



D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version

Document Identification			
Status	Final	Due Date	31/12/2024
Version	1.0	Submission Date	21/01/2025

Related WP	WP2	Document Reference	D2.4
Related Deliverable(s)	D2.1, D2.2, D2.3	Dissemination Level (*)	PU
Lead Participant	UTH	Lead Authors	Apostolos Apostolaras UTH Ilias Syrigos UTH
Contributors	UTH, INTRA, UPRC, ATOS, DBC, FHG, NOR, VTT, FSDE, FUJ_LU, UMU, UOM, DUT, UoG, CEA, SQD, XLAB, QBE, LSTECH, EXUS, KUL, DBC.	Reviewers	Evi Kopanaki UPRC, Elena Avatangelou UPRC Dolores Ordóñez, ANYS

Keywords:

Use case scenarios, system requirements, functional & non-functional requirements, security requirements, technical specifications, platform architecture, social & legal assessment, Architecture, Data Usage Control, Data Sovereignty, Dataspaces.

This document is issued within the frame and for the purpose of the TANGO project. This project has received funding from the European Union's Horizon Europe Framework Programme under Grant Agreement No. 101070052. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

The dissemination of this document reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission.

This document and its content are the property of the TANGO Consortium. The content of all or parts of this document can be used and distributed provided that the TANGO project and the document are properly referenced.

Each TANGO Partner may use this document in conformity with the TANGO Consortium Grant Agreement provisions.

Document Information

List of Contributors	
Name	Partner
Apostolos Apostolaras	UTH
Ilias Syrigos	UTH
Stergios Lantzios	UTH
Nicolas Belleville	CEA
Tomás Pariente Lobo	ATOS
Iván Martínez Rodríguez	ATOS
Sergio Salmerón Majadas	ATOS
Kaitai Liang	DUT
Dazhuang Liu	DUT
Mehdi Akbari Gurabi	FHG
Felix Hermsen	FHG
John Zaras	SQD
Salshyam Panda	UoG
Manos Panaousis	UoG
Athanasios Stratikopoulos	UOM
Erik Hieta-aho	VTT
Nejc Bat	XLAB
Urban Kos	XLAB
Anja Božič	XLAB
Evangelia Kopanaki	UPRC
Elena Avatangelou	UPRC
Ioannis Katsanakis	UPRC
Asterios Stoumpoulis	UPRC
Maria Hernandez Padilla	UMU
Antonio Skarmeta	UMU
William Greenall	QBE
Niklas Palaghias	QBE
Anaxagoras Fotopoulos	EXUS
Christina Nichiforov	EXUS
Alexandra Papageorgiou	KUL
Ioannis Drivas	DBC
Vitalii Demianets	NOR
Eleni Veroni	INTRA
Panos Matzakos	INTRA
Jürgen Neises	FSDE
Claudia Mertinger	FSDE
Sven Rasmussen	FUJ_LU

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	2 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

List of Contributors	
Ibrahim Mecirdi	FUJ_LU
Sofiane Lagraa	FUJ_LU
Moussa Ouedraogo	FUJ_LU

Document History			
Version	Date	Change editors	Changes
0.01	11/11/2024	UTH	Initial ToC
0.1	02/12/2024	UTH	Integration of first input received
0.2	13/12/2024	UTH	Second iteration: Integration of input received
0.3	23/12/2024	UTH	Third iteration: Integration of input received
0.4	07/01/2025	UTH	Fourth iteration: Integration of input received
0.5	10/01/2025	UTH	Fifth iteration: Integration of input received
0.6	13/01/2025	UTH	Sixth iteration: Integration of input received
0.7	15/01/2025	UTH	Seventh iteration: Integration of input received
0.8	16/01/2025	UTH	Eighth iteration: Integration of input received
0.9	19/01/2025	UTH, ANYS, UPRC	Ninth iteration: Internal Review Received
1.0	20/01/2025	UTH	Final version ready for submission

Quality Control		
Role	Who	Approval Date
Deliverable leader	Apostolos Apostolaras (UTH)	20/01/2025
Quality manager	Jürgen Neises (FSDE)	21/01/2025
Project Coordinator	Tomás Pariente Lobo (ATOS)	21/01/2025

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	3 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

Table of Contents

Document Information	2
Table of Contents	4
List of Tables.....	9
List of Figures	10
List of Acronyms.....	11
Executive Summary	13
1 Introduction	14
1.1 Purpose of the document.....	14
1.2 Relation to other project work.....	14
1.3 Structure of the document	15
2 Concept & Methodology	16
2.1 Methodological Framework.....	16
2.1.1 Project Methodology	16
2.1.2 Refinements to User and System Requirements.....	18
2.1.3 Refinements to TANGO Architecture.....	19
3 Final User Requirements	21
3.1 Pilot 1: Smart Hospitality.....	21
3.1.1 Brief overview of the Pilot study.....	21
3.1.2 Updates and Advancements	21
3.2 Pilot 2: Autonomous Vehicles	23
3.2.1 Brief overview of the Pilot study.....	23
3.2.2 Updates and Advancements	23
3.3 Pilot 3: Smart Manufacturing – Case 1 (3D-printing).....	25
3.3.1 Brief overview of the Pilot study.....	25
3.3.2 Updates and Advancements	25
3.4 Pilot 3: Smart Manufacturing – Case 2 (RIAS)	27
3.4.1 Brief overview of the Pilot study.....	27
3.4.2 Updates and Advancements	27
3.5 Pilot 4: Banking	29
3.5.1 Brief overview of the Pilot study.....	29
3.5.2 Updates and Advancements	29
3.6 Pilot 5: Public Organizations	30
3.6.1 Brief overview of the Pilot study.....	30
3.6.2 Updates and Advancements	30

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	4 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

3.7 Pilot 6: Retailers.....	31
3.7.1 Brief overview of the Pilot study.....	31
3.7.2 Updates and Advancements	32
3.8 Overview of pilot cases / technology mapping	33
4 Final System Requirements and Specifications.....	35
4.1 Blockchain-based Data Storage and Sharing [T3.1]	35
4.1.1 Component Overview.....	35
4.1.2 Final Functional & Non-functional Requirements	35
4.2 Trustworthy Data Sharing [T3.2]	35
4.2.1 Component Overview.....	35
4.2.2 Functional & Non-functional Requirements	37
4.3 Confidentiality and Privacy by Design [T3.3]	37
4.3.1 Component Overview.....	37
4.3.2 Functional & Non-functional Requirements	37
4.4 Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms [T3.4]	38
4.4.1 Component Overview.....	38
4.4.2 Functional & Non-functional Requirements	38
4.5 Self-sovereign Identity Management [T4.1]	38
4.5.1 Component Overview.....	38
4.5.2 Functional & Non-functional Requirements	39
4.6 Seamless Onboarding for Users and Devices [T4.2]	39
4.6.1 Component Overview.....	39
4.6.2 Functional & Non-functional Requirements	40
4.7 User continuous behavioural authentication [T4.3]	40
4.7.1 Component Overview.....	40
4.7.2 Functional & Non-functional Requirements	40
4.8 Device continuous behavioural authentication [T4.4]	40
4.8.1 Component Overview.....	40
4.8.2 Functional & Non-functional Requirements	42
4.9 Hardening Against Side-channel Attacks [T4.5]	42
4.9.1 Component Overview.....	42
4.9.2 Functional & Non-functional Requirements	42
4.10 Exploratory Data Analysis Engine [T5.1].....	42
4.10.1 Component Overview.....	42
4.10.2 Functional & Non-functional Requirements	42
4.11 Energy efficient AI model training [T5.2]	43

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	5 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

4.11.1	Component Overview.....	43
4.11.2	Functional & Non-functional Requirements	44
4.12	Dynamic Intelligent Execution on Heterogeneous Systems [T5.3]	44
4.12.1	Component Overview.....	44
4.12.2	Functional & Non-functional Requirements	44
4.13	Privacy Threat Modelling & Identification for Trustworthy AI [T5.4]	45
4.13.1	Component Overview.....	45
4.13.2	Functional & Non-functional Requirements	45
4.14	X-AI For Privacy and Trust Enhancement [T5.5]	45
4.14.1	Component Overview.....	45
4.14.2	Functional & Non-functional Requirements	46
4.15	Infrastructure Management based on AI [T5.6].....	46
4.15.1	Component Overview.....	46
4.15.2	Functional & Non-functional Requirements	46
4.16	User Interfaces [T6.3]	47
4.16.1	Component Overview.....	47
4.16.2	Functional & Non-functional Requirements	47
4.17	Visualisation Techniques [T6.4]	47
4.17.1	Component Overview.....	47
4.17.2	Functional & Non-functional Requirements	48
4.18	TANGO Integrated Platform [T6.1-2]	48
4.18.1	Deployment View.....	48
4.18.2	Non-functional Requirements	49
5	TANGO Reference Architecture	50
5.1	Introduction	50
5.1.1	Architecture Overview	50
5.1.2	Alignment with dataspace initiatives	51
5.1.3	Enabling Pilots with the TANGO Architecture.....	52
5.2	TANGO Ecosystem Overview.....	52
5.3	TANGO Connector	53
5.3.1	Authentication Portal.....	53
5.3.2	SSI Verifier.....	53
5.3.3	Access and Usage Control.....	54
5.3.4	DB / Data Service API	55
5.3.5	Scoring Modules.....	55
5.3.6	Encryption Modules	55
5.3.7	Configuration Manager	56

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	6 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
		Status:	Final		

5.3.8	Logging Service	56
5.3.9	Implementation of Connector at the Provider's side	57
5.3.10	TANGO Connector on the Consumer side.....	59
5.4	Blueprint.....	61
5.5	TANGO Management Connector	63
5.5.1	Deployment Orchestrator	65
5.5.2	Blueprint Repository	65
5.5.3	TANGO App Store.....	66
5.5.4	Verifiable Data Registry.....	66
5.5.5	CP-ABE Key Authority and Self-Encryption Key Storage.....	66
5.5.6	TANGO Centralized Services	67
5.6	Practical Sequence	67
6	Privacy, Ethical, Social and Legal Impact Assessment.....	70
6.1	Legal assessment of the TANGO technology	70
6.1.1	Self-Sovereign Identity (SSI) Management [T4.1]	70
6.1.2	Seamless Onboarding for Users and Devices (SOUND) [T4.2]	77
6.1.3	User Continuous Behavioural Authentication (UCBA) [T4.3]	83
6.2	Ethical assessment of the TANGO technology.....	86
6.2.1	Human participation	87
6.2.2	AI ethical requirements	89
6.3	Social assessment of the TANGO technology	92
7	Conclusions	94
8	Bibliography.....	95
Annexes		100
A.	Updated User Requirements Overview	100
A.1	Pilot 1: Smart Hospitality.....	100
A.2	Pilot 2: Autonomous Vehicles.....	102
A.3	Pilot 3: Smart Manufacturing – Case 1	105
A.4	Pilot 3: Smart Manufacturing – Case 2	107
A.5	Pilot 4: Banking.....	110
A.6	Pilot 5: Public Organizations.....	112
A.7	Pilot 6: Retailers.....	114
B.	System Requirements for Distributed Privacy-preserving Data Management and Storage.....	116
B.1	Functional Requirements.....	116
B.2	Non-Functional Requirements.....	118
C.	System Requirements for Distributed Trust Management Framework.....	119
C.1	Functional Requirements.....	119

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	7 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

C.2 Non-Functional Requirements.....	121
D. System Requirements for AI-based Framework for Green & Trustworthy Operations	123
D.1 Functional Requirements.....	123
D.2 Non-Functional Requirements	126
E. System Requirements for Visualisation Techniques & User Interfaces.....	128
E.1 Functional Requirements	128
E.2 Non-Functional Requirements.....	130
F. System Requirements for the TANGO Integrated Platform.....	131
F.1 Non-Functional Requirements	131
G. Privacy, Ethics, Legal, and Societal Requirements	133

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	8 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

List of Tables

Table 1: Defined Categories of Non-Functional Requirements.	19
Table 2: Blockchain-based Data Storage and Sharing Component Functional Requirements (Author: NOR)	116
Table 3: Trustworthy Data Sharing Component Functional Requirements (Author: FHG, FUJ_DE, VTT)	116
Table 4: Confidentiality and Privacy by design Component Functional Requirements (Author: UMU)	117
Table 5: Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms Functional Requirements (Author: DUT)	117
Table 6: Blockchain-based Data Storage and Sharing Component Non-Functional Requirements (Author: NOR)	118
Table 7: Trustworthy Data Sharing Component Non-Functional Requirements (Author: FHG, FUJ_DE, VTT)	118
Table 8: Confidentiality and Privacy by Design Non-Functional Requirements (Author: UMU)	118
Table 9: Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms Non-Functional Requirements (Author: DUT)	119
Table 10: Self-sovereign identity management Functional Requirements (Author: VTT, UMU, ATOS)	119
Table 11: Seamless Onboarding for Users and Devices Functional Requirements (Author: QBE)	120
Table 12: User continuous behavioural authentication Functional Requirements (Author: QBE)	120
Table 13: Device continuous behavioural authentication Functional Requirements (Author: UTH)	121
Table 14: Hardening Against Side-channel Attacks Functional Requirements (Author: CEA)	121
Table 15 Self-sovereign identity management Non-Functional Requirements (Author: VTT, UMU, ATOS)	121
Table 16: Seamless Onboarding for Users and Devices Non-Functional Requirements (Author: QBE)	122
Table 17 User continuous behavioural authentication Non-Functional Requirements (Author: QBE)	122
Table 18: Device continuous behavioural authentication Non-Functional Requirements (Author: UTH)	122
Table 19: Hardening Against Side-channel Attacks Non-Functional Requirements (Author: CEA)	123
Table 20: EDAE Component Functional Requirements (Author: EXUS)	123
Table 21: Federated Learning Component Functional Requirements (Author: ATOS)	124
Table 22: MLOps Component Functional Requirements (Author: ATOS)	124
Table 23: AutoML Component Functional Requirements (Author: ATOS)	124
Table 24: TornadoVM Component Functional Requirements (Author: UOM)	125
Table 25: Privacy Enhancing Component Functional Requirements (Author: UOG)	125
Table 26: Privacy Assurance Tool Functional Requirements (Author: FUJ_LU)	125
Table 27: XAI Component Functional Requirements (Author: SQD)	125
Table 28: RENOPS Component Functional Requirements (Author: XLAB)	126
Table 29: EDAE Component Non-Functional Requirements (Author: EXUS)	126
Table 30: Federated Learning Component Non-Functional Requirements (Author: ATOS)	126
Table 31: MLOps Component Non-Functional Requirements (Author: ATOS)	127
Table 32: AutoML Component Non-Functional Requirements (Author: ATOS)	127
Table 33: TornadoVM Non-Functional Requirements (Author: UOM)	127
Table 34: Privacy Enhancing Component Non-Functional Requirements (Author: UOG)	127
Table 35: Privacy Assurance Tool Non-Functional Requirements (Author: UOG)	127
Table 36: XAI Component Non-Functional Requirements (Author: SQD)	127
Table 37: RENOPS Component Non-Functional Requirements (Author: XLAB)	128
Table 38: User Interfaces Functional Requirements (Author: LST)	128
Table 39: Visualization and Reporting Techniques Component Functional Requirements (Author: SQD)	129
Table 40: User Interfaces Non-Functional Requirements (Author: LST)	130
Table 41: Visualization and Reporting Techniques Component Non-Functional Requirements (Author: SQD)	130
Table 42: TANGO Integrated platform Non-Functional Requirements (Author: INTRA, NOR)	131

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	9 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

List of Figures

Figure 1: TANGO Methodology roadmap. _____	16
Figure 2: Trustworthiness Scoring. _____	36
Figure 3: TANGO Ecosystem. _____	51
Figure 4: TANGO Connector on the Provider's side. _____	54
Figure 5: FIWARE Data Space Connector high-level overview. _____	58
Figure 6: TANGO Connector on the Consumer's side. _____	60
Figure 7: YAML configuration file of a Kubernetes Deployment. _____	61
Figure 8: ConfigMap option _____	61
Figure 9: Passing environment variables to containers. _____	62
Figure 10: Sample configuration file using the "ImagePullSecrets" option. _____	63
Figure 11: TANGO Management Connector. _____	64
Figure 12. SSI and eIDAS compatibility (Schwalm & Allamilo-Domingo, 2021) _____	78

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	10 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

List of Acronyms

Abbreviation / acronym	Description
ABE	Attribute-Based Encryption
AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
AutoML	Automated Machine Learning
CAV	Connected and Automated Vehicle
CI/CD	Continuous Integration/ Continuous Delivery and/or Deployment
CP-ABE	Cypher text Policy – Attribute Based Encryption
CSV	Comma-Separated Values
CUDA	Programming model and a platform for parallel computing
DCBA	Device-Continuous Behavioural Authentication
DID	Decentralized Identifier
DL	Deep Learning
DnAMS	Decentralized norbloc Access Management System
DNS	Domain Name Server
DoS	Denial of Service
DRILL	Data Redundancy In Legal Limitations - norbloc's decentralized legally compliant data backend
eID	Electronic Identification
eIDAS	Electronic Identification, Authentication and trust Services
EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
EC	European Commission
eMRTD	electronic Machine-Readable Travel Document
ESSIF	European Self Sovereign Identity framework
FL	Federated Learning
FPGA	Field Programmable Gate Arrays (integrated circuits)
FR	Functional Requirement
GAIA-X	Initiative created to allow for the secure, open, and transparent use of data
GDPR	General Data Protection Regulation
GPGPU	General-Purpose Graphics Processing Unit
GPU	Graphics Processing Unit
HTTP	Hypertext Transfer Protocol
HIPAA	Health Insurance Portability and Accountability Act
ICAO	International Civil Aviation Organization
IDSA	International Data Spaces Association
IIC	Industrial Internet Consortium
IMEI	International Mobile Equipment Identity

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	11 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Abbreviation / acronym	Description
IoT	Internet of Things
IR	Intermediate Representation
JSON	JavaScript Object Notation
JWT	JSON Web Tokens
KA	Key Authority
KPI	Key Performance Indicator
KYB	Know Your Business
KYC	Know Your Customer
MAC	Media Access Control
ML	Machine Learning
MLOps	Machine Learning Operations
NIST	National Institute of Standards and Technology (US)
NFC	Near Field Communication
NFR	Non-Functional Requirement
OIDC	OpenID Connect
OKVS	norbloc's Oblivious Key-Value Storage
P2P	Peer-to-Peer
PET	Privacy-Enhancing Technologies
PAT	Privacy-Assurance-Tool
RF	Radio Frequency
SDK	Software Development Kit
SIOP	Self-Issued OpenID Provider
SSI	Self-Sovereign Identity
SSID	Service Set Identifier
UAM	User Access Management
UBEM	User Behavior Exchange Module
UCBA	User Continuous Behavioural Authentication
UI	User Interface
UPCV	Ubiquitous Personal Context Vector
UX	User Experience
VC	Verifiable Credential
VDR	Verifiable Data Registry
VP	Verifiable Presentation
VRN	Volatile Random Numbers
WLAN	Wireless Local Area Network
W3C	World Wide Web Consortium
XAI	Explainable Artificial Intelligence
ZK	Zero-Knowledge
ZKP	Zero-Knowledge Proof
ZTP	Zero Touch Provisioning

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	12 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Executive Summary

This document is the final deliverable of WP2 and its aim is to integrate and expand upon the findings of prior TANGO activities held under the context of WP2 providing the relative updates and presenting a comprehensive overview of the project's achievements and their implications for the work conducted in the other technical WPs. It consolidates the updates on the user requirements, the system requirements considering technical components, and pilot use case mappings outlined in earlier phases, while incorporating new advancements and lessons learned from their implementation.

In TANGO, the need for a transparent, secure, fair, and sustainable framework for managing distributed data, which is critical for modern digital ecosystems is addressed initially by WP2. Therefore, this deliverable aims to provide a holistic understanding of how TANGO bridges identified gaps in existing processes and technologies. Readers will gain insight into the iterative process of defining user requirements, aligning technical offerings, and validating the framework across diverse use cases, including Smart Hospitality, Autonomous Vehicles, Smart Manufacturing, Banking, Public Organizations, and Retail.

- **User Requirements and KPIs:** Building on D2.2, this deliverable consolidates and refines user requirements and KPIs across six pilot use cases. Each pilot is presented with detailed user stories, personas, and journeys, offering a clear view of current challenges and future scenarios enabled by the TANGO solution.
- **Technological Advancements:** Expanding on the initial technology offerings (WP3-WP6), this deliverable details the refined TANGO Reference Architecture. Following DSBA recommendations that aim to converge FIWARE, IDSA and GAIA-X principles, the architecture is structured into three conceptual layers (trust, management, and user) and distributed across multiple environments. Key updates include:
 - The TANGO Connector: Serving as the ecosystem's primary entry point, facilitating secure and seamless integration.
 - Configuration Blueprints: Enabling efficient deployment, construction, and management of Connectors.
 - Mapping Technical Offerings to Use Cases:
 - Aligning technical components with pilot requirements through iterative discussions and analyses, the deliverable highlights how TANGO's solutions address specific security, privacy, and operational needs of each pilot. This mapping leverages insights from D2.1 and dedicated stakeholder engagements.
- **System-Level Requirements:** Functional and non-functional requirements (FRs and NFRs) are presented, with prioritizations and mappings to relevant technologies and user needs. These requirements guide the ongoing development and validation of the TANGO framework.
- **Ethical, Legal, and Privacy Compliance:** Preliminary assessments underscore TANGO's adherence to GDPR and other legal frameworks, with continuous monitoring ensuring alignment with ethical standards. Technical and operational measures implemented to protect fundamental rights are outlined, with a roadmap for future impact assessments.

This deliverable provides a unified framework for understanding the progress, challenges, and solutions within the TANGO project. By integrating findings from previous deliverables and incorporating iterative feedback, it lays a robust foundation for the implementation and validation of the TANGO solution in pilot use cases. Key takeaways include the critical importance of user-centric design, the flexibility of the TANGO architecture, and the project's alignment with ethical, legal, and societal standards. These insights will drive the advancements within the remaining time of the project and ensure the long-term impact of the TANGO framework.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	13 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

1 Introduction

1.1 Purpose of the document

This document serves as the final consolidated deliverable for the WP2 of the TANGO project, incorporating updates and refinements on insights, methodologies, and findings with respect to the work conducted so far and the previous deliverables. It provides a comprehensive reference for understanding the TANGO framework's development, aligning user requirements, technical specifications, and system architecture with project objectives and pilot use cases.

The key objective of this document is to provide the updates on the following tasks:

1. **T2.2 User Needs and Requirements for Data Management, Processing & Storage and T2.3 Use Case Scenarios & KPIs Definition:** This document includes a report that highlights the refinements and updates of the final scenarios and the technology mappings. It acts as a final iteration and provides final adjustments and improvements to ensure completeness and alignment with the overall description of the initial document deliverable D2.2
2. **T2.4 Definition of System Requirements & Technical Specifications:** An overview of all the technology offerings involved in TANGO (WP3-WP6) is provided, covering the following aspects:
 - Description of their envisioned functionality, internal architecture, and interoperability with other components.
 - Description of their association with specific pilots of TANGO, based on the corresponding pilot specifications provided by *T2.3: Use Case Scenarios & KPIs Definition*, through [1].
 - Description of the identified security threats per component, accompanied by mitigation measures that each technology offering will provide.
 - A list of functional and non-functional requirements (FRs and NFRs, respectively) that each technology offering is expected to cover at system level. These requirements are strongly related to the User Requirements per defined TANGO pilot which are provided by *T2.2: User Needs and Requirements for Data Management, Processing & Storage*, through [1].
3. **T2.5 Security-and-Privacy-by-design Architecture & API Specifications:** The first consolidated version of the TANGO architecture is provided. This architecture is aligned with the principles and reference architecture of IDSA and GAIA-X associations, adopting some of their main concepts and building blocks. In this framework, the envisioned role and placement of the technology offerings (WP3-WP6) in the TANGO reference architecture according to their technical specifications (output of T2.4) has been largely identified and described.
4. **T2.6 Privacy, Ethical, Social and Legal Impact Assessment:** The results of the preliminary comprehensive impact assessment, known as Privacy Impact Assessment Plus (PIA+), covering privacy, ethical, social, and legal issues related to the TANGO framework are provided. As a first step, a data mapping process has been implemented, where partners have been asked to report on their activities, personal data processing actions, data storage, security measures, and possible ethical considerations that may be raised related to data subjects' rights.

The document is designed to be a comprehensive resource for project stakeholders, including technical teams, pilot partners, and evaluators. By synthesizing prior work and incorporating updated findings, it establishes a clear roadmap for deploying and validating the TANGO solution in real-world scenarios, ensuring that the project's outcomes align with its overarching goals of transparency, security, fairness, and sustainability.

1.2 Relation to other project work

This deliverable D2.4 provides updated findings from technical components and pilots. It serves as a key output of WP2 ensuring the final version reflects the project's evolving scope and the lessons learned

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	14 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

during its implementation phases. Deliverable D2.4 is closely related to previous WP2 deliverables as it has received information from the deliverables *D2.1- SOTA and GAP analysis*, *D2.2-User Needs and Requirements and Use Case Scenarios* and *D2.3 - System Requirements & Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment* as well as with the subsequent deliverables in the other technical WPs (WP4-WP6) and the WP7 for pilot demonstration and validation. Its aim is to provide the latest updates and refinements up to date with respect to the previous WP2 deliverables and contribute with critical advancements that guide subsequent tasks and work packages aiming at consistent alignment of the technical development with the project goals.

1.3 Structure of the document

This document is structured in seven major sections, as presented below:

Section 2 provides an overview of the TANGO concept and how it is associated with the TANGO key technological areas, as well as the methodological framework adopted in the project.

Section 3 presents a brief overview of each of the seven pilot studies and the related updates and advancements on the user needs and requirements.

Section 4 presents the updates and the refinements for the functional and non-functional requirements of the TANGO technical offerings which are linked with the following technology domains as listed below:

- Distributed Privacy-preserving Data Management and Storage.
- Distributed Trust Management Framework.
- AI-based Framework for Green and Trustworthy Operations.
- Data visualization techniques and User Interfaces.

Section 5 delivers the final version of the TANGO reference architecture.

Section 6 documents the final outcomes of the TANGO impact assessment, covering privacy, ethical, social and legal issues.

Section 7 concludes the document.

Additionally, the interested reader is referred to Annexes A-F that provide the related tables describing the requirements either user-centric or technical ones which have been modified, re-considered or added as new entries.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	15 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

2 Concept & Methodology

2.1 Methodological Framework

2.1.1 Project Methodology

As described in the DoA, the project methodology has been based upon the identification of the operational challenges that stakeholders face in the context of data operations in data spaces, across the data life cycle. The TANGO methodology follows a 4-step approach, where each of these is associated with a project Work Package (WP) that includes the tasks planned to address the project objectives as presented in Figure 1. The *Baseline* (M06) step has been triggered in WP2 by the in-depth investigation of the current state-of-the-art for all prominent technologies leveraged in TANGO (D2.1, M06), followed by the elicitation of the user needs & requirements and the definition of the use case scenarios (D2.2, M09). Deliverable D2.3 (M12) concluded this set of essential deliverables produced as part of the *Baseline* step, reporting on the system requirements and technical specifications of all technical offerings, delivering TANGO's reference architecture designed in line with the IDSA/GAIA-X standards to ensure compatibility, interoperability, and finally, identifying relevant ethical, legal, social and privacy related themes, data flows, and possible associated risks.

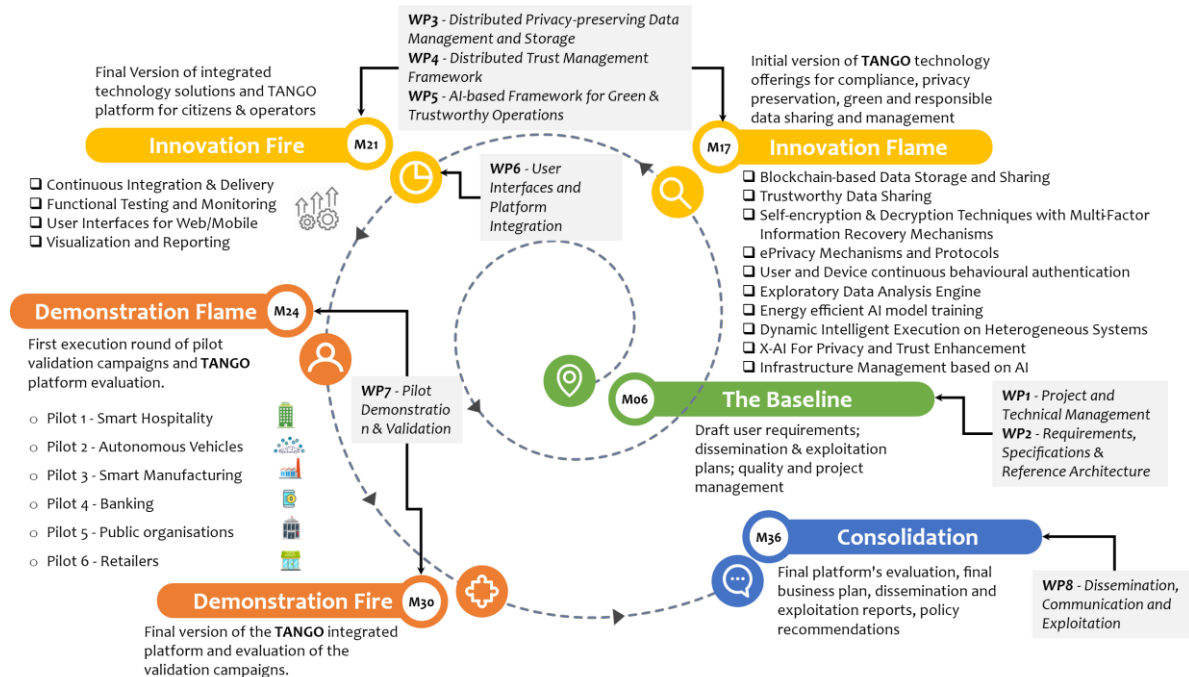


Figure 1: TANGO Methodology roadmap.

During the *Innovation Flame* (M17) phase, we leveraged the insights extracted from the previously mentioned deliverables as a foundation for the technical Work Packages (WPs) to integrate their individual technologies within an agile, decentralized, and highly scalable architectural framework. This framework has been designed to facilitate the seamless coordination of various services operating within the broader TANGO ecosystem. The elicited system requirements have served as a roadmap for enhancing the capabilities of the different components, aligning them with the precise technical specifications set for the platform, which have been reported in D2.3 (M12). This process essentially involved expanding the functionalities of each component to ensure they align seamlessly with the platform's defined technical requirements and objectives. Moreover, the privacy, ethical, and legal

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version	Page:	16 of 139
Reference:	D2.4	Dissemination:	PU
	Version:	1.0	Status: Final

principles, defined in the same deliverable, have served as a compass for the technical partners to seek and incorporate appropriate technical or operational measures with special attention given to privacy, social impact, security, and lawful basis. This phase concluded with the submission of the deliverables D3.1, D4.1, D5.1 (M17), which contain detailed descriptions on the intermediate versions of all TANGO technology offerings that have been developed within the technical work packages WP3, WP4, and WP5, respectively.

The next phase, named *Innovation Fire (M21)*, was a pivotal stage in which initial prototypes and technical components underwent iterative development with a strong emphasis on interconnectivity, while staying aligned with the project's goals for performance and privacy. This phase saw significant progress in WP3, WP4, and WP5, which focused on enhancing the platform's core functionalities, including privacy-preserving data management, trust management, and AI-driven operations. Concurrently, efforts within WP6 laid the groundwork for seamless integration in subsequent phases, ensuring that all technical innovations were primed for pilot demonstrations and real-world applications. By M21, the project achieved a key milestone with the delivery of D6.1, which outlined the integration plan. This comprehensive document detailed the critical specifications for integration, encompassing the availability and utilization of CI/CD services, endpoint definitions, and a thorough testing plan, thereby ensuring the robustness and reliability of the TANGO platform.

The *Demonstration Flame (M24)* phase represented a significant transition, moving from conceptual integration to the realization of the initial building blocks of the TANGO platform. These components were extended with a view toward their validation within the framework of the pilots. This phase, primarily driven by WP6 and WP7, concentrated on mapping the platform's core capabilities with the defined use-case scenarios. Due to the high complexity of the project, this phase strategically prioritized the integration of smaller elements of the platform to ensure the critical features were ready for preliminary stakeholder interaction in forthcoming phases. By M24, the project had planned possible small-scale pilot tests in controlled environments, that would enable various stakeholders to engage with and evaluate the specific functionalities. These early interactions were designed not only to validate the technical robustness and usability of the integrated components but also to address key operational needs identified earlier in the project. WP7, which is responsible for collecting and assessing stakeholder feedback, outlined a clear process for gathering insights during these interactions and defining the next steps. This feedback will play a crucial role in refining the platform and preparing it for the more extensive testing and deployment in the final phases.

Currently in the *Demonstration Fire (M30)* phase, TANGO is undergoing an intensive period of integration, during which its building blocks are being refined to meet the interconnection requirements of various services and components. This critical phase ensures that all modules are adapted and extended to function cohesively within a fully integrated environment, paving the way for the upcoming pilot validations. As part of concluding the WP2 efforts, the project successfully delivers the current deliverable D2.4, which contains the final version of the system requirements and specifications, platform architecture, and the privacy, ethical, social, and legal impact assessment. This crucial report provides comprehensive updates before the final phase on all the aforementioned aspects, ensuring the platform's adherence to both end-user and technical requirements, as well as to regulatory standards. Furthermore, key activities taking place within WP3, WP4, and WP5, focus on fine-tuning the technology offerings in response to various feedback, resolving performance bottleneck, and ensuring alignment with technical specifications and end-user requirements. The outcomes of said activities will be reported in D3.2, D4.2, and D5.2 (M30), which will document the final versions of the technology offerings developed within their respective work packages, marking a significant milestone in the project's implementation. During this period, particular emphasis is also being placed on fostering collaboration between technical teams and stakeholders through a focused synergy between WP6 and WP7. This coordinated effort aims to tackle the challenges emerged as we progress towards the

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	17 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

finalization of the pilot deployment plans, carefully considering the unique needs of each pilot in terms of resources, including infrastructure and expertise.

In the final implementation step, the *Consolidation (M36)* phase, TANGO will focus on finalizing the integration of the platform and ensuring its readiness for deployment at pilot premises. In this phase, the integration efforts will be concluded with the delivery of D6.2 (M31), ensuring all components are seamlessly interconnected and fully functional before deployment at the pilot premises. Comprehensive functional and end-to-end testing will be conducted to validate the system's performance according to the use-case scenarios, ensuring the platform operates efficiently and reliably. Following the successful testing, the platform's components and services will be either directly deployed at designated pilot sites or at the central TANGO cloud infrastructure that will be securely connected to the pilot sites, according to the TANGO reference architecture (section 5) and deployment view (section 4.18.1). In this context the platform will be actively used and evaluated by the various stakeholders (D7.1, M35). A key component of this phase will be the collection of detailed feedback from the stakeholders. This feedback will provide valuable insights into the platform's usability, technical performance, and overall effectiveness, enabling the project team to make any final adjustments before concluding the project. This last phase will ensure that TANGO is fully validated, aligned with the stakeholder expectations and achieving the intended TRL (D7.2, M36).

2.1.2 Refinements to User and System Requirements

2.1.2.1 User Requirements (Section 3)

The TANGO user requirements were presented in detail in D2.2 (v1 and v2). The document presented the user requirements, the use case scenarios and the related KPIs for each one of the TANGO pilot use cases, namely Smart Hospitality, Autonomous Vehicles, Smart Manufacturing, Banking, Public Organizations and Retail.

Since the delivery of D2.2, the pilot use case scenarios and the respective user requirements have been further analysed and refined, in close collaboration with the technical partners of the project. A high-level description of the current version of the pilot case scenarios is available in Section 3 of this document. The updated list of user requirements is available in the Annex.

