E-CORRIDOR
Edge Enabled Privacy & Security Platform For Multi Modal Transport

D2.2

Design and Architecture for the Airport and Train (AT) Pilot

WP2 – Airport and Train (AT) Pilot

E-CORRIDOR

Edge enabled Privacy and Security Platform for Multi Modal Transport

Due date of deliverable: 31/05/2021
Actual submission date: 31/05/2021

31/05/2021
Version 1.0

Responsible partner: ADP
Editor: Olivier Mercier
E-mail address: Olivier.MERCIER@adp.fr

Project co-funded by the European Union within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The E-Corridor Project is supported by funding under the Horizon 2020 Framework Program of the European Union DS-2018-2019-2020, GA #883135

Authors: Stefano Sebastio, Hajer Saada, Amine Lamine, Shane Daly, Riccardo Orizio (UTRC), Abdelghani Chibani, Roghayeh Mojarad (PEC), Christian Plappert (FhG), Olivier Mercier (ADP)

Approved by: Veronica Elena Bocci, Guido Ancarani (DIG), Gianpiero Costantino (CNR)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.01	12-Mar-2021	S. Sebastio	UTRC	Initial table of content
0.02	07-Apr-2021	H. Saada	UTRC	First draft of the security models for the pilot, architecture diagrams
0.03	09-Apr-2021	S. Sebastio	UTRC	Some notes on the analytics and security services, grouping of use cases with steps to be performed in each and some DSAs
0.04	15-Apr-2021	H. Saada	UTRC	Updated the architecture diagrams and added some description
0.05	19-Apr-2021	H. Saada	UTRC	Update on the Security model section
0.06	29-Apr-2021	S. Sebastio	UTRC	Deployment models, data formats, requirement matrix
0.07	05-May-2021	S. Sebastio	UTRC, PEC	Executive summary, description of the PRM related block diagram
0.08	06-May-2021	S. Sebastio, H. Saada	UTRC	Improved system architecture description and diagrams
0.09	07-May-2021	A. Chibani, R. Mojarad	PEC	Draft intro and system overview
0.10	09-May-2021	S. Sebastio, C. Plappert	UTRC, FhG	Recap of the analytics and advanced security services adopted
0.11	10-May-2021	S. Sebastio	UTRC	Block diagram match to user stories and requirements
0.12	10-May-2021	S. Sebastio	UTRC	Deployment of the E-CORRIDOR framework in the AT pilot
0.13	11-May-2021	S. Sebastio	UTRC	Security models
0.14	11-May-2021	R. Mojarad, A. Chibani, O. Mercier	PEC, ADP	Block diagrams for the first two scenarios and descriptions for the multi-biometric case. Use of PEC components in the AT pilot
0.15	12-May-2021	S. Sebastio	UTRC	Block diagrams for the collaborative data sharing with description
0.16	13-May-2021	S. Sebastio	UTRC	Relevance of the AT pilot expected impact from E-CORRIDOR plus intro of Sec 9
0.17	14-May-2021	S. Sebastio, A. Lamine, S. Daly	UTRC	Analytics and security services in the AT pilot
0.18	14-May-2021	O. Mercier, A. Chibani, R. Mojarad	ADP, PEC	KPI, Hardware and Software Requirement, Update schema and components description
0.19	15-May-2021	O. Mercier, A. Chibani, R. Mojarad	ADP, PEC	Connectors, Update schema and components description
0.20	17-May-2021	O. Mercier, A. Chibani, R. Mojarad	ADP, PEC, FhG	Connectors, Update schema and components description. Version sent to internal reviewers
0.21	26-May-2021	S. Sebastio	UTRC	Several corrections throughout the whole document
0.22	27-May-2021	A. Chibani	PEC	Some additions to the data sharing section
1.0	28-May-2021	S. Sebastio, R. Orizio	UTRC	Integration of the reviewers comments, new data sharing, final corrections to text, diagrams and evaluation metrics – Released version

Executive Summary

This deliverable introduces the first iteration of the Airport-Train (AT) pilot architecture in the E-CORRIDOR project. The architecture design is guided by the pilot requirements expressed at month six (M6) in the deliverable D2.1 “Requirements for the AT pilot” and the general architecture of the E-CORRIDOR framework described at M12 in the deliverable D5.2 “First version of the E-CORRIDOR architecture”. The final goal of this document is to set the basis for performing implementation, integration and subsequent validation of the E-CORRIDOR framework instantiated in the AT pilot.
The AT pilot architecture has placed special attention in providing a frictionless experience in multi-modal travels (particularly caring about passengers with reduced mobility) and the controlled sharing of the data among different security domains and stakeholders for service optimization and enhanced cyber-security capabilities.

