralised data-sharing ecosystem leveraging blockchain technology,
- Designing and implementing a dynamically configurable trustworthiness module,
- Evaluating security risks associated with data sharing and storage,
- Enabling users to retain full ownership of their data throughout its entire lifecycle,
- Ensuring data confidentiality and traceability through distributed encryption and decryption'
- Extending confidentiality principles to non-personal data.

At the heart of the TANGO platform, distributed data management, storage and sharing solutions play a critical role by interconnecting various tools that facilitate secure and tamper-proof data handling, sharing [T3.2] and reuse. These capabilities extend to multiple sectors, including public administration, smart hospitality, autonomous vehicles, smart manufacturing, banking and retail.

The distributed data management and sharing system will leverage energy-efficient blockchain technology [T3.1] to ensure data traceability, integrity and ownership while remaining compliant with GDPR regulations. Additionally, a distributed data tokenisation solution, designed with privacy and confidentiality at its core [T3.3], will enforce access control measures.to enhance security in data storage and sharing, a combination of distributed self-encryption/decryption and trust-based recovery solutions [T3.4] will be implemented, ensuring robust protection against unauthorised access.

Figure 1 (Overview of the WP3 components) represents the key tasks and components that support the distributed privacy-preserving data management system.

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

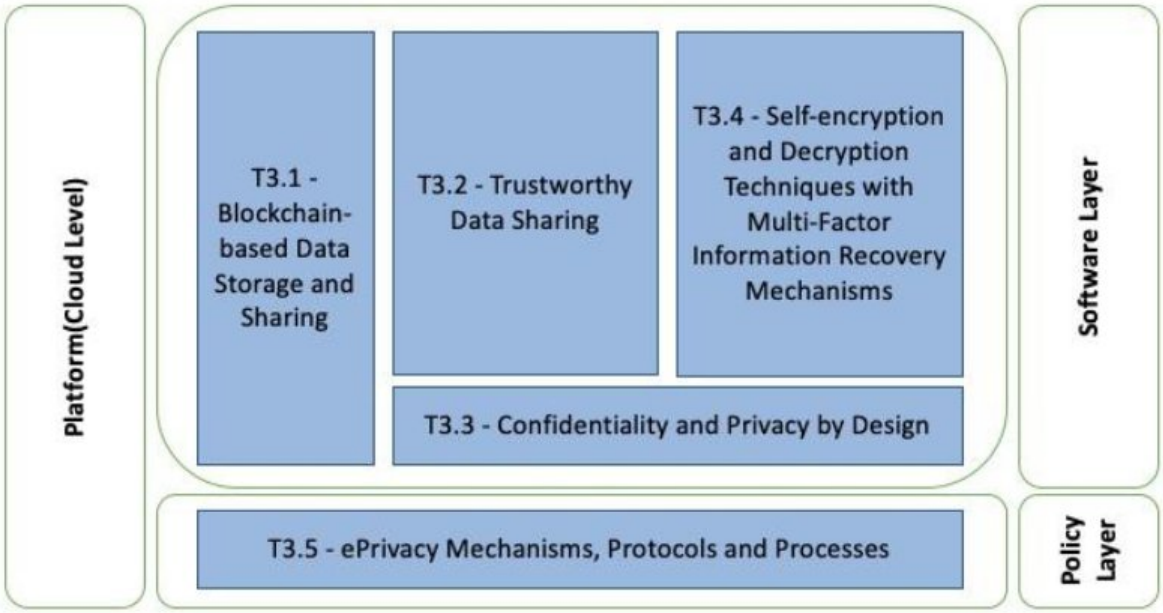

Figure 1: Overview of the WP3 components.

2.1.1 Blockchain-based data storage and sharing

TANGO's infrastructure for Pilot 5 (Public Administration)[7]uses a data-sharing platform called *Fides,* developed by the consortium member Norbloc. The Fides solution offers fully decentralised, legally compliant storage and enhanced data redundancy.The Norbloc Fides[8] ecosystem offers several core features that support secure and compliant data-sharing operations. The following features were implemented for TANGO:

- **Explicit consent management.** This feature ensures that users grant clear and verifiable consent before their data is accessed or shared. Proofs of consent and data access permissions are securely facilitated and recorded.
- **Private data sharing in regulated environments.** The component is designed for use cases within a strict regulatory framework and when two or more independent parties are involved. In cases where privacy regulations are less restrictive or no private data by means of the regulations is shared, alternative TANGO components shall be used.
- **Immutable audit logs.** The integration of blockchain technology ensures that all metadata access events are permanently recorded and cannot be altered, providing transparency and security for internal and external audits.

Two proprietary Norbloc components from the Fides' internal infrastructure, namely DRILL and DnAMS They rely on blockchain technologies to enable decentralised data storage and access management:

- **DRILL (Data Redundancy in Legal Limitations**): A P2P storage network consisting of DRILL nodes, which are integral to every Fides node. It is designed for secure data storage while ensuring compliance with privacy regulations such as GDPR. To support

[7] https://tango-project.eu/pilots/public-administration
[8] https://norbloc.com/fides/

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

this, DRILL incorporates symmetric encryption as a core feature. DRILL encrypts and fragments data before distributing it across multiple storage peers, preventing any single node from reconstructing complete datasets.

- **DnAMS (Decentralised Access Management System):** It manages symmetric data keys used for the DRILL encryption of individual data pieces. It also manages the private keys of data subjects, eliminating the need for separate external wallets. DnAMS controls access rights by managing the corresponding encryption keys and only releases a key when presented with a valid *data access permission proof* (a "proof of consent"). When a *data access permission proof* is provided, the DnAMS component retrieves relevant information from the blockchain, enabling a DRILL peer to gather all chunks from other peers and reconstruct the encrypted data. The DnAMS component then releases the encryption key, allowing decryption of the reconstructed data.
- **Blockchain**: This component serves as the foundation for ensuring immutable storage, secure timestamping and verifiable data integrity. Blockchain technology is heavily utilised in DRILL (storing data hashes) and DnAMS (storing proofs of consent/data access permission proofs). By default, Fides offers Hyperledger, but in TANGO Fabric blockchain will be fully utilised. In general, any private blockchain can be used.

Fides is deployed as a decentralised network consisting of multiple interconnected P2P systems and installed as a set of nodes at each participant's premises. These include the DRILL P2P network as the decentralised distributed legally compliant data backend, the DnAMS P2P network for key and access management and the Blockchain P2P network, which reinforces data integrity through immutability and reliable timestamping.