The final version of pilot case scenarios that will be used for the TANGO platform evaluation and validation at pilot sites will be described in full detail in D7.2.

2.1.2.2 System Requirements (Section 4)

Section 4 provides an analytic overview of the TANGO components' system requirements and specifications. More specifically, sections 4.1 - 4.18 present an overview of the implementation updates for each TANGO component, as well as an updated status on their corresponding functional and non-functional requirements which were defined in D2.3. To this end, summary tables of each component's functional and non-functional requirements are presented in Annexes B - F. System Requirements for the TANGO Integrated Platform. In these tables a "Status" column has been added to describe the implementation state of the different Functional and Non-Functional requirements according to the following list:

- **In progress:** To indicate that the implementation of the corresponding system requirement is ongoing.
- **Done:** To indicate that the implementation of the corresponding system requirement is completed and verified.
- **Postponed:** To indicate that the implementation of the system requirement is postponed for later within the project's implementation timeline, due to its dependency to other ongoing developments.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	18 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

- **Dropped:** To indicate that the implementation of the system requirement is not considered anymore.
- **Newly identified:** To indicate that the implementation of a new system requirement, not initially foreseen in D2.3, has been added.

Table 1: Defined Categories of Non-Functional Requirements.

Code	Category	Description
NFR_COMP	Compatibility	Qualities that describe the degree to which the software can exchange information with other systems. Includes the concepts of co-existence and interoperability
NFR_MAIN	Maintainability	Qualities that describe the ability of the software to be changed, enhanced and supported over time with a fair degree of effortlessness. Includes the concepts of modularity , reusability , modifiability etc.
NFR_PER	Performance	Qualities that describe the relationship between the level of performance of the software and the number of resources used, under stated conditions. Includes the concepts of capacity , resource utilization , and scalability .
NFR_PORT	Portability	Qualities that describe the ability of the software to be transferred from one environment to another. Includes the concepts of adaptability , replaceability etc.
NFR_REL	Reliability	Qualities that describe the capability of the software to maintain its level of performance under stated conditions for a stated time period. Includes the concepts of availability , recoverability , fault tolerance etc.
NFR_SEC	Security	Qualities that describe the protection of the software against attacks. Includes the concepts of confidentiality , integrity , authenticity , accountability etc.
NFR_UI	Usability	Qualities that describe the effort needed by the users to use the software. Includes the concepts of accessibility , user error protection , UX , UI aesthetics etc.
NFR_EXIST	HW and SW Constraints	Hardware and software constraints due to integration of existing assets.
NFR_SUST	Sustainability	Qualities that describe the capability of a software solution to be energy efficient , mitigating its ecological footprint .

2.1.3 Refinements to TANGO Architecture

The updated TANGO Reference Architecture further aligns with DSBA recommendations by adopting the FIWARE Data Space Connector as its foundational implementation, ensuring interoperability and compliance with the technical convergence principles set by GAIA-X, IDSA, and BDVA. The FIWARE Connector serves as a modular and extensible platform that supports decentralized data storage, enabling Providers to maintain control over their data until it is shared with trusted Consumers. This distinction between Providers and Consumers is a central aspect of the architecture, ensuring that data usage remains subject to the Provider's defined policies while enabling Consumers to access and process data securely through authorized channels. By integrating Self-Sovereign Identity (SSI) for decentralized authentication and XACML-based access control for fine-grained data governance, the architecture

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	19 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

provides a cohesive framework for trusted, secure, and policy-driven interactions between Providers and Consumers.

The placement of technical components within the architecture reflects its modular and layered design, ensuring scalability and flexibility across deployment scenarios. Core functionalities are distributed into three layers: the Trust Layer, the Management Layer, and the User Layer. The Trust Layer includes components such as the SSI Verifier for identity validation, CP-ABE encryption modules for policy-driven data protection, and Usage Control for enforcing XACML-based access policies. The Management Layer incorporates the Deployment Orchestrator and Configuration Manager for dynamic service orchestration, while the User Layer hosts technology offerings like MLOps, Federated Learning, and Privacy Enhancing Components for end-user interactions. These containerized microservices are instantiated within TANGO Connectors, which act as secure entry points for both Providers and Consumers, although there is a clear distinction on what components and how are deployed on each side. The architecture ensures that these individual components can operate independently, while seamlessly interacting to enable trustworthy and decentralized data exchanges across the ecosystem.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	20 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

3 Final User Requirements

3.1 Pilot 1: Smart Hospitality

3.1.1 Brief overview of the Pilot study

In the Smart Hospitality pilot, focus is on providing personalised services to hotel guests, while preserving their privacy. Guests' identity data during check-in will be securely handled by the TANGO platform with GDPR compliance without the fear of exposing identity information to staff or other stakeholders. Personalised configuration will be loaded at the guests' room without the danger of exposing personal data. During the pilot validation, users will be using the system to receive personalized recommendations about activities and services that may be of interest to them. At check-out, guests will provide feedback regarding the user satisfaction and their overall experience and will receive a report related to their carbon footprint during their stay.

Hotel managers have access to reports based on the guests' preferences, evaluation and energy consumption to make informed decision for improving the overall hotel experience.

3.1.2 Updates and Advancements

The updated scenarios for the Smart Hospitality pilot case are the following:

Persona: Tourist / Hotel customer

Scenario Step	Description	Components involved
Tourist onboarding	<p>Before travelling, the tourist acquires a digital identity (ePassPort) on their mobile phone.</p> <p>The tourist uses the digital identity to become onboarded to TANGO, to be able to use the TANGO services related to the scenario.</p>	<p>SOUD (ePassport)</p> <p>SSI Agent/Wallet</p> <p>UI for onboarding and getting access to various services.</p> <p>Policy configuration for user authorization (based on user role)</p>
Tourist checks-in at the hotel using digital wallet identity	The tourist checks-in at the hotel through a dedicated application on a tablet. For this purpose, the tourist digital identity stored on the tourist's mobile phone is used.	<p>UI –</p> <p>Dedicated mobile application</p> <p>PAT</p> <p>PEP/PDP</p>

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	21 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
Tourist receives suggestions for activities and services.	While on location, the tourist has access to activity recommendations on an application on their mobile phones. The tourist has access to the application through the TANGO platform.	UPCV UI for getting access to various services. PAT
Hotel room settings are monitored and set according to tourist preferences.	While staying at the hotel, the NADIA platform gathers data from sensors installed in the room. The data refers to: room temperature, light usage, AC usage, etc.	NADIA platform
Upon check-out the tourist evaluates the overall experience.	At check-out, the tourist evaluates the overall experience on a dedicated application provided by the hotel.	Hotel mobile app for service evaluation.
Upon check-out the tourist receives a report on energy and resources	After check-out the tourist receives a report about the energy and resources used during their stay.	UI for getting access to various services. EDAE for data analysis

Persona: Hotel manager

Scenario Step	Description	Components involved
Managers and hotel employees onboarding	The manager acquires a digital identity (ePassport) on their mobile phone. The manager uses the digital identity to become onboarded to TANGO, to be able to use the TANGO services related to the scenario.	SOUD (ePassport) SSI Agent/Wallet UI for onboarding and getting access to various services. Policy configuration for user authorization (based on user role)

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	22 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
Managers access reports on energy and resources consumption and on tourist satisfaction.	<p>The manager has access to reports based on customer data that is collected by various existing hotel platforms (e.g. NADIA, user experience evaluation platform, etc.).</p> <p>Managers' access varies depending on their level (local, regional, group manager).</p>	<p>PEP/PDP</p> <p>CP-ABE</p> <p>EDAE</p> <p>VIS</p>

3.2 Pilot 2: Autonomous Vehicles

3.2.1 Brief overview of the Pilot study

In the Autonomous Vehicles pilot case TANGO provides IDIADA with data protection and privacy, trusted user authentication, in two distinct cases:

- During the autonomous vehicle ride, to protect the communication and data flow (communication user-server, car-server).
- In B2B cases, where TANGO provides a solution for protecting IDIADA's virtual maps, when these are shared with customers.

3.2.2 Updates and Advancements

The updated scenarios for the Autonomous Vehicles pilot case are the following:

Persona: Car passenger

Scenario Step	Description	Components involved
Passenger onboarding	<p>The passenger acquires a digital identity (ePassport) on their mobile phone.</p> <p>The passenger uses the digital identity to become onboarded to TANGO, to be able to use the TANGO services related to the scenario.</p> <p>The vehicle device is onboarded to TANGO.</p>	<p>SOUD (ePassport)</p> <p>SSI Agent/Wallet</p> <p>UI for onboarding and getting access to various services.</p> <p>Policy configuration for user authorization (based on user role)</p>
Passenger arrives at IDIADA and registers for the car ride	The passenger is authenticated by TANGO to perform a test ride.	<p>SOUD (ePassport)</p> <p>SSI Agent/Wallet</p>

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	23 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
Passenger uses the smartphone app to call the car to his/her location and control the car's destination.	The app is provided by IDIADA over a secure network.	TSM PEP-PDP
Car application accesses the maps to reach desired location.	The car application is authenticated and authorized to access the IDIADA maps to perform the requested ride.	TSM PEP-PDP
Car communicates with server and with passenger application during the ride.	TANGO ensures secure communication.	TSM PEP-PDP

Persona: IDIADA Client (B2B)

Scenario Step	Description	Components involved
Client onboarding	<p>The client acquires a digital identity (ePassport) on their mobile phone.</p> <p>The client uses the digital identity to become onboarded to TANGO, to be able to use TANGO services related to the scenario.</p>	SOUD (ePassport) SSI Agent/Wallet UI for onboarding and getting access to various services. Policy configuration for user authorization (based on user role)
IDIADA employee sets the access rights and time period for the specific client.	Through the TANGO UI.	UI for getting access to various services. SSI

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	24 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
		PEP-PDP
The client asks IDIADA to access their maps.	The client submits a request either through traditional means (e.g. email) or through the TANGO UI.	UI for getting access to various services. SSI PEP-PDP
The client gets access to the maps.	The client accesses the appropriate files.	UI for getting access to various services. SSI CP-ABE
The access period expires. The client is no longer able to use the maps.	TANGO restricts access to the files when the permitted period is over.	SSI CP-ABE

3.3 Pilot 3: Smart Manufacturing – Case 1 (3D-printing)

3.3.1 Brief overview of the Pilot study

In the 3D printing pilot case, FMAKE will evaluate TANGO in additive manufacturing and in particular in the context of Digital Twins. FMAKE has an additive manufacturing infrastructure which allows research and piloting of cybersecurity solutions. Given the strict confidentiality requirements in aerospace, medical etc. the TANGO framework will provide high security in terms of elements such as data management/sharing/storage as well as authentication, access rights, IoT devices and 3D printers.

3.3.2 Updates and Advancements

The updated scenarios for the Smart Manufacturing (3D printing) pilot case are the following:

Persona: Customers and Employees

Scenario Step	Description	Components involved
Customer / Employee onboarding	<p>The customer acquires a digital identity (ePassport) on their mobile phone.</p> <p>The customer uses the digital identity to become onboarded to TANGO, to be able to use TANGO services related to the scenario.</p>	<p>SOUND (ePassport)</p> <p>SSI Agent/Wallet</p> <p>UI for onboarding and getting access to various services.</p>

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	25 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
		Policy configuration for user authorization (based on user role)
Customer creates 3D printing design locally	This occurs at the customer's premises using existing platforms and tools (not related to TANGO).	---
Customer uploads design to FMAKE for printing	Through TANGO, FMAKE allows the customer to access a secure location online for uploading the printing job files.	CP-ABE SEDSS UI for onboarding and getting access to various services.
The design file is accessed by FMAKE personnel with various roles and access levels to be prepared for printing	TANGO controls access to the files as long as the printing job request is active.	CP-ABE UI for onboarding and getting access to various services.
Access to the design file changes upon completion of each printing phase	TANGO controls access to the files as long as the printing job request is active.	CP-ABE

Persona: Data Scientist

Scenario Step	Description	Components involved
Employee (data scientist) onboarding	<p>The employee (data scientist) acquires a digital identity (ePassport) on their mobile phone.</p> <p>The employee uses the digital identity to become onboarded to TANGO, to be able to use TANGO services related to the scenario.</p>	SOUD (ePassport) SSI Agent/Wallet UI for onboarding and getting access to various services.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	26 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
		Policy configuration for user authorization (based on user role)
The data scientist investigates the existing data in the summary print job report, to check if the quality issue was predicted by the model.	This activity is performed through existing tools and platforms.	---
The data scientist updates the model by retraining it.	The data scientist prepares and combines data from different customers at various locations (edge, cloud, and potentially at customer). XAI supports the data scientist in the model training.	MLOps, FLEviden RenOps XAI
The retrained model is downloaded from the TANGO platform to the printer.	This activity is performed through existing tools and platforms.	---

3.4 Pilot 3: Smart Manufacturing – Case 2 (RIAS)

3.4.1 Brief overview of the Pilot study

In the manufacturing scenario, RIAS will use TANGO to monitor and enforce access restrictions related to shopfloor workers in a secure and transparent way. An additional scenario for RIAS, with lower implementation priority, is the monitoring of remote vendors accessing RIAS online systems for maintenance purposes. The scenario faces certain challenges due to the current processes followed by the system maintenance collaborating organizations. The technology providers of TANGO components involved in this case are researching how these challenges could be mitigated to provide a proof-of-concept for the specific scenario.

3.4.2 Updates and Advancements

The updated scenarios for the Smart Manufacturing (Factory) pilot case are the following:

Persona: Factory worker / Manager

Scenario Step	Description	Components involved
Worker onboarding	The factory worker acquires a digital identity (ePassport) on their mobile phone. The factory workers use the digital identity to become onboarded to TANGO,	SOUD (ePassport) SSI Agent/Wallet

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	27 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
	to be able to use TANGO services related to the scenario.	UI for onboarding and getting access to various services. Policy configuration for user authorization (based on user role)
Worker enters the factory premises – activates location monitoring via smart device.	The worker registers with their smart phone and then uses the smart watch to be located when in the factory premises. Upon entrance to the factory the user scans the QR code with the phone, and then the smart watch location begins being monitored.	SSI Agent/Wallet
Worker is at their designated work area. The worker's location on the shopfloor is monitored to prevent unauthorized access to certain areas.	TANGO is monitoring the worker's location.	DCBA
Worker moves to unauthorized area. The system notifies the supervisor.	The worker's location triggers an alert. The supervisor/manager receives a push notification on their mobile device. The incident is registered in the factory incidents list.	DCBA UI
The supervisor and the manager have access to all access violations reports.	The manager receives a report with incidents at the end of the week.	PEP-PDP VIS

Persona: Vendor (SW maintenance / provider)

Scenario Step	Description	Components involved
Vendor onboarding	The vendor acquires a digital identity (ePassport) on their mobile phone. The vendor uses the digital identity to become onboarded to TANGO, to be able to use TANGO services related to the scenario.	SOUND (ePassport) SSI Agent/Wallet UI for onboarding and getting access to various services.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	28 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
		Policy configuration for user authorization (based on user role)
Vendor is granted access to factory systems for maintenance purposes.	TANGO authenticates and authorizes the vendor to access the RIAS systems.	SSI Agent/Wallet PEP-PDP
Continuous authentication and access monitoring.	TANGO monitors the vendor and verifies that the user that is logged in is indeed the authenticated one. The system records the actions of the vendor for future reference and reporting.	UCBA
In case of unauthorized access attempt, the system notifies the supervisor.	The supervisor/manager receives a push notification on their mobile device. The incident is registered in the factory incidents list.	UCBA UI
The supervisor and the manager have access to all access violations reports.	The manager receives a report with incidents at the end of the week.	PEP-PDP VIS

3.5 Pilot 4: Banking

3.5.1 Brief overview of the Pilot study

The Banking pilot aims at experimenting with Federated Learning for Anti-Fraud detection in a multi-bank scenario, to leverage the collective intelligence of multiple institutions while maintaining data privacy and security. This collaborative approach may represent an outstanding opportunity to enhance fraud detection capabilities and provide more accurate and robust fraud prevention systems for the banking sector.

3.5.2 Updates and Advancements

The updated scenario for the Banking pilot case are the following:

Persona: Anti-fraud Operator

Scenario Step	Description	Components involved
Anti-fraud operator accesses the Federated Learning platform	Anti-fraud operator accesses the Federated Learning platform	MLOps FLEVIDEN AUTOML

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	29 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
Anti-fraud operator performs data analysis	Analyses the results provided by the model trained with the contribution of all participants	MLOps FLEVIDEN AUTOML XAI
Anti-fraud operator uses results	Based on the results obtained from the federated learning system, adapt the anti-fraud systems to promptly intercept fraudulent transactions	Bank anti-fraud systems

3.6 Pilot 5: Public Organizations

3.6.1 Brief overview of the Pilot study

In Public Organizations pilot case TANGO framework will be used for managing the high-risk process for visa applications. Through the pilot VISAR will be exchanging personal data with visa applicants and relevant public administrations through TANGO, ensuring privacy, transparency, and security of data gathered and processed by citizens.

3.6.2 Updates and Advancements

The updated scenarios for the Public Organizations pilot case are the following:

Persona: VISA Case Manager, Employer and Public Authority Employees

Scenario Step	Description	Components involved
Employer and Authority employees onboarding	VISAR acquires a professional user account on Fides. Employee, Employer and Authority employees acquire Fides user accounts.	Fides
Employer initiates visa application	Employer fills out the initial visa application with the applicant's details, completes their own profile, and submits it to VISAR.	Fides
Relocation Employee fills-in information	Relocation Employee verifies email and ID and completes individual details (marital status, degree).	Fides
VISAR Employee receives relocation case assignment	VR Employee gets the relocation case assigned. Monitors and verifies the Relocation Employee profile (indicated by checkmarks that signify the data has been confirmed by VISAR personnel). Prepares and submits completed Relocation Employee application.	Fides

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	30 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Scenario Step	Description	Components involved
	Relocation Employee gets notified that application was submitted by VISAR.	
Authority Employee works on the case	<p>Authority Employee (Federal Employment Agency, Immigration Office) receives notification about new application.</p> <p>Reviews available documents (checkmarks from VISAR employees confirm data verification, while Employer checkmarks indicate data entered by the Employer).</p> <p>Approves or rejects the application by selecting the relevant decision status and uploading the supporting document. If necessary, sends a request for additional documentation.</p>	Fides
VISAR Employee finalizes the case	<p>VISAR Employee sends final status confirmation to the Relocation Employee and to Employer and closes the relocation case in Fides.</p> <p>Informs Relocation Employee on the entry procedure to Germany.</p>	Fides

Persona: VISAR IT Personnel

Scenario Step	Description	Components involved
Employee onboarding	<p>The employee acquires a digital identity (ePassport) on their mobile phone.</p> <p>The employee uses the digital identity to become onboarded to TANGO, to be able to use TANGO services related to the scenario.</p>	<p>SOUND (ePassport)</p> <p>SSI Agent/Wallet UI for onboarding and getting access to various services.</p>
Privacy Risk Assessment	The IT personnel checks the privacy risks and potential impact of data sharing on the VISAR platform.	PEC

3.7 Pilot 6: Retailers

3.7.1 Brief overview of the Pilot study

The Retailers pilot focuses on the analysis of purchasing data in a cross-border scenario, across two different retail entities in Greece and Cyprus acting as competitors, both owned by METRO group.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	31 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Historical anonymized data (collected during the past two years) will be used for the training of the AI algorithms representing shopping preferences of consumers/wholesalers. Emphasis will be placed on the efficiency of the data exchange mechanisms in the retail sector under strict legal and ethical conditions. Federated learning mechanisms combined with tokenization will be deployed targeting insightful and personalised recommendations in a privacy preserving way for both consumers and wholesalers.

3.7.2 Updates and Advancements

The updated scenarios for the Retailers pilot case are the following:

Persona: IT Manager

Scenario Step	Description	Components involved
Employee onboarding (IT Manager)	The employee acquires a digital identity (ePassport) on their mobile phone. The employee uses the digital identity to become onboarded to TANGO, to be able to use TANGO services related to the scenario.	SOUND (ePassport) SSI Agent/Wallet UI for onboarding and getting access to various services.
IT Manager prepares data	IT Manager checks data availability in both Athens and Cyprus. Prepares / extracts data to be used by TANGO. Places data in the predefined location and removes existing files.	TANGO is not involved in this step.
IT Manager initiates data analysis	The IT Manager logs into TANGO and notifies the EDAE that there are available data for analysis.	SSI, SOUND PDP-PEP UI for getting access to various services. EDAE
IT Manager is notified when data processing is completed	Notification appears on the IT Managers dashboard.	UI for getting access to various services.

Persona: Managers (Marketing, Sales, Product, various levels)

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	32 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Scenario Step	Description	Components involved
Employee onboarding	<p>The employee acquires a digital identity (ePassport) on their mobile phone.</p> <p>The employee uses the digital identity to become onboarded to TANGO, to be able to use TANGO services related to the scenario.</p>	<p>SOUD (ePassport)</p> <p>SSI Agent/Wallet</p> <p>UI for onboarding and getting access to various services.</p>
Manager requests data analysis	Manager logs in to TANGO and selects data search parameters.	<p>SSI, SOUD</p> <p>PDP-PEP</p> <p>VIS</p> <p>UI for getting access to various services.</p>
Manager receives results	Manager views data analysis results and visualizations.	VIS

3.8 Overview of pilot cases / technology mapping

Component	Hospitality	Vehicles	Man. FMAKE	Man. RIAS	Public Sector	Retail	Banking
FIDES (T3.1)					X		
TSM (T3.2)		X		X			
UPCV (T3.2)	X					X	
CP-ABE (T3.3)	X	X	X	X		X	
UCM (T3.3)	X	X	X	X		X	
PEP/PDP (T3.3)	X	X	X	X		X	
SEDSS (T3.4)			X				
SSI-Agent (T4.1)	X	X	X	X		X	
SSI-Wallet (T4.1)	X	X	X	X		X	
SOUD (T4.2)	X	X	X	X		X	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	33 of 139	
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Component	Hospitality	Vehicles	Man. FMAKE	Man. RIAS	Public Sector	Retail	Banking
UCBA (T4.3)				X		X	
DCBA (T4.4)				X			
SCA (T4.5)	X						
EDAE (T5.1)	X		X			X	
MLOps (T5.2)			X				X
FLEVIDEN (T5.2)			X				X
AUTOML (T5.2)			X				X
TornadoVM (T5.3)	X		X			X	
PEC (T5.4)					X		
PAT (T5.4)	X					X	
XAI (T5.5)			X				X
RENOPS (T5.6)			X				
UI (T6.3)	X	X	X	X		X	
VIS (T6.4)	X			X		X	

4 Final System Requirements and Specifications

4.1 Blockchain-based Data Storage and Sharing [T3.1]

4.1.1 Component Overview

The Fides platform offers decentralized storage of regulated data / attestations together with verification stamps and sharing stored data across interested parties.

The full solution is truly decentralized and offers legal compliance, great data redundancy, system resilience and enforced data verification upon entry with support for independent data verification entities.

The overall design follows the description of Fides as specified in the deliverable D2.3. Most of the functional and non-functional requirements are met due to the chosen design of Fides component. The key Fides functionalities that contribute to meeting the requirements are:

- ▶ Explicit consent management.
 - This functionality is delivered by DnAMS Fides internal component
- ▶ Private data sharing in regulated environments.
 - This functionality is delivered by overall Fides design
- ▶ Immutable audit logs
 - This functionality is delivered by blockchain Fides component. A set of metadata for every data access is immutable stored, ready for external/internal audit

For the implementation of Fides as a part of Tango project the “external API” approach was selected, mainly due to the proprietary nature of Fides. All aspects of Tango integration will be managed by a well-defined set of externally available API endpoints. The same concerns the integration with Tango CI/CD pipeline, as was specified in the deliverable D6.1.

4.1.2 Final Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex A. System Requirements for Distributed Privacy-preserving Data Management and Storage (DUT + WP3 partners), in Table 2 (functional) and Table 6 (non-functional). This list reflects the link of the FIDES module with the Public Administration pilot.

4.2 Trustworthy Data Sharing [T3.2]

4.2.1 Component Overview

The term “Trustworthy Data Sharing” may cover a widespread understanding of Trust. Within the TANGO project two facets of Trust are covered.

4.2.1.1 Trustworthiness as an enabler of access or usage control in combination with the TANGO PEP/PDP

Core of the Trustworthiness assessment for access or usage control is the Trustworthiness Scoring Module. It interacts with the Privacy Risk Analysis tool as an option of obtaining a privacy score and the PEP/PDP based on configuration and runtime data of the use cases.

Overall, the way the Trustworthiness Scoring works is illustrated in Figure 2: Trustworthiness Scoring.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	35 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

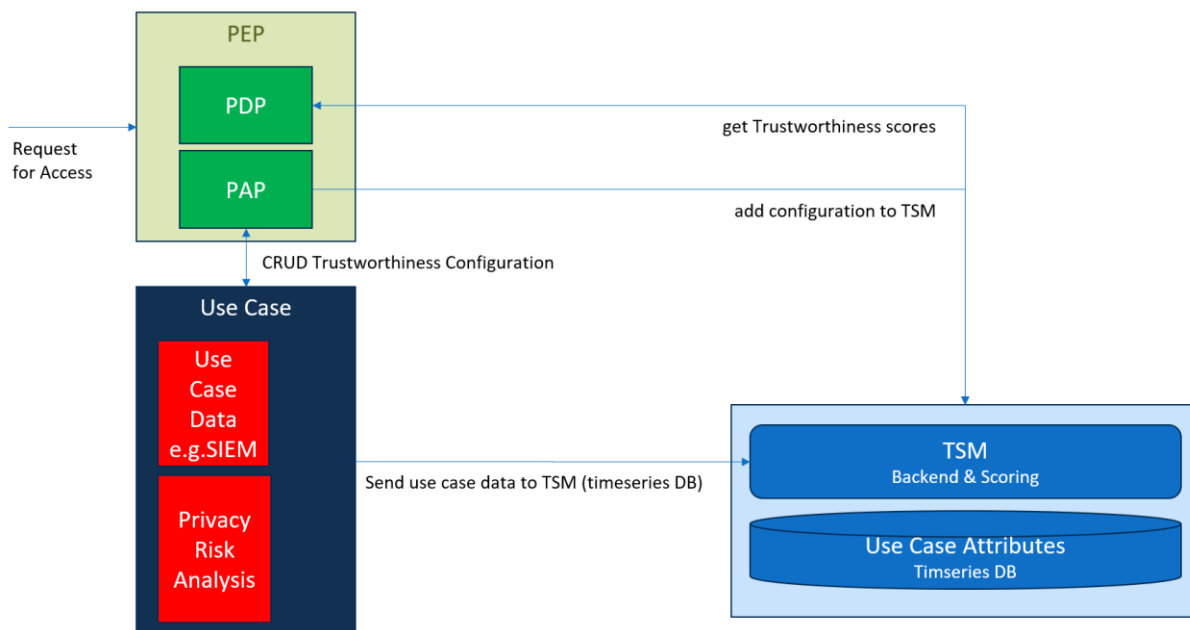


Figure 2: Trustworthiness Scoring.

The use case generates and handles a Trustworthiness configuration specifying attributes and weights for currently five characteristics (Security, Privacy, Reliability, Resilience and Safety) using the Policy Authoring Point (PAP) of the PEP. This configuration then is stored in the TSM module's backend.

The use case then sends data representing the attributes to the TSM, which stores them in a timeseries DB. This way future visualization and analysis of the Trustworthiness over time is possible.

One part of the data may be the score provided by the Privacy Risk Analysis module (TSM-PRAM).

This currently is designed to be deployed on user side. In summary, the TSM-PRAM operates on a time series and evaluates the degree to which it satisfies a predefined privacy policy. The computed scores for each time series element are then stored in the Timeseries database. Currently, the TSM-PRAM supports the autonomous driving use case. The approach focuses on a time series of pre-anonymized images and assesses the level of privacy protection achieved through the prior anonymization. Different privacy policies can be applied.

For example, a privacy requirement might be to check whether GDPR requirements are met. Another setting could assume a higher threat level, which would reduce the effectiveness of basic face anonymization, resulting in a lower privacy score given the same anonymization. When it comes to an access request, the PDP shall decide using the Trustworthiness score obtained through the PIP calling the TSM.

4.2.1.2 Privacy preserving UPCV technology for personalized recommendations, service personalization and advertising, based on user behaviour.

Recommenders, in general, aim at predicting user behaviour, therefore the technology can be assumed to apply for business intelligence as well, e.g., for defining user groups and item clusters. UPCV can be implemented into a decentralized or distributed architecture, enabling information sharing between different vendors without breaching users' privacy.

As described in D2.3, in TANGO T3.2 the UPCV technology has been extended to a distributed architecture. In this distributed architecture of the UPCVs, each user and each vendor have an instance of a User Behaviour Exchange Module (UBEM) as a mobile Web App, which implements a recommender that is technically a symmetric component - similar on user and vendor (service) side.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	36 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

UBEM aggregates user behaviour into Volatile Random Numbers (VRN) maintaining no association of personal action history. Each instance of UBEM must have a data repository into which VRNs are collected – typically a few kilobytes total per user and per item.

It should be noted that UBEM itself may act as the recommender; creating recommendations may take place on either side - or by a third party. In the T3.2 implementation, recommendations are created on user (mobile device) side.

The UPCV recommendation algorithm is using user actions as its input for learning, conceptually in a format of UserID/ItemID. In a distributed implementation, each user has its own instance of the UBEM storing their VRN collection and each vendor has an instance of UBEM storing one VRN collection per item.

VTT has created and demonstrated a mobile Web App based system for distributed end-user recommendations, mainly to be used in the Smart Hospitality use case as a tourist attraction recommender. For the Retail use case, the background UPCV recommendation engine has been modified for the providing business intelligence; applicability to be validated.

4.2.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex A. System Requirements for Distributed Privacy-preserving Data Management and Storage (DUT + WP3 partners), in Table 3 (functional) and Table 7 (non-functional). This list reflects the link of each of the modules with the use cases: **Privacy Risk Analysis** is linked to mainly the Autonomous Vehicles use cases, the **Trustworthiness Scoring Module** is linked to use cases Autonomous Vehicles and Smart Manufacturing, and the **UPCV** module is linked to the use cases Smart Hospitality and Retail.

4.3 Confidentiality and Privacy by Design [T3.3]

4.3.1 Component Overview

Confidentiality and Privacy by Design embed privacy considerations into system design, proactively addressing data privacy throughout its lifecycle rather than as a later compliance requirement. As described in D2.3., two mechanism are adopted by TANGO to approach this concept. On the one hand, user consent management is approached by the implementation of a Policy Enforcement architecture following XACML's attribute-based policies, and sticky policies, where data is encrypted using CP-ABE to enforce attribute-based policies, ensuring control and authentication. Together, these mechanisms enable fine-grained privacy control, compliance, and trust between users and data providers. Full final implementation details will be provided in D3.2.

4.3.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented Annex A. System Requirements for Distributed Privacy-preserving Data Management and Storage (DUT + WP3 partners), in Table 4 (functional) and Table 8 (non-functional). This list reflects the link of the modules with pilots: Smart Hospitality, Autonomous Vehicles, Smart Manufacturing (FMAKE, and RIASTONE) and Retail.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	37 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

4.4 Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms [T3.4]

4.4.1 Component Overview

The SEDSS module ensures data confidentiality by encrypting information into a secure format that can only be decrypted using the corresponding key or algorithm. This mechanism allows secure storage and transmission of sensitive data, protecting it from unauthorized access or tampering.

The primary object and scope of self-encryption and decryption techniques with multi-factor information recovery mechanisms component (SEDSS) remains consistent with the details provided in D3.1. In details, SEDSS is designed to be utilized by use cases and other technical components which requires data protection.

The main features implemented in SEDSS includes: (1) encrypt data with its own features; (2) keep track of users who decrypt the data; (3) distribute keys (for decryption) with arbitrary security level customized by users; (4) divide encrypted data in the form of data chunks to convenient data transmission. See more detailed description in D3.1.

4.4.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex A. System Requirements for Distributed Privacy-preserving Data Management and Storage (DUT + WP3 partners), in Table 5 (functional) and Table 9 (non-functional). This list reflects the link of the module, pilot 3 smart manufacturing (case for customers and employees).

4.5 Self-sovereign Identity Management [T4.1]

4.5.1 Component Overview

The Self-Sovereign Identity (SSI) landscape has changed and continues to spread and mature since the previous version of this deliverable D2.3. For one the GAIA-X specification continues to evolve as seen with this latest, but still incomplete Identity, Credential and Access Management specification[2], which is now based on OpenID SSI technology rather than Hyperledger Aries at the time of the previous deliverable D2.3. Additionally, with the publishing of the DSBA Technical Convergence recommendations [3] in mid-2023 to follow the SSI approach the project decided to integrate with the FIWARE Dataspace Connector [4] (FIWARE DSC) with its support for OpenID4VP [5] and alignment with EBSI Guidelines [6]. Considering the continually changing specifications for GAIA-X there is no specific integration support for GAIA-X in the project, however the TANGO SSI components are aligned with the same OpenID specifications and the JWT VC variant supported by GAIA-X.

The TANGO SSI Solution comprises of the same architecture previously described in D2.3 with an SSI Wallet and Agent. However, due to the timeline of the project two variations are supported an SSI Wallet / Agent supporting JWT VCs and another SSI Wallet / Agent supporting LDP VCs with ZKP.

The TANGO SSI will support the consumer side with SSI Issuer / Verifier and Wallet functionality and prove interoperability with the FIWARE DSC presenting Verifiable Credentials to its Data Provider side and follow its Trusted Issuer List approach.

Additionally, the FIWARE DSC VCVerifier [7] component has been modified to further support ZKP cryptography.

The SSI Solution developed in the project includes the following components:

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	38 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

4.5.1.1 SSI Agent (jwt_vc)

The SSI Agent implemented supports OpenID4VP & OpenID4VCI and the EBSI Conformance Guidelines for jwt_vc type credentials. It acts as an Issuer of Verifiable Credentials for ePassport, Employee and Customer Verifiable Credentials and a verifier of ePassport Verifiable Credentials.

4.5.1.2 SSI Wallet (jwt_vc) - VTT

Secure end user wallet that securely stores the user's Verifiable Credentials, provides a User Interface for the user to manage their credentials and provides the cryptographic operations when submitting & receiving Verifiable Credentials including handling of the Decentralized Identifiers.

4.5.1.3 SSI Agent (ldp_vc with ZKP) – UMU

A compliant issuer and verifier adhering to OpenID4VP & OpenID4VCI and EBSI Conformance Guidelines. It issues ldp_vc type Verifiable Credentials using Zero-Knowledge Proof cryptographic algorithms and verifies ZKP credentials to ensure they are correctly signed and comply with specified policies.

4.5.1.4 SSI Wallet (ldp_vc with ZKP) – UMU

A secure wallet designed to receive ZKP-based credentials and perform attribute derivations to conceal unnecessary information in accordance with defined policies.

4.5.1.5 FIWARE VCVerifier Modified for ZKP - UMU

A modified FIWARE verifier that delegates the verification of ZKP presentations to a specialized verifier capable of handling Zero-Knowledge Proof algorithms.

4.5.1.6 IoT Device M2M – UMU

An entity designed to handle the issuance, storage, and presentation of Verifiable Credentials within machine-to-machine (M2M) communications. It interacts with the SSI Agent and FIWARE Verifier to manage the credential lifecycle in IoT environments, ensuring secure and efficient credential handling.

4.5.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex C. System Requirements for Distributed Trust Management Framework, in Table 10 (functional) and Table 15 (non-functional). This list reflects the link of the module(s) with all of the pilots except the Banking and Public Organizations pilots.