Table of contents

1. Introduction

1.1 Overview

The AT pilot aims to demonstrate how E-CORRIDOR technologies can support the achievement of seamless, secure and privacy preserving authentication procedures for passengers employing a multi-modal transport. Indeed, the passenger journey is usually not confined between departing and destination airports but more often multiple modes of transportation are involved. E.g., the passenger could use a car sharing service to reach the closest train station, and from there she could take a train connecting to the airport. Sometimes there is also the need to take connecting flights. And the multi-modal scenario continues at destination as well, e.g., by taking a train to reach the desired city and then using the car sharing to reach the hotel. Several identification, monitoring, and authentication services owned by different transport entities need to interoperate and exchange data with the final goal of providing a frictionless experience to the passengers.

1.2 Scope

The main purpose of this deliverable is the description of the architecture design of the AT pilot by considering the integration of the E-CORRIDOR framework. Basically, it will lay the foundation for all the subsequent implementation, validation and evaluation efforts of the E-CORRIDOR technologies (of both the core framework and the customized components) in the pilot scenario. The architecture design in the pilot will progress hand in hand with the one of the general E-CORRIDOR architecture (carried out in Task T5.2 "E-CORRIDOR platform architecture"): pilot specific requirements are generalized and integrated in the E-CORRIDOR architecture, the latter is then customized and deployed in the pilot.

With respect to the E-CORRIDOR project objectives (Obj.), discussed in detail in Section 9.1, by analyzing the requirements expressed in D2.1, the key aspects considered in designing the architecture of the AT pilot are the need for: (i) a *privacy-aware data sharing* among all the stakeholders involved in the multi-modal journey - Obj.1; (ii) performing *edge computation* (due to regulatory requirements while managing highly sensitive data) – Obj.2; (iii) *enforcing cyber-security* in the multiple domains characterizing the pilot – Obj.3; (iv) supporting a secure token-based multi-biometric *seamless authentication* and access – Obj.5.

The pilot architecture will be evaluated according to: (i) its ability to ensure an effective and efficient integration in the pilot environment by satisfying all the AT pilot requirements; (ii) its maintainability and ability to be accepted by passengers, transportation entities, and any other stakeholder involved in the transport services. In particular, a successful evaluation of the second point is tightly related to the achievement of the project Objectives 4 and 6 related to the creation of *products for the pilot and their adoption*.

1.3 Structure of the Deliverable

The remaining of this deliverable is structured as follows. First, in Section 2, the overall scenario, actors and goals of the AT pilot are recalled from D2.1 wherein requirements have been drawn. Then, Section 3 starts the description of the architecture designed for the AT pilot, which stems from the features available in the E-CORRIDOR core framework. In particular, components available and tailored for the pilot requirements in the Information Sharing Infrastructure (ISI), Information Analytics Infrastructure (IAI) and Advanced Security Infrastructure (ASI) subsystems are mentioned.

Application and design of the data analytics and the security service components to the AT pilot are discussed in Section 4.1. The mode of operations of those components and their usefulness to fulfill the pilot requirements are exemplified through a few block diagrams in Section 4.2. Data, security and deployment models considered in the AT pilot architecture are described, respectively in Section 5, 6 and 7. The requirements matrix presented in Section 8 summarizes how the designed architecture is able to achieve the AT pilot needs.
Contribution of the AT pilot architecture to the E-CORRIDOR objectives and the expected impact of the innovation brought are discussed in Section 9. Finally, some measures that will be considered in the next months of the project while implementing, validating and evaluating the architecture and the proposed solutions are included in Section 10. The deliverable ends with some final remarks in Section 11.

