D2.2 User Needs and Requirements & Use Case Scenarios

Document Identification			
Status	Final	**Due Date**	30/09/2023
Version	2.0	**Submission Date**	30/09/2023

Related WP	WP2	**Document Reference**	D2.2
Related Deliverable(s)		**Dissemination Level (*)**	PU
Lead Participant	LSTECH	**Lead Author**	Evangelos Kotsifakos
Contributors	UPRC, ANYSOL, FMAKE, RIA, SQUAD, IDIADA, VISAR, METRO, ABILAB, UOM, VTT, KUL, NTT, NOR, UTH, UMU, INTRA, QBE, EXUS, UOG	**Reviewers**	Raul Villalba, IDIADA Hugo Steep, Dries Verhees, FMAKE Yin Chen, EGI

Keywords:
Requirements elicitation, user stories, user journey, personas

Document Information

List of Contributors	
Name	Partner
Evangelos Kotsifakos, Pavlos Kalfantis, Tasos Zias	LST
Evangelia Kopanaki, Elena Avatangelou, Asterios Stroumpoulis, Ioannis Katsanakis	UPRC
Dolores Ordóñez, Juan Ortells	ANYSOL
Vasili Schewelow, Darya Skuratova, Andreas Kopysov	VISAR
Dries Verhees, Hugo Steep	FMAKE
George Tsiatiris, Georgia Kyriakopoulou, Giannis Vlachonikoleas, Antonios Giannopoulos	METRO
Paulo Soeiro, Marco Correia; Susana Branco	RIA
Athanasios Stratikopoulos	UOM
Isabela Rosal Santos	KUL
Raul Villalba	IDIADA
Pedro Pina, Pedro Santos, Marisa Brioso	SQUAD
Manca Gianluca, Barbara Cacciamani, Marco Rotoloni,	ABILAB
Luca Mangiagalli, Mario Trinchera, Gisberto Rondinella	NTT
Ville Ollikainen, Anni Karinsalo, Sami Lehtonen, Erik Hieta-aho	VTT
Kristina Thim	NOR
Konstantinos Kentrotis, Cristina Nichiforov	EXUS
Jesus Garcia, María Hernández Padilla	UMU
Ilias Syrigos, Stavroula Maglavera, Apostolos Apostolaras	UTH
Eleni Veroni, Panos Matzakos, Maria Fritzela	INTRA
Niklas Palaghias, Giorgos Sachpatzidis	QBE
Manos Panaousis, Sakshyam Panda	UOG

Document History			
Version	Date	Change editors	Changes
0.11	21/11/2022	Elena Avatangelou, Evangelia Kopanaki (UPRC)	Initial version of ToC with sample material and examples in several sections
0.12	12/12/2022	Evangelos Kotsifakos (LST), Elena Avatangelou, Evangelia Kopanaki, Asterios Stroumpoulis (UPRC)	Integration of first round input from pilot users. ANYSOL, FMAKE, RIA, SQUAD, VISAR, METRO, IDIADA
0.13	31/01/2023	Evangelos Kotsifakos (LST), Elena Avatangelou, Evangelia Kopanaki, Asterios Stroumpoulis (UPRC)	Integration of second round input from pilot users. ANYSOL, FMAKE, RIA, SQUAD, VISAR, METRO, IDIADA
0.14	15/03/2023	Evangelos Kotsifakos (LST), Elena Avatangelou, Evangelia Kopanaki, Asterios Stroumpoulis, Ioannis Katsanakis (UPRC)	Integration of third round input from pilot users. ANYSOL, FMAKE, RIA, SQUAD, VISAR, METRO, IDIADA.

Document History			
Version	Date	Change editors	Changes
			First draft of requirements tables.
0.15	08/05/2023	Evangelos Kotsifakos (LST), Elena Avatangelou, Evangelia Kopanaki, Asterios Stroumpoulis, Ioannis Katsanakis (UPRC)	Pilot requirements text refinement, sections for personas, user stories, journeys, KPIs, ABILAB initial input. Document ready for internal review.
0.16	19/05/2023	Evangelos Kotsifakos (LST), Elena Avatangelou, Evangelia Kopanaki, Asterios Stroumpoulis, Ioannis Katsanakis (UPRC)	Internal review collected and incorporated
1.0	30/05/2023	Evangelos Kotsifakos (LST), Elena Avatangelou, Evangelia Kopanaki, Asterios Stroumpoulis, Ioannis Katsanakis (UPRC)	Final version ready for submission
2.0	29/09/2023	Evangelos Kotsifakos (LST), Elena Avatangelou, Evangelia Kopanaki, Asterios Stroumpoulis, Ioannis Katsanakis (UPRC)	Second version of the deliverable, updated banking pilot use case.

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	Evangelos Kotsifakos (LST)	30/05/2023
Quality manager	Juergen Neises (FSDE)	31/05/2023
Project Coordinator	Tomás Pariente (ATOS)	31/05/2023
Deliverable leader	Evangelos Kotsifakos (LST)	29/09/2023
Quality manager	Juergen Neises (FSDE)	30/09/2023
Project Coordinator	Tomás Pariente (ATOS)	30/09/2023

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AI	Artificial Intelligence
AIV	Autonomous Intelligent Vehicles
AM	Additive Manufacturing
AWS	Amazon Web Services
B2B	Business to Business
B2C	Business to Consumer
CAD	Computer-aided design
CRM	Customer Relationship Management
DCBA	Device Continuous Behavioural Authentication
DoA	Description of Action
DoS	Denial of Service
Dx.y	Deliverable number y belonging to WP x
EC	European Commission
EDAE	Exploratory Data Analysis Engine
EDI	Electronic Data Interchange
ERP	Enterprise Resource Planning
EU	European Union
FEA	Federal Employment Agency
FMS	Factory Management System
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
GPS	Global Positioning System
HD	High Definition
HR	Human Resources
HVAC	Heating, Ventilation, and Air Conditioning
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
ML	Machine Learning
OTA	Online Travel Agency
PMS	Production Management System
PoA	Power of Attorney
QR code	Quick Response Code
R&D	Research and Development
SOTA	State Of The Art
SSI	Self-Sovereign Identity
TASF	Tableware Automated Single Firing
ToC	Table of Contents
Tx.y	Task number y belonging to WP x

Abbreviation / acronym	Description
UCD	User-centred Design
UNWTO	United Nations World Tourism Organization
WP	Work Package
X-AI	Explainable Artificial Intelligence
XML	Extensible Markup Language

Executive Summary

This document presents 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. The main instrument for collecting the requirements was the interviews with the partners responsible for each one of the pilots. Several iterations took place to describe the existing situation, the current weaknesses, the expectations from the TANGO solution and finally the definition of the user requirements, the user stories, including personas and user journeys and the related KPIs.

The current processes and procedures are in detail described in each pilot use case, while the user stories also define the expected, future scenarios that will be implemented using the TANGO solution. For each pilot a list of user requirements is provided, while a summarised table for all of the pilots is also presented.

One of the goals of this deliverable was also to understand the needs of the pilots in relation to the TANGO technical offerings and to provide a first mapping between them. This mapping was also based in material from the deliverable D2.1 “State-of-the-Art & GAP analysis Distributed Data Management Processing and Storage” while dedicated meetings with the technical offering providers and the pilot owners took place to align with the requirements.

The aforementioned outcomes of this deliverable will be used to define the system requirements in deliverable D2.3. They will form the basis for the implementation of the TANGO solution and its application and the validation in the pilot use cases in WP7 “Pilot Demonstration and Validation”.

1 Introduction

1.1 Purpose of the document

This document is a report on the methodology and the techniques that were used for gathering the user requirements from the 7 pilot partners in the 6 thematic areas: hospitality, autonomous vehicles, smart manufacturing (two cases), banking public organisations and retail. Following an intensive, user-centred design process, the document is a comprehensive report on each pilot case, including:

- the existing situation of the pilot partners and related technologies and stakeholders
- the needs and weak points in the existing situation that TANGO should contribute to
- the user and functional requirements
- the personas and uses case scenarios
- the mapping of pilot cases with TANGO technology offerings
- the KPIs for the demonstration, validation and evaluation of the project's pilots

The purpose of the document is to serve as the basis for both technology-related decisions and the planning of the pilot implementations.

1.2 Relation to other project work

This document is closely related to other WP2 deliverables. It has received information from D2.1, SOTA and GAP analysis, where the TANGO technologies were presented and an initial mapping between pilot cases and technologies was attempted. It will contribute to D2.3, System Requirements and Specifications, Platform Architecture, and Privacy, Ethical, Social and Legal Impact Assessment by delivering the user requirements, and an initial functional requirements list, that will serve as the basis for the system specifications.

Moreover, D2.2 serves as the basis for the work to be performed in WP7, Pilot Demonstration and Validation.

1.3 Structure of the document

This document is structured in the following Chapters.

Chapter 2 presents the methodological framework (user centred design process) that was followed for the collection and analysis of information by the pilot partners.

Chapters 3 – 9 present the outcomes of the user centred design process for each pilot partner. In each chapter, the following information is included:

- Pilot case overview.
- Organisations involved.
- Existing Situation Mapping, including a brief description of the existing platform, key Stakeholders involved, main operations flow of the system, data flows, related infrastructure (devices, software, hardware) and their settings in the current system, weak points of the system that can be enhanced, ways TANGO can enhance the system, type of Information required for TANGO.
- User Requirements.
- Use Case Scenarios (Personas and User Journeys).
- Technology offerings used in each use case scenario.
- KPIs.

Chapter 10 presents an overview of findings, namely a summary table for user requirements and proposed functional requirements from all pilot cases, and an overview of technologies mappings with pilot cases.

Finally, **Chapter 11** presents the conclusions of this document and next steps.

2 Methodological Framework

The methodology and techniques that were used for gathering the user requirements in TANGO followed user-centred design principles and tools. User-centred design (UCD) is an approach for designing products, services, and systems that prioritises the needs, preferences, and experiences of the end-users. The primary goal of UCD is to create designs that are intuitive, easy to use, and meet the needs of the user. Throughout the UCD process, designers put the users and their needs at the centre. By involving users in the design process, designers can create products that meet the users' needs and are more likely to be successful in the marketplace.

The UCD process typically involves the following steps:

1. **Understand the User**: In this stage, designers conduct research to gain an understanding of the users' needs, preferences, and behaviours. This can be done through user interviews, surveys, focus groups, and other research methods.
2. **Define the Problem**: Based on the user research, designers define the problem they are trying to solve. This includes identifying the user's pain points, needs, and desires.
3. **Ideate Solutions**: In this stage, designers brainstorm ideas for solutions to the problem.
4. **Prototype and Test**: Once designers have a range of potential solutions, they create prototypes and test them with users. This allows them to get feedback on the designs and make improvements before finalising the product.
5. **Implement**: After the testing phase is complete, designers can implement the final design.

Within the frames of T2.2 and T2.3 (presented in this deliverable), the focus was on the first two steps of the UCD process. More specifically, the following activities took place to understand the users and define the problems:

A. Existing situation mapping

Pilot users were interviewed to discuss the existing situation in each of the pilot cases. The key organisations involved in each pilot case were identified and their role in the pilot implementation was defined. Then pilot partners discussed the current platform/technologies supporting their daily operations and the key stakeholders (internal and external) involved. The current situation analysis continued with a detailed description of the main operations and data flows supported by the existing system and all related infrastructure. This analysis enabled the pilot partners to identify the weak points of their system that could be enhanced with the TANGO platform. Finally, the information that should be shared with TANGO was identified.

B. User requirements collection

Based on the existing situation analysis and the identification of the existing platforms' weak points, it was possible to extract a comprehensive list of user requirements related to the TANGO platform. User requirements are the needs, goals, and expectations of the user that the product or service is being designed for.

The user requirements categories were:

- Trusted user authentication.
- Data access.
- Trustworthy Data sharing.
- Data management.
- Data flow monitoring.
- Data storage.
- Data upload.

- Data analysis and reporting.
- GDPR and related regulation compliance.
- User interaction.
- Protection from cyberattacks.
- Data integrity.
- Process monitoring.

The user requirements were then analysed in categories and prioritised in three levels (high, medium, low).

Based on the user requirements, an initial set of functional requirements was defined for the TANGO platform.

C. Definition of Use Case Scenarios

The next step was to define the key personas for each pilot case, and to develop the user journeys for each persona.

Personas are fictional characters that represent the various user types, needs, and behaviours of a product or service's target audience. They are used to create a deeper understanding of the users' needs, goals, motivations, and pain points. Personas help to humanise the design process, making it easier to empathise with users and to create designs that are more intuitive and user-friendly.

The personas in TANGO included information on the user's demographic situation, their goals, frustrations and pain points, the technologies and tools they use, and representative quotes related to their role in TANGO.

For each persona, the main user journey was developed. A user journey is the series of steps that a user takes to achieve a particular goal or complete a task within a product or service. It involves mapping out the user's experience from their initial point of contact with the product or service, through each interaction and touch point, up to the successful completion of their goal. User journeys are important for designing user-centred experiences because they help designers and product teams understand the user's perspective and identify areas for improvement in the design. By mapping out the user journey, designers can gain insight into how users interact with the product or service, identify opportunities for optimising the user experience, and create designs that are more intuitive, user-friendly, and satisfying.

The user journeys in TANGO monitored the steps and touch points of each persona while performing their tasks. The persona's emotions and context, as well as the related stakeholders were also depicted in the user journeys. This facilitated the identification of the pain points in each journey, and the opportunities for improvement by adopting the TANGO technologies in each case.

D. Technologies used in use case scenario

Based on the user requirements and the user journeys, the process continued with identifying the TANGO technology offerings that could be applied to each use case scenario. To this end, several meetings between pilot and technical partners took place to facilitate the communication and information exchange among project participants. Initially, all technical offerings were presented to the pilot partners in a technical workshop, presenting their key features and their potential use in TANGO. Then, pilot-based meetings took place, where the user journeys were presented, and technical partners had the opportunity to examine whether their technology could be useful to each pilot case. In the next round of meetings, technical and pilot partners discussed in depth their technical offerings, and finally a technology mapping was defined for each use case.

E. KPIs definition.

The last step of the process was to define the KPIs for evaluating the successful implementation of the TANGO platform in each pilot. The KPIs identified in TANGO measure metrics such as accuracy in user verification and authentication, customer and employee satisfaction rate, reduction in time to

perform certain tasks, improvement in data privacy and security, reduction in cybersecurity incidents, etc.

All pilot users were actively involved in the user requirements process through regular, biweekly, online meetings that took place between each pilot, LSTECH and UPRC (between November 2022 and May 2023). In each meeting a specific step of the above process was discussed in detail, analysed and agreed upon. The process was iterative, and pilot users had the opportunity to review and comment on the work performed in previous meetings. In certain cases, technical partners also joined the meetings to discuss in more detail the application of specific technologies in the pilots. This ensured that all information presented in this deliverable presents the pilot use cases (existing and future) accurately and captures the users' requirements in the best possible way.

3 Pilot 1: Smart Hospitality

3.1 Pilot case overview

The first pilot is about Smart Hospitality will be implemented in the task T7.2 in the months M24 – M36 of the project. In this task, CESGARDEN SL (CESGA), a world leader in luxurious smart hospitality, will offer the facilities in Spain to the project to pilot the TANGO framework in the context of smart hospitality. ANYSOL and AHOP given their expertise in smart hospitality will lead and assist in the implementation of the smart hospitality pilot. Guests' identity data will be securely handled by the TANGO platform with GDPR compliance without the fear of exposing identity information to staff or others. 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 evaluate the correctness of the operation such as impersonation, while also providing feedback regarding the user satisfaction and their overall experience with the framework.

CESGA is a Mallorca's hotel chain which has been recognised at international level thanks to their initiatives in circular economy. Indeed, the circular hotel initiative has been recognised by UNWTO as an international best practice for the tourism sector. Digitalisation is fundamental for the tourism industry and especially for the hotel sector.

The TANGO framework will be implemented in one of the hotels of this chain in Mallorca.

ANYSOLUTION (ANYSOL) and ASSOCIACION HOTELERA DE PLATJA DE MURO (AHOP) given their expertise in smart hospitality will lead and assist in the implementation of the smart hospitality pilot. AHOP will be more focused on the dissemination part and transfer of project results to the hotel chains they are representing while ANYSOL will lead the task and will be managing the technological and non-technological implementation of the pilot.

The ultimate goal of providing a seamless, comfortable and secure customer experience is to allow the guests to check-in to the hotel through their smartphone and to go directly to their room, without having to go through the time-consuming process at the reception. Currently, apart from the technological limitations, there are other factors that do not allow such a process and they are related to the state regulations that require the guest to check-in through the reception to ensure the legitimate access to the hotel and to also allow the gathering of the personal data necessary to identify the guests. In alignment to these regulations[1] and at the same time trying to move closer to achieving the above mentioned goal, the quests in the TANGO pilot will use a tablet available at the reception to provide their personal preferences and other personal information. This information along with data gathered from sensors inside the rooms, will be used to configure the room conditions (the lights and the HVAC in the room based on their presence in the room for example) and to also provide recommendations to the guests about gastronomic offers at the hotel or other activities of their interest. The collected information will be also analysed and through the TANGO pilot application the guests will be informed about their contribution to the circularity principles of the hotel. The guests will be able to see the positive impact they make in the energy saving and in the organic waste management and sustainability sectors.

Guests' identity and personal data will be securely handled by the TANGO platform in a GDPR compliant way, preventing their exposure to the staff or others as it will be detailed in the respective technical requirements of each technical offering. The personalised configuration will be loaded at the guests' room without the danger of exposing their personal data. The pilot will have a 4-month duration with two phases. During the pilot, the users/guests, who will be pre-selected persons as it will be

[1] Organic Law 4/2015, of 30 March, on the Protection of Citizen Security.

Order INT/1922/2003 of 3 July on books-registers and entry forms for travellers in hotel and catering establishments and other similar establishments.

Royal Decree 933/2021, of 26 October, which establishes the documentary registration and information obligations of natural or legal persons who carry out accommodation and motor vehicle rental activities.

described in detail in the pilot implementation work package, will be using the system to evaluate the functionality of the system through a number of tests, like trying to impersonate another guest or by exchanging smartphones containing different user data. At the same time, they will also provide feedback regarding the user satisfaction and their overall experience with the framework.

3.2 Organisations involved

3.2.1 AnySolution

AnySolution is a Spanish SME that develops strategic methodologies and projects in the field of Research, Development and Innovation. The company specialises in tourism and Smart Cities. It is member of the SmartDestination Working Group in the University of the Balearic Islands, and vice-president and member of the executive committee of TURISTEC (International ICT -tourism cluster) and president of PLANETIC (technological platform on ICT) and it is a member of other international technological platforms. AnySolution is a member of the FIWARE community and of AIOTI. AnySolution is co-founder of the Digital Innovation Hub of the Balearic Islands for Artificial Intelligence and Tourism (DIHBAI-TUR), and now manages the technical office of DIHBAI-TUR. AnySolution has been recognized as an Innovative SME (PYME Innovadora) by the National Ministry of Economy, Industry and Competitiveness. It holds the vice-presidency of Gaia-X Spain and leads the Tourism Working Group.

AnySolution has a large track record of EU projects management. It has 2 main departments: innovation strategies and engineering. As technological developments, AnySolution has developed a data-driven platform called NADIA which is being used to contribute to the digital transformation of smart destinations and the digitalization of the agrifood sector, among other functionalities.

3.2.2 Playa De Muro Hotel Association

The Hotel Association of Playa de Muro (Associacion Hotelera De Platja De Muro (AHOP)) was founded in 1978 and represents 30 of the 32 existing hotel establishments in the area and its 16,400 hotel beds. Regarding the members, it should be noted that the majority of the establishments (22) are 4-star hotels and the rest are 5 and 3-star hotels, belonging to 20 different hotel chains, such as: Iberostar, Viva H, Grupotel, Garden H, Prinsotel, Zafiro H, Allsun, Bq H, Bg H, Eix H.

The mission of the Hotel Association of Playa de Muro is to act as a lobby to create synergies between the different actors in the value chain of the tourist experience and to optimise the quality of the destination.

In Tango, AHOP will support the pilot implementation and be active in dissemination activities.

3.2.3 Garden Hotels

Garden Hotels is a family business from Mallorca founded in 1986, with more than 30 years of experience in the hotel business. Thanks to the entrepreneurial character of the president (Mr. Miquel Ramis), the support of his family and the business vision of the team, the chain has been able to reinvent itself and currently has eleven 3- and 4-star hotels in four Spanish destinations: Mallorca, Menorca, Ibiza and Huelva, with a wide range of services and a great national and international gastronomic offer. Garden Hotels' establishments, with more than 4,900 beds, are aimed at four main segments: family holidays, adults-only holidays, sports holidays and wellness holidays.

The characteristics that differentiate Garden Hotels are the specialisation in the sun and beach segment, the excellent location of their hotels, the quality of the service offered by their more than 650 employees and the satisfaction of their guests.

Special mention for Garden Not Common.

Garden Not Common is the programme that puts a face to the entire sustainability programme that Garden Hotels have been carrying out since their beginnings. Since then, back in 1986, they have established solid values based on innovation, hospitality, commitment, enthusiasm, trust, quality and, of

course, sustainability. They were pioneers in the field of circular economy almost without knowing it, putting into practice certain actions aimed at taking care of their land and their people.

The first step was to become the first hotel chain to put into practice an action that today may even seem obvious: converting the organic waste generated in their establishments into ecological compost and, in this way, closing the circle of the circular economy by producing fertiliser and at the same time promoting ecological agriculture in the Balearic Islands.

This was the first step of many others and of all those that remain on this exciting path towards environmental sustainability.

Their commitment is real: real actions with real impact. As seen in the following list:

Nº1: To make ecological compost in a self-sufficient and profitable way for its use.

Nº2: Revitalise organic farming and the local economy.

Nº3: Make the good practices and actions of hotel chains and associations visible to the rest of society.

Nº4: To involve social enterprises in the project.

Nº5: To reduce environmental and transport costs.

Nº6: To reduce the carbon footprint in the transport of organic matter and pruning.

Nº7: Create alliances with different sectors (agricultural, hotel and municipal).

3.3 Existing Situation Mapping

3.3.1 A brief description of the platform

Tourism is a complex industry that consumes and produces huge amounts of data. Considering that people are at the centre of this industry, most of the data produced and consumed is personal data.

In our pilot, we are going to focus our activity in the hospitality sector, implementing it in one of the Garden Hotels located in Mallorca.

Customers and hotel companies exchange many data and legal documents among them to improve and enhance the tourism experience and to comply with sectoral regulations. There also are various other entities which participate at this exchange such as tour operators, travel agents and local authorities (e.g., police). This is because the booking systems require a huge amount of personal data to be able to deliver the service.

Hotels have different booking channels: the direct one is the one in which clients book the hotel room directly at the hotel's web. But this is not the most popular one. In fact, in the Balearic Islands, it is being worked extremely hard to reduce the dependency on tour-operation, which still represents more than 50% of the total bookings of the island. But then there are other channel managers with Online Travel Agencies (OTAs) and travel agencies that are offering the hotel, therefore, when a booking is done, they are asking for all kinds of personal details.

In fact, clients coming from a direct channel are already registered in the CRM of the hotel, but for the ones coming through other channels, the hotel has no data from them.

As mentioned in the beginning, the Spanish law requires that clients go through reception to register. At this moment, a copy of their ID/passport is sent to the police department.

Digital transformation in the tourism sector has been accelerated due to two main factors: the COVID pandemic and the fact that tourists are digital. COVID has accelerated the introduction of new digital solutions in the tourism sector based on the use of new and advanced technologies. On the other hand, tourists use digital solutions even before the travel experience. Tourists use smartphones and tablets before, during and after their stay generating and consuming large amounts of data. The tourism experience will be enhanced thanks to the combination of technologies and data that will allow the improvement of the personalisation of the tourism experience.

The acceleration of the digital transformation and the fact that tourists are using more digital and online services to enhance their experience increase the need for new applications provided by the hotel companies, tourist agencies and local organisations, that will provide recommendations, personalized content and ways to organize visits and touristic experiences.

Another key point is sustainability, especially after COVID19, there is an increasing demand for respectful and conscient tourism. So, all issues related to plastic recycling, energy efficiency and food waste management are starting to be requested by the new tourists. All these areas represent a huge challenge in this industry.

Playa de Muro, as a tourism destination, the Hotel Association of Playa de Muro, Anysolution and Garden Hotels are committed to the implementation of sustainability and sustainable actions for the protection and respect of the environment and the society. In fact, as mentioned in the summary of garden Hotels, they have been pioneers in the circular hotel initiative in which organic waste is transformed into compost for the Mallorcan farmers. They are also very well-known for the promotion of local products and the use of these products as a gastronomic offer in their restaurants.

3.3.2 Key Stakeholders involved

In this subsection we list the different stakeholders that are involved in the pilot implementation. They will be further described and analysed in the personas and user journeys subsection.

1. Hotel client.
2. Hotel receptionist.
3. Experience provider.
4. Hotel manager.
5. Hotel Group Manager.

3.3.3 Main operations flow of the system

Today, due to the different booking channels that exist, hotels have no control of the data flows. In most of the cases, hotels do not receive the information of their clients and the establishments do not have any information on the public preferences. Commonly, the clients book the hotel through a travel agency, OTA, or Tour-operator directly. Many times, the clients know the hotel chain, but they do not know exactly the hotel in which they will be during their holidays.

In the booking stage, OTAS and tour-operators are the controllers of the personal data of clients as well as their travel preferences. So the hotel cannot adapt the promotion campaigns or be in contact with their clients.

3.3.4 Data flows

The user data are gathered mainly by tour-operators, Online Travel Agents (OTAS) or travel agencies, and only a small percentage of the booking is done by the direct channel through the official web of the hotel chain.

When carrying out the booking, clients are asked about their preferences, but this information is not shared with the hotel. Tour-operators, OTAs and travel agencies use the data gathered to personalise their promotional campaigns and be in contact with the clients.

When clients arrive at the hotel, they present their ID/passport to the reception and they use it to fill in a paper form. In most of the cases, this information is not introduced in the CRM, so the hotel does not know who its client is and which their preferences are.

3.3.5 Related infrastructure

No infrastructure apart from the CRM of the hotel.

The hotel is using the NADIA PLATFORM, provided by ANYSOLUTION for handling and combining data from various sources into a single point of analysis and reporting. NADIA is not only limited to a storage software solution, data analysis and visualisation. NADIA is composed of a set of software and

hardware solutions ranging from the sensor that takes the data, the gateways that process it and the different technologies to send the information from the EDGE to the CLOUD. NADIA is a FIWARE-based platform.

3.3.6 Weak points of the system that can be enhanced

The hotel is not storing the client's data and they do not know their preferences. Without having this information, it is overly complicated to develop personalised services and to enhance the tourism experience.

On the other hand, clients are not sure about how their personal data is being managed and preserved when they give them.

Without data flows that allow the hotel to learn more about the clients while preserving their privacy, it is not possible to offer personalised services.

The departure point is that clients are not used to offer their preferences to the hotels, so it is very important to define an easy-to-use system that allows the hotel to fulfil the tourists' preferences during their stay.

3.3.7 Ways TANGO can enhance the system

The TANGO platform will provide a unique experience to customers, allowing them to have their own personalised room through the use of specific interfaces on their smartphones and other smart devices. The platform will also provide personalised proposals for local activities and businesses, helping to increase customer satisfaction and strengthen the local economy and society. Due to the sensitive and large amounts of data that will be exchanged, the TANGO platform will also provide strong security and data privacy measures to ensure the safety of the customers' information.

Through the platform, customers will also be connected to the local society and small businesses, contributing to the financial and social pillars of the community.

Through the implementation of the TANGO platform, ANYSOL will be able to help to create a unique and personalised experience for hotel clients, while also contributing to the local economy and society. The platform will also help to reduce food waste and provide strong security and data privacy measures to protect customers' information.

3.3.8 Type of Information required for TANGO

Type of Information that we should collect and use:

- Check-in data,
- Personal account / data,
- Intermediates and data exchange,
- Preferences (activities, drinks, foods, etc.),
- Client needs for use of smart hotel and IoT applications (specific applications),
- Sustainability activities / actions / policy.

3.4 User Requirements

The system developed should be a non-intrusive system that generates alarms/messages to customers in the way they have preselected.

Code	**UR-TUA-HT-001**
Category	**Trusted user authentication**
Description	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.
Priority level	High

Code	**UR-DMN-HT-002**
Category	**Data management**
Description	Hotels must be able to collect clients' personal data directly through the web (direct booking).
Priority level	High

Code	**UR-DMN-HT-003**
Category	**Data management**
Description	The hotel must be able to collect the clients' preferences in order to provide them with personalised services.
Priority level	High

Code	**UR-DMN-HT-004**
Category	**Data management**
Description	The hotel must be able to collect data from rooms, hotel facilities, logistics information, etc.
Priority level	High

Code	**UR-DMN-HT-005**
Category	**Data management**
Description	The hotel must collect data from the various systems that it uses (e.g., CRM, NADIA, etc.).
Priority level	High

Code	**UR-DMN-HT-006**
Category	**Data management**
Description	The client must be able to evaluate the recommendations received by the system.
Priority level	High

Code	**UR-DMN-HT-007**
Category	**Data management**
Description	The client must be able to evaluate the overall experience.
Priority level	High

Code	**UR-DMN-HT-008**
Category	**Data management**
Description	The experience provider must have access to the hotel's suggestion system to provide and enter data and information about the provided experience.
Priority level	High

Code	**UR-DAR-HT-009**
Category	**Data analysis and reporting**
Description	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.
Priority level	High

Code	**UR-TDS-HT-010**
Category	**Trustworthy Data sharing**
Description	The users must feel safe when they share their data.
Priority level	High

Code	**UR-GCO-HT-011**
Category	**GDPR and related regulation compliance**
Description	The customer's data must be handled according to GDPR.
Priority level	High

Code	**UR-PCY-HT-012**
Category	**Protection from cyberattacks**
Description	The customer must feel safe when uploading his/her personal data.
Priority level	High

Code	**UR-DMN-HT-013**
Category	**Data management**
Description	The hotel should be able to collect and record the clients' preferences during their stay.
Priority level	Medium

Code	**UR-UIN-HT-014**
Category	**User interaction**
Description	The client should be able to choose among various suggestions based on their preferences (food, activities, etc.).
Priority level	Medium

Code	**UR-UIN-HT-015**
Category	**User interaction**
Description	The client should receive personalised information based on his/her preferences and other external data sources (e.g., weather, monuments or activities schedule, etc.).
Priority level	Medium

Code	**UR-DAR-HT-016**
Category	**Data analysis and reporting**
Description	The clients should be able to be informed about the hotel's sustainability data and environmental footprint in a user-friendly way.
Priority level	Medium

Code	**UR-DAR-HT-017**
Category	**Data analysis and reporting**
Description	The hotel management and the hotel association should be able to be informed about their sustainability data and environmental footprint.
Priority level	Medium

Code	**UR-DMN-HT-018**
Category	**Data management**
Description	The users must be able to access data/information from external sources (weather, monument or activities schedule, etc.).
Priority level	Low

Code	**UR-TDS-HT-019**
Category	**Trustworthy Data sharing**
Description	The hotels of the same chain could be able to share customer information and profiles in a secure way.
Priority level	Low

3.5 Use Case Scenarios

Hotel clients who visit Playa de Muro expect a comfortable room and good services to complement their tourist experience. Receptionists are responsible for the direct contact with clients during check-in and check-out and support them with any needs or requirements they may have. Experience providers are also responsible to design activities to enhance the tourism experience and promote them at hotels.

On the other hand, the Hotel Manager is responsible for the daily management and operation of the hotel, ensuring that clients receive a high level of service and overall enjoy their tourism experience. They monitor various KPIs to ensure the hotel is performing well. In addition, the Group Hotel Manager is responsible for the daily management of all hotels in the group, ensuring that clients receive the same quality of service in all hotels. They also monitor various KPIs to ensure the group's hotels are performing well. To be able to further evaluate all these criteria, different personas and user journeys will be part of the use case regarding smart hospitality.

3.5.1 Personas

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
ANYS_01	**Hotel client**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*

Erika Schmidt German 35 years old Works as a businesswoman in the industrial sector Has 10 years of experience	*"The quality of the services received during our stay was awesome."* *"We enjoyed the best quality of the room and premises ever."* *"Incredible experience at an astonishing place."* *"Thanks to this hotel we had the possibility to taste and know the local products of the island."* *"Good atmosphere all around without massification in the common areas."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Wonderful experience Convenience Relax Enjoy the free time Seamless travel Nice and comfortable room Good service from professional workers Updated information on the hotel and activities in the surrounding areas	Long waiting times (reception, in the restaurant, if they ask something at the room service) Lack of variety in the buffet restaurant Massification (in the common areas) Lack of information (about the surroundings, attractions, etc.) Has to enter all personal details everywhere repeatedly. Is concerned, how long her data will be stored in different systems and if there can be any abuse of the data.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Apps Smart devices SSI module	Erika is a returning customer to the specific hotel, and to other hotels in this group. She enjoys being welcomed as a returning customer, with all the benefits of the hotel "knowing" her as a customer.
SHORT DESCRIPTION	
Hotel clients are usually tourists that visit this part of the island to relax and enjoy the nice weather, great beaches and different leisure activities offered by the various experience providers in the area. They expect to have a comfortable room and to receive good services, as well as to complement their tourist experience during their stay at the hotel. By using SSI manager, Erika can conveniently provide only required information about herself, while being certain that the information is used for that purpose only and won't be stored after her visit.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
ANYS_02	**Hotel receptionist**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Maria Vargas 30 years old She has 3 years working experience. She is fluent in English, German and French. She is trained on the digital systems of the hotel.	*"Client satisfaction is always first."* *"I like the nice working atmosphere in the hotel."* *"It helps my job when I have all the potential required information in a single App/tool to provide the best services to our clients."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Increase client's satisfaction Organise the work in an efficient way Reduce number of complains Be prepared for any question/need Reduce waiting time in reception	Stressed when too many clients arrive at the same time Lacking information requested by tourists Clients complaints Lack of good communication channels with other workers (e.g. cleaning room staff…)
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
CRM (computer) Web/app (browser, weather app, etc)	Maria would be delighted, if clients could have convenient self-service options, in addition to being able to ask the reception.
SHORT DESCRIPTION	
Receptionists are the people having direct contact with clients when they arrive at the hotel for check-in and check-out. They also support clients with any need, requirement, complaint that clients may have.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
ANYS_03	**Experience provider**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Jose Martinez 40 years old 15 years of experience in the tourism sector He is fluent in languages English, German, French	*"I want to provide our customers with the best experiences ever."* *"We offer great experiences at the best price."* *"Digital technologies make things easier."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Offer the best tourism experience Develop new and attractive tourism experiences Increase the number of clients Social media reputation Improve efficiencies in terms of offer/demand matching (including schedule and number of people) Balanced cost/benefit Good relations with relevant other enterprises in the proximity for win-win.	Clients not informed about their offer Clients not satisfied Client expectations not met Number of potential clients is unknown until the last minute. Problems to organise resources Other enterprises in the proximity have sometimes kept the competitors informed first.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Web Social media App (paper)	Wide variety of offers Easy to use format
SHORT DESCRIPTION	
Experience providers offer activities at each destination to enhance the tourism experience. They design these experiences and then promote them at large hotels, so that receptionists and concierges suggest them to potential clients who ask for recommendations.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
ANYS_04	**Hotel manager**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Francisco Gomez 40 years old He has previously worked in different hotels with distinct positions He has 7 years of experience in hotel management He has a high-level education and specialised training in hotel management He is fluent in English, German and French. He is trained on the digital systems of the hotel.	*"I want our hotel to have the reputation of the best hotel at the best destination."* *"I want to provide high quality services to our clients."* *"I want all clients to leave the hotel satisfied."* *"Our hotel is all you need to enjoy and relax."* *"It is important to me that I manage a sustainable and circular hotel."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Increase clients satisfaction (loyalty – returning customers) High quality in all the hotel services Reputation Economic benefits Sustainability	Clients not satisfied Hotel brand is not known Regulations Seasonality High resources consumption Lack of qualified staff
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
CRM/ PMS/ NADIA/ TANGO	
SHORT DESCRIPTION	

The Hotel Manager is responsible for the daily management and proper operation of the hotel. His goal is to ensure that clients receive a vast number of services at their destination, and overall enjoy the tourism experience. The Manager regularly monitors certain KPIs about the hotel's operation, the hotel's energy consumption, the client satisfaction, etc. The hotel is part of a chain/group, which should offer similar services to all clients, either new or returning.