4.6 Seamless Onboarding for Users and Devices [T4.2]

4.6.1 Component Overview

The component provides a system for onboarding users based on their ePassport and biometric data. In essence, the component performs remotely, identity verification of a person based on their existing physical identity document. Currently the technology supports the ePassport and explores the potential to support the national identity documents. The remote identity verification is performed based on the eIDAS regulation, and in particular due to the verification of the information based on the Near Field Chip (NFC), it is able to achieve High Level of Assurance. The person that is about to perform the identity verification process remotely, goes through a particular wizard. During this wizard the person is informed about the data that will be collected and the processing that will take place. The component follows the design from D2.3. The process involves providing biometric data such as a photo, and scan of the data from the RFID chip in the passport. Optical Character Recognition technology reads through the back camera of the smartphone the Machine-Readable Zone of the ePassport in order to derive the

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	39 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
		Status:	Final		

information visible on the ePassport. Facial image and identity information stored at the NFC chip are extracted and temporarily stored at the apps' memory. During the face recognition process, liveness detection is performed to detect any cases of impersonation and spoofing, while face matching compares the facial images between the person performing the onboarding and the facial image of the person of the identity document. The component currently has been tested and is proven operational on a wide range of European passports. It includes component that conducts liveness detection, to check that the image provided is of a live person so as to avoid e.g. fake profiles using photographs set up by malicious actors. We are currently looking to expand to national ID cards where appropriate, as many also include relevant RFID tags.

4.6.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex C. System Requirements for Distributed Trust Management Framework, in Table 11 (functional) and Table 16 (non-functional). This list reflects the link of the module with the Smart Hospitality pilot, Retail and Vehicle Passenger Pilot, as well as the Manufacturing pilot (RIASTONE).

4.7 User continuous behavioural authentication [T4.3]

4.7.1 Component Overview

This component utilises user behavioural biometric data in order to provide continuous behavioural authentication based on device usage characteristics. The component collects various behavioural data of the person interacting with a system, either on the mobile or on the computer, in order to derive behavioural patterns, towards the continuous and secure authentication of the user. The component collects behavioural data from the sensors of the device such as mouse movements, keyboard typing etc. Specifically, having constructed a behavioural profile via operation of an app with the QBE SDK integrated the component is capable of identifying an individual, continuously providing an evaluation of the likelihood of an individual being who they claim to be. The technology uses a wide range of factors, including location data, sensor micro-electronic mechanical systems (MEMS) data such as accelerometer and gyroscope data, and touch behaviour (strokes/swiping) to construct a behavioural profile for a given individual.

4.7.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex C. System Requirements for Distributed Trust Management Framework, in Table 12 (functional) and Table 17 (non-functional). This list reflects the link of the module with the Retail Pilot, as well as the Manufacturing pilot (RIASTONE).

4.8 Device continuous behavioural authentication [T4.4]

4.8.1 Component Overview

The primary objective of this task is to implement Continuous Authentication (CA) for devices by monitoring and analysing two key metrics: device behaviour and device location. Regarding device behaviour, the authentication process will leverage Android System Logs to capture and analyse usage patterns during typical shifts. This will enable the detection of any deviations or anomalies in device behaviour. As for device location, Continuous Authentication will be achieved by tracking the device's location using RSSI (Received Signal Strength Indicator) signals from nearby access points, such as Wi-Fi or Bluetooth. The main components of this task are as follows:

- **Android Application:** Responsible for capturing and transmitting Android logs from devices to the server.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	40 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

- **Server:** Responsible for storing and analysing the Android logs to detect deviations in devices behaviour using machine learning techniques or to estimate the device's location by applying localization mechanisms.

4.8.1.1 Continuous Authentication Based on Device Location

To enable Continuous Authentication (CA) based on device location and to continuously monitor and estimate it, two localization algorithms have been implemented: Least Squares Optimization and Euclidean Distance:

- The Least Squares Optimization algorithm estimates the coordinates of a device.
- The Euclidean Distance algorithm determines the approximate area where the user's device is likely located.

Both algorithms rely on the Received Signal Strength Indicator (RSSI) from nearby access points, such as Wi-Fi or Bluetooth Low Energy (BLE). However, due to limitations in the Android OS, which does not continuously provide logs for nearby access points and their corresponding RSSI signals, the Android application periodically performs scans—currently set at 10-second intervals—to detect nearby access points and capture their RSSI signals. Once a scan is complete, this information is logged in the Android system and transmitted to the server for localization purposes. After the log is transmitted to the server, the localization mechanism processes the data using a predefined heatmap to evaluate whether the estimated location (coordinates or area) is acceptable. If the location is acceptable, the user's session remains active; otherwise, the server triggers an alert associated with that device and user. Although both algorithms are implemented and ready for use, additional evaluation tests are necessary to identify which algorithm provides the best performance metrics and accuracy.

4.8.1.2 Continuous Authentication Based on Device Behaviour

To enable Continuous Authentication (CA) based on device behaviour, we leverage Android system logs to capture the patterns of user devices during typical conditions. The primary goal is to train an AI/ML model on these usage patterns to establish a baseline of normal behaviour. This enables the model to detect deviations or abnormalities that differ from the baseline. Importantly, we do not have pre-defined labelled data or logs classifying anomalous behaviour or abnormalities. Therefore, the model must be trained using unsupervised or self-supervised learning methods. The pipeline is as follows:

- **Log Filtering and Transmission:** The application filters logs based on interfaces of interest—Networking, Bluetooth, and Battery—to manage the large volume of data. The filtered logs are then transmitted in real-time to the server for further processing.
- **Data Pre-Processing:** The server pre-processes the data to prepare it for input to the AI/ML model using a parser.
- **AI/ML Model for Behavioural Analysis (Risk Assessment Engine):** The pre-processed logs are fed into a Machine Learning model to detect abnormalities and deviations in device behaviour. The AI/ML model architecture primarily consists of the state-of-the-art pre-trained BERT (Bidirectional Encoder Representations from Transformers) model, enhanced with a custom Neural Network architecture on top to enable tailored training mechanisms. Since no labelled data is available, the model uses unsupervised or self-supervised learning. Once trained for each user, the model is expected to have learned the patterns of the established baseline behaviour. So, if an anomaly is detected, the model generates an alert associated with the user and prompts for authentication. Otherwise, the user's session remains active.
- **Retrieve Abnormality Scores:** A request can be made to the Server at any time to retrieve the abnormality scores for a specific device. The server maintains these scores for each device and provides them upon request.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	41 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

4.8.1.3 Implementation Progress Overview

Currently, the localization mechanisms—Least Squares Optimization and Euclidean Distance—are implemented and ready for use. However, additional tests are required to evaluate their accuracy and performance metrics to determine the best-performing method, as discussed earlier. The AI/ML model architecture has been defined, with minor adjustments planned to further enhance its accuracy. Additionally, the Android application is under development to ensure compatibility across various devices—including smartwatches, tablets, and phones—with a focus on user interface (UI) interactions. The server, which is also currently under development, will integrate a secure database to store workers' credentials and shift logs. This will enable the detection of deviations in both device behaviour and location, as well as the generation of abnormality scores for devices upon request.

4.8.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex C. System Requirements for Distributed Trust Management Framework, in Table 13 (functional) and Table 18 (non-functional). This list reflects the link of the module with the Smart Manufacturing-Case 2.

4.9 Hardening Against Side-channel Attacks [T4.5]

4.9.1 Component Overview

The component is composed of automated and manually applied countermeasures. As such, it slightly deviated from D2.3, where only automated countermeasures were planned.

First, the code polymorphism countermeasure has been extended, and is applicable automatically by a dedicated compiler, provided that the target ISA is ARMv7m, as planned in D2.3. Then, we developed C macros to help for the application of loop shuffling. In addition, we worked on finding better balance between security and performance impact, by considering the combination of countermeasures (loop shuffling and code polymorphism first, but also code polymorphism and masking more theoretically), and by developing and optimising a masked AES implementation by combining several state-of-the-art techniques for that purpose. Although manually applied, this work is paramount for the component due to the large usage of AES in practice, and the need for larger ISA support for the pilot (not only ARMv7m).

4.9.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex C. System Requirements for Distributed Trust Management Framework, in Table 14 (functional) and Table 19 (non-functional). This list reflects the link of the module with the smart hospitality pilot.

4.10 Exploratory Data Analysis Engine [T5.1]

4.10.1 Component Overview

Exploratory Data Analysis Engine (EDAE) has developed a series of services for ensuring data quality in order to be used from other TANGO components. Furthermore, EDAE has developed a series of reports in regard to transactions, sales volume, profitability, customer segmentation, customer preferences, popular products, shops profitability, sales etc. Results of the analyses will be reported within the corresponding deliverable. All services are dockerised. EDAE as a back-end service interacts with the TANGO front-end in order to provide in a dynamic manner results for the end users.

4.10.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex D. System Requirements for AI-based Framework for Green & Trustworthy Operations , in Table 20 (functional) and Table 29

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	42 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

(non-functional). This list reflects the link of the EDAE module with the Smart Hospitality, Retail and FMAKE pilots.

4.11 Energy efficient AI model training [T5.2]

4.11.1 Component Overview

T5.2 delivers three components to help on the process of generating and keep track of Machine Learning (ML) models to the TANGO pilots. The main goals and scope of these three components have not changed since the D2.3 release. The components are aimed to be used mainly by data scientist once the data is available to them. Due to the nature of the pilots, where the data is only shared among organisations sitting in the same pilot, the components are intended to be deployed at the pilots' sites, rather than in the central TANGO platform.

Deliverable D5.1 provides a more detailed description of the components. A short summary of the components is the following:

- The **Federated Learning (FL) support** provides the ability to perform federated training of ML models. In practical terms, the training process is divided among different client nodes with access to data. A central node is responsible of averaging the results of the local trainings to come up eventually with a new model. Note that this way of training does not require sharing the data, but rather the results of the local trainings (mainly local weights of the model). This is useful when participants in the training do not want to share the datasets for different reasons (e.g., sensitive or business reasons). List of features:
 - Based on FLEVIDEN, a tool under development by ATOS with extensions needed to support TANGO pilots. FLEVIDEN is modular and encapsulate different FL capabilities in Pods, which can be customised, replaced or extended to implement new functionalities.
 - The tool has delivered 2 versions so far. The most advanced version provides support for model creation based on Keras and PyTorch (recent addition to support the FMAKE scenario).
 - Local node communication can be done via HTTP protocol.
 - Added support for HDF5 datasets (requirement from FMAKE scenario).
- The **MLOps** support component enables the life-cycle management of ML models using a MLOps tool (MLFlow) in combination with other elements (e.g., MinIO, Jupyter Notebooks). Data scientists and ML engineers can use the component to track the entire training and model serving process. List of features:
 - Support for integrated Jupyter Notebooks.
 - Support for model training.
 - Support for model serving.
 - Support for model registry and versioning.
 - Support for creating end-to-end ML pipelines (workflow) for experimentation.
- The **AutoML** provides data scientists with automated processes to avoid repetitive steps to design and train ML models. The component comes with two favours. The first one is based on the MLJAR library and provides programmatic access. The second version is aimed towards less advanced users and provides a GUI based on the Mercury framework to access to the underlying MLJAR features. List of features:
 - Initial training using a CSV dataset provided by the user with different typical ML-based models.
 - Model comparison report, used to check the performance of each model.
 - The model selected can be used directly for prediction or being the baseline for further training or experimentation using the MLOps component.
 - Configuration capabilities

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	43 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

From a non-functional perspective, the technologies selected intend to minimise the energy footprint. The tools can be combined with other components to achieve this goal (e.g., MLOps combined with RENOPS to shift the training process when/where the renewable energy is available).

4.11.2 Functional & Non-functional Requirements

The final status of the requirements for this task is presented in Annex D. System Requirements for AI-based Framework for Green & Trustworthy Operations . Table 21 (Federated Learning), Table 22 (MLOps), and Table 23 (AutoML) present the status of the functional requirements of each of the components. The non-functional requirements of the components are listed in Table 30 (Federated Learning), Table 31 (MLOps), and Table 32 (AutoML). This list reflects the link of the modules to the Banking and Smart Manufacturing (FMAKE) pilots.

4.12 Dynamic Intelligent Execution on Heterogeneous Systems [T5.3]

4.12.1 Component Overview

Since D2.3, the technology developed in T5.3 for dynamic and intelligent execution on heterogeneous systems has been advanced. In a nutshell, the following functionality has been carried out till M28:

- **Development of a Python binding:** This software binding enables the interfacing of Python programs that offload the data processing onto hardware accelerators (e.g., multi-core CPUs, GPUs, etc.). The accelerated code is developed in Java, and it is transformed to a parallel implementation that can yield high performance via TornadoVM. The communication between Java and Python is transparent to users and it is powered by the polyglot runtime implementation of the Truffle framework[8]. An example of how to use polyglot programming is available in the TornadoVM blog series [9].
- **Containerized deployment:** The containers for deploying the T5.3 technology for dynamic and intelligent execution are available in DockerHub. Currently, we have created two Docker images, one for NVIDIA GPU hardware [10] and one for Intel CPU/GPU hardware [11]. The most recent tag is tango-v1.0.8. However, additional releases are going to follow till the completion of WP5.
- **Intelligent Execution Plan:** A Machine Learning model is trained based on various attributes, such as compiler features, performance counters, and power consumption counters. The trained model is going to be used to predict the most energy-efficient hardware to run the parallel implementations of data processing.

4.12.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex D. System Requirements for AI-based Framework for Green & Trustworthy Operations . The status of the functional requirements presented in Table 24 is still in progress, since the integration between the EDAE (T5.1) and TornadoVM (T5.3) is ongoing in the context of WP5 and WP6. Additionally, the non-functional requirement shown in Table 33 (non-functional) is dropped since the code implemented in T5.1 for data analytics will not explicitly use the Java API of TornadoVM. On the contrary, some analytic functions implemented in Java will be indirectly invoked by Python by exploiting the benefits of polyglot runtime implementations (i.e., via the Truffle framework). The T5.3 technology for dynamic intelligent execution on heterogeneous systems will be utilized to run parts of the analytic functions of the EDAE (T5.1). Therefore, it can be indirectly utilized by the TANGO pilots that use the data analytics functions, such as Smart Hospitality - Pilot 1, Smart Manufacturing - Pilot 3, and Retail - Pilot 6.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	44 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

4.13 Privacy Threat Modelling & Identification for Trustworthy AI [T5.4]

4.13.1 Component Overview

T5.4 introduces two advanced components designed to enhance privacy and fortify compliance with GDPR requirements. The **Privacy Enhancing Component (PEC)**, developed by UOG, serves as a comprehensive platform offering the following capabilities: (i) evaluate the necessity of conducting a data protection impact assessment (DPIA) for organisations managing personal and sensitive data, ensuring regulatory alignment; (ii) perform DPIA for both generic processes and services, and AI applications using sensitive data; (iii) identify and assess cyber threats that lead to potential privacy implications; and (iv) suggest countermeasures to mitigate the privacy threats. To date, two iterations of PEC have been released, with the latest version integrating enhanced countermeasure recommendation capabilities, building on the functionalities of its predecessor. PEC supports organisations in conducting a holistic DPIA, aligning with GDPR requirements while addressing privacy implications and offering robust countermeasures to manage risks effectively.

Complementing PEC is the **Privacy Assurance Tool (PAT)**, developed by FUJ_LU. This tool focuses on **user consent management**, ensuring secure and privacy-preserving data exchange while adhering to GDPR requirements. PAT operates through a consent-based access control mechanism, allowing data subjects to retain full control over who can access their data, for what purposes, and for how long. This ensures compliance with data protection regulations while fostering trust between organisations and users. Together, these tools provide a comprehensive suite for privacy enhancement, offering organisations not only compliance assurance but also a proactive stance in managing privacy risks and user consent effectively. Deliverable D5.1 provides a more detailed description of the components highlighting the requirements, methodology, architecture and support for pilots.

4.13.2 Functional & Non-functional Requirements

The final status of the requirements for this task is presented in Annex D. System Requirements for AI-based Framework for Green & Trustworthy Operations . Table 25 (PEC), and Table 26 (PAT) present the status of the functional requirements of each of the components. The non-functional requirements of the components are listed in Table 34 (PEC), and Table 35 (PAT). This list reflects the link of the modules with the Public Administration, Smart Hospitality, and Retail pilots.

4.14 X-AI For Privacy and Trust Enhancement [T5.5]

4.14.1 Component Overview

The primary objective and scope of this component remain consistent with the details provided in D2.3. It is designed to be primarily utilized by data scientists once the relevant data becomes available. Given the nature of the pilots, where data sharing occurs exclusively among organizations within the same pilot, these components are intended for deployment at the pilot sites rather than on the central TANGO platform.

The XAI module is used to describe an AI model, its expected impact and potential biases. It will help characterize model accuracy, fairness, transparency and outcomes in AI-powered decision making.

Apart from helping build trust in the predictions produced by the Machine Learning models, it also helps debug the models in cases where bias in the decision-making process is discovered.

Main features:

- Provide Machine Learning and Deep Learning model explainability.
- Present the explainability results in an easy-to-understand visual way.

A more detailed description can be found in D5.1.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	45 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

4.14.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex D. System Requirements for AI-based Framework for Green & Trustworthy Operations , in Table 27 (functional) and Table 36 (non-functional). This list reflects the link of the XAI module with the Banking and Smart Manufacturing (FMAKE) pilots.

4.15 Infrastructure Management based on AI [T5.6]

4.15.1 Component Overview

RENOPS (Renewable Energy Forecast Production Service) is a tool that provides accurate price predictions for renewable energy sources. It uses three components, including prediction services i.e., models providing the forecast for renewable availability or price, and an API gateway to interact with clients using REST API. The service serves as the main entry point into the system and runs new queries to obtain requested predictions based on parameters such as forecast location and type. It also uses feature engineering techniques to enhance the existing feature set and Temporal Fusion Transformer and Self-attention for forecasting renewable energy potential in different locations.

RENOPS integrates with other modules such as electricity price and job scheduling through its API gateway. The service acts as a gateway to the rest of the system, allowing clients to make requests for renewable energy availability or price predictions using REST API.

For example, in order to integrate with an electricity pricing module, RENOPS can be used to provide accurate predictions of renewable energy availability and price, which can then be used by the pricing module to determine optimal prices for different types of energy sources. Similarly, RENOPS can also be integrated with a job scheduling module to optimize the use of renewable energy sources in various industries such as transport, residential, and industrial use cases.

Overall, RENOPS' integration with other modules allows for more efficient and effective management of renewable energy resources, contributing to a more stable grid and maximizing the use of clean energy sources.

Some of the key features that have been developed so far include:

- A user interface (UI) for inputting coordinates and viewing forecasts
- Integration with various data sources such as historical weather and forecasted future weather variables
- An internal architecture for processing and forwarding inputs to the model
- Use of REST API for communication between components
- Implementation of an AI-based framework for green trustworthy operations
- Feature engineering to enhance the existing feature set, including constructing date-time features such as day-of-week, work-free-day, max-consecutive-work-free hours and others.
- The use of Temporal Fusion Transformer and Self-attention for forecasting renewable energy potential in different locations.

However, there are still several features that are yet to be developed or implemented. These include:

- Integration with other modules such as electricity price and job scheduling
- Improvements to the UI for better user experience
- Investigation into synergies with other tasks and tools that can benefit from using RENOPS
- Updates and future development of the tool's functionality
- Searching applicable jobs that can be time or geographically shifted.

4.15.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex D. System Requirements for AI-based Framework for Green & Trustworthy Operations , in Table 28 (functional) and Table 37

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	46 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

(non-functional). This list reflects the link of the RENOPS module FMAKE pilot and the possible integration between the tasks T5.1, T5.2 and T5.3.

4.16 User Interfaces [T6.3]

4.16.1 Component Overview

As described in D2.3, this component implements a unified User Interface for the TANGO platform. For most of the pilot applications within TANGO, this will be the central hub for end users and administrators.

An important function of the TANGO UI will be to integrate the various services developed or utilized by the project for user registration, authentication and authorization. Furthermore, after a user is authenticated, the UI will pass on the appropriate credentials to the pilot applications, in the form of cookies or tokens, ensuring that the user has access only to the content appropriate for their role.

Access to the technical offerings of the project from the UI will take one of two forms: either integrated within the UI (for example, the visualizations), or through an embedding of (or redirection to) their own web interfaces. In addition, where appropriate, the UI will provide access to user preferences, administration tasks, etc. for each pilot.

Due to differences of the various pilot applications that will make use of the UI (regarding the configuration of authentication services each applications uses, the type of integration with the UI, and the additional services provided by the UI), it is expected that it will not be possible for a single instance of the UI to serve them all. Instead, the UI will be configurable and modular so that separate instances, appropriately customized, will serve different groups of pilot applications.

The TANGO UI is being implemented as a Node.js web application, comprised of

- a frontend (user-facing) application, which will offer a rich and responsive UI to the users, and
- a backend (server) application, which will store necessary data and communicate (via REST API calls) with the other services.

At this point, integration with the registration and authentication services of the TANGO platform has progressed. Furthermore, discussions with the partners developing the pilot applications are underway in order to specify the best way to integrate each of them with the TANGO UI.

4.16.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex E. System Requirements for Visualisation Techniques & User Interfaces, in Table 38 (functional) and Table 40 (non-functional). This list reflects the link of the module with most of the pilots, since it involves not only the specific pilot functionalities in part of the pilots but the registration and login process of the TANGO platform

4.17 Visualisation Techniques [T6.4]

4.17.1 Component Overview

The scope of this component has slightly changed as to its support for the pilots, dropping Smart Manufacturing (FMAKE) one, as their visualisation needs will be addressed by other components.

In short, the Visualisation and Reporting Techniques component implements data visualisation interfaces to analyse big amounts of information, gathered from multiple sources and thus help decision-making pilot users to make informed, data-driven, decisions. This component provides visualisations for data analytics, including structured data and model patterns extracted from the analysis of processed data.

A more detailed description can be found in D6.1.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	47 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

4.17.2 Functional & Non-functional Requirements

The final status of the requirements for this component is presented in Annex E. System Requirements for Visualisation Techniques & User Interfaces, in Table 39 (functional) and Table 41 (non-functional). This list reflects the link of the module with the Smart Hospitality, Smart Manufacturing (RIAS) and Retail pilots.

4.18 TANGO Integrated Platform [T6.1-2]

4.18.1 Deployment View

As it has been described in D2.3, the TANGO integrated platform is based on software containerization, microservices and container orchestration technologies to benefit from features like software and resources isolation, portability across different deployment environments, load balancing, automatic deployments, secure communication among deployed services and fault tolerance. Specifically, it has been a strategic decision which has been followed since the beginning of the project to containerize the TANGO software components as much as possible and provide their docker images to the common private TANGO registry[12]. In this context the majority of TANGO components has been containerized and is available in the registry.

Moreover, Kubernetes has been used as the container orchestration technology for automating containerized applications' deployment, management and scaling, while satisfying the requirements for software and resources isolation as dictated from IDSA reference architecture [13]. Kubernetes is also the native deployment environment for FIWARE connector [14], which facilitates the integration for TANGO components and services, which extend the services of FIWARE DataSpace allowing deployment in different cloud providers and on-premises environments, enhancing portability and flexibility. This feature facilitates the deployment of the TANGO platform across different cloud environments, and it is beneficial, as for the deployments of the different TANGO pilots both cloud providers (e.g., AKS cluster [15]) and on-premises deployments are being used. In this context it is also essential for future exploitation of the TANGO solution. [15]) and on-premises deployments are being used. In this context it is also essential for future exploitation of the TANGO solution.

From a deployment view, following the hybrid deployment approach described in D2.3, the TANGO integrated platform consists of:

- The central TANGO cluster which is based on Kubernetes and has been set up with a dual role:
 - To provide an appropriate and common development/testing environment for all TANGO components, with the objective to validate their intended functionalities and integration among different components and services before their deployments in an operational context (TANGO pilot environments).
 - To host the TANGO Management domain consisting of centralized services, accessible across pilots as described in section 5.

The separation among the two roles is associated with the requirement for resources isolation among them and it is achieved using dedicated namespaces within the central Kubernetes cluster, utilized either for development/testing or production (pilot execution) deployments.

- The pilot-specific Kubernetes clusters hosting the Data Provider services for each pilot, as described in section 5.
- The pilot-specific consumer hosts (e.g., Docker supporting terminals or mobile devices) serving the TANGO consumer/client services.

To facilitate efficient deployments and testing across the development/testing and production environments of TANGO, a CI/CD system has been put in place, as it has been indicated in D2.3 and described in detail in D6.1. The role of the CI/CD system is to leverage automation procedures for software build, testing and deployment procedures, shortening the development cycles and in parallel

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	48 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

ensuring that TANGO component updates are first tested in the development/testing environment before getting transferred to the pilot execution environments as well. At the same time the deployments towards the different pilot execution environments are facilitated through the utilization of a central point (CI server) that can trigger all deployments through dedicated pipelines configured and accessed from the corresponding component providers.

Moreover, functionalities for automating the full-range of pilot-specific deployments towards the TANGO Management and Data Providers' Kubernetes clusters are planned to be put in place through the TANGO deployment orchestrator. As described in D2.3, the Deployment Orchestrator makes use of corresponding blueprint files and access to the TANGO container registry to manage such larger-scale deployments. These functionalities are envisioned to be accessible to specific roles of end-users (e.g., admin roles) through the TANGO UI dashboard as well.

More implementation details on the instantiation of TANGO integrated platform's deployment view will be provided in D6.2.

4.18.2 Non-functional Requirements

The final status of the non-functional requirements for the TANGO Integrated platform is presented in Annex F. System Requirements for the TANGO Integrated Platform (INTRA), in Table 42.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	49 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

5 TANGO Reference Architecture

5.1 Introduction

5.1.1 Architecture Overview

As acknowledged by a multitude of stakeholders and ecosystems (e.g., IDSA[16], Gaia-X [17], EOSC [18]), the development and evolution of trustworthy data sharing across domains are still in progress. This is due to the existence of numerous significant challenges that must be surmounted, including barriers such as data sovereignty, governance, interoperability, and environmental sustainability. The TANGO project is committed to addressing these challenges by delivering a secure and privacy-preserving framework that is designed in accordance with its Reference Architecture. This framework will utilize the innovative solutions provided by the consortium partners and will adhere to the principles of decentralization, federation, transparency, and compliance.

The architecture introduces a comprehensive and modular framework that is consistent with the fundamental technical principles of the TANGO ecosystem. This framework is based on containerized microservices and enables the dynamic orchestration of a variety of services and data-sharing workflows. These workflows are adaptable to a variety of deployment scenarios, including cloud-based, on-premise, and on user devices. The modularity of the system allows for a pick-and-mix approach, in which each module or service operates independently while still contributing to a cohesive ecosystem. This guarantees adaptability, enabling stakeholders to select and customize data services in accordance with their specific requirements.

The Reference Architecture consolidates a variety of heterogeneous technological assets, which are subsequently divided into three distinct layers based on their functionality:

- **Trust Layer:** This layer encompasses all the services and functionalities that enable the secure and trustworthy exchange of data and interaction between TANGO participants, such as the SSI Agent, PDP/PEP, CP-ABE, User Continuous Behavioural Authentication, etc.
- **Management Layer:** It includes the necessary services and functionalities for the orchestration, automatic deployment, and fine-grained control of the TANGO ecosystem (e.g., Configuration Manager, Deployment Orchestrator).
- **User Layer:** This layer is composed of the technology offerings developed by the TANGO consortium that provide users with added value in terms of efficient and privacy-preserving data operations, sharing, and visualization (e.g., Exploratory Data Analysis Engine, MLOps, Federated Learning, Privacy Enhancing Component, Explainable AI).

Modules from the three distinct layers are distributed across multiple runtime environments and physical locations in the form of containerized (micro)services. These modules are subsequently perplexed and interconnected to facilitate secure, sustainable, and transparent data sharing flows.

The TANGO Reference Architecture is further defined in the subsequent sections, which describe the roles of the data sharing participants and the functionalities of the relevant components. Additionally, a practical sequence of a demonstrative scenario is provided.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	50 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

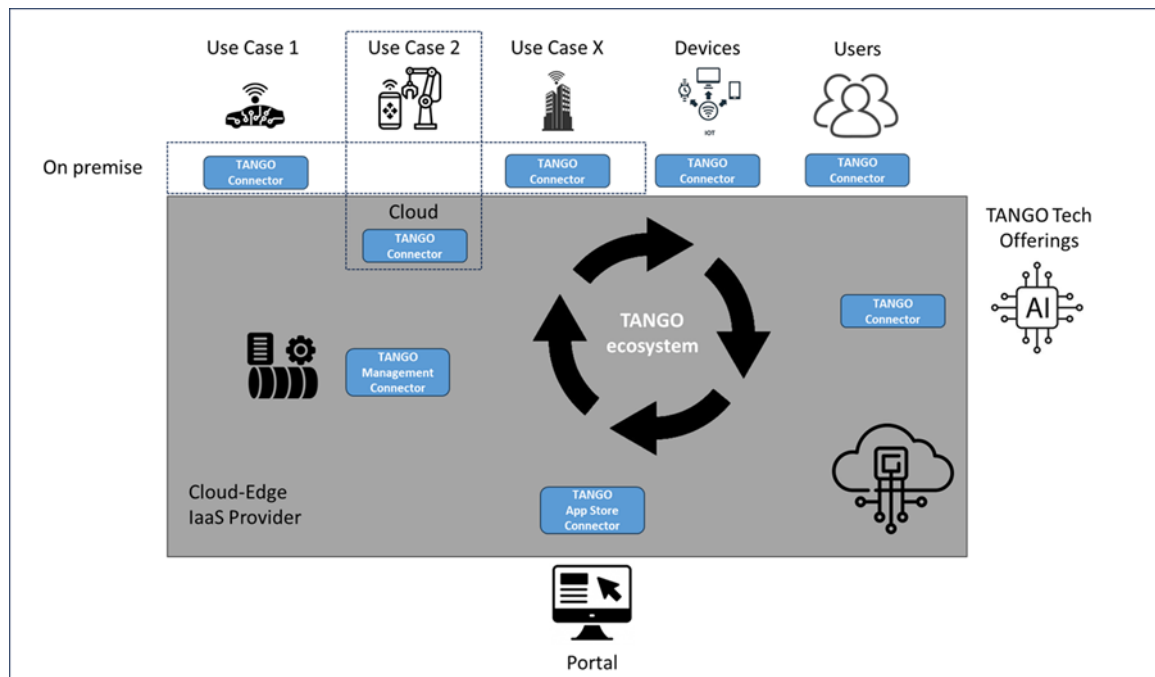


Figure 3: TANGO Ecosystem.

5.1.2 Alignment with dataspace initiatives

While the TANGO project is not directly involved in the design and development of tools and frameworks that are used for managing and maintaining a dataspace, its architecture still adheres to the principles of related dataspace initiatives (e.g. IDSA and Gaia-X) by incorporating a variety of technical components and approaches to guarantee the provision of data services and the exchange of sovereign, secure, and trusted data. To be more precise, the TANGO consortium adopted the viewpoint of the Data Space Business Alliance (DSBA[19]), which is dedicated to establishing a unified technical framework and a common perspective on dataspace that will facilitate alignment among its members (BDVA [20], FIWARE[21], Gaia-X, and IDSA) in order to achieve interoperability and portability of solutions across data spaces.

The TANGO Reference Architecture, similar to the GAIA-X and IDSA approaches, is based on a microservices approach and incorporates the concepts of Provider and Consumer. It also implements a decentralized data storage strategy, which entails that the data is physically stored within the data owner's infrastructure until it is transferred to a trusted entity outside of its connector. Data and service consumers are required to accept the provider's usage policies, which are subsequently enforced on the data and service offerings. By enabling well-defined interaction between connectors, the architecture fosters interoperability and relies on a decentralized identity management system for mutual authentication, thereby eliminating the necessity for a central authority to guarantee trust between participants.

Furthermore, TANGO incorporates the connector concept into its architecture, which provides a secure and isolated environment for data and services to be hosted. This concept also includes all the necessary functionalities for authenticating and authorizing users prior to granting them access to data. The TANGO consortium decided that the from-scratch development of a connector is beyond the scope of the project and its DoA. Consequently, it decided to enhance an existing open-source implementation of a dataspace connector with the consortium's tools for SSI authentication and attribute-based access control. To achieve this objective, we investigated numerous open-source implementations, including the Eclipse Dataspace Components (EDC [22]), a comprehensive framework that offers a fundamental set of features (functional and non-functional) that dataspace implementations can re-use and customize.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	51 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Additionally, we examined the Dataspace Connector [23], which was initially maintained by Fraunhofer ISST and subsequently by sovity. This connector utilizes the IDS Information Model and the IDS Messaging Services to facilitate message exchanges with other IDS components. Ultimately, we chose to proceed with the FIWARE Data Space Connector [14], a collection of multiple components that implement the DSBA Technical Convergence recommendations, with which the project aligns, after conducting a thorough analysis of the advantages and disadvantages of each implementation.

5.1.3 Enabling Pilots with the TANGO Architecture

Several pilot use cases will be deployed and presented to demonstrate the TANGO Reference Architecture's ability to provide a flexible, user-friendly, and trustworthy platform for data sharing. Each use case requires only a subset of the TANGO ecosystem's components for successful execution. Nonetheless, the modularity and elasticity of the microservices-driven TANGO Architecture will permit the accommodation of all use case pilots concurrently, by instantiating and configuring all the necessary components either on demand or proactively. This functionality will be enabled by a "blueprint" file containing all configuration parameters of the enabling services and connectors for each specific use case pilot. This file will be used by the system orchestrator to deploy and/or configure service chains hosted on multiple connectors that implement all operations required for the pilots' realization.

5.2 TANGO Ecosystem Overview

A typical dataspace ecosystem consists of several participants in various roles:

- The Provider, an organization offering data/services related to their sector, responsible for making data available in the dataspace and defining access policies and terms of use.
- The Consumer, another organization using these data/services after requesting access.
- The Application/Service provider, offering tools or services to enhance dataspace usability such as analytics, visualization or other data-related services.
- The Marketplace, which connects consumers and providers, facilitating data discovery and transactions between providers and consumers.
- The Identity Provider, who issues and verifies participant identities in the dataspace.
- The Trust Anchor, who ensures that participants and their activities comply with the dataspace standards.
- The Dataspace Operator, who manages the infrastructure and services enabling the dataspace.

In TANGO, we provide a variety of tools and frameworks, including AI and data analytics tools (WP5), for the use of Consumer participants in a dataspace. These tools can be deployed locally as on-premises applications or as centralized services. Nevertheless, we also introduce technology solutions that are designed to ensure the security, privacy, and trustworthiness of the data exchanges between a Provider and a Consumer. These solutions will also be tested and evaluated in the six pilot use cases. These are offerings that will be integrated to the connector's data flow, which in turn serves as the endpoint for data exchanges. They implement authentication, authorization, trustworthiness evaluation, and distributed storage founded on blockchain technology. As a result, the TANGO Architecture is primarily concerned with the interactions between a Provider and a Consumer, as well as with the Dataspace Operator, who is referred to as the TANGO Administrator. The Dataspace Operator is responsible for the management of the infrastructure and the provision of centralized services that are consumed by the participants. Additionally, TANGO is not directly involved in the establishment or maintenance of a specific dataspace, even though it aligns with and adopts the principles of dataspace initiatives. It rather offers the tools and frameworks necessary for secure and trustworthy data exchanges, which can be applied to a diverse array of use cases, as demonstrated by the evaluation of the TANGO pilots. Therefore, we may depart from the original concept, which assumes that Consumers and Providers are members of distinct organizations and define the employees of the Provider organization or its individual customers as data Consumers.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	52 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

5.3 TANGO Connector

The TANGO ecosystem is entirely composed of TANGO Connectors, each of which enables the provision and consumption of data and services from other TANGO Connectors. Consequently, there is no requirement for a centralized point that stores data and hosts services. The Connector is the primary entry point for a person, organization, or IoT device into the secure and trustworthy TANGO ecosystem. All Connectors are accessible through the standard IP protocol and can be deployed either on-premises or in the cloud.

The TANGO Connector is a secure and isolated environment that encapsulates a variety of management and trust-based services or technology offerings that are made available to the TANGO ecosystem. Each service is containerized and provides a variety of data transfer and configuration endpoints. The TANGO Connector is essentially a container management system (Docker, Kubernetes) that enables communication with other Connectors and their relevant services. Nevertheless, only data that is intended for sharing with other TANGO entities is made public. Secure protocols, including HTTPS, are implemented for both internal and external communication.