2 System Overview

The architecture designed for the AT pilot is based on the E-CORRIDOR core framework and its components and features. In particular, the AT pilot architecture offers a set of privacy-aware capabilities enabling a seamless access to the transportation services for the passengers and facilitating the operational management of passengers flow and security for all the entities involved in the passenger transport. These are widely considered by large airports and train stations as the main area for unleashing the potential of an integrated transportation. To this end, the AT pilot architecture will leverage on a set of innovative technological components enabling privacy-aware multi-modal sensing, data sharing, security and analytics services collaboratively working on the different domains characterizing the multi-modal transportation system.

In the following, we briefly recall actors, scenario and goals considered in the AT pilot as introduced in D2.1.

2.1 Recall of the pilot actors

Users:

a. Passenger – adult not needing any mobility assistance during her/his (multi-modal) journey.
b. Passenger with Reduced Mobility (PRM) requiring assistance – any person whose mobility, when using transport, is permanently or temporarily reduced and therefore needs appropriate attention (e.g., disabled or elderly). In particular, we focus on passengers using assistive devices (e.g., wheelchair).
c. PRM assistant – person in charge of providing assistance to the PRM passenger on behalf of the transportation entity. In multi-modal journeys, PRM assistants of different entities must collaborate to ensure a smooth travel for the passenger.

Airport:

a. Airport Managing Body (AMB) – body that, under national legislation, administers and manages the airport infrastructures, and coordinates and controls the activities performed in the airport.
b. Airport services - aviation and non-aviation services offered in the airport premises

Train station:

a. Station manager – the organizational entity responsible for the management of the railway station.

Carriers:

a. Air carrier
b. Train carrier
c. Potentially, any other carrier reaching/connecting with the airport.

In the AT pilot, carrier operations are represented by the Departure Control System (DCS) used for managing reservations, the check-in, printing the boarding pass and baggage handling. DCS simulators will be considered within the E-CORRIDOR project, e.g., Amadeus [1] and Sabre Rail DCS [2].

2.2 Recall of the pilot scenario

The overarching scenario that has led the design of the AT pilot architecture contemplates the multi-modal journey of (PRM) passengers and how to enhance it through seamless, secure, and privacy preserving authentication procedures while enhancing security and operations management for the transportation entities (a vision aligned with the IATA NEXTT [3]). Indeed, passenger journeys usually encompass connections with both same and different mode of transport. In this pilot, the focus is on the train and airport interconnection.

An example of multi-modal transportation in the AT pilot includes the passenger taking the train as first mode of transport, and reaching the airport for a connecting flight. In the railway station, the passenger performs the required identification and check-in operations. Once arrived in the airport, the information about the initial passenger authentication performed at the railway station is exchanged and enriched, e.g., the flight onboarding procedures require the additional verification of the passenger identity through passport or identity card. In the airport, throughout a collaborative environment instantiated among the two transportation entities, the passenger is seamlessly re-authenticated also exploiting the initial knowledge gained at the beginning of the journey. Such a knowledge will include both identification and authentication information as well as passenger preferences to enable a frictionless end-to-end multi-modal passenger journey and access to the transportation services. To improve the passenger experience, context-aware multi-factor authentication, distributed context-aware sensing technologies and robust identity management are implemented. These technologies have the power and goal of speeding up all the passenger-related procedures while improving the security and at the same time protecting the privacy of passengers, as well as the one of railway and airport personnel. The above mentioned scenario is represented in Figure 1, where the E-CORRIDOR framework and the technologies available therein, tailored for and deployed in the AT pilot (as discussed in detail in Sections 3 and 4), have the potential to successfully realize the above depicted multi-modal transportation scenario.