To further improve its functionality and interoperability, Fides will introduce additional APIs to provide decentralised data storage and sharing platform capabilities to other TANGO components:

- **Data API** will enable other components to store and retrieve data securely within the DRILL system,
- **Consent API** will facilitate managing data access permissions within the DnAMS component.

These enhancements aim to align Fides with EU industry standards such as IDSA, GAIA-X and DID frameworks, thereby expanding its potential applications and making it a more versatile solution for decentralised data management.

2.1.2 Trustworthy data sharing

TANGO's infrastructure utilises a row of components and a data space connector to provide trustworthy data sharing.

2.1.2.1 TANGO components for trustworthy data sharing

Trustworthy data sharing is essential in all use cases and data sharing ecosystems. It involves tools that support policies for access and usage control but does not enforce these policies directly. Instead, it helps to ensure controlled and secure data usage across entities, contributing to trustworthiness in data sharing. This trust is crucial for creating an environment where participants can confidently engage in privacy-preserving, secure data use. By incorporating trustworthiness-focused policies, the ecosystem fosters collaboration and maximises the value of shared data. Thus, data access and usage should be policy-driven and supported by enforcement mechanisms that control how data is processed, stored, aggregated, or forwarded.

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

Three major components were developed[9] to address these issues:

- **Trustworthiness Scoring Module (TSM):** The TSM is a backend solution designed to contribute to the Policy Information Point (PIP). The PIP gathers information that helps the Policy Decision Point (PDP) make decisions regarding access control, which are then enforced by the Policy Enforcement Point (PEP). The TSM can also be used to allow resource scheduling by a use case-specific component (e.g., in the Autonomous Vehicles use case). It supports a configurable scoring scheme based on system characteristics aligned with the IIC Trustworthiness schema and continuously gathered attribute data. The TSM provides APIs for configuring, submitting data and evaluating trustworthiness scores. Data is associated with a registered user identified by their DID and attribute data is stored in a time series based on a configurable window. The trustworthiness score can then be used by the PEP or other components (e.g., for resource access or scheduling decisions).

- **Usage Control – Privacy Risk Score (PRS):** The PRS is a backend solution that supports the TSM in the automotive use case by providing privacy scores, which can also operate independently. It performs quality assurance tests on anonymised data and generates a time series of privacy scores, contributing to the final trustworthiness score in the TSM. Images are collected, anonymised and uploaded to the cloud for assessment of privacy protection. A module evaluates the quality of image anonymisations across various scenarios to ensure privacy in vehicles. The PRS can also be used for experimenting with different anonymisation methods under various privacy settings. Developed using open-source data, it includes an anonymisation module, implemented due to confidentiality issues with the autonomous driving use case's proprietary module. The anonymisation approach closely aligns with the use case provider's procedure.

- **Ubiquitous Personal Context Vectors (UPCVs):** The UPCV recommendation technology consists of two main components: a vendor-side server that manages item data and a web app for users, which stores personal data and generates recommendations. Since vendors only have item data and no user information, data can be shared between vendors offering similar items. This privacy-preserving approach could also support business intelligence in multi-vendor environments.
  The system tracks user behaviour anonymously using a privacy wallet containing Volatile Random Numbers (VRNs), which cannot be linked to individuals. When a user views an item, VRNs are exchanged between the user's and the item's privacy wallets. Over time, users and items with similar interactions accumulate matching VRNs, enabling item recommendations based on privacy wallet similarities. Even though the component was developed for the Hospitality use case, UPCV technology has also been evaluated for analysing shopping baskets in Retail use case.

2.1.2.2 Trustworthy data sharing via FIWARE Data Space Connector

To ensure a robust and scalable data exchange framework, the TANGO project conducted a thorough evaluation of several open-source data space connectors. The goal was to integrate a solution that aligned with TANGO's architecture while minimising the need for custom

[9] D3.1: Chapter 3 (https://tango-project.eu/sites/default/files/materials/TANGO_D3.1%20Distributed%20Privacy-preserving%20Data%20Management%20and%20Storage_v1.0.pdf)

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

development. The FIWARE Data Space Connector was ultimately selected based on its adherence to data space standards, security capabilities and modularity.

FIWARE's alignment with DSBA Technical Convergence recommendations[10], support for SSI and attribute-based access control (ABAC) made it a strong candidate. Additionally, the connector benefits from active community maintenance and containerised, flexible architecture that supports easy deployment and customisation. While the FIWARE Data Space Connector is still maturing and initially focuses on ETSI NGSI-LD data exchange, its adaptability made it a suitable choice for TANGO's broader use cases.

TANGO integrates several FIWARE Data Space Connector components while modifying, or extending, others to fit project needs. Notably, TANGO replaced, or enhanced, the Verifier, Issuer and Policy Decision Point (PDP) to align with its security and authorisation requirements[11].

The TANGO SSI Agent, deployed on the Data Consumer side, facilitates Verifiable Credentials (VCs) issuance and management. Users present VCs to the Data Provider's FIWARE Data Space Connector to gain authorisation for data services. The authentication process involves verifying:

- The type and scope of the VC against the requested authorisation.
- The validity of the VC and its cryptographic signature.
- The issuer's authorisation via trusted registries.

To enable seamless integration, the FIWARE Data Space Connector supports provisioning calls for new credential types, JWT VCs and configurable authorisation formats.

TANGO extends the FIWARE Data Space Connector's security model by introducing additional policy enforcement capabilities. The architecture follows the ABAC approach and integrates:

- **Policy Administration Point (PAP):** Defines and distributes access control policies.
- **Policy Information Point (PIP):** Supplies dynamic attribute data for authorisation decisions.
- **Policy Enforcement Point (PEP)** and **Policy Decision Point (PDP):** Evaluate access requests using SSI Verifier-issued JWTs containing VCs.

To further enhance security, the decision-making process issues capability tokens, which serve as authentication tokens, defining permissions for authorised operations.

Beyond core integration, TANGO enhances the FIWARE Data Space Connector with additional security and functionality improvements, including:

- **Advanced Encryption Mechanisms**: Implementing CP-ABE (Ciphertext-Policy Attribute-Based Encryption) and self-encryption to complement the existing PDP/PEP security model.
- **Replacement of Orion-LD**: Substituting backend systems to better support AI and data analysis use cases in WP7.

---

[10] https://data-spaces-business-alliance.eu/wp-content/uploads/dlm_uploads/Data-Spaces-Business-Alliance-Technical-Convergence-V2.pdf

[11] D3.1: Chapter 3.3 (https://tango-project.eu/sites/default/files/materials/TANGO_D3.1%20Distributed%20Privacy-preserving%20Data%20Management%20and%20Storage_v1.0.pdf)

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

- **Portal Redesign and Message Routing**: Enhancing user experience and enabling seamless data flow between backend components, encryption services and existing FIWARE modules.