Several containerized applications are hosted by the Connector, which operates over one or multiple bare metal servers, virtual machines, or even IoT devices (although its capabilities may be restricted in this scenario). At least one containerized data service consumes or provides data from or to other participants in the ecosystem, as each Connector is associated with a TANGO technology offering or use case. Furthermore, the Connector may download and deploy multiple containers that implement additional TANGO technology offerings, including data preprocessing and hardware acceleration, from the App Store.

Figure 4 provides a high-level representation of the TANGO Connector that has been deployed on the Provider side. Each of the modules illustrated is briefly described in the subsequent subsections.

5.3.1 Authentication Portal

After being successfully authenticated and authorized for access, the Authentication Portal functions as a critical graphical user interface for TANGO users, enabling them to easily browse and examine the provider's technology offerings and data. The Portal offers a log in interface that redirects users to the SSI Verifier's interface, which manages the OIDC authentication process, enabling them to log in using their Verifiable Credentials. Following successful login, the user is able review the provider's available offerings, which may include data analysis and processing services, data visualizations, or raw data.

5.3.2 SSI Verifier

In order to establish trust and access control, the SSI Verifier is an essential part of the TANGO ecosystem that verifies the authenticity and integrity of verifiable credentials (VCs) presented by participants (e.g., data providers, data consumers, or users). It is essential to enabling secure and privacy-preserving interactions among participants in accordance with the principles of self-sovereign identity (SSI). Before engaging in data transactions or accessing resources, the SSI Verifier ensures that participants satisfy the necessary criteria, such as identity validation or certification. Specifically, the Verifier is responsible for verifying the validity of VCs by employing cryptographic methods to confirm that the VCs are signed by a trusted SSI Issuer and are not expired or revoked. Additionally, it resolves Decentralized Identifiers (DIDs) associated with the credential to ensure that the DID document corresponds to the public key or metadata used for validation. The Verifier generates an OIDC-compatible ID token that is structured to include claims derived from the VC after successful VC validation. This token is then sent back to the user, who will use it in their subsequent data transactions.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	53 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

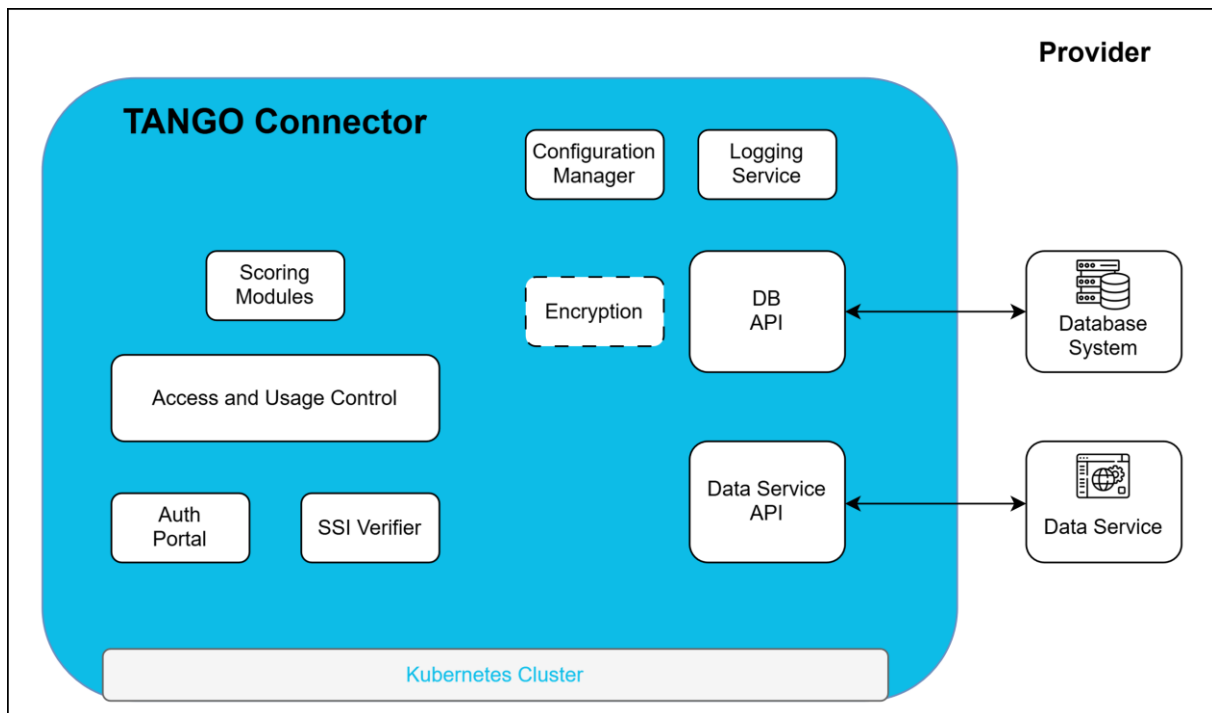


Figure 4: TANGO Connector on the Provider's side.

5.3.3 Access and Usage Control

The Access and Usage Control module is responsible for implementing and enforcing the Provider's data usage policies. These policies determine who may access data, under what circumstances, and for what purpose. The component is tightly integrated with the Attribute-Based policies described in Section 3.3.

While access control refers to a set of rules that define and specify who is permitted or has the rights to perform certain actions (e.g., gain access, read, write, transfer, copy) on a filesystem or more generally on the data resources of an IT system, the need to improve the control over the usage purposes of the data stored or the data flowing in a IT system, requires increased level of control capabilities and fine granularity on the data usage. To achieve this capability for enabling data usage control, it is required a data management framework that allows data producers to define and specify a set of rules that describe the usage of their data from other users (data consumers).

In the IDS Reference Model, the definition, the enforcement and the execution of specific rules, permissions and restrictions on the data usage is orchestrated by the IDS connector that performs the "Data Usage Control". The way that IDS connector enforces data usage control policies is described in the Position Paper of members of the IDS Association named "Data Usage Control in the International Dataspaces 3.0" [24], [25]. The paper explains how the data usage control is implemented within IDS Connectors.

More specifically, in the IDS Reference Model the access control is based on the XACML (eXtensible Access Control Markup Language) Standard to define policies and set ABAC (Attribute-Based Access Control) rules. In the data flow model of XACML specific components (that act as control points) are responsible for the policies implementation. Namely, Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Information Point (PIP), and Policy Administration Point (PAP). Relying on the access control model, the IDS Reference model extends it and uses it for the enforcement of usage rules by leveraging the aforementioned components to monitor, intercept and assess not only the existing but also additional information (e.g. metadata: involved stakeholders, owner, consumer, key dates, issued

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version	Page:	54 of 139
Reference:	D2.4	Dissemination:	PU
	Version:	1.0	Status: Final

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. There are three different type of conditions that refer to the data itself and are related in a timely manner with the actual time during usage (on-condition) and with the time before (pre-condition) and the time after (post condition usage).

The implementation of data usage and access control in TANGO Architecture, when a consumer requests access to certain data, involves two parallel sub-processes to ensure privacy and confidentiality: authentication through Verifiable Credentials (VCs) and authorization using the XACML framework. First, the user registers and authenticates at the connector, and when requesting access to an asset, the Verifier asks for VCs to validate that the user meets the attribute-based policies required for access. The Verifier ensures that the credentials are issued by trusted ecosystem participants and, if successful, issues a token to the user. The user uses this token to request the asset, and the Policy Enforcement Point (PEP) and Policy Decision Point (PDP) validate the claims in the token against defined policies, with the Policy Information Point (PIP) providing additional attributes if needed. If all conditions are met, the request is authorized, and the consumer gains access to the asset securely and in compliance with privacy requirements.

5.3.4 DB / Data Service API

The Database or Data Service API is a component designed to handle interactions between the PEP/PDP system and external services or resources, ensuring controlled access to the data stored by the provider. It acts as an intermediary that adapts to the providers' storage mechanisms or data processes, enabling secure communication and data retrieval based on access policies. When a requester sends a request to access a resource, the API is triggered by the PEP service, which verifies the requester's identity and permissions through the PDP. The API supports operations such as retrieving resources using a `GET` method or posting new resource data with a `POST` method, accommodating query parameters for filtering or resource details, respectively. The API's response depends on the type of operation, returning either the requested resource or a success/error message.

In a typical workflow, a user initiates a request to access a resource, including their identity information and a valid access token. The request is processed by the PEP, which validates the token and applies the necessary policies via the PDP. If authorized, the PEP issues a capability token to the user, allowing them to interact with the API to perform specific actions like querying or modifying a resource. The API translates these requests into a format understood by the pilot's external services, ensuring compatibility with the storage system. After processing the request and retrieving the data from storage, the API formats and returns the data to the requester, completing a secure and policy-compliant interaction. This API plays a critical role in ensuring seamless and secure data access within the TANGO ecosystem.

5.3.5 Scoring Modules

These are a variety of scoring modules that assess the trustworthiness and authenticity of the consumers who engage in the data exchange with the provider's Connector. The Trustworthiness scoring module, the User Continuous Behavioural Authentication module, and the Device Continuous Behavioural Authentication module are all involved. In order to issue a new or revoke an existing capability token for accessing requested data, the PDP component of the Access Control module utilizes a score for the trustworthiness or authenticity of the consumers generated by each of them.

5.3.6 Encryption Modules

The encryption modules in the provider's Connector allow for optionally encrypting data before being transferred to the consumer. The CP-ABE (Ciphertext-Policy Attribute-Based Encryption) module ensures confidentiality by encrypting data based on attribute-based policies. It allows data providers to define fine-grained access controls, where only consumers with attributes matching the encryption policy can decrypt the data. The process involves the producer encrypting data using a master public

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	55 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

key from a key authority, embedding sticky policies directly into the ciphertext. Consumers, after being authorized via the PEP/PDP system, receive the encrypted data and can decrypt it using a decryption key generated based on their attributes by the key authority. This mechanism integrates seamlessly into the TANGO Connector and with SSI components, enabling secure and privacy-preserving data sharing. The Self-Encryption module provides a unique, file-content-based encryption mechanism combined with a multi-factor information recovery system for enhanced data security. In this approach, files are split into chunks, with each chunk encrypted using the hash of its neighbouring chunk, ensuring that even minor changes in file content result in a completely different encryption outcome. Additionally, the encryption key is split into multiple pieces and distributed among participants or mapped to object features. Decryption requires a threshold number of these pieces to reconstruct the original key, offering a robust, multi-factor recovery process. The self-encryption module operates independently within the TANGO framework and can be deployed as a standalone API, ensuring adaptability across various platforms and secure file handling in distributed environments.

5.3.7 Configuration Manager

The Configuration Manager is responsible for receiving and applying configuration commands to the Connector, as its name implies. It configures aspects including container images, environment variables, networking, and service endpoint discovery. It can receive configuration information as configuration commands or YAML files. YAML files are a popular, human-readable configuration format used in Kubernetes-based environments that permits the definition of structures and their relationships.

The configuration options include the following, but are not limited to:

- **Container Images:** This option specifies the container image to be used for the deployment of a particular application/service, as well as the location of the registry where the image will be located and downloaded, and potentially the authentication key to be used with the registry.
- **Environment Variables:** This option specifies the values of several environment variables to be used and accessed by the associated application/service, as well as credentials and/or configuration parameters that customize the application's operation.
- **Networking:** Configuration options used to manage networking aspects such as connectivity and communication between containers in the Connector and the external ecosystem. The Configuration Manager is responsible for establishing networking rules, such as Service IP addresses and ports, exposing services via LoadBalancers and NodePorts, and managing network policies.
- **Service Discovery:** Configuration options for intra-cluster (within the Connector) and inter-cluster (with the outside ecosystem of TANGO) DNS-based service discovery.

The Configuration Manager can apply these configuration options both as initial settings during deployment and as dynamic changes to running containers without requiring applications to be restarted. In addition, if the Connector spans multiple nodes, it is the responsibility of the Configuration Manager to synchronize their configurations in order to maintain consistency.

5.3.8 Logging Service

The Logging component of the TANGO Connector is responsible for recording and optionally storing locally the details of all data transactions that occur both internally and externally with other TANGO Connectors. Each data transaction is associated with specific information, such as a unique identifier for the data, the Connector DID, the target URL of the external service with which the data is being exchanged, and data utilization and processing information.

When a data transaction concludes, it is the responsibility of the Logging component to store the transaction details to a database system for later inspection. This operation provides an additional layer of data integrity by ensuring that the Provider has all the necessary information to monitor and validate the data flows between the consumers and the Connector. In addition, the transaction details can be used

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	56 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

for auditing purposes and to ensure compliance with data usage policies and GDPR regulations, thereby promoting data management transparency and accountability.

5.3.9 Implementation of Connector at the Provider's side

As mentioned earlier, the TANGO consortium explored several options in order to select a suitable implementation of a dataspace connector, on which it will provide extensions and modifications in order to deliver the TANGO Connector. The primary goal was to select a connector that would align with TANGO's architecture and meet the project's specific needs without requiring the reinvention of existing solutions.

The decision to avoid reinventing existing solutions was driven by the recognition of the fact that existing open-source connectors are already offering a substantial foundation of features and capabilities, and consequently, reinventing these would have required a significant amount of time and resources, detracting from the project's primary objectives. Utilizing an established connector allowed us to:

- **Leverage Existing Solutions:** Exploit already-developed and thoroughly tested components, thus ensuring reliability and robustness.
- **Ensure Compliance and Interoperability:** Align with dataspace standards and practices, specifically those outlined by IDSA and Gaia-X.
- **Focus on Enhancements and Customization:** Allocate resources to enhance and customize the chosen connector, rather than building from scratch.

To this end we considered the following three connectors:

1. **Dataspace Connector:** IDS connector, originally developed at the Fraunhofer ISST and then maintained by sovity.
2. **Eclipse Dataspace Components (EDC):** A well-supported option with strong community.
3. **FIWARE Data Space Connector:** Recommended by the Data Space Business Alliance (DSBA).

The following criteria were considered in order to evaluate the connectors:

- **Alignment with initial Architecture:** Compatibility with TANGO's predefined architecture and support for integrating existing TANGO components.
- **Support for Decentralized Identity (SSI):** Interoperability with TANGO's solutions based on Decentralized Identities and Verifiable Credentials.
- **Community and Maintenance:** Regular updates and an active community to ensure long-term sustainability.
- **Ease of Deployment and Configuration:** Simplification of the deployment process and less complex configurations.

After thorough evaluation that included the deployment of the connector under test, an operation of a simple data exchange and an extensive source code inspection, we opted to select the FIWARE Data Space Connector for fulfilling the needs of our project. Based on the evaluation criteria, we considered the following advantages of this connector:

- **Alignment with DSBA Recommendations:** Implements DSBA Technical Convergence recommendations, which aim to provide a common technical framework for the technical alignment between BDVA, FIWARE, Gaia-X and IDSA, thus ensuring interoperability and portability across data spaces.
- **Support for SSI and ABAC:** Implements authentication based on W3C DID [26] with VC/VP standards [27] and authorization based on attribute-based access control (ABAC), aligned with XACML architecture [28].

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	57 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

- **Regular Maintenance:** Actively maintained with regular commits, ensuring ongoing support and updates.
- **Alignment with the TANGO Architecture:** Fits with the flexibility and modularity that our microservices approach aims to achieve, by being constituted of a collection of individual containerized components.

However, there are some minor disadvantages that we have also considered:

- **Maturity:** Although not fully mature, the connector was deemed usable and adaptable to the TANGO's needs.
- **Current scope:** Initially supports ETSI NGSI-LD data exchange [29], which require extensions for the broader use cases of TANGO.

Technically, the FIWARE Data Space Connector is a Helm chart [30], which bundles charts for all the necessary components and simplifies the deployment of all these components. Thus, being provided as Helm chart, the FIWARE Data Space Connector can be deployed on Kubernetes environments.

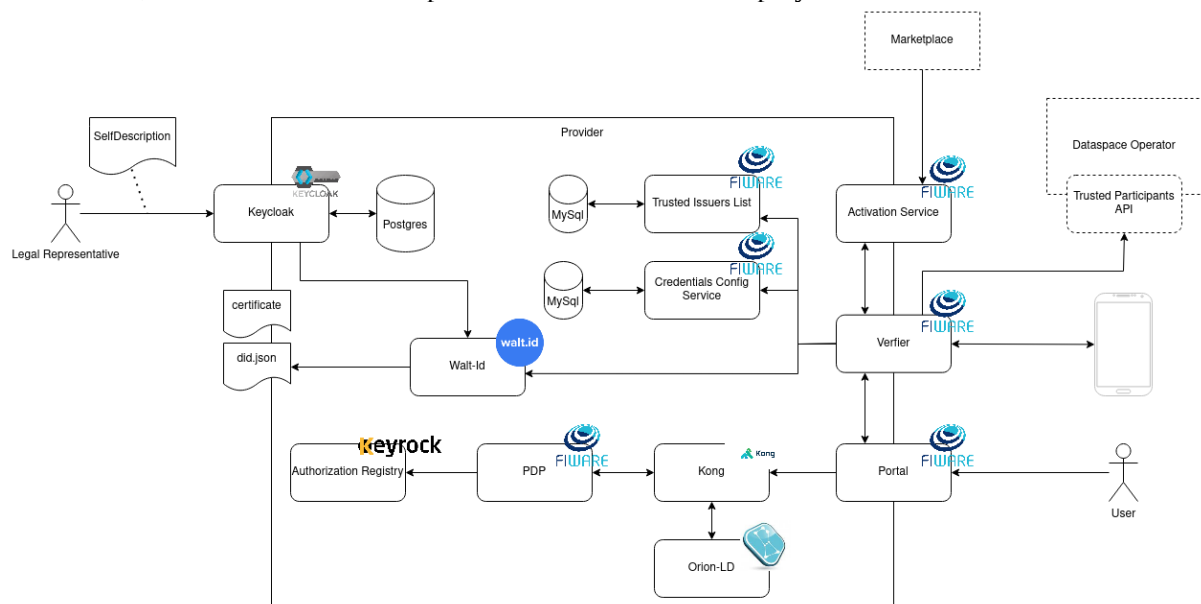


Figure 5: FIWARE Data Space Connector high-level overview.

The figure provides a high-level overview of the different components that constitute the FIWARE Data Space Connector and which are enabled for the Provider role. A list is following that briefly describes them:

- **Portal:** GUI for users to manage their service interactions.
- **Keycloak (IDM System) [31]:** Issues Verifiable Credentials (VCs) to employees and offers self registration capabilities.
- **Walt-Id [32]:** Creates and signs the actual Credentials and offers the did.json, corresponding to the participants identity. Also, it verifies various parts of the credentials.
- **Activation Service:** Interfaces with the marketplace to register new consumers.
- **Verifier:** Provides the authentication capabilities for the portal (allowing users to log-in).
- **Credentials Config Service:** Supplies the Verifier with necessary information about the scope and trust anchors.
- **Trusted Issuers List:** Used to verify whether issuers are authorized to issue certain credentials.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	58 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

- Kong (API Gateway) [33]: Enforces authorization on requests to the Orion-LD, acting as a Policy Enforcement Point (PEP).
 - PDP (Policy Decision Point): Decides on the authorization requests.
 - Authorization Registry: Provides policies used by the PDP.
 - Orion-LD: NGSI-LD backend system that handles data exchanges.
 - Trusted Participants Registry: Lists trusted participants via an EBSI-compliant API.

The TANGO consortium will reuse several components of the FIWARE Data Space Connector where their functionality aligns with and supports the project's goals. However, for components such as the Verifier and Issuer, PDP (Policy Decision Point), and PEP (Policy Enforcement Point), TANGO will replace these or extend them with its own solutions.

5.3.10 TANGO Connector on the Consumer side

We also adopt the concept of the TANGO Connector on the Consumer side, although the implementation details differ significantly. We are referring to the Connector as the collection of individual components that are deployed on the Consumer's workstation in a Docker environment or on their smartphone/tablet.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	59 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

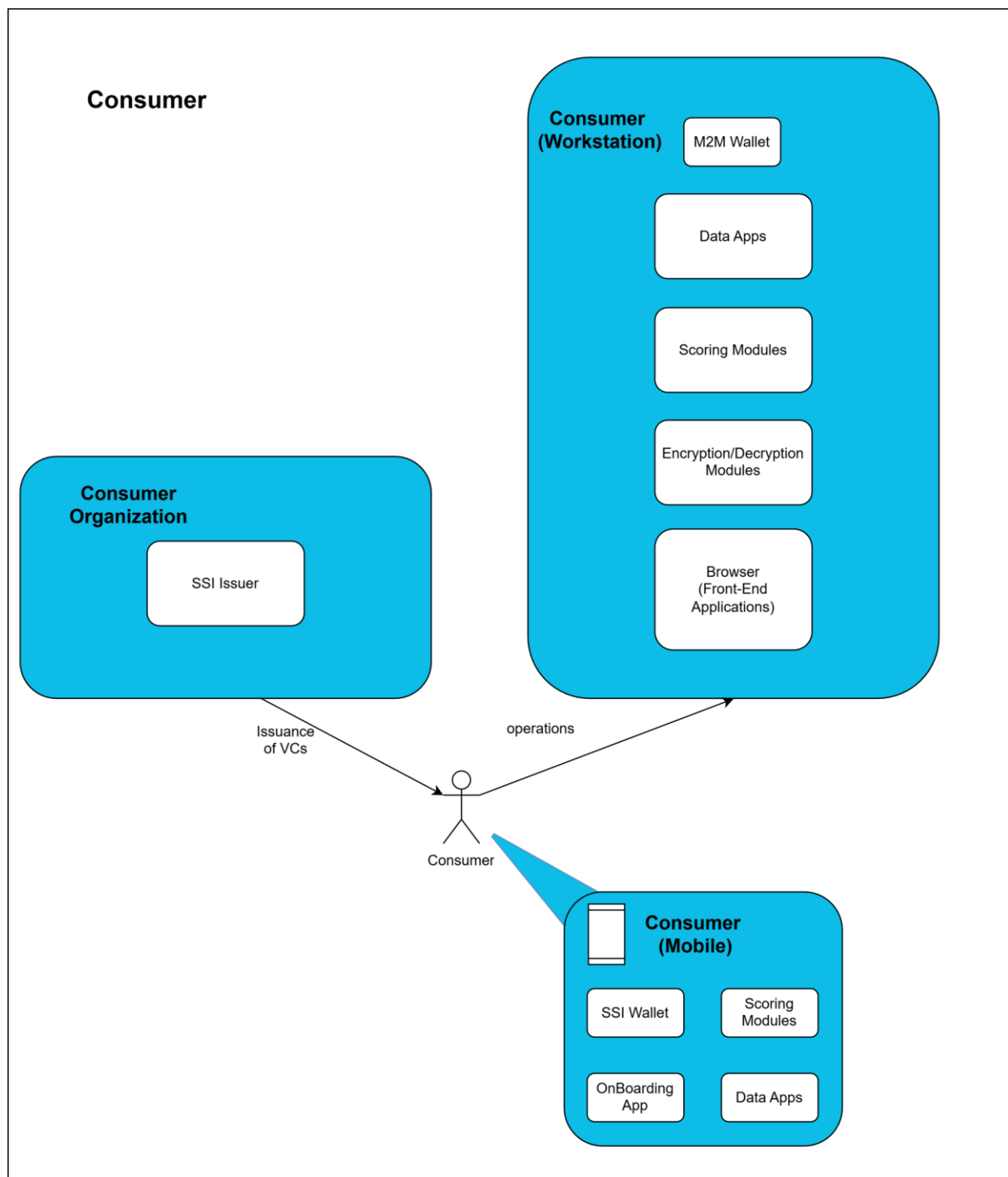


Figure 6: TANGO Connector on the Consumer's side.

This set of components involves SSI-related tools, including the SSI Wallet, which is applicable for both cross-device and machine-to-machine authentication flows. Additionally, it includes an Onboarding Application that facilitates the user's entry into the TANGO ecosystem, encryption and decryption modules, client-side implementations of the various scoring modules that are deployed on the Provider (Trustworthiness, UCBA, DCBA), and a variety of data applications that are either locally installed or accessible through the Consumer's browser. Moreover, the SSI Issuer is deployed on the Consumer's

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version	Page:	60 of 139
Reference:	D2.4	Dissemination:	PU
	Version:	1.0	Status: Final

organization to issue Verifiable Credentials to its employees, which will be utilized during transactions with the various Providers.

5.4 Blueprint

For the instantiation of every TANGO Connector, an appropriate configuration is needed in order to bring the Connector to the desired state that is required for being able to perform a specific operation in the scope of a specific scenario or a pilot use-case. Such configuration is defined in an agreed format (i.e., a YAML file) and stored into a file that will serve as the declarative definition of the Connector and its associated containerized components. It enables the definition of properties and attributes that specify how the components are created, managed and interconnected within the Connector.

As the TANGO Connectors are based on a Container Management System such as Kubernetes, a helpful example of a configuration file like the aforementioned would be a YAML file that defines a “Deployment” in Kubernetes and which is provided below.

```

1  apiVersion: apps/v1
2  kind: Deployment
3  metadata:
4    name: my-deployment
5  spec:
6    replicas: 3
7    selector:
8      matchLabels:
9        app: my-app
10   template:
11     metadata:
12       labels:
13         app: my-app
14     spec:
15       containers:
16       - name: my-container
17         image: my-image:latest
18         ports:
19         - containerPort: 8080

```

Figure 7: YAML configuration file of a Kubernetes Deployment.

This example specifies a “Deployment” Kubernetes resource that holds three replicas of a pod that consists of a single container that is named “my-container” and is based on the image “my-image”. This “Deployment”, also, is executed as a service that exposes an endpoint at port 8080.

There are several options that can be configured via YAML files, and besides the ones shown with this example, another useful option is the definition of a “ConfigMap”.

```

1  apiVersion: v1
2  kind: ConfigMap
3  metadata:
4    name: my-configmap
5  data:
6    my-property: my-value

```

Figure 8: ConfigMap option

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	61 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

A “ConfigMap” allows to define properties as key-value pairs that are later passed as environment variables within containers. Below is an extended example of the previous “Deployment” that uses the attribute “my-property” from the above “ConfigMap” in order to pass it as an environment variable to the “my-container” container.

```

1  apiVersion: apps/v1
2  kind: Deployment
3  metadata:
4    name: my-deployment
5  spec:
6    replicas: 3
7    selector:
8      matchLabels:
9        app: my-app
10   template:
11     metadata:
12       labels:
13         app: my-app
14     spec:
15       containers:
16         - name: my-container
17           image: my-image:latest
18           ports:
19             - containerPort: 8080
20           env:
21             - name: MY_PROPERTY
22               valueFrom:
23                 configMapKeyRef:
24                   name: my-configmap
25                   key: my-property

```

Figure 9: Passing environment variables to containers.

Another useful option to be used in the scope of TANGO is the “imagePullSecrets” that define the encryption keys that are used to authenticate for pulling containers from a private container registry. The below code snippet extending the previous “Deployment” example illustrates the process.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	62 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

```

1  apiVersion: v1
2  kind: Secret
3  metadata:
4    name: my-secret
5  type: kubernetes.io/dockerconfigjson
6  data:
7    .dockerconfigjson: <base64-encoded-docker-config-json>
8  ---
9  apiVersion: apps/v1
10 kind: Deployment
11 metadata:
12   name: my-deployment
13 spec:
14   replicas: 3
15   selector:
16     matchLabels:
17       app: my-app
18   template:
19     metadata:
20       labels:
21         app: my-app
22     spec:
23       imagePullSecrets:
24         - name: my-secret
25       containers:
26         - name: my-container
27           image: registry.example.com/my-image:latest
28           ports:
29             - containerPort: 8080

```

Figure 10: Sample configuration file using the “ImagePullSecrets” option.

The “Secret” resource contains a Docker registry credential secret, which is a base64-encoded Docker configuration JSON and the private repository from where the image of the container is pulled is indicated in the field “image” of the “containers” section.

In the scope of TANGO, we define as a “blueprint” or “recipe” a configuration file (i.e., a Kubernetes YAML file) or a collection of configuration files (i.e., a Helm chart) that are used to define and configure a complete service chain, which consists of multiple interconnected and interdependent services that collectively constitute a TANGO technology offering. The blueprint describes the desired state of services, including their configuration, environment variables, dependencies, and relationships. Blueprints provide a flexible way of deployment, configuration and management of the lifecycle of TANGO Connectors and the efficient reuse of the infrastructure in order to accommodate the needs of TANGO technology offerings and pilot use-cases.

5.5 TANGO Management Connector

The TANGO Administrator is responsible for the operation and maintenance of the TANGO Management Connector, which is equipped with all the necessary services and modules to ensure the reliable management of the TANGO ecosystem and its transactions. The TANGO Management Connector is responsible for hosting the TANGO Management and Trust Services, as well as interacting with and configuring the TANGO Connectors. It is also responsible for the administration and orchestration of the ecosystem, for managing configuration file repositories, the deployment of TANGO connectors, and their configuration to facilitate use-case-specific operations. The TANGO Trust services

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	63 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

are responsible for the establishment of trust relationships within the ecosystem. Furthermore, the TANGO Management Connector hosts general-use centralized services, including RENOPS and PEC, as well as key storage for encryption and decryption modules. The TANGO Management Connector is illustrated at a high level in Figure 11.

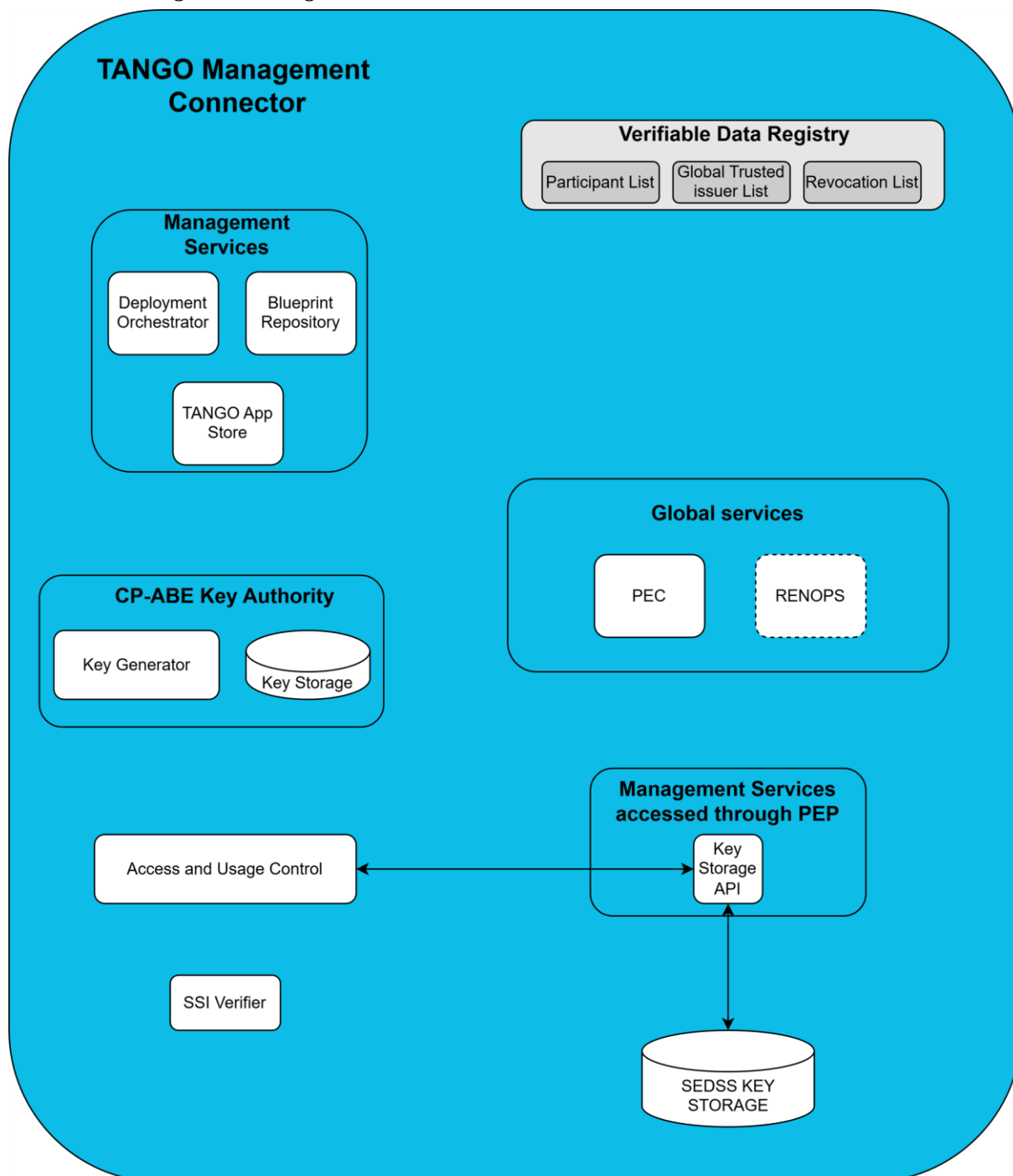


Figure 11: TANGO Management Connector.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	64 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

5.5.1 Deployment Orchestrator

The Deployment Orchestrator is a control-plane component that ensures the efficient, consistent, and harmonious deployment of various software components and services within the TANGO environment. Its main objective is to bridge the sometimes-vast gap between the multiple operational environments by automating various software deployment processes.

The orchestrator offers a robust suite of features. At its core, it manages configurations, holding vital details for services ranging from environment variables to runtime settings. A generic lightweight resource abstraction layer has been developed, thus enabling uniform deployment and execution of various services and applications, while the execution model is based on the adoption and adaptation of the serverless paradigm. Moreover, the orchestrator promotes automated deployments, providing tools to facilitate a seamless transition from development to production through Continuous Integration and Continuous Deployment (CI/CD) methodologies. It also takes on the role of a diligent resource manager, allocating and dynamically scaling resources like compute power, memory, and storage based on the service demands.

With every new service/application deployment request, the orchestrator fetches deployment configurations tailored for the target environment. It conducts thorough dependency checks, followed by resource allocation based on specific service requirements. Services are then deployed, adhering to a defined sequence that ensures their smooth operation and inter-service communication. Post-deployment, a continuous monitoring mechanism watches over the services, ensuring optimal operations and alerting in case of discrepancies or outright failures. TANGO Connector instantiation and/or configuration is orchestrated by the Deployment Orchestrator module. It accepts a blueprint configuration file as input and instantiates and configures the service chain of a technology offering by selecting the appropriate deployment environment (e.g., on-premises, remote cloud) and interacting with the suitable configuration endpoints of the TANGO Connectors.

5.5.2 Blueprint Repository

The Blueprint Repository is a centralized storage or version control system that hosts a collection of configuration files, “blueprints”, in standard formats (YAML files, Ansible Playbooks, Helm charts, Dockerfiles for docker container images creation, etc.) that define and configure service chains within the context of the TANGO ecosystem. These blueprints serve as declarative definitions of TANGO Connectors and their associated containerized components, providing the necessary instructions to bring the Connectors to the desired operational state for specific scenarios or pilot use cases. The Repository is organized for easy access and management of the blueprints and incorporates a version control system, allowing tracking changes over time.

The Blueprint Repository enables efficient reusability of configurations and infrastructure settings, making it easier to deploy and maintain similar TANGO technology offerings or adapt existing blueprints for new use cases. Furthermore, it incorporates access controls to ensure that only authorized users can access, modify and contribute to the blueprints and facilitates collaboration between the various service owners to share and contribute to the configurations and deployment plans.