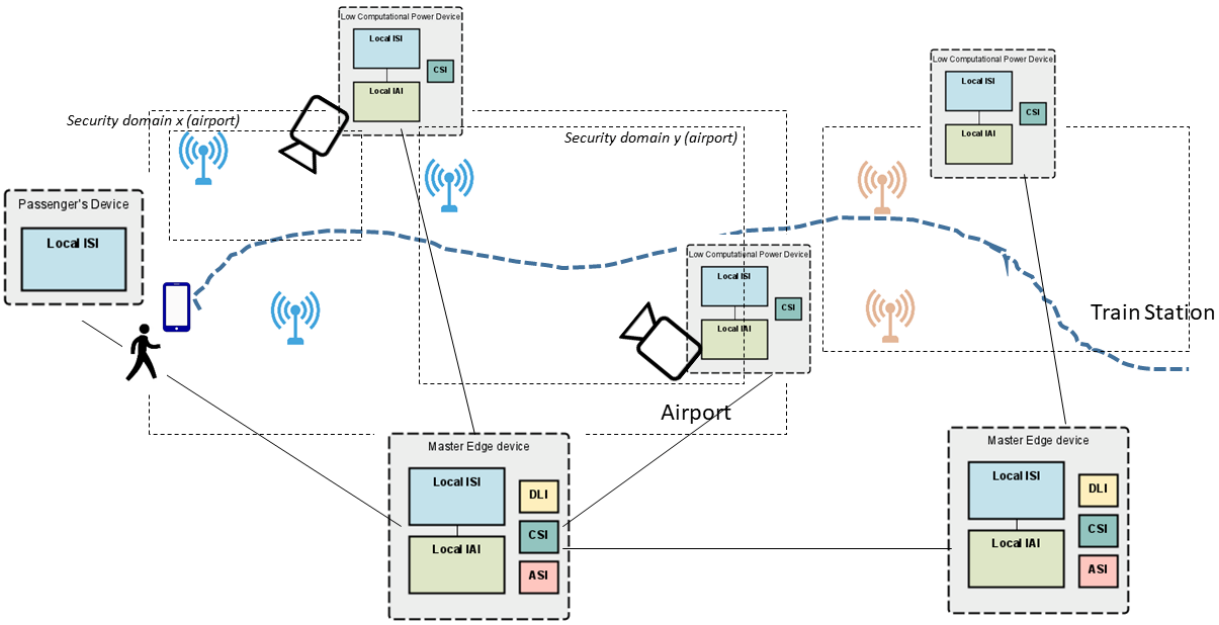

Figure 1. Overview of the AT pilot architecture for a multi modal journey

Currently, respecting the privacy of passengers and transport operators, a deluge of data about operations and service access are collected at several touch points by the different stakeholders involved in the above depicted scenario. Unfortunately, it is not possible to take full advantage

of the information contained in such data due to the presence of isolated systems and data silos owned by each stakeholder.
Improved data exchange and processing are often considered as key drivers to deliver the most long-term economic value in the considered scenario. Indeed, better decisions require access to and analysis of the relevant information in a timely manner. By exploiting all the available information, it is possible to achieve a global optimization for processes, and improve situational awareness and compliance to standards and regulations. A pivotal role is covered by the data sharing infrastructure that must be capable of properly supporting disparate sources of data, and their privacy, access and control issues concerning many of the collected data.

Based on the above described scenario, this document details the specifications of the pilot architecture including the components that will be used to implement the different use cases introduced in deliverable D2.1.

2.3 Recall of the pilot technical goals

All in all, the above technical goals are considered in the AT pilot:

- Goal 1: achieve a frictionless passenger experience by improving the current scenario where long waiting lines, discontinued travel flow, manual and tedious procedures, or slow response to/understanding of the passenger needs are all factors potentially frustrating the passenger.
- Goal 2: enhance the quality of the assistance provided to the PRM passengers whose needs require the adoption of appropriate policies and the enabling of different services to ensure a non-discriminatory treatment and offer them better support.
- Goal 3: enable privacy-preserving, continuous and context-aware authentication of passengers by exploiting multi-biometric sensors deployed in the different touch points and exploiting multi-factor solutions.
- Goal 4: improve operations management through collaborative and privacy-aware data analytics able to exploit sensors deployed in systems owned by different stakeholders.
- Goal 5: provide multi-domain services and location-aware services respectful of the passenger privacy and able to accommodate individual preferences.
- Goal 6: ensure security in the multi-transportation processes by adopting robust authentication procedures, and sharing and collecting threat and vulnerability alerts. The latter also by exploiting the capabilities of the Multi-Modal Transportation-Information Sharing and Analysis Center (MMT-ISAC) pilot (please see D4.2).

3 System Architecture

Figure 2 shows the component diagram for the instantiation of the E-CORRIDOR framework in the AT pilot. Pilot stakeholders, introduced in D2.1 and recalled in Section 2, constitute the data *prosumer* (producer and consumer) of the framework.