2.1.3 Confidentiality and privacy by design

Confidentiality and Privacy by Design embed privacy considerations into system architecture from the outset, ensuring that data protection is not an afterthought but a fundamental principle. This approach anticipates privacy risks before they occur, making privacy the default setting. Throughout the data lifecycle, security measures must be applied to maintain transparency and compliance with legal requirements, including the GDPR. TANGO aligns with ISO 31700-1:2023[12] to integrate these principles into its design process.

TANGO employs two key mechanisms to FIWARE to achieve these goals:

1) Data encryption uses CP-ABE, enabling producers to encrypt data based on attribute-based policies. After access is granted, consumers can only decrypt data if their identity attributes match the policy, ensuring strict access control and confidentiality. Sticky Policies ensure that machine-readable policies remain attached to the data throughout its journey, enforcing permissions and restrictions consistently.
2) User consent and access control are managed through the XACML framework, which includes the PEP, PDP, PAP and PIP. These components, combined with Verifiable Credentials and zero-knowledge proofs from the SSI module, determine user authorisation for asset access.

TANGO's confidentiality and privacy framework follows two interrelated processes. First, authentication and authorisation rely on Verifiable Credentials (VCs**)** and Verifiable Presentations (VPs) to grant access. Users authenticate through the connector, request access to assets and provide VCs. A verifier ensures that the user is a trusted participant and that the credentials are valid. If the verification process is successful, the user receives a token that allows access, enforced by PEP and PDP. This verification process ensures that only authorised users are granted access, reinforcing confidentiality principles. The dataflow between the PEP and PDP is depicted in Figure 2.

Second, data encryption and decryption mechanisms protect sensitive information. Producers encrypt data using CP-ABE and attach sticky policies. Once a consumer is authorised, they receive the encrypted data, which can only be decrypted using a key linked to their identity attributes. This ensures that only authorised users can access the information, maintaining confidentiality throughout the data lifecycle. The CP-ABE client module operates on both ends, ensuring that data encryption remains robust and consistently enforced.

[12] https://www.iso.org/obp/ui/en/#iso:std:iso:31700:-1:ed-1:v1:en

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

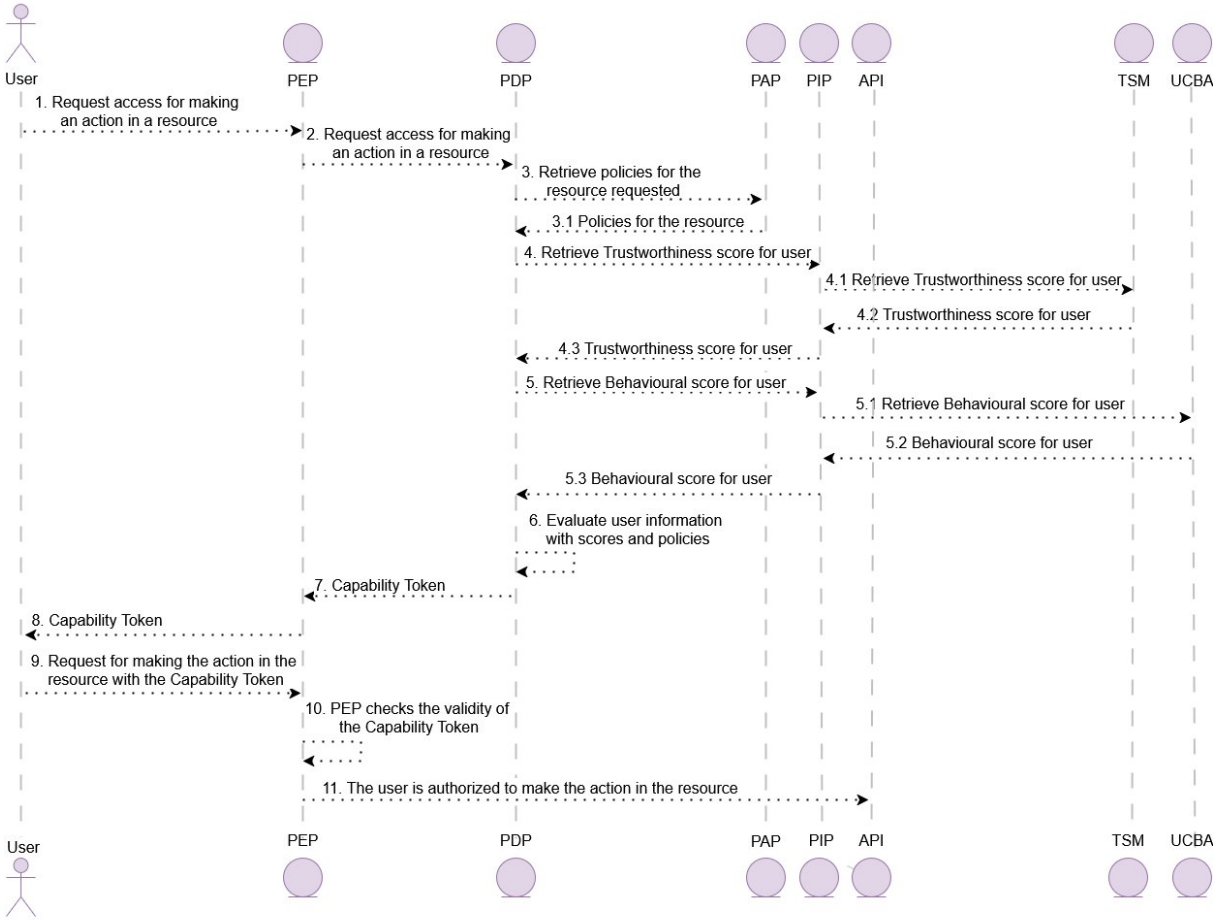

Figure 2: Internal Workflow of the PEP/PDP Component for User Access Requests

TANGO's architecture integrates several key components to support Confidentiality and Privacy by Design. The **ABE Toolse**t consists of three core submodules:

- The **Key Generator** issues cryptographic keys for encryption and decryption.
- The **Encryptor,** used by data providers, applies CP-ABE encryption to secure data and define access policies.
- The **Decryptor** enables authorised users to access encrypted data if their attributes match the policy, ensuring selective decryption.