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
ANYS_05	**Hotel Group Manager**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Manuel Rodriguez 45 years old He has 5 years of experience as a group manager but was a hotel manager for 10 years. He had previous experience in different positions in the same hotel chain. He has a high level education and a master's degree in Tourism Management.	*"I want our hotel chain to have the reputation of the best hotels at the best destinations."* *"I want to provide high quality services to our clients."* *"I want all clients to leave our group hotels satisfied."* *"Our hotels are all you need to enjoy and relax."* *"It is important to me that I manage a sustainable and circular hotel group."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Increase tourists' satisfaction (loyalty – returning customers) High quality in all the hotel services Reputation Economic benefits Sustainability Same services in all hotels of the chain	Clients not satisfied Hotel brand is not known Regulations Seasonality High resources consumption Lack of qualified staff Lack of interoperability among the hotels of the chain Lack of overall picture from all hotels of the chain
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
CRM / PMS/ NADIA/ TANGO	
SHORT DESCRIPTION	
The Group Hotel Manager is responsible for the daily management of all hotels in the group. His goal is to ensure that clients in all hotels receive the same quality of services at their destination, and overall enjoy the tourism experience. The Group Manager regularly monitors certain KPIs about the group's hotels operation, energy consumption, client satisfaction, etc.	

3.5.2 User Journeys

PERSONA:	Tourist/ hotel client				
	JOURNEY STAGE	**TOUCHPOINTS/Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Arrives at Mallorca airport. Travel to the hotel to check-in.	Device (mobile, tablet, web)	Does not like waiting Anxious to arrive as soon as possible to the destination	Public transport Rent a car Bus Hotel Tour operator	People arrive in Mallorca to relax and enjoy themselves. The airport is located in Palma and the hotel is on the other side of the island. They will be arriving with great expectations and tired from the trip.
2.	Fills-in the check-in form.	Check-in form online at hotel device TANGO Platform	Prefers not to provide the same information multiple times.	Receptionist	The client can either fill-in the check-in form at a hotel device, on their own smartphone, or transfer their identity information automatically through TANGO.
3.	Provides preferences at the reception. The client gives information about their room settings preferences, interests, hobbies, restaurant/ food preferences, what they would like to see/visit on the island, etc.	Tablet at the reception Or on the client's smartphone TANGO Platform	Eager to start the holidays. Would like this to be a quick process. Honoured when "recognised" and greeted as a returning customer.	Receptionist Concierge	The information should be saved for returning customers, or for customers visiting different hotels of the same chain.
4.	Goes to reception desk to sign check-in document	Reception, formal documents (physical)	Tired from the travel. They are not willing to fill in thousands of documents again	Receptionist Tour operator	All hotel clients must go through reception to show their identification documents and sign the check-in form. Required by Spanish law.
5.	Goes to hotel room	Sensors in place gathering information from the room and adapting the conditions of the room to the client's preferences.	Feel like home	Hotel Tech provider	The room will be at the temperature desired by the client. The presence sensors will inform if the client is in the room to inform the cleaning services. Sustainability in saving energy, water consumption

PERSONA:	Tourist/ hotel client				
	JOURNEY STAGE	**TOUCHPOINTS/Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
6.	Goes to the hotel restaurant. Based on their preferences, they are directed by the hotel app to the organic part of the buffet.	App Waiters TANGO Platform	Willing to taste local products	Hotel Tech provider Local products producers	Hotel clients want to test local products. Sustainability is key, and the circular hotels initiatives use organic waste. Information if offered through hotel's app
7.	The client wants to go for an excursion. The system recommends based on their preferences to visit Cabo Formentor. The client accepts the recommendation and receives more information on their phone. They book a place at the group tour through the app.	App Reception NADIA Experience provider TANGO Platform	Willing to complement their tourist experience with an excursion.	Hotel Reception Tech provider Concierge	Hotel clients want to know about the destination. The app recommends experiences provided by the experience providers based on their profile and preferences.
8.	The clients check-out. A summary of the client's stay is sent to the client's phone: about energy and resources consumption – CO2 footprint (positive mindset), about the experience they selected during their stay. The client evaluates the overall experience through the app (room, tours, visits, etc.).	App Reception TANGO Platform	Sorry to leave. Overall satisfied with their stay and experience.	Hotel Reception	The client's stay summary (preferences, experiences, evaluation) is stored in their profile, to be used in future visits to this hotel, or other hotels of the same chain.

PERSONA:	Hotel receptionist				
	JOURNEY STAGE	**TOUCHPOINTS/Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Prepares the reception to welcome the clients	App CRM PMS	Good mood and prepared for an intense activity	Other hotel workers External providers	The hotel receptionist should have everything ready for welcoming clients. All rooms

PERSONA:		Hotel receptionist			
	JOURNEY STAGE	**TOUCHPOINTS/Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
				Tourism experiences providers Technology providers	should be prepared and assigned to each client based on their category and requirements
2.	Receives clients for the check-in.	App Tablet Internal software	Good mood (sometimes quite stressed)	Other hotel workers External providers Tourism experiences providers Technology providers	All rooms should be prepared and assigned to each client based on their category and requirements. Rooms should be offered in the fastest way possible.
3.	The client's check-in information is filled automatically through their TANGO identity.	TANGO Platform	Happy to go through the process quickly		The client only needs to sign the check-in form. Personal documents should be scanned and sent to the national police.
4.	The receptionist provides recommendations and information to the client about potential visits and other services provided by the experience providers.	App Tablet Internal software TANGO Platform	Good mood (sometimes quite stressed)	Other hotel workers External providers Tourism experiences providers Technology providers	Clients should go to the reception to solve their doubts on the destination and to get some recommendations on places to visit.
5.	Prepares the check-out.	Internal software	Good mood (sometimes quite stressed)	Technology providers	Farewell of the clients in the fastest way possible.
6.	A summary of the client's stay (preferences, experiences, evaluation) is stored in the hotel system anonymously.	TANGO platform			This is to improve the recommendations algorithm.

PERSONA:		Experience provider			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Design of the tourism experience in collaboration with the local providers.	Local providers Hotels	Be open minded and flexible	Hotel Local providers	Knowledge of the local attractions and local providers to offer attractive tourism experiences. The local providers are key in the tourism experience.
2.	They are in contact with hotels to advertise their experience for hotel clients.	Hotels	Seriousness	Hotels Local providers Tourism associations	Information campaigns to hotels to explain the tourism experiences they are offering.
3.	The hotel approves the experience. The experience provider gets access to the platform. They enter the experience information on the TANGO platform to be accessed by both Hotel Receptionist and hotel clients.	Hotel TANGO Platform	Interested in knowing the experience that is offered	Hotels Local providers	The hotel evaluates the experience offered to ensure that it has high quality for their clients.
4.	The experience providers offer the tourism experience to the hotel clients that have received the recommendation and have booked a seat at the tour.	Hotels	Passion nervous	Local providers Tech providers	Deliver the tourism experience. Organise the visit. Go with the clients

PERSONA:		Hotel manager			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	It is Monday morning and the Manager logs in to the hotel platform to receive the weekly report.	CRM TANGO Platform	Passion Seriousness		The hotel manager wants to be informed on anything happening at the hotel. He is also accountable for certain KPIs regarding the operation and energy consumption of the hotel.

PERSONA:		Hotel manager			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
2.	The manager accesses the weekly report about the hotel's energy consumption, evaluation of recommendations for experiences by the clients, client satisfaction, any problems reported, economic impact, sustainability indicators, etc.	CRM TANGO Platform			
3.	The Manager follows up on complaints, requirements, customer loyalty management (e.g., voucher or discount for energy efficient clients)	CRM Hotel Workers PMS Internal software	Passion Seriousness	Hotel workers	The hotel manager wants to ensure that all clients are satisfied with the hotel experience and will be visiting again as returning customers.
4.	The hotel group manager accesses the platform to review the same reports, but on a group level.	TANGO Platform			The Group Manager has different access rights due to his profile and position.
5.	The hotel group manager can identify trends, patterns and associations between specific customer traits/preferences, to adjust/personalise the hotel group's services and (marketing) policies.	TANGO Platform (EDAE)	Eagerness to identify gaps and opportunities	Hotel employees Clients Sales department	The Group Manager lacks the overall picture from all hotels of the chain.

3.5.3 Technology offerings used in use case scenario

TECHNOLOGY OFFERING	RELATION TO PILOT
Trustworthy Data Sharing	Customers will get a personalised view of Offerings, based on the behaviour of their peers. Hotels using the TANGO system may also collaborate exchanging their UBEM data, to increase user satisfaction in the region, or even sell the data (which is privacy-preserving by nature and only offered as aggregated and anonymised data) to third parties (e.g., information that if customers have been interested in Offering A, they might be interested in Offering B as well)
Confidentiality and Privacy by Design	Attribute-based policies and sticky policies can be used to protect data shared through CRM boundaries (e.g., with experiences…) User/data controller can control who has access to the data throughout its lifetime.
Self-sovereign Identity Management	Hotel employees get access to ABE encrypted guest data using SSI credentials to get access to ABE key. Hotel employees (Organization members) need to be issued with organisation credentials. Enable guests to perform remote identity verification through their mobile phone, to be able to bypass the check-in process at the hotel. SSI Module enables the user to manage his data and provide only necessary information for the accommodation provider. Interfacing with PEC and PAT. The user is aware of what information is shared, to whom, and for how long.
Seamless Onboarding for Users and Devices	The User onboarding will constitute the mechanisms for seamlessly and securely allowing people (both guests and hotel employees) to onboard to the SSI. In particular , guests will be able to onboard to the SSI in order to perform remote identity verification before arriving at the hotel. The onboarding will take place through the TANGO wallet that will incorporate the user onboarding mechanism through an SDK. For device onboarding, a particular mechanism will be employed for onboarding devices based on public decentralized identifiers and their verification based on DID authentication following a zero trust approach.
User Continuous Behavioural Authentication	The component allows strong access control at the TANGO wallet to ensure that only the owner of the wallet has access and is able to showcase and verify the SSI based verifiable credentials. The component leverages multiple behavioural characteristics of the user, such as the way the user is moving, the way the user uses the device, biometrics and other behavioural patterns in order to continuously authenticate the user. Through the continuous secure assessment of the authenticity of the user, the users will have the ability to use the TANGO wallet to verify their identity at various places of the hotel.
Hardening against Side-channel Attacks	Make side-channel attacks harder, to prevent an attacker to find encryption keys used by the room sensors. The use of sensors in the rooms could create a potential way for an attacker to perform a side-channel attack that would allow him to find encryption keys used for the communication between the sensors and the NADIA platform. This could allow an attacker to get information about customer preferences, or even to modify the sensor information transmitted to the platform. As such, hardening against side-channel attacks seems to be relevant for smart hospitality context.

	CEA will provide countermeasures to increase the security with respect to these attacks.
Exploratory Data Analysis Engine	Integration with NADIA hotel system for data preparation. The EDAE may provide: - statistics on the customers' traits and preferences - associations, trends and patterns among customers' traits and preferences. Hotel Managers will be able to receive statistics and analysis reports on the data collected across all hotels. Both Receptionists and Hotel Managers will be able to see patterns, trends and associations between a client's traits and preferences and those of other clients. Anonymisation of collected data so that specific data details (e.g. nationality, gender and booking dates) do not lead to identification of specific individuals.
Dynamic Intelligent Execution on Heterogeneous Systems	TornadoVM will be indirectly used for the hardware acceleration of the data analytics that will be performed within the EDAE engine in the context of this pilot.
Privacy Threat Modelling and Identification for Trustworthy AI	The following functionalities that could be supported from the PAT component (to be further investigated and finalized in D2.4): In user side: ▸ Fill-in the requested data (ex. personal data) ▸ Preferences (activities, drinks, foods, etc. in smart hospitality use case), ▸ Data policies and privacy awareness. ▸ Monitoring privacy risks of the requested data In organization side: ▸ Request the data (ex. personal data) ▸ Data policies Data policies and privacy awareness.
Infrastructure Management based on AI	RENOPS could utilised in two ways (to be further investigated and finalized in D2.4). First way would be directly via RENOPS scheduler script, that would find most optimal time to schedule backups, analytics, or AI model training. Second way would be indirectly as part of other related and energy intensive jobs as part of WP5. One possibility would be as part of T5.1 EDAE, where it could be used to shift the calculations and would be specifically beneficial in cases where calculations are periodic.

3.6 KPIs

TITLE	DESCRIPTION
Reduction in energy consumption	KPI measuring the improvement in energy efficiency / energy consumption after the adoption of TANGO
Accuracy of user verification and authentication > 99.6%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate and failure to access.
Accuracy of device verification and authentication > 90%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate and failure to access.

Customer satisfaction rate	This KPI measures the level of satisfaction of the customer based on the overall experience and the interaction with the hotel.
Guest satisfaction regarding the room/facilities > 90%	Improvement in guest satisfaction regarding room facilities controlled / suggested by TANGO
Reduction in check-in time > 50%	Reduction in check-in process duration with the use of the TANGO platform
Employee satisfaction	This KPI measures the level of satisfaction that hotel staff, including receptionists and experience providers, have with the TANGO platform and their ability to provide quality service to customers.
Local business engagement	Measure the number of local businesses that are engaged through the TANGO platform, to demonstrate the platform's contribution to the local economy.
Data privacy and security	Ensure that the TANGO platform is meeting high standards of data privacy and security, as this is critical for maintaining customer trust.
Brand reputation	Track the impact of the TANGO platform on the brand reputation of the hotel, to ensure that it is positively contributing to the overall image of the hotel and the ANYSOLUTION brand.

4 Pilot 2 - Autonomous Vehicles

4.1 Pilot case overview

The second pilot is about Autonomous Vehicles, and it is to be implemented in the task T7.3 between the months M24 – M36 of the project.

In this pilot, IDIADA will provide the appropriate infrastructure to implement the pilot of the Autonomous Vehicles. IDIADA will offer autonomous vehicles to the project to allow the integration of the TANGO distributed identity and trust management as well as the validation of the solution through a pilot. A workshop will take place prior to the pilot in order to offer hands-on and state-of-the-art cyber security training and exercises to the participants. The pilot will take place in Spain and/or the UK for an overall duration of 8 months and will be split into two phases with 4- month duration each:

a) Phase 1: initial deployment and evaluation of the TANGO framework where users feedback is collected;

b) Phase 2: having received the feedback from the users and performed the appropriate improvements and optimisations, the final phase of the pilot will be executed.

The TANGO framework will be evaluated in terms of the identity and trust management such as sharing the autonomous vehicles among trusted users, exploiting on board IoT devices, loading personalised preferences on the vehicle configuration etc.

4.2 Organisations involved

4.2.1 IDIADA

IDIADA is a global partner to the automotive industry with over 30 years' experience supporting its clients in product development activities by providing design, engineering, testing and homologation services.

IDIADA provides comprehensive design, engineering, and validation services for vehicle development projects. In the electronics department, the ADAS & CAV team performs R&D activities, with an important role in several EU projects.

Within the testing and validation services IDIADA provides to their clients, IDIADA has available digital maps of their facilities so that the clients can perform simulations on the same scenario they can test physically.

In the TANGO project, IDIADA's role will be offering the tools (Autonomous vehicles) so that the TANGO framework can be tested in this environment and helping on its integration and validation.

IDIADA has the need to protect and licence their digital maps, so TANGO could provide a solution to such a need, which will be provided for the Pilots by IDIADA.

In addition, IDIADA needs to comply with the GDPR regulations on the data sets generated by the multiple sensors equipped on the vehicles. To do so, blurring and anonymization is needed.

4.3 Existing Situation Mapping

4.3.1 A brief description of the platform

Autonomous vehicles share data with other cars and users, companies. The purposes include identifying passengers and other cars, "read" the road, etc. So, there is a tremendous need to ensure that all these data are secured from any leak and possible modifications.

IDIADA has developed its own "robo-taxi": It is called CAVRide. The CAVRide works as a self-driving taxi inside IDIADA's facilities. A smartphone app is available so the user can call the taxi, and the car goes autonomously to the place where the user is waiting.

So, there are different data exchanges present in the process: user to car, car to user and environment to car. The car uses its sensors to scan the environment and uses HD maps together with its GPS positioning to know its location in real-time inside IDIADA's facilities.

There is a need to protect this data exchange. TANGO will work on providing solutions to guarantee that the needed data sharing is done following the best practices, guaranteeing further security to the information and citizens.

These data are uploaded to a cloud platform (AWS) via cellular, using IDIADA's private network.

4.3.2 Key Stakeholders involved

In this subsection we list the different stakeholders that are involved in the pilot implementation. They will be further described and analysed in the personas and user journeys subsection.

The different groups of stakeholders are:

1. Autonomous vehicle passenger.
2. IDIADA client. IDIADA as maps supplier.
3. IDIADA client: OEM or other companies which IDIADA works for.
4. Developers and maintainers: Engineering team in charge of the system.

4.3.3 Main operations flow of the system

The following steps summarise the main operation flow of the current system.

- The user calls the car using an app installed on their smartphone.
- The information is sent to the car via cellular and a cloud platform.
- The information goes from the cloud infrastructure to the car.
- The car receives the information, and starts sending back information to the user.

Parallelly:

- The car gets the information from the server (user's requests and HD Map)
- The car sends information to the cloud infrastructure and then information gets back to the car.

In more detail:

- The user sends a request for a ride through the mobile application to the server.
- The server sends the request to the car with the location of the user and the maps.
- The car gets the info from the server, and using information also from its sensors, it drives itself to pick up the user.
- The car sends information to the user through the app (e.g., location, speed, ETA…).
- The car picks-up the user and the user sets the destination – which is a list of predefined locations.
- The car interacts with the server sending its location.
- When the car arrives at the destination, the driver is getting out and the car stays there. An IDIADA employee later drives the car into the parking space or the car is sent to another location to pick-up a new user, following the same steps.

4.3.4 Data flows

While the system is running, the car is updating its position and status to the cloud server. If the car is available, it can be summoned by any user (the vehicle is parked on its location while there is no service to provide). The user's data are generated on a smartphone app. The data go to the cloud server. The request is automatically evaluated in the cloud, and if the logic is met (availability of the vehicle, correct state, etc.) it forwards the request to the car.

Once the car gets the request, the car accepts the request, and the server starts to send the car information to the user (location). The data flows from the car to the server to the user and doesn't finish until the process has finished (Successful arrival to the destination, user asks for an early stop or emergency stop by the system).

Parallelly, while the vehicle is driving, it is gathering data with its sensors. The data are processed on the on-board unit, and they are also uploaded to the cloud using IDIADA's private network for further use. Details on the data to be uploaded will be defined in the pilot implementation phase of the project.

4.3.5 Related infrastructure

In brief, the related infrastructure can be depicted in the following figures.

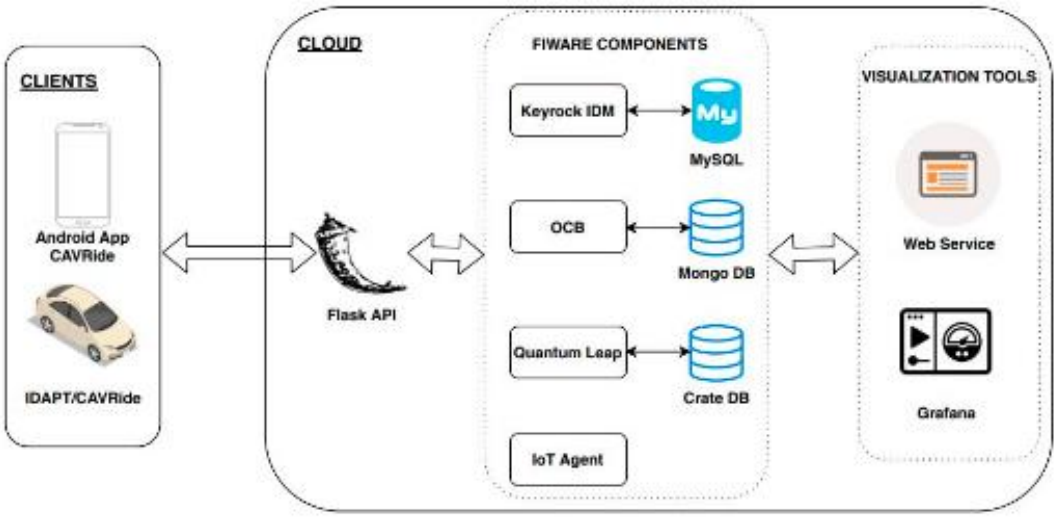


Figure 1 IDIADA Robo-taxi smartphone application

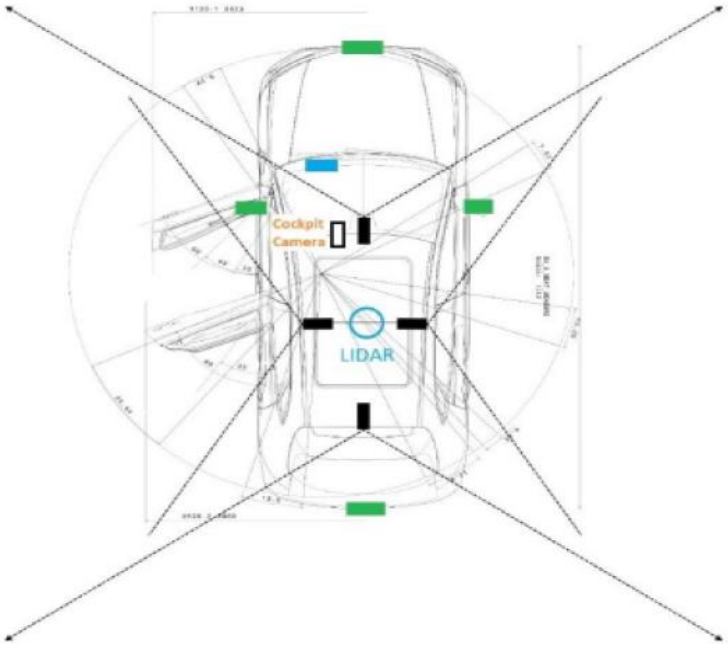


Figure 2 Vehicle sensors setup

- 4 SVM cameras (Basler a2a1920-51gc PRO)
- 1 central LiDAR (Ouster OS2-128)

- 1 Continental Radar (ARS430)
- 1 cockpit camera (Logitech C930E)
- 1 Smart eye for driver behaviour analysis
- 2 Data logging setups based in
  - RT MAPS (dSPACE)
  - Vector
- Occupant tagging tablet
  - FOT Monitoring
  - ADAS events
- 5G router

4.3.6 Weak points of the system that can be enhanced

The data flow should be protected from possible attacks. However, there are some vulnerabilities that will be points of further attention in TANGO. The project intends to work on mitigation measures for avoiding:

- Any kind of modification on the user's request can change the car's behaviour, arising multiple risks.
- It is needed to ensure that the request has been done by a trustworthy user.
- The communication between the user device and the vehicle needs to be protected.
- Any kind of modification on the HD maps, can make the car go off the track, even crashing.
- Since the HD maps are used by IDIADA's clients to perform simulations, there is a need to protect such maps (virtual test tracks). IDIADA would like to explore the possibility of applying blockchain to protect those maps.
- Data collected by the sensors and stored in the cloud also need to be protected. It is needed to apply blurring for anonymization. It would be interesting to be able to apply low energy consumption algorithms.

4.3.7 Ways TANGO can enhance the system

Tango, through its platform, will be able to provide the company with data protection and privacy, trusted user authentication, and the ability to manage all these data with flexibility. It will also contribute to the energy efficiency, because IDIADA could apply optimal algorithms to perform anonymization on the raw data.

TANGO should protect the data flow (communication user-server, car-server).

TANGO should provide a solution for protecting IDIADA's virtual maps.

4.3.8 Type of Information required for TANGO

Data that are going to be needed are:

- Communication data from the interaction among the autonomous vehicles.
- Smartphone application input data and specifications.
- Communication data need to be exchanged with IDIADA infrastructure.
- RAW data from the sensors.
- IDIADA's virtual maps.

The data from the sensors consist of video streams, point cloud data, radar data and so on. It means that the amount of data can be some GB per minute of recording. The data format is still to be defined. It could be RTMaps (dSpace), MF4 (Vector), ROS, ROS2.

4.4 User Requirements

For the pilots, the user must be at IDIADA's facilities. With their smartphone, the user asks for the Autonomous vehicle to pick them up. The user must be able to see at any moment where the vehicle is.

It means that trustworthy communication must be provided. Currently it is using the toolchain provided by Fiware, https://www.fiware.org/, (from the EU project "SecureIoT").

Once the vehicle has arrived at the requested meeting point, the user selects where they want to go. They must feel safe all along the way. The vehicle must drive giving the user the confidence that it is safe. So, the user should be able to get all the information in real time.

IDIADA clients should be sure that the digital maps IDIADA share with them are trustworthy. Blockchain protection would be the best option from IDIADA point of view. Thus, IDIADA is currently working on applying blockchain for this purpose.

Since IDIADA must comply with GDPR requirements, anonymization algorithms will be applied to the raw data. Thus, as a rule, only anonymized data will be stored. Personal data will only be processed for the necessary purposes, that will be informed to the users.

Code	**UR-TUA-AV-001**
Category	**Trusted user authentication**
Description	The user must be authenticated through the application on smartphones or other smart devices (tablets, etc.).
Priority level	High

Code	**UR-DIN-AV-002**
Category	**Data integrity**
Description	The autonomous vehicle passenger must feel safe and relaxed during the ride.
Priority level	High

Code	**UR-PCY-AV-003**
Category	**Protection from cyberattacks**
Description	The autonomous vehicle passenger must feel safe and relaxed regardless of any external threat during the ride.
Priority level	High

Code	**UR-PCY-AV-004**
Category	**Protection from cyberattacks**
Description	The management must feel safe that the car is protected and cannot be accessed by malicious intruders.
Priority level	High

Code	**UR-DUP-AV-005**
Category	**Data upload**
Description	The engineering team must be able to upload sensor data to the system in a trustworthy way.
Priority level	High

Code	**UR-GCO-AV-006**
Category	**GDPR and related regulation compliance**
Description	The engineering team must be able to upload GDPR compliant sensor data to the system.
Priority level	High

Code	**UR-DAC-AV-007**
Category	**Data access**
Description	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).
Priority level	High

Code	**UR-TDS-AV-008**
Category	**Trustworthy Data sharing**
Description	The automotive services company must be able to prevent their customers from sharing their maps with third parties.
Priority level	High

Code	**UR-PCY-AV-009**
Category	**Protection from cyberattacks**
Description	The automotive services company must be able to control if somebody modifies the content of the files (the maps).
Priority level	High

Code	**UR-DAC-AV-010**
Category	**Data access**
Description	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).
Priority level	Medium

Code	**UR-TDS-AV-011**
Category	**Trustworthy Data sharing**
Description	Clients should be sure that the digital maps are trustworthy.
Priority level	Medium

Code	**UR-PCY-AV-012**
Category	**Protection from cyberattacks**
Description	The automotive services company could be able to control and monitor any attempts of cyberattacks.
Priority level	Low

Code	**UR-DMN-AV-013**
Category	**Data management**
Description	The engineering team could be able to change the data real time.
Priority level	Low

Code	**UR-DMN-AV-014**
Category	**Data management**
Description	The autonomous vehicle passenger could be able to request a change during the ride.
Priority level	Low

Code	**UR-UIN-AV-015**
Category	**User interaction**
Description	Clients could be able to use a smart device via a user-friendly interface to use the autonomous vehicle.
Priority level	Low

4.5 Use Case Scenarios

The challenge for IDIADA is to protect the data exchange between the car and the cloud platform. They knew that the data could be vulnerable to cyber-attacks, and they need to ensure that it was secured from any leak. To do this, they have a team of developers and maintainers who were responsible for the system's security.

The passengers who used the CAVRide are not only testing the technology, but they are also experiencing a new way of transportation. IDIADA had to ensure that the passengers feel safe and secure while using the car.

IDIADA's clients are also an important part of the project. As maps suppliers, they have to set the access policies to the files, and they are responsible for ensuring that the maps are up-to-date and accurate. The companies that worked with IDIADA have to trust that the data is secure and reliable against any attempt of cyberattacking.

4.5.1 Personas

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
IDIADA_01	**Autonomous vehicle passenger**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Mark Smith 35 years old Has a taxi company	*"I'm excited to have a trip on an autonomous vehicle, but I'm also a bit worried. I may feel anxious on the ride"*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Mark has a taxi company and is interested in expanding his business with autonomous taxis. He wants his taxi customers to feel comfortable, safe and relaxed during the ride.	How does this experience work? Will the car crash? Will the car get lost? Will the car run over any pedestrian?
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**

Android mobile app.	
SHORT DESCRIPTION	
The autonomous vehicle passenger can be any person using the robo-taxi to test the technology or have a new experience. Although they use the car in a controlled environment, still there are many factors that cause anxiety regarding the safety of the vehicle, as this is a new technology and a new experience for them.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
IDIADA_02	**IDIADA client: IDIADA as maps supplier**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
IDIADA. Automotive services company.	
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
They want to control who is using their maps, allowing access to the maps for a certain period of time.	Nowadays they cannot control who has access to the maps, and cannot avoid sharing it with a third party. They cannot control if somebody modifies the content of the files (the maps).
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
SHORT DESCRIPTION	
They are the maps providers, so they need to set the access policies to the files (maps).	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
IDIADA_03	**IDIADA client: OEM or other companies which IDIADA works for**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Automotive company developing (and testing) automotive vehicles / ADAS functions.	"We need to use IDIADA's facilities maps knowing that we can trust it has not been modified"
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
They want to use the digital maps on their vehicles / on their simulations for testing purposes.	They do not know if the map has been modified.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
SHORT DESCRIPTION	
They are the ones that use the maps.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
IDIADA_04	**Developers and maintainers: Engineering team in charge of the system**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Engineering team in charge of the data upload to the cloud.	"We are worried on the GDPR compliance of the data we are uploading to the cloud"
GOALS	**FRUSTRATIONS / PAIN POINTS**

(what he/she wants to achieve)	*(what frustrates him/her currently at work)*
They want to upload the sensors' data to the cloud in a trustworthy way, being GDPR compliant.	Disclosure of personal information
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
AWS API SSI	
SHORT DESCRIPTION	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
IDIADA_05	**Cyber-attacker (interested on the car)**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
A cyber-attacker interested in taking control of the vehicle. Call it to its place, so that they can modify the car, steal any component / the vehicle itself.	"I want to take control of the car so that I can steal it."
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
To be able to call the car to a third location.	
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
SHORT DESCRIPTION	

4.5.2 User Journeys

PERSONA:		Autonomous vehicle passenger			
	JOURNEY STAGE	**TOUCHPOINTS/Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT/ TECHNOLOGIES USED**
1.	Arrives to IDIADA premises	IDIADA's representative	Excited to try the autonomous vehicle	IDIADA's engineering team	
2.	Gets a smartphone with robo-taxi app installed from IDIADA's representative.	Smartphone Robo-taxi app IDIADA's representative TANGO platform			IDIADA's representative explain them how it works.
3.	Uses the smartphone app to call the car to its location.	Smartphone Robo-taxi app	Curious for the new experience		
4.	Once the car arrives, they get into the car.	Autonomous vehicle Smartphone Robo-taxi app	Anxious about getting into the vehicle without a driver		
5.	Once in the car, they select the destination on the car's touch-screen.	Autonomous vehicle touch-screen	Excited Anxious Afraid about the car being hacked		
6.	The car starts the ride, so the user enjoys the ride.	Autonomous vehicle Smartphone Autonomous vehicle touch-screen	Relaxed Excited		The user sits on the car, and meanwhile they get information on the car's screen.
7.	The car arrives at the destination.				

PERSONA:		IDIADA client: OEM or other companies which IDIADA works for			
	JOURNEY STAGE	**TOUCHPOINTS/ Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	The client asks IDIADA to provide their maps.			IDIADA provider.	
2.	IDIADA employee sets the access rights and time period for the specific client.				
3.	The client gets access to the maps.				
4.	The client uses the maps on their systems. The platform monitors that the files have not been tampered.			IDIADA provider	IDIADA sets the access right and the accessibility period.
5.	The access period expires. The client is no longer able to use the maps.				They no longer have access to the maps. The usage period has expired.

PERSONA:		Developers and maintainers: Engineering team in charge of the system			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	They have data collected by the vehicle sensors and cameras to be uploaded to the cloud.				
2.	They blur the faces and licence plates from the videos.				
3.	They encrypt the data collected by the vehicle sensors and cameras.				
4.	They upload the data to the cloud.	Usage of AWS API.			

PERSONA:		**IDIADA_04:** Cyber-attacker			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	The attacker gets access to the robo-taxi mobile app	Robo-taxi smartphone app.			
2.	They attempt to log-in.	Robo-taxi smartphone app.			They should not be able to log-in into the system.

PERSONA:		IDIADA_04: Cyber-attacker			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
3.	If they eventually succeed on logging-in, they try to call the car to their location.	Robo-taxi smartphone app.			
4.	The platform identifies that the device behaviour is not as per usual and blocks access to the vehicle.	Robo-taxi smartphone app.			