Considering the aforementioned requirements, GitHub code hosting and version control platform [36] is used for the blueprint repository. Selected blueprints of the repository relevant to the configuration of service chains will be accessible through the App Store to be provided to the deployment orchestrator (section 7.4.2). GitHub repository will also be an integral part of the CI/CD system described briefly in section 8.1, as the main project’s repository supporting both daily development/testing operations and production deployments. Access control is provided through the creation of distinct and dedicated projects within GitHub, where only authorized parties involved in the corresponding developments and service chain deployments have access.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	65 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

5.5.3 TANGO App Store

The TANGO App Store is a centralized storage system where container images that constitute TANGO technology offerings are stored. The images are pre-packaged, ready-to-run and can be deployed to any Connector that by default has a container runtime. The TANGO App Store supports versioning of the container images, so that different versions of the same technology offering can be stored, enabling easy rollbacks, upgrades, and maintenance. It integrates with container management systems like Kubernetes, enabling smooth image deployment and orchestration. Along with the container images, additional metadata is stored that provides information, such as version, authorship, and usage instructions. Finally, security measures such as image signatures, checksums, and digital certificates are implemented to safeguard the integrity of container images. Authentication and authorization mechanisms will restrict access to images to specific users or groups.

For hosting and managing container images according to the aforementioned requirements, a Docker registry [43] is employed. The private image repository will also be accessible by TANGO developers and testers through the CI/CD system for automated software testing and deployment pipelines (described in section 8.1) to retrieve and deploy the target containers at the corresponding connector (Kubernetes) environment.

To secure the private image repository, strong authentication and access authorization measures are put in place, using security certificates, HTTPS connections, and access control to ensure that only authorized parties have access to specific software artifacts.

5.5.4 Verifiable Data Registry

The Verifiable Data Registry is a core component of the Self-Sovereign Identity (SSI) ecosystem, serving as a decentralized repository that enables secure and trustworthy management of verifiable credentials. It acts as the backbone for recording, verifying, and referencing critical information, such as a participant list, a trusted issuers list, and a revocation list. The participant list ensures that all entities that participate in the SSI ecosystem, such as users, organizations, or devices, are identifiable through Decentralized Identifiers (DIDs), maintaining transparency and accountability. The trusted issuers list contains a registry of credential issuers authorized to create and sign verifiable credentials and the revocation list enables real-time status updates for issued credentials, allowing participants to determine whether a credential has been revoked, expired, or remains valid. Together, these components ensure interoperability, compliance, and a robust trust model within the SSI-enabled TANGO data-sharing ecosystem.

5.5.5 CP-ABE Key Authority and Self-Encryption Key Storage

In the CP-ABE (Ciphertext-Policy Attribute-Based Encryption) operations, the Key Authority plays a central role in ensuring secure and controlled data access. It is responsible for generating and managing cryptographic keys, specifically the master public key used for encrypting data and the private key used to create decryption keys. The Key Generator submodule within the Key Authority issues decryption keys tailored to the attributes of a consumer, ensuring that only users whose attributes satisfy the defined access policy can decrypt the data. This attribute-driven approach enforces fine-grained access control, maintaining confidentiality throughout the data lifecycle.

For the Self-Encryption module, the encryption keys are securely stored and managed, using a robust secret management tool (i.e. HashiCorp Vault). This tool provides an API for key storage and retrieval, facilitating secure access to encryption keys during the encryption and decryption processes. The consumers of encryption/decryption mechanism interact with the Key Storage API to securely store hashed encryption keys or retrieve them when required. This interaction goes through the PEP/PDP access control modules that enforce policies for access control. This integration ensures that the self-encryption process remains secure, scalable, and adaptable for distributed environments.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	66 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

5.5.6 TANGO Centralized Services

The TANGO Management Connector additionally hosts centralized services offered by the TANGO Administrator across the entire ecosystem and which are use case agnostic. Such services can be considered the Privacy Enhancing Component (PEC) or the Renewable Energy Forecast Production Service (RENOPS). PEC is a centralized service designed to facilitate Privacy Risk Assessment by identifying privacy threats, calculating risk scores, and recommending safeguards for mitigating these risks. PEC integrates seamlessly into the TANGO platform as a decision-support tool, helping organizations align with GDPR compliance while addressing privacy risks associated with cyber threats and data processing activities. Its modular architecture includes components like a Risk Identifier, Scoring Engine, and Recommendation Engine, which collectively provide actionable insights and tailored privacy safeguards. The backend services running on the TANGO Management Connector are integrated with a user-friendly dashboard to visualize risks, evaluate compliance, and document privacy impact assessments, enabling efficient privacy management at scale. On the other hand, RENOPS operates as a centralized service for predicting renewable energy availability and energy prices, aiding organizations in optimizing energy-intensive tasks. Its REST API, hosted on the TANGO Management Connector, acts as a gateway for accessing forecast data and powering applications like scheduling tools. The RENOPS Scheduler, integrated with the service, automates periodic tasks such as AI model training, enabling cost-effective and environmentally efficient energy use by identifying optimal execution windows based on forecast data. Both PEC and RENOPS provide centralized, user-centric services that address critical aspects of privacy and energy management within the TANGO ecosystem.

5.6 Practical Sequence

What follows is a practical and demonstrative scenario of a user onboarding to TANGO and requesting access to a data resource that is protected under a specific access policy defined by the Provider, as well as encrypted with CP-ABE encryption:

Step 1: Issuance of Verifiable Credential

1. User Onboarding with ePassport Credential:

- The user downloads the necessary apps (ePassport Issuer app and SSI Wallet).
- The user scans their ePassport and provides biometric data (e.g., facial recognition) through the ePassport Issuer app.
- The app validates the ePassport's electronic authentication and biometrics.
- Upon successful validation, a Verifiable Credential (ePassport) is issued and added to the user's SSI Wallet.

2. Requesting Additional Credentials from an Organization:

- The user accesses the organization's onboarding portal and requests an employee/customer credential.
- A QR code is generated by the portal and scanned by the user's SSI Wallet.
- The wallet presents the user's existing ePassport credential to the organization's SSI Agent for verification.
- The SSI Agent validates the credential and queries the organization's database for relevant claims.
- A new Verifiable Credential (e.g., EmployeeCredential) is issued and stored in the user's SSI Wallet.

Step 2: Encryption of Data by the Provider

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	67 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

1. **Key Initialization:**
 - The **Key Authority Server Module** generates a master public key and private key pair.
 - The master public key is published and made available to the Provider.
2. **Data Publishing:**
 - The Provider initializes encryption using the **ABE Toolbox**.
 - The Provider encrypts the data using **CP-ABE** based on an access policy (e.g., specific user attributes like role or organization).
 - The encrypted data and its associated metadata are stored to a database.
3. **Key Distribution:**
 - The consumer's client (e.g., CP-ABE client) requests the attribute decryption keys from the **Key Authority Server Module**.
 - The Key Authority Server verifies the user's attributes (via SSI credential verification and claims).
 - If the attributes align with the defined policy, the decryption keys are generated and provided to the consumer.

Step 3: Retrieving an Access Token Using the SSI Verifier

1. **User Initiates Authentication:**
 - The user opens a frontend application that redirects them to the login page of the SSI Verifier.
 - The SSI Verifier displays a QR code containing an openid: connection string with the necessary information to start the authentication process.
 - The user scans the QR code using their SSI Wallet.
2. **Authentication and Credential Verification:**
 - The SSI Verifier retrieves the scope information from its configuration service.
 - The user approves the interaction between their wallet and the SSI Verifier.
 - The wallet presents the Verifiable Credential using the OIDC4VP flow.
3. **Credential Validation:**
 - The SSI Verifier verifies the presented credential against:
 - The configured policies.
 - Trusted participants' registries.
 - Trusted issuer lists to confirm that the issuer is authorized to issue the credential with the given claims.
4. **Token Generation:**
 - After successful verification, the SSI Verifier generates a JWT (access token).
 - The frontend application is informed via a callback, and the token is retrieved through the token endpoint.

Step 4: Accessing Protected Data Resources

1. **User Request:**
 - The user sends a request to access protected (encrypted) resources (e.g., GET/POST) using the obtained JWT.
 - The Policy Enforcement Point (PEP) intercepts the request and forwards it to the Policy Decision Point (PDP) for evaluation.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	68 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

2. Authorization Evaluation:

- The PDP verifies the JWT and associated claims, such as roles, permissions, and validity.
- If authorized, the PDP issues a Capability Token to the user for subsequent requests.

3. Resource Access:

- The user includes the Capability Token in their request, which is forwarded by the PEP to the API.
- The API interacts with the external service/database to retrieve the requested data securely.
- The data is returned to the user in a secure format (e.g., JSON).

4. Key Verification and Retrieval:

- If the user has the required decryption attributes, the CP-ABE client retrieves the attribute decryption keys from the Key Authority Server Module.

5. Decryption Process:

- The CP-ABE client uses the decryption keys to decrypt the data locally.

6. Data Delivery:

- The decrypted data is presented to the user.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	69 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

6 Privacy, Ethical, Social and Legal Impact Assessment

6.1 Legal assessment of the TANGO technology

The current section provides a conclusive legal assessment of TANGO's framework, focusing on certain aspects of its components that have not been developed in previous deliverables, but should not, nonetheless, be left unexamined. This entails a more in-depth approach solely to certain of the technologies developed under the Distributed Trust Management Framework component. As regards the choice of the technologies assessed, the former is not arbitrary. It is rather based on their sensitivity and/or prevalence in the current time, and under the consideration that the Distributed Privacy Preserving Data Management and Storage component has been sufficiently detailed in D3.1; it should be furthermore noted that additional considerations will be provided in D3.2 in that regard. Insofar as the technologies developed under the AI-Based Framework for Green and Trustworthy operations component are concerned, the former are solely subject to an extensive ethical assessment in subsection 6.2 of the present section.

The structure which this subsection follows includes (a) a descriptive part, where general information on the technology are provided with respect to the relevant legal framework, (b) an assessment part, where a Privacy Impact Assessment (PIA) is conducted, in order to assess any privacy risks identified for the technology in question, and provide recommendations on mitigation measures thereto, (c) a consultative part, where general guidelines for compliance are presented in a neutral manner, in the form of a user-friendly checklist.

Additionally, the results of the data summary part of the Data Management and Ethics Questionnaire (WP7) provide some supplementary information with respect to the PIA. These results are attached as an Annex (Annex G) to the present deliverable.

6.1.1 Self-Sovereign Identity (SSI) Management [T4.1]

6.1.1.1 On the concept of Self-Sovereign Identity (SSI)

In an attempt to better understand what the SSI entails, it is important to break down the concept and focus on its main component, that of **identity**. Identity is inherent to human beings, as it something intrinsically linked to concepts such as self-awareness and self-determination. On the evolution of identity, Allen speaks of four distinct phases which have drawn the contours and subsequently defined identity in the digital era [34]:

- During the first phase, identity was strictly **centralised**. Only centralised authorities were able to issue and authenticate digital identities. Examples of such organisations are IANA (1988) and ICANN (1998) which were responsible for the validation and distribution of IP addresses and domain names respectively. Unfortunately, centralised digital identities controlled by few authorities are plagued by similar problems such as the ones that occur in the physical world: users are being dependent on the decision of an authority, which unavoidably holds alone all that power and is subject to very limited control for the decisions that it takes.
- In the second phase, control was exercised by multiple and federated authorities, and identity entered in a **federated** state. Two initiatives of two tech rivals marked this phase: Microsoft's Passport (1999) and Sun Microsystem's Liberty Alliance (2001). Especially the latter, while seemingly resolving the issues with power concentration of single centralised authorities by allowing users to use the same digital identity in multiple, different sites, resulted in the creation

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	70 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

of a digital identity oligarchy, where authority was less centralised but remained in the hands of a limited number of authorities.

- The third phase was marked by a groundbreaking shift to a **user-centric** identity, with an individual or administrative control being exercised by multiple authorities, and a complete absence of federation elements. Based on the fundamental assumption that each individual ought to enjoy their right to control their own online identity, the Augmented Social Network (2000) suggested the creation of a ‘persistent online identity’ that had little to do with what the previous initiatives (Microsoft’s Passport and Sun Microsystem’s Liberty Alliance) represented (i.e. viewing users as mere consumers, and as such, putting all their focus on privatising and keeping the control of users’ personal information to themselves). The Identity Commons (2001) worked further on that idea by introducing the Internet Identity Workshop working group and expanded further on the idea of putting the user in the epicentre. OpenID (2005) and other endeavours such as OAuth (2010) and FIDO (2013) envisaged users obtaining more power over their identities, putting them in a position where they can exercise full and autonomous control over the latter. Unfortunately, the concept got distorted after Facebook Connect made its appearance in 2008 and profited off of the prior knowledge gained, but only to establish itself as another sole entity controlling the identity authentication of users.
- The fourth and final phase of identity is that of **self-sovereignty**, which was initiated only a bit over a decade ago, when Devon Loffreto spoke of a ‘right to an identity’ [35]. According to him, identity is a construction whose full control individuals enjoy before they become a part of the society (i.e. by registering as infants to national civil registries) and as such, lose it to national bodies who govern and administer identities. This situation being in his opinion deeply contradictory, Loffreto advocates for the return of control over identity to individuals, a concept upon which he continued to build over the years [36]. Popularity, and both public and institutional discourse has risen since, and several policies on how SSI can be addressed have been proposed (e.g. mathematical, legal [37], international [38]).

What can be concluded from the elements discussed above is that SSI constitutes the continuation of the user-centric identity in the sense that users remain the sole administrator of their identity. By drawing on previous works on the principles of identity [39], Allen has also identified **the Ten Principles of SSI** in an effort to provide the contours of a **framework in which digital identities are developed and managed**, ensuring that the user control that lies at the core of the SSI is safeguarded [40]. These principles also acknowledge and take into consideration the fact that identity is a powerful tool that can be wielded for both good and harm, meaning that any identity system management ought to strike the delicate balance between transparency, fairness and collective good, while at the same time protecting individual rights. These principles, enhanced to a certain extent, are the following:

1. **Existence:** Users must have an independent existence that goes beyond the digital realm. Self-sovereign identity must reflect and support the essential “I” that defines a person, making selected aspects of it accessible without wholly digitalising identity. Thus, this connection between the person and its digital representation must be clarified, in order to ensure that digital identities will not go as far as compromising the user’s intrinsic identity. A statement on the ethical use of digital identities could, for instance, provided sufficient safeguard against the dehumanisation of digital identities.
2. **Control:** Users should have ultimate control over their identities, backed by secure and transparent algorithms, and they should also retain the ability to reference, update, or conceal their identities as they see fit. However, there should be an acknowledgement of ‘edge cases’, where identity control might require external intervention. These cases should remain, however, exceptional and clearly defined.
3. **Access:** Users must have unrestricted access to the data associated with their identity. While users may not have control over all claims, they should always know what data exists and how it is used. Equal access does not extend to others’ data, but users should have full visibility into

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	71 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

their own. To ensure that sensitive data is not exposed, mechanisms for verifying access (e.g. zero-knowledge proofs)[41] could be introduced.

4. **Transparency:** The systems and algorithms underpinning identity networks must operate openly. Their design, management, and updates should be accessible for examination, relying on open-source and widely recognized methodologies. Beyond open-source algorithms, other accountability mechanisms should be established for administrators and contributors: an SSI system should be relying upon a governance model that supports audits and updates in a transparent manner.
5. **Persistence:** Identities should endure for as long as users desire, ideally indefinitely. While data or keys may need updating, the core identity must remain intact. This principle should align with a user's right to be forgotten, allowing identities and associated claims to be disposed of when necessary. An interesting aspect to be explored is that of aligning persistence with evolving technological standards, ensuring backward compatibility [42].
6. **Portability:** Identity data must be transferable, free from dependency on any single third-party entity. This ensures that users maintain control even if a service ceases operation or they relocate to another jurisdiction. Broadening this principle to explicitly include resilience against state-sponsored censorship or geopolitically influenced disruptions could serve well the current turbulent landscape.
7. **Interoperability:** Identities must function across various platforms and jurisdictions, facilitating global use without compromising user control. Interoperability ensures identities remain relevant and usable in diverse contexts, rendering the inextricable link to portability evident. and can be implemented through cross-jurisdictional agreements or standardised APIs. Practical models such as W3C VCs can provide a solid framework for SSI interoperability.
8. **Consent:** Users must explicitly agree to the use of their identity data, meaning their consent should be intentional and clearly understood. While others may present claims about a user, the user's consent is essential for these claims to gain validity. Consent management should also afford more layers, such as dynamic or revocable consent systems [43] offering users tools to manage their consent effortlessly.
9. **Minimalization:** Data disclosure should be limited to the minimum required for any given purpose. Advanced techniques like selective disclosure and zero-knowledge proofs can help minimise unnecessary exposure while safeguarding privacy. Differential privacy techniques could also be introduced to that end.
10. **Protection:** User rights must take precedence over network needs in cases of conflict. Decentralised, censorship-resistant, and resilient algorithms should underpin identity systems to preserve individual freedoms. Implementing 'conflict resolution' mechanisms, such as arbitration protocols, could help mitigate scenarios where decentralised networks fail to address individual grievances.

6.1.1.2 Self-Sovereign Identity (SSI) under the General Data Protection Regulation (GDPR)

The interest around the question of compatibility of the concept of the SSI with the GDPR has been growing during the past few years. On the one hand, the conceptual and definitional foundations of the GDPR were based on the idea of centralised identity models; but on the other hand, the concept of the SSI is based on decentralised architectures. This fundamental difference between the two leads inevitably to the creation of substantial tensions, which subsequently begs the question of compatibility of the GDPR with the SSI.

6.1.1.2.1 General elements

In order to approach the question in a systematised manner, it suffices to first consider the aspects where an overlap between them arises. First of all, the **material scope** of the GDPR includes solely the

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	72 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

processing of personal data [44] Even though there are various SSI uses, and therefore the way in which they process personal data can substantially differ, *credentials and their revocations* concern natural persons, so the GDPR is applicable to them [45]. As far as *private and public keys* are concerned, both the European Commission, as well as the Spanish and French Data Protection Authorities have concluded that they qualify as well as personal data [46], [47], [48]. Secondly, as SSI is based on the idea of giving full control back to the users (see above under subsection 6.1.1.1), the most obvious choice of **legal basis** for the eventual/potential processing of users' data is no other than that of *consent* [49]. Such a consideration entails proper development of SSI systems in a way that ensures that users can navigate SSI applications easily; given that consent is in a sense 'built in' these applications, makes such procedures more efficient and accurate [45].

Insofar as the question of **controllership and processorship** is concerned, again the fundamental conception of having users regain such controllership over the data may seemingly create a paradox; if users are controlling their data themselves, and since the GDPR necessitates the presence of a third, external party as controller of the data being processed, the GDPR and the SSI are then simply incompatible. The fusion of the two necessary, separate entities (i.e. controller and data subject) into one would render the GDPR inapplicable in that case. Nonetheless, it is supported that the individuals and/or legal entities which build and operate SSI in any manner whatsoever indeed qualify as controllers and/or processors under the GDPR [50], with certain exceptions such as for household uses, parents and legal custodians controlling children's identities, etc. System developers are as well exempt, but only if they do not engage in building and operating SSIs [50]. In other cases, however, it is also argued that users can qualify as controllers themselves, meaning that the GDPR applies only to processors, e.g. SSI system developers [51]. In light of the uncertainty around this question, determining the roles of actors in each case requires an *in concreto* analysis [52].

Another area of friction concerns one of the rights granted to data subjects, the 'right to be forgotten' [53]. An inherent characteristic of SSI, since most of its implementations entail the use of blockchain technologies, is the impossibility to erase entries registered on the chain [54]. Nevertheless, blockchain technologies can offer themselves a solution to this so-called GDPR-Blockchain paradox, by keeping sensitive personal data 'off-chain' and store only relevant proofs 'on-chain' [55], [56]. For instance, SSI Governance Systems such as *Sovrin* are by default prohibiting the storage of personal data on public ledgers directly [57]. However, in cases where personal data are indeed stored on the chain, then their erasure can no longer be ensured. It should be recalled that the right to be forgotten does not constitute an absolute right, meaning that if the 'available technology and the cost of its implementation' do not allow for such an erasure to take place, then alternative technical solutions can be found in order to compensate for this impossibility of the data subject's data erasure [53].

6.1.1.2.2 Conceptual differences and similarities between GDPR and SSI principles

Building upon the SSI principles as discussed above, which present similarities as well as differences with some of GDPR principles, there is some value in comparing the two in order to evaluate the SSI/GDPR compatibility on a more conceptual level [58], [59]. Given that each set of principles derives from frameworks of diverse natures (legal vs technical), inasmuch as there are significant overlaps, definitional gaps might render this compatibility exercise more complex than anticipated.

1. **Existence:** The concept of a real person is considered essential for protecting personal data belonging to individuals. Although the term isn't explicitly mentioned in the GDPR, the regulation's material scope, along with its exclusion of deceased individuals, points to a similar understanding [60]. On the contrary, the concept of identity hinges on accuracy, meaning that the personal data processed in identity management systems should truthfully reflect an individual's information. This is not the case for the GDPR, where data are protected regardless of whether they are accurate or not [61].

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	73 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

2. **Control:** Both SSI and the GDPR share the common goal of increasing individual control over personal data. Problems arise, however, when attempting to define the term, especially with regard to personal data. Control in the GDPR is linked to other concepts such as transparency and accountability, whereas as far as the SSI principles are concerned, controllership seems to be a more practical and mono-dimensional concept.
3. **Access:** the right to access are recognised under the GDPR purely focuses on the possibility of the data subject to request to the data controller access to their personal data [62]. This is not the case of access as foreseen in the SSI framework, which is including public blockchain layers, thus enabling third-party access to the data.
4. **Transparency:** In SSI, transparency is facilitated by the public and auditable nature of blockchain technology. However, under the GDPR, transparency is not meant as public but limits itself to the interaction between data controllers and data subjects.
5. **Persistence:** This principle is referred to solely in the context of the SSI principles, and not those of the GDPR.
6. **Portability:** The right to data portability is a significant feature of the GDPR, allowing individuals to transfer their personal data between controllers in a machine-readable format. SSI enhances portability with digital wallets and peer-to-peer data transfers. Nonetheless, as far as the GDPR is concerned, the right to erasure can still be invoked, creating a potential conflict with the immutable nature of blockchain ledgers, which prevents data from being deleted once registered, as also discussed above.
7. **Interoperability:** In the sense that portability also supports and strengthens interoperability, the latter is vaguely referenced to in the GDPR as an operational duty of controllers to develop interoperable formats that enable data portability [63]. It being a purely technical requirement, no tensions are identified between the GDPR and SSI perspectives at present.
8. **Consent:** Consent being one of the main legal bases for processing under the GDPR [49], there are numerous SSI management cases which do not involve the granting of consent as the legal basis for processing.
9. **Minimi(li)sation:** Data minimisation is a core principle in the GDPR [64], argued to be supported by technologies such as Decentralized Identifiers (DIDs) and digital wallets, which enable the selective disclosure of personal data by individuals. Nonetheless, given that data minimisation in the GDPR also entails the obligation for the data controller to retain data only for the period which is strictly necessary, blockchain's immutability is most probably not very well aligned with this principle. The elements presented above with regard to possible way-outs from this impasse could also be considered here.
10. **Protection:** To the degree that protection constitutes a broad term that can potentially encompass data protection, as well as data and information security, the approaches of the GDPR and the SSI seem to differ. On the one side, the GDPR requires that personal data be processed in a way that ensures appropriate security, protecting against unauthorised processing and accidental loss or damage through appropriate technical or organizational measures, as well as puts the emphasis on the availability and resilience of data processing systems. The fact, however, the GDPR is a technologically neutral legislation, when SSI is based on blockchain technologies, there are questions that arise with regard to whether the level of protection required by the GDPR can be sufficiently achieved by SSI.

6.1.1.3 TANGO SSI privacy impact assessment

On the basis of the data flow mapping of TANGO's SSI component provided in D2.3, the privacy risks that occur can be classified as follows:

- (1) **Data collection:** Inputs include personal information, DID registrations, and identity claims required for Attribute-Based Encryption (ABE) keys. Risks in this stage involve unauthorised access to sensitive data, improper handling of personal information, and excessive data

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	74 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

collection. Mitigation strategies include minimizing data collection to only essential information, enforcing explicit user consent, and ensuring data encryption both at rest and in transit.

- (2) **Data usage:** This involves the issuance, storage, and verification of VCs (VCs), the creation of proofs, and DID authentication for IoT devices. Risks include the misuse of personal data beyond its intended scope and inadequate user control over shared data. To mitigate these risks, user-friendly interfaces should be implemented to enable data control, zero-knowledge proof (ZKP) mechanisms should be used for selective disclosure, and data usage policies should be clearly defined.
- (3) **Data storage and security:** The cryptographic material and credentials stored within the SSI Wallet present risks such as credential theft, unauthorised access to the wallet, and improper lifecycle management of credentials. Mitigations include using strong encryption for wallet storage, implementing multi-factor authentication (MFA) for wallet access, and defining clear policies for credential revocation and expiration.
- (4) **Data sharing and interoperability:** Interactions involve sharing credentials with verifiers and ensuring interoperability with GAIA-X components and eIDAS frameworks. Risks here include potential data exposure during transmission and interoperability issues that may lead to privacy breaches. Mitigation measures include the use of secure transmission protocols like HTTPS and DIDCOMM, enforcing strict compliance with relevant standards (e.g., W3C, OpenID), and monitoring and auditing data-sharing processes.
- (5) **IoT Device Integration:** This process involves DID authentication for verifying device identity and managing access tokens. Risks include the compromise of IoT device credentials and unauthorised access to IoT services. Mitigations for these risks could potentially involve robust DID onboarding procedures, the use of token expiration mechanisms, and monitoring IoT authentication events for anomalies.

The threat landscape as described in D2.3 involves dependencies on connectivity of users, vulnerabilities of the end-user device, granular disclosure and data aggregation, and quantum computing attacks. These threats, however, being described in a vague manner, and thus not being inherent or tied to a specific element of the SSI technology developed in TANGO, possible mitigation measures, per threat, could include:

- **Connectivity risks:** Decentralised redundancy, offline functionality, load balancing and resilient communication protocols (e.g. DTLS).
- **End-user device security:** Regular updates and patches, behavioural anomaly detection.
- **Data aggregation:** advanced ZKP, time-bound credentials, dynamic data mapping.
- **Quantum threats:** hybrid cryptography, continuous cryptographic assessments.

6.1.1.4 General recommendations and action points for data protection compliance based on GDPR's principles

To ensure **GDPR compliance** for TANGO's **Self-Sovereign Identity (SSI) Solution** as discussed above, several legal recommendations can be made based on the GDPR's principles and the specific functionalities of the SSI technology itself. These recommendations are largely based on the analysis provided under the previous sub-sections on SSI and are based on a holistic assessment of TANGO's SSI component.

Purpose limitation (Art. 5(1)(b) GDPR)

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	75 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

- Define and restrict the purposes for which personal data, especially identity data, is processed in the SSI ecosystem. The SSI system should clearly specify the purposes of using VCs (VCs) and should not use personal data for other incompatible purposes.

Data minimisation (Art. 5(1)(c) GDPR)

- Ensure that **selective disclosure** is implemented as a core feature, where individuals share only the minimum necessary personal data required for a specific transaction or use case. This can be for instance achieved via the ZKP implementation. Other granular disclosure methods, e.g. binary disclosures, selective data fingerprinting, and tracking can also be implemented for the same purposes.

Storage limitation and data retention (Art. 5 (1)(e) GDPR)

- Define retention policies for behavioural and sensor data, ensuring data is not stored longer than necessary for its authentication purposes.
- Automate data deletion processes after defined periods or when users terminate their accounts.

Lawful basis for processing (Art. 6 GDPR)

- Determine the appropriate **lawful basis** for processing personal data in the SSI solution. While **consent** is often relied upon, there may be other lawful bases, such as **contractual necessity** or **legitimate interests**, depending on the context in which the data is used.
- Ensure that users provide **explicit consent** before issuing or sharing VCs, particularly when sensitive data (e.g., health, biometric data) is involved. This is especially pertinent for the User Continuous Behavioural Authentication component.
- Implement mechanisms that allow users to easily **withdraw consent** at any time.

Transparency and User Information (Art. 12-14 GDPR)

- Provide clear, concise, and easily accessible information to users about how their personal data is processed within the SSI solution. This includes informing users about the **issuers**, **verifiers**, and any other entities involved in processing their data.

How? Develop a **user-friendly privacy notice** that explains the functioning of the SSI system, detailing what personal data is collected, the purpose of processing, how it will be shared, and the rights of users under the GDPR.

Data subject rights (Art. 15-22 GDPR)

Ensure that the SSI solution supports the full suite of **data subject rights**, including the right to access, rectification, erasure (right to be forgotten), restriction of processing, and data portability.

How? Design the SSI wallet and the agent systems to allow users to easily exercise these rights, such as:

- Enable **easy access to personal data** stored in VCs and allow users to correct or update their data.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	76 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

- Offer mechanisms for users to request **erasure** or **restriction** of their data from the system, ensuring that the data can be effectively **deleted** or anonymised upon request.
- Implement a **data portability feature** that allows users to export their VCs in a commonly used machine-readable format.

Third-party data processors and data sharing (Art. 28 GDPR)

- When integrating with third parties (e.g., Verifiers, Issuers, or other service providers), ensure that appropriate **data processing agreements (DPAs)** are in place to ensure that third-party processors comply with the GDPR's requirements.

6.1.2 Seamless Onboarding for Users and Devices (SOUD) [T4.2]

6.1.2.1 SSI and the eIDAS Regulation

Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (**eIDAS Regulation**) [65] establishes a framework aiming at creating a secure, efficient, and fast environment for electronic transactions across European Union countries. It was initially introduced in response to the fragmented development of electronic identity systems by individual countries, which lacked interoperability. eIDAS addresses two significant issues in the European digital landscape: enabling EU citizens to use their electronic identification across Member States and ensuring enforceable laws for trust services.

On the basis of eIDAS, a **legal framework for various trust services** is created, including electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, and qualified certificates for website authentication. While each EU Member State defines the legal value and governing laws for these trust services, eIDAS allows Member States to introduce additional services to the framework. This ensures trust service providers can market their products within a legally safeguarded ecosystem, fostering greater security. However, it also imposes legal responsibility on providers to maintain the quality and reliability of their services [66].

eIDAS does not aim at creating a unified EU identity for users but instead focuses on interoperability among Member States' identity systems. Given the variations in privacy and security standards across Member States, a **Level of Assurance (LoA)** system was developed. The LoA includes three tiers – low, substantial, and high – that represent the confidence level in verifying a user's identity [67].

The weak point of eIDAS was, however, electronic identification. **With the aim of integrating decentralisation and SSI**, eIDAS was amended and updated with **Regulation (EU) 2024/1183 (eIDAS 2.0)** [68], whose most noteworthy innovation is the European Digital Identity Wallet (EDWI) which enables users to securely store, manage and present their credentials both online and off-line, and in cross-border cases [69].

DID owners can present claims about themselves, but the trustworthiness of VCs for a verifier depends on the credibility of the issuer. The issue lies in the DID solely identifying the issuer, and the trust problems around it. In that light, eIDAS presents itself precisely as the legislative framework needed to enhance the reliability and trustworthiness of VCs. In an effort to promote eIDAS as a trust framework for the SSI ecosystem, the European Commission has developed the **SSI eIDAS bridge**, which provides assistance VC issuers in the signing process, as well as verifiers with the automation of the identification of the of the organisation behind the issuers' DID. In other words, by 'crossing' the eIDAS Bridge, the trustworthiness of a VC can be in the whole of the EU [70].

With respect to the ways in which the SSI principles can be embodied in eIDAS 2.0, Schwalm & Allamilo-Domingo are supporting the following [71]:

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	77 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Representation	Notified eID Scheme and EU Digital Wallet
Interoperability	Certified EU-Digital Wallet, conformity assessed QTSP and notified eID as well as eIDAS nodes. Common European standards referenced by implementing acts.
Decentralisation	EU-Digital Wallet and proven issuer as well as relying parties
Control and Agency	EU-Digital wallet, proven issuer and relying party
Participation	Only obligations for acceptance no obligation to use the wallet nor the identities
Equity and Inclusion	Equal regulation for whole EU and EFTA
Useability, Accessibility and Consistency	Certified EU-Digital Wallet and qualified trust service providers based on common European standards proved by accredited CAB.
Portability	Any identities or attestation from EU Digital Wallet can be moved. Details defined in European standards.
Security	State-of the art security requirements defined in common European standards which will be mentioned by implementing acts. Proved by CAB during certification of wallet, relying party or conformity assessment of QTSP. Trust provable via Trust List.
Verifiability and authenticity	Verifiability and authenticity of attestations, signatures, seal, timestamps provable via (qualified) validation services, attestation services etc.
Privacy and minimal disclosure	Ensured by EU Digital wallet and the fact that only holder decides which information he'll provide but due to fact that relying parties are approved, the holder can really be sure to whom they'll provide which information. Selective Disclosure and Zero Knowledge Proof included.
Transparency	European wide regulation with common and via implementing acts mandatory European standards which are basement for notification of eID-schemes, certification of EU-Digital wallet, relying parties, QTSP and all notifications and certification/successful conformity assessment published.

Figure 12. SSI and eIDAS compatibility (Schwalm & Allamilo-Domingo, 2021)

Both the development of eIDAS 2.0 and the rise of SSI are both important milestones in the evolution of digital identity. These initiatives aim to enhance privacy and security, empower individuals, and facilitate seamless cross-border exchange of digital services. The combination of the two can undoubtedly create exciting opportunities and synergies with the aim of building a truly user-centric, secure, and inclusive digital identity ecosystem. While challenges remain, especially around regulation,

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	78 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

standardisation, and widespread adoption, the potential benefits are enormous. In a forward-looking spirit, eIDAS 2.0 and SSIs will transform the digital landscape and have a profound impact on how we navigate and trust the digital world.

6.1.2.2 eIDAS and the General Data Protection Regulation (GDPR)

Concerns were voiced around the initial text of the Proposal for eIDAS 2.0 [72], especially with regard to its Article 11 which included a provision on the establishment of a ‘unique and persistent identifier’, which would be used also for the addition of electronic attestations of attributes to the EDWI. The EDPS in its formal comments addressed the matter by raising the issue of constitutionality of such a provision, by pointing out that in some countries, unique identifiers are seen as ‘a violation of human dignity’, and as such, are characterised as unconstitutional [73]. Such countries include Portugal and Germany; the General Constitutional Court has found that a general personal identification number for all public services that makes it possible to ‘register and catalogue the individual citizen in his or her entire personality’ is contrary to the Constitution [74]. Moreover, suggestions for the implementation of the privacy by design principle were made by the ITRE Committee which highlighted the need for an impossibility of the issuers of the EDIW to track the use of the latter and advocated for the use of zero-knowledge proof (ZKP) approach [75].

Fortunately, the EU legislator considered the criticism expressed and incorporated GDPR considerations across the whole of eIDAS, which can be presented as follows:

- **General data protection principles (Art. 2(4)):** It is emphasised that eIDAS operates without prejudice to the GDPR ensuring that personal data processing complies with established data protection laws.
- **Data minimisation and purpose limitation (Art. 5(14)):** Providers of EDWI must not collect or combine personal data beyond what is necessary for their services, ensuring logical separation from other data.
- **User control over personal data (Art. 5(14)):** Users have full control over their personal data within the European Digital Identity Wallet, including tracking data usage and requesting immediate erasure of data shared with third parties
- **Voluntary use and privacy-preserving techniques (Art. 5(15–16) and Rec. 14):** The use of wallets must be voluntary, and privacy-preserving techniques like unlinkability (e.g., avoiding linkable data) and ZKP must be implemented.
- **Security breach and incident reporting (Art. 5e):** In the event of a security breach affecting wallets, Member States must promptly notify users and take corrective action. Providers are also required to suspend or revoke compromised wallets.
- **Cross-border identity matching (Art. 11a):** Identity matching must include high-level safeguards to protect personal data and prevent profiling.
- **Interoperability and data protection by design (Art. 12):** The interoperability framework is required to implement privacy and security by design, ensuring the minimal collection and use of personal data.
- **Certification and cybersecurity (Art. 26–27):** The regulation mandates that wallets undergo certification for compliance with cybersecurity and data protection standards, involving cooperation with data protection authorities.
- **Electronic attestation of attributes (Art. 45h):** Providers of attribute attestation services must keep personal data logically separate from other services and avoid combining it with unrelated data.
- **Selective disclosure (Art. 59):** Wallets must allow users to disclose only necessary attributes, supporting the principle of data minimisation.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	79 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

6.1.2.3 TANGO SOUD privacy impact assessment

The two main threats and attacks against which TANGO's SOUD is vulnerable to are fake identity document threats and presentation attack threats.