Usage Control is managed via the XACML framework:

1. **PDP** evaluates access policies by processing identity attributes and making informed decisions.
2. **PEP** intercepts access requests and enforces authorisation decisions, ensuring only permitted users can proceed.
3. **PIP** provides external contextual information to enhance policy enforcement, supporting dynamic and adaptive access control.
4. **PAP** is used when the PDP needs to retrieve policies that govern access to a specific resource or service and to register new policies.

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

Additionally, signature verification ensures the authenticity and integrity of data by allowing consumers to verify digital signatures using the provider's public key. The data provider generates a digital signature using their private key, ensuring that the integrity of the data remains intact. Consumers can then use the provider's public key to decrypt and verify the signature, confirming that the data has not been altered during transmission and originates from a trusted entity. This mechanism adds an additional layer of security and trustworthiness to the data-sharing process.

2.1.4 Self-encryption and decryption techniques with multi-factor recovery

This section introduces a secured encryption/recovery mechanism designed to support the storage and distribution of confidential information for TANGO use cases. The core functionality consists of two primary components: the self-encryption and decryption module and the multi-factor information recovery (MFIR) mechanism. The system ensures that confidential data remains protected during distribution by using encryption and enhanced security features, such as multi-factor recovery, to prevent unauthorised access.

Self-encryption is a unique form of encryption where the key to encrypt a document is not supplied by the user. Instead, the document's own contents generate the key, ensuring that even a minor change in the document results in a significantly different encrypted version. This technique guarantees that each encrypted document has a unique key, making it more secure than traditional methods.

The multi-factor information recovery mechanism adds another layer of security. This mechanism splits the encryption key into multiple pieces and distributes them among several participants or entities. To decrypt the document, a certain threshold of these key shares is required. This makes it less likely that malicious actors will have enough access to recover the key, thus ensuring greater security.

SEDSS with MFIR consists of four key modules: encryption, decryption, multi-factor information sharing and multi-factor information recovery. The encryption and decryption modules are linked to the TANGO framework's data connector, while the sharing and recovery modules support secure key management.

After encryption, the encrypted data and shared keys are stored in a user-specified location (e.g., remote storage or a database). During decryption, a request containing key fragments and the data location is submitted. The multi-factor recovery module reconstructs the original encryption key, enabling decryption. The recovered plain text is then returned to the user via the data connector.

Figure 3 (System architecture of the self-encryption and decryption with multi-factor information recovery system). shows the system architecture of the self-encryption and decryption with multi-factor information recovery system.

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

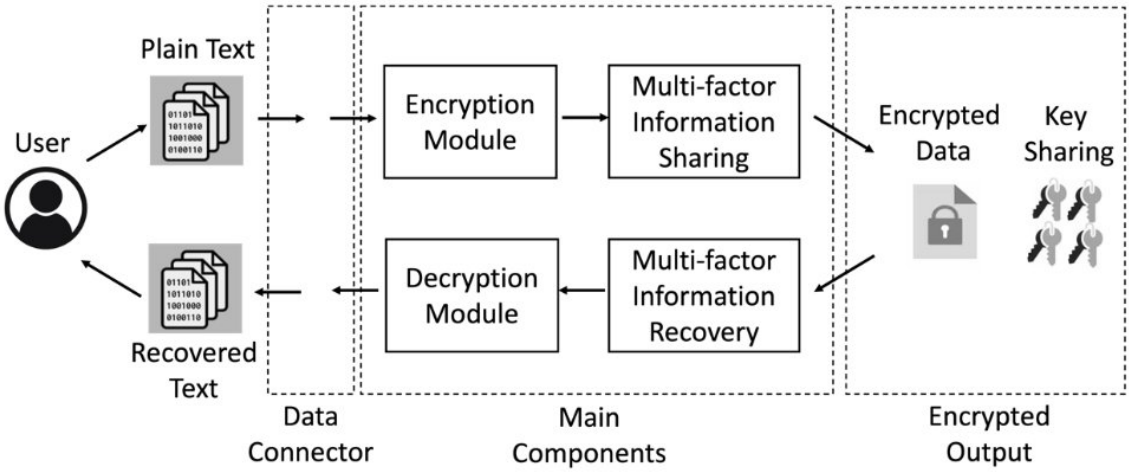

Figure 3: System architecture of the self-encryption and decryption with multi-factor information recovery system.

The self-encryption and decryption module is designed to be used as a callable interface within the TANGO project. It depends on the Data Connector to pass the necessary parameters and data. Additionally, the Fides component may be used to store the encrypted data and keys for users who do not have their own storage service.

2.2 Identity and Access Management

The TANGO project's approach to Identity and Access Management (IAM)[13] is designed to provide a decentralised, trustworthy and user-centric architecture for handling identities, authentication and access control. The architecture integrates advanced technologies such as Self-Sovereign Identity (SSI), seamless onboarding mechanisms and continuous behavioural authentication methods for both users and devices. These technologies contribute to building a robust distributed trust framework that underpins secure and privacy-preserving access to the TANGO platform and its services.

2.2.1 SSI management

The foundation of TANGO's IAM lies in the deployment of Self-Sovereign Identity (SSI), which enables users and organisations to own, manage and control their digital identities without reliance on a centralised authority. TANGO has implemented SSI components aligned with OpenID standards[14] and European Blockchain Services Infrastructure (EBSI) specifications[15]. This includes support for W3C Verifiable Credentials (VCs), DIDs and cryptographic proofs such as Zero-Knowledge Proofs (ZKPs).

The SSI system comprises two core components: the SSI Agent and the SSI Wallet. The SSI Agent supports both credential issuance and verification roles. It handles credential lifecycle processes, including DID generation, verifiable presentation construction and validation, cryptographic proof management and integration with data registries. The Wallet interacts with the Agent to enable credential storage, presentation and selective disclosure. There are two

[13] https://en.wikipedia.org/wiki/Identity_and_access_management
[14] https://openid.net/developers/specs/
[15] https://hub.ebsi.eu/apis

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

versions of the wallet: one that supports JWT-VCs with granular disclosure and another that incorporates ZKPs and supports machine-to-machine (M2M) interactions and LDP-VCs.

2.2.1.1 Credential Issuance and Verification Process

To ensure interoperability across platforms, the SSI implementation supports OID4VCI[16] and OID4VP[17] protocols, along with the EBSI conformance profiles. Integration with the FIWARE Data Space Connector (DSC) has been a key milestone, allowing TANGO's SSI components to interoperate with external trust frameworks and data spaces. Credential formats supported include ePassport-based VCs for natural persons, Employee Credential and Customer Credential for organisational roles, all issued and verified within a standard-compliant SSI framework.