4.5.3 Technology offerings used in use case scenario

TECHNOLOGY OFFERING	RELATION TO PILOT
Trustworthy Data Sharing	Evaluating the Trustworthiness of the car's system based on security monitoring results provided by the car's system, and the CAVRide service or app bearing device as an extension, e.g., based on behavioural authentication. Cars share data among themselves, and Cars communicate with an interface to humans. Establishing Trustworthiness is a critical component.
Confidentiality and Privacy by Design	Ensuring privacy during data sharing (e.g., data from users and their preferences or maps) Users GDPR rights will be ensured through proper access control and user consent. Sticky policies and related identity-based techniques may be used to ensure that only allowed entities may decrypt data. For instance, only (specific) cars may decrypt user's service preferences or allow clients to decrypt maps.
Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms	For data encryption during data uploading to the cloud. Maps will be encrypted while stored on the cloud for advanced protection.
Self-sovereign Identity Management	SSI Module enables the user to manage his data and provide only necessary information for the vehicle (and further to other vehicles/users). SSI used to get access to ABE Keys. The car system can be a candidate to authenticate itself by SSI to get access to ABE Keys to get access to encrypted driver data. The driver shares preferred payment, and car preferences from a mobile wallet to the cars system.
Seamless Onboarding for Users and Devices	This components enable both users and devices to onboard to the SSI Management and then securely verify their identity. For users the primary focus in on verifying the identity of drivers and other relevant people e.g. passengers of the vehicle. The users will be able through the TANGO wallet app to verify their identity based on their passport and create the verifiable credentials required for their identity verification when accessing various aspects of the autonomous vehicle. For the devices that are already integrated in the autonomous vehicle, the solution could allow the onboarding of these devices and thus the secure communication with the rest of the vehicle.
User Continuous Behavioural Authentication	
Device Continuous Behavioural Authentication	Create device behavioural patterns based on operational measurements such networking metrics and power consumption. DCBA mechanism will assess the behavioural performance of a device based on power consumption and network analytics --and will be able to detect deviations in comparison to their normal operation based on specific performance efficiency metrics (e.g. power consumption, RSSI, network traffic metrics) and infer whether a specific operational behaviour is suspicious or not. So, the DCBA mechanism will be able to assess the continuous

	authentication procedure and enable the authentication of the trusted user while sharing cars among them.
Privacy Threat Modelling and Identification for Trustworthy AI	PEC will assess the impact of cyber threats from a privacy perspective. It will quantify the impact, helping IDIADA to combine the privacy risk score with their cyber risk assessment and to better prioritise the threats and select countermeasures. PEC will assess the privacy risks and potential impact of data sharing activities. As it is a requirement by GDPR to perform privacy impact assessment, PEC will assist IDIADA with the implementation of the privacy impact assessment and thus complement their effort towards complying with GDPR.

4.6 KPIs

TITLE	DESCRIPTION
Reduction of privacy violation incidents in data sharing	Privacy assessment results comparison of existing infrastructure with TANGO proposed data sharing platform.
Accuracy of user verification and authentication > 99.6%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate, and failure to access.
Accuracy of device verification and authentication > 90%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate, and failure to access.
>20% reduction in autonomous vehicles' accidents	Measurement of accident reduction.
Feeling of safety regarding the driving experience	Improvement in customer feeling of safety before and after the TANGO implementation
Passenger satisfaction	This KPI measures how satisfied passengers are with the services of IDIADA. It can be measured through surveys and feedback from the passengers and can be used to determine how well the company is meeting its clients' needs and expectations.
Employee satisfaction	This KPI measures the satisfaction of IDIADA's employees with their jobs, work environment, and company culture. It can be measured through surveys and feedback from employees.
Cybersecurity	This KPI measures the effectiveness of IDIADA's cybersecurity measures in protecting sensitive data from cyber threats. It can be measured through penetration testing and vulnerability assessments and can be used to determine the company's ability to protect its clients' data.
Customer satisfaction in accessing and using the maps	Measurement of customer satisfaction based on metrics such as speed and ease of access, feeling of safety.

TITLE	DESCRIPTION
Reduction of time to access maps	Average time to grant access to new map files requested by customers.

5 Pilot 3 - Smart Manufacturing – Case 1

5.1 Pilot case overview

The third first pilot is about Smart Manufacturing and it is to be implemented in the task T7.4 during months M24 – M36 of the project. This pilot has two sub-cases, one about additive manufacturing[2] and a second one about industrial shop floor security. This chapter analyses the case of additive manufacturing.

Flanders Make (FMAKE) will provide a manufacturing scenario to pilot the TANGO solution 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.

5.2 Organisations involved

5.2.1 FMAKE

Flanders Make (FMAKE) is a research centre aiming to establish the bridge between the academic and industrial expertise in Flanders. It has built up extensive experience from various research projects. It has also been involved in many consulting activities for industrial partners. For almost a decade, FMAKE has been performing research activities for additive manufacturing (AM). FMAKE has been focusing on monitoring and controlling the AM process with the objective to achieve better productivity and increasing the robustness and print quality, which leads to the reduction in scrap (waste) and costs.

Additive manufacturing is used in a variety of industries (aerospace, medical, etc.) where data confidentiality is critical. Managing access rights and privacy is important when printing information is made available externally.

FMAKE has a single-laser LPBF industrial printer, which will serve the pilot case in TANGO, that is equipped with advanced in-situ monitoring technologies as well as the ability to control the printing process through different controllers. Using these rich sensory data, FMAKE has been developing advanced AI based algorithms to create a digital twin of the printing process.

In TANGO, FMAKE will contribute to the context of its digital twin (a virtual model that is designed to accurately reflect a physical object) for quality assurance, which runs partially on the edge and partially in the cloud. FMAKE will focus on the data efficiency in terms of data management/storage/sharing and privacy preserving of their digital twin.

5.3 Existing Situation Mapping

5.3.1 A brief description of the platform

FMAKE has additive manufacturing infrastructure which allows research into a variety of topics. It is an open and modular platform that allows printing in metal (stainless steel), using selective laser melting. The infrastructure is built on top of an industrial 3D printer with building volume of 275 x 275 x 400 mm, hence the experiments and findings are relevant for industrial players.

The additive manufacturing infrastructure is used in a variety of projects, either internally or externally funded.

[2] Additive manufacturing (AM) or additive layer manufacturing (ALM) is the industrial production name for 3D printing, a computer controlled process that creates three dimensional objects by depositing materials, usually in layers.

The goal of the pilot case is to achieve smooth data sharing between the customers and the printing company. The paragraph below explains the typical interactions and perspective for the three stakeholders.

- Company_A is a customer of the printing company
- Company_B is a customer of the printing company
- Printing company has two customers: Company_A and company_B.

In those cases, both customers are creating a new design and want to have it printed by the printing company. The flow is illustrated below:

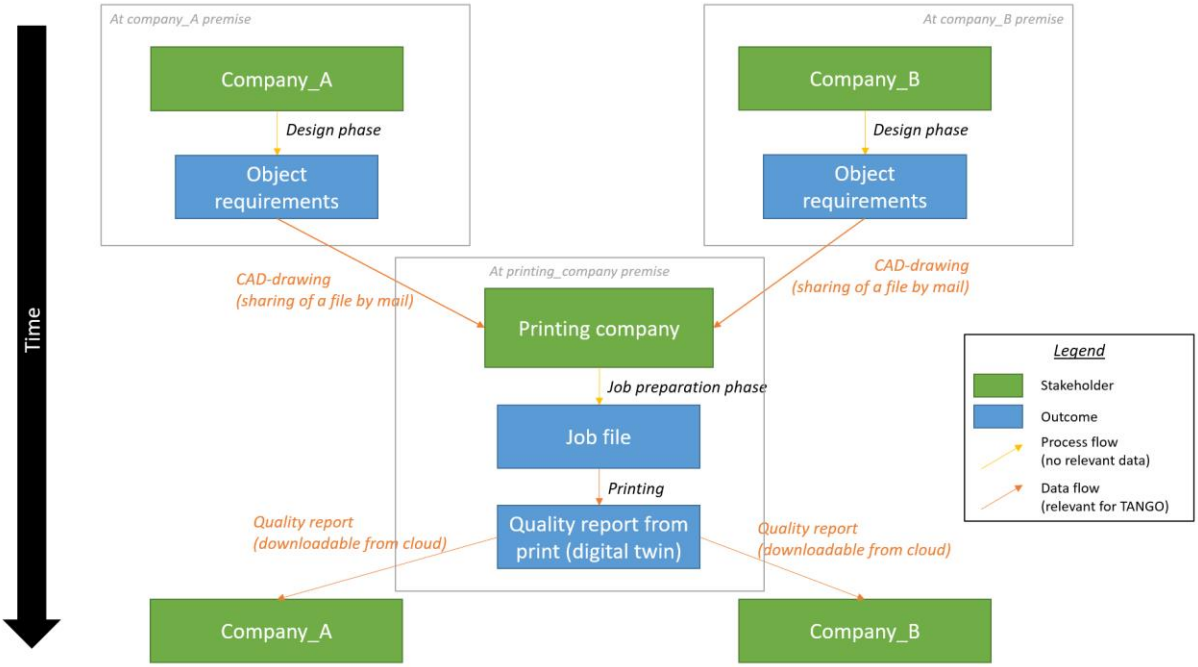


Figure 3 FMAKE data flow and data processing

Every company stakeholder wants to share their data (CAD-drawing) in a secure manner with the printing company. Although it is happening nowadays by mail, it is preferred through an online application. The printing company gathers the data from all company stakeholders (company_A, company_B) into a combined data container. This is happening during the job preparation phase. After the printing company executes the print, the printing company wants to share the quality report in an efficient manner with every company stakeholder, without revealing data/information from the other company. Please note that the quality report will include information from the initial CAD-drawing, so only a subset needs to be shared with the respective IP owners (company_A, company_B). TANGO can enhance this data sharing in an efficient way, with preserving the IP ownership. The company stakeholders want to view their own quality report, as illustrated in the figure below.

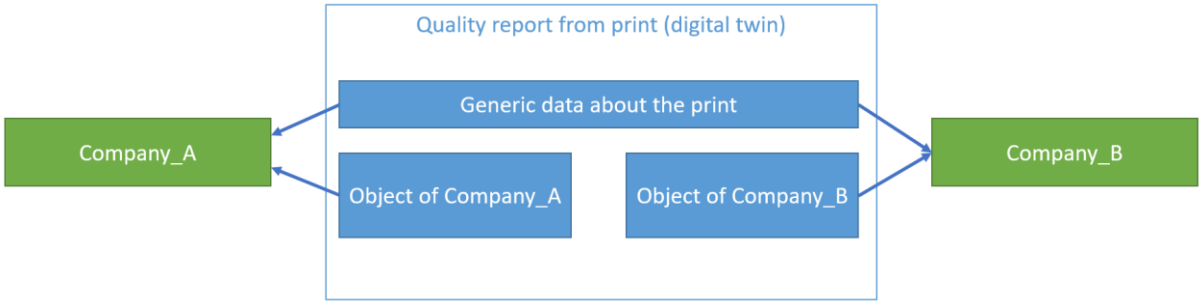


Figure 4 FMAKE report generation and sharing

The following section describes the data formats that are being used in this pilot case.

The job file consists of several files:

- One XML file which contains the overall information; including printing parameters.
- For each object, a binary file with an unknown structure, so not readable. This file is not used in the data flow after the print is finished.

An example of the XML-file is given below. The <*Parts*>-section lists all the objects that are being printed, together with their volume, specified in millimetres. This information is relevant to correlate the digital twin information back to their respective owners.

```
<Parts>
    <Part>
        <ID>0</ID>
        <Name>sample009</Name>
        <Dimensions>
            <Xmin>111.500</Xmin>
            <Ymin>111.500</Ymin>
            <Zmin>0.000</Zmin>
            <Xmax>118.500</Xmax>
            <Ymax>118.500</Ymax>
            <Zmax>7.500</Zmax>
        </Dimensions>
    </Part>
    <Part>
        <ID>1</ID>
        <Name>sample010</Name>
        <Dimensions>
            <Xmin>111.500</Xmin>
            <Ymin>131.500</Ymin>
            <Zmin>0.000</Zmin>
            <Xmax>118.500</Xmax>
            <Ymax>138.500</Ymax>
            <Zmax>7.500</Zmax>
        </Dimensions>
    </Part>
```

Figure 5 XML sample of print job file

Although it is technically possible, it can be assumed that the objects do not intersect for the TANGO pilot case, since this is valid for almost all prints.

The information below shows the general structure of the XML-file where only the Parts-section is relevant for the quality report. It is desired that the other sections remain on the edge (local network) as they might contain sensitive information. The parsing of the XML file needs to happen on the edge on only the relevant information can be transferred to the cloud.

<BuildJob>

<JobID>…</jobID>

<Parts>…</Parts>

…

</BuildJob>

The digital twin consists of a list of binary files. A single binary file is created for every layer, where a layer corresponds with a fixed height (z-coordinate). One could use the following formulate to derive the height in millimetre:

$$height = layer_{index} * 3e^{-2}$$

The layer index is encoded in the file name. For example, the digital twin information will have the following files:

- Layer0000.bin
- Layer0001.bin
- Layer0002.bin
- Layer0003.bin
- …

These files typically have a size of a couple of megabytes, but it can increase in case video footage is included. It is fair to assume a maximum size of 100MB will be used during the pilot. These files are internally structured as follows:

- The first bytes are reserved for the header; containing mainly a version number and other metadata. This data is not relevant for this pilot case, so the header info can be ignored.
- The remaining bytes represent an array of items where each item consists of a fixed number of bytes. Each item has the following data items:
    - Relative timestamp: uint64
    - X-position in millimetres: float32
    - Y-position in millimetres: float32
    - Laser Power: uint32
    - Laser Speed: uint32
    - Quality_feature_1: uint32
    - Quality_feature_2: uint32
    - Quality_feature_3: uint32

  Note that the amount of quality features might change, but this should not impact the flow and structure of the data.

This file can be parsed using numpy.memmap in Python; but other tools can also be selected.

The flow of the different files is illustrated in the diagram below:

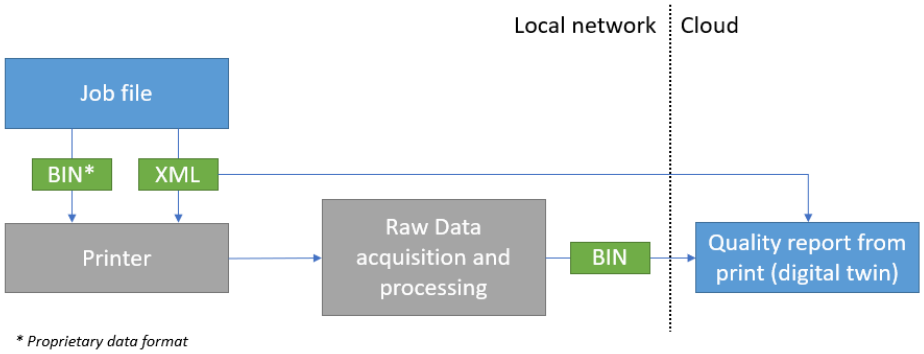


Figure 6 FMAKE flow of the different files

The job file consists of two underlying files, of which the binary file is proprietary and is only used by the printer itself. The xml file can be parsed and the relevant section is explained above. The xml-file is useful to match the coordinates from the printing process onto the processed data (bin-file per layer) of the quality report.

The quality report itself consists of several 2D visualisations which illustrate the quality (linking to the features *Quality_feature_1*) for every layer. The image below shows the (x,y)-visualisation of a single layer from a cylindrical object:

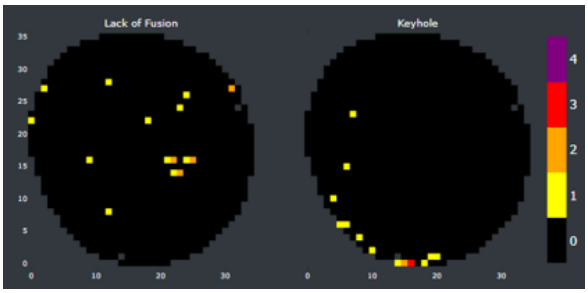


Figure 7 FMAKE quality report visualisation

The same data is visualised on a phase diagram for every layer:

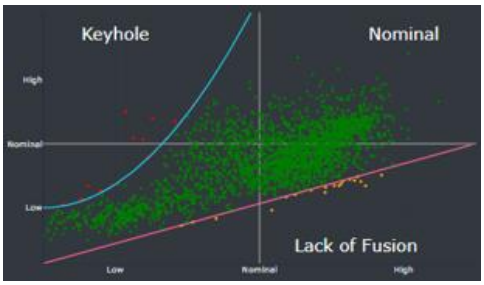


Figure 8 FMAKE quality report visualisation

Finally, the quality features are visualised in function of the layer.

Figure 9 FMAKE quality report visualisation

5.3.2 Key Stakeholders involved

In this subsection we list the different stakeholders that are involved in the pilot implementation. They will be further described and analysed in the personas and user journeys subsection.

1. Printer operator (working for FMAKE)
2. Technical expert (working for FMAKE)
3. Printer customer
4. Data Scientist (working for FMAKE)

5.3.3 Main operations flow of the system

For additive manufacturing, the main operation flow consists of several steps:

1. **Design step**
   The customer designs a part that needs to be printed. This is typically done in design software on the computer. The outcome of this step is a CAD-file, which is sent to the printing company.
2. **Print preparation**

The printing company combines different designs (CAD-files) into a single print job to increase the productivity of the printing machine and reduce lead times. The outcome of this step is a job file which is uploaded to the printer.

3. **Print execution**
   The print job is executed to print multiple designs in a single build area. While printing, monitoring data is generated and analysed for real-time quality indicators.
4. **Print post-processing**
   The parts are removed from the build area and finished afterwards.

The steps above describe the general high-level flow in a commercial environment. Within TANGO, FMAKE will perform the relevant steps in their laboratory.

5.3.4 Data flows

The operation flow is explained in the previous section. At every step, data is generated. During the operation, data flows from one step to the next step as it is depicted in Figure 10.

The design step itself is not considered part of the use case. The use case starts when the CAD-data is available. This data is typically manually sent (file-sharing) from the customer to the printing company/ FMAKE to the next step. The print preparation is typically done on a powerful computer, using licensed software. After the preparation, a job file is available which is manually uploaded to the printer controller using SFTP.

During print execution, machine controller data is in real-time (<1Hz) available and high-speed monitoring data is sent directly to a processing computer. The monitoring data is analysed in real-time (digital twin) and, after every printing step, key indicators are sent to the cloud; together with the controller data. Due to the high amount of data, only limited parts are sent to the cloud platform for further analysis. After the print, the job file is manually uploaded to the cloud for archiving purposes.

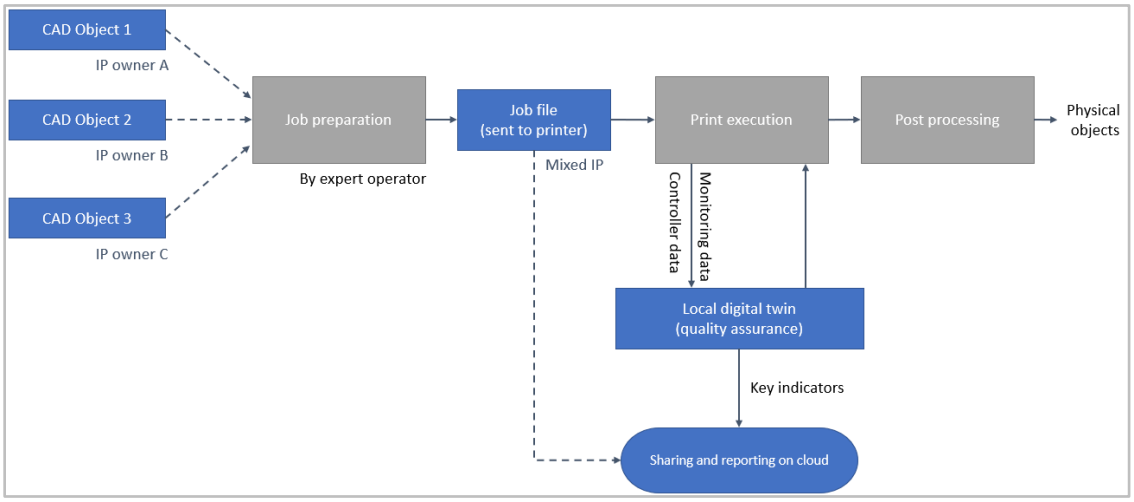


Figure 10 FMAKE data flows

Note that the data is aggregated after the print preparation and no data is linked back to their IP owner (CAD).

5.3.5 Related infrastructure

The relevant infrastructure for the pilot case within TANGO consists of:

- **[edge]** Machine controller, running on embedded hardware with proprietary software.
- **[edge]** Processing computer where high-speed sensing is connected to. The PC has approx. 100TB of storage, a Nvidia GPU, an Intel Core i9 and 128GB RAM. The computer has a high-speed connection to the monitoring equipment and regular-speed connection to the company

network and internet. Note that part of the storage and processing power is also needed during printing.
- **[cloud]** Azure subscription with virtual machines, blob storage, databases, function applications, etc.

5.3.6 Weak points of the system that can be enhanced

Considering the actions already taken in TANGO, the following vulnerabilities were mapped:

- Part of the infrastructure components (like sensors, machine controller, etc.) run proprietary software with limited flexibility. Nevertheless, there is flexibility on the edge device(s) and the cloud implementation.
- Due to its size (1GB/sec) and confidentiality, the raw data is typically stored on a local NAS on the company network with no external access. The derived post-processed data is available on the Azure-cloud, but with limited size.

5.3.7 Ways TANGO can enhance the system

During the development of the pilots, the TANGO partners will work on enhancing:

- How to manage the entire data flow, enabling **traceability**, but preserving **confidentiality**. From design (different IP-owners) to quality reports from digital twin (aggregated information). Using the job file, it is technically possible to link part of the data back to the IP owner, but not in an efficient and secure manner.
- **Efficient** storage and data sharing mechanisms, including a secure manner to combine edge and cloud infrastructure.

5.3.8 Type of Information required for TANGO

The data for the use cases consists of production data from FMAKE. Only essential data will be used for the pilots, which do not include any personal data. The production data consists of:

- Design data: CAD-drawings, print job files, printing settings.
- Monitoring data: high-speed raw data (images, time series, etc); but also derived quality indicators which are part of the digital twin.
- Post-process quality information like X-ray data or 3D scan information.

During TANGO, either real or mock-up data can be used, depending on the requirements and the confidentiality level established for the information, especially considering IP protection and company secrets.

5.4 User Requirements

Code	**UR-TUA-M1-001**
Category	**Trusted user authentication**
Description	The customer must be authenticated to have access to the system.
Priority level	High

Code	**UR-TDS-M1-002**
Category	**Trustworthy Data sharing**
Description	The customer must upload the design to an online working space shared with the printing company in an efficient, smooth and secure way.
Priority level	High

Code	**UR-TUA-M1-003**
Category	**Trusted user authentication**
Description	The printer operator and the technical expert must be authenticated to have access to the system.
Priority level	High

Code	**UR-DAC-M1-004**
Category	**Data access**
Description	The technical expert must have full access to all printing jobs to combine designs and prepare the print job file.
Priority level	High

Code	**UR-DST-M1-005**
Category	**Data storage**
Description	The customers need to be able to access their printing job data for a predefined short period of time.
Priority level	High

Code	**UR-DUP-M1-006**
Category	**Data upload**
Description	The technical expert must have access to an automatically uploaded print job file after the printing job for data review and finalisation (data lock).
Priority level	High

Code	**UR-DAC-M1-007**
Category	**Data access**
Description	The customer must have access to his/her printing jobs in a secure way.
Priority level	High

Code	**UR-DAC-M1-008**
Category	**Data access**
Description	The customer must not be able to access printing data of other customers.
Priority level	High

Code	**UR-DAR-M1-009**
Category	**Data analysis and reporting**
Description	The customers (different IP-owners) must be able to access and view their own quality report only.
Priority level	High

Code	**UR-DAR-M1-010**
Category	**Data analysis and reporting**
Description	The technical expert must receive reports on the print jobs to improve the printer operation and the printing quality.
Priority level	High

Code	**UR-DAR-M1-011**
Category	**Data analysis and reporting**
Description	The manager must be able to read/view the data of all customers to get KPIs from them.
Priority level	High

Code	**UR-DAR-M1-012**
Category	**Data analysis and reporting**
Description	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.
Priority level	High

Code	**UR-GCO-M1-013**
Category	**GDPR and related regulation compliance**
Description	The customer's data must be handled according to GDPR.
Priority level	High

Code	**UR-PCY-M1-014**
Category	**Protection from cyberattacks**
Description	The customer's printing data must be protected from any kind of cyber-attacks.
Priority level	High

Code	**UR-DMN-M1-015**
Category	**Data management**
Description	The technical expert and printing operator should be able to modify the printing data and improve them.
Priority level	Medium

Code	**UR-PMT-M1-016**
Category	**Process monitoring**
Description	The technical expert should be able to inspect the printing process data and the changes made.
Priority level	Medium

Code	**UR-DMN-M1-017**
Category	**Data management**
Description	The customer should be able to manage his/her printing jobs, e.g., request a reprint, etc.
Priority level	Medium

Code	**UR-DAR-M1-018**
Category	**Data analysis and reporting**
Description	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.
Priority level	Medium

Code	**UR-DAR-M1-019**
Category	**Data analysis and reporting**
Description	The Data Scientist should be able to pre-process the existing data.
Priority level	Medium

Code	**UR-DAR-M1-020**
Category	**Data analysis and reporting**
Description	The Data Scientist should be able to improve the model for better predictions.
Priority level	Medium

Code	**UR-PMT-M1-021**
Category	**Process monitoring**
Description	The technical manager could be able to inspect the printing process per customer (IP owner).
Priority level	Low

5.5 Use Case Scenarios

The team at FMAKE includes a Printer Operator who is responsible for ensuring that the printer is in operating condition by performing manual operations like putting the build plate in the machine and adding and removing powder. The Technical Expert aggregates all the CAD drawings from different customers into a single job file, and this expert's decisions impact the final quality of the objects and the efficiency of the printer.

The Printer Customer is a representative of a company that wants to create a specific design. This person must be able to make CAD drawings, or they may be supported by someone with this experience. Finally, the Data Scientist at FMAKE combines data from different prints, which may not be available on their computer. Currently, the Data Scientist follows an ad-hoc approach and does not consider all data. Some of the data is manually copied to a local computer, where the data analysis and model training are performed.

5.5.1 Personas

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
FMAKE_01	Printer operator (working for FMAKE)
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
John Schmidt 30 years old 5 years of experience Engineer with experience in laser techniques and mechatronic and electronic systems.	*"I would like to have a report about the printing job once that is finished, so I can improve the print data and avoid print fails."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
He wants to operate the machine and needs to make sure the printer is in good operating conditions.	Print could fail and he needs to redo the printer operations. He also does not get sufficient feedback after the print is finished.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Proprietary software which is delivered with the machine. He also uses mechanical tools (like screwdriver, etc) to operate the machine.	He is allowed to see jobs and print data to ensure that they are correct. Verifies data quality.
SHORT DESCRIPTION	
The printer operator is responsible for the printer itself. He or she needs to make sure that the printer is in operating conditions by performing manual operations (putting build plate in the machine, removing and adding powder, etc).	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
FMAKE_02	Technical expert (working for FMAKE)
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Anna Jenssen 36 years old 8 years experience Engineer who is familiar with CAD-work and is an expert in 3D printing challenges.	*"Every print job is a new challenge to combine the print files of many customers into one."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Their main objective is to print efficiently high-quality objects. They need to deliver job files which will be forwarded to the printer operator. Receives the design from the customer and combines different designs into a single printing job. Downloads the designs to his own computer to prepare them using proprietary software.	
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
They use print preparation software where they need to perform several manual and automated steps. The software is licensed and proprietary. Has access to the designs through email – downloads the files to his PC.	Mainly in contact with the customer

SHORT DESCRIPTION
The technical expert takes all the CAD drawings from different customers and aggregates them into a single job file. The technical expert takes decisions which will have an impact on the final quality of the objects and on the efficiency of the printer.

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
FMAKE_03	Printer customer
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Maria Peeters 30 years old 4 years of experience Works for an architecture company	
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
They want to have a physical object of their design (CAD drawing).	They must take the printability into account, which limits the freedom to design any shape. They want to be sure her design won't end in the wrong hands.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Any CAD drawing software Sends printing design by email to the printing company.	
SHORT DESCRIPTION	
The printer customer is a person, technical or non-technical, who is representative for a company that wants to have a certain design being created. The person should be able to make CAD drawing or is supported by someone who has this experience.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
FMAKE_04	Data Scientist (working for FMAKE)
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Jurgen Jacobs 42 years old 7 years of experience The data scientist is an engineer with a couple of years' of experience in data handling and statistics. They are also at a high-level aware of the 3D printing challenges.	"I need a lot of labelled data to build an accurate model"
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
He/she wants 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.	Only limited labelled data is available and might be scattered at different locations.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
They use Python (+modules) to process the data and build a ML model. As it is computationally intensive, he/she uses GPU optimization, if possible, to speed-up the training and data processing.	They need to get access to the printing data and the labels. They mainly interact with the technical expert and exceptionally with the printing operator.
SHORT DESCRIPTION	
The data scientist combines data from different prints, so they should access data from all customers. This data might not be available on their computer. Currently, they follow an ad-hoc approach and does not consider all data. Part of the data is manually copied to a local computer where the data analysis and model training is executed.	

Ensures that current quality models are up to date, trained and validated with the latest data. They combine data from different customers (stored in various locations), raw machine data hard to transfer because of high volume. All data need to be put in the same location, which should be avoided in the future. Ideally, every object/print can be used to train a part of the model and afterwards all prints are combined into one model.

5.5.2 User Journeys

PERSONA:		Customer/ technical expert			
	JOURNEY STAGE	**TOUCHPOINTS/ Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Customer creates a new design	Own software to create computer-aided designs (CAD)			
2.	Customer shares the design with the printing company by uploading it to a shared online working space – gets successful uploading confirmation by platform.	Own CAD software and file-sharing (mail) TANGO Platform	Wants to have a smooth sharing	Technical expert	
3.	Customer is waiting for feedback from the printing company. The customer wants to follow-up the status real-time.	Data sharing and visualisation platform		Technical expert Printing operator	The printing company makes sure that the data and status is shared properly and securely.
4.	The technical expert looks at the customer designs and combines it into a printing job with other customers' files.	Proprietary print preparation software TANGO Platform		Technical expert	No interaction with the customer.
5.	The customer monitors the progress of the printing job: 1. Job preparation by technical expert 2. Printing operated by printing operator 3. Final post-processing by printing operator 4. Shipment by external company	TANGO Platform		Technical expert Printing operator	
6.	Customer receives a digital report of their print and is able to access the data of his print and stores a local copy.	TANGO Platform Efficient data sharing (report can be large)			Report includes printing information with some graphs (screenshot or pdf). The report should be generated with part of the dataset that belongs to the specific customer. Prevent customer from seeing the data of other customers.

PERSONA:		Customer/ technical expert			
	JOURNEY STAGE	**TOUCHPOINTS/ Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
7.	The customer accesses their "area" on the shared files to request a reprint of a previous job.	TANGO Platform			
8.	In case of quality issues with the printed object, the customer contacts the technical expert again with the quality information. The technical expert contacts the data scientist to identify why this issue is not identified by the model.			Technical expert Data scientist	

PERSONA:		Technical expert/ printing operator			
	JOURNEY STAGE	**TOUCHPOINTS / Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	The technical expert accesses the customer's files to prepare the data for the print job.	TANGO Platform shared workspace		Customer Printing operator	The technical expert and printing operator have access to the data during the printing job.
2.	The technical expert modifies the data slightly (manual annotations) to improve them. The platform monitors which users access which files, and which changes were made.	TANGO Platform			The technical expert and printing operator have access to the data during the printing job.
3.	The printing operator gets access to the files to perform the printing job.	TANGO platform shared workspace		Technical expert	The technical expert and printing operator have access to the data during the printing job.
4.	After the job is printed, the printing operator stops having access to the files.	TANGO platform shared workspace			
5.	At the end of the printing job, the technical expert reviews the data and locks it – read only for historical purposes or for a special procedure.	TANGO platform shared workspace			Locking data – no write access

PERSONA:	Technical expert/ printing operator				
	JOURNEY STAGE	**TOUCHPOINTS / Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
	The technical expert will still have access to the files for a fixed time (typically approx. 1-6 months), together with the data scientist				

PERSONA:	Manager				
	JOURNEY STAGE	**TOUCHPOINTS / Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	The manager requests a report from the system based on several criteria.				Only read-access to subset of the data
2.	Should be able to read/view the data of all customers to get KPIs from them. He/she should only have access to some overall key indicators (overall quality, printing time, etc) and should not be able to dive into the details.	TANGO platform			Component for KPIs, statistics/ Visualisation component

PERSONA:	Data scientist				
	JOURNEY STAGE	**TOUCHPOINTS/ Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	A customer complains to the company that the printed quality was not good enough.			Technical expert Customer	
2.	The data scientist, together with the technical expert, investigate the existing data if the quality issue was predicted by the model.			Technical expert Data scientist	
3.	If the issue was not predicted by the model (see previous step), then the data scientist decides to improve the model.			Data scientist	
4.	The data scientist examines the raw data related to the customer and the print. The data scientist pre-processes the raw data. He checks for data integrity;	TANGO Platform		Data scientist	

PERSONA:		Data scientist			
	JOURNEY STAGE	**TOUCHPOINTS/ Possible Technical Offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
	especially to see if the data is complete, removes noise and outliers if present.				
5.	The data scientist collects feedback from the customer and updates the labels that are used for training.	Data scientist should have the possibility to access and alter the data for training		Data scientist Customer	
6.	The data scientist updates the model by retraining. They combine data from different customers at various locations (edge, cloud, and potentially at customer)	TANGO Platform			Federated learning and XAI to explain the results of the trained models.
7.	The final retrained model is uploaded on the printer (edge device) by the data scientist and the printing operator and technical expert check if it is working properly.			Data scientist Technical expert Printing operator	
8.	Oral feedback is given to the customer and they can request a new print with the updated model.			Technical expert Customer	

5.5.3 Technology offerings used in use case scenario

TECHNOLOGY OFFERING	RELATION TO PILOT
Confidentiality and Privacy by Design	Support the access control to data, like printing job information for specific clients. Attribute-based and sticky policies can be applied to establish fine-granular control of who has access to the encrypted data based on identity. E.g., upload all data from a printing job to the sharing platform, but each part encrypted with specific policies so that only allowed users can decrypt (e.g., data from a client's request).
Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms	Ensuring data privacy, even when files are accessed.
Self-sovereign Identity Management	SSI Module enables the staff members to manage their data and provide only necessary information for the customers.
Seamless Onboarding for Users and Devices	The component will be used in order to verify the identity of the staff members and the customers, by leveraging their passport and remotely verifying their identity through the TANGO wallet. Having verified their identity, the SSI management will be able to generate the verifiable credentials which will be then used by the staff members to verify their identity seamlessly and then ensure that the customers access only the necessary information. The component will also allow the onboarding of devices.
User Continuous Behavioural Authentication	Workers will be continuously authenticated when using the printer jobs
Exploratory Data Analysis Engine	EDAE Module enables technicians to automatically generate reports based on failed prints. The EDAE will provide statistics of raw print data (before training) as well as key indicators for the manager, including: 1. outlier data (among failed prints) 2. trends and insights on which parts fail (e.g. associations between failed prints) 3. KPIs for printing tasks
Energy-efficient AI model training	Federated Leaning techniques could be applied to train AI models with data at edge or other computing nodes without having to move or disclose the raw data. This will help in reducing energy consumption and privacy concerns. Usage of MLOps for ML Model management life-cycle, potentially AutoML techniques.
Dynamic Intelligent Execution on Heterogeneous Systems	TornadoVM will be indirectly used for the hardware acceleration of the data analytics that will be performed within the EDAE engine in the context of this pilot
X-AI for Privacy and Trust Enhancement	Use Explainable Artificial Intelligence (XAI) to help data scientists better understand the decisions made by the trained AI model and help debug it in cases where bias is discovered in the results.