In the airport and train station premises, several environmental sensors are available e.g., RFID reader, camera, Bluetooth (BLE) beacons, luminosity sensors and Lidars (light detection and ranging). Those devices produce data collected while passengers access the transportation infrastructures and use the related services during their multi-modal journey. Sensors can directly pour data in the Information Sharing Infrastructure (ISI) or may need a connector in case the data are first processed by services hosted in the train station and airport and external to the E-CORRIDOR project (e.g., a self-service kiosk may read the RFID data embedded in the e-passport). Moreover, the framework can leverage the passengers' sensors available in their own smartphone and wearable devices to collect and analyze data (e.g., gyroscopes and accelerometers). In any case the appropriate Data Manipulation Operations (DMO) available in the DMO toolbox will perform the necessary initial (pseudo-) anonymization and encryption operations before storing the data in a Data Bundle.

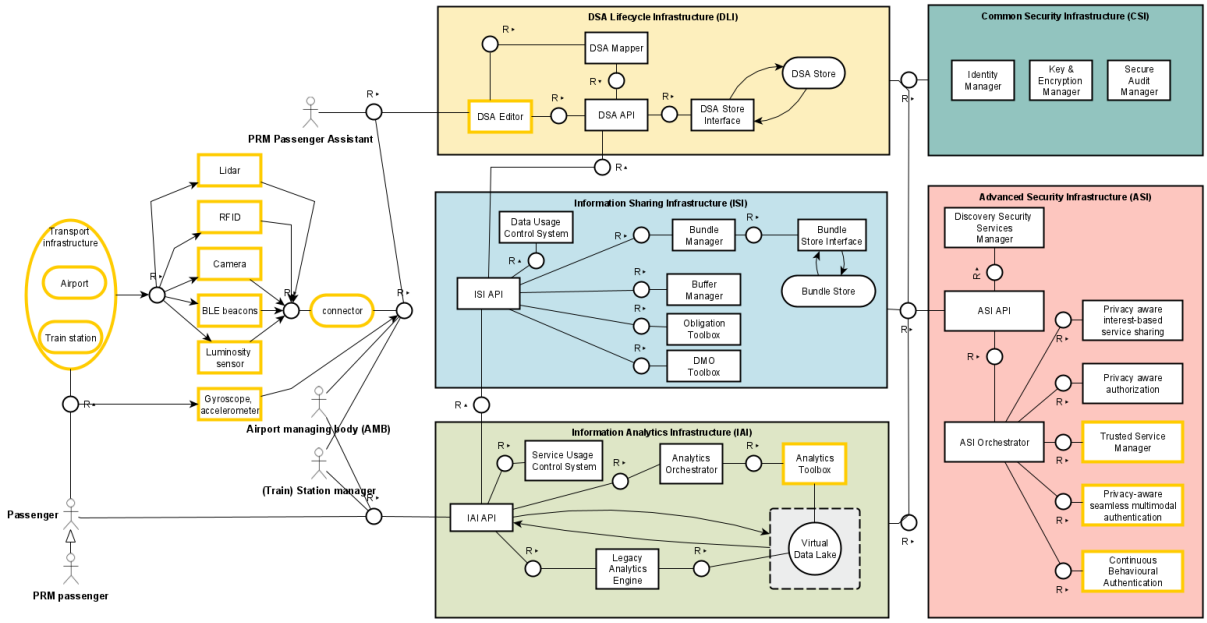

Figure 2. Architecture of the E-CORRIDOR framework instantiated in the AT pilot

Several analytics available in the Information Analysis Infrastructure (IAI) are exploited by the AT pilot to perform passenger identification and monitoring, and cyber-security services. The Analytics toolbox module of the E-CORRIDOR framework has been expanded in the Figure 3, to highlight the data analytics components exploited in the AT pilot related to the passenger (i.e., contextual, gait-based, localization, face and activity recognition analysis) and to the transportation infrastructure (i.e., intrusion detection system).

The AT pilot also exploits the features available in the Advanced Security Infrastructure (ASI) subsystem of the E-CORRIDOR framework. In this case, seamless multi-modal and federated authentication components, and the trusted identity management are considered.