2.2.1.2 Interoperability with External Systems

The integration of TANGO's SSI framework with GAIA-X and IDSA ensures compliance with EU-wide interoperability requirements. By adopting EBSI-conformant credential verification, the system enhances cross-platform trust while maintaining decentralised control over identity attributes.

To summarise, the key functionalities of the SSI solution include:

- **DIDs**: Secure, decentralised identity generation and resolution without reliance on centralised authorities.
- **Credential Lifecycle Management:** Efficient issuance, verification and management of Verifiable Credentials.
- **Cryptographic and ZKP Capabilities:** Use of digital signatures, encryption and Zero-Knowledge Proofs for selective disclosure and secure authentication.
- **Granular Disclosure and Privacy Preservation:** Selective data sharing capabilities embedded in the SSI Wallet implementations.
- **M2M Authentication:** Support for autonomous identity negotiation between IoT devices within trusted data spaces.

2.2.2 Seamless onboarding for users and devices

To complement the decentralised identity infrastructure, TANGO incorporates a seamless onboarding process for both individuals and devices. This ensures that identities are not only self-managed and verifiable but also issued through secure, privacy-preserving and user-friendly procedures that align with regulatory and operational requirements.

2.2.2.1 ePassport-Based Identity Verification

TANGO's onboarding process is designed to be secure, efficient and user-friendly, minimising friction while maintaining rigorous identity verification. The seamless onboarding component developed in WP4 (Task 4.2) focuses on remote identity verification based on government-issued e-passports. This system includes a mobile application and SDK capable of reading and validating e-passport data, leveraging NFC technology.

[16] https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
[17] https://openid.net/sg/openid4vc/

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

The onboarding process includes multiple layers of validation such as document authenticity checks, biometric face matching and liveness detection. This process ensures that only legitimate users are issued verifiable credentials. These credentials are then passed to the SSI wallet for ongoing identity management.

2.2.2.2 Integration with IoT and Legal Entity Onboarding

A critical development in this domain is the extension of onboarding capabilities to legal entities and IoT devices. While natural person onboarding is handled through mobile applications, organisational identity onboarding is achieved via integration with registries such as the EBSI Trusted Issuer Registry[18]. For IoT devices that are not resource-constrained, identity provisioning is performed through machine-to-machine SSI flows, enabling credential issuance and autonomous authentication in line with DSBA guidelines.

2.2.3 User Continuous Behavioural Authentication

Continuous authentication of users plays a critical role in maintaining the security posture of a distributed and dynamic system like TANGO. Rather than relying solely on one-time logins or static credentials, TANGO continuously assesses user identity through behavioural signals gathered during regular usage. This method supports a zero-trust approach while improving user experience by reducing the need for intrusive re-authentication events.

In addition to initial identity verification, TANGO enhances identity assurance through continuous user authentication mechanisms. The User Continuous Behavioural Authentication (UCBA) component is designed to authenticate users dynamically by analysing behavioural patterns collected from mobile devices during interaction with services.

Setup requires a selfie or passport photo, which is verified using security mechanisms. The component can fully replace traditional password systems by linking a unique user ID with biometric and behavioural data. It can also serve as a secondary authentication method and complies with PSD2 regulations for strong customer authentication, making it a secure alternative to one-time passwords, particularly for financial transactions.

The UCBA system includes an SDK integrated into a mobile application and a backend server responsible for processing and classifying behavioural data. Key behavioural traits include interaction patterns, usage context and system logs. To assess the trust level, a risk score is computed based on the similarity of current behaviour to known user profiles. Manual labelling processes have been incorporated to improve the accuracy of session classification.

The component supports session management, API access for TANGO components and real-time decision-making based on behavioural analytics. This contributes to secure, passive and user-friendly authentication, maintaining security without repeated credential entry.

2.2.4 Device Continuous Behavioural Authentication

Complementing user authentication, the Device Continuous Behavioural Authentication (DCBA) component ensures that the physical devices accessing TANGO services remain under legitimate control. The DCBA component continuously monitors system-level behaviours to distinguish between authorised and unauthorised use.

[18] https://hub.ebsi.eu/apis/conformance/trusted-issuers-registry/v5

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

The system operates by capturing a broad set of behavioural indicators from Android devices, including logs related to battery status, Bluetooth activity, network conditions, location changes and application usage patterns. These logs are processed to build a behavioural fingerprint of the device, which is used to maintain persistent authentication over time.

A key distinction between UCBA and DCBA is their focus: while UCBA prioritises behavioural patterns in user interaction, DCBA relies on device-specific attributes to verify legitimacy. Both components work in tandem to create a seamless yet highly secure authentication framework.

By integrating user and device behavioural authentication within the broader IAM framework, TANGO enforces a zero-trust approach, ensuring continuous identity verification at multiple levels. These IAM components collectively strengthen the security and trustworthiness of the TANGO platform, supporting its use across diverse operational domains and pilot scenarios.

2.3 Security and Privacy Enhancements

Ensuring data confidentiality, integrity and compliance with ethical and regulatory frameworks is central to TANGO's design. Security and privacy are not viewed as afterthoughts but are embedded deeply within both infrastructure and AI-driven components. This chapter outlines the concrete mechanisms developed within TANGO to enhance security and privacy, focusing on side-channel attack mitigation and privacy threat modelling for AI.

2.3.1 Hardening against side-channel attacks

TANGO addresses low-level hardware vulnerabilities through dedicated research and implementation of compiler-based countermeasures, particularly targeting side-channel attacks that are critical to embedded systems and IoT devices. These attacks exploit physical leakage – such as power consumption, electromagnetic emissions or timing behaviour – to infer sensitive information like cryptographic keys.

The core of TANGO's mitigation strategy lies in a hardened cryptographic component, primarily the implementation of a masked AES (Advanced Encryption Standard) algorithm. The masking technique involves splitting sensitive intermediate values into random shares, ensuring that no single trace reveals meaningful information. This implementation, optimised for the smart hospitality pilot, significantly reduces the effectiveness of side-channel analysis.

TANGO's security enhancements combine multiple techniques:

- **Masking countermeasures**: Hides the correlation between intermediate values and leaked data.
- **Hiding countermeasures**: Introduces noise or randomisation to disrupt attacker observations. This is done by combining code polymorphism and loop shuffling

A hybrid technique combining both approaches was successfully validated in lab settings, with real-world deployment prepared for environments using embedded or IoT hardware.

2.3.2 Privacy threat modelling & identification for trustworthy AI

Within TANGO's AI-based components, privacy risks are addressed systematically through the Privacy Enhancing Component (PEC) and the Privacy Assurance Tool (PAT), developed under WP5.4. These tools perform proactive threat modelling and provide actionable insights for mitigating privacy risks in machine learning pipelines.