Infrastructure Management Based on AI	As Training of AI models is not time critical, tasks may be shifted in time. Since data is not always transferable due to size. Geographical shifting is not possible.

5.6 KPIs

TITLE	DESCRIPTION
Reduction/Elimination of privacy violation incidents in data sharing	Privacy assessment results comparison of existing infrastructure with TANGO proposed data sharing platform (Currently 10-15 events last year).
Accuracy of user verification and authentication > 99.6%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate, and failure to access.
Customer Satisfaction Score	This KPI measures the satisfaction level of customers with the products and services provided by FMAKE.
Data Analysis Accuracy/ Improvement in printing model	This KPI measures the accuracy of data analysis performed by the Data Scientist at FMAKE. It ensures that the insights generated from the data are reliable and trustworthy. Keep the model accuracy >80%. Ideally reach >85% with Federated learning (Currently >80%)
Cybersecurity	This KPI measures the effectiveness of company's cybersecurity measures in protecting sensitive data (e.g., protected by IP) from cyber threats. It can be measured through penetration testing and vulnerability assessments and can be used to determine the company's ability to protect its clients' data.
Overall Equipment Effectiveness	This KPI measures the effectiveness of the additive manufacturing equipment in terms of availability, performance, and quality.
Improvement in print job report availability (performance)	The print job report should be generated and become available to the customer in less than 10 seconds upon request. (currently ~10 sec.)
Improvement in print job data traceability	Ability to trace back the data for each print job and customer. (YES/NO KPI)

6 Pilot 3 - Smart Manufacturing – Case 2

6.1 Pilot case overview

The third first pilot is about Smart Manufacturing and it is to be implemented in the task T7.4 during months M24 – M36 of the project. This pilot has two sub-cases, one about additive manufacturing and a second one about industrial shop floor security. This chapter analyses the case of the shop floor security. In this case, the proposed platform will be used to securely share and ensure data ownership of information such as human resources and employees, corporate information, intellectual property, manufacturing system suppliers etc. At the same time, the infrastructure should be protected from cyberattacks.

6.2 Organisations involved

6.2.1 RIA STONE

RiaStone (RIA) is part of "Visabeira Industria" a sub-holding of the GRUPO VISABEIRA[3] conglomerate, RiaStone was created in 2014, after a novel contract being awarded by IKEA Sweden (https://ikea.today) for the Europe based manufacturing of 486 million tableware products in the period 2014-2026. Through that awarded contract, RST manufactures the IKEA Europe wide supply of "Dinera", "Fargrik" and "Flitighet" IKEA tableware families, being these products fabricated through an innovative Industrial ceramics production process: Tableware Automated Single Firing (TASF).

The introduction of this advanced and innovative ceramics production process (TASF) has allowed for stark reduction of energy-associated costs, substituting the traditional dual-firing technique, all this resulting in a significatively lowered carbon footprint associated with the production of IKEA tableware.

To progress towards better OPE KPI´s RiaStone started to participate in several Horizon2020 initiatives as a premium pilot factory. The Horizon 2020 initiatives presently being implemented in the RiaStone Factory are focused in the areas of:

Big Data – RiaStone participated in the 36 months https://boost40.eu Horizon 2020 initiative, devoted to the implementation of systemic solutions for the processing of big data in industrial environments.

Zero Defect Manufacturing – RiaStone is currently participating in the 36 months https://qu4lity-project.eu Horizon 2020 project, dedicated to the implementation of product and process centred ZDM systems for the implementation of flexible manufacturing TQM solutions, namely in-line inspection technologies, and integration of ICT tools for autonomous, automatic, smart system decision taking.

Industrial Data Services in flexible manufacturing - RiaStone is currently participating in the 36 months https://www.i4q-project.eu Horizon 2020 project, dedicated to the implementation of advanced prime matter inspection techniques and industrial data integration.

To achieve the factory required KPI improvement goals, Riastone is applying a systems-level strategy consisting in the integration of new advanced FoF and industry 4.0 techniques to its production line systems. This means that RiaStone is presently strongly progressing towards the full adoption of Industry 4.0 standards and therefore becoming increasingly reliant on interconnected data systems and technologies.

However, as a consequence of the continuous adoption of Industry 4.0 systemic approaches by RiaStone, the introduction of new and advanced externally interconnected data systems significantly increases the vulnerability of RiaStone to internal and external cyber-attacks.

Namely any production system data, that migrates from production technology systems on the factory floor to the new interconnected information technology (IT) systems in the corporate network, and external networks is vulnerable to intrusions, as well as the fact that these new systems often need new

[3] https://grupovisabeira.com/en/home

remote system access entrance points constituting themselves additional cyber security liabilities to the previously existing ones.

RiaStone is one of two manufacturing demonstrators in TANGO, and will perform the following main tasks in the project:

- Contribute to the project scoping activities, definition of the use-cases and elicitation of business requirements and key performance indicators.
- Implementation of a pilot demonstration in the area of Secure manufacturing operations in the digital Workplace
- Post Implementation assessment of Tango solutions performance and KPI measuring activities that will effectively demonstrate the benefits and positive impacts of TANGO solutions in the To-Be manufacturing Pilot situation.

RiaStone brings to TANGO the following factors and assets:

- RiaStone has a production line which is 99% automated and digitally controlled.
- RiaStone has a Factory management System (FMS) implemented end-to-end, controlling a modern factory production line with high levels of automation, which makes available high volumes of production data that is easily available for collection and availability to the project.
- RiaStone has implemented a complete "Key Production Metrics System" that has relevant and significant KPI´s already being tracked and mapped over time.
- All the previous plus factors will allow for precise tracking of functional impacts in the KPI´s, after the Demonstration/Proofs of Concept in the areas of intelligent Cyber Sec operations and secure data sharing reach Post-Implementation Status.

6.2.2 SQUAD IT Portugal

SQUAD is an Independent Software Vendor developing and selling software products for blue-chip customers located in Europe and the Middle East and Africa regions.

SQUAD is one of the leading developers of software applications headquartered in Portugal with more than 120 full-time senior software and data-science engineers, serving more than 20 Mio end-users, and more than 35 blue-chip B2B customers,

SQUAD develops business applications for data science, and Machine-Learning, including desktop applications, industrial shopfloor applications, as well as web, and mobile apps and applets.

SQUAD is focused on creating consumer-driven software solutions, adaptive to flexible system requirements and diverse operating requirements, with an operational profile characterised by low error rates, and over-the-top user friendliness.

SQUAD has broad experience in creating server, edge, and cloud-based systems which are highly scalable, flexible, and elastic in the handling of any-size data processing systems.

Due to its large user base, SQUAD applies its knowledge in the B2B Domain namely Industry 4.0, Government, and Media, as well as in the B2C consumer domain, in the e-Health and culture domains.

SQUAD IT will perform the following main tasks in the Tango project:

Assist RiaStone in the processes of:

- Use-case definition for the RiaStone Tango Pilot.
- Assistance to RiaStone in Tango scoping activities.
- Support RiaStone in the elicitation of business requirements and key performance indicators.
- Support RiaStone in the implementation of the manufacturing pilot demonstrator in the area of Secure manufacturing operations in the digital Workplace.
- Support RiaStone in the Post Implementation assessment of Tango solutions performance and KPI measuring activities.
- Support RiaStone in the effective demonstration of benefits and positive impacts of TANGO solutions in the To-Be manufacturing Pilot situation.

In TANGO SQUAD is a solutions and technology supplier to RiaStone, and brings to TANGO the following assets:

- 120+ senior programmers and system developers focused on the implementation of diverse HW+SW integrated systems.
- Existing knowledge in the RiaStone production systems and digital infrastructure.

6.3 Existing Situation Mapping

6.3.1 A brief description of the platform

RST manufactures the IKEA Europe wide supply of "Dinera", "Fargrik" and "Flitighet" IKEA tableware families, being these products fabricated through an innovative Industrial ceramics production process: tableware automated single firing.

The "Dinera", "Fargrik" and "Flitighet" IKEA tableware families, include the fabrication of regular round shaped pieces of tableware as well as angular pieces of tableware.

For that purpose, Riastone production Lines are equipped with the latest state of the art automation equipment from the most relevant automation manufacturers such as Lippert, Siemens, Festo, SAMA, Riedhammer, Johnson Controls and others.

The Main RiaStone Automated production line systems are:

Table 1 The Main RiaStone Automated production line systems

#	NUMBER OF SYSTEMS	PROCESS NAME	EQUIPMENT SUPPLIER
1	19	Iso-Static pressing	SAMA Maschinenbau GmbH
2	19	Abrasive trimming finishing and edging	SAMA Maschinenbau GmbH / KUKA Robotics Aktiengesellschaft
3	2	Pre-cure warehousing	LIPPERT GmbH & Co. KG - Engineering Solutions
4	6	Glaze preparation	Exsepi - Industrial automation and Robotics
5	8	Tableware Glazing	LIPPERT GmbH & Co. KG - Engineering Solutions
6	3	Pre-firing product Grouping	KUKA Robotics Aktiengesellschaft
7	3	Oven Single Firing	Riedhammer GmbH / Induzir - Kilns
8	10	Quality Control inspection	Exsepi - Industrial automation and Robotics
9	3	Sorting and Packing	Exsepi - Industrial automation and Robotics

Presently RiaStone has one main production contract, to supply 30 million tableware pieces up to 2021, which implies a monthly production of 300 000 tableware pieces.

- Additionally, RiaStone has received a request from IKEA to extend and increase, the present Contractual Delivery Scope up to 2026, increasing the number of produced tableware parts to 486 million pieces.
- For that goal to be achieved, RiaStone has expanded the Factory shopfloor systems in +60%, and it has to be able to use its production shopfloor interrupted during 95% of the available calendar time available until the contract end-period of 2026.

In the RiaStone production shopfloor, RiaStone uses a synchronised daisy-chain in-line manufacturing system, which relies on intersystem cycle time synchronisation that is hard to restore making the time length of any production outage critical.

The main business motivations for RiaStone in the Tango project are the following:

- To implement Secure Data Operations through the implementation of cybersecurity ML models based on behavioural patterns that enable RiaStone to attain and maintain a high-level Cybersecurity defensive posture.

The attained Cybersecurity defensive posture shall enable RiaStone achieve the following Business continuity goals in the TANGO Project, as stated in 6.3.7.

6.3.2 Key Stakeholders involved

In this subsection we list the different stakeholders that are involved in the pilot implementation. They will be further described and analysed in the personas and user journeys subsection.

1. Operational worker (shopfloor)
2. Shopfloor supervisor
3. Maintenance staff
4. Management staff (all kinds of managers in depts)
5. Technology provider (vendor)

6.3.3 Main operations flow of the system

In the shopfloor production system, there are two major groups of digital platforms and connections, those are:

a) Remote Maintenance Accesses intended for remote system maintenance,
b) Continuous always-on connections between company ERPs

In order to attain high availability ratios from the completely installed shopfloor machine systems, RiaStone has established 24/7 maintenance contracts with relevant technology suppliers that ensure continuous availability of all running production systems.

Under those maintenance contracts, most of the technology suppliers have established direct digital remote accesses into the RiaStone IT Network to have the capability to access their supplied production systems remotely, by using several different Remote Access applications:

Table 2 RIAS technology suppliers

#	#ACCESSES	EQUIPMENT SUPPLIER	TYPE OF CONNECTIONS
1	2	SAMA Maschinenbau GmbH	AnyDesk Remote connection
2	2	KUKA Robotics Aktiengesellschaft	AnyDesk Remote connection
3	5	LIPPERT GmbH & Co. KG - Engineering Solutions	TeamViewer Remote connection
4	3	Exsepi - Industrial automation and Robotics	TeamViewer Remote connection
5	2	Riedhammer GmbH	TeamViewer Remote connection
6	2	Induzir - Kilns	TeamViewer Remote connection

6.3.4 Data flows

While integrating the Global IKEA Supply Chain, Riastone must comply with the IKEA requirement to be permanently in an open channel and communicate with IKEA in a continuous always-on manner.

Systems wise that requirement led to establishing a permanent SAP EDI Connection in between both companies, through where IKEA and RiaStone´s ERP´s are constantly connected 24/7/365.

The same type of connection is also established between RiaStone and Grupo Visabeira.

Table 3 RIAS and vendors connection type

#	CONNECTION	ERP SYSTEM	ENTITY	TYPE OF DATA	SENSITIVITY
1	EDI	SAP	IKEA Global	Commercial Exchanges	Very High
2	EDI	SAP	Grupo Visabeira	Corporate information	Very High
3	EDI	SAP	Grupo Visabeira	HR Information	Very High
4	Ethernet	SmartTi	Grupo Visabeira	Procurement/ Production KPI´s/Dashboarding	Very High

In the scope of physical perimeter security Riastone also has several digital assets that are critical to the operation continuity, and that can become a point of entrance for unwanted intrusions.

Table 4 RIAS systems and connections

#	CONNECTION	SYSTEM	MANUFACTURER	RANGE	SENSITIVITY
1	Ethernet	CCTV	UniViewer	24 CCTV perimeter security cameras	Very High
2	Ethernet	Physical access	Datelka	5 electronically controlled access entrances	Very High

6.3.5 Related infrastructure

As stated above, regarding external digital platforms, there are two major groups of platforms and connections, Remote Maintenance Accesses intended for remote system maintenance, and continuous connections between company ERPs. All the related infrastructure is mentioned in the previous section.

6.3.6 Weak points of the system that can be enhanced

RiaStone, being a fully automated production facility where several different shopfloor systems from different technological suppliers are associated and interconnected, is permanently connected in the industrial internet network to multiple other entities within a vast supply chain ecosystem, this causing many possible entry points. Thus, RiaStone is vulnerable to hacking activities such as intellectual property theft, data theft, intentional shut down of production systems, intentional disruption of production timetables, and disruptions of product quality.

Furthermore, and compounding on top of these system level vulnerabilities RiaStone uses a synchronised daisy-chain in-line manufacturing system, which relies on intersystem cycle time synchronisation that is hard to restore making the time length of any production outage critical.

In this landscape the integration of the new flexible production systems, such as robotics, cyber physical systems, and the new H2020 programs such as Big Data, ZDM, Artificial intelligence, and other advanced manufacturing systems, have created new challenges to RiaStone to securely integrate the new systems with the older legacy systems, without opening or leaving open cyber vulnerabilities.

Up to the present date RiaStone has been already targeted twice by external hackers that have significantly disrupted shopfloor operations, both events were detected due to the significant disruptions in shopfloor production system cycle times that were detected by operating factory personnel.

Both events led to full shopfloor production being stopped during significant periods, until the system disruptors were located and the smurf/fraggle attacks were stopped by resetting the attacked routers that were provoking network denial-of-service (DoS) by internally broadcasting large amounts of spoofed traffic.

During the first disruption event, there was the need to react through a factory wide shut down, and systems reset that took a period of around 5 hours of production disruption.

In the following disruption event, the maintenance teams performed selective systems shutdown, until the source fault was located as being newly installed Wireless routers part of the new AIV (Autonomous Intelligent Vehicles) that are part of the shopfloor distribution product distribution network.

6.3.7 Ways TANGO can enhance the system

Riastone has the ambition of under the scope of the TANGO project to be able to implement Secure Data Operations through the implementation of blockchain technologies, and cybersecurity ML models based in behavioural patterns, that enable RiaStone to attain and maintain a high-level Cybersecurity defensive posture, characterised by the following functional conditions:

Table 5 RIAS TANGO objectives

#	RiaStone functional business continuity conditions to be achieved through the TANGO Project
1	To be able to maintain stable, continuous, uninterrupted, business operations
2	To be able to avoid the theft of intellectual property either from RiaStone as well as from RiaStone internal and external Business Stakeholders
3	To be able to avoid the theft of Corporate or individual data from RiaStone Data repositories
4	To be able to avoid that RiaStone Systems are used as entrance doors to any of our RiaStone internal and external Business Stakeholders Systems
5	To be able to avoid the intentional shut down of production systems,
6	To be able to avoid the intentional disruption of production timetables
7	To be able to avoid disruptions to manufactured product quality.

Using TANGO technologies RiaStone will implement a set of Data security management systems consisting of:

Table 6 RIAS data security objectives

#	Innovative Data security management systems
1	Data processing pipelines exploiting the potential of the computing continuum from cloud to edge
2	Strong encryption as well as proactive and preventive cybersecurity mechanisms for secure data transfer and access control.
3	Trust, transparency, accountability and privacy-preserving identity management based on eIDAS compliant Self-Sovereign Identity.
4	High security in a user-friendly manner through AI-powered continuous behavioural authentication for users and devices based on behavioural patterns

6.3.8 Type of Information required for TANGO

The following type of information should be available to the TANGO technical partners in order to be able to assess the situation and provide solutions.

- Applications access logs
- Access records
- User/employee data

The details of the above information will be described in the related technical documentation with the implementation details.

6.4 User Requirements

Code	**UR-TUA-M2-001**
Category	**Trusted user authentication**
Description	Shopfloor workers must have access only to their designated areas.
Priority level	High

Code	**UR-TUA-M2-002**
Category	**Trusted user authentication**
Description	The company files must be protected in a smart way, enabling access based on each person's role.
Priority level	High

Code	**UR-PMT-M2-003**
Category	**Process monitoring**
Description	The supervisor must know every time a worker is not at the designated area.
Priority level	High

Code	**UR-PMT-M2-004**
Category	**Process monitoring**
Description	The supervisor must be notified every time a worker is not at the designated area.
Priority level	High

Code	**UR-TUA-M2-005**
Category	**Trusted user authentication**
Description	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.
Priority level	High

Code	**UR-PCY-M2-006**
Category	**Protection from cyberattacks**
Description	The company's data must be protected from any kind of cyber-attacks.
Priority level	High

Code	**UR-GCO-M2-007**
Category	**GDPR and related regulation compliance**
Description	The customer's data must be handled according to the GDPR.
Priority level	High

Code	**UR-PMT-M2-008**
Category	**Process monitoring**
Description	The supervisor should have records of all unauthorised access attempts in the platform system.
Priority level	Medium

Code	**UR-DAR-M2-009**
Category	**Data analysis and reporting**
Description	The supervisor should receive a report of all unauthorised access attempts in the platform system.
Priority level	Medium

Code	**UR-PMT-M2-010**
Category	**Process monitoring**
Description	The company should be able to monitor the shopfloor for any strange movements and be notified.
Priority level	Medium

Code	**UR-TUA-M2-011**
Category	**Trusted user authentication**
Description	Each technology partner should access the factory through a Data Gate Keeper.
Priority level	Medium

Code	**UR-TUA-M2-012**
Category	**Trusted user authentication**
Description	Specific users should know if the technology providers are not following the authorised path for their applications.
Priority level	Medium

Code	**UR-TUA-M2-013**
Category	**Trusted user authentication**
Description	Specific users should receive security breach notifications if the technology providers are not following the authorised path for their applications.
Priority level	Medium

Code	**UR-PMT-M2-014**
Category	**Process monitoring**
Description	The company should have a clear view and records of the technology partners' actions during their presence in the system.
Priority level	Medium

Code	**UR-PCY-M2-015**
Category	**Protection from cyberattacks**
Description	The company's operation should not be interrupted by any unauthorised access.
Priority level	Medium

Code	**UR-TUA-M2-016**
Category	**Trusted user authentication**
Description	The Data Gate keeper could ensure authentication, restricted application access, and other security data security measures.
Priority level	Low

Code	**UR-DMN-M2-017**
Category	**Data management**
Description	The company documents could be shared but not changed by the people accessing them.
Priority level	Low

Code	**UR-DMN-M2-018**
Category	**Data management**
Description	Specific clients should be able to share data to specific users.
Priority level	Low

6.5 Use Case Scenarios

RiaStone is a renowned manufacturing company that produces high-quality products such as IKEA tableware. The company follows strict guidelines for hiring operational workers and conducts thorough background checks to ensure compliance with GDPR rules.

One of the main goals of the operational workers is focused on increasing the value of the product through all the manufacturing processes and aims to avoid any system failures or unauthorised access.

The shopfloor supervisor is committed to promoting a positive working environment and fostering teamwork among her peers and subordinates. He keeps up to date with the latest production technologies and organisation methods, monitoring that workers are in their designated areas, and performing other shopfloor operational tasks.

The RIA shopfloor maintenance staff, as a specialised machinery engineer from a software or mechatronics background, focuses on maintaining the shopfloor systems' operationally during production. The staff mainly performs corrective maintenance tasks, while preventive maintenance is left to specific vendor personnel.

The RIA H&S management staff, as a specialised safety engineer from a chemical or mechatronics background with additional H&S certification, implements and maintains H&S procedures in the factory according to ISO 18001 requirements.

The company is supported by Squad, an independent software vendor that provides essential services to keep the operations running smoothly. The technology provider performs remote maintenance on the existing software used in the machines using three different types of remote maintenance to keep the software up to date. They have easy and low-security remote access to the RIASTONE internal production system, but there are no dual or triple authentication verifications. They use TeamViewer software to access the RIAS devices remotely. However, sometimes the factory's internet access infrastructure has downtimes, preventing them from accessing the systems at any time.

A cyber attacker attempts to penetrate all the systems and steal reports and personal data, which they can use to blackmail the CEO of the company. With all these challenges, RIASTONE's team must remain vigilant and work together to ensure the smooth operation of the factory and the safety of its employees.

6.5.1 Personas

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
RIAS_01	**Operational worker (shopfloor)**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Maria Age: 27 years old Occupation: Machine Operator for Quality Inspection Domain: Conformity Inspection Years of experience: 5 years	Accessing the facilities is cumbersome sometimes. Enjoys the experience of working in a high-tech factory. Has pride in producing such a recognized product as the IKEA tableware. Has contact with the latest production technologies. Good atmosphere in the working place with colleagues working towards ambitious production goals.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Adds value to the product. Packaging, machine operators, quality inspection, etc. Works next and with the production line machinery. Avoids people without access rights at the floor.	System failures sometimes prevent access by mistake. Lost connection to system servers. Lost cards by workers. Multiple workers accessing the shopfloor with the same card.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Currently: ID card. Revolving barriers. The system is a very primitive revolving triple bar, which is disapproved by the majority. Biometrics system with fingerprint only registers that you are in, does not open the revolving door. Worker has the card on a neckline and usually their phone with them.	There is one security person at the entrance. On average 2-3 times per day people without access are actually on the shopfloor. People enter usually by mistake, other times to steal. Workers from different areas of the shopfloor wear different shirt colours. Supervisors check unauthorised access to areas by checking the shirt colour.
SHORT DESCRIPTION	
Maria, as an operational worker, is hired through an organised onboarding process. During this, she is checked regarding criminal registers, immigration status, legal liabilities etc. She is informed that this data is processed and stored according to GDPR rules. Her goal is to increase the value of the product through all these manufacturing processes and to not be disturbed by any system failure or by other people, who are in the same area without access rights.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**

RIAS_02	Shopfloor supervisor
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Gerarda Age: 35 years old Occupation: Production line Operational control Domain: Uninterrupted operation of the production lines Years of experience: 12 years	Wants to promote a good working environment atmosphere in the working place with peers and subordinates working together towards ambitious production goals. Accessing the facilities for the production team is cumbersome sometimes and may cause small but significant delays. Enjoys the experience of working in a high-tech factory. Has pride in producing such a recognized product as the IKEA tableware. Has contact with the latest production technologies, and team work organisation methods.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Monitors that workers are in their designated areas. Other shopfloor operational tasks.	Systems do not go further than monitoring worker shopfloor access. Would like to have automated identity checking and validation systems inside the shopfloor areas. Sometimes workers trade shifts between themselves with advanced notice that would allow to prepare monitoring systems in advance. Lost cards by workers. Multiple workers accessing the shopfloor with the same card.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Has a mobile device (phone, wearable, tbc). They have a specific smartwatch for shift control.	Supervises a team of around 15-20 elements during an eight-hour shift. During resting intervals, the team elements will normally access the outside of the shopfloor and re-enter after 15m.
SHORT DESCRIPTION	
Gerarda is a professional who is committed to promoting a positive working environment in her workplace. She believes in fostering a sense of teamwork and collaboration among her peers and subordinates, with the aim of achieving ambitious production goals. Despite facing some challenges with accessing facilities, she is passionate about working in a high-tech factory and takes pride in producing recognized products such as IKEA tableware. Gerarda keeps up to date with the latest production technologies and team organisation methods and is responsible for monitoring that workers are in their designated areas, as well as other shopfloor operational tasks.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
RIAS_03	**Maintenance staff**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Luis Age: 37 years old Occupation: Production line Operational Maintenance Domain: Uninterrupted operation of the production Systems Years of experience: 15 years	Focused in promoting continuous shopfloor systems uptime. Enjoys working with modern latest technology production machinery with diminished downtimes. Latest tech has complex but efficient maintenance tooling regarding fault diagnosis and fault resolution. Facilities access systems are traditional and relatively low tech compared to production line systems in RiaStone. Enjoys the experience of working in a high-tech factory.

	Has pride in producing such a recognized product as the IKEA tableware. Has contact with the latest production technologies, and team work organisation methods.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Contacts vendor to ask for support, upgrade, etc. Wants to be informed if there is a security breach. Would like to have control of access for any remote system entrance being performed by external elements. Would like to have advanced multiple factor authentication implemented for any remote access entrance channels.	Access to RiaStone shopfloor systems is made by external entities without his knowledge. Sometimes external accesses are used by technology providers to install SW and FW updates/upgrades/ patches that are faulty and cause unexpected and radical systems disruption. Already suffered two highly disrupting hacker attacks, expecting more to happen.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Involved in the maintenance processes from RIAS side. Manages the connection with the vendor via Teamviewer.	No double or triple authentication factor systems are implemented across vendor maintenance staff. He functionally works in a 4x shift scheme in an 8-10 people team, and operates locally with the remote support of diverse remote vendor teams
SHORT DESCRIPTION	
Luis as Rias Shopfloor maintenance staff is specialised machinery engineer, who is coming from software or mechatronics backgrounds. His job is focused in maintaining full operationality of the shopfloor systems, while production is underway. He performs mostly corrective maintenance tasks, being preventive maintenance left to specific vendor personnel.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
RIAS_04	Management staff (all kinds of managers in depts)
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Susana Age: 44 years old Occupation: Factory Health and Safety Manager Domain: H&S processes, environmental safety, Carbon footprint assessment and management Years of experience: 22 years	Focuses in promoting workplace safety for all employee's operation in the Riastone shopfloor. Focuses in promoting lower environmental impacts of the RiaStone operation whenever possible. Enjoys the experience of working in a high-tech factory. Works hard to achieve safety and environmental indicators significantly higher than standard in the ceramics industry. Has pride in producing such a recognized product as the IKEA tableware. Has contact with the latest production technologies, and teamwork organisation methods.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Has ambitions of having newer & more evolved safety systems in place to monitor incidents in the Riastone factory.	Lack of real time data-based systems, allows only for post-event actions. Has no systems that enable to preview or recognise incidents in real time that could allow significant impact mitigation actions.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
OHSAS ISO 18001 – processes and tools. Files are stored in the folder system; access is controlled through folder access rights.	Most processes are stored digitally, some are implemented in paper registers due to its nature. Would like to have automated data collection systems for H&S and facilities access systems that can complement the currently implemented access systems.
SHORT DESCRIPTION	

Susana as a Rias H&S management staff is a specialised safety engineer, who is coming from chemical or mechatronics backgrounds with additional H&S certification. Her job is focused in implementing and maintaining H&S procedures in the factory according to ISO 18001 requirements.

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
RIAS_05	**Technology provider (vendor)**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Heinz Age: 45 years old Occupation: Technology provider preventive and corrective maintenance specialist Domain: remote maintenance of manufacturer installed technology assets. Years of experience: 23 years	Remote Access to RiaStone internal production system is easy and with low security. There are no dual or triple authentication verifications. Remote access is always open, he can get into the factory production systems whenever he wants without asking or notifying anyone.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Performs remote maintenance (three types) to existing software for the machines.	Sometimes the factory internet access infrastructure has downtimes that prevent him from getting into the systems at any time.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Has access through the software of Teamviewer to the RIAS devices.	Multiple vendors with multiple systems. Each machine has its own software vendor. After accessing Teamviewer they can get access anywhere. Corrective maintenance. Preventive maintenance (software updates - mandatory, software upgrades – optional paid).
SHORT DESCRIPTION	
Heinz is a technology provider for RiaStone, and his primary goal is to perform remote maintenance on the existing software used in the machines. He uses three different types of remote maintenance to keep the software up to date. He also has easy and low-security remote access to the RiaStone internal production system. However, there are no dual or triple authentication verifications, and the remote access is always open, which means Heinz can get into the factory production systems whenever he wants without notifying anyone. He uses TeamViewer software to access the RIAS devices remotely. However, sometimes the factory's internet access infrastructure has downtimes, which prevents him from accessing the systems at any time.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
RIAS_06	**Cyber Attacker**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Juan Kar Age: 34 Occupation: Digital Systems Domain: Specialised in stealing sensitive data from companies. Years of Experience: 12	Wants to break the cyber defence of any company.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Want to steal the data and reports from the company.	To get caught during the attempt and not steal the data. To be arrested.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Web services, AI tools, Linux system.	

SHORT DESCRIPTION
Juan Kar is an experienced hacker. His aim is to penetrate all the systems and steal reports and personal data. Then, he will use all this information to blackmail the CEO of the company.

6.5.2 User Journeys

PERSONA:		Operational worker (shopfloor)			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Worker accesses the factory premises – scans the ID to pass turnstile 1.	TANGO interface Smart device (wearable)	Indifferent, it is a routine procedure.		
2.	Worker goes to the main door – scans the ID to pass turnstile2 to access the shopfloor.	TANGO interface Smart device (wearable)	Indifferent, it is a routine procedure.		
3.	Worker walks to their designated work area (e.g. purple area).		Feels a sense of purpose and responsibility as he prepares to perform his job duties.		
4.	The system monitors the location of the workers through their wearable device.	TANGO platform Smart device (wearable)	Feels a sense of security knowing that their location is being tracked and that they are accounted for in case of an emergency.		
5.	Worker moves from purple area to yellow area (unauthorised access).		if the worker is unaware that they are entering an unauthorised access area, they may feel confused or disoriented and may be unsure of how to proceed.		
6.	System detects that the worker is moving towards an unauthorised area OR outside of the purple group– issues an alert to the supervisor.	TANGO platform Smart device (wearable)		Supervisor	

PERSONA:	Operational worker (shopfloor)				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
7.	Supervisor takes a countermeasure.	Smart device (tablet, wearable)	The supervisor approaches the worker in a calm and respectful manner and explains the situation clearly, the worker may feel relieved that the issue was brought to their attention before any harm was done.	Supervisor	
8.	Worker returns to his main area and finishes his tasks.		Relieved that the whole situation has ended.		

PERSONA:	Shopfloor supervisor				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Workers walk to their designated work area.		Indifferent, it is a routine procedure.		
2.	System detects that the worker is moving towards an unauthorised area OR outside of the purple group– issues an alert to the supervisor.	TANGO platform Smart device (wearable)		Operational worker	
3.	The supervisor receives a notification on his mobile device (phone, wearable, etc.).	TANGO interface	Concern: The supervisor may feel worried about the safety of the worker and other employees in the unauthorised area. They may also be concerned about the potential consequences		

PERSONA:		Shopfloor supervisor			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
			of the worker's actions, such as damage to equipment or delays in production.		
4.	Supervisor takes a countermeasure.		Supervisor may feel anxious or stressed about having to take action to correct the situation.	Operational worker	
5.	Unauthorised Access attempts are also recorded in the (security) platform system.	TANGO platform		Operational worker	
6.	The supervisor receives a report of all unauthorised access attempts – Interesting for repeating attempts from the same people.	TANGO interface	May feel the need to investigate further and take more drastic measures to prevent unauthorised access, such as reviewing security camera footage or increasing security measures.		

PERSONA:		Management staff			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Review and analyse safety and environmental data from reports	TANGO platform	Would likely view the safety and environmental reports as important tools for tracking progress and identifying areas for		

PERSONA:	Management staff				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
			improvement in their efforts to promote a safe and environmentally responsible workplace.		
2.	Meet with the environmental team to discuss strategies for reducing the environmental impact of the RiaStone operation.		Concern: may feel concerned about the environmental impact of the company's operations and may want to take urgent action to address any issues that have been identified.		
3.	Work with the safety team to develop and implement new safety systems to monitor incidents in real-time and enable early recognition and mitigation actions.		May feel a sense of pride in their ability to work towards achieving their goal of promoting workplace safety.		