Firstly, TANGO's SOUD currently employs several mitigation strategies to protect against fake identity documents, such as **comparing MRZ data, OCR-extracted information, and NFC chip data**, a multi-step verification which processes cross-references various pieces of data to validate the authenticity of the identity document, and a **three-step verification process**, where the system follows a verification procedure in line with eIDAS, ensuring that multiple checks are performed to confirm the document's legitimacy.

While these measures are robust and provide a high level of assurance, potential vulnerabilities could arise if **NFC chips are compromised** to insert fraudulent data, or **OCR processes fail** to detect subtle manipulations in document text or images. For these reasons, additional mitigation strategies could be adopted, such as:

- (1) **Document forensics:** Incorporating advanced AI-powered forensics can help detect subtle alterations in document materials, such as tampered holograms, watermarks, or microtext. This would add another layer of security to the document verification process.
- (2) **Database validation:** Cross-checking the data extracted from the identity document with trusted government or international databases can further verify the document's authenticity. This ensures that the presented identity is legitimate and registered in a recognized database.
- (3) **NFC integrity checks:** To enhance the security of NFC data, a checksum or hash validation step can be implemented. This ensures that the NFC chip data has not been tampered with, adding an additional layer of protection against compromised chips.

Secondly, with regard to presentation attack threats, TANGO'S SOUD solution currently uses **liveness detection** to prevent various presentation attacks, such as those using photos, videos, 2D masks, and 3D masks. This technique ensures that the person being verified is physically present and is not trying to spoof the system with pre-recorded or artificial biometric data. While liveness detection is an essential defence, attackers may increasingly employ sophisticated techniques such as ultra-realistic **deep-fakes** or **hybrid attacks**, where legitimate documents are combined with fake biometric data. These emerging threats could potentially bypass current liveness detection systems.

- (1) **Behavioural biometrics:** Analysing behavioural patterns, such as blinking frequency, micro expressions, or head movements, can make it much harder for attackers to replicate the behaviours of a real person. These traits are difficult to simulate in deep-fakes and add an additional layer of verification.
- (2) **Multi-modal biometrics:** Combining **face recognition** with other biometric modalities, such as **voice** or **fingerprint recognition**, would further strengthen the verification process. Even if facial recognition is bypassed by a presentation attack, other biometric modalities can help confirm the user's identity.
- (3) **Environmental context checks:** AI can be used to detect **inconsistencies in the environment**, such as mismatched lighting or unusual background elements, which might suggest that the biometric data is being spoofed. This could provide an additional level of protection against fake biometrics.
- (4) **Continuous authentication:** For extended verification scenarios, such as ongoing sessions, **periodically re-checking liveness** ensures that the person being authenticated remains the same throughout the session. This continuous check can prevent the system from being tricked by a spoofed biometric during initial authentication.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	80 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

6.1.2.4 General recommendations and actions for data protection compliance based on eIDAS and GDPR's principles

With regard to the GDPR, the following general recommendations can be given for a GDPR compliant SOUD:

Data minimisation (Art. 5(1)(c) GDPR)

- Only collect the minimum amount of data necessary for the on-boarding process and creation of VCs. Avoid collecting excessive or unnecessary information.
- Regularly review and update the data collection procedures to ensure they align with the principle of data minimization.

Lawful basis for processing (Art. 6 GDPR)

- Obtain explicit consent from users for the collection and processing of their personal data, including biometric data. Ensure that consent is clear, unambiguous, and given freely.
- Provide users with the option to withdraw consent at any time and ensure that the process to do so is simple and accessible.

Transparency and User Information (Art. 12-14 GDPR)

- Provide users with clear, concise, and transparent privacy notices that inform them of their data collection, usage, processing purposes, and retention periods. The privacy policy should also explain their rights under GDPR.
- Make it clear how biometric data and identity documents are processed, stored, and shared with third parties (such as service providers).

Data subject rights (Art. 15-22 GDPR)

- Implement mechanisms that allow users to exercise their rights under GDPR, including the right to access, rectification, erasure, data portability, and objection to processing.
- Users should be able to request to delete or modify their personal data stored within the system, and these requests should be processed within the statutory time frame (typically within 30 days).

As far as eIDAS 2.0 is concerned, the following recommendations can be made:

Support for European Digital Identity (EUDI)

- Ensure the Onboard SSI solution is compatible with the European Digital Identity Wallet introduced under eIDAS 2.0.
- Implement protocols that allow the Onboard SSI platform to generate, store, and manage VCs (VCs) that are compliant with the European Digital Identity standards.
- The system should support the EUDI format, ensuring that identity data can be accessed and shared across EU member states securely and efficiently.

How?

- Use DID (Decentralized Identifiers) and VCs (VCs) to support cross-border authentication and credential sharing across EU member states.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	81 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

- Implement the capability for users to import/export their EUDI credentials seamlessly into and out of the Onboard SSI system.

Enhanced User Control and Consent

- Comply with the increased emphasis on user control and explicit consent introduced under eIDAS 2.0.
- Ensure that users are fully informed about the data collected and how it will be used, allowing them to provide granular consent for different aspects of the identity verification process.

How?

- Implement a user-friendly interface where users can manage their consents, including granular control over biometric data and identity attributes they share for each transaction or service request.
- Ensure the system adheres to principles of data minimization, where only the essential data needed for identity verification is collected and used, in line with GDPR principles.

Cross-Border Interoperability

- Ensure that VCs (VCs) issued by the Onboard SSI solution are recognised and accepted across all EU Member States.
- The platform should facilitate seamless authentication using the EUDI across different services in various EU countries, enabling cross-border transactions and access to services.

How?

- Establish integration points for the Onboard SSI platform to communicate with national eID systems to verify identity credentials.
- Implement standardised protocols (e.g., DIDComm, W3C VCs) that can be accepted across EU Member States, ensuring consistent and secure identity verification processes.

Privacy and data protection enhancements

- Strengthen data protection mechanisms in the Onboard SSI platform to meet the stricter privacy standards, particularly around biometric data and VCs.
- Ensure compliance with GDPR while also taking into account the new privacy measures introduced in eIDAS 2.0 that give users more control over their digital identity.

How?

- Use zero-knowledge proof (ZKP) mechanisms to allow users to prove their identity without exposing unnecessary personal data (e.g., only showing the age rather than the birthdate).
- Encrypt biometric data and personal attributes both in transit and at rest. Ensure that users can revoke or update their data securely in the system.
- Provide users with the ability to delete or anonymize their identity data if they choose not to use the service further, in line with GDPR's right to erasure.

Secure storage and management of digital identity data

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	82 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

- Ensure that digital identity data, including VCs and biometric data, are stored in a highly secure manner that adheres to the eIDAS 2.0 requirements.
- Leverage secure methods for storing and accessing user credentials, particularly for data that is used for authentication and digital signature purposes.

How?

- Store data in secure cloud environments with strong access controls, ensuring only authorized entities can access identity information.
- Use hardware-based security modules (HSMs) for key management and encryption of sensitive data like biometric templates and NFC chip data.

Ongoing User Authentication and Session Management

- Implement mechanisms for continuous authentication throughout the user's session. This may be necessary for applications that require high assurance during interactions with service providers.

How?

- Utilise techniques such as behavioural biometrics or session re-authentication at intervals to confirm the user's identity during the course of the interaction.
- Ensure that users have a clear process for session termination, allowing them to log out and revoke any active session tokens that might give unauthorised access.

Dispute Resolution and User Rights

- Provide a mechanism for users to dispute and correct any identity data that may have been incorrectly verified or recorded, aligning with eIDAS 2.0's data accuracy provisions and GDPR's right to rectification.

How?

- Implement an appeals process where users can challenge decisions made based on their digital identity verification, such as denials of access to services or transactions.
- Offer easy-to-use tools for users to update their digital identity and request corrections where applicable.

6.1.3 User Continuous Behavioural Authentication (UCBA) [T4.3]

6.1.3.1 User Continuous Behavioural Authentication under the General Data Protection Regulation (GDPR)

The rise of continuous authentication and behavioural biometrics as a solution to the limitations that come with traditional authentication measures is tied to the increasing presence and evolution of all the more sophisticated cybersecurity threats [76]. Their capability to identify irregularities and adjust security measures according to the assessed risk, their potential to transform user authentication and access management is high. Behavioural biometrics, such as keystroke patterns, mouse activity, and touchscreen interactions, enable the creation of unique digital profiles for users, significantly improving the precision and resilience of the authentication process. The benefits that accompany UCBA are numerous, including improved privacy and user-friendlier experience.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	83 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Nonetheless, from the perspective of privacy and data protection, UCBA also comes with considerable risks [77]. The use of biometric data in authentication systems, data which fall under the category of sensitive data of Art.9 GDPR, presents several risks and challenges. Controllers may **misuse stored biometric data for unauthorised purposes**, such as unlawfully tracking employees, enforcing disciplinary actions, or creating detailed user profiles. Additionally, the **amount of data collected could be excessive in relation to its purpose**, violating the principle of data minimisation. Continuous biometric monitoring may also create a **chilling effect**, as users could feel apprehensive about being tracked or profiled, discouraging them from engaging with such systems. A **lack of transparency** is another concern, with organizations sometimes failing to inform individuals that their biometric data is being captured and used to train artificial intelligence algorithms, often without valid legal justification. Furthermore, algorithmic inaccuracies can lead to issues like false positives or unjust denial of access to services, especially as systems adapt to changes in user behaviour. Lastly, users have **limited control over when and how this technology is applied**, and any data breaches involving biometric information can have significant impacts, as biometric traits, unlike passwords, unfortunately cannot be changed.

6.1.3.2 TANGO UCBA privacy impact assessment

On the basis of the data flow mapping of TANGO's SSI component provided in D2.3, the privacy risks that occur can be classified as follows:

- (1) **Data collection:** TANGO's UCBA collects a range of sensitive behavioural and biometric data. Risks in this stage include unauthorised access, profiling, or excessive data collection beyond authentication needs. To mitigate these concerns, data minimisation practices could be employed, ensuring only necessary data is collected. Transparency could be furthermore maintained through clear privacy policies, and explicit user consent being required before data collection begins. Thanks to on-device preprocessing, the transfer of data to the cloud can also be limited, reducing exposure.
- (2) **Data usage:** The primary use of collected data is for continuous authentication. However, there is a risk of inappropriate secondary uses or misuse of the data. To address this, strict usage policies that restrict data processing solely to authentication purposes should be enforced. Secure AI algorithms are used for data processing, and users are provided with tools to control and review how their data is utilized.
- (3) **Data storage and security:** Storing sensitive behavioural and biometric data presents challenges such as theft, unauthorised access, or long-term storage leading to profiling risks. To safeguard against these risks, data encryption for both data at rest and in transit can be employed. Regular audits could also be conducted to ensure cloud storage security and access controls are robust. Data retention policies should be also implemented in order to automatically delete data after its intended use is fulfilled.
- (4) **Data sharing and interoperability:** TANGO's UCBA interacts with components like the TANGO Wallet and other privacy-focused modules. Risks associated with these interactions include potential data leakage during sharing and vulnerabilities arising from interoperability issues. These risks can be mitigated through the use of secure data-sharing protocols like HTTPS and secure SDK communication. Compliance with relevant standards should as well be enforced to ensure seamless and secure integration.
- (5) **Continuous monitoring and behavioural Analysis:** While continuous monitoring enhances security, it may lead to user discomfort or perceptions of surveillance. Additionally, AI-based behavioural analysis could result in false positives or negatives. To address these concerns, TANGO'S UCBA users should be given the option to opt in or out of continuous monitoring. Authentication results, such as confidence levels, need also to be shared transparently with users. Regular validation and refinement of the AI algorithms is necessary to ensure fairness and accuracy.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	84 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

- (6) **Biometric and behavioural data fusion:** Combining biometric and behavioural data in TANGO's UCBA component increases the sensitivity of the information collected and heightens risks if these datasets are compromised. Such risks can be mitigated by isolating the datasets and using robust encryption to secure them.

Additionally, the **threats** described in D2.3 include impersonation, replay, evasion and model poisoning attacks, which are mitigated by specific threat detection mechanisms that allow filtering and validation at various stages of the inference process. Nonetheless, additional protective mechanisms

- (1) **Tamper Detection:** Implement runtime application self-protection (RASP) to monitor and defend against tampering or exploitation in real time.
- (2) **Hardware Security:** Ensuring that the device is not tampered with could be achieved through the use hardware-backed keys and secure elements to protect sensitive computations and data storage.

6.1.3.3 General recommendations and action points for data protection compliance based on GDPR's principles

To ensure **GDPR compliance** for TANGO's **User Continuous Behavioural Authentication** as discussed above, several legal recommendations can be made based on the GDPR's principles and the specific functionalities of the UCBA technology itself. These recommendations are largely based on the analysis provided under the previous sub-sections on UCBA and are based on a holistic assessment of TANGO's UCBA component.

Purpose limitation (Art. 5(1)(b) GDPR)

- Clearly **define and restrict the purposes for processing** behavioural and sensor data. Specify that UCBA data is solely used for continuous authentication and risk assessment, avoiding any secondary use of data for unrelated purposes.
- Establish clear policies preventing the use of collected data for unauthorised purposes, such as profiling beyond the scope of authentication.

Data minimisation (Art. 5(1)(c) GDPR)

- Limit the collection of data to what is strictly necessary for the UCBA system to function effectively. For example, **prioritise collecting high-value data points** (e.g., swipe gestures, typing patterns) over redundant or peripheral data inputs.
- Implement **on-device preprocessing** (e.g., within the Inference Module) to minimise the transmission of raw data to the cloud.

Accuracy and Fairness (Art. 5 (1)(d) GDPR)

- Monitor and enhance the accuracy of algorithms to **reduce false positives or negatives** in user authentication.
- Ensure that behavioural changes, such as those caused by disabilities or temporary impairments, do not unfairly affect the user's access.
- **Regularly test and validate the Inference Module** to mitigate biases in user classification (e.g., legitimate, imposter).

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	85 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Storage limitation and data retention (Art. 5 (1)(e) GDPR)

- Define retention policies for behavioural and sensor data, ensuring data is not stored longer than necessary for its authentication purposes.
- Automate data deletion processes after defined periods or when users terminate their accounts.

Lawful basis for processing (Art. 6 GDPR)

- Determine the appropriate **lawful basis** for processing personal data in the SSI solution. While **consent** is often relied upon, there may be other lawful bases, such as **contractual necessity** or **legitimate interests**, depending on the context in which the data is used.
- Ensure that users provide **explicit consent** before issuing or sharing VCs, particularly when sensitive data (e.g., health, biometric data) are involved. This is especially pertinent for the User Continuous Behavioural Authentication component.
- Implement mechanisms that allow users to easily **withdraw consent** at any time.

Transparency and User Information (Art. 12-14 GDPR)

Provide clear, concise, and easily accessible information to users about how UCBA processes data, including the types of data collected, processing purposes, and entities involved.

How?

Develop a **user-friendly privacy notice** that explains the functioning of the SSI system, detailing what personal data is collected, the purpose of processing, how it will be shared, and the rights of users under the GDPR.

Data subject rights (Art. 15-22 GDPR)

Ensure that the UCBA solution supports the full suite of **data subject rights**, including the right to access, rectification, erasure (right to be forgotten), restriction of processing, and data portability.

Third-party data processors and data sharing (Art. 28 GDPR)

Establish Data Processing Agreements (DPAs) with third parties, such as service providers integrated via the Communication or Integration Module. These agreements should ensure that all processors comply with GDPR requirements.

6.2 Ethical assessment of the TANGO technology

Ethical compliance is considered a matter of outmost importance in the TANGO project in order to ensure that the developed framework is based on activities and procedures during which paramount ethical considerations were respected.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	86 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

6.2.1 Human participation

6.2.1.1 Participation procedures

In this subsection, we will refer to the measures implemented, and the procedures being followed in order to ensure compliance with the ethical considerations related to the participation of people, especially third parties, in the project related activities. This refers both to the procedures related to their actual participation in the project related activities and consequential aspects, such as the processing of their personal data.

As a starting point, in terms of the pilots to which people will be participating to test and evaluate the function of the TANGO framework, inclusion criteria have been defined. Through the designed pilots and the TANGO action overall, some initial suggestions have been made regarding the economic sectors that could be benefited, through the use of the TANGO framework and as a result, the people participating in the pilots shall be relevant to those sectors. As a result, it was decided that people working in the partner in charge of the relevant pilot will be participating, thus ensuring that the developed framework will be evaluated by a stakeholder in the relevant field. On the other hand, in the case of the smart hospitality pilot, the testing phase will be taking place in the premises of the pilot leader during the next general assembly, organized by them, and the people participating will be the project partners' representatives that will be attending the meeting. This decision ensures that people with relevant experience will be able to evaluate the TANGO framework, provide the necessary feedback and thus ensure its adequacy.

Furthermore, it is ensured that the participation of the people in the pilots is voluntary and does not cause any harm or additional psychological burden to the participants. Although in most of the cases the participants are employees of the project partner's, the latter ensure that none of the participants is forced to participate but rather they operate in the way they normally do during their day-to-day activities. The ethics advisor of the TANGO project has also conducted a plan to monitor the pilot activities and identify any potential deviations from this element, through anonymous questionnaires that will be provided to the participants in order for their latter, amongst the rest of the matters, to evaluate their experience during the course of the pilots. The participants will also become aware of their possibility to terminate their participation whenever they wish to, freely and out of charge.

Their participation will be based on their consent, provided by each participant before the start of any piloting activities. Their consent will be provided through a written form, in which information will be provided to them regarding the TANGO project and the developed framework, the level and the reason of their participation and of course the fact that they could withdraw from their provided consent on any instance freely and without additional effort. Their consent will be provided in a distinguishable way to the consent provided for the processing of their personal data for any misunderstandings to be avoided and to ensure accountability.

Moreover, no discrimination or in any way exclusion of any people will be taking place as a result of their gender, race or origin is taking place. The selection of people is strictly related to their expertise on their respective field and their position in the respective partner or participating stakeholder. Vulnerable people, such as patients or people under 18 years of age, will be excluded since their participation is not required and may cause additional ethical and legal risks. As important factors, during the ethical monitoring of the pilots, targeted questions, related to this matter, will be also included in the questionnaires referred above.

6.2.1.2 Processing of personal data

In terms of the processing of personal data during the course of the pilots, it should be highlighted that overall, the project partners have implemented the necessary procedures and measures to ensure lawful processing and data security and integrity. It is envisaged that in some of the pilots synthetic or

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	87 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

anonymized data will be processed, thus ensuring that there will be no processing operations on personal data, while in the rest of the pilots personal and work-related information will be mostly collected and processed, for the purpose of organization of the actual piloting activities and the evaluation of the TANGO framework.

In terms of the legal basis for the processing of personal data, the provision of prior consent is considered suitable. The participants, through the consent process referred to in the previous subsection, will also provide their consent to the processing of their personal data, prior to the start of any piloting activities. Both documents will be provided in a language understandable to the users (preferably, their native language). This consent is based in articles 6 par. 1a and 7 of the GDPR and the participants will be informed regarding the purpose of the processing, the categories of personal data that will be processed and the processing operations, their data protection related rights and how to exercise them, the period of storage, the details of the data controllers and any potential data processor that will be in charge of the processing operations and their ability to withdraw from their provided consent at any time. The partners ensure that this consent will be also provided freely, while additional information will be provided to the data subjects – participants whenever requested.

Both the consent mentioned in this section and the consent related to the actual participation of people in the pilots, will be provided as a first step on the TANGO platform. The latter is developed in this way in order to ensure that the users will be able to use the platform only following the prior provision of their consent. Additional consent will be asked in order for specific components of the TANGO platform to be used, in order to ensure that through this process, the users obtain the necessary information at any time regarding the processing of their personal data. A privacy policy will be also conducted in order to help the users gather the necessary information. Overall, the project partners in charge of each pilot will provide the necessary information to the data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language that they could understand (though the use of their native language or English).

The consent forms and the personal data of the participants will be stored in each pilot leader premises. Each pilot leader will have access only to the personal data of the data subjects participating in their pilot. Data transfers will not take place between the partners directly but only through the use of the TANGO platform, in case it is needed as a result of its function. Those transfers will be relevant to the purpose of the processing operations and the data subjects will be thoroughly informed regarding them, through the consent provision process. Following the end of each pilot activity, the respective partner will be in charge of deleting the personal data, in order to comply to the principle of purpose limitation and the right of erasure, foreseen in the GDPR.

In this point though, a specific reference shall be done to the RIAS pilot. Following the conduction of the pilot's plan, potential issues have arisen since it is envisaged that though the use of the TANGO framework, the participants position in the RIAS premises will be monitored. This of course raises both ethical and privacy related issues since it may result to a direct violation of the participants' privacy and as a result, the purpose of the processing operations has been assessed, in relevance to the respect of the data subjects' rights.

Following the collection of information from partner RIAS regarding this pilot, we managed to identify that:

- i. The people participating in the pilot will be executive officers or managers of the several departments of RIAS. The actual number of those people is close to 10 (not over 10 in total), depending on the people that will eventually participate.
- ii. Through the pilot, there will be no GPS data collection, and the actual positioning of the people will be unknown to them. There will be only an indicator of the area that they will be in the premises of the entity.
- iii. This pilot will be taking place only during work hours and of course, inside the RIAS premises.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	88 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

- iv. The participants will be providing their consent for participation and processing of their data freely and without any pressure by the RIAS representatives.
- v. The purpose of this action is the protection of RIAS intellectual property, as a result of some incidents that occurred in the past.

Furthermore, as an additional measure, the Ethics Advisor of the project (DBC) will interact with the participants through questionnaires before, during and after the pilot activities commence, in order to collect information regarding their experience. The information will be provided anonymously by the participants as a default (they could provide their personal information if they wish) and in case an issue arises regarding the human participation procedures, the pilot will be interrupted.

6.2.2 AI ethical requirements

The European Commission formed the "High-Level Expert Group on Artificial Intelligence" (HLEG-AI), which issued in 2019 the "Ethics Guidelines for Trustworthy AI" (High-Level Expert Group on Artificial Intelligence, 2019). These guidelines set out a framework that presents the EU's strategy for achieving trustworthy AI systems. It is stated that a trustworthy AI system shall follow the following rules:

- I. It should be lawful, complying with all applicable laws and regulations. Several legally binding rules at both European and national level already apply or are relevant to the development, deployment and use of AI systems, most crucially in the European level the AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024).
- II. It should be ethical, ensuring adherence to ethical principles and values, most crucially respect for human autonomy, prevention harm, fairness and explicability.
- III. It should be robust both from a technical and social perspective. The improvement of many different aspects of human's life should be faced with a parallel awareness of the possible unintentional harm that those systems may cause. Robustness, security, and reliability should be ensured as well as safeguards should be foreseen to prevent any unintended adverse impacts. These requirements must be ensured both from a technical as well as a social perspective.

Following the aforementioned rules, the following "ethical elements" have been considered appropriate and shall be investigated during an ethical assessment of the development and use of an AI system, in order to ensure ethical compliance:

- i. Human agency and oversight
- ii. Technical robustness and safety
- iii. Privacy and data governance
- iv. Transparency
- v. Diversity, non-discrimination, and fairness
- vi. Societal and environmental wellbeing
- vii. Accountability

6.2.2.1 Ethics and AI in TANGO

The development of components that utilize the AI technology is foreseen in the WP5 activities of the TANGO project. For the purposes of this assessment, we will proceed to references to the overall aforementioned components in order to highlight their adherence to the ethical considerations and the way compliance is achieved in terms of the overall TANGO framework.

6.2.2.1.1 Exploratory Data Analysis Engine [T5.1]

The Exploratory Data Analysis Engine (EDAE) has developed a series of services to provide in a dynamic manner results for the end users and ensure the quality of the data to be used by other TANGO components. Furthermore, EDAE has also developed a series of reports regarding transactions, sales

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	89 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

volume, profitability, customer segmentation, customer preferences, popular products, shops profitability, sales, store popularity etc.

This component acts as a tool which adheres to the technical robustness and transparency components of the aforementioned assessment. It operates as a tool that for starters “filters” and assesses the quality of the data on a preliminary basis. This data is expected to be used by other TANGO components both for operational and implementation purposes. This ensures that any data that will be utilized will be correct, accurate and the relevant for the purposes of provision of the TANGO services, thus avoiding mistakes, misuse, or overall failure of the TANGO framework.

The use of accurate data both for the purposes of implementation and overall utilization of the services provided by the TANGO platform also guarantees the development of technically robust and safe AI system. This limits the possibility of critical, adversarial or damaging consequences and strengthens the procedure of evaluation of the data to be used both in terms of training and in terms of operation of the AI system.

6.2.2.1.2 Energy efficient AI model training [T5.2]

As a result of this task, 3 components will be developed, the Federated Learning (FL) support, the MLOps support component and the AutoML component. As an overview, these components adhere mostly to the “Privacy and Data governance”, the “Technical Robustness and Safety”, the “Transparency” and the “Environmental well-being” requirements of the assessment list.

The use of the Federated Learning Model on the development of an AI system offers the option to avoid the transfer of the datasets that will be utilized for training purposes. The limitation of data transfers ensures that personal data will not be further processed, thus adhering to the purpose limitation principle of the GDPR. This ensures the protection and proper exercise of the data subjects’ rights since the data will be stored only in the premises of the data controller who initially collected them, thus ensuring clarity. The data controller will be also able to maintain its control on the data and ensure lawfulness of the processing operations, depending on the internal policies adopted by their entity and as a result, they will be able to respond to any of the data subjects’ demands related to their rights, in compliance with the principle of accountability.

Data security and integrity will be also ensured, since less processing operations result to less potential risks, especially in the field of data transfers, a processing operation that is quite demanding. Data transfers, according to the GDPR, require additional measures and procedures to be followed beforehand, regarding which there is always the threat of non-compliance of any of the involved data controllers or processors. There is always also the threat of data breach events occurring as a result of the implementation of inadequate technical or organizational measures in terms of security, granting of unauthorised access during the transfer procedure etc.

As a result, in terms of privacy, this component strengthens the protection of personal data, ensures privacy and overall offers a tool to the data controllers to ensure proper data governance. Additionally, as a security measures, access to the data is provided through the protection of the HTTP protocol, which ensures secure data transfers and the prohibition of any unauthorised access to the data.

Furthermore, through the MLOps component, technical robustness is supported. Through this component, a developer or data scientist will be able to track the entire training and model serving process of the AI system, while keeping track of the different model versions. This enhances the technical robustness of the AI system since it creates a tool for a developer to identify potential threats, misuse, technical failure and in general issues related to its development and/or operation. Through the subsequent human intervention, it is ensured that any issues will be identified and anticipated in time and properly, thus ensuring robustness and security, while maintaining the “human oversight” principle.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	90 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

Moreover, as an additional tool to ensure technical robustness and security, the AutoML component provides a model comparison report, through which the developer/operator could trace any potential issues and overall check the performance of each AI model. Additionally, this tool adheres to the “traceability” ethical component, part of the “transparency” requirement, since the reporting function provides a way to monitor the AI models, thus increasing transparency. It also follows the “human oversight” principle since, as a functional requirement (Table 24 of the current deliverable), it will provide metrics that allow the end user to be aware of the evaluation carried out during the model training, in order for the latter to decide the best model to choose.

Lastly, the aforementioned components aim to the minimization of the energy footprint, in combination with other components (e.g., MLOps combined with RENOPS to shift the training process when/where the renewable energy is available). More information and a more thorough assessment, related to the T5.2 5.3 and 5.6 actions, regarding the respect of the “environmental well-being” principle, will be provided in D5.2, due to be published in M30 (February 2025) of the TANGO project.

6.2.2.1.3 Privacy Threat Modelling & Identification for Trustworthy AI [T5.4]

As a result of the T5.4 action, two advanced components designed to enhance privacy and fortify compliance with GDPR requirements will be developed, the Privacy Enhancing Component (PEC) and the Privacy Assurance Tool (PAT). This action is directly linked to the “privacy and data governance” ethical requirement and ensures the lawfulness of processing of personal data throughout the use of the AI components and the TANGO framework, in compliance with the privacy by design principle of the GDPR.

The Privacy Enhancing Component (PEC) aims to provide assistance to the user on the conduction of a Data Protection Impact Assessment (DPIA), the identification of potential privacy risks and implementation of the necessary measures to anticipate them. With the help of this tool, the end user will be noted regarding the obligation of conducting of a DPIA, especially in the cases of processing of special categories of personal data. Since the technology will be already provided to the end user and will be used for processing operations (as a result of its function), the processing of special categories of personal data through the use of the TANGO framework is considered a matter that could raise issues as a result of the additional measures foreseen by the GDPR for such processing operations. As a result, since recommendations in order to anticipate any potential issues will be also provided, the TANGO platform provides the end user with a tool to identify his/her potential obligations and ensure compliance.

Furthermore, the Privacy Assurance Tool offers the end user a tool for him/her to manage their provided consent. Since the processing of personal data through the use of the platform will be based in the consent provided by the data subjects, TANGO provides the users with the option to manage their consent at any time, modify it according to their needs and wishes or even withdraw from it. Apart from the management function, this tool will be subsequently responsible to ensure the respect of the data minimization and purpose limitation principles since it will help the data subjects identify their needs and adjust the consent form accordingly, keep up to date his/her personal data (especially personal information), while simultaneously assisting the data controllers to identify safely the data subjects in case any interaction is needed with them (for instance in the case of exercise of any data protection rights by the data subject).

6.2.2.1.4 X-AI For Privacy and Trust Enhancement [T5.5]

This X-AI component is designed to enhance explainability and technical robustness, thus ensuring the compliance to the relevant ethical requirements. It describes an AI model, its expected impact and potential biases and explains the model’s predictions and which features had a great impact on creating the specific results. This information will be provided both to the end user and the data scientist, adhering also to the human agency component of the “Human Agency and Oversight” ethical requirement.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	91 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Through this process, the data scientist will be provided with a way to easily identify problems during the model training and the operation of the AI system overall. The reliability of this component will be thoroughly assessed through its implementation on the pilots. This will help characterize model accuracy, fairness, transparency and outcomes in AI-powered decision making.

To conclude, this component is designed to provide the end users and the data scientists with the necessary information in order for them to comprehend the decision process of the AI systems, identify any potential issues or failures, in order to ensure robustness and help the users realize that they interact with an AI system.

6.3 Social assessment of the TANGO technology

The TANGO platform is projected to have an overall positive social impact, having in mind mostly the privacy and environmental well-being preserving components, alongside the development of trustworthy AI.

Privacy is a matter of utmost importance in the past years, given the implementation of the General Data Protection Regulation. A privacy preserving environment, such as the TANGO framework, could create a sense of security to the end users and enhance their sense of trust to the entities who will be offering their services through the use of the TANGO platform. The users' direct involvement on privacy related matters, such as the management of their consent, and overall control on their personal data, provides additional guarantees to the end users that their personal data will be lawfully processed and data security and integrity is ensured.

Additionally, privacy-preserving applications can rebuild people's trust in digital services. Most of the users tend to consider that their personal data, uploaded in a platform or the internet overall, will be further unlawfully processed by other entities, mostly for commercial purposes. Providing the end users with tools that ensure data protection and lawful processing will end up increasing their trust in new technologies, fostering a more inclusive digital society where privacy is a fundamental right, not a privilege. This could be proved essential especially in factors such as healthcare, education, or public safety services, due to strict data sharing rules and the reluctance of many people to share such information.

Moreover, the use of trustworthy AI components, according to the relevant legal and regulatory framework, could also have a positive social impact. The respect to human agency principle builds confidence among users, providing them with the sense of security and safe interaction with the AI system. This will additionally strengthen the user's trust to the digital services, as mentioned above, since AI will act in a transparent, fair, and predictable manner. The users will be able to understand the decision process of the AI system, realize that they are actually interacting with it and request for additional information by the developer.

In addition to this, the interaction with an AI system will limit the potential fears or anxiety as a result of the use of the AI technology. There is a recurring theme nowadays that the AI technology will take over jobs, cause harm to people or reach to biased decisions. By addressing these fears, trustworthy AI could lead to greater social acceptance of AI-driven technologies, while simultaneously enhancing the sense that the AI technology's purpose is to assist people in their daily lives.

Furthermore, an application that also ensures environmental well-being can have a range of social impacts, from raising awareness to fostering sustainable behaviour. The steps that the TANGO platform will be taking in order to help prevent the environmental well-being could raise environmental awareness to the users, help the shift to sustainable energy and raise public awareness and understanding of these critical topics.

The fact that a platform (hence several cooperating entities) promotes the environmental well-being through its use and the practices followed, could pave the way for similar developed applications or

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	92 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

services that could have similar characteristics. The TANGO platform could be considered an example of how a platform could be effective and simultaneously help minimize the use resources, thus protecting the environment and ensuring the minimization of the energy and carbon footprint. Through the use of this application, environmentally friendly entities could further promote their services, thus boosting their operations economically and strengthening their sustainability cause.

To conclude, the development of a framework focused on the aforementioned factors could have wide-ranging positive social impact. By highlighting its privacy preserving components/capabilities, the end users could feel secure to input their personal data and take advantage of the platform's services. Additionally, the use of a trustworthy AI framework could help strengthen people's trust to the AI technology, through the implementation of procedures that adhere to the relevant legal and ethical provisions. Lastly, by integrating environmental consciousness, the application could help reshape cultural and social norms and sustainability could move from a niche concern to a mainstream value in several socioeconomic sectors.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	93 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

7 Conclusions

This final deliverable D2.4 of WP2 concludes the effort undertaken in the TANGO project to establish a data ecosystem that prioritizes transparency, security, fairness, accountability, and environmental sustainability. Building on the principles of IDSA and GAIA-X for data management and sharing, it provides the final updates and refinements that synthesize user requirements, system architecture, and technical specifications while addressing the challenges and diversity of the pilot use cases.

The key results stemming from the WP2 work include:

- **The TANGO Reference Architecture:** It is a cornerstone of the TANGO project and incorporates critical modules that can enable data sovereignty, trust, and interoperability. This architecture ensures data operations and supports data/information exchange among participants. It has been iteratively refined based on the insights and feedback gathered throughout the project, ensuring alignment with evolving technological and legal standards.
- **User-oriented design:** The project successfully identified and categorized user requirements for each pilot, overcoming challenges related to the diversity of business procedures and the underlying needs. These requirements, along with user journeys and KPIs, form the foundation for the pilot evaluation against specific scenarios and ensure that the TANGO solution addresses real-world needs.
- **Alignment of Technical Offerings and Pilots:** A mapping of the TANGO's technical components to specific pilot requirements has already been created, highlighting the adaptability and relevance of the framework to diverse cases such as Smart Hospitality, Autonomous Vehicles, Smart Manufacturing, Banking, Public Organizations, and Retail. This collaborative effort between technical and pilot partners enabled the development of functional and non-functional requirements critical to the system's success.
- **Security, Privacy, and Ethical Compliance:** The document details also the updates on measures implemented to ensure GDPR compliance, protect fundamental rights, and address ethical considerations. TANGO's Privacy, Ethical, Social, and Legal Impact Assessment forms a solid foundation for continuous monitoring and adaptation, supporting the long-term sustainability of the framework.

As this deliverable serves also as the final reference for the subsequent deliverables of the TANGO technical work packages (WP3-WP6) and their validation in WP7, it ensures that the technical and operational measures, as well as the user-centric insights, are effectively integrated into the solution and pilot demonstrations.