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

The Privacy Enhancing Component streamlines the Data Protection Impact Assessment (DPIA) process, as required by the GDPR and the EU AI Act[19]. Through its graphical interface, PEC helps organisations document data flows and processes (including AI applications), identify cyber threats, assess their impact and recommend risk mitigation measures. This ensures compliance with EU data protection regulations while improving privacy management.

PEC incorporates a multi-step methodology:

- **Privacy Impact Assessment for AI:** PEC enables targeted privacy impact assessments for AI/ML-powered systems. The system specifically evaluates AI/ML processes to identify potential threats to AI models.
  It analyses privacy risks that may arise from the use of AI technologies. Based on this analysis, PEC recommends appropriate safeguards to mitigate identified risks.

- **Threat Management:** PEC consolidates threat assessment reports and presents them in a structured format. This allows users to efficiently manage privacy threats and implement suitable countermeasures. The threat assessment covers both traditional IT services and processes as well as modern AI applications that handle sensitive and personal data.

- **LLM for Recommendations:** PEC integrates Large Language Models (LLMs) to enhance recommendations for countermeasures against identified threats. Through LLM integration, the system provides more detailed explanations of the recommended safeguards. Users receive well-founded justifications for the selection of specific security controls, helping to mitigate risks effectively. This improves decision-making and enhances transparency in privacy protection measures.

The Privacy Assurance Tool[20] provides a variety of features aimed at strengthening data privacy and security. It supports data sharing between users and organisations by giving users confidence in the protection of their personal information. Additionally, PAT enables privacy monitoring, allowing both parties to track data sharing activities, manage consent and identify any privacy risks associated with the requested data throughout its lifecycle. PAT complements PEC by offering a secure, role-based data exchange and compliance-checking environment.

PAT is distinguished by its three main features and contributions:

- **Secure Framework:** PAT is designed with strong security measures, employing encryption to safeguard data both during transmission and while at rest. This ensures that unauthorised entities cannot access or interpret the data, maintaining its confidentiality and making PAT a secure solution for data exchange.
- **Trusted and Authentic Record:** PAT guarantees data accuracy and consistency by preventing unauthorised alterations during transmission. It ensures that the data arrives at its destination in the exact form in which it was sent, thereby preserving its integrity.
- **Role-Based Access:** While creating a consent form within a data controller's PAT environment, PAT can retrieve a list of employees – along with their roles and intended purposes – to assist data controllers in generating GDPR-compliant consent request forms.

[19] https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)769509
[20] https://securecontrolsframework.com/

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

The privacy threat modelling approach draws on NIST's privacy engineering methodology and adapts it to dynamic AI environments. Key techniques include:

- **Mapping Data Flows** to attack scenarios and problematic data actions.
- **Identifying Privacy Engineering Objectives**, including predictability, manageability and disassociability.
- **Risk Visualisation and Reporting** to inform data scientists and system integrators.

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

3 TANGO Distributed Infrastructures: Policies and Recommendations

In the digital landscape of the TANGO Project, ensuring the secure exchange of data is essential to maintaining the integrity and confidentiality of information.

This chapter introduces a comprehensive framework designed to safeguard data through robust encryption, secure communication protocols and stringent access controls.

It emphasises the implementation of Identity and Access Management (IAM) and Data Loss Prevention (DLP) measures, as well as the need for ongoing security training and audits. Furthermore, it explores the development and enforcement of Contract and Runtime Policies, supported by tools such as the Open Digital Rights Language (ODRL), to ensure the effective management and compliance of data exchange agreements.

3.1 Privacy and security legal requirements

The policies presented in Section 3 of the first TANGO White Paper are not mere theoretical guidelines; they are actively embedded in the project's design and operations. Each policy is implemented through concrete technical features and then analysed from a legal standpoint to ensure that the system's operation aligns with regulatory expectations.

This sub-chapter presents a detailed, policy-by-policy exposition of how these compliance measures have been applied in practice. By bridging the gap between legal theory and technological application, this evaluation serves as a roadmap for designing distributed data infrastructures that uphold the highest standards of privacy, transparency and accountability. A more detailed analysis of the observations made below can be found in deliverable D3.2[21].

3.1.1 Compliance Policies

3.1.1.1 Data mapping

Responsible data handling requires clarity about what is being processed. In the context of the **Blockchain-Based Data Storage and Sharing** component, this principle is partially embodied through DRILL, the system responsible for storing encrypted data chunks. Here, the types of data anticipated for processing are predetermined and scoped with the assumption of the highest sensitivity. The DnAMS module further strengthens this structure by governing consent through verifiable proof mechanisms. However, the peer-to-peer topology of this system introduces the risk that individual nodes may misinterpret, mishandle, or inconsistently categorise data types – particularly when metadata classification or schema enforcement mechanisms are lacking. This means that a complete data taxonomy, bolstered by metadata tagging and enforced uniformly across all nodes, is essential.

The **Confidentiality and Privacy by Design** component addresses data type specificity through attribute-based encryption (CP-ABE) and access control mechanisms (XAMCL). While this allows data access to be constrained based on defined user attributes and roles, it does not automatically validate the nature or legitimacy of the underlying data. There is an evident need to implement automated tagging and classification checks to pre-empt the introduction of data that falls outside defined use conditions.

[21] D3.2 Distributed Privacy-preserving Data Management and Storage Final Version will be published on https://tango-project.eu/materials/public-deliverables, once available.

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

The design of the **Self-Encryption with Multi-Factor Information Recovery** component presumes a high-stakes environment in which any data being encrypted is considered potentially personal or sensitive. This conservative stance obviates some classification risk, yet the absence of explicit categorisation or logging of data types leaves gaps in traceability and later accountability. Incorporating a pre-processing classification step would allow this system to encrypt securely and provide transparency about what is encrypted and why.

3.1.1.2 Data obfuscation

Encrypting data is not merely a technical task; it is an ethical commitment to render information inaccessible to those who do not have the right to access it. The **Blockchain-Based Data Storage and Sharing** module utilises symmetric encryption and hashing within DRILL to obscure data from unauthorised viewers. The release of decryption keys is controlled by DnAMS, contingent upon verifiable user consent. This setup provides a strong privacy shield, yet it remains relatively traditional. Additional obfuscation techniques – such as differential privacy, dynamic pseudonymisation, or tokenisation – could serve to enhance protection, especially in scenarios where aggregated or inferred data might otherwise expose individual identities.