PERSONA:	Maintenance staff				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Contact Vendor to ask for support, upgrade etc.	Email, phone	Feel relief that they can get help	Vendor	
2.	Allow control of remote access to the vendor	TeamViewer TANGO Platform	Feel a sense of responsibility and pressure to ensure that	Vendor	

PERSONA:		Maintenance staff			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
			the vendor's access is secure		
3.	Security breach notification if the vendor is not following the path that he must follow.	TANGO platform	Anxiety, because something is wrong with the standard process		

PERSONA:		Technology provider (vendor)			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Vendor is informed by RIAS maintenance staff that a maintenance process needs to take place.	Email, phone	Feel a sense of responsibility to assist with the maintenance staff	Maintenance staff	
2.	Vendor connects remotely with RIASTONE	TeamViewer TANGO Platform	Excited to assist the company and demonstrate their expertise		
3.	Continuous authentication and access monitoring.	TANGO interface	Anxious about the security implications of remote access and the responsibility of maintaining the company's systems		
4.	The system records the actions of the vendor for future reference and reporting.	TANGO platform			

PERSONA:		Cyber attacker			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Attempting to connect to system (every data flow node – TANGO – Uploading data – Downloading reports - data)	Every device	Nervous, because he desperately wants to penetrate the system.	IT Department	The system does not allow connection from unauthorised users.
2.	Reattempts to enter system	Every device	Frustrated, because he is not able to achieve his goals.	IT Department	

6.5.3 Technology offerings used in use case scenario

TECHNOLOGY OFFERING	RELATION TO PILOT
Trustworthy Data Sharing	Evaluate Trustworthiness of remote maintenance clients, or of machines on the shopfloor based on security monitoring provided by RIAS systems. Moreover, workers Trustworthiness might be assessed using profiles (needs to be checked on GDPR and Ethics). Extension of ABAC (Attribute-Based Access Control).
Confidentiality and Privacy by Design	Support access control to infrastructure and equipment through the definition of attribute-based policies. This will enable the definition of policies such that the authorization mechanism, using identity data, can decide which digital resources should be accessed by who, especially in remote access (from vendors or employees).
Self-sovereign Identity Management	SSI Module enables the staff members to manage their data and provide only necessary information for the factory and its customers. SSI used (via ABE keys) to allow access to the manufacturing platform by organisation members, contractors, and 3rd parties.
Seamless Onboarding for Users and Devices	The mobile will enable seamless remote identity verification for staff members in order to allow them to manage their data and access the necessary information in terms of the factory and the customers. The onboarding will take place through the TANGO wallet, performing 3-step identity verification and allowing the creation of verifiable credentials through the SSI management. The component will allow also the onboarding of devices.
User Continuous Behavioural Authentication	Perform continuous behavioural authentication for workers and factory staff when accessing infrastructure and equipment.
Device Continuous Behavioural Authentication	For identifying and monitoring workers' wearable smart devices (e.g. smartwatch, smartphone, etc.) to identify any suspicious movement or behaviour.
Energy-efficient AI model training	A part of the security systems mentioned in the RIASTONE use case description are based on AI-powered continuous behavioural authentication, in case that model requires to be updated based on locally collected data without need of sharing that data, the usage of the Federated Learning component might be studied in case the current model is supported by the proposed component and there are resources for the model training (to be further investigated and finalized in D2.4).

6.6 KPIs

TITLE	DESCRIPTION
Reduction of privacy violation incidents in data sharing	Privacy assessment results comparison of existing infrastructure with TANGO proposed data sharing platform
Accuracy of user verification and authentication > 99.6%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate and failure to access.

TITLE	DESCRIPTION
Accuracy of device verification and authentication > 90%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate and failure to access.
Reduction of privacy violation incidents on shopfloor	This KPI measures the number of privacy violation incidents on the shopfloor, e.g., the number of unauthorised access attempts to restricted areas.
Cybersecurity Reduction in DNS attacks	This KPI measures the level of protection against cyber-attacks and unauthorised access to the company's systems and data.
Unauthorised Access attempt	This KPI measures the number of attempts per day/week/month. This KPI can provide insights into the effectiveness of the security measures.
Access monitoring (online)	This KPI measures the average time it takes to detect and respond to online unauthorised access attempts
Access monitoring (physical)	This KPI measures the average time it takes to detect and respond to shopfloor unauthorised access attempts.
Maintenance	This KPI measures the efficiency of the shopfloor maintenance staff in terms of minimising system failures and ensuring the operationality of the shopfloor systems during production.
Deviation compliance rate	The percentage of time that workers are in the different "colour" area.

7 Pilot 4 – Banking

7.1 Pilot case overview

The fourth pilot is about Financial/Banking Institutions and it is to be implemented in the task T7.5 during the months M24 – M36 of the project.

The 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.

ABI Lab will lead the execution of the pilot in the banking environment, focusing on the creation of a community of banking stakeholders external to the Project, who will: i) co-design, discuss and validate the results of the pilot; ii) communicate, and disseminate the pilot to engage end-users and additional banks; iii) interact with European and global standardisation entities to support policy/standard evolution.

7.2 Organisations involved

7.2.1 ABI Lab

ABI Lab is the Research and Innovation Center for the Bank promoted by ABI (Italian Banking Association) with the aim of encouraging dialogue between banks and innovation partners. We are a Consortium of 122 Banks and 70 companies whose mission is to analyse and promote innovation in the Italian banking sector. We carry out research with the aim of identifying innovative technologies and systems applicable to the banking world to improve processes, operations, services, and make management and interaction models between banks and customers even more efficient and cutting-edge.

Observing the opportunities offered by technology, we work to promote sustainable development for the benefit of all the players involved: banks, companies and the end customer. In addition to research activities, we collaborate with various institutions using our expertise to develop shared frameworks and guidelines. ABI Lab is leading the banking pilot.

7.2.2 NTT Data

NTT Data is a global company that provides IT services and solutions in the field of consultancy and in the field of system integration and outsourcing. A reality born in 1967 in Tokyo, listed on the stock exchange in 1995, which today has over 110,000 professionals, with offices in 50 countries, including Italy. NTT Data Italy represents a primary player in consulting and IT services, operating in system integration and consulting services. NTT Data Italy operates in all the main sectors with a particular focus on banking. NTT Data Italia has a partnership with ABILab to support innovative projects in this sector.

In the TANGO project NTT Data Italy is the technical partner for the banking pilot and provides technical expertise in analysis, design and implementation phases.

7.3 Existing Situation Mapping

Current situation

Currently, banks use diverse techniques to manage Anti-Fraud, including analysing suspicious transactions, verifying customer identities, monitoring customer behaviour, and collaborating with other banks and organisations through a logic of info-sharing.

Although the technological tools that PSPs have equipped themselves with for monitoring and detecting attacks aimed at their customers, they can be very different from each other, it is worth considering some results deriving from the annual survey carried out by CERTFin - The Italian Financial CERT. According to the CERTFin's "Bank Security and Cyber Fraud 2023" almost all the Italian respondent PSPs (96%) have equipped themselves with tools for monitoring anomalous transactions arranged via internet banking, followed by tools for monitoring anomalous transactions through Mobile app (84%), access monitoring tools on Mobile app and the provision of software useful for detecting the presence of malware on the device used by the user (83%).

Network monitoring tools are also widespread to identify clone/counterfeit sites (78%), to analyse internet banking access logs (75%) and intelligence tools to detect attacks or compromises (70%).

Almost 70% of respondents reported the use of AI technologies which, where indicated, form the basis of 65% of the tools used.

It is also worth mentioning that the 50% of the PSP respondents indicated that they use outsourced solutions.

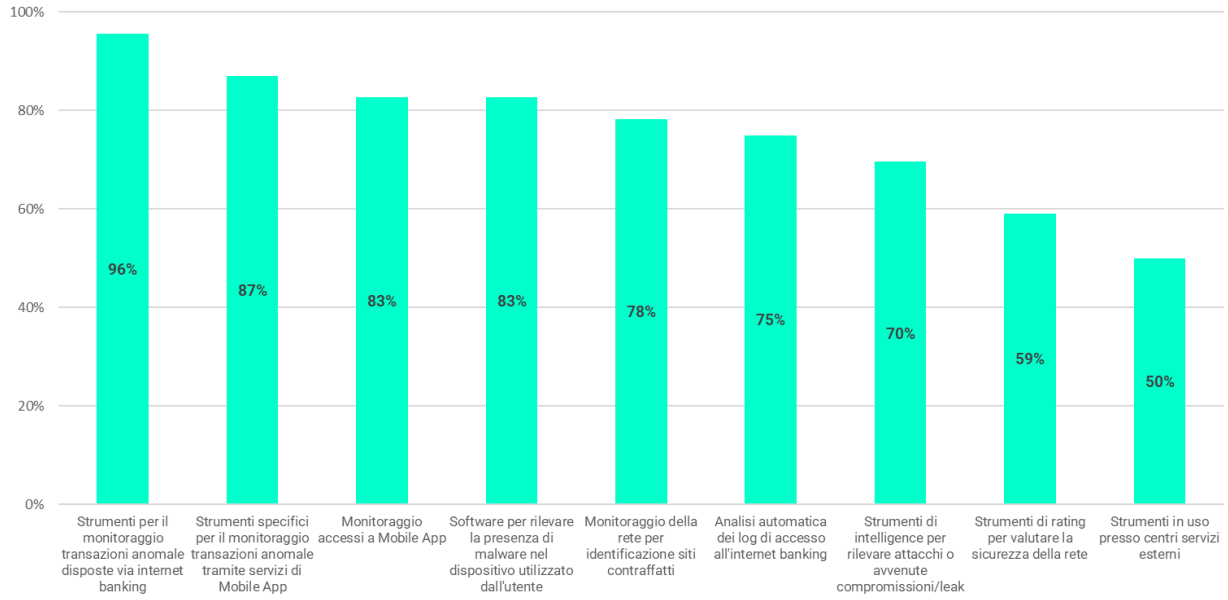


Figure 11: Technological tools used by PSPs to monitor and detect attacks aimed at their customers. Source: "CERTFin - Bank Security and Cyber Fraud 2023"

Outcome and Efficiency

Anti-fraud detection management in the banking sector, such as analysing suspicious transactions, verifying customer identities, monitoring customer behaviour, collaboration among banks and organisations, have proven to be extremely effective for identifying fraudulent transactions. Nevertheless, all of them require a significant allocation of resources and time. While anti-fraud detection systems can be costly, organizations should consider the potential consequences of fraud and the benefits of prevention.

7.3.1 A brief description of the platform

The banking ecosystem is highly fragmented (banks with different sizes, business models, products offered). In fact, some work on a regional, local scale, while others work on an international and wider scale. Due to the strong heterogeneity of the sector, mapping a common situation is quite complex. It is

possible to recognize a strong tendency to promote internally data driven approaches for the management of Anti-fraud operations.

To manage Anti-Fraud in the banking industry, PSPs (Payment Service Providers) use various platforms and systems. Some of them use platforms which provide comprehensive fraud management solutions, including fraud detection, investigation, and case management. Those platforms usually utilise advanced analytics, cognitive computing, and machine learning algorithms to detect potential fraud in real-time and provide alerts to fraud investigators. Therefore, 63% of banks, according to ABI Lab survey on ICT priorities of 2023, are starting to experiment with AI for security management (in particular anti-fraud). Those platforms can be integrated with other systems, such as customer relationship management and transaction monitoring systems, to provide a complete fraud management solution.

7.3.2 Key Stakeholders involved

Given the different nature of the banks operating in the Italian market, specifically defining which functions are involved in managing and monitoring Anti-fraud issues is particularly complex. Therefore, below we have provided a view of the reference areas and the functionalities used in monitoring the necessary activities:

- **Compliance Officer & Internal Auditor**: The Compliance Officer focuses on preventing compliance risks through policy and procedure development, while the Internal Auditor focuses on evaluating the effectiveness of existing policies and procedures to ensure that the organisation operates in compliance with applicable laws and regulations.
- **Data Analyst**: plays a critical role in Anti-Fraud processes by analysing large sets of data and identifying potential risks and threats to the organisation.
- **IT Specialist & Operations Manager**: play a crucial role in supporting Anti-Fraud processes. IT Specialists ensure that the necessary technology infrastructure is in place and functioning effectively, while Operations Managers oversee the day-to-day activities and ensure that policies and procedures are followed.
- **Risk Manager**: are responsible for identifying and mitigating risks associated with financial crimes. They work closely with other stakeholders to develop and implement risk management strategies and policies and ensure that staff are properly trained on those policies and procedures.
- **Area CISO security**: the CISO and the security team are responsible for protecting the bank's information and information systems from cyber threats. They work closely with other stakeholders to implement security policies and procedures, conduct risk assessments, monitor security systems, and respond to security incidents.

These stakeholders can play different roles and have different responsibilities, depending on the organisation and its specific needs. However, they all play a critical role in ensuring that the organisation's Anti-Fraud processes are effective, efficient, and compliant with regulatory requirements.

7.3.3 Main operations flow of the system

Anti-Fraud in the Banking Industry:

- Fraud Detection: The system uses advanced analytics and machine learning algorithms to detect potential fraud in real-time. The system can also generate alerts for potential fraud that requires further investigation.
- Investigation: The system allows fraud investigators to review alerts, investigate potential cases of fraud, and collaborate with other stakeholders to resolve cases.
- Case Management: The system enables fraud investigators to manage cases from detection to resolution, including tracking case details, documenting investigation findings, and collaborating with other stakeholders to resolve cases.

This operational flow is not exhaustive and can vary depending on the specific needs of the organisation and the systems used. However, it provides a general overview of the main activities involved in managing Anti-Fraud in the banking industry.

7.3.4 Data flows

Data Governance has been a priority for Italian banks. Today the initiatives are no longer exclusively linked to regulatory and control duties, but they insist more and more on the capitalization of data and knowledge assets in support of digital evolution. There is an increasing awareness of the strategic importance of data and their value for the business; a precious resource that the bank, equipping itself with adequate tools for enhancing its still unexpressed potential, can be used to speed up the process of digital transformation and to enable new (even innovative) usage scenarios of information. Therefore, the sector has been working increasingly hard on the setting and implementation of a technical-organisational system for the governance of corporate information. For this purpose, each bank has designed a tailor-made implementation path, carefully considering the starting situation, the technological and organisational maturity, the strategic objectives, and the conditions of the context.

Data flows vary according to the management model used by each bank.

It is possible to give a high-level view of data flows that are commonly used for Anti-Fraud operations:

- **Transaction Data**: The system collects and stores transaction data, including the transaction type, amount, and location.
- **Watchlist Data**: The system compares customer and transaction data against internal and external watchlists to identify potential matches.
- **Alert Data**: The system generates alerts for potential suspicious activities or potential fraud, which include relevant customer, transaction data.
- **Rules Data**: The system uses predefined rules to detect potential fraud, which include relevant transaction data.
- **Behavioural data**: The system records clients' habits and uses the data to prevent fraudulent transactions. In addition, such systems can be used to flag user behaviours that indicates an attempt to open fraudulent accounts using stolen identities.

These data flows are not exhaustive and can vary depending on the specific needs of the organisation and the systems used. However, they provide a general overview of the main data sources and data types involved in managing Anti-Fraud in the banking industry.

7.3.5 Related infrastructure

The technological structure of banks in terms of fraud monitoring varies according to the history of the institution. In order to provide a general overview of the related infrastructure and their settings involved, below are listed some possible examples:

Anti-Fraud use case:

- Fraud Detection Software: The system may use fraud detection software to detect potential fraud. The software may have specific settings for fraud detection rules, thresholds, and alerting.
- Monitoring Devices: The system may use specific data to detect potential fraud, such as location, identity cloaking services, such as hidden proxies and VPNs.
- Authentication Software: The system may use authentication software to verify the identity of users or devices. The software may have specific settings for authentication methods, access control, and session management.

These examples are not exhaustive and can vary depending on the specific needs of the organisation and the systems used.

7.3.6 Weak points of the system that can be enhanced

While Anti-Fraud systems in the banking industry are designed to be robust and secure, there are still some weak points that can be enhanced. Here are some examples:

- Enhancing the system with advanced analytics and machine learning can help detect and prevent new fraud techniques. Insider threat is a risk, but access controls, monitoring, and audits can

help mitigate it. Integration with other systems can enhance the effectiveness of the anti-fraud system.

Continuous improvement and adaptation to emerging threats are essential to maintaining the security and effectiveness of these systems.

7.3.7 Ways TANGO can enhance the system

Federated learning is a form of distributed machine learning that allows data to be kept locally while still enabling the creation of a global, collaborative model. This makes it ideal for the banking industry, where companies need to protect transaction data while still being able to apply machine learning algorithms to analyse patterns and predict future behaviour. With a federated learning platform, banks can pool their data without sacrificing privacy, and develop models that benefit from the collective intelligence of the entire network. By democratising access to data and providing a secure and privacy-preserving way to train machine learning models, federated learning has the potential to revolutionise the banking industry, enabling banks to make better, more accurate decisions while maintaining the highest levels of confidentiality and privacy.

We have proposed to an ecosystem of banks to choose between three use cases regarding AML, Distributed Intrusion Detection and Anti-Fraud, in order to find the most suitable ones based on their needs. From an analysis of the feedback we decided to focus on the Anti-fraud one.

In recent years, the growing digitalization of banking systems has led to an exponential increase in the amount of data processed and managed by financial institutions. However, this technological evolution has also brought an increase in risks related to data security and banking fraud. To effectively counter these risks, banks and financial institutions must adopt increasingly advanced and sophisticated fraud detection systems. In this context, Machine Learning represents one of the most promising technologies. Through the use of automatic learning algorithms, Machine Learning enables the processing of large amounts of data and the rapid identification of any anomalies or suspicious behaviours. This allows banks to identify fraud in real-time and intervene promptly to limit the damage. However, to achieve effective results, it is crucial that the Machine Learning model used is robust and precise. This means that it must be able to adapt to new forms of fraud and avoid false positives or false negatives, which could have serious consequences for both the bank and its customers. Therefore, the structuring of a reliable Machine Learning model represents a crucial aspect for the prevention of banking fraud and the protection of customer data.

The goal of the use case will be to considerably improve the capabilities of a predictive model for the management of banking operations. The sharing of model parameters, instead of sensitive data, allows banks to create a synergy in a safe way with the aim of structuring a more robust and efficient model.

Model parameters sharing provides two main advantages with respect to training on local data:

- **it improves models generalisation capabilities, thanks to the increase of data for training.**
- **It accelerates model updates to variations in data, allowing faster response to emerging threats.**

The platform will use federated learning to address two main needs of machine learning applications in banking: the need for huge quantities of data and the necessity of high privacy standards. The process is based on distributing model training between entities joining the network. Each entity trains a model on its own data and shares it with a central node, without sharing data necessary for training and evaluation. The central node generates a global model by aggregation of models received and shares it with federated entities. This process, repeated periodically, allows all entities to obtain a global model with consistent performance improvements with respect to the model trained locally.

The stakeholders identified for the use case are an ecosystem of national banks (4-6), which will take advantage of transaction monitoring models trained on bigger amounts of data.

Parameters of all the models generated by banks are transferred to the central node. The central node shares the parameters of the global model with the banks. Data flows will be checked to ensure consistency and rollback capabilities in case of failures.

The infrastructure will be distributed between the central node and banks. Models training will be performed on machines provided by the banks. The central node, on TANGO infrastructure, will extract parameters of the global model applying statistics to parameters obtained by banks.

The precondition to start the experimentation is that the model must be nearly identical for all participants in the network; there can be some small tolerances, meaning slight differences, but essentially the model is almost coincident across all peripheral systems.

The parameters to be exchanged will be dynamically constructed based on a dataset that will be initially agreed upon by all participants. The dataset cannot be simply limited to basic information such as transaction amount, time, IBAN, etc., which are undoubtedly fundamental but may not be sufficient.

Our idea is to expand the database as much as possible to facilitate the system's training. For example, it could be interesting to include additional information, such as whether the transaction was initiated via mobile or home banking, details on the operating system used, and the brand and model of the device being used, among others.

These are still "neutral" pieces of information that would be useful to have, but we can also explore the possibility of including extremely sensitive information precisely because these data will never leave the bank.

For instance, customer gender, customer nationality (if the beneficiary is from a high-risk country, we can imagine that this transaction may carry a higher risk factor compared to others), and so on.

7.3.8 Type of Information required for TANGO

We would expect to collect:

- **Model parameters**;

These will be data structures produced by each bank after training a model on their own data. Model parameters will be shared with a central node. The central node will share optimised global parameters with each bank.

- **Financial and bank data**;

These data will not be shared between participants due to legal restrictions. However, we believe it will be feasible to collect some synthetic samples for testing purposes.

- **Network operations**;

We believe that a form of monitoring of parameter sharing to and from the central node will be necessary in order to ensure correct operation of the whole federated network. We expect communications for periodic sharing of parameters. Some Federated Learning frameworks offer tools to manage this communication.

7.4 User Requirements

Code	**UR-TUA-BN-001**
Category	**Trusted user authentication**
Description	All categories of users must be authenticated to the system in order to have access to the relevant information.
Priority level	High

Code	**UR-PMT-BN-002**
Category	**Process monitoring**
Description	Participants should be able to monitor the performance of the system over time to ensure that it flags fraudulent activity accurately.
Priority level	High

Code	**UR-SAD-BN-003**
Category	**System adaptability**
Description	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.
Priority level	High

Code	**UR-TDS-BN-004**
Category	**Trustworthy Data sharing**
Description	Participants must be able to share data in a trustworthy and secure way.
Priority level	High

Code	**UR-DMN-BN-005**
Category	**Data management**
Description	Participants must be able to upload financial data to the system in a trustworthy way.
Priority level	High

Code	**UR-DMN-BN-006**
Category	**Data management**
Description	The datasets must be prepared to comply with the data structure required by the platform (data preparation and harmonization).
Priority level	High

Code	**UR-DAR-BN-007**
Category	**Data analysis and reporting**
Description	Participant should be able to understand the reason why the system detect anomalies that may indicate fraudulent activity.
Priority level	High

Code	**UR-DAR-BN-008**
Category	**Data analysis and reporting**
Description	Participants must be able to review the overall system performance and regularly assess results to identify if any modifications are required.

Code	**UR-DAR-BN-008**
Category	**Data analysis and reporting**
Priority level	High

Code	**UR-GCO-BN-009**
Category	**GDPR and related regulation compliance**
Description	The financial data must be handled according to the GDPR.
Priority level	High

Code	**UR-GCO-BN-010**
Category	**GDPR and related regulation compliance**
Description	The financial data must be handled according to Banking Secrecy and AML regulations.
Priority level	High

Code	**UR-PCY-BN-011**
Category	**Protection from cyberattacks**
Description	The confidentiality, integrity and availability (CIA) of the system must be always preserved.
Priority level	High

7.5 Use Case Scenarios

Banks, also referred as “Payment Service Providers (PSPs)”, regularly perform Anti-fraud monitoring using fraud prevention solutions in order to identify and block the fraudulent activity in real time.

Ideally, the anti-fraud solution analyses each transaction and based on various parameters, associates it a risk. If this risk exceeds a threshold, the transaction is most likely fraudulent and is instantly blocked and/or deeply analysed by operators of the anti-fraud team.

Italian PSPs participating in the pilot will enhance their actual anti-fraud solution by integrating the results returned by the system developed within TANGO project. They will leverage federated learning technologies to share model parameters that are trained only with local financial transactional data and other relevant information avoiding data privacy leakages.

Italian PSPs participating in the pilot (between 4 and 6), will obtain the same federated learning model and use it to detect anomalies that may indicate fraudulent activities.

In order to allow each bank to train its own model, a common data structure will be necessary. Our preliminary analysis shows that data used by each bank can differ significantly, but we expect to find a consistent number of features in common between those datasets. Applying Federated Learning even with a reduced number of features can show the benefits of this approach with respect to on premise training only with local data.

7.5.1 Personas

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
AF_01	**Bank Employee** **Antifraud Operator**
IDENTITY	**QUOTES**
Name: Fabio Age: 25 years Occupation: Antifraud operator Domain: Antifraud Years of experience: 5 years	*"I take pride in my role as an Antifraud Operator, analyzing suspicious financial transactions and working tirelessly to stop fraudulent activities. However, there's always a concern about making a mistake and blocking genuine transactions."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
1. Analyse suspicious financial transactions 2. Stop quickly fraudulent transactions	1. A possibility to make a mistake by stopping genuine financial transactions 2. Do not identify new fraud patterns in time
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
1. Antifraud platforms 2. Federated learning technologies	N/A
SHORT DESCRIPTION	
Fabio is 25 years old, and he is working as Antifraud operator in a bank. His daily activities revolves around analysis of suspicious financial transaction in order to prevent e stop fraud. His daily activities include analyse and understand new fraud patterns, identify, and block fraudulent transactions involving IBAN managed by fraudster and money mules.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
AF_02	**Bank Customer Service Representative**
IDENTITY Name: Maria Age: 28 years Occupation: Bank Customer Service Representative Domain: Customer Support and Anti-Fraud Years of experience: 6 years	**QUOTES** *"I often encounter frustrated customers who have been victims of fraud. I wish there was a more effective way to prevent these incidents and protect our customers."*
GOALS	**FRUSTRATIONS / PAIN POINTS**

(what he/she wants to achieve)	*(what frustrates him/her currently at work)*
1. Provide excellent customer support to bank clients. 2. Minimize instances of fraud-related complaints and issues.	1. A lack of comprehensive tools for identifying and stopping fraud early. 2. Deal with irate customers who have fallen victim to fraudulent transactions.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
1. Banking software and customer service platforms. 2. Fraud monitoring and detection systems.	Good communication and problem-solving skills. Understanding of various fraud schemes and methods.
SHORT DESCRIPTION	
Maria, a 28-year-old bank customer service representative, has been working in the customer support and anti-fraud domain for 6 years. She takes pride in providing excellent assistance to the bank's clients. However, she often encounters frustrated customers who have been victims of fraud, which motivates her to find better ways to prevent such incidents. Maria wishes there were more comprehensive tools available to identify and stop fraud early, reducing the negative impact on customers. She possesses strong communication and problem-solving skills, essential for addressing fraud-related issues effectively.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
AF_03	**Chief Information Security Officer (CISO)**
IDENTITY Name: Giovanni Age: 50 years Occupation: Chief Information Security Officer (CISO) Domain: Information Security and Risk Management Years of experience: 25 years	**QUOTES** *"The evolving sophistication of fraud attempts keeps me up at night. Our security measures must be one step ahead to protect our organization and customers."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
1. Enhance the bank's overall cybersecurity posture. 2. Proactively identify and mitigate potential fraud risks. 3. Ensure compliance with industry regulations and standards.	1. Securing the increasing number of endpoints and devices in the bank's ecosystem. 2. Dealing with budget constraints while maintaining robust security measures.

TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
1. Security monitoring and threat detection tools. 2. Incident response and crisis management protocols. 3. Experience in conducting security audits and risk assessments.	Knowledge of regulatory requirements related to data security and fraud prevention. Strong leadership and communication skills.
SHORT DESCRIPTION	
Giovanni, a 50-year-old Chief Information Security Officer (CISO), possesses a wealth of experience in the domain of information security and risk management, totalling 25 years. As the CISO, his primary concern is safeguarding the bank's digital assets and protecting both the organization and its customers from fraud attempts. Giovanni is dedicated to continuously enhancing the bank's cybersecurity posture and proactively identifying potential risks. He works diligently to ensure compliance with relevant industry regulations and standards. However, the evolving nature of fraud and the growing number of endpoints and devices pose challenges. Despite budget constraints, Giovanni leverages his expertise in security monitoring, incident response, and risk assessments to maintain robust security measures. His strong leadership and communication skills enable him to effectively guide the organization in addressing security challenges.	

7.5.2 User Journeys

Our ambition is to improve the fraud rate of Italian banks, which is an index that describes how often fraud occurs in transactions. Currently, we not only know the average fraud rate but also the rates of false positives and false negatives, which provide further details on the effectiveness of the anti-fraud systems currently used by banks.

We want to try and achieve this goal by using the technique known as federated learning, which is a federated system composed of a network of N nodes, where each node individually learns how to recognize a fraudulent transaction through interactions with its internal system. Subsequently, the nodes share only the parameters that characterize the learning model of the peripheral system with a centralized system. The central system will be responsible for aggregating, normalizing, and redistributing these parameters to all nodes in the network. One of the advantages is that all sensitive information remains within the peripheral system, yet each node benefits from what other entities learn during their experiences.

Workflow as is

We currently have an existing user journey model represented by the first workflow, where the anti-fraud system sends an alert that can refer to:

An operation that the system was able to handle autonomously: The predefined criteria inputted into the system are fully satisfied, enabling it to recognize with a certain degree of accuracy if a specific transaction is fraudulent. Consequently, the system autonomously blocks the transaction.

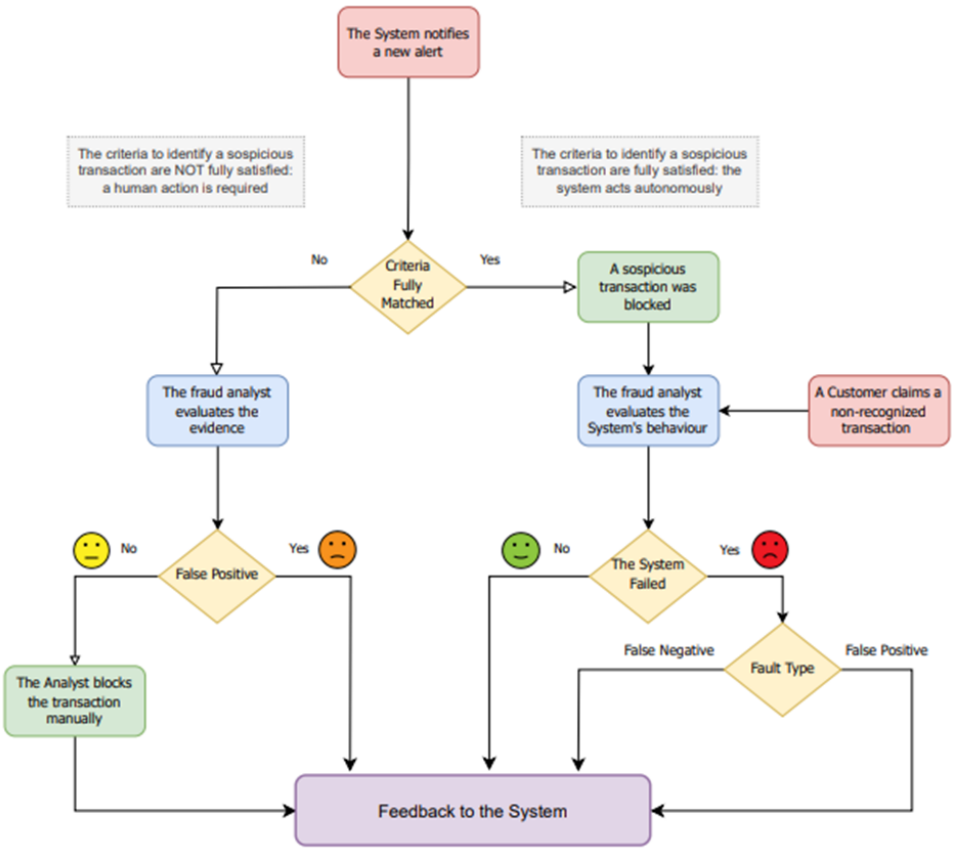
An operation that the system was NOT able to handle autonomously: In other cases, when these criteria are not fully met, the system raises an alert that requires further action by an anti-fraud operator. The operator will then assess whether the individual transaction is legitimate or not, making a manual decision.

There are also additional considerations in both cases:

a) There might be situations where the system acted autonomously but made a mistake, resulting in a false positive. In such cases, the system thought the transaction was fraudulent when it was not.

b) Conversely, there could be instances where a customer disputes a transaction that the system deemed genuine, resulting in a false negative.

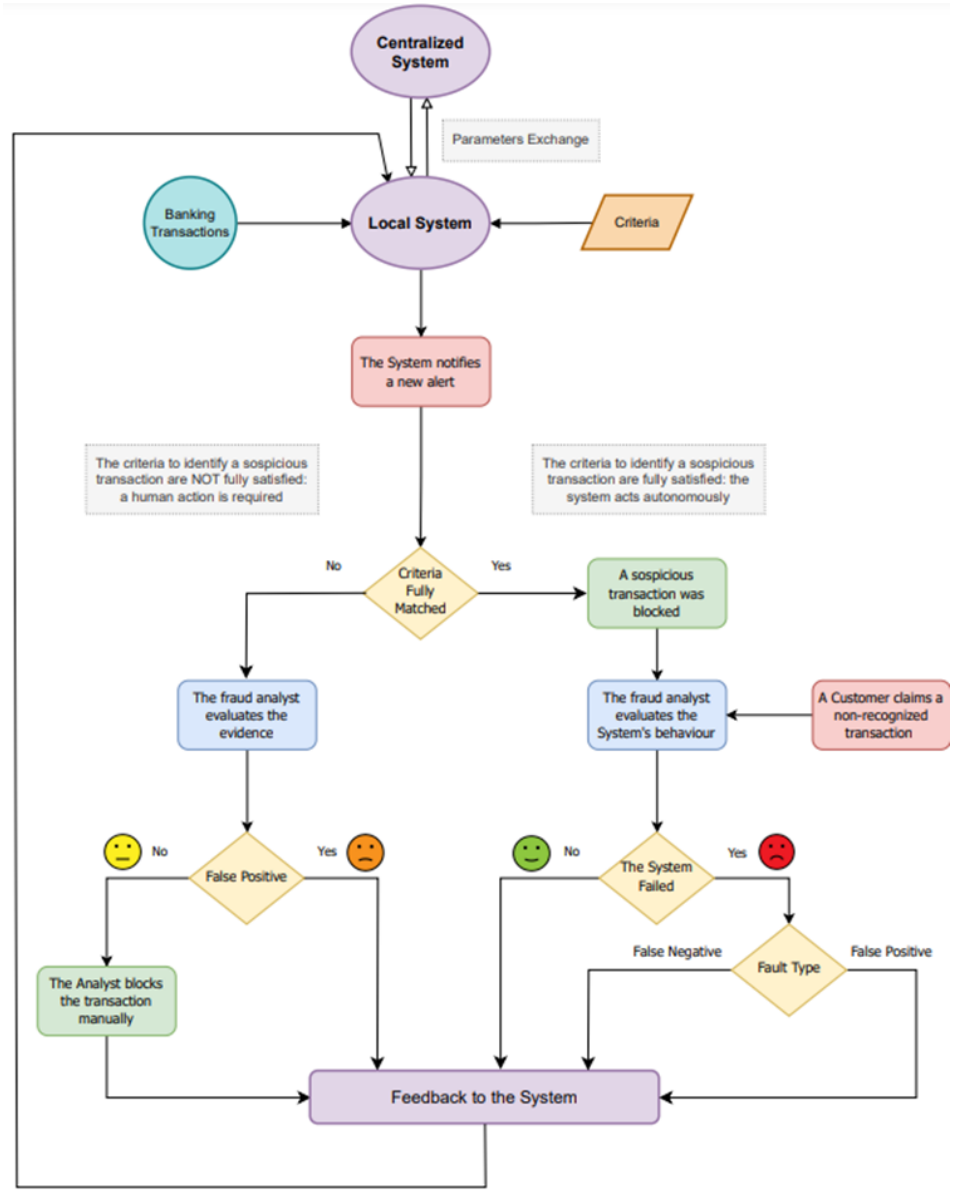
These scenarios highlight the complexity of the anti-fraud system, where balancing the autonomy of fraud detection with the potential for errors requires continuous refinement and improvement.