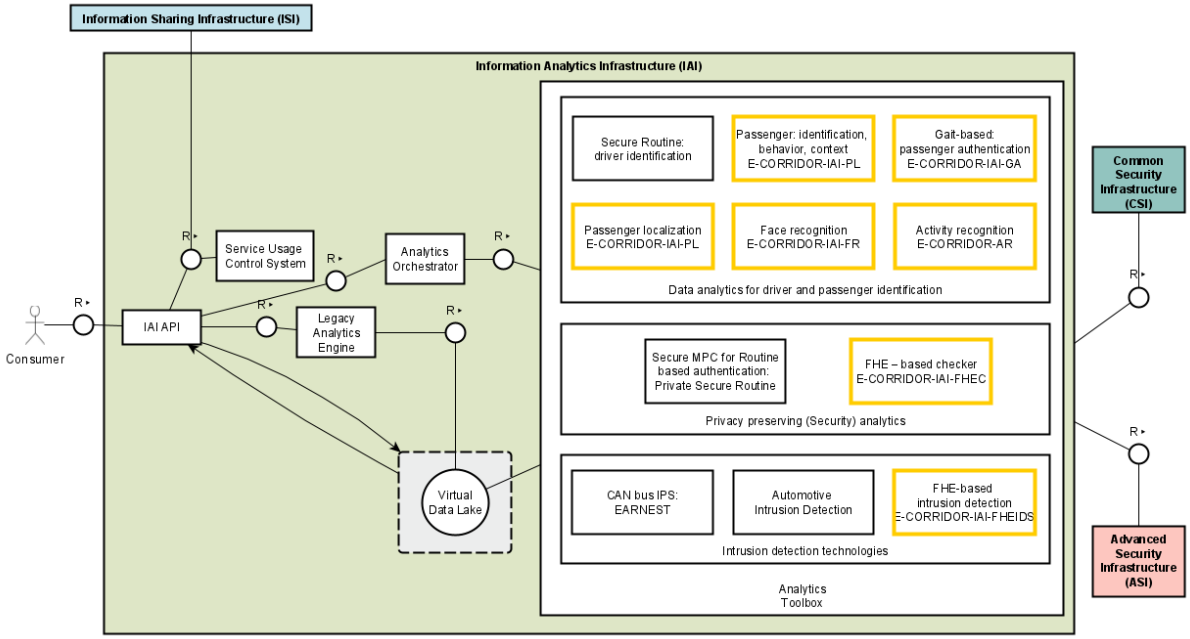

Figure 3. Architecture of the IAI subsystem of the E-CORRIDOR framework as instantiated in the AT pilot, with a focus on the components of the Analytics Toolbox (blocks marked in orange represents the analytics actually used by the Pilot).

Goals and the overall functioning of the data analytics components and advanced security services adopted in the AT pilot are briefly recalled respectively in Section 3.2 and 3.3, whereas their use in the pilot is discussed in Section 4.1. A more detailed description of the analytics and security components available in the IAI and ASI are available in D7.1 (“Data Analytics techniques requirements and architecture”) and D8.1 (“Advanced Security Services requirements and architecture”).

In both Figure 2 and Figure 3, components adopted by the AT pilot or used by its stakeholder are highlighted in orange. For a detailed description of the E-CORRIDOR framework please refer to D5.2 (“First version of the E-CORRIDOR Architecture”), whereas for the IAI and ISI subsystems details are in D6.1 (“Sharing and Analytics Infrastructures and architecture”).

3.1 Data Sharing

To reach an effective multi-modal transportation the establishment of a collaborative environment covers a pivotal role. Such an environment must subsume the presence of a data sharing able to take into account privacy, ownership and controlled access.

In the AT pilot, a plethora of sensitive and personal data are treated such as person identification and biometrics. Transportation entities have a general consensus about the high potential in exploiting such information for providing novel services to the passenger, improve travel experience and operations in airport and train station. Neverhteless, the current practice foresees the presence of many data silos hindering any global optimization. The main roadblocks are constituted by the need of keeping data ownership, control the access to such data and guarantee the privacy to the sensitive information. The solutions adopted in the AT pilot architecture and proposed by the E-CORRIDOR core framework (in particular by the ISI subsystems) are able to cope with the above mentioned requirements. Data Sharing Agreements (DSAs) associated with each piece of data shared in the ISI are able to regulate and enforce access and usage by the consumer, according to the requirements expressed by the data producer. According to the

AT pilot scenario the attributes of subject, context and data that can be used in the specification of the DSA authorization, prohibition and obligation rules are reported in Table 1.