In the **Confidentiality and Privacy by Design** module, a more sophisticated landscape unfolds. CP-ABE ties access privileges to complex combinations of user attributes, while digital signatures and zero-knowledge proofs enable the sharing of proof without disclosure. Furthermore, the integration of VC and DIDs allows entities to affirm their identity and authorisation without revealing excess information. However, a central vulnerability remains: the current reliance on a centralised key authority. This singular locus of trust risks undermining the decentralisation TANGO aims to champion. Moving toward federated or blockchain-based key distribution would fix this vulnerability and restore architectural integrity.

By contrast, the **Self-Encryption with Multi-Factor Information Recovery** module offers a minimalist yet robust approach. Employing AES-256 and SHA-256 cryptographic standards, it ensures that both content and structure are rendered indecipherable. The simplicity of its design, however, also highlights its limitations – most notably the absence of layered obfuscation for metadata and contextual elements. These seemingly minor details can, in aggregate, reveal as much about a user as the content itself. A more holistic obfuscation strategy, encompassing metadata anonymisation and entropy-aware hashing, would ensure end-to-end confidentiality.

3.1.1.3 Data minimisation

At the heart of data protection lies the principle of necessity. Data minimisation demands that only the information strictly required for a given purpose be collected, stored and processed. Within the **Blockchain-Based Data Storage and Sharing** module, this principle comes into conflict with the immutable and redundant nature of blockchain technology. While only consented data is stored in plain text and hashes are used to limit exposure, the distributed structure complicates timely and uniform data deletion. Without a centralised deletion mechanism or expiration control on data chunks, there is a tangible risk of over-retention. The recommended remedy is twofold: implement automated data deletion protocols on DRILL nodes and ensure that only cryptographic references, rather than raw data, are ever recorded on-chain.

The **Confidentiality and Privacy by Design** module offers more granular control. CP-ABE and XAMCL allow data to be filtered and shared based on contextual rules and user roles. Moreover, zero-knowledge proofs provide an elegant solution to data minimisation, enabling validation without disclosure. To further enhance alignment, these modules should incorporate automated data lifecycle management – ensuring data is not just limited in access but also time-bound in retention.

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

In the **Self-Encryption with Multi-Factor Information Recovery** module, the use of data chunking inherently limits the scope of exposure. Only fragments of a file are distributed and none retain contextual coherence in isolation. Yet this system overlooks the metadata that accompanies these chunks. File names, timestamps, or access logs can form a mosaic of personal insight if left unprotected. Encrypting or stripping this metadata, or applying pseudonymisation, would complete the minimisation loop.

3.1.1.4 Data abstraction

In line with the minimisation principle, data abstraction seeks to limit the granularity at which data is handled – especially where exactness is unnecessary for functionality. The **Blockchain-Based Data Storage and Sharing** module observes this principle by storing only essential logging data and avoiding comprehensive personal records on-chain. However, as regulatory expectations shift toward demonstrable compliance, abstraction tools – such as summarisation engines or aggregation-based queries – should be introduced to reconcile auditability with privacy.

The **Confidentiality and Privacy by Design** module, by virtue of CP-ABE's attribute filtering and XAMCL's contextual enforcement, inherently encourage abstraction. Still, these controls could benefit from the introduction of higher-order tools for pre-processing aggregation, such as statistical binning or category-based summarisation. These would ensure that even when data is accessed or transferred, it retains a level of abstraction that protects user identity.

In the **Self-Encryption with Multi-Factor Information Recovery** module, abstraction is achieved at the binary level. Files are split into unintelligible fragments before storage. However, when data is decrypted and reconstituted, the outputs – be they logs, summaries, or derived reports – may reintroduce personal detail. Incorporating controlled summarisation in post-processing steps would reinforce privacy even at the output stage.

3.1.1.5 Data separation

Segregating data logically and physically helps contain breaches and enforces access controls. In the context of the **Blockchain-Based Data Storage and Sharing** module, logical separation through DRILL's chunking mechanism and separate encryption key management by DnAMS are implemented. However, this separation depends heavily on DnAMS configuration. A single misstep could inadvertently centralise access or permit recombination of datasets. To prevent this, automated configuration validation and fail-safe access rules should be integrated into node deployment procedures.

The **Confidentiality and Privacy by Design** module enforces separation via policy-based encryption and modular architecture (e.g., FIWARE). Logical boundaries are clearly defined, but physical separation – such as using geographically dispersed or sandboxed environments – is not consistently applied. Including this layer would mitigate cross-environment vulnerabilities and increase system resilience.

The **Self-Encryption with Multi-Factor Information Recovery** module stands out for its comprehensive separation model. By using secret-sharing schemes, it not only divides data but ties its recovery to a quorum of participant approvals. The primary risk here is operational: if too few users are available (k_min not met), recovery becomes impossible. Making this threshold dynamically adjustable based on risk profiles or access tiers would balance resilience with usability.

3.1.1.6 Security of processing

The security of processing policy requires appropriate measures to ensure confidentiality. Security is the lifeblood of privacy. The **Blockchain-Based Data Storage and Sharing** module exhibits strong cryptographic safeguards and structural redundancy but falls short in operational response. Without a formal incident response framework that includes breach

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

detection, notification and recovery workflows, the system remains vulnerable to compliance failures under Articles 32 and 33 of the GDPR.

At the same time, the **Confidentiality and Privacy by Design** module excels in its cryptographic discipline but lacks broader cybersecurity infrastructure. Integrating intrusion detection, firewalls and behavioural analytics would address the growing landscape of external threats.

The **Self-Encryption with Multi-Factor Information Recovery** module is technically robust but operationally minimal. Its design lacks mechanisms for breach logging or user alerting. An integrated monitoring and incident response plan would transform it from a secure system to a resilient one.

3.1.1.7 Record-keeping and demonstrability

The **Blockchain-Based Data Storage and Sharing** module offers immutable audit logs that provide robust evidence of actions taken. However, if these logs are too abstract or inaccessible, they may fail to demonstrate actual compliance. Developing GDPR-aligned reporting tools that extract meaningful, anonymised insights from the logs would make them practically useful.

Confidentiality components use verifiable credentials and event logs to trace consent and policy enforcement. Still, questions remain regarding how long these logs are retained, how they are secured and how they evolve over time. Establishing life cycle management and audit trails with defined retention policies would improve demonstrability.

In the context of the **Self-Encryption with Multi-Factor Information Recovery** module, a record of encryption parameters and chunking activity in separate audit files is maintained. However, it does not yet track the complete data lifecycle – including access, transformation, or deletion. Enhancing the logging framework to include these steps, along with time-stamped records and integrity checks, would elevate it from a secure tool to a fully accountable one.