WORFLOW TO BE (FEDERATED LEARNING INTEGRATION)

In the new envisioned workflow, each node leverages the collaboration of other nodes. Through a centralized system and with a frequency yet to be defined, there will be an exchange of parameters among all individual systems. This periodic exchange will enrich the knowledge and, consequently, the capabilities of each system in recognizing anomalous transactions.

The federated learning approach fosters a collective learning process, where the nodes contribute their local insights while preserving sensitive data. By sharing model updates and knowledge, the overall fraud detection system becomes more robust and effective in detecting emerging fraud patterns and improving accuracy over time. This collaborative learning mechanism ensures that each node benefits from the collective intelligence of the entire network while maintaining data privacy and security.



By adopting the federated learning approach, we expect that it can individually improve both the rates of false positives and false negatives, ultimately leading to an enhancement in the overall fraud rate.

Through regular nationwide assessments, we will be able to easily compare the performance of the federated system with industry benchmarks. This will allow us to promptly gauge whether the experimentation is moving in the right direction or not. The ability to monitor and analyze the system's performance against established industry standards will provide valuable insights into the effectiveness of the federated learning model in combating fraud.

This ongoing evaluation will enable us to fine-tune and optimize the federated system continually, making it more adept at recognizing and preventing fraudulent transactions while also reducing the number of legitimate transactions incorrectly flagged as fraudulent (false positives) and the number of fraudulent transactions that go undetected (false negatives). The goal is to achieve an efficient and accurate anti-fraud system that protects both the bank and its customers.

With respect to the user personas identified, below we describe the user journeys:

PERSONA:		**Antifraud Operator**			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Login to the Federated Learning platform	Secure login portal, Multi-factor authentication	Eager, prepared	Antifraud Team	As the day begins, the operator logs into the Federated Learning platform with a sense of readiness to tackle potential fraud cases and leverage the collaborative power of the system.
2.	Analyse the results provided by the model trained with the contribute of all participants	Interactive dashboard, Data visualization tools	Focused, analytical	Antifraud Team	The operator navigates through an interactive dashboard and uses data visualization tools to carefully analyze flagged transactions, identifying potential fraudulent patterns and trends.
3.	Based on the results obtained from the federated learning system, adapt the anti-fraud systems to promptly intercept fraudulent transactions	Anti-fraud systems	Proactive, determined	Antifraud Team	Drawing insights from the federated learning model, the operator promptly adapts the anti-fraud systems through a user-friendly fraud detection interface to intercept and prevent fraudulent transactions. Their proactive approach contributes to enhancing the

					system's efficiency.

PERSONA:		**Bank Customer Service Representative**			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Receive customer query about a flagged transaction	Customer Call or CRM system	Attentive	Antifraud Team or Bank Customer	The customer service representative receives a query from a bank customer regarding a flagged transaction. They ensure a reassuring and empathetic response, explaining that the transaction is being reviewed by the antifraud team.
2.	Collaborate with the Antifraud Team for investigation	Internal communication channels, collaboration tools	Cooperative, proactive	Antifraud Team	The representative collaborates with the antifraud team, providing additional customer information and context for the flagged transaction. Their collaboration aids in the timely resolution of the customer's concerns.
3.	Communicate resolution to the customer	Customer call, email, CRM system	Helpful, informative	Antifraud Team	Once the investigation is completed, the representative communicates the resolution to the customer. If the transaction is legitimate, they provide assurance and clarity, but if fraudulent, they initiate appropriate

					actions to secure the customer's account.
4	Share customer feedback for system improvements	Feedback system, communication channels	Proactive	Antifraud Team, Data Scientists	The representative shares valuable customer feedback on the accuracy and efficiency of the antifraud system. This feedback is utilized by data scientists to enhance the model's performance.

PERSONA:		**Chief Information Security Officer**			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Evaluate the potential of federated learning	Reports, Research articles	intrigued	Top Management, Data Scientists	The CISO learns about the potential benefits of federated learning for anti-fraud and initiates discussions with data scientists and top management to assess its feasibility.
2.	Formulate a plan for implementation	Meetings/ Collaboration tools	Focused, strategic	Top Management, Data Scientists	The CISO collaborates with data scientists and top management to formulate a detailed plan for implementing federated learning in the anti-fraud system. They consider data privacy, security, and cost implications.

3.	Oversee the deployment of federated learning	Project management tools, Progress reports	Responsible, diligent	Data Scientists, IT Team	The CISO oversees the deployment process, ensuring that the federated learning system is integrated effectively, and that data is shared securely among the participating nodes.
4.	Report on the success of the federated learning implementation	Management presentations, Reports	Confident, satisfied	Top Management, Antifraud Team	The CISO presents the outcomes of the federated learning implementation to top management, highlighting its success in reducing fraud rates and enhancing customer protection. These stages illustrate the experiences and responsibilities of the Bank Customer Service Representative and the Chief Information Security Officer in utilizing the federated learning approach to combat fraud and enhance the bank's overall security posture.

7.5.3 Technology used in each use case scenario

TECHNOLOGY OFFERING	RELATION TO PILOT
Blockchain-based Data Storage and Sharing	If there is a need for sharing verified regulated data within the Banking pilot, norbloc's decentralized solution Fides will allow for compliant and secure data sharing.
Self-sovereign Identity Management	Organization service (machine) authenticates to other service to share data with other organizations. Organization´s added to trusted registry based on their well-known public Decentralized identifiers
User Continuous Behavioural Authentication	Continuous behavioural authentication incorporates transaction patterns that allow the detection of unauthorised access and potential fraud. The solution can provide the basis for the transactional patterns detection in a federate learning concept. Further behavioural elements such as the device usage, biometrics and user movements can be potentially explored
Energy-efficient AI model training	Machine learning can be the base for a solution capable to analyse the large amounts of data depicted in the three scenarios proposed for this use case. Data sharing might offer a great opportunity for the creation of robust predictive models, but due to the nature of the data in this use case, data sharing is sometimes not possible. In this case, the inclusion of a federated learning component as the one here presented might facilitate the training of predictive models in a de-centralized way, with no need for data sharing. In order to ease the predictive model creation in order to process the large amounts of data depicted in the banking use case description, the AutoML component might be of consideration for its use with this purpose. This component will ease the creation of an optimised predictive model by means of evaluating different hyperparameters automatically in order to search for the best result metrics
X-AI for Privacy and Trust Enhancement	The financial pilot is interested in training Machine Learning models that among others will be able to detect fraudulent activities. XAI would be great at explaining why a specific activity was characterized as fraudulent and in turn detect flaws in the training process.
Infrastructure Management based on AI	RENOPS could utilised in two ways (to be further investigated and finalized in D2.4). First way would be directly via RENOPS scheduler script, that would find most optimal time to schedule backups, analytics, or AI model training. Second way would be indirectly as part T5.2 Energy efficient model training and its proposed MLops pipeline.

7.6 KPIs

- Difference in performance between model trained only with local data and model obtained after parameter centralization.
- Algorithm accuracy percentage >90%
- Number of weights aggregation processes concluded successfully.

8 Pilot 5 - Public organisations

8.1 Pilot case overview

The fifth pilot is about Public Organizations and it is to be implemented in the task T7.6 during the months M24 – M36 of the project.

In this pilot TANGO framework will be tested to demonstrate its effectiveness in bureaucratic but at the same time high-risk processes for visa applications. VISARIGHT will lead the pilot in Berlin supported by the local migration office ensuring privacy, transparency, and security of data gathered and processed by citizens and facilitating the digitization process of the collected data. Technology-based data sources, ensuring the data sovereignty, integrity, and authenticity will be demonstrated considering third party software solutions which are involved in the entire process and lead to more exposure. Legal and ethical assessment of the proposed solutions will be carried out, along with recommendations for appropriate auditing mechanisms to check whether data retention laws are respected in the process.

8.2 Organisations involved

8.2.1 VISAR

VISARIGHT (VISAR) is an immigration tech scale up with a clear mission: to revolutionise visa procedures and migration to Germany and the European Union. To achieve this, VISAR combines innovative technology and algorithms with professional expertise. This professional experience starts with the founder of VISARIGHT, who previously worked for years at the German Foreign Office and various foreign missions and can draw on broad experience in visa and migration issues. From the headquarters in Magdeburg and home offices worldwide, they work as one team across several time zones to support their clients and partners around the globe. As a team of almost 35 experts in visa procedures, German immigration law, customer support and IT development, they combine different cultures and experiences from all over the world. VISAR is committed to equal rights for all people in the workplace, regardless of religion, gender, ethnic background or sexual identity.

During the TANGO project, VISAR will lead the Task T7.6 and is going to collaborate with the local migration office in Berlin. By doing so, the TANGO framework will be tested in order to demonstrate its effectiveness in bureaucratic but at the same time high-risk processes for residence permit applications. VISARIGHT is very experienced in this environment, as they are dealing with similar procedures, which are characterised by long delays, non-transparent process, more paper and less digitalization, anxiety, and pressure on the applicants.

8.3 Existing Situation Mapping

VISAR is a platform that assists third-country nationals with the relocation process to Germany. Applying for a visa in a home country and obtaining the residence permit in Germany are multi-stage processes in which the correct implementation of all the nuances and requirements is critical. VISAR platform's is divided into steps according to the main points of the standard relocation - visa application in a home country, city registration in Germany, application for the long-term residence permit in Germany. Upon successful completion of all steps, the relocation employee receives the long-term residence permit in Germany and VISAR successfully completes the task of assisting the relocation employee in the relocation process.

The platform is primarily intended for use by employers, who are registered on the platform. Employers can create cases for their relocation employees on the platform, and the relocation employees will receive an activation link for registration. After a relocation employee is registered, an introduction email from the responsible VISAR employee is automatically sent to them. The VISAR platform uses inbuilt algorithms to assess the eligibility of employees for the preferred visa types. The type of visa will depend on the relocation employee's employment's requirements, educational and professional

background, the documents the relocation employee can provide, etc. Once the appropriate visa type has been determined by the VISAR platform, it is also checked manually by the VISAR employee to eliminate the possibility of technical error.

As the relocation employee moves through the relocation process and all required steps, getting assistance from the VISAR employee, the employer can constantly follow the progress on the VISAR platform and be informed in case there are any delays or issues during the procedure. The same feature is available for the relocation employee - the employee gets notified by the email in case the VISAR employee does any changes in his/her profile (e.g., create a checklist for the next appointment or book an appointment at the Diplomatic Mission or the immigration office). The VISAR employee is also able to see if the employer or the relocation employee changes any details in the profiles. The possibility of tracking the progress by all stakeholders ensures the transparency and openness of the VISAR platform.

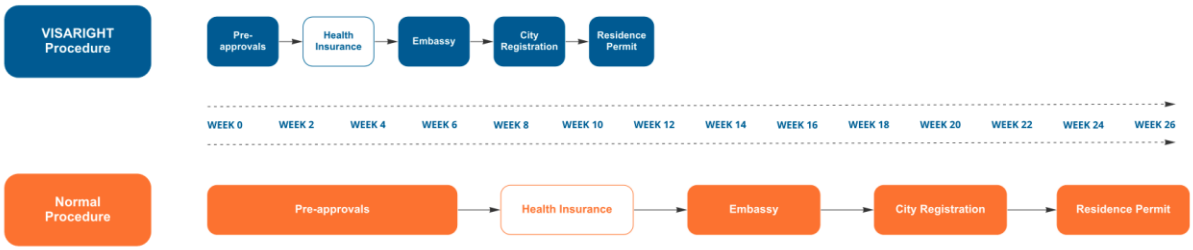


Figure 12 VISAR visa application procedure vs normal procedure

In summary, the VISARIGHT platform is designed to make the relocation process to Germany as efficient and user-friendly as possible for both employers and relocation employees. It streamlines the process, provides a centralised place for tracking cases, and provides support for the visa and residence permit application processes by assigning the responsible VISAR employee.

8.3.1 Key Stakeholders involved

In this subsection we list the different stakeholders that are involved in the pilot implementation. They will be further described and analysed in the personas and user journeys subsection.

1. VISAR employee - Customer Support Manager OR Case manager,
2. Employer - HR Manager,
3. Relocation employee,
4. Authority employee (Diplomatic Mission, Federal Employment Agency, City Hall, Immigration office).

8.3.2 Main operations flow of the system

Employers are a key stakeholder of VISAR. They initiate the registration process and are the first point of contact with the VISAR platform. The process for an employer using VISAR platform includes creating an account, understanding the benefits of the platform, and providing necessary documents and information for verification as a company, such as registration documents, VAT number etc. (A1). After this step, the employer is finished with initial onboarding and is ready to create cases. The employer is asked to choose the services required for the particular relocation employee (apartment packages, relocation for family members etc.) and indicate the relocation employee's job details. Once the employer gives all the details, VISAR platform sends an email invitation to the relocation employee to access the platform (A2). From now on, the employer can follow the progress of each relocation employee's relocation, starting with the preparation of the necessary documents in the home country till the successful obtaining of the residence permit in Germany, on the platform.

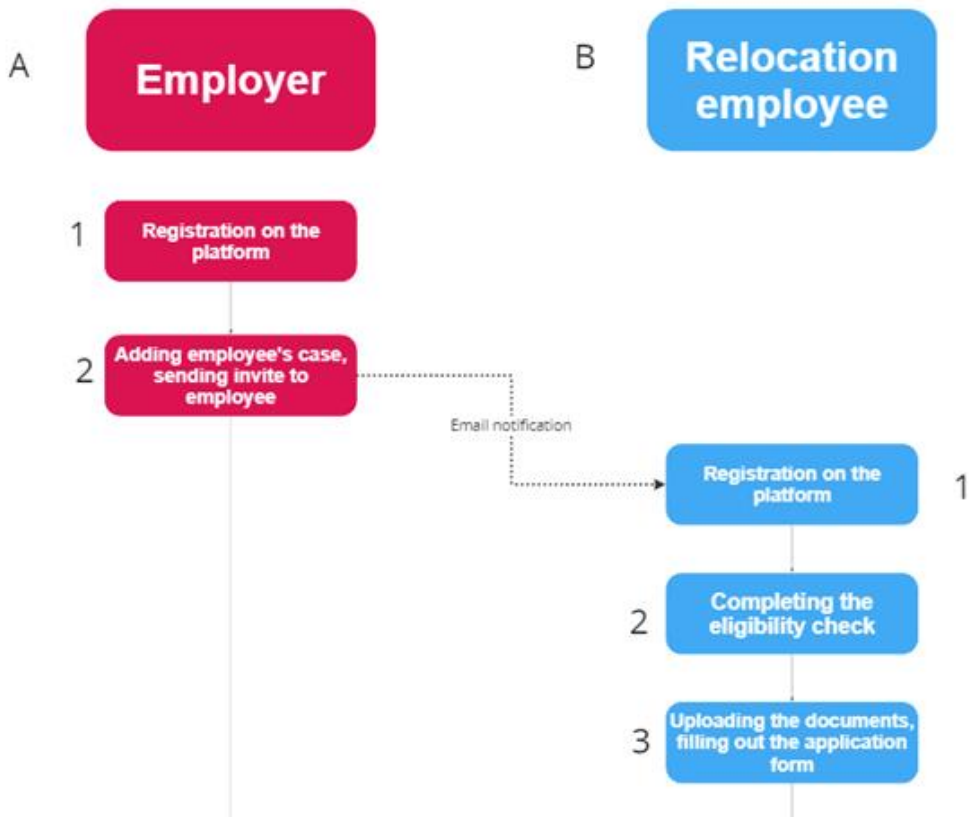


Figure 13 VISAR steps and flow between stakeholders

Once the relocation employees sign-in to VISAR platform (B1), the application starts the eligibility check process. This is one of the central components of our platform. Eligibility checks, which are based on a variety of laws, provide a relocation employee with an initial overview of his or her chances of success. The relocation employee is asked for individually relevant information and then he/she is automatically classified according to the legal basis. The eligibility check provides an informed initial assessment, confirms visa eligibility, or identifies any gaps for the relocation employee (B2).

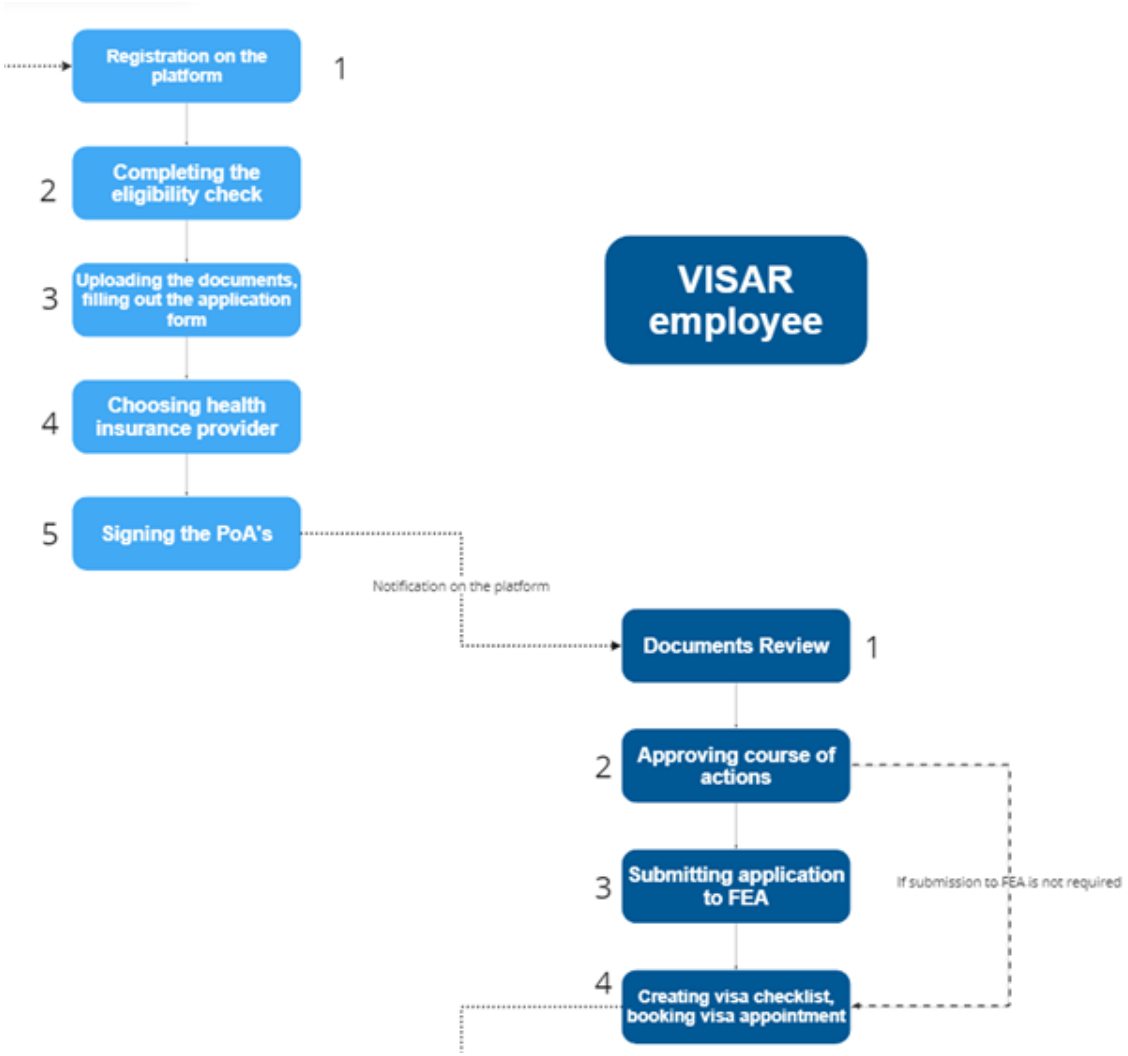


Figure 14 VISAR steps and flow between stakeholders

After relocation employees have passed the eligibility check to confirm their eligibility for a visa, they complete their profile and upload all required documents (B3). Moreover, the relocation employees have a possibility to choose a health insurance provider if the employer approved this service for the relocation employees before (B4). The last step of the relocation employee's registration on the VISAR platform is to sign the Power of Attorney PoA to make the VISAR its own representative at all authorities' offices (B5). A VISAR employee then reviews the application (C1) and determines the course of actions in the personalised dashboard on the platform (C2). Depending on the relocation employee's home country, educational and professional background, the type of visa and job details the next steps might include legalisation/certification/translation of the documents, recognition of Foreign Qualification, and/or FEA (Federal Employment Agency) (pre-)approval processes (C3) — the VISAR employee informs the relocation employee as well as the employer whatever the case. When all the formalities are completed, the VISAR employee schedules an appointment at the Diplomatic Mission and provides the relocation employees (and family members if there are any) with a checklist of documents for their in-person interview (C4).

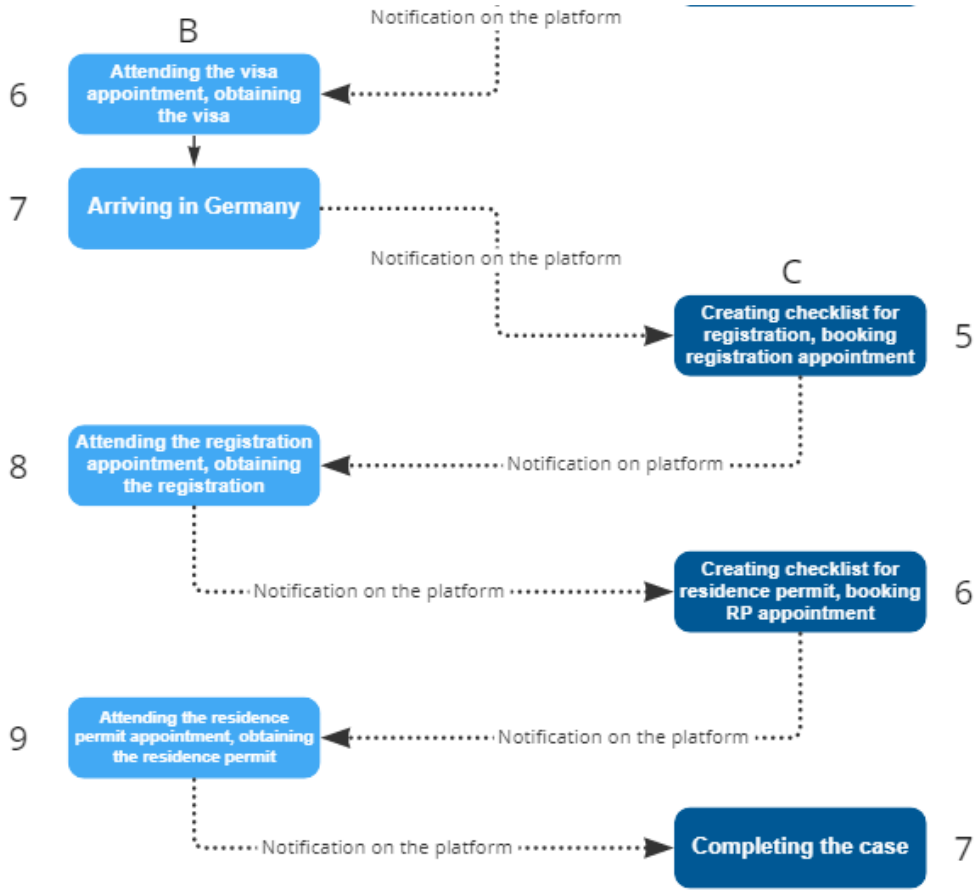


Figure 15 VISAR steps and flow between stakeholders

After the visa interview, the relocation employee only needs to wait for the visa approval (B6). The visa processing time depends on multiple factors like the current capacity and the workflow of the Diplomatic Mission, completeness of the relocation employee's documents, processing of additional procedures (e.g. verification of family members' certificates). Once the relocation employee arrives in Germany after the visa issuance (B7), VISAR employee assists with documents' preparation for the city registration at the local City Hall (C5, B8) and submitting the application to the immigration to obtain the residence permit(C6, B9). The residence permit is checked by the VISAR employee once the relocation employee has it at hand. After that, the case can be finalised (C7).

8.3.3 Data flows

In the current case of VISAR, the data is entered manually into the platform by the respective user (employer or relocation employee). The personal data is uploaded to VISAR's platform by the employers and relocation employees in digital form, mostly in PDF files, before they start the visa process. Data entered by both parties into the system is to be then evaluated and processed. Depending on the respective step, data is either used for filling out the corresponding documents or sent to the relevant stakeholders (e.g. authorities).

By allowing employers and relocation employees to upload their relevant data once, VISAR can streamline the immigration process and make it more efficient for both. This can save them time and effort, as they will not have to repeatedly enter the same information for different forms. Additionally, using this data can help ensure that the information entered in the forms is accurate, reducing the risk of errors or delays in the immigration process.

8.3.4 Related infrastructure (devices, software, hardware) and their settings in the current system

VISARIGHT Platform is the central unit through which all relevant processes and operations are performed. All processes such as document generation, eligibility-check, and the individual visa workflow are technically reproduced and initiated via this system. The platform is a management unit for relocation employees, VISAR employees and employers alike. The VISARIGHT platform is divided into a few parts depending on the purposes and goals. There are relocation employees' applications and backend services that communicate with users and between each other.

Our main databases are encrypted in rest by AWS RDS and AWS ElastiCache encryption features. The data transit between employers, relocation employees and our servers is encrypted by SSL certificate. Our internal services communication is protected by VPC and strict security group rules for resources. In production, our main databases are replicated in two availability zones. They are replicated via AWS RDS/AWS MemCache automatically. For our main DBS, backups are performed automatically via AWS RDS, every day during the maintenance period. The last 7 backups are stored in time. We also automate backups right before essential system updates and data schema migrations. The access to backups is restricted only to developers' team members participating in maintaining the particular services. Automatic encryption at rest is enabled for all backups.

8.3.5 Weak points of the system that can be enhanced

As VISAR strives to provide support to relocation employees in their national visa applications for Germany, it is important to be aware of its limitations. Currently, those seeking visas for other countries within the EU may not find the platform to be a useful resource. However, VISAR recognizes the importance of ensuring a smooth and seamless experience for employers and relocation employees, and that is why the platform heavily relies on VISAR employees to assist with the visa application process. These individuals are crucial in guiding both employer and relocation employee through the process, but if they lack expertise or are unresponsive, it could result in delays or other issues for the immigration procedure.

Furthermore, all employers and relocation employees' data are stored on a cloud server and so far we only use access control on the server, and we think the data stored on the data hub could be exposed to network attackers.

As the TANGO framework continues to be developed and implemented, VISAR advises paying attention to the concerns of data storage, transfer, and protection. From VISAR's standpoint, the following vulnerabilities may arise in relation to the processing of immigration cases:

- Data security and privacy: Without appropriate security measures, there is a risk that personal and sensitive information provided by employers and relocation employees could be compromised.
- Data accuracy: Inaccuracies in collecting and storing personal user information could result in errors within the visa application process.
- Data completeness: If the platform fails to gather all necessary information from employers and relocation employees, it could cause incomplete visa applications and delays.
- Data sharing: Sharing employers and relocation employees' data with third parties without proper consent or security measures in place could lead to data protection concerns.
- Data retention: Without adequate policies for the retention or deletion of user data, there may be security risks or compliance issues.
- Data analytics: Inability to effectively analyse the personal data may lead to incorrect assessments of visa eligibility or other issues.

8.3.6 Ways TANGO can enhance the system

The TANGO platform will be used in order to provide effective resiliency against multiple attack vectors aiming to exploit a series of vulnerabilities of the host device. TANGO should be able to help us to enhance data security and protect data privacy in what context and under what condition. Furthermore,

should technologies such as blockchain or AI be used, we could improve our technology in terms of data transfer and data security. TANGO through its platform and technologies could solve problems of bureaucracy, delays, uncertainty, leak of data, and transparency through the whole time. Moreover, it could:

- Provide 100% paperless procedures (environmental pillar),
- Create satisfied citizens, companies, and partners (social pillar). The most important it could guarantee real control over the data used and sent for the visa procedures, allowing them to reuse the data in a safe manner for related purposes.
- And it could increase the financial performance of all the above stakeholders by dramatically reducing the time needed to get someone the visa.

8.3.7 Type of Information required for TANGO

There is no unique set of data that is needed for the immigration process, as the specific requirements can vary depending on the country and the individual's circumstances. As VISAR is an in Germany operating company and the public organisation's pilot will also be conducted with the immigration authority in Berlin, the specific personal data that is required for the immigration process to Germany can vary depending on the individual's circumstances and the type of immigration application they are submitting. In general, however, some common types of personal information that may be required for immigration to Germany include:

- Full name and date of birth.
- Place of birth.
- Nationality and country of origin.
- Passport or other identification document.
- Details of any previous visas or residence permits.
- Family information, including the names and dates of birth of any family members who will be accompanying the individual.
- Employment and education history.
- Information about any criminal record or security concerns.
- Medical and health information, including any disabilities or special needs.

In addition to the data entered by keyboard, personal documents in PDF format are collected and processed by us. This information is typically collected and used by German immigration authorities to determine an individual's eligibility for immigration and to process their application. It may also be shared with other government agencies or authorities as necessary.

8.4 User Requirements

Code	**UR-TUA-PA-001**
Category	**Trusted user authentication**
Description	The applicants must be authenticated to have access to the system.
Priority level	High

Code	**UR-TUA-PA-002**
Category	**Trusted user authentication**
Description	The VISAR employees must be authenticated to have access to the system.
Priority level	High

Code	**UR-TUA-PA-003**
Category	**Trusted user authentication**
Description	The employers must be authenticated to have access to the system.
Priority level	High

Code	**UR-TUA-PA-004**
Category	**Trusted user authentication**
Description	The authority employees must be authenticated to have access to the system.
Priority level	High

Code	**UR-DUP-PA-005**
Category	**Data upload**
Description	The applicants must be able to upload documents and data to the system in a trustworthy way.
Priority level	High

Code	**UR-DUP-PA-006**
Category	**Data upload**
Description	The VISAR employees must be able to upload documents and data to the system in a trustworthy way.
Priority level	High

Code	**UR-DUP-PA-007**
Category	**Data upload**
Description	The employers must be able to upload documents and data to the system in a trustworthy way.
Priority level	High

Code	**UR-DUP-PA-008**
Category	**Data upload**
Description	The authority employees must be able to upload documents and data to the system in a trustworthy way.
Priority level	High

Code	**UR-DMN-PA-009**
Category	**Data management**
Description	The VISAR employee must be able to monitor and manage the documents and the data flow in the system.
Priority level	High

Code	**UR-TDS-PA-010**
Category	**Trustworthy Data sharing**
Description	The users must be able to share data in a trustworthy and secure way.
Priority level	High

Code	**UR-GCO-PA-011**
Category	**GDPR and related regulation compliance**
Description	The applicant's data must be handled according to GDPR.
Priority level	High

Code	**UR-PCY-PA-012**
Category	**Protection from cyberattacks**
Description	The users must feel secure that the data and document flow is not compromised.
Priority level	High

Code	**UR-PCY-PA-013**
Category	**Protection from cyberattacks**
Description	The applicants must feel secure when uploading and sharing their data within the platform.
Priority level	High

Code	**UR-DMN-PA-014**
Category	**Data management**
Description	The VISAR employees should ensure that the uploaded documents are real and can authenticate them.
Priority level	Medium

Code	**UR-UIN-PA-015**
Category	**User interaction**
Description	Applicants could be able to have a better experience via the use of AI technology.
Priority level	Low

Code	**UR-DMN-PA-016**
Category	**Data management**
Description	VISAR employees could use a document recognition and PDF mapping software to automatically identify mismatches and incorrect information inputs.
Priority level	Low

Code	**UR-DMN-PA-017**
Category	**Data management**
Description	VISAR employees could use a document validation system to verify authenticity and detect fakes.
Priority level	Low

8.5 Use Case Scenarios

A VISAR employee is a Customer Support Manager who provides excellent support to their employers and relocation employees, while an employer is a German company cooperating with VISAR is responsible for the relocation employees' immigration process. The relocation employee, an IT specialist from a third country, uses VISAR's services with pleasure to navigate the complicated German immigration system. Meanwhile, the German authority's employee reviews the applications, interviews the relocation employees, asks about their purpose of stay in Germany, etc.

Overall, VISARIGHT (VISAR) has the potential to transform the visa application process in Germany and the European Union by simplifying it, making it more efficient, transparent, and secure.

8.5.1 Personas

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
VISAR_01	**VISAR Employee** **Customer Support Manager OR Case manager**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Emily Age: 25 years Occupation: International relations, Management, HR Domain: Visa, relocation, immigration services Years of experience: 5 years	*"It is very rewarding to be able to guide people through the relocation process to Germany."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
1. Quick and non-stressful relocation process for all customers 2. Get a 5-star review from the customer at the end of the process. 3. Fewer emails with the same questions from the customers.	1. A possibility to make a mistake which will negatively affect the customer's relocation. 2. Misunderstanding with the customer or employer on any point of the relocation.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
1. VISAR platform 2. Help Scout 3. Gmail 4. Google documents 5. Offline PDF converters 6. Online booking systems of the authorities' websites 7. Fax	1. Welcomes the customer with a "welcome to VISARIGHT" email. 2. Presents the main steps of relocation to Germany to the customer. 3. Supports the customer throughout the whole relocation procedure. 4. Explains what documents are required for processing. 5. Informs about the date and time of appointments.

SHORT DESCRIPTION
Emily is 25 years old, and she is working remotely as Customer Support Manager at VISAR. She has been studying International Relationship and has worked at the visa application centre and at a relocation company in her local country before. Her expertise helps to provide the best support to the VISAR's customers and complete her daily tasks: communication with the customer, preparing the required documents and booking the appointment at the relevant authorities' offices.