Table 1 List of DSA attributes by category for the AT pilot (as identified at the time of writing this deliverable)

Subject	Context	Data
Role	Environmental state	Producer entity
Organization	Number of people in the environment	Producer appliance
Business sector (e.g., airport, train station)	Emergency state	Producer appliance owner
Nationality	E-CORRIDOR framework integrity	Producer physical position
Physical position		Type
		Validity

Especially while dealing with personal information, data protection directives (e.g., the General Data Protection Regulation, GDPR) enforced by the national authorities (such as the CNIL in France) must be respected. The main GDPR principles [4] are: (i) lawfulness, fairness and transparency; (ii) purpose limitation; (iii) data minimization; (iv) accuracy; (v) storage limitation; (vi) integrity and confidentiality; (vii) accountability. In the following, we discuss how the adopted solutions are able to support the compliance of the AT pilot architecture with the GPDR only from a technological point of view and without demanding completeness. An exhaustive discussion of the processes which need to be adopted by the stakeholders involved in the AT pilot is out of the scope of this document and of the project.

The transparency principle requires that the passengers are aware of the reason for the data collection and of the way their data are managed. DSA are specified with a controlled natural language. It is constituted by a restricted simplified English that can be automatically processed but also understood by people. The AT pilot considers a scenario in which the passenger reads and accepts the DSA enforced on her data collected.

The different analytics adopted in the pilot have different goals and source of data. In line with the GDPR principle of purpose limitation and data minimization, sensor data could require the execution of Data Manipulation Operations (DMOs) before being stored in the ISI and processed by the IAI. For instance, if the environmental cameras are only used for monitoring the passengers, there is no need to collect also their face. In such a case, the ISI will perform the face redaction DMO over the received video stream before running the required analytics in the IAI.

Through the DSA obligations it is also possible to define and enforce data retention policies to comply with the principles of storage limitation. Moreover, the subject that has produced the data retains their control and can therefore request their cancellation to the ISI.

DSA prohibition and authorization along with the data encryption in the “data bundle” and the anonymization via DMOs ensure the respect of integrity and confidentiality.

The Common Security Infrastructure (CSI) subsystem of the E-CORRIDOR framework include a logbook tracing all the operations performed on the shared data that can be used for accountability purposes.

The ISI subsystems of the E-CORRIDOR core framework is discussed in detail in D6.1.

3.2 Data Analytics

As highlighted in Figure 3, to fulfil the requirements of the AT pilot, several analytics available in the IAI of the E-CORRIDOR framework needs to be exploited. Here we briefly summarize the analytics deployed in the AT pilot:

1. Passenger location and flow optimization (E-CORRIDOR-IAI-PL): it performs Bluetooth-based indoor-localization, with the purpose of providing navigation to passengers, and enhanced service infrastructure (e.g., flow optimization, and contextual information sharing). Also, the results of this analysis can be exploited by other components performing behavioral and seamless authentication.
2. Passenger: identification, behavior, context (E-CORRIDOR-IAI-PBI): from the feeds collected by the cameras deployed in the transportation infrastructures, it is possible to perform passenger identification, behavioral and contextual analysis. This would be useful to identify any unexpected behavior to increase safety and security of the infrastructure other than supporting a robust touchless authentication.
3. Gait analysis – passenger authentication (E-CORRIDOR-IAI-GA): wearable and smartphone devices can unobtrusively collect biometric data referring to the user behavior. In particular, gyroscope and accelerometer sensors can constitute a source of information for building a gait model of the user useful for authentication purpose in a Bring-Your-Own-Device (BYOD) approach.
4. Face recognition – passenger authentication (E-CORRIDOR-IAI-FR): face recognition is a widely adopted approach for biometric authentication whose use has been largely accepted by the users for personal devices and, more recently, even for self-service applications (e.g., kiosks). It can be used as the sole authentication system (e.g., by matching the captured face with the picture contained in identification documents) or in conjunction with other approaches.
5. Activity recognition – passenger authentication (E-CORRIDOR-IAI-AR): activity recognition is able to identify the performed movements with the goal of obtaining contextual information. The latter can be used to enhance biometric-based authentication. Models can be built through a skeletal representation of the human body from data collected from different sensors (e.g., wearable, cameras), and the identification of the joints and their movements over time.
6. FHE-based checker (E-CORRIDOR-IAI-FHEC): a source-to-source (S2S) compiler is used to apply homomorphic cryptographic techniques and perform privacy-preserving calculations. Thanks to this component, analysis over sensitive data can be performed on their encrypted version. Therefore private search, data retrieval and condition check can be performed without posing any risk related to the exposure of sensitive data in clear.