3.1.2 Policy Enforcement

In a distributed data space environment like TANGO, where data is published, shared and accessed across multiple administrative domains, robust and scalable policy enforcement is critical to maintain trust, ensuring data protection and enforcing compliance. To achieve this, TANGO adopts a modular, standards-based architecture that integrates Attribute-Based Access Control (ABAC) principles, enabling fine-grained, context-aware authorisation decisions for every data access or manipulation request. At the heart of this architecture are the PEP and PDP, supported by the PAP and the PIP. Together, these components ensure that access decisions are dynamically evaluated based on pre-defined policies and up-to-date contextual information.

When a user or client initiates an access request – typically accompanied by a VC-based access token issued by the SSI Verifier – the PEP intercepts the request and delegates the decision-making to the PDP. The PDP retrieves applicable policy rules from the PAP and gathers relevant attributes, such as trust and behavioural scores, from the PIP. If all policy requirements are met, the PDP issues a time-limited capability token, which the PEP uses to authorise subsequent interactions with the protected APIs.

Policy enforcement is implemented within the Provider Connector, which is deployed as a self-contained Kubernetes-based module at the data provider's infrastructure. Each component of the Provider Connector, including the PEP/PDP subsystem, runs as an independent containerised service, enabling isolated management and scalable deployment. All data services within the connector – exposed via standardised RESTful APIs – are protected by the PEP, which ensures that only authorised, policy-compliant clients are granted access.

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

The TANGO platform enforces a standardised API specification (/api/access-with-token) to ensure interoperability across different pilot implementations. This abstraction layer allows diverse infrastructures to integrate seamlessly with the PEP/PDP subsystem without requiring bespoke connectors or adapters. By aligning with the XACML reference model and leveraging JWT tokens enriched with verifiable identity and attribute claims, the policy enforcement mechanism achieves both interoperability and semantic precision.

Unlike conventional access control systems, TANGO's enforcement logic also considers external trust metrics and behavioural data, retrieved in real-time by the PIP, allowing dynamic and risk-sensitive access decisions. This adaptive enforcement is crucial in environments where data sovereignty, regulatory compliance (e.g., GDPR) cross-organisational trust are essential. Furthermore, the issuance of capability tokens ensures not only secure session management but also provides auditable trails of authorisation decisions, supporting accountability and transparency across the data space.

By building upon and extending components of the FIWARE Data Space Connector and replacing key modules such as the PEP and PDP with its own implementations, TANGO ensures that policy enforcement remains aligned with its architectural vision while supporting modularity, scalability trust-aware decision-making in a distributed infrastructure.

3.2 Measures for Secure Data Transfer within TANGO

The TANGO platform manages to ensure secure data exchange through a combination of encryption, secure communication protocols, access control, identity management and privacy measures, as described in detail in the previous publication. The platform also adopts privacy-focused protocols in line with the GDPR and conducts regular security audits with the purpose of safeguarding the confidentiality, integrity and compliance of personal and non-personal data, contributing to the platform's overall security and reliability.

This section focuses on the security measures implemented within the TANGO platform to safeguard the secure exchange of both personal and non-personal data.

Key components of the platform's security include:

1. **Data Encryption**: The TANGO platform uses advanced encryption standards, including Advanced Encryption Standard (AES) with 256-bit keys to protect sensitive data during transmission and storage. A self-encryption tool has also been developed to ensure data confidentiality and traceability, allowing users to recover data using a unique key linked to its source.
2. **Secure Communication Protocols**: Protocols such as HTTPS, SFTP, FTPS and standardised protocols such as Message Queuing Telemetry Transport (MQTT) and Open Data Protocol (OData) have been implemented to ensure secure real-time data transmission while preventing unauthorised access and cyber threats.
3. **Access Controls**: A tokenisation solution has been developed, which incorporates privacy by design to establish strict access controls. Access control protocols rely on continuous behavioural authentication of users and devices, ensuring that only authorised parties can access sensitive data.
4. **Identity and Access Management (IAM)**: IAM solutions were implemented to TANGO project, aiming to manage digital identities and user permissions to ensure only authorised access to data.
5. **Data Loss Prevention (DLP)**: Measures are in use to detect, monitor and prevent unauthorised data transfers.

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

6. **Privacy-related Protocols**: The TANGO platform complies with privacy-related legislation, including the GDPR and the ePrivacy Directive. A standardised level of security is applied to both personal and business-sensitive data.
7. **Regular Security Audits**: Periodic security audits identify and address vulnerabilities, ensuring the ongoing security and reliability of the TANGO platform.
8. **Compliance with Data Protection Regulations**: The partners involved ensure that the TANGO platform complies with relevant data protection regulations, including GDPR and CCPA.

The aforementioned measures aim to guarantee the security and integrity of data exchanged – transferred within the TANGO platform in compliance with data protection related legislation and regulations.

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

4 Conclusions

This white paper draws several conclusions regarding TANGO. The most important are:

The TANGO framework offers a comprehensive and forward-looking solution for secure and trustworthy data sharing, addressing key challenges such as data sovereignty, privacy and compliance in decentralised environments. By integrating blockchain-based storage with components like Fides' DRILL and DnAMS, TANGO enables tamper-proof, consent-driven and legally compliant data exchange.

Advanced trust mechanisms – including the Trustworthiness Scoring Module, Privacy Risk Score and the UPCV technology – support policy-driven, risk-aware data sharing. The platform builds on open standards such as FIWARE, CP-ABE encryption and XACML-based access control to ensure scalable, privacy-preserving interoperability aligned with GDPR and ISO 31700-1. Features like self-encryption and multi-factor recovery further enhance resilience against unauthorised access and key compromise.

TANGO also redefines Identity and Access Management by incorporating Self-Sovereign Identity, seamless onboarding and continuous behavioural authentication for users and devices. This decentralised trust model aligns with European goals for interoperability and data sovereignty. The combination of cryptographic techniques, dynamic risk assessment and behaviour-based authentication ensures continuous identity verification without compromising user experience.

Security is reinforced through countermeasures against hardware-level threats such as side-channel attacks and through privacy-by-design methodologies embedded in AI components. Tools like the Privacy Enhancing Component and Privacy Assurance Tool enable proactive threat modelling, compliance monitoring and secure data governance.

Overall, TANGO offers a modular, interoperable and standards-aligned architecture for building trustworthy data ecosystems – empowering individuals and organisations to maintain control over their data while enabling responsible, cross-sector collaboration.

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