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
VISAR_02	**Employer**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Katrin Age: 30 years Occupation: Human Resources Domain: relocation, global mobility Years of experience: 10 years	*"I want the relocation process to run smoothly and fast, to achieve the best result in the minimum required time."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
1. Have an employee on board on time. 2. No extra costs for the employee's relocation	1. Frequent delays in the employees' relocation 2. Extra costs are often required
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
1. VISAR platform 2. Gmail	1. Gets the personal details from the relocation employee and adds them to the VISAR's platform, creating the relocation case. 2. Ask VISAR employee about an update on the particular relocation employee's relocation process to be informed about the progress.
SHORT DESCRIPTION	
Katrin is an HR specialist at the German company cooperating with VISAR. She is the one who is responsible for the employees' relocation and has access to the VISAR platform. Katrin adds new relocation cases to the platform and regularly checks the progress of each relocation employee. She is always in contact with VISAR's responsible employees in case there are any additional documents or information required for the employees' relocation.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
VISAR_03	**Relocation employee**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Ahmed Age: 30 years Occupation: IT, Design. Finance	*"I am happy that VISAR will assist me with the relocation process. It makes a complicated process simple and stress-free."* *"I want to start working for my new employer as fast as possible."*

Domain: software development, software engineer, 3D designer, finance controller Years of experience: 10 years Has a wife and 2 children	
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
1. Join employer in Germany on time 2. Getting the visa easily 3. Obtaining the residence permit in Germany easily	1. Afraid of the long and complicated visa process. 2. Afraid of losing a job offer in Germany in case of problems/ delays with visa. 3. Disclosure of personal information to the wrong hands
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
1. VISAR platform 2. Gmail 3. SSI	1. Ahmed would like to know all the details of the relocation to Germany. 2. He informs VISAR's employee about his schedule to make sure he will be able to attend all appointments booked for him. 3. Ahmed asks many questions throughout the relocation to not miss any important information.
SHORT DESCRIPTION	
Ahmed is an IT specialist from a third country who recently got an offer from a German company. Ahmed is starting to prepare for the relocation, and his German employer offers VISAR's services for that. He uses these services with pleasure, because he is aware of the complicated German immigration system.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
VISAR_04	**Authority employee (Diplomatic Mission, Federal Employment Agency, City Hall, Immigration office)**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Lilia Age: 30-40 Occupation: German migration law Domain: relocation to Germany for employment purposes Years of experience: 10-15	*"With so many applications and so many documents, the process takes too long."*
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
1. Process all applications on time 2. Reduce stress	1. Too many applications and not enough time to process them. 2. Uncompleted and inappropriate documents. 3. Applicants being late for an appointment
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
1. Gmail 2. Internal CRM system	1. Approves or rejects the application submitted by the relocation employees.

3. Official website and online booking system 4. Fax	2. Requests additional documents to process the application. 3. Interviews the relocation employees during the appointment. This is the general description of the officers working at all authorities (German Diplomatic Missions, City Halls, Employment Agencies and immigration offices) based on our experience dealing with them, so this information cannot be considered as absolute truth.
SHORT DESCRIPTION	
Lilia is the officer at the German authority. Her workload is always high because of the many applications. She does not have enough time to process all of them, and that often causes delays in the procedure. Lilia interviews the relocation employees at the appointment, asks questions about their purpose of stay in Germany and takes fingerprints.	

8.5.2 User Journeys

PERSONA:		VISAR employee			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Get the relocation case assigned	VISAR platform	Curious about the new relocation employee	VISAR employee, relocation employee	
	Send welcome email to the relocation employee	Help Scout		VISAR employee, relocation employee	
2.	Observe on how the relocation employee completes the profile	VISAR platform	Waiting to start to work on case	VISAR employee, relocation employee	The profile can be filled online or transferred from the applicant's online identity from Fides component of TANGO.
3.	Review the relocation employee's profile and determines the next steps At this step first set of relocation employee data verified by VISAR employee enters Fides	VISAR platform Fides component of Tango	A little stressed and in a hurry because relocation employee wants to know the next steps asap	VISAR employee	
4.	Prepare the checklist, book visa appointment, inform relocation employee	VISAR platform, online booking system of the Diplomatic Mission, Help Scout		VISAR employee, relocation employee	
5.	Wait for relocation employeer's feedback after the visa appointment	VISAR platform, Help Scout	Curious on the result of visa application	VISAR employee	
6.	Check the visa sticker.	VISAR platform,		VISAR employee	

PERSONA:	VISAR employee				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
	At this step visa information verified by VISAR employee enters Fides	Fides component of Tango			
7.	Inform relocation employee on the entry procedure to Germany	Help Scout		VISAR employee, relocation employee	
8.	Prepare the checklist, book appointment for registration in Germany, inform relocation employee	VISAR platform, online booking system of the City Hall, Help Scout		VISAR employee, relocation employee	
9.	Wait for relocation employee's feedback after the registration appointment	VISAR platform, Help Scout		VISAR employee	
10.	Check the registration certificate At this step registration certificate information verified by VISAR employee enters Fides	VISAR platform, Fides component of Tango		VISAR employee	
11.	Prepare the documents for residence permit application, submit them to the immigration office	VISAR platform, the immigration office's website, Gmail Fides component of Tango	Face difficulties, because each immigration office in Germany has own system of submitting the applications	VISAR employee	
12.	Waiting for getting appointment confirmation from the immigration office	Gmail Fides push notifications + VISAR platform (through integration with Fides)	Feeling impatient	VISAR employee	

PERSONA:	VISAR employee				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
13.	Getting appointment confirmation and inform relocation employee	Gmail, VISAR platform, Help Scout		VISAR employee, relocation employee	
14.	Waiting for relocation employee to attend the appointment and receive feedback	VISAR platform, Help Scout		VISAR employee	
15.	Getting feedback from relocation employee after appointment, checking the confirmation letter from the immigration office	VISAR platform, Help Scout Fides component of Tango (to receive the confirmation letter)		VISAR employee, relocation employee	
16.	Waiting for relocation employee to receive the residence permit card	VISAR platform, Help Scout	Feeling excited about the end of the process	VISAR employee	
17.	Check the residence permit card and send the final letter to the relocation employee At this point the residence permit information verified by VISAR employee enters Fides	VISAR platform, Help Scout, Google documents Fides component of Tango		VISAR employee, relocation employee	
18.	Close the relocation case	VISAR platform	Happy to successfully complete the case	VISAR employee	

PERSONA:	Employer				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Create account	VISAR platform	Excited to get assistance with the employees' relocation	Employer	

PERSONA:	Employer				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
2.	Add the first employee's relocation case	VISAR platform	Afraid to make mistake in employee's details	Employer	
3.	Observe the employee's progress	VISAR platform		Employer	
4.	Sign the documents and the forms required for employees' relocation	VISAR platform		Employer	
5.	Get requests from VISAR employee on the particular employees' relocation	Gmail		Employer, VISAR employee	
6.	Contact the VISAR employee to get an update on the particular relocation case	Gmail		Employer, VISAR employee	
7.	Gets automate notifications from the VISAR platform once employee completes one of the steps of the relocation	Gmail	Happy to know there is progress in relocation	Employer	
8.	Gets automate notification once employee's relocation is successfully completed	Gmail	Happy to know relocation is completed	Employer	

PERSONA:	Relocation employee				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Gets invitation to login from VISAR platform	Gmail	Happy to get the assistance in relocation	Relocation employee	

PERSONA:		Relocation employee			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
2.	Login, complete eligibility check, fill out the application form and upload the documents	VISAR platform		Relocation employee	
3.	Get welcome email from the VISAR employee assigned to his relocation case	Gmail	Happy to have a personnel VISAR employee	Relocation employee	
4.	Wait for his profile to be reviewed and the next steps to be determined	VISAR platform		Relocation employee	
5.	Get notification from VISAR platform that his profile is fine and hisVISAR employee starts to prepare the checklists and book an appointment for visa application.	Gmail	Happy to start the actions	Relocation employee	
6.	Get notification that checklist is ready, prepare the documents according to the provided checklist	VISAR platform, relocation employee's original documents		Relocation employee	
7.	Get notification with the date and time of visa appointment.	VISAR platform		Relocation employee	
8.	Attend appointment at the Diplomatic Mission	Original documents, reception at the Diplomatic Mission's building, counter for application submission, counter for fingerprints		Relocation employee, security guard, authority employee	
9.	Waiting for visa issuance, collect the passport with the visa sticker	Reception at the Diplomatic Mission's building, counter for passport collection,	Happy to get the visa	Relocation employee security guard, authority employee	

PERSONA:		Relocation employee			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
10.	Upload the visa to the VISAR platform	VISAR platform		Relocation employee	
11.	Get notification that checklist for registration in Germany is ready, prepare the documents according to the provided checklist	VISAR platform, relocation employee's original documents		Relocation employee	
12.	Get notification with the date and time of registration appointment.	VISAR platform		Relocation employee	
13.	Attend appointment at the City Hall	Original documents, reception at the City Hall's building, counter for application submission		Relocation employee, security guard, authority employee	
14.	Upload the registration certificate to the VISAR platform	VISAR platform		Relocation employee	
15.	Waiting for VISAR employee to book an appointment for residence permit application	VISAR platform		Relocation employee	
16	Get notification that checklist for residence permit application is ready, prepare the documents according to the provided checklist	VISAR platform, relocation employee's original documents		Relocation employee	
17.	Get notification with the date and time of residence permit appointment.	VISAR platform		Relocation employee	
18.	Attend appointment at the immigration office	Original documents, reception at the immigration office's building, counter for application submission		Relocation employee, security guard, authority employee	

PERSONA:		Relocation employee			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
19.	Upload the confirmation letter from the immigration office to the VISAR platform	VISAR platform		Relocation employee	
20.	Waiting to receive the residence permit card		Excited to get the residency in Germany	Relocation employee	
21.	Receive the residence permit card and upload it to the VISAR platform for checking	VISAR platform		Relocation employee	
22.	Get final email from the VISAR employee	Gmail	Happy to complete the relocation	Relocation employee, VISAR employee	
23.	Get automate notification that his relocation case is successfully closed.	VISAR platform		Relocation employee	

PERSONA:		**Authority employee (Federal Employment Agency, Immigration office).** *(Personal presence of a VISAR applicant is not required during the submission of the application.)*			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Get notified once the new application is uploaded to the shared data space by VISAR. Get notified once the new application is shared with the authority through Fides by VISAR.	Gmail, shared data space Fides component of Tango		Authority employee, VISAR employee	A VISAR employee uploads the application from the VISAR platform to a shared data space. VISAR employee uploads the application data from VISAR platform the Fides component of Tango, at the same time

PERSONA:		Authority employee (Federal Employment Agency, Immigration office). *(Personal presence of a VISAR applicant is not required during the submission of the application.)*			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
					creating a Fides Lead to the authority
2.	Review the documents Authority employee sees the verification stamp of VISAR delivered by Fides, and because of trust to VISAR that was built during the long previous period of cooperation spends less time on meticulous verification of the relocation employee's data	Computer, printed documents		Authority employee	Authority employees may review the documents in digital or printed form.
3.	Contact another authority to get the approval (if required).	Shared data space Fides component of Tango or internal online system, post		Authority employee and another authority's employee	The immigration office in Germany might contact the Federal Employment Agency and Diplomatic Mission for approval while processing the application for a residence permit. In the case of FEA, the communication might take place via the Fides component offered by TANGO. If contact with a Diplomatic Mission is required, communication can be in the online system that authorities already use.
4.	Waiting to get approval from another authority	Shared data space Fides component of Tango or internal online system, post		Authority employee and another authority's employee	
5.	Get approval from another authority	Shared data space Fides component of Tango		Authority employee	

PERSONA:		Authority employee (Federal Employment Agency, Immigration office). *(Personal presence of a VISAR applicant is not required during the submission of the application.)*			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
		or internal online system, post			
6.	Approve the application			Authority employee	
7.	Inform the VISAR employee and relocation employee about approval by adding some additional data points regarding the approval to Fides	Shared data space Fides component of Tango		Authority employee, VISAR employee, relocation employee	FEA employee sends an approval via email and via post. The immigration office's employee invites relocation employee for an appointment to take the biometric data. Both actions can be taken using the Fides component of Tango by uploading approval from FEA or invitation from the immigration office. and/or some other data points such as approval date etc

8.5.3 Technology offerings used in use case scenario

TECHNOLOGY OFFERING	RELATION TO PILOT
Blockchain-based Data Storage and Sharing	Sharing of confidential data, Explicit customer consent management, Real-time data updates As long as both VISAR and Immigration Authority are connected to Fides, they will be able to share relocation employee's data between them, including: - Sending an initial application to the Immigration Authority, - Receiving comments from the Immigration Authority - Updating and enhancing relocation employee's data from VISAR side Receiving Immigration Authority decision together with supporting data points
Confidentiality and Privacy by Design	Ensuring privacy principles are held for user data in the procedures. GDPR should be enforced through proper data access control and user consent. Sticky policies and related identity-based techniques may be used to ensure only allowed actors to retrieve data (apart from access control to the database), even with fine-grained control. E.g., only the corresponding manager (and team leaders) can access data from a case.
Self-sovereign Identity Management	SSI Module enables the organisation members to manage their data and provide only necessary information. The personal data is restricted to the ABE policies and persons acting for public administration need to use SSI to get access to the ABE claims being encrypted to guarantee the limited access.
Seamless Onboarding for Users and Devices	The module will enable the organisation members to onboard to the SSI leveraging their passport, and performing a remote 3-step identity verification. This process will allow organisations' member to verify remotely their identity without human presence and having the ability to create verifiable credentials, which will then be used to perform authentication to manage data at the organisation.
User Continuous Behavioural Authentication	Strong authentication for applicants, employees, employers when accessing the TANGO platform
Privacy Threat Modelling and Identification for Trustworthy AI	The following functionalities could be supported from the PAT component (to be further investigated and finalized in D2.4): In user side: ▸ Fill-in the requested data (ex. personal data) ▸ Preferences (activities, drinks, foods, etc. in smart hospitality use case), ▸ Data policies and privacy awareness. ▸ Monitoring privacy risks of the requested data In organization side: ▸ Request the data (ex. personal data) ▸ Data policies

	Data policies and privacy awareness

8.6 KPIs

TITLE	DESCRIPTION
Reduction of privacy violation incidents in data sharing	Privacy assessment results comparison of existing infrastructure with TANGO proposed data sharing platform.
Accuracy of employees' verification and authentication > 99.6%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate and failure to access.
60% faster residence permit application processes	Comparison between existing process duration and TANGO-based process duration.
Number of residence permit applications processed	This KPI measures the total number of residence permit applications that VISAR processes over a given period. It is a key indicator of the company's overall productivity and efficiency.
Processing time per residence permit application	This KPI measures the average time it takes for VISAR to process a residence permit application. Reducing the processing time can result in increased customer satisfaction. Target: Reduction of 20-30 %. Depending on the authority.
Authorities' employee satisfaction rate	This KPI measures whether the implementation of TANGO technology has led to an increase in authorities' employee satisfaction with the workflow. Target: Increase of 20-30 %.
VISARIGHT employee satisfaction rate	This KPI measures whether the implementation of TANGO technology has led to an increase in VISAR employee satisfaction with the workflow. Target: Increase of 10-20 %.
Authorities' employee effort rate	This KPI measures whether the implementation of TANGO technology has led to the reducing the amount of authorities' effort put into the process. Target: Reduction of 20-30 %.
VISARIGHT employee effort rate	This KPI measures whether the implementation of TANGO technology has led to the reducing the amount of VISAR effort put into the process. Target: Reduction of 10-20 %.
Data security breach incidents	This KPI measures the number of incidents where VISAR's customer data is compromised. Ensuring data security is crucial for the company's reputation and can help avoid legal issues.

9 Pilot 6 – Retailers

9.1 Pilot case overview

The sixth pilot is related to Retailers and it will be implemented in the task T7. 7 between the months M24 – M36 of the project. This task is dedicated to the exchange of data in a secure and privacy preserving way for personalised recommendations in the form of shopping list to consumers/wholesalers. METRO (MET) will test the TANGO solution in a cross-border scenario, across two different retail entities in Greece and Cyprus acting as competitors, both owned by MET group. 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. In parallel, data sharing technologies between different platforms will be tested supporting the interconnection between different corporate systems. Federated learning mechanisms combined with tokenization will be deployed targeting insightful and personalised recommendations in a privacy preserving way for both consumers and wholesalers.

9.2 Organisations involved

9.2.1 METRO

METRO is a Greek company (Retailer- Supermarket), operating since 1976 and serving the Greek market with consistency and reliability. Its purpose is to offer clients a memorable, captivating buying experience, through a unique relationship, based on trust, that allows them to live a better life.

The company's main values include the respect for the customer, the non-negotiable quality of products and services, the safe working environment and the contribution to society.

Today, METRO employs over 10,600 people, making it one of the largest employers in Greece. It has 231 retail stores, 50 metro Cash & Carry stores and 4 Distribution centres. It also operates in Cyprus via its subsidiary MCC Best Value Ltd (hereafter MCC).

Metro has a large IT department, which has developed most of the company's information systems in house. It has also developed e-shops (e-supermarkets) for both consumers and professional wholesalers.

Through Tango, METRO aims to further exploit and harness the existing data environment with new technologies, such as Machine Learning, to better understand the customer needs and become customer centric. It aims to better understand buying patterns and preferences between customers of different countries using different systems and data structures.

Possible results may include:

- Ability to divide customers based on frequency and spending to identify loyalty.
- Optimization of marketing spending and differentiate across customer segments.
- Ability to understand cross sell/up sell opportunities for key customers.
- Use of online recommendation engines.
- Enhance in-store product placement (display promotions etc.).
- Provision of customised emails.
- Optimization of trade spending by investing in the right customers & products.
- Identification of "next best item".
- Group products that co-occur in store layout design to increase chance of cross-selling.
- Enhance catalogue designs.
- Personalise offerings.

- Offer relevant products aligned with customer needs and demographics.

9.3 Existing Situation Mapping

9.3.1 A brief description of the platform

There are 3 main groups of application platforms in the company's IT infrastructure that will be involved in this project.

1. Stores Applications System. There is a store checkout application and a store back-office system.
2. Central Offices Applications. A custom-made ERP System where transactions from all stores are gathered.
3. Data Warehouse. Each one of the 2 companies has a different data warehouse system. A legacy SYBASE IQ for MCC and Oracle Data warehouse Database for METRO.

9.3.2 Key Stakeholders involved

The different stakeholders that will be involved in the pilot implementation are the following:

1. Marketing Manager.
2. Commercial Product Manager.
3. Sales Manager.
4. IT Operator.
5. IT Security Officer.

These stakeholders will be further described and analysed in the personas and user journeys subsection.

9.3.3 Main operations flow of the system

The daily data update procedure includes the following steps:

1. Stores Sales EDI File creation (a file including the stores' sales is created).
2. Stores Sales EDI File ftp transfer to the Central ERP (sales info is sent to the Central ERP system of the company).
3. Data loading to ERP System.
4. ETL procedure to Sybase IQ.
5. ETL procedure to Oracle Data Warehouse.

These data flows are described in the following section.

9.3.4 Data flows

Analytical sales data is collected at physical stores. Each transaction is stored at the stores' back-office system called Metrisys. At the end of the day, in each store a custom EDI file is created containing analytical raw data for all transactions. The file is transferred through secure ftp to Central Offices of Metro.

An ETL (Extract-Transform-Load) procedure triggered by the Central ERP system loads the files to the OLTP database (Oracle) where all transactions are stored.

Then different scheduled ETL procedures transfer data from OLTP to Data warehouse (OLAP). For Metro, Data warehouse is an Oracle database, while for MCC is a Sybase IQ system.

9.3.5 Related infrastructure

Besides the Stores Applications System, the Central ERP and the Data Warehouses, mentioned above, METRO's IT infrastructure comprises the following systems:

Cyprus: Windows server 2016 Std 32GB RAM 26Vcores Oracle 11.2.0.4 64bit

Windows server 2016 Std 8GB RAM 8Vcores Ftp Server

Athens: Windows Server 2012 R2 40GB RAM 8Vcores Sybase IQ 16.1 SQL Server 12

AIX 7.1 64GB RAM POWER 7 8 CPU Oracle 11.2.0.4 64bit

Oracle Linux 8.3 65GB RAM 12Vcores Oracle 19c

9.3.6 Weak points of the system that can be enhanced

The main weak points of the company's existing systems and IT infrastructure are the following:

- Through Metro's system it is difficult to apply customer segmentation procedures and extract results for customers and their buying patterns.
- Users need to extract and combine data from many different reports.
- A lot of time is needed for the execution of data of all customers and all stores in the company's network.
- In the retail activity in Cyprus the operating capability is not the same.
- It is difficult to compare results from different systems of the two companies to identify similarities and differences in segmentation analysis.
- The meaningful market basket analysis for the applied segments currently is done on a pilot basis and for specific personalised customers.
- Combination and consolidation of different reports requires additional effort to identify instant variances (differences and similarities).

9.3.7 Ways TANGO can enhance the system

As demonstrated in the following figure, the TANGO platform is expected to enable secure sharing of anonymized data between the different systems of METRO and MCC. Moreover, the Tango platform is expected to facilitate the mapping and analysis of data and provide improved recommendations. Thus, it will enable the company to apply customer segmentation procedures, extract results for customers and their buying patterns and give more personalised shopping experience, respecting GDPR issues.

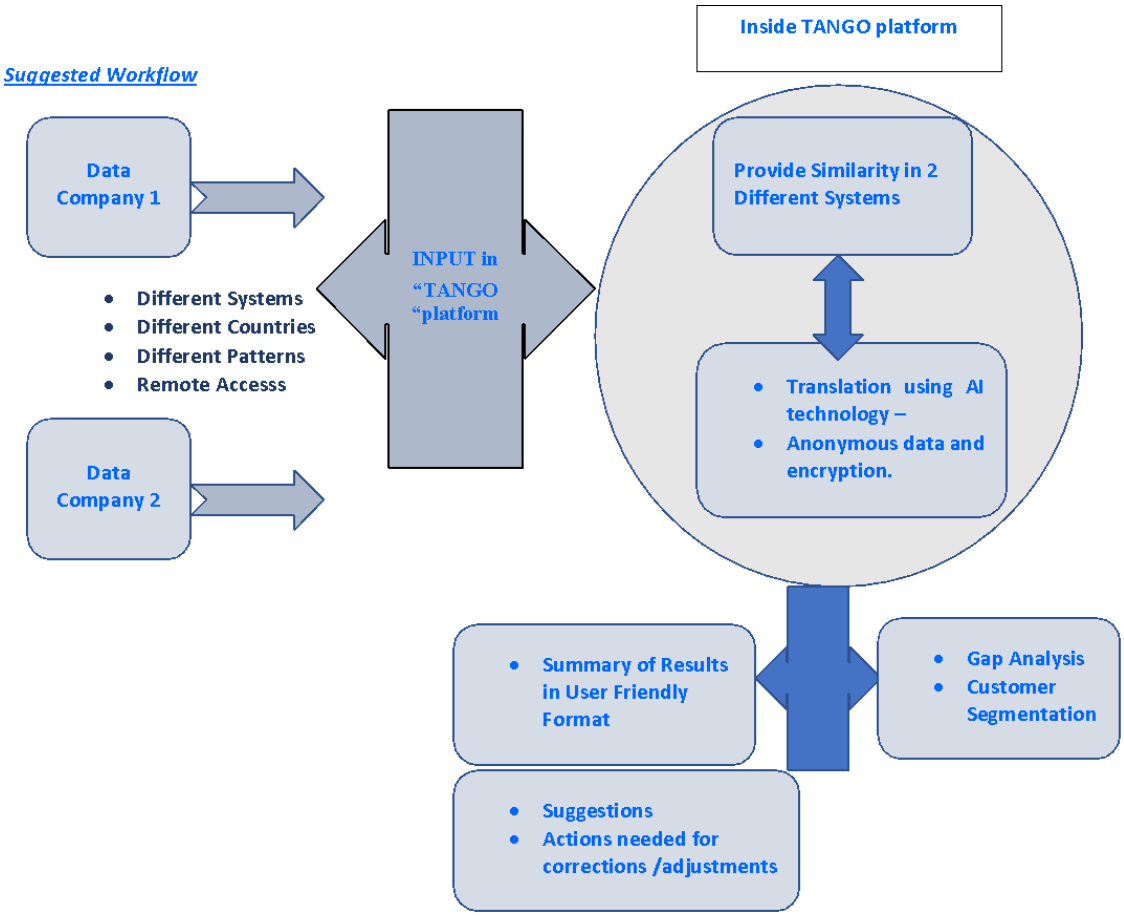


Figure 16 METRO TANGO suggested workflow

Tango as a platform will help to achieve the following:

- Effective and efficient data sharing for customer and product analysis.
- Transform data in the same format, summarise and unify product solutions from 2 different countries.
- Provide insightful conclusions (using AI technology) to current stakeholders, mainly commercial managers, marketing specialists and finance professionals.
- Group the results in an Executive summary format and analyse trends.
- Provide security and anonymity of data for possible data sharing between internal and external systems.
- The platform could be uses as a future solution for data sharing of sensitive information with strategic partners.
- Identify and correct possible disruption of IT operations through the whole process (i.e., the platform should work efficiently in parallel mode so as not to interrupt the daily routines).
- Secure backups and use encryption cybersecurity methods to protect data flows of sensitive information.

Therefore, the main aims of TANGO are:

- To increase customer awareness and provide useful integrated data insights
- To perform customer, product and basket analysis across different systems.
- To compare data from different systems and draw useful conclusions for similarities.
- To secure anonymity between different data for retail customers.
- To apply effective and efficient customer segmentation.

By using the TANGO platform IT Operators will be able to manage the extraction of data from different systems and retrieve information and analysis results in a fast, secure and easy way.

Moreover, the company's business users (e.g. the product and marketing managers) will be able to extract and use results of specific customers for different groups of products. The results of data analysis could be extracted in the form of a summary (daily, weekly, monthly or yearly) providing information related to customer loyalty, frequency of buying patterns and visits, as well as purchase volumes in different time periods. This will facilitate the creation of a marketing-commercial plan in collaboration with key stakeholders. Finally, the effectiveness of data analysis will be measured through comparing results with threshold goals at specific product category and customer level, as well as through identifying relevant KPI's.

9.3.8 Type of Information required for TANGO

Data that may be used include:

- Financial transactions (B2C, B2B). (Sales information). The platform should be able to include different financial variables in the future and combine data from 2+ variables.
- Customer's profile (name, address, email, gender, etc.)
- QR codes and other data from thousands of products.

9.4 User Requirements

Code	**UR-TUA-RT-001**
Category	**Trusted user authentication**
Description	All categories of users should be authenticated to the system to have access to the relevant information via various devices.
Priority level	High

Code	**UR-DMN-RT-002**
Category	**Data management**
Description	Specific users must be able to upload data to the system.
Priority level	High

Code	**UR-DMN-RT-003**
Category	**Data management**
Description	Specific users must be able to request data harmonisation from the master and transactional databases.
Priority level	High

Code	**UR-DMN-RT-004**
Category	**Data management**
Description	Specific users must be able to request a common view and analysis of data.
Priority level	High

Code	**UR-DMN-RT-005**
Category	**Data management**
Description	Specific users must be able to view the harmonised data in various views with various filters and search parameters.

Code	**UR-DMN-RT-005**
Category	**Data management**
Priority level	High

Code	**UR-DMN-RT-006**
Category	**Data management**
Description	Specific users must be able to run queries to the harmonised data.
Priority level	High

Code	**UR-DMN-RT-007**
Category	**Data management**
Description	Specific users must be able to request for specific data analysis results.
Priority level	High

Code	**UR-DMN-RT-008**
Category	**Data management**
Description	Specific users must be able to combine data from various external sources.
Priority level	High

Code	**UR-DMN-RT-009**
Category	**Data management**
Description	Specific users must receive recommendations for targeted and effective campaigns.
Priority level	High

Code	**UR-DMN-RT-010**
Category	**Data management**
Description	Specific users must be able to retrieve the requested data (e.g., sales data, etc.).
Priority level	High

Code	**UR-DMN-RT-011**
Category	**Data management**
Description	Specific users must be able to delete the uploaded data from the system.
Priority level	High

Code	**UR-TDS-RT-012**
Category	**Trustworthy data sharing**
Description	Specific users must be able to share data in a safe and trustworthy way.
Priority level	High

Code	**UR-DAR-RT-013**
Category	**Data analysis and reporting**
Description	Specific users must receive notifications from the system after data processing or analysis is completed.
Priority level	High

Code	**UR-DAR-RT-014**
Category	**Data analysis and reporting**
Description	Specific users must be able to analyse data.
Priority level	High

Code	**UR-DAR-RT-015**
Category	**Data analysis and reporting**
Description	Specific users must be able to visualise data.
Priority level	High

Code	**UR-DAR-RT-016**
Category	**Data analysis and reporting**
Description	Specific users must be able to produce customised reports.
Priority level	High

Code	**UR-GCO-RT-017**
Category	**GDPR and related regulation compliance**
Description	The company's data must be handled according to GDPR.
Priority level	High

Code	**UR-PCY-RT-018**
Category	**Protection from cyberattacks**
Description	The users must feel secure that the data flow is not compromised.
Priority level	High

Code	**UR-PCY-RT-019**
Category	**Protection from cyberattacks**
Description	The company must feel safe from cyberattacks.
Priority level	High

Code	**UR-DMN-RT-020**
Category	**Data management**
Description	Specific users should be able to view the automatically mapped data from various sources and data structures.
Priority level	Medium

Code	**UR-DMN-RT-021**
Category	**Data management**
Description	Specific users should be able to retrieve market/ marketing/ product data from external sources, periodically or not.
Priority level	Medium

Code	**UR-DMN-RT-022**
Category	**Data management**
Description	The users should use anonymized data.
Priority level	Medium

9.5 Use Case Scenarios

METRO, a leading retailer with stores in both Greece and Cyprus, had been struggling with combining their different operational systems. The company's marketing team was finding it difficult to perform effective customer segmentation and basket analysis due to the challenges of identifying similarities and differences in customer purchasing behaviour across different regions.

To overcome these challenges, METRO decided to invest in a unified platform that would combine the data from both countries and provide the marketing team with better insights into customer behaviour. The commercial product manager would also have access to immediate sale analysis for product categories in charge, allowing them to initiate specific promotional activities with suppliers from the platform.

Additionally, the sales manager would be able to correlate data from different sources, including company sales data and competitors' data, to identify market trends on a regional and national level. This would help METRO to stay ahead of the competition and make data-driven decisions to optimise sales.

METRO also recognized the importance of cybersecurity and wanted to ensure that the platform would provide adequate protection against cyber threats. The IT security officer would be responsible for dealing with any potential hackers attempting to steal customer data or breach the system.

The implementation process was challenging, but METRO worked closely with their IT team to ensure a smooth transition. The new platform provided a user-friendly environment for the IT operators to initiate and monitor the procedure, ensuring the smooth operations of all systems.

The unified platform was a meaningful change for METRO, providing the company with better insights into customer behaviour and market trends, allowing for more effective marketing campaigns and sales optimization. The company was able to take advantage of their global presence and operate more efficiently, providing a better customer experience and improving their bottom line.

In conclusion, the investment in a unified platform was a wise decision for METRO. It allowed the company to overcome the challenges of combining their operational systems and provided a range of benefits, including better customer segmentation, improved sales analysis, and enhanced cybersecurity. The platform was a key factor in METRO's continued success as a leading retailer in the region.

Based on the above scenario, there have been six personas and their journeys. These personas and journeys are presented in the next sections.

9.5.1 Personas

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**

METRO_01	Marketing Manager
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Maria Age: 43 Occupation: Business Administration Domain: Specialised in marketing plan and campaigns by product category and markets. Years of Experience: 15	The basket analysis for the specific consumer trends in shop requires tedious and time-consuming people's efforts.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Perform customer segmentation and basket analysis for specific products.	It is difficult to identify similarities and differences in customer purchasing behaviour by combining the data of both companies in Cyprus and Greece.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Both reporting systems (Greece & Cyprus). CRM	Sensitivity, anonymous data for data sharing between different stakeholders.
SHORT DESCRIPTION	
Maria is the marketing manager of the company. One of the main roles based on her job description is to perform customer segmentation and basket analysis for specific products. She understands the benefits in organising the advertising campaigns based on predicted behaviour of what consumers would buy next in each region. However, this task is difficult for her and her department because there are many obstacles to identify similarities and differences in the behaviour of the customers who are in different countries, such as the combination of the different data in one platform. One of these obstacles is maintaining compliance with different regulations, under which consolidating any data should be carefully designed.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
METRO_02	**Commercial Product Manager**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Christos Age: 46 Occupation: Industrial Management and Technology Domain: Specialised in category management (both food and non-food categories). Years of Experience: 13	It is time consuming to perform product analysis considering data from both Cyprus and Greece entities.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
He wants to have immediate sale analysis for product categories in charge, to initiate specific promotional activities with suppliers.	It is difficult to consolidate data from both Greece and Cyprus.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Company's MIS system transformed to custom excel files.	Sensitivity, anonymous data for data sharing between different stakeholders
SHORT DESCRIPTION	
Christos is the commercial product manager of the company. One of his main goals is to produce sales analysis for product categories immediately. However, it is incredibly difficult for him and his team to consolidate data from both Greece and Cyprus operation systems, also in respect to GDPR legal requirements.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
METRO_03	**Sales Manager**

IDENTITY *(name, age, occupation, domain, years of experience)*	QUOTES *(important things he/she said)*
Name: Kristin Age: 42 Occupation: Business Administration Domain: Specialised in managing sales departments at regional and national level. Years of Experience: 11	Must identify positive and negative trends for different geographical segments and product categories in order to derive actionable insights.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
She needs to correlate data from different sources (company sales data, competitors' data) to identify market trend in regional and national level	Difficult to combine data from multiple sources
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Company's reports and custom excel files.	Sensitivity, anonymous data for data sharing between different stakeholders
SHORT DESCRIPTION	
Kristin is one of the sales managers of the company. One of her main goals is to gather and analyse data from different sources to be able to identify specific trends inside the task environment. However, it is difficult for her and her team to combine data from all the different external sources.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
METRO_04	**IT Operator**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: George Age: 37 Occupation: Software engineer Domain: Specialised in initiating and monitoring scheduled operations. Years of Experience: 8	Must manage different systems and needs to simplify daily operations.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Needs a user-friendly environment in order to initiate and monitor the procedure. Reassure the smooth operations of all systems.	The systems should operate all the time.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Operating systems, Cloud computing technologies, Database technologies, Web technologies,	Sensitivity, anonymous data for data sharing between different stakeholders
SHORT DESCRIPTION	
George is one of the many IT operators of the company. One of his main goals is to reassure the user-friendly environment of the systems and to monitor the procedures and their smooth operations. However, it is truly challenging for him and his team to manage all the daily issues in such a huge group of shops.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
METRO_05	**IT Security Officer**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Mike Age: 47 Occupation: Software engineer Domain: Specialised in monitoring systems and applications and checks security rules are followed. Years of Experience: 18	Security first.

GOALS *(what he/she wants to achieve)*	FRUSTRATIONS / PAIN POINTS *(what frustrates him/her currently at work)*
His goal is to reassure that no cyberattack will harm the security systems of the company. Needs notifications and reports for all security related issues.	Must identify and analyse security threats. Needs to be assured of a single point of truth, trustworthy data etc. Data should be transferred securely and anonymized.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Security software, Encryption technologies, Network security technologies, Security awareness and training technologies	Must conduct penetrate tests to be absolutely sure about the company's systems.
SHORT DESCRIPTION	
Mike is one of the IT security officers of the company. His goal is to reassure that no hacker will harm the company. However, it is truly challenging for him and his team to manage all the cyber threats.	