The TANGO project has established a robust and adaptable foundation for modern data ecosystems, addressing key challenges in data management and sharing. Through its iterative and collaborative approach, the project has successfully aligned technical offerings with user needs, ensuring the framework's relevance and scalability.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	94 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

8 Bibliography

- [1] TANGO Project Horizon Europe Consortium, “D2.2: User Needs and Requirements & Use Case Scenarios,” 2023. doi: 10.3030/101070052.
- [2] “Identity, Credential and Access Management Document - 24.07 Release.” Accessed: Jan. 15, 2025. [Online]. Available: <https://docs.gaia-x.eu/technical-committee/identity-credential-access-management/24.07/>
- [3] “DSBA releases ‘Technical Convergence Discussion Document’ - Data Spaces Business Alliance.” Accessed: Jan. 15, 2025. [Online]. Available: <https://data-spaces-business-alliance.eu/dsba-releases-technical-convergence-discussion-document/>
- [4] “GitHub - FIWARE/data-space-connector: FIWARE Data Space Connector following DSBA TC recommendations.” Accessed: Jan. 15, 2025. [Online]. Available: <https://github.com/FIWARE/data-space-connector>
- [5] “OpenID for Verifiable Presentations - draft 23.” Accessed: Jan. 15, 2025. [Online]. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
- [6] “Conformance guidelines | EBSI hub.” Accessed: Jan. 15, 2025. [Online]. Available: <https://hub.ebsi.eu/conformance>
- [7] “GitHub - FIWARE/VCVerifier: A software component that provides the necessary Relying Party endpoints required for authentication.” Accessed: Jan. 15, 2025. [Online]. Available: <https://github.com/FIWARE/VCVerifier>
- [8] “Truffle Language Implementation Framework.” Accessed: Jan. 15, 2025. [Online]. Available: <https://www.graalvm.org/latest/graalvm-as-a-platform/language-implementation-framework/>
- [9] “Hardware Acceleration for Polyglot Runtimes.” Accessed: Jan. 15, 2025. [Online]. Available: <https://www.tornadovm.org/post/hardware-acceleration-for-polyglot-runtimes>
- [10] “beehivelab/tornadovm-polyglot-graalpy-23.1.0-nvidia-openc1-container Tags | Docker Hub.” Accessed: Jan. 15, 2025. [Online]. Available: <https://hub.docker.com/r/beehivelab/tornadovm-polyglot-graalpy-23.1.0-nvidia-openc1-container/tags>
- [11] “beehivelab/tornadovm-polyglot-graalpy-23.1.0-oneapi-intel-container Tags | Docker Hub.” Accessed: Jan. 15, 2025. [Online]. Available: <https://hub.docker.com/r/beehivelab/tornadovm-polyglot-graalpy-23.1.0-oneapi-intel-container/tags>
- [12] “Harbor.” Accessed: Jan. 15, 2025. [Online]. Available: https://harbor.tango.rid-intrasoft.eu/account/sign-in?redirect_url=%2Fharbor%2Fprojects
- [13] “Reference Architecture - International Data Spaces.” Accessed: Jan. 15, 2025. [Online]. Available: <https://internationaldataspaces.org/offers/reference-architecture/>
- [14] “GitHub - FIWARE/data-space-connector: FIWARE Data Space Connector following DSBA TC recommendations.” Accessed: Jan. 15, 2025. [Online]. Available: <https://github.com/FIWARE/data-space-connector>
- [15] “What is Azure Kubernetes Service (AKS)? - Azure Kubernetes Service | Microsoft Learn.” Accessed: Jan. 15, 2025. [Online]. Available: <https://learn.microsoft.com/en-us/azure/aks/what-is-aks>
- [16] “Home - International Data Spaces.” Accessed: Jan. 15, 2025. [Online]. Available: <https://internationaldataspaces.org/>

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	95 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

- [17] “Home - Gaia-X: A Federated Secure Data Infrastructure.” Accessed: Jan. 15, 2025. [Online]. Available: <https://gaia-x.eu/>
- [18] “EOSC Association - EOSC Association.” Accessed: Jan. 15, 2025. [Online]. Available: <https://eosc.eu/>
- [19] “The Data Spaces Business Alliance - Data Spaces Business Alliance.” Accessed: Jan. 15, 2025. [Online]. Available: <https://data-spaces-business-alliance.eu/>
- [20] “Big Data Value Association - Accelerating data-driven innovation in Europe ↗.” Accessed: Jan. 15, 2025. [Online]. Available: <https://bdva.eu/>
- [21] “FIWARE - Open APIs for Open Minds.” Accessed: Jan. 15, 2025. [Online]. Available: <https://www.fiware.org/>
- [22] “Eclipse Dataspace Components | projects.eclipse.org.” Accessed: Jan. 15, 2025. [Online]. Available: <https://projects.eclipse.org/projects/technology.edc>
- [23] “GitHub - International-Data-Spaces-Association/DataspaceConnector: This is an IDS Connector reference implementation.” Accessed: Jan. 15, 2025. [Online]. Available: <https://github.com/International-Data-Spaces-Association/DataspaceConnector>
- [24] “Usage Control in the International Data Spaces.” Accessed: Jan. 15, 2025. [Online]. Available: <https://zenodo.org/records/5675884>
- [25] A. Eitel *et al.*, “Usage Control in the International Data Spaces”, doi: 10.5281/ZENODO.5675884.
- [26] “Decentralized Identifiers (DIDs) v1.0.” Accessed: Jan. 15, 2025. [Online]. Available: <https://www.w3.org/TR/did-core/#sotd>
- [27] “Verifiable Credentials Data Model v1.1.” Accessed: Jan. 15, 2025. [Online]. Available: <https://www.w3.org/TR/vc-data-model/>
- [28] “eXtensible Access Control Markup Language (XACML) Version 3.0 Errata 01.” Accessed: Jan. 15, 2025. [Online]. Available: <https://docs.oasis-open.org/xacml/3.0/errata01/csprd01/xacml-3.0-core-spec-errata01-csprd01.html>
- [29] “www.etsi.org - /deliver/etsi_gs/CIM/001_099/009/01.07.01_60/.” Accessed: Jan. 15, 2025. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/CIM/001_099/009/01.07.01_60/
- [30] “Helm.” Accessed: Jan. 15, 2025. [Online]. Available: <https://helm.sh/>
- [31] “Keycloak.” Accessed: Jan. 15, 2025. [Online]. Available: <https://www.keycloak.org/>
- [32] “walt.id | Powerful digital identity and wallet infrastructure.” Accessed: Jan. 15, 2025. [Online]. Available: <https://walt.id/>
- [33] “GitHub - Kong/kong: 🏠 The Cloud-Native API Gateway and AI Gateway.” Accessed: Jan. 15, 2025. [Online]. Available: <https://github.com/Kong/kong>
- [34] “The Path to Self-Sovereign Identity - Life With Alacrity.” [Online]. Available: <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>
- [35] Devon Loffreto, “What is ‘Sovereign Source Authority’?” Accessed: Jan. 17, 2025. [Online]. Available: <https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html>
- [36] Devon Loffreto, “Self-Sovereign Identity.” Accessed: Jan. 17, 2025. [Online]. Available: <https://www.moxytongue.com/2016/02/self-sovereign-identity.html>
- [37] Respect Network, “The Respect Trust Framework v2.1”, Accessed: Jan. 17, 2025. [Online]. Available: <https://oixnet.org/wp-content/uploads/2016/02/respect-trust-framework-v2-1.pdf>
- [38] Mariana Dahan and John Edge, “The World Citizen: Transforming Statelessness into Global Citizenship.” Accessed: Jan. 17, 2025. [Online]. Available:

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	96 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

- <https://blogs.worldbank.org/en/digital-development/world-citizen-transforming-statelessness-global-citizenship>
- [39] Kim Cameron, “The Laws of Identity.” Accessed: Jan. 17, 2025. [Online]. Available: [https://learn.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456\(v=msdn.10\)](https://learn.microsoft.com/en-us/previous-versions/dotnet/articles/ms996456(v=msdn.10))
 - [40] da Jacopo Sesana, “The 10 principles of Self-Sovereign Identity (SSI).” Accessed: Jan. 17, 2025. [Online]. Available: <https://www.selfsovereignidentity.it/the-10-principles-of-self-sovereign-identity-ssi/>
 - [41] Lu Zhou and others, “Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities.” Accessed: Jan. 17, 2025. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2214212623002624>
 - [42] Megha Srivastava and others, “An Empirical Analysis of Backward Compatibility in Machine Learning Systems.” Accessed: Jan. 17, 2025. [Online]. Available: <https://dl.acm.org/doi/10.1145/3394486.3403379>
 - [43] Mpyana Mwamba Merlec and others, “A Smart Contract-Based Dynamic Consent Management System for Personal Data Usage under GDPR.” Accessed: Jan. 17, 2025. [Online]. Available: <https://www.mdpi.com/1424-8220/21/23/7994>
 - [44] “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).” Accessed: Jan. 17, 2025. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
 - [45] Thomas Stimakovits, “Is Self-Sovereign Identity Compliant with the GDPR?” Accessed: Jan. 17, 2025. [Online]. Available: <https://stdl.medium.com/is-self-sovereign-identity-compliant-with-the-gdpr-f997da413d9d>
 - [46] Commission Nationale de l’Informatique et des Libertés (CNIL), “Blockchain. Solutions for a Responsible Use of the Blockchain in the Context of Personal Data.” Accessed: Jan. 17, 2025. [Online]. Available: https://www.cnil.fr/sites/cnil/files/atoms/files/blockchain_en.pdf
 - [47] Michèle Finck, “Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?” Accessed: Jan. 17, 2025. [Online]. Available: <https://op.europa.eu/en/publication-detail/-/publication/9b759744-be40-11e9-9d01-01aa75ed71a1/language-en>
 - [48] Agencia Española de Protección de Datos (AEPD), “Encryption and Privacy V: The Key as Personal Data.” Accessed: Jan. 17, 2025. [Online]. Available: <https://www.aepd.es/en/prensa-y-comunicacion/blog/encryption-and-privacy-v-the-key-as-personal-data>
 - [49] “GDPR, Art. 6.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/art-6-gdpr/>
 - [50] Andrés Chomczyk Penedo, “Self-Sovereign Identity Systems and European Data Protection Regulations: An Analysis of Roles and Responsibilities.” Accessed: Jan. 17, 2025. [Online]. Available: <https://dl.gi.de/server/api/core/bitstreams/0095b277-eeb1-423e-b930-2bf6237c5586/content>
 - [51] Johan Rauber and Bernd Grzeszick, “Anwendbarkeit Der DS-GVO Durch Einschaltung Dritter? Auswirkungen Bei Der Datenverarbeitung in Der Praxis,” *Zeitschrift für Datenschutz*, vol. 12, no. (Volume 12), p. 560, 2018.
 - [52] Galia Kondova and Jörn Erbguth, “Self-Sovereign Identity on Public Blockchains and the GDPR,” in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, Association for Computing Machinery (ACM), 2020. Accessed: Jan. 17, 2025. [Online]. Available: <https://dl.acm.org/doi/10.1145/3341105.3374066>

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	97 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

- [53] “GDPR, Art. 17.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/art-17-gdpr/>
- [54] Esteban Landerreche and Marc Stevens, “On Immutability of Blockchains,” in *Proceedings of the 1st ERCIM Blockchain Workshop 2018*, Reports of the European Society for Socially Embedded Technologies (EUSSET), 2018. Accessed: Jan. 17, 2025. [Online]. Available: <https://dl.eusset.eu/items/ae52ca6b-0a4f-4274-8a37-da4934733952>
- [55] Fábio Coelho and George Younes, “The GDPR-Blockchain Paradox: A Work Around,” 2018. Accessed: Jan. 17, 2025. [Online]. Available: https://www.researchgate.net/publication/329656420_The_GDPR-Blockchain_paradox_a_work_around
- [56] Andries Van Humbeeck, “The Blockchain-GDPR Paradox,” *Journal of Data Protection & Privacy*, vol. 2, p. 208, 2019.
- [57] The Sovrin Foundation, “Innovation Meets Compliance. Data Privacy Regulation and Distributed Ledger Technology.” Accessed: Jan. 17, 2025. [Online]. Available: https://sovrin.org/wp-content/uploads/GDPR-Paper_V1.pdf
- [58] Bilgesu Sümer, “Can Self-Sovereign Identity (SSI) Fit Within the GDPR?: A Conceptual Data Protection Analysis (Part I),” Jun. 03, 2022. Accessed: Jan. 17, 2025. [Online]. Available: <https://www.law.kuleuven.be/citip/blog/can-self-sovereign-identity-ssi-fit-within-the-gdpr-part-i/>
- [59] Bilgesu Sümer, “Can Self-Sovereign Identity (SSI) Fit Within the GDPR?: A Conceptual Data Protection Analysis (Part II),” Jun. 03, 2022. Accessed: Jan. 17, 2025. [Online]. Available: <https://www.law.kuleuven.be/citip/blog/can-self-sovereign-identity-ssi-fit-within-the-gdpr-part-ii/>
- [60] “GDPR, Rec. 27.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/recitals/no-27/>
- [61] Clare Sullivan, *Digital Identity: An Emergent Legal Concept*. University of Adelaide Press, 2011. Accessed: Jan. 17, 2025. [Online]. Available: <https://www.jstor.org/stable/10.20851/j.ctt1sq5wqb>
- [62] “GDPR, Art. 15.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/art-15-gdpr/>
- [63] “GDPR, Rec. 68.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/recitals/no-68/>
- [64] “GDPR, Art. 5.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/art-5-gdpr/>
- [65] “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (OJ L 257/73 2882014).” Accessed: Jan. 17, 2025. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2014/910/oj/eng>
- [66] “GDPR, Art. 11.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/art-11-gdpr/>
- [67] “GDPR, Art. 8.” Accessed: Jan. 17, 2025. [Online]. Available: <https://gdpr-info.eu/art-8-gdpr/>
- [68] “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 3042024).” Accessed: Jan. 17, 2025. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>
- [69] Giuseppe De Marco, Francesco Antonio Marino, and Andrea De Maria, “Bridging eIDAS 2.0 Legal Requirements and Technical Solutions,” CEUR Workshop Proceedings, 2024. Accessed: Jan. 17, 2025. [Online]. Available: <https://ceur-ws.org/Vol-3863/paper2.pdf>

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	98 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

- [70] CEF Digital - European Commission, “SSI eIDAS Bridge - ISA2 Innovative Public Services Action.” Accessed: Jan. 17, 2025. [Online]. Available: https://interoperable-europe.ec.europa.eu/sites/default/files/document/2020-04/SSI%20eIDAS%20Bridge_Flyer_1.pdf
- [71] Steffen Schwalm and Ignacio Allamillo-Domingo, “Self-Sovereign Identity & eIDAS: A Contradiction? Challenges and Chances of eIDAS 2.0,” *European Review of Digital Administration & Law (ERDAL)*, vol. 2, p. 89, 2021, Accessed: Jan. 17, 2025. [Online]. Available: <https://www.erdalreview.eu/free-download/979125994752910.pdf>
- [72] “Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity”, Accessed: Jan. 17, 2025. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0281>
- [73] European Data Protection Supervisor (EDPS), “Formal Comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity,” 2021. Accessed: Jan. 17, 2025. [Online]. Available: https://www.edps.europa.eu/system/files/2021-07/21-07-28_formal_comments_2021-0598_d-1609_european_digital_identity_en.pdf
- [74] Federal Constitutional Court, *Case 1 BvR 209, 269, 362, 420, 440, 484/83*. Accessed: Jan. 17, 2025. [Online]. Available: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/1983/12/rs19831215_1bvr020983en.pdf?__blob=publicationFile&v=3
- [75] R. and E. (ITRE) Committee on Industry, “Draft Report on the Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity.” Accessed: Jan. 17, 2025. [Online]. Available: https://www.europarl.europa.eu/doceo/document/ITRE-PR-732707_EN.pdf
- [76] Sailesh Oduri, “Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era,” *International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)*, vol. 13, p. 13632, 2024, Accessed: Jan. 17, 2025. [Online]. Available: https://www.researchgate.net/publication/382329835_Continuous_Authentication_and_Behavioral_Biometrics_Enhancing_Cybersecurity_in_the_Digital_Era
- [77] Nasir Memon, “How Biometric Authentication Poses New Challenges to Our Security and Privacy [In the Spotlight],” *IEEE Signal Process Mag*, vol. 34, p. 196, 2017, Accessed: Jan. 17, 2025. [Online]. Available: <https://ieeexplore.ieee.org/document/7974880>

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	99 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

Annexes

A. Updated User Requirements Overview

A.1 Pilot 1: Smart Hospitality

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-HT-001	Trusted user authentication	All categories of users must be authenticated to the system in order to have access to the relevant information, services and applications via various devices.	High	RETAINED	
UR-DMN-HT-002	Data management	Hotels must be able to collect clients' personal data directly upon check-in through the web (direct booking).	High	UPDATED	
UR-DMN-HT-003	Data management	The hotel must be able to collect the clients' preferences in order to provide them with personalised services.	High	DROPPED	The recommender does not need initial preferences.
UR-DMN-HT-004	Data management	The hotel must be able to collect data from rooms, hotel facilities, logistics information, etc.	High	RETAINED	Handled by existing NADIA platform.
UR-DMN-HT-005	Data management	The hotel must collect data from the various systems that it uses (e.g., CRM, NADIA, etc.).	High	RETAINED	
UR-DMN-HT-006	Data management	The client must be able to evaluate the recommendations received by the system.	High	RETAINED	
UR-DMN-HT-007	Data management	The client must be able to evaluate the overall experience.	High	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	100 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-DMN-HT-008	Data management	The experience provider must have access to the hotel's suggestion system to provide and enter data and information about the provided experience.	High	DROPPED	The recommender service requires an initial list of experiences to operate. No need to provide external access.
UR-DAR-HT-009	Data analysis and reporting	The hotel manager and the hotel group manager must be able to analyse the data collected from customers and produce reports that can be exported in various forms.	High	RETAINED	
UR-TDS-HT-010	Trustworthy Data sharing	The users must feel safe when they share their data.	High	RETAINED	
UR-GCO-HT-011	GDPR and related regulation compliance	The customer's data must be handled according to GDPR.	High	RETAINED	
UR-PCY-HT-012	Protection from cyberattacks	The customer must feel safe when uploading his/her personal data.	High	RETAINED	
UR-DMN-HT-013	Data management	The hotel should be able to collect and record the clients' preferences during their stay.	Medium	RETAINED	
UR-UIN-HT-014	User interaction	The client should be able to choose among various suggestions based on their preferences (food, activities, etc.).	Medium	RETAINED	
UR-UIN-HT-015	User interaction	The client should receive personalised information based on his/her preferences and other external data sources (e.g., weather, monument	Medium	DROPPED	No interaction with external data sources.

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	101 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		or activities schedule, etc.-).			
UR-DAR-HT-016	Data analysis and reporting	The clients should be able to be informed about the hotel's sustainability data and environmental footprint in a user-friendly way.	Medium	RETAINED	
UR-DAR-HT-017	Data analysis and reporting	The hotel management and the hotel association should be able to be informed about their sustainability data and environmental footprint.	Medium	RETAINED	
UR-DMN-HT-018	Data management	The users could be able to access data/information from external sources (weather, monument or activities schedule, etc.-).	Low	DROPPED	
UR-TDS-HT-019	Trustworthy Data sharing	The hotels of the same chain could be able to share customer information and profiles in a secure way.	Low	DROPPED	

A.2 Pilot 2: Autonomous Vehicles

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-AV-001	Trusted user authentication	The user must be authenticated through the application on smartphones or other	High	RETAINED	only for onboarding or also for authentication

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	102 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		smart devices (tablets, etc.).			
UR-DIN-AV-002	Data integrity	The autonomous vehicle passenger must feel safe and relaxed during the ride.	High	RETAINED	
UR-PCY-AV-003	Protection from cyberattacks	The autonomous vehicle passenger must feel safe and relaxed during the ride regardless of any external threat during the ride.	High	RETAINED	
UR-PCY-AV-004	Protection from cyberattacks	The management must feel safe that the car is protected and cannot be accessed by malicious intruders.	High	RETAINED	
UR-DUP-AV-005	Data upload	The engineering team must be able to upload sensor data to the system in a trustworthy way.	High	RETAINED	
UR-GCO-AV-006	GDPR and related regulations compliance	The engineering team must be able to upload GDPR compliant sensor data to the system.	High	RETAINED	
UR-DAC-AV-007	Data access	The automotive services company must be able to control who is using their maps, allowing access to the maps for a certain period of time (i.e., set access policies).	High	RETAINED	
UR-TDS-AV-008	Trustworthy Data-sharing	The automotive services company must be able to prevent their	High	DROPPED	TANGO cannot control how files are used

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	103 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		customers from sharing their maps with third parties.			after being downloaded.
UR-PCY-AV-009	Protection from cyberattacks	The automotive services company must be able to control if somebody modifies the content of the files (the maps).	High	RETAINED	
UR-DAC-AV-010	Data access	The user should have access to all relevant information in real time (e.g., route, real time traffic, obstacles, speed, autonomous vehicles near him, time to pick-up, time to destination, specific vehicle id to cross check).	Medium	RETAINED	Handled by IDIADA application
UR-TDS-AV-011	Trustworthy Data sharing	Clients should be sure that the digital maps are trustworthy.	Medium	RETAINED	
UR-PCY-AV-012	Protection from cyberattacks	The automotive services company could be able to control and monitor any attempts of cyberattacks.	Low	RETAINED	Part of access control
UR-DMN-AV-013	Data management	The engineering team could be able to change the data real time.	Low	DROPPED	Not supported by TANGO
UR-DMN-AV-014	Data management	The autonomous vehicle passenger could be able to request a change during the ride.	Low	RETAINED	Handled by IDIADA application
UR-UIN-AV-015	User interaction	Clients could be able to use a smart device via a user friendly interface to use the autonomous vehicle.	Low	RETAINED	Handled by IDIADA application

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	104 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

A.3 Pilot 3: Smart Manufacturing – Case 1

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-M1-001	Trusted user authentication	The customer must be authenticated to have access to the system.	High	RETAINED	
UR-TDS-M1-002	Trustworthy Data sharing	The customer must upload the design to an online working space shared with the printing company in an efficient, smooth and secure way.	High	RETAINED	
UR-TUA-M1-003	Trusted user authentication	The printer operator and the technical expert must be authenticated to have access to the system.	High	RETAINED	
UR-DAC-M1-004	Data access	The technical expert must have full access to all printing jobs to combine designs and prepare the print job file.	High	RETAINED	
UR-DST-M1-005	Data storage	The customers need to be able to access their printing job data for a short defined period of time.	High	RETAINED	
UR-DUP-M1-006	Data upload	The technical expert must have access to an automatically uploaded print job file after the printing job for data review and finalisation (data lock).	High	RETAINED	Part of the existing FMAKE process
UR-DAC-M1-007	Data access	The customer must have access to his/her printing jobs in a secure way.	High	RETAINED	
UR-DAC-M1-008	Data access	The customer must not be able to access	High	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	105 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		printing data of other customers.			
UR-DAR-M1-009	Data analysis and reporting	The customers (different IP-owners) must be able to access and view their own quality report only.	High	RETAINED	
UR-DAR-M1-010	Data analysis and reporting	The technical expert must receive reports on the print jobs to improve the printer operation and the printing quality.	High	RETAINED	Part of the existing FMAKE process
UR-DAR-M1-011	Data analysis and reporting	The manager must be able to read/view the data of all customers to get KPIs from them.	High	RETAINED	
UR-DAR-M1-012	Data analysis and reporting	The Data Scientist must be able to build an accurate machine learning (ML) model that is being used in the digital twin. The model is responsible for providing the correct quality information.	High	RETAINED	
UR-GCO-M1-013	GDPR and related regulation compliance	The customer's data must be handled according to GDPR.	High	RETAINED	
UR-PCY-M1-014	Protection from cyberattacks	The customer's printing data must be protected from any kind of cyberattacks.	High	RETAINED	
UR-DMN-M1-015	Data management	The technical expert and printing operator should be able to modify the printing data and improve them.	Medium	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	106 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-PMT-M1-016	Process monitoring	The technical expert should be able to inspect the printing process data and the changes made.	Medium	RETAINED	
UR-DMN-M1-017	Data management	The customer should be able to manage his/her printing jobs, e.g., request a reprint, etc.	Medium	DROPPED	Not supported by TANGO
UR-DAR-M1-018	Data analysis and reporting	The Data Scientist, together with the technical expert, should be able to investigate the existing data if the quality issue was predicted by the model.	Medium	RETAINED	
UR-DAR-M1-019	Data analysis and reporting	The Data Scientist should be able to pre-process the existing data.	Medium	RETAINED	
UR-DAR-M1-020	Data analysis and reporting	The Data Scientist should be able to improve the model for better predictions.	Medium	RETAINED	
UR-PMT-M1-021	Process monitoring	The technical manager could be able to inspect the printing process per customer (IP owner).	Low	DROPPED	Not supported by TANGO

A.4 Pilot 3: Smart Manufacturing – Case 2

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-M2-001	Trusted user authentication	Shopfloor workers must have access only to their designated areas.	High	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	107 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-M2-002	Trusted user authentication	The company files must be protected in a smart way, enabling access based on each person's role.	High	RETAINED	
UR-PMT-M2-003	Process monitoring	The supervisor must know every time a worker is not at the designated area.	High	RETAINED	
UR-PMT-M2-004	Process monitoring	The supervisor must be notified every time a worker is not at the designated area.	High	RETAINED	
UR-TUA-M2-005	Trusted user authentication	Each technology provider must be able to access their provided solution remotely to perform support services (e.g., software updates, configuration, troubleshooting, problem resolution, etc.) in a secure way.	High	RETAINED	
UR-PCY-M2-006	Protection from cyberattacks	The company's data must be protected from any kind of cyber-attacks.	High	RETAINED	
UR-GCO-M2-007	GDPR and related regulation compliance	The customer's data must be handled according to GDPR.	High	RETAINED	
UR-PMT-M2-008	Process monitoring	The supervisor should have records of all unauthorised access attempts in the platform system.	Medium	RETAINED	
UR-DAR-M2-009	Data analysis and reporting	The supervisor should receive a report of all unauthorised access attempts in the platform system.	Medium	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	108 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-PMT-M2-010	Process monitoring	The company should be able to monitor the shopfloor for any strange movements and be notified.	Medium	RETAINED	
UR-TUA-M2-011	Trusted user authentication	Each technology partner should be onboarded to access the factory.	Medium	UPDATED	Through TANGO onboarding mechanism.
UR-TUA-M2-012	Trusted user authentication	Specific users should know if the technology providers are not following the authorised path for their applications.	Medium	RETAINED	
UR-TUA-M2-013	Trusted user authentication	Specific users should receive security breach notifications if the technology providers are not following the authorised path for their applications.	Medium	RETAINED	
UR-PMT-M2-014	Process monitoring	The company should have a clear view and records of the technology partners' actions during their presence in the system.	Medium	RETAINED	
UR-PCY-M2-015	Protection from cyberattacks	The company's operation should not be interrupted by any unauthorised access.	Medium	RETAINED	
UR-TUA-M2-016	Trusted user authentication	Authentication and restricted application access should be ensured for all users,	Low	UPDATED	
UR-DMN-M2-017	Data management	The company documents could be shared but not	Low	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	109 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		changed by the people accessing them.			
UR-DMN-M2-018	Data management	Specific clients could be able to share data to specific users.	Low	RETAINED	

A.5 Pilot 4: Banking

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-BN-001	Trusted user authentication	All categories of users must be authenticated to the system in order to have access to the relevant information.	High	RETAINED	
UR-PMT-BN-002	Process monitoring	Participants should be able to monitor the performance of the system over time to ensure that it flags fraudulent activity accurately.	High	RETAINED	
UR-SAD-BN-003	System adaptability	The system must adapt to changes of the fraud landscape. In other words, the system should learn from past fraud cases, estimate probability, and adapt to new patterns as they emerge, making them more effective in detecting and preventing fraud.	High	RETAINED	
UR-TDS-BN-004	Trustworthy Data sharing	Participants must be able to share data in a trustworthy and secure way.	High	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	110 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-DMN-BN-005	Data management	Participants must be able to upload financial data to the system in a trustworthy way.	High	RETAINED	
UR-DMN-BN-006	Data management	The datasets must be prepared to comply with the data structure required by the platform (data preparation and harmonization).	High	RETAINED	
UR-DAR-BN-007	Data analysis and reporting	Participant should be able to understand the reason why the system detects anomalies that may indicate fraudulent activity.	High	RETAINED	
UR-DAR-BN-008	Data analysis and reporting	Participants must be able to review the overall system performance and regularly assess results to identify if any modifications are required.	High	RETAINED	
UR-GCO-BN-009	GDPR and related regulation compliance	The financial data must be handled according to the GDPR.	High	RETAINED	
UR-GCO-BN-010	GDPR and related regulation compliance	The financial data must be handled according to Banking Secrecy and AML regulations.	High	RETAINED	
UR-PCY-BN-011	Protection from cyberattacks	The confidentiality, integrity and availability (CIA) of the system must be always preserved.	High	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	111 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

A.6 Pilot 5: Public Organizations

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-PA-001	Trusted user authentication	The applicants must be authenticated to have access to the system.	High	RETAINED	
UR-TUA-PA-002	Trusted user authentication	The VISAR employees must be authenticated to have access to the system.	High	RETAINED	
UR-TUA-PA-003	Trusted user authentication	The employers must be authenticated to have access to the system.	High	RETAINED	
UR-TUA-PA-004	Trusted user authentication	The authority employees must be authenticated to have access to the system.	High	RETAINED	
UR-DUP-PA-005	Data upload	The applicants must be able to upload documents and data to the system in a trustworthy way.	High	RETAINED	
UR-DUP-PA-006	Data upload	The VISAR employees must be able to upload documents and data to the system in a trustworthy way.	High	RETAINED	
UR-DUP-PA-007	Data upload	The employers must be able to upload documents and data to the system in a trustworthy way.	High	RETAINED	
UR-DUP-PA-008	Data upload	The authority employees must be able to upload documents and data to the system in a trustworthy way.	High	RETAINED	
UR-DMN-PA-009	Data management	The VISAR employee must be able to monitor and manage the documents and the	High	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version	Page:	112 of 139
Reference:	D2.4	Dissemination:	PU
	Version:	1.0	Status: Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		data flow in the system.			
UR-TDS-PA-010	Trustworthy Data sharing	The users must be able to share data in a trustworthy and secure way.	High	RETAINED	
UR-GCO-PA-011	GDPR and related regulation compliance	The applicant's data must be handled according to GDPR.	High	RETAINED	
UR-PCY-PA-012	Protection from cyberattacks	The users must feel secure that the data and document flow is not compromised.	High	RETAINED	
UR-PCY-PA-013	Protection from cyberattacks	The applicants must feel secure when uploading and sharing their data within the platform.	High	RETAINED	
UR-DMN-PA-014	Data management	The VISAR employees should be able to ensure that the uploaded documents are real and can authenticate them.	Medium	RETAINED	
UR-UIN-PA-015	User interaction	Applicants could be able to have a better experience via the use of AI technology.	Low	DROPPED	Not part of the final scenarios
UR-DMN-PA-016	Data management	VISAR employees could use a document recognition and pdf mapping software to automatically identify mismatches and incorrect information inputs.	Low	DROPPED	Not supported by TANGO technologies
UR-DMN-PA-017	Data management	VISAR employees could use a document validation system to verify authenticity and detect fakes.	Low	DROPPED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	113 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

A.7 Pilot 6: Retailers

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
UR-TUA-RT-001	Trusted user authentication	All categories of users must be authenticated to the system in order to have access to the relevant information via various devices.	High	RETAINED	
UR-DMN-RT-002	Data management	Specific users must be able to upload data to the system.	High	RETAINED	
UR-DMN-RT-003	Data management	Specific users must be able to request data harmonisation from the master and transactional databases.	High	RETAINED	
UR-DMN-RT-004	Data management	Specific users must be able to request a common view and analysis of data.	High	RETAINED	
UR-DMN-RT-005	Data management	Specific users must be able to view the harmonised data in various views with various filters and search parameters.	High	RETAINED	
UR-DMN-RT-006	Data management	Specific users must be able to run queries to the harmonised data.	High	RETAINED	
UR-DMN-RT-007	Data management	Specific users must be able to request for specific data analysis results.	High	RETAINED	
UR-DMN-RT-008	Data management	Specific users must be able to combine data from various external sources.	High	RETAINED	Part of METRO process, not handled by TANGO.
UR-DMN-RT-009	Data management	Specific users must receive recommendations	High	DROPPED	Not supported by TANGO

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	114 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		for targeted and effective campaigns.			
UR-DMN-RT-010	Data management	Specific users must be able to retrieve the requested data (e.g., sales data, etc.).	High	RETAINED	
UR-DMN-RT-011	Data management	Specific users must be able to delete the uploaded data from the system.	High	RETAINED	
UR-TDS-RT-012	Trustworthy data sharing	Specific users must be able to share data in a safe and trustworthy way.	High	RETAINED	
UR-DAR-RT-013	Data analysis and reporting	Specific users must receive notifications from the system after data processing or analysis is completed.	High	RETAINED	
UR-DAR-RT-014	Data analysis and reporting	Specific users must be able to analyse data.	High	RETAINED	
UR-DAR-RT-015	Data analysis and reporting	Specific users must be able to visualise data.	High	RETAINED	
UR-DAR-RT-016	Data analysis and reporting	Specific users must be able to produce customised reports.	High	RETAINED	
UR-GCO-RT-017	GDPR and related regulation compliance	The company's data must be handled according to GDPR.	High	RETAINED	
UR-PCY-RT-018	Protection from cyberattacks	The users must feel secure that the data flow is not compromised.	High	RETAINED	
UR-PCY-RT-019	Protection from cyberattacks	The company must feel safe from cyberattacks.	High	RETAINED	
UR-DMN-RT-020	Data management	Specific users should be able to view the automatically mapped data from	Medium	RETAINED	

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	115 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0
				Status:	Final

CODE	CATEGORY	USER REQUIREMENTS DESCRIPTION	PRIORITY	UPDATE	COMMENTS
		different sources and data structures.			
UR-DMN-RT-021	Data management	Specific users should be able to retrieve market/marketing/ product data from external sources, periodically or not.	Medium	DROPPED	External sources connection not supported
UR-DMN-RT-022	Data management	The users should use anonymized data.	Medium	RETAINED	

B. System Requirements for Distributed Privacy-preserving Data Management and Storage

B.1 Functional Requirements

Table 2: Blockchain-based Data Storage and Sharing Component Functional Requirements (Author: NOR)

ID	Description	Priority	Status
FR-DATA-BDSS-001	The TANGO system must be able to collect and manage customer consent for every act of customer data sharing. TANGO system must be able to keep the collected consent, enforce consented policies and demonstrate it to the auditing authority.	High	Done
FR-DATA-BDSS-002	The TANGO system must ensure that the data sharing mechanism is fully compliant with the relevant regulations concerning private data handling.	High	Done
FR-DATA-BDSS-003	The TANGO system must ensure that the data access logs are stored immutably, in a safe and legally compliant manner, and are available to auditing authorities upon request.	High	Done

Table 3: Trustworthy Data Sharing Component Functional Requirements (Author: FHG, FUJ_DE, VTT)

ID	Description	Priority	Status
FR-DATA-TDS-001	Simulated privacy attacks based on predefined adversary settings against the data sharing process or the shared data to estimate the risk of possible privacy leakages. The privacy risk analysis must be performed to aid in the creation of a suitable Trustworthiness score.	High	In Progress
FR-DATA-	The TANGO system must provide a module configuring the Trustworthiness calculation and a module calculating the Trustworthiness scores based on this configuration.	High	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	116 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
TDS-002			
FR-DATA-TDS-003	Thus, the TANGO system must provide a module configuring the Trustworthiness calculation and a module calculating the Trustworthiness scores based on this configuration for the Data Gate Keeper system .	High	Dropped as covered by FR-DATA-TDS-002
FR-DATA-TDS-004	The TANGO system should provide a data repository of few kilobytes for each end guest and each vendor (i.e. hotel, activity provider etc.).	Medium	In Progress
FR-DATA-TDS-005	The TANGO system should provide user transaction data, e.g., shopping baskets.	Medium	In Progress