7. FHE-based intrusion detection (E-CORRIDOR-IAI-FHEIDS): any modern transportation infrastructure is constituted by a cyber-part. Email messages can constitute spam and contacted IP addresses corresponding to malicious actors. Both pose high risk for the cyber-security. The structure of the internal network is an asset that needs to be kept confidential. Similarly, emails are sensitive data. The fully homomorphic encryption intrusion detection system is able to identify the presence of blacklisted IP addresses and check for the presence of spam messages without affecting the confidentiality of this information.

3.3 Advanced Security Services

In the AT pilot, advanced security services will serve three main purposes: multi-factor and multi-biometrics authentication, multi-modal authentication and secure identity management through trusted service manager (please see the ASI subsystem in Figure 2):

1. Multi-biometric and multi-factor authentication: thanks to a sensor fusion approach, the information produced by several sources (biometric sensors and analytics) are optimally combined to provide an improved and more robust authentication mechanisms with respect to other simpler mechanisms such as hardware tokens, passwords or single biometric systems.
2. Context reasoning: the main goal of this component is to check the consistency of the predictions used by the advanced security components, e.g., by the multi-biometric passenger authentication. Since the predictions provided by the analytic components could include inaccuracies, the component can provide confidence on the performed evaluation and avoid decision errors while delivering services to the users.
3. Federated authentication: single sign-on service can be provided in presence of bi-lateral and multi-lateral agreements among security domains (e.g., different transportation domains) belonging to the same Circle of Trust. Through the adoption of standard protocols (e.g., SAML) and the EU eIDAS, a pan-European identity management can be achieved.
4. Trusted Identity Provider: by adopting roots-of-trusts (RoTs), identities can be managed in a secure way. It provides cryptographic keys for higher-level identity management or authentication systems, e.g., in case of entities adopting a token-based authentication.

4 Component Adoption and Architecture

To fulfil the AT pilot requirements expressed in D2.1, several components (mentioned in the previous Sections 3.2 and 3.3) available in the IAI analytics framework and ASI have been adopted and tailored for the characteristics of the pilot. In this section, the application of the components in the AT pilot is first considered, then the functioning of the same is highlighted with respect to a few block diagrams representing the pilot use cases.

In accordance with the other project deliverables, the following naming convention is adopted:

1. AT-AF-x and AT-SF-x identify analytics and security functions as used in the AT pilot (please refer respectively to D7.1 and D8.1 for a detailed description of the components).
2. AT-BD-x refers to block diagrams presenting at high level subsystems and components of the E-CORRIDOR framework involved in the AT pilot use cases (UCs).
3. AT-DSA-x refers to a policy associated to the block diagram to exemplify the rules governing the data sharing in such a scenario.

4.1 Component Design

Analytics and security services components, listed respectively in Sections 3.2 and 3.3, tailored for the AT pilot and applied in the overarching pilot scenario operates as discussed in the following.

4.1.1 AT-AF-01: Passenger Localization and Flow Optimization (E-CORRIDOR-IAI-PL)

In the AT pilot, Bluetooth Low Energy (BLE) beacons can be deployed in the airport and train station premises to provide indoor localization services. BLE devices are low power and affordable, and are already available in many smartphone and wearable devices. Thanks to the low range of the BLE signals, the interferences are reduced and it is possible to localize the passengers with a good accuracy for the pilot's applications.

To localize the passengers, the components will work in two ways (see Figure 4). In the first, the BLE beacons deployed in the AT pilot will collect the Receiver Signal Strength (RSS) of the signals transmitted by the passengers' devices and infer position and number of the passengers while the flow of people moves in the terminals. In the second, the BLE beacons will transmit their positions codified through the Eddystone protocol [5]. In the first scenario, the E-CORRIDOR framework deployed on the passenger's device will only need the ISI. Whereas in the second, also the IAI will be required to perform an inference of the position at the edge.