TANGO PERSONA	
PERSONA ID	**PERSONA ROLE IN TANGO**
METRO_06	**Hacker**
IDENTITY *(name, age, occupation, domain, years of experience)*	**QUOTES** *(important things he/she said)*
Name: Nikos Age: 36 Occupation: Digital Systems Domain: Specialised in stealing sensitive data from companies. Years of Experience: 10	Want to break the cyber defence of any company.
GOALS *(what he/she wants to achieve)*	**FRUSTRATIONS / PAIN POINTS** *(what frustrates him/her currently at work)*
Want to steal the data and reports from the company. Will try to provide meaningful identity via SSI without revealing his true identity.	To get caught during the attempt and not steal the data. To be arrested.
TECHNOLOGY / TOOLS USED	**OTHER IMPORTANT INFO**
Web services, AI tools, Linux system. SSI	
SHORT DESCRIPTION	
Nikos is an experienced hacker. His aim is to penetrate all the systems and steal reports and personal data. Then, he will use all this information to blackmail the CEO of the company.	

9.5.2 User Journeys

PERSONA:		Marketing Manager			
	JOURNEY STAGE	**TOUCHPOINTS/Related Technical offerings**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Logins to the system	Login from any device (mobile, tablet, web)	Indifferent, it is a routine procedure.	Marketing Team	
2.	Selects data search parameters (e.g. product characteristics, customer groups, stores group, geographical area, timing)	TANGO interface	She is not sure, and he possibly needs to change filtering parameters	Marketing Team	Retrieval of data (There should be a repository in Tango).
3.	Request data analysis results (customer segmentation, basket analysis)	TANGO user interface UPCV product clustering and prediction.	Nervous about the right choices of the parameters		
4.	Combines data from other external sources	TANGO user interface UPCV/UBEM interface to others.	Curious about the results that will occur from the combination.	Marketing Team	The system retrieves additional data from the internet.
5.	Receives recommendations for targeted and effective campaigns	TANGO user interface	Happy to receive the right data that she is looking for.	Marketing Team	
6.	Export result to feed CRM	TANGO user interface	Relieved that she did her job easily.	Marketing Team	

PERSONA:		Commercial Product Manager			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Logins to the system	Check-in form Device (mobile, tablet, web)	Indifferent, because it is a routine procedure.	Commercial Team	
2.	Retrieves data filtered according to the product categories in charge	TANGO user interface	He is not sure, and he possibly needs to	Commercial Team	

PERSONA:	Commercial Product Manager				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
			change filtering parameters		
3.	Retrieves data across the companies, which items belong to the same shopping baskets.	UPCV recommender used in item-item mode			
4.	Retrieves sales data by store, product category, supplier	TANGO user interface	Satisfaction, because the sales data shows that the products have performed well.	Commercial Team	
5.	Visualise the results of the analysis	Device (mobile, tablet, pc)	Excitement, because the visualised data reveals new opportunities or trends that they can leverage to drive sales and growth.	Commercial Team/ Marketing Team	

PERSONA:	Sales Manager				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Logins to the system	Check-in form Device (mobile, tablet, web)	Indifferent, it is a routine procedure.		
2.	Provides data of query -search data (e.g., product categories, customer groups, stores, geographical area, timing)	TANGO user interface	She is not sure, and she possibly needs to change filtering parameters		
3.	Asks sales data by store, by product category by supplier and by customer groups.	TANGO user interface UPCV recommender in user-user mode (within each company separately).	Curiosity, because the sales data reveals unexpected trends or patterns that require further analysis and	Coordinates business users for achieving profitability and Profit and Loss goals	

PERSONA:	Sales Manager				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
			exploration to understand.		
4.	Visualise the results of the analysis. Trustworthy data sharing	Choose from predefined analysis tools in Tango to have the Proposals' results - Solutions	Excitement, because the data reveals new opportunities or trends that they can leverage to drive sales and growth.	Finance -Business users to inform about the results and analyse.	

PERSONA:	IT Operator				
	JOURNEY STAGE	**TOUCHPOINTS/Possible Technical Offerings involved**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Logins to the company's system	Login from a Company's PC	Indifferent, it is a routine procedure.		
2.	Checks data availability in both Athens and Cyprus	Uses the Company's systems to check the availability of data	Concern, because the data may not be available or there may be issues with accessing the data.	Marketing Manager, Product Manager, Finance Coordinator	
3.	Logs into TANGO	Login from a Company's PC	Indifferent, it is a routine procedure.		
4.	Initiates the data transfer from Cyprus and Athens to the Tango platform	TANGO user interface	Accomplishment, because he is able to initiate and complete the data transfer successfully.	Marketing Manager, Product Manager ,Finance Coordinator	The data deriving from two different sources (databases – in Greece and Cyprus) needs to be Data anonymization is required A data repository is needed.

PERSONA:	IT Operator				
	JOURNEY STAGE	**TOUCHPOINTS/Possible Technical Offerings involved**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
5.	He is notified when data processing is completed	TANGO user interface	Pride, because he contributes to the success of the business, knowing that the processed data will be used to drive informed decisions and actions.	Marketing Manager, Product Manager Finance Coordinator	
6.	Request the deletion of the data set from Tango	TANGO user interface	Responsibility, because the data set is properly handled and deleted in accordance with company policies and legal requirements.	Marketing Manager, Product Manager Finance Coordinator	

PERSONA:	IT Security Officer				
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT/Possible Technical Offerings involved**
1.	Receives notification for hacking attempt	Email or Mobile notification	Anxiety, until he sees the report and takes control of the situation.		
2.	Logins to Tango	Login from a Company's PC	Concern, because of the potential impact of the attack on the company's data and systems.		
3.	View security reports	The TANGO user interface for security related issues	Satisfied, security rules are followed		The system should contain UI for security related issues

PERSONA:		Hacker			
	JOURNEY STAGE	**TOUCHPOINTS**	**EMOTIONAL STATUS**	**STAKEHOLDERS**	**CONTEXT**
1.	Attempting to connect to system (every data flow node – TANGO – Uploading data – Downloading reports - data)	Every device	Nervous, because he desperately wants to penetrate the system.	IT Department	The system does not allow connection from unauthorised users.
2.	Reattempts to enter system	Every device	Frustrated, because he is not able to achieve his goals.	IT Department	

9.5.3 Technology offerings used in use case scenario

TECHNOLOGY OFFERING	RELATION TO PILOT
Trustworthy Data Sharing	UPCV-based collaborative personalization. Customers will get a personalised view of Offerings, based on the behaviour of their peers. Companies will get data, grouping users (within each company) and products (across companies), as well as some predictions of product sales derived from this insight. UPCV/UBEM modules (one module per company) require user-item data, in the absence of loyal customer's persistent data, also shopping receipts (baskets) can be used as input.
Confidentiality and Privacy by Design	Ensuring confidentiality of data and partners' absolute control over how it is shared. Sticky policies and related identity-based techniques may be used to ensure only allowed entities may decrypt data. This offers a further step of protection for data at rest (apart from access control to cloud sharing platforms) and gives partners that share data complete control over their data, establishing policies for who can access it. That way, data shared by partners through the platform, like analytical data from specific physical stores, is always protected according to their wishes.
Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms	Data can be encrypted before data transfer.
Self-sovereign Identity Management	SSI Module enables the customer to manage his data and provide only necessary information to the retailer. Customer information can be shared to the retailer and transferred if the customer so wishes. Endorsing capabilities help other customers to choose products to their liking.
Seamless Onboarding for Users and Devices	The module will perform identity verification for the customers and the employees from the retailer, creating verifiable credentials, which will be later on used for authentication. The module will provide an SDK for the TANGO wallet, that will allow users to perform a 3-step verification process based on existing identity document such as the passport, and verify that the person on the actual identity document is the same with the person that is trying to onboard to the SSI Management.
User Continuous Behavioural Authentication	
Exploratory Data Analysis Engine	Dividing customers based on shopping frequency, amounts spent and recency to define their loyalty levels. Understanding shopping patterns and preferences between customers of different countries using different systems and structures. Exposing data to analysts of suppliers, new customer prospects that are setting up their business case, other markets, and the tourism industry.

TECHNOLOGY OFFERING	RELATION TO PILOT
	The Exploratory Data Analysis Engine (EDAE) can be used to provide a deep analysis of the sales data, product data, and customer data. EDAE can later be used by business/store managers to spot weak areas in a store in order to suggest areas that can be targeted for increased revenue. EDAE can be also used to provide a range of insights into customer behaviour. For example, exploring large datasets pertaining to customer purchasing patterns can indicate regional taste preferences, such as what is the most popular food in each country.
Dynamic Intelligent Execution on Heterogeneous Systems	In the analysis of data performed by the previous technology offering (T5.1), some processing may be offloaded to heterogeneous hardware (e.g., GPU). In this case, a dynamic intelligent plan (developed in T5.3) will be used to reduce the execution time of the processing, while also achieving high energy efficiency.
Energy-efficient AI model training	Federated Leaning techniques could be applied to train AI models with data at edge or other computing nodes without having to move or disclose the raw data. This will help in reducing energy consumption and privacy concerns.
Privacy Threat Modelling and Identification for Trustworthy AI	PEC will assess the privacy leakage of AI/ML services used to support this case. It will further assess privacy implications on anonymized data leading to measuring the strength of anonymization vs usability of the data.
Infrastructure Management based on AI	RENOPS could utilised in two ways (to be further investigated and finalized in D2.4). First way would be directly via RENOPS scheduler script, that would find most optimal time to schedule backups, analytics or AI model training. Second way would be indirectly as part of other related and energy intensive jobs as part of WP5. One possibility would be as part of T5.1 EDAE to find the most optimal time to run the analytics. The second possibility would be as part of T5.2 Energy efficient AI model training where RENOPS could be added as one of the features.

9.6 KPIs

TITLE	DESCRIPTION
Reduction of privacy violation incidents in data sharing	Privacy assessment results comparison of existing infrastructure with TANGO proposed data sharing platform.
Accuracy of user verification and authentication > 99.6%	Performance evaluation considering metrics such as false acceptance rate, false rejection rate and failure to access.
Accuracy of planning the hardware accelerated code for execution on the most energy efficient device in the system (single node) > 98%	This KPI measures the effectiveness of the intelligent execution plan that will be offered by T5.3. The ML-based scheduling plan will be trained to deploy input code on the most energy efficient device of the system (single node).
Cybersecurity	This KPI measures the effectiveness of the platform's cybersecurity measures in protecting sensitive data from cyber threats. It can be measured through penetration testing and vulnerability assessments and can be used to determine the company's ability to protect its clients' data.

Accuracy in recommendations	Evaluation of recommendations as evaluated by experts and customers.
Reduction in data processing time for the IT Manager	Comparison between existing processing time and after the TANGO implementation.
Reduction in data processing time for the marketing/sales manager	Comparison between existing processing time and after the TANGO implementation.
Employee satisfaction	Evaluation of the overall TANGO platform contributing to daily processes and operations.

10 Summary of findings

10.1 Overview of User and Functional Requirements

An overview of the user requirements is presented in the following table. The table also includes a list of proposed functional requirements that will be further refined and analysed in D2.3.

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-TUA-HT-001	Hospitality	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.	The system must support trusted user authentication for all user categories via various devices.	High
UR-DMN-HT-002	Hospitality	Data management	Hotels must be able to collect clients' personal data directly through the web (direct booking).	The system must allow the collection of clients' personal data directly through the web (direct booking).	High
UR-DMN-HT-003	Hospitality	Data management	The hotel must be able to collect the clients' preferences in order to provide them with personalised services.	The system must support the collection of the hotel's clients' preferences in order to provide them with personalised services.	High
UR-DMN-HT-004	Hospitality	Data management	The hotel must be able to collect data from rooms, hotel facilities, logistics information, etc.	The system must facilitate the collection of data from rooms, hotel facilities, logistics information etc. (or through interconnection with NADIA platform).	High
UR-DMN-HT-005	Hospitality	Data management	The hotel must collect data from the various systems that it uses (e.g., CRM, NADIA, etc.).	The system must allow the collection of clients' data from the various systems that the hotel uses in a unified and integrated way.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DMN-HT-006	Hospitality	Data management	The client must be able to evaluate the recommendations received by the system.	The system must allow clients to evaluate the recommendations they received from the system.	High
UR-DMN-HT-007	Hospitality	Data management	The client must be able to evaluate the overall experience.	The system must allow clients to evaluate the overall experience.	High
UR-DMN-HT-008	Hospitality	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.	The system must allow the experience provider to have access to the hotel's suggestion system to provide and enter data and information about the provided experience.	High
UR-DAR-HT-009	Hospitality	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.	The system must enable the manager and the hotel group manager to analyse the data collected from customers and produce reports that can be exported in various forms.	High
UR-TDS-HT-010	Hospitality	Trustworthy Data sharing	The users must feel safe when they share their data.	The system must enable data sharing only among the relevant stakeholders/business partners.	High
UR-GCO-HT-011	Hospitality	GDPR and related regulation compliance	The customer's data must be handled according to GDPR.	The data must be managed based on GDPR.	High
UR-PCY-HT-012	Hospitality	Protection from cyberattacks	The customer must feel safe when uploading his/her personal data.	The platform must protect the uploaded data from cyberattacks.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DMN-HT-013	Hospitality	Data management	The hotel should be able to collect and record the clients' preferences during their stay.	The system should support the collection and recording of tourists' preferences during their stay.	Medium
UR-UIN-HT-014	Hospitality	User interaction	The client should be able to choose among various suggestions based on their preferences (food, activities, etc.).	The system should suggest/provide services to clients based on their preferences.	Medium
UR-UIN-HT-015	Hospitality	User interaction	The client should receive personalised information based on his/her preferences and other external data sources (e.g., weather, monument or activities schedule, etc.).	The system should suggest/provide information to clients based on their preferences and other external data sources (e.g. weather, monument or activities schedule, etc.).	Medium
UR-DAR-HT-016	Hospitality	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.	The system should be able to present to the clients the hotel's sustainability data and environmental footprint in a user-friendly way.	Medium
UR-DAR-HT-017	Hospitality	Data analysis and reporting	The hotel management and the hotel association should be able to be informed about their sustainability data and environmental footprint.	The system should analyse/combine the sustainability data and report/visualise the output to the hotel management/hotel association.	Medium
UR-DMN-HT-018	Hospitality	Data management	The users must be able to access data/information from external sources (weather, monument or activities schedule, etc.).	The system must be able to access/process data from external sources (e.g. weather, monument or activities schedule, etc.).	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-TDS-HT-019	Hospitality	Trustworthy Data sharing	The hotels of the same chain could be able to share customer information and profiles in a secure way.	The platform could allow sharing customer information and profiles in a secure way among the hotels of the same chain.	Low
UR-TUA-AV-001	Autonomous Vehicles	Trusted user authentication	The user must be authenticated through the application on smartphones or other smart devices (tablets, etc.).	The system must support user authentication through the application on smartphones or other smart devices (tablets, etc.).	High
UR-DIN-AV-002	Autonomous Vehicles	Data integrity	The autonomous vehicle passenger must feel safe and relaxed during the ride.	The platform must ensure data accuracy and integrity.	High
UR-PCY-AV-003	Autonomous Vehicles	Protection from cyberattacks	The autonomous vehicle passenger must feel safe and relaxed during the ride regardless of any external threat during the ride.	The platform must protect the data flow from cyberattacks during the ride.	High
UR-PCY-AV-004	Autonomous Vehicles	Protection from cyberattacks	The management must feel safe that the car is protected and cannot be accessed by malicious intruders.	The platform must protect the data flow from cyberattacks during the ride.	High
UR-DUP-AV-005	Autonomous Vehicles	Data upload	The engineering team must be able to upload sensor data to the system in a trustworthy way.	The system must ensure safe data upload.	High
UR-GCO-AV-006	Autonomous Vehicles	GDPR and related regulations compliance	The engineering team must be able to upload GDPR compliant sensor data to the system.	The data must be managed based on the GDPR and all the related data protection regulations.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DAC-AV-007	Autonomous Vehicles	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).	The system must support data access control.	High
UR-TDS-AV-008	Autonomous Vehicles	Trustworthy Data sharing	The automotive services company must be able to prevent their customers from sharing their maps with third parties.	The data must be shared only among the relevant stakeholders at each time.	High
UR-PCY-AV-009	Autonomous Vehicles	Protection from cyberattacks	The automotive services company must be able to control if somebody modifies the content of the files (the maps).	The platform must protect the map data from cyberattacks.	High
UR-DAC-AV-010	Autonomous Vehicles	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).	The system should provide 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
UR-TDS-AV-011	Autonomous Vehicles	Trustworthy Data sharing	Clients should be sure that the digital maps are trustworthy.	The system should ensure the trustworthiness of digital maps.	Medium
UR-PCY-AV-012	Autonomous Vehicles	Protection from cyberattacks	The automotive services company could be able to control and monitor any attempts of cyberattacks.	The system could ensure protection from cyberattackers and unauthorised attempts of access / attacks.	Low

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DMN-AV-013	Autonomous Vehicles	Data management	The engineering team could be able to change the data real time.	The data could be managed with flexibility and speed.	Low
UR-DMN-AV-014	Autonomous Vehicles	Data management	The autonomous vehicle passenger could be able to request a change during the ride.	The system could provide immediate response to user requests.	Low
UR-UIN-AV-015	Autonomous Vehicles	User interaction	Clients could be able to use a smart device via a user friendly interface to use the autonomous vehicle.	The system could allow and provide the use of the autonomous vehicle via a smart device's user's interface.	Low
UR-TUA-M1-001	Manufacturing 1 FMAKE	Trusted user authentication	The customer must be authenticated to have access to the system.	The system must support trusted user authentication for customers.	High
UR-TDS-M1-002	Manufacturing 1 FMAKE	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.	The system must provide efficient and smooth data sharing between customers and the printing company, through a shared online working space.	High
UR-TUA-M1-003	Manufacturing 1 FMAKE	Trusted user authentication	The printer operator and the technical expert must be authenticated to have access to the system.	The system must support trusted user authentication for printer operator and technical expert.	High
UR-DAC-M1-004	Manufacturing 1 FMAKE	Data access	The technical expert must have full access to all printing jobs to combine designs and prepare the print job file.	The system must provide full access to the technical expert to all printing jobs.	High
UR-DST-M1-005	Manufacturing 1 FMAKE	Data storage	The customers need to be able to access their printing job data for a short defined period of time.	The system must provide a back-up solution on the online shared working space for the client's data for a short period of time.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DUP-M1-006	Manufacturing 1 FMAKE	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).	The data from the printer must be uploaded automatically and safely to the online shared working space.	High
UR-DAC-M1-007	Manufacturing 1 FMAKE	Data access	The customer must have access to his/her printing jobs in a secure way.	The system must allow restricted data access according to user rights.	High
UR-DAC-M1-008	Manufacturing 1 FMAKE	Data access	The customer must not be able to access printing data of other customers.	The system must ensure IP ownership protection.	High
UR-DAR-M1-009	Manufacturing 1 FMAKE	Data analysis and reporting	The customers (different IP-owners) must be able to access and view their own quality report only.	The system must be able to extract a part of the dataset that belongs to a specific customer, analyse it and generate a report.	High
UR-DAR-M1-010	Manufacturing 1 FMAKE	Data analysis and reporting	The technical expert must receive reports on the print jobs to improve the printer operation and the printing quality.	The system must be able to produce reports and enable data analysis.	High
UR-DAR-M1-011	Manufacturing 1 FMAKE	Data analysis and reporting	The manager must be able to read/view the data of all customers to get KPIs from them.	The system must be able to produce reports and enable data analysis from all printing jobs.	High
UR-DAR-M1-012	Manufacturing 1 FMAKE	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.	The system must ensure the use of machine learning models for the digital twins and the production of printing quality reports.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-GCO-M1-013	Manufacturing 1 FMAKE	GDPR and related regulation compliance	The customer's data must be handled according to GDPR.	The data must be managed based on the GDPR and all the related data protection regulations.	High
UR-PCY-M1-014	Manufacturing 1 FMAKE	Protection from cyberattacks	The customer's printing data must be protected from any kind of cyber-attacks.	The platform must protect the data from cyberattacks.	High
UR-DMN-M1-015	Manufacturing 1 FMAKE	Data management	The technical expert and printing operator should be able to modify the printing data and improve them.	The system should allow the technical expert and printing operator to modify the printing data.	Medium
UR-PMT-M1-016	Manufacturing 1 FMAKE	Process monitoring	The technical expert should be able to inspect the printing process data and the changes made.	Secure mechanisms should facilitate the monitoring of the printing process, the access to files and of the conducted changes	Medium
UR-DMN-M1-017	Manufacturing 1 FMAKE	Data management	The customer should be able to manage his/her printing jobs, e.g., request a reprint, etc.	The system should allow data management for the customer according to his/her rights.	Medium
UR-DAR-M1-018	Manufacturing 1 FMAKE	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.	The system should enable users to investigate and analyse quality issues.	Medium
UR-DAR-M1-019	Manufacturing 1 FMAKE	Data analysis and reporting	The Data Scientist should be able to pre-process the existing data.	The systems should allow specific users to pre-process the existing data.	Medium
UR-DAR-M1-020	Manufacturing 1 FMAKE	Data analysis and reporting	The Data Scientist should be able to improve the model for better predictions.	The system should allow specific users to make improvements to the prediction model.	Medium

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-PMT-M1-021	Manufacturing 1 FMAKE	Process monitoring	The technical manager could be able to inspect the printing process per customer (IP owner).	The system could allow the printing process traceability per IP owner.	Low
UR-TUA-M2-001	Manufacturing 2 RIASTONE	Trusted user authentication	Shopfloor workers must have access only to their designated areas.	The system must support trusted user access to their designated areas.	High
UR-TUA-M2-002	Manufacturing 2 RIASTONE	Trusted user authentication	The company files must be protected in a smart way, enabling access based on each person's role.	The system must support trusted user authentication for each user.	High
UR-PMT-M2-003	Manufacturing 2 RIASTONE	Process monitoring	The supervisor must know every time a worker is not at the designated area.	The system must be able to detect potential unauthorised access to specific areas.	High
UR-PMT-M2-004	Manufacturing 2 RIASTONE	Process monitoring	The supervisor must be notified every time a worker is not at the designated area.	The system must support sending notifications to specific users.	High
UR-TUA-M2-005	Manufacturing 2 RIASTONE	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.	The system must allow specific technology providers to use and make changes to specific services and applications in a secured way.	High
UR-PCY-M2-006	Manufacturing 2 RIASTONE	Protection from cyberattacks	The company's data must be protected from any kind of cyber-attacks.	The platform must protect the data from cyberattacks.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-GCO-M2-007	Manufacturing 2 RIASTONE	GDPR and related regulation compliance	The customer's data must be handled according to GDPR.	The data must be managed based on the GDPR and all the related data protection regulations.	High
UR-PMT-M2-008	Manufacturing 2 RIASTONE	Process monitoring	The supervisor should have records of all unauthorised access attempts in the platform system.	The system should record all unauthorised access attempts in the platform system.	Medium
UR-DAR-M2-009	Manufacturing 2 RIASTONE	Data analysis and reporting	The supervisor should receive a report of all unauthorised access attempts in the platform system.	The system should be able to produce and send reports of all unauthorised attempts in the platform system to specific users.	Medium
UR-PMT-M2-010	Manufacturing 2 RIASTONE	Process monitoring	The company should be able to monitor the shopfloor for any strange movements and be notified.	The system should monitor for strange movement patterns and be able to automatically issue an alarm or send notifications to specific users.	Medium
UR-TUA-M2-011	Manufacturing 2 RIASTONE	Trusted user authentication	Each technology partner should access the factory through a Data Gate Keeper.	The system should support trusted user authentication for each technology provider.	Medium
UR-TUA-M2-012	Manufacturing 2 RIASTONE	Trusted user authentication	Specific users should know if the technology providers are not following the authorised path for their applications.	The system should be able to monitor all unauthorised attempts in the platform system to specific users.	Medium
UR-TUA-M2-013	Manufacturing 2 RIASTONE	Trusted user authentication	Specific users should receive security breach notifications if the technology providers are not following the authorised path for their applications.	The system should be able to send reports and security breach notifications of all unauthorised attempts in the platform system to specific users.	Medium

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-PMT-M2-014	Manufacturing 2 RIASTONE	Process monitoring	The company should have a clear view and records of the technology partners' actions during their presence in the system.	The system should monitor and record the actions of the technology providers' access.	Medium
UR-PCY-M2-015	Manufacturing 2 RIASTONE	Protection from cyberattacks	The company's operation should not be interrupted by any unauthorised access.	The system should not allow any unauthorised access attempt.	Medium
UR-TUA-M2-016	Manufacturing 2 RIASTONE	Trusted user authentication	The Data Gate keeper could ensure authentication, restricted application access, etc.	The system could ensure authentication, restricted application access, etc. via a centralised data gate keeper.	Low
UR-DMN-M2-017	Manufacturing 2 RIASTONE	Data management	The company documents could be shared but not changed by the people accessing them.	The system could allow data file sharing and access according to their user rights.	Low
UR-DMN-M2-018	Manufacturing 2 RIASTONE	Data management	Specific clients could be able to share data to specific users.	The system could enable data sharing between specific users in a secured way.	Low
UR-TUA-PA-001	Public Admin	Trusted user authentication	The applicants must be authenticated to have access to the system.	The system must support trusted user authentication for applicants.	High
UR-TUA-PA-002	Public Admin	Trusted user authentication	The VISAR employees must be authenticated to have access to the system.	The system must support trusted user authentication for VISAR employees.	High
UR-TUA-PA-003	Public Admin	Trusted user authentication	The employers must be authenticated to have access to the system.	The system must support trusted user authentication for employers.	High
UR-TUA-PA-004	Public Admin	Trusted user authentication	The authority employees must be authenticated to have access to the system.	The system must support trusted user authentication for authority employees.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DUP-PA-005	Public Admin	Data upload	The applicants must be able to upload documents and data to the system in a trustworthy way.	The system must ensure safe document and data upload.	High
UR-DUP-PA-006	Public Admin	Data upload	The VISAR employees must be able to upload documents and data to the system in a trustworthy way.	The system must ensure safe document and data upload.	High
UR-DUP-PA-007	Public Admin	Data upload	The employers must be able to upload documents and data to the system in a trustworthy way.	The system must ensure safe document and data upload.	High
UR-DUP-PA-008	Public Admin	Data upload	The authority employees must be able to upload documents and data to the system in a trustworthy way.	The system must ensure safe document and data upload.	High
UR-DMN-PA-009	Public Admin	Data management	The VISAR employee must be able to monitor and manage the documents and the data flow in the system.	The system must enable specific users to monitor and manage the data flow in the system.	High
UR-TDS-PA-010	Public Admin	Trustworthy Data sharing	The users must be able to share data in a trustworthy and secure way.	The system must allow users to share data and documents in a trustworthy and secure way.	High
UR-GCO-PA-011	Public Admin	GDPR and related regulation compliance	The applicant's data must be handled according to GDPR.	The data must be managed based on the GDPR and all the related data protection regulations.	High
UR-PCY-PA-012	Public Admin	Protection from cyberattacks	The users must feel secure that the data and document flow is not compromised.	The platform must protect the documents and data flow from cyberattacks.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-PCY-PA-013	Public Admin	Protection from cyberattacks	The applicants must feel secure when uploading and sharing their data within the platform.	The platform must protect the applicants' data from cyberattacks.	High
UR-DMN-PA-014	Public Admin	Data management	The VISAR employees should be able to ensure that the uploaded documents are real and can authenticate them.	The system should provide a document validation system, to verify authenticity and detect fakes.	Medium
UR-UIN-PA-015	Public Admin	User interaction	Applicants could be able to have a better experience via the use of AI technology.	System could enhance the applicants' experience through the incorporation of AI technology, to provide faster response time and 24/7 availability. (e.g. an AI chat).	Low
UR-DMN-PA-016	Public Admin	Data management	VISAR employees could use a document recognition and pdf mapping software to automatically identify mismatches and incorrect information inputs.	System could provide the company with document recognition and PDF mapping capabilities, to automatically identify potential mismatching, and ensure correct information extraction.	Low
UR-DMN-PA-017	Public Admin	Data management	VISAR employees could use a document validation system to verify authenticity and detect fakes.	System could provide a document validation system, to verify authenticity and detect fakes.	Low
UR-TUA-RT-001	Retail	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.	The system must support trusted user authentication for all user categories via various devices.	High
UR-DMN-RT-002	Retail	Data management	Specific users must be able to upload data to the system.	The system must enable specific users to upload data to the system.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DMN-RT-003	Retail	Data management	Specific users must be able to request data harmonisation from the master and transactional databases.	The system must enable data harmonisation from the master and transactional databases.	High
UR-DMN-RT-004	Retail	Data management	Specific users must be able to request a common view and analysis of data.	The system must support a common view and analysis of data.	High
UR-DMN-RT-005	Retail	Data management	Specific users must be able to view the harmonised data in various views with various filters and search parameters.	The system must allow specific users to view the harmonised data in various views with various filters and search parameters.	High
UR-DMN-RT-006	Retail	Data management	Specific users must be able to run queries to the harmonised data.	The system must allow specific users to run queries to the harmonised data.	High
UR-DMN-RT-007	Retail	Data management	Specific users must be able to request for specific data analysis results.	The system must be able to produce specific data analysis reports based on users requests.	High
UR-DMN-RT-008	Retail	Data management	Specific users must be able to combine data from various external sources.	The system must be able to combine data from various external sources based on user requests.	High
UR-DMN-RT-009	Retail	Data management	Specific users must receive recommendations for targeted and effective campaigns.	The system must produce and send to specific users recommendations for targeted and effective campaigns.	High
UR-DMN-RT-010	Retail	Data management	Specific users must be able to retrieve the requested data (e.g., sales data, etc.).	The system must allow and enable specific users to retrieve the requested data (e.g. sales data, etc.).	High
UR-DMN-RT-011	Retail	Data management	Specific users must be able to delete the uploaded data from the system.	The system must allow specific users to delete the uploaded data from the system.	High

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-TDS-RT-012	Retail	Trustworthy data sharing	Specific users must be able to share data in a safe and trustworthy way.	The system must allow specific users to share data in a safe and trustworthy way.	High
UR-DAR-RT-013	Retail	Data analysis and reporting	Specific users must receive notifications from the system after data processing or analysis is completed.	The system must produce and send notifications to specific users after data processing or analysis is completed.	High
UR-DAR-RT-014	Retail	Data analysis and reporting	Specific users must be able to analyse data.	The system should allow specific users to analyse data.	High
UR-DAR-RT-015	Retail	Data analysis and reporting	Specific users must be able to visualise data.	The system should allow specific users to visualise data.	High
UR-DAR-RT-016	Retail	Data analysis and reporting	Specific users must be able to produce customised reports.	The system must enable specific users to produce customised reports.	High
UR-GCO-RT-017	Retail	GDPR and related regulation compliance	The company's data must be handled according to GDPR.	The data must be managed based on the GDPR and all the related data protection regulations.	High
UR-PCY-RT-018	Retail	Protection from cyberattacks	The users must feel secure that the data flow is not compromised.	The platform must protect the data flow from cyberattacks.	High
UR-PCY-RT-019	Retail	Protection from cyberattacks	The company must feel safe from cyberattacks.	The system must protect the data from cyberattacks.	High
UR-DMN-RT-020	Retail	Data management	Specific users should be able to view the automatically mapped data from different sources and data structures.	The system should enable automatic mapping of data from different sources and data structures.	Medium
UR-DMN-RT-021	Retail	Data management	Specific users should be able to retrieve market/ marketing/ product data from external sources, periodically or not.	The system should be able to retrieve market/ marketing/ product data from external sources, periodically or not.	Medium

CODE	PILOT	CATEGORY	USER REQUIREMENTS DESCRIPTION	PROPOSED FUNCTIONAL REQUIREMENTS DESCRIPTION	PRIORITY
UR-DMN-RT-022	Retail	Data management	The users should use anonymized data.	The system should enable data anonymization.	Medium

10.2 Overview of technologies used per Use Case

	Technology / Pilot	Smart hospitality (ANYSOL)	Autonomous Vehicles (IDIADA)	Smart manufacturing (FMAKE)	Smart manufacturing (RIA)	Public administration (VISAR)	Retail (METRO)	Banking (ABILAB)
T3.1	Blockchain-based Data Storage and Sharing					X		(X)
T3.2	Trustworthy Data Sharing	X	X		X		X	
T3.3	Confidentiality and Privacy by Design	X	X	X	X	X	X	
T3.4	Self-encryption and Decryption Techniques with Multi-Factor Information Recovery Mechanisms		X	X			X	
T3.5	ePrivacy Mechanisms, Protocols and Processes	X	X	X	X	X	X	X
T4.1	Self-sovereign Identity Management	X	X	X	X	X	X	
T4.2	Seamless Onboarding for Users and Devices	X	X	X	X	X	X	
T4.3	User Continuous Behavioural Authentication	X	X	X		X	X	X
T4.4	Device Continuous Behavioural Authentication		X		X			

	Technology / Pilot	Smart hospitality (ANYSOL)	Autonomous Vehicles (IDIADA)	Smart manufacturing (FMAKE)	Smart manufacturing (RIA)	Public administration (VISAR)	Retail (METRO)	Banking (ABILAB)
T4.5	**Hardening against Side-channel Attacks**	**X**						
T5.1	**Exploratory Data Analysis Engine**	**X**		**X**			**X**	
T5.2	**Energy-efficient AI model training**			**X**	**(X)**			**(X)**
T5.3	**Dynamic Intelligent Execution on Heterogeneous Systems**	**X**		**X**			**X**	
T5.4	**Privacy Threat Modelling and Identification for Trustworthy AI**	**X**	**X**			**X**	**X**	
T5.5	**X-AI for Privacy and Trust Enhancement**			**X**				**X**
T5.6	**Infrastructure Management based on AI**	**(X)**		**X**			**(X)**	**(X)**

Conclusions

Having conducted several interviews with the use case - pilot partners, we have defined the user requirements to be implemented in the TANGO solution using the TANGO technical offerings.

The requirements have been coded and listed separately by pilot and in a summarised table and will be used also for the evaluation of the pilots in the WP7 “Pilot Demonstration and Validation”.

Apart from the complexity of each of the pilots, the diversity of the procedures and business requirements imposed a challenge in collecting the requirements in a common and homogeneous way to be able to group them into categories and map them to the TANGO technical offerings. Collaboration between the pilot partners and the technical partners of the project was also necessary to align the requirements and the offerings and to provide the needed information for the next phase, the definition of the system requirements and the system architecture in deliverable D2.3. Refinements of the requirements, journeys and KPIs might happen during the implementation of the TANGO solution and the implementation of the pilots.

This deliverable provided input to the deliverable D2.1 while it also received input from it.

The basic outcomes of this deliverable are thus the user requirements for each pilot, the technology to pilots mapping and the definition of the KPIs for each pilot that along with the user journeys will be used for the pilot evaluation.