Table 4: Confidentiality and Privacy by design Component Functional Requirements (Author: UMU)

ID	Description	Priority	Status
FR-DATA-CPD-001	The TANGO system must allow an administrator or policy authors to define the policies based on attributes.	High	Done
FR-DATA-CPD-002	The TANGO system must enforce access control decisions based on policies evaluation.	High	Done
FR-DATA-CPD-003	The TANGO system must apply fine-grained control over data access and usage.	High	Done
FR-DATA-CPD-004	The TANGO system should define the appropriate security controls at each stage of the data lifecycle.	Medium	Done
FR-DATA-CPD-005	The TANGO system must involve mechanisms to enforce policies and restrictions.	High	Done
FR-DATA-CPD-006	The TANGO system must support the enforcement of defined policies by an encryption/decryption mechanism.	High	Done

Table 5: Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms Functional Requirements (Author: DUT)

ID	Description	Priority	Status
FR-DATA-SEDT-001	The TANGO system must implement robust data encryption techniques to protect sensitive information generated and collected by autonomous vehicles or smart manufacturing systems. Encryption ensures that data remains unreadable to unauthorized parties and maintains its confidentiality throughout storage and transmission.	High	Done
FR-DATA-SEDT-002	The TANGO system should support multi-factor authentication mechanisms, requiring users to provide multiple authentication factors such as passwords, biometrics, or physical tokens to access sensitive data or system functionalities. This adds an extra layer of	Medium	Postponed

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	117 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
	security, ensuring that only authorized individuals with valid credentials can gain access.		
FR-DATA-SEDT-002	The TANGO system should implement encryption algorithms and techniques that are highly efficient in terms of computational resources and processing time. The encryption process should be optimized to minimize any performance impact on the overall system functionality.	Medium	In Progress

B.2 Non-Functional Requirements

Table 6: Blockchain-based Data Storage and Sharing Component Non-Functional Requirements (Author: NOR)

ID	Description	Priority	Status
NFR-PER-BDSS-001	The TANGO system must deliver reasonable performance.	High	Done
NFR-REL-BDSS-001	The TANGO system must guarantee 100% data delivery when data sharing component is involved.	High	Done
NFR-SEC-BDSS-001	The TANGO system must guarantee that user data is being handled securely.	High	Done

Table 7: Trustworthy Data Sharing Component Non-Functional Requirements (Author: FHG, FUJ_DE, VTT)

ID	Description	Priority	Status
NFR-SEC-TDS-001	The TANGO system could provide the continuous Privacy Risk Score to a monitoring system, which could visualize the Privacy for easy evaluation.	Low	In Progress
NFR-SEC-TDS-002	The TANGO system could provide the continuous Trustworthiness Score to a monitoring system, which could visualize the Trustworthiness of the vehicle or the platform for easy evaluation by a user.	Low	In Progress
NFR-SEC-TDS-003	The TANGO system could facilitate the assessment of the regular operations of the shopfloor	Low	Postponed
NFR-UI-TDS-001	The TANGO system should provide hotel guests recommendations in a user-friendly personalized order	Medium	In Progress
NFR-UI-TDS-002	The TANGO system should provide business intelligence from retail locations that are not per se allowed to share customer data with each other.	Medium	In Progress

Table 8: Confidentiality and Privacy by Design Non-Functional Requirements (Author: UMU)

ID	Description	Priority	Status
NFR-SEC-CPD-001	The TANGO system must prioritize and enforce robust security measures to protect data.	High	Done

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	118 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
NFR-SEC-CPD-002	The TANGO system must ensure the privacy of individuals and sensitive data aligned with GDPR.	High	Done
NFR-PER-CPD-001	The TANGO system should not introduce significant performance overhead that could impact system responsiveness.	Medium	Done
NFR-REL-CPD-001	The TANGO system must ensure continuous enforcement of policies.	High	Done

Table 9: Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms Non-Functional Requirements (Author: DUT)

ID	Description	Priority	Status
NFR-MAIN-SEDT-001	The TANGO system must be designed with a modular architecture, where the self-encryption and decryption component is a self-contained and easily maintainable module. It should be capable of independent updates or enhancements without affecting the overall system functionality.	High	Done
NFR-PER-SEDT-001	The TANGO system should exhibit high-performance efficiency in terms of encryption, decryption, and multi-factor information recovery operations. The component should be optimized to minimize processing time, computational resources, and memory usage, without compromising the overall system performance.	Medium	Done
NFR-COMP-SEDT-001	The TANGO system should demonstrate interoperability with commonly used communication protocols and data formats in the autonomous vehicle or smart manufacturing domain as far as self-encryption and decryption techniques are considered. It should seamlessly exchange information with other systems to facilitate smooth integration and collaboration.	Medium	In Progress

C. System Requirements for Distributed Trust Management Framework

C.1 Functional Requirements

Table 10: Self-sovereign identity management Functional Requirements (Author: VTT, UMU, ATOS)

ID	Description	Priority	Status
FR-TRUST-SSIM-001	The TANGO dp-ABC cryptographic system must generate a public and a private key.	High	Done
FR-TRUST-SSIM-002	The TANGO dp-ABC cryptographic system must be able to generate a digital signature.	High	Done
FR-TRUST-SSIM-003	The TANGO dp-ABC cryptographic system must be able to verify signatures with the public key.	High	Done
FR-TRUST-SSIM-004	The TANGO dp-ABC cryptographic system must generate a token corresponding to the selective disclosure ZK proof.	High	Done
FR-TRUST-SSIM-005	The TANGO dp-ABC cryptographic system must be able to verify the Zkey token generated.	High	Done

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	119 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
FR-TRUST-SSIM-006	The TANGO system should give users granular control over the amount of personal information revealed about them, for instance by considering what information is revealed by combining multiple data disclosures made at different times.	Medium	Done
FR-TRUST-SSIM-007	The TANGO system must provide a wallet or a manager for personal credentials. This is an independent part of the whole SSI module.	High	Done
FR-TRUST-SSIM-008	The TANGO system should provide methods for detecting any use of data contrary to what was agreed to, for instance storing the data for longer time than agreed.	Medium	Dropped
FR-TRUST-SSIM-009	The TANGO system could provide methods for repudiation of disclosed data, to minimize the risk of user data being used in harmful ways.	Low	Dropped
FR-TRUST-SSIM-010	The TANGO system must issue eID Verifiable Credentials to end users to simulate the EU Digital Identity Wallet	High	In Progress Newly Identified
FR-TRUST-SSIM-011	The TANGO system must issue Organization Members with Verifiable Credential to be able to act on behalf of their organization as according to their rôle/ job title.	High	In Progress
FR-TRUST-SSIM-012	The TANGO system must verify both eID and Organization Member Verifiable Credentials and return the identity claims in an ID Token.	High	In Progress

Table 11: Seamless Onboarding for Users and Devices Functional Requirements (Author: QBE)

ID	Description	Priority	Status
FR-TRUST-SOUD-001	The TANGO system must allow hotel guests to perform remote identity verification.	High	Done
FR-TRUST-SOUD-002	The TANGO system must allow visa applicants to perform remote identity verification.	High	In Progress

Table 12: User continuous behavioural authentication Functional Requirements (Author: QBE)

ID	Description	Priority	Status
FR-TRUST-UCBA-001	The TANGO system must guarantee that the hotel guest accessing the platform, is who they claim they are.	High	Done
FR-TRUST-UCBA-002	The TANGO system must guarantee that the person (staff employee) accessing the platform, is who they claim they are.	High	Done
FR-TRUST-UCBA-003	The TANGO system must guarantee that the person (visa application and organisation employee) accessing the platform, is who they claim they are.	High	In Progress
FR-TRUST-UCBA-004	The TANGO system must guarantee that the person accessing the platform, is who they claim they are.	High	Done
FR-TRUST-UCBA-005	The TANGO system must be able to detect fraud in different transactions.	High	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	120 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Table 13: Device continuous behavioural authentication Functional Requirements (Author: UTH)

ID	Description	Priority	Status
FR-TRUST-DCBA-001	The TANGO system must be able to monitor, poll and log the device's hardware information (id, manufacturer, model, processor type, speed, etc.)	High	<u>In Progress</u>
FR-TRUST-DCBA-002	The TANGO system must be able to monitor, poll and log the device's network status (IMEI number, IP address, MAC address, WLAN SSID, etc.) as well as the device's network traffic patterns (DNS queries, packet size and timing, port usage etc.)	High	<u>In Progress</u>
FR-TRUST-DCBA-003	The TANGO system must be able to monitor, poll and log the device's location familiarity (nearby RF signals such as WiFi, Bluetooth devices, etc.)	High	<u>Done</u>
FR-TRUST-DCBA-004	The TANGO system should be able to render extracted data in a predefined and standard format, handle invalid entries and undefined values and prepare the processes data for feeding into AI/ML models for behavioural analysis and classification.	Medium	<u>Done</u>
FR-TRUST-DCBA-005	The TANGO system must be able to feed the preprocessed data to an AI/ML model for behavioral recognition and anomaly detection.	High	<u>In Progress</u>
FR-TRUST-DCBA-006	The TANGO system must be able to generate alerts based on the verdict of the AI model for abnormal behavior, and provide contextual information, including the affected device along with details of the behavior change that triggered the alert.	High	<u>In Progress</u>

Table 14: Hardening Against Side-channel Attacks Functional Requirements (Author: CEA)

ID	Description	Priority	Status
FR-TRUST-HASA-001	The smart hospitality components for sensor data ciphering physically accessible to an attacker must include side-channel countermeasures.	High	In Progress

C.2 Non-Functional Requirements

Table 15 Self-sovereign identity management Non-Functional Requirements (Author: VTT, UMU, ATOS)

ID	Description	Priority	Status
NFR-SEC-SSIM-001	The TANGO dp-ABC cryptographic system could enable distributed issuance processes, through the aggregation of public keys and combination of signatures into a single one.	Low	Done
NFR-SEC-SSIM-002	The TANGO dp-ABC cryptographic system must ensure the confidentiality of sensitive information.	High	Done
NFR-SEC-SSIM-003	The TANGO dp-ABC cryptographic system must ensure the integrity of sensitive information.	High	Done
NFR-SEC-SSIM-004	The TANGO dp-ABC cryptographic system must ensure the authenticity of proofs.	High	Done

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	121 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
NFR-PER-SSIM-001	The TANGO dp-ABC cryptographic system should scale effectively as the number of proof requests and system participants increases.	Medium	Done
NFR-REL-SSIM-001	The TANGO dp-ABC cryptographic system must produce accurate and correct outputs.	High	Done
NFR-REL-SSIM-002	The system should be highly available, allowing users to access the method without significant downtime or interruptions in case of faults or failures.	Medium	Done
NFR-COMP-SSIM-001	The SSI Agent must follow the GDPR to respect the privacy of the user's personal data.	High	Done
NFR-SEC-SSIM-005	The SSI Agent must comply with the GDPR and any related regulations as identified by the pilot partners.	High	Done

Table 16: Seamless Onboarding for Users and Devices Non-Functional Requirements (Author: QBE)

ID	Description	Priority	Status
NFR-COMP-SOUD-001	The TANGO system must be compatible with SSI.	High	Done
NFR-PER-SOUD-001	The TANGO system must support identity verification in a performant, reliable, secure manner.	High	Done
NFR-EXIST-SOUD-001	The TANGO system must perform the identity verification through smartphones.	High	Done

Table 17 User continuous behavioural authentication Non-Functional Requirements (Author: QBE)

ID	Description	Priority	Status
NFR-COMP-UCBA-001	The solution must be compatible with the TANGO mobile and web apps.	High	Done
NFR-REL-UCBA-001	The TANGO system must ensure that the user continuous behavioural authentication will operate in real-time, reliably and to be secure.	High	Done
NFR-EXIST-UCBA-001	The TANGO system must support smartphone and web apps	High	Done
NFR-REL-UCBA-002	The TANGO system should be able to accurately and reliably detect fraud based on different types of transactions.	Medium	In Progress

Table 18: Device continuous behavioural authentication Non-Functional Requirements (Author: UTH)

ID	Description	Priority	Status
NFR-COMP-DCBA-001	The TANGO system should ensure compatibility and applicability of the DBCA module.	Medium	Done
NFR-PER-DCBA-001	The TANGO system should ensure the efficient execution of the DBCA module, as well as the rapid reaction to abnormal behavior.	Medium	In Progress
NFR-REL-DCBA-001	The TANGO system must ensure continuous and accurate device behavioral authentication.	High	In Progress
NFR-SEC-DCBA-001	The TANGO system must ensure that personal data is not leaked, and data handling is GDPR-compliant.	High	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	122 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Table 19: Hardening Against Side-channel Attacks Non-Functional Requirements (Author: CEA)

ID	Description	Priority	Status
NFR-EXIST-HASA-001	The smart hospitality components for sensor data ciphering physically accessible to an attacker must include side-channel countermeasures.	High	In Progress
NFR-COMP-HASA-001	The code polymorphism countermeasure relies on dynamic code generation: write and execute permissions should be given to a memory segment in order to deploy this countermeasure.	Medium	Dropped
NFR-SEC-HASA-001	Securing against side-channel attacks forces to find a trade-off between performance (i.e. clock cycles) and security (i.e. how resistant to an attack the code will be). Security must be as good as possible for a given performance constraint.	High	Done

D. System Requirements for AI-based Framework for Green & Trustworthy Operations

D.1 Functional Requirements

Table 20: EDAE Component Functional Requirements (Author: EXUS)

ID	Description	Priority	Status
FR-AI-EDAE-001	The TANGO system must divide customers into categories based on shopping frequency, amounts spent and recency and generate relevant reports.	High	Done
FR-AI-EDAE-002	The TANGO system must detect and report shopping patterns and preferences between customers of different countries using different systems and structures.	High	Done
FR-AI-EDAE-003	The TANGO system must expose data to analysts of suppliers, new customer prospects that are setting up their business case, other markets, and the tourism industry.	High	Done
FR-AI-EDAE-004	The TANGO system must provide a deep analysis of the sales data, product data, and customer data.	High	Done
FR-AI-EDAE-005	The TANGO system must spot weak areas in a store.	High	Done
FR-AI-EDAE-006	The TANGO system should explore large datasets pertaining to customer purchasing patterns.	Medium	In Progress
FR-AI-EDAE-007	The TANGO system must provide hotel (group) managers with statistics and analysis reports on the data collected across all hotels.	High	In Progress
FR-AI-EDAE-008	The TANGO system must inform hotel (group) managers on patterns, trends and associations between a client's traits and preferences and those of other clients.	High	In Progress
FR-AI-EDAE-009	The TANGO system must provide technicians with reports on the print (incl. failed) jobs to improve the printer operation and the printing quality.	High	Dropped

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	123 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
FR-AI-EDAE-010	The TANGO system must provide managers with customers' data to get KPIs from them.	High	Done
FR-AI-EDAE-011	The TANGO system should provide data scientists with data related to prints' quality issues.	Medium	Dropped
FR-AI-EDAE-012	The TANGO system must be able to provide users with tools to perform fusion from multiple sources (possibly with different data structures/schemas) and visualize the results.	High	In Progress
FR-AI-EDAE-013	The TANGO system must be able to generate notifications regarding the status of all EDAE processing tasks that will be sent to the visualization and the UI components.	High	In Progress

Table 21: Federated Learning Component Functional Requirements (Author: ATOS)

ID	Description	Priority	Status
FR-AI-FL-001	The TANGO system must provide the capability to setup a data processing machine as a training node of a federated learning architecture.	High	In Progress
FR-AI-FL-002	The TANGO system must provide the capability to setup a data processing machine as a main node of a federated learning architecture.	High	Done
FR-AI-FL-003	The TANGO system should support the usage of python programming language in the federated learning process	Medium	Dropped The tools is implemented in python
FR-AI-FL-004	The TANGO system should support pyTorch and Keras	Medium	Newly Identified Done

Table 22: MLOps Component Functional Requirements (Author: ATOS)

ID	Description	Priority	Status
FR-AI-MLOPS-001	The TANGO system must offer the functionality to keep track of different model versions generated during experimentations	High	Done
FR-AI-MLOPS-002	The TANGO system should be able to allow the deployment of models that have been persisted in the MLOps component.	Medium	Done

Table 23: AutoML Component Functional Requirements (Author: ATOS)

ID	Description	Priority	Status
FR-AI-AUTOML-001	The TANGO system must provide a mechanism to generate a model resultant from the automatic optimization of its parameters	High	Done
FR-AI-AUTOML-002	The TANGO system must provide metrics that allows the end user to be aware of the evaluation carried out during the model training to decide the best model to choose.	High	Done

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	124 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Table 24: TornadoVM Component Functional Requirements (Author: UOM)

ID	Description	Priority	Status
FR-AI-TVM-001	The data analytics that will be developed by the EXUS engine in Task T5.1 must not use any data dependency.	High	In Progress
FR-AI-TVM-002	The data sizes that will be given for the analytics (developed by the EXUS EDAE engine in Task T5.1) must be beyond the scale of 2k elements (array length).	High	In Progress

Table 25: Privacy Enhancing Component Functional Requirements (Author: UOG)

ID	Description	Priority	Status
FR-AI-PEC-001	The TANGO system must provide privacy impact assessment to identify critical data actions, threats and their possible privacy impact, and mitigation measures to be able to preserve privacy of users and assure trust on the system.	High	Done
FR-AI-PEC-002	The TANGO system must provide a list of recommendations to address the identified privacy risks	Medium	Done
FR-AI-PEC-003	The TANGO system could enable data protection impact assessment mandated by GDPR when handling sensitive data.	Low	Done

Table 26: Privacy Assurance Tool Functional Requirements (Author: FUJ_LU)

ID	Description	Priority	Status
FR-AI-PAT-001	The TANGO system must be able to collect client's personal data directly through the web. In addition, it must be able to collect the clients' preferences to provide them with personalised services.	High	Done
FR-AI-PAT-002	The TANGO system must enable data sharing only among the relevant stakeholders/business partners.	High	Done
FR-AI-PAT-003	The TANGO system must allow management of data based on GDPR requirements.	High	Done
FR-AI-PAT-004	The TANGO system must provide a trusted user authentication for VISAR applicants.	High	Done
FR-AI-PAT-005	The TANGO system must provide a trusted user authentication for VISAR employees.	High	Done
FR-AI-PAT-006	The TANGO system must provide a secure data uploading channel.	High	Done
FR-AI-PAT-007	The TANGO system must provide a data management approach for monitoring and managing the shared data.	High	Done

Table 27: XAI Component Functional Requirements (Author: SQD)

ID	Description	Priority	Status
FR-AI-XAI-001	The TANGO system must explain the model's predictions and describe which features had a great impact on creating the specific results.	High	In progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	125 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
FR-AI-XAI-002	The TANGO system must explain the model's predictions, giving the data scientist the opportunity to easily identify problems during the model training	High	In progress

Table 28: RENOPS Component Functional Requirements (Author: XLAB)

ID	Description	Priority	Status
FR-AI-RENOPS-001	The TANGO system must provide an accurate forecast of renewable energy availability.	High	Done
FR-AI-RENOPS-002	The TANGO RENOPS must provide the model prediction via an API.	High	Done
FR-AI-RENOPS-003	The TANGO RENOPS system must be able to utilize information from the forecasting service and schedule energy intensive tasks in time.	High	Done
FR-AI-RENOPS-004	The TANGO RENOPS system could utilize information from the forecasting service to geographically schedule the workload.	Low	In Progress

D.2 Non-Functional Requirements

Table 29: EDAE Component Non-Functional Requirements (Author: EXUS)

ID	Description	Priority	Status
NFR-COMP-EDAE-001	The TANGO system should be compatible with all TANGO components that consume its data and with any user platform that feeds the EDAE.	Medium	In Progress
NFR-PORT-EDAE-001	The TANGO EDAE component should be dockerised.	Medium	Done

Table 30: Federated Learning Component Non-Functional Requirements (Author: ATOS)

ID	Description	Priority	Status
NFR-PER-FL-001	The TANGO system must ensure that the training nodes in federated learning offer technical resources to perform the model training	High	Done
NFR-PER-FL-002	The TANGO system should provide the capability of defining thresholds for the model performance and training.	Medium	Dropped
NFR-SEC-FL-001	The TANGO system must ensure connectivity between the training nodes and the master node in a federated learning scenario	High	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	126 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

Table 31: MLOps Component Non-Functional Requirements (Author: ATOS)

ID	Description	Priority	Status
NFR-PORT-MLOPS-001	The TANGO system must provide the MLOps component in a virtualized way	High	Done
NFR-UI-MLOPS-001	The TANGO system should provide an interactive UI where the MLOps component user can check the stat of all the ML experiments tracked as well as all the models or artifacts registered.	Medium	Done (MLFlow UI)

Table 32: AutoML Component Non-Functional Requirements (Author: ATOS)

ID	Description	Priority	Status
NFR-PER-AUTOML-001	The TANGO system must ensure that the AutoML component is ran in devices that allow the execution of the training process of the models to be generated	High	Done

Table 33: TornadoVM Non-Functional Requirements (Author: UOM)

ID	Description	Priority	Status
NFR-COMP-TVM-001	The EDAE engine of the TANGO system could utilize the Java API of TornadoVM in Task 5.3.	Low	Dropped

Table 34: Privacy Enhancing Component Non-Functional Requirements (Author: UOG)

ID	Description	Priority	Status
NFR-COMP-PEC-001	The TANGO system must be able to initiate request/share data among other components to support data visualisation.	High	Done
NFR-UI-PEC-001	The TANGO system must be able to capture user input through usable interfaces to support the tasks of PEC.	High	Done

Table 35: Privacy Assurance Tool Non-Functional Requirements (Author: UOG)

ID	Description	Priority	Status
NFR-SEC-PAT-001	The TANGO system must provide a UI to authenticate and request data in compliance to the GDPR.	High	Done
NFR-UI-PAT-001	The TANGO system must provide an easy-to-use UI to authenticate and share data with preferences in a trustworthy and privacy aware way.	High	Done

Table 36: XAI Component Non-Functional Requirements (Author: SQD)

ID	Description	Priority	Status
NFR-COMP-XAI-001	The TANGO XAI component must support communication over Hypertext Transfer Protocol (HTTP) with the rest of the system.	High	In Progress
NFR-PER-XAI-001	The TANGO XAI component must have an optimal performance.	High	Done

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	127 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
NFR-PER-XAI-002	The TANGO XAI component must have the required resources available.	High	Done
NFR-PORT-XAI-001	The TANGO XAI component should be dockerized.	Medium	In Progress
NFR-REL-XAI-001	The TANGO XAI component must produce reliable results.	High	Done

Table 37: RENOPS Component Non-Functional Requirements (Author: XLAB)

ID	Description	Priority	Status
NFR-MAIN-RENOPS-001	The TANGO RENOPS service should be developed in CI/CD pipeline.	Medium	In Progress
NFR-PORT-RENOPS-001	The TANGO RENOPS service should be located inside a containerized environment.	Medium	Done
NFR-REL-RENOPS-001	The TANGO RENOPS system could be managed by an orchestrator to scale the resources with demand.	Low	Postponed
NFR-SEC-RENOPS-001	The TANGO RENOPS system must enable secure communication and maintain integrity.	High	Done

E. System Requirements for Visualisation Techniques & User Interfaces

E.1 Functional Requirements

Table 38: User Interfaces Functional Requirements (Author: LST)

ID	Description	Priority	Status
FR-S-UI-001	The TANGO UI must be able to receive messages from the system and notify the user accordingly, and vice versa.	High	In Progress
FR-S-UI-002	The TANGO technical offerings must follow the OPEN API specification for providing their data and parameters to the UI	High	In Progress
FR-S-UI-003	The TANGO technical offerings must use API REST back-end service that uses JSON documents for payloads. All the necessary input for the UI must use JSON documents for their payloads, in order for the UI to process them and visualize them under a common template. Specific requirements for these payloads will be drafted per technology offering, but all of them should provide an Authorization header for instance.	High	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	128 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
FR-S-UI-004	The TANGO technology offerings must use the Swagger tool to define their interfaces, end points and the respective documentation.	High	In Progress

Table 39: Visualization and Reporting Techniques Component Functional Requirements (Author: SQD)

ID	Description	Priority	Status
FR-S-VIS-001	The TANGO system must enable the hotel manager and the hotel group manager to visualize the reports produced by the analyzed data collected from customers.	High	In Progress
FR-S-VIS-002	The TANGO system should be able to inform the clients about the hotel's sustainability data and environmental footprint in a user-friendly way.	Medium	In Progress
FR-S-VIS-003	The TANGO system should be able to inform the hotel management and the hotel association about their sustainability data and environmental footprint.	Medium	In Progress
FR-S-VIS-004	The TANGO system must be able to allow customers to visualize their own quality report only.	High	Dropped These reports will not be viewed through the VIS component in TANGO platform.
FR-S-VIS-005	The TANGO system must be able to allow the technical expert to visualize quality reports to help them improve the printer operation and the printing quality.	High	Dropped These reports will not be viewed through the VIS component in TANGO platform.
FR-S-VIS-006	The TANGO system must be able to produce visualizations for the reports by the analyzed customer data.	High	In Progress UR-DAR-M1-011 was disassociated from this FR
FR-S-VIS-007	The TANGO system should be able to visually show to supervisors reports of all unauthorized attempts in the platform system.	Medium	In Progress
FR-S-VIS-008	The TANGO system should be able to visually show to supervisors reports of all unauthorized attempts in the platform system.	Medium	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	129 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
FR-S-VIS-009	The TANGO system must allow specific users to visualize data.	High	In Progress

E.2 Non-Functional Requirements

Table 40: User Interfaces Non-Functional Requirements (Author: LST)

ID	Description	Priority	Status
NFR-PER-UI-001	The TANGO UI must response fast to the user actions. Users should not wait long to see the options of the UI or to edit and save attributes. All their actions should be performed in a reasonable amount of time.	High	In Progress
NFR-PORT-UI-001	The TANGO UI should be responsive in order to be able to efficiently work on the majority of the user devices.	Medium	In Progress
NFR-SEC-UI-001	The TANGO UI must implement secure front-end technologies to avoid attacks. The technologies that will be used for implementing the UI must have inherent ways on protecting it from attacks. Furthermore, we should employ techniques that protect the UI from specific UI related attacks.	High	In Progress Newly Identified
NFR-UI-UI-001	The TANGO UI must provide an easily accessible, informative, user friendly and self-explanatory way for the user to access and configure the technical offerings and their attributes.	High	In Progress

Table 41: Visualization and Reporting Techniques Component Non-Functional Requirements (Author: SQD)

ID	Description	Priority	Status
NFR-COMP-VIS-001	The TANGO system must be able to initiate requests to the visualization component or send back responses to it with the appropriate data. Data sources must be accessible.	High	In Progress
NFR-MAIN-VIS-001	The TANGO visualizations component must be maintainable.	High	In Progress
NFR-PER-VIS-001	The TANGO visualizations component should produce the visuals in a timely manner.	Medium	In Progress
NFR-REL-VIS-001	The TANGO visualizations component must present reliable results.	High	In Progress
NFR-SEC-VIS-001	The TANGO visualizations component must be accessed only by certain users.	High	In Progress
NFR-UI-VIS-001	The TANGO system visualizations component should have user friendly UI/UX	Medium	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	130 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

F. System Requirements for the TANGO Integrated Platform

F.1 Non-Functional Requirements

Table 42: TANGO Integrated platform Non-Functional Requirements (Author: INTRA, NOR)

ID	Description	Priority	Status
NFR-COMP-TIP-001	The software components/services of the TANGO system must expose appropriate open and/or easily manageable and secure APIs (e.g., RESTful APIs over HTTPS) to ensure interoperability with other components/services.	High	Done
NFR-MAIN-TIP-001	The TANGO system must be connected with a continuous integration and continuous delivery framework which will ensure that all the components' developments can be smoothly integrated and deployed in an operational context.	High	Done
NFR-MAIN-TIP-002	The updates on the components of the TANGO system should not cause any sort of interruption to the operation of the platform and remain transparent to the end user.	Medium	Done
NFR-PER-TIP-001	The software components of the TANGO system should be packaged and hosted in a way that will ensure efficient resource utilization.	Medium	Done
NFR-PER-TIP-002	The TANGO system should natively support the capability to easily scale the deployed applications according to the dynamic requirements.	Medium	Done
NFR-PER-TIP-003	The TANGO system could support the building of new artifacts (e.g., container images) within seconds.	Low	Done
NFR-PER-TIP-004	The TANGO system could support the components deployment from new artifacts within seconds.	Low	Done
NFR-PORT-TIP-001	The software components of the TANGO system must be packaged appropriately to be easily transferred and deployed to different hosting environments.	High	Done
NFR-PORT-TIP-002	The TANGO system could be able to run on any cloud or on-premise infrastructure.	Low	Done
NFR-REL-TIP-001	The TANGO system must be highly available and fault-tolerant to avoid single points of failure.	High	Done
NFR-COMP-TIP-002	The TANGO system should be able to support a level of automation in decision-making with respect to the deployment environment (cluster) where an application instance should be deployed, according to specific configuration requirements.	Medium	Done
NFR-SEC-TIP-001	The management interface of the TANGO integrated platform must be accessible only for admin members and protected through access restrictions and authentication/authorization measures.	High	Done
NFR-SUST-TIP-001	Each pilot use case must be using only the absolutely necessary components of the TANGO system to operate, eliminating transactions/processes that are not mandatory.	High	Done

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	131 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
NFR-SUST-TIP-002	The software component executables which are integrated in the TANGO platform must be lightweight to eliminate any redundant use of hardware resources and power consumption.	High	Done

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	132 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

G. Privacy, Ethics, Legal, and Societal Requirements

ID	Description	Priority	Status
Data protection principles	Ensure through the use of the TANGO platform the adherence to the principles of “lawfulness, fairness and transparency”, “purpose limitation”, “data minimisation”, “accuracy”, “storage limitation”, “integrity and confidentiality” and “accountability” (article 5 of the GDPR)	High	In Progress
Consent	Ensure that the consent acquisition process is compliant to the relevant privacy and ethical provisions	High	In Progress
Data protection rights	Ensure through the use of the TANGO platform the respect to the data protection related rights foreseen in articles 12-22 of the GDPR	High	In Progress
Data breach event	Ensure that a plan is in place to identify potential data breach events through the monitoring of the use of the platform	High	In Progress
Data security and integrity	Ensure that the appropriate technical and organizational measures are implemented, in respect to the risk-based approach of the GDPR, to ensure data security and integrity	High	In Progress
Data storage	Ensure that the storage of personal data in the platform is limited only to the period necessary, depending on the relevant processing operations.	High	In Progress
Data transfers	Ensure that only the necessary data transfers will take place, depending on the relevant processing operations	High	In Progress
Voluntary participation	Ensure that throughout the piloting activities, the necessary procedures are followed in terms of human participation to ensure ethical compliance. This also applies to the development of trustworthy and ethical AI systems	High	In Progress
Respect to human safety and integrity	The pilot leaders and partners overall shall ensure that there will be no harm caused to the participants, physically or mentally.	High	In Progress
Inclusion criteria	The pilot leaders and partners overall shall implement inclusion criteria regarding the participation of people in the pilots	High	In Progress
Provision of information	The participants receive the necessary information needed relevant to their participation in the pilot(s)	High	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version					Page:	133 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status:	Final

ID	Description	Priority	Status
Ethical AI	The AI components of the TANGO platform shall adhere to the ethical guidelines and considerations related to the development of trustworthy AI	High	In Progress

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	134 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Qs		PARTNER NAME						
		ABILab (banking)	ANYSOL (hospitality)	FMAKE	IDIADA (vehicles)	METRO (retailers)	RIASStone (manufacturing)	VISAR & NOR
PERSONAL DATA	Is the data personal or non-personal, or is it a mixed dataset?	Mixed dataset	Non-personal	Non-personal, only production data from the 3D printer	Mixed	Non personal	The information utilised for RiaStone's dual use cases (UC1 and UC2) comprises of a diverse dataset. This dataset incorporates anonymised details belonging to both individuals and corporate entities	Personal by nature, but in the pilot we will be using only dummy data
	If there are any personal data, please specify which type of data that is (e.g. name, surname, height, biometric data, etc...)	Identification of the recipient's account, Beneficiary account country identifier, Payer's account identifier	None (the one from the hotel will be anonymised)	N/A	Name, surname, company, job position	No personal data	All personal data to be used in the TANGO Demo's, will reside in a protected data repository server, the repository server will deliver on demand, transient data to a cryptographic app, that will generate singular unique	Full name, sex, nationality, birth date, email, phone, purpose of stay (Study, Family, Employment, Language), travel document number, marital status, job title, annual salary, degree, employer

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	135 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Qs		PARTNER NAME						
		ABILab (banking)	ANYSOL (hospitality)	FMAKE	IDIADA (vehicles)	METRO (retailers)	RIASStone (manufacturing)	VISAR & NOR
							anonymous data tokens to serve as data stack identifiers for the information assets to be monitored, and after the token generation is complete will erase the data received from the Cryptographic server.	
	If there are any personal data, please specify whether they belong to one or more of these categories: genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, data on a natural person's sex life or sexual orientation, data revealing racial	Financial data	N/A	N/A	No	No personal data	No	No

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	136 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Qs		PARTNER NAME						
		ABILab (banking)	ANYSQL (hospitality)	FMAKE	IDIADA (vehicles)	METRO (retailers)	RIASone (manufacturing)	VISAR & NOR
	or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning children or vulnerable adults							
	What is the purpose of the processing of the aforementioned personal data?	Anti fraud machine learning detector	N/A	N/A	N/A	N/A	The personal data to be processed will be, solely the RiaStone employee number “SQL primary Key” a.k.a. employee number will be delivered as transient data to a cryptographic app, that will use RSA to generate singular unique anonymous data tokens to serve as data stack identifiers, for the information assets to be monitored, after the token	N/A (dummy data)

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version			Page:	137 of 139	
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Qs		PARTNER NAME						
		ABILab (banking)	ANYSOL (hospitality)	FMAKE	IDIADA (vehicles)	METRO (retailers)	RIASone (manufacturing)	VISAR & NOR
							generation is complete will erase the data received from the Cryptographic server.	
	What are the planned/foreseen actions (processing operations) related to the aforementioned personal data?	Training dataset for local models	N/A	N/A	N/A	N/A	No actions are planned or foreseen / forecasted related with the use of RiaStone employee number	N/A (dummy data)
	Will the processing operations be based in the provision of consent from the participants?	Yes	Yes	N/A (there are no participants in the data set)	Yes	Not needed	All data processing operations will be based in the consent of the participants	Yes (but in the pilot we will use dummy data)
	If no, on which legal basis will the processing operations be based?	N/A		N/A	N/A	N/A	N/A	N/A
	Are the participants informed about their data protection related rights?	Yes	Yes	N/A	Yes	Not needed	All participants will be informed in a face-to-face meeting about their data protection	N/A (dummy data)

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	138 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final

Qs		PARTNER NAME						
		ABILab (banking)	ANYSOL (hospitality)	FMAKE	IDIADA (vehicles)	METRO (retailers)	RIASone (manufacturing)	VISAR & NOR
							rights related with this Tango-Pilot	
	What security measures do you implement as an organisation that could be relatable to the project related activities?	Federated learning, which means all the data are anonymised by design	https protocol	The data will be stored internally, protected by IT security		TBD	Riastone implements regular data protection measures such as administrator granted data access levels	Data encryption, access controls, using Tango component Fides which is designed to process private data in a secure and legally compliant way
	Have you appointed a Data Protection Officer (DPO)?	Yes	No			No	Yes	N/A
	Is there any non-personal data that may be protected under EU, national or contract law? (e.g. trade secrets, statistical confidentiality, etc.)	N/A	No	Sole use public data sets and generation of non-confidential data	No	Yes	Riastone has industrial trade secrets, but there was not an effort for the enumeration, qualification, and listing of the confidentiality scope of those secrets	N/A (dummy data)

Document name:	D2.4 System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment Final Version				Page:	139 of 139
Reference:	D2.4	Dissemination:	PU	Version:	1.0	Status: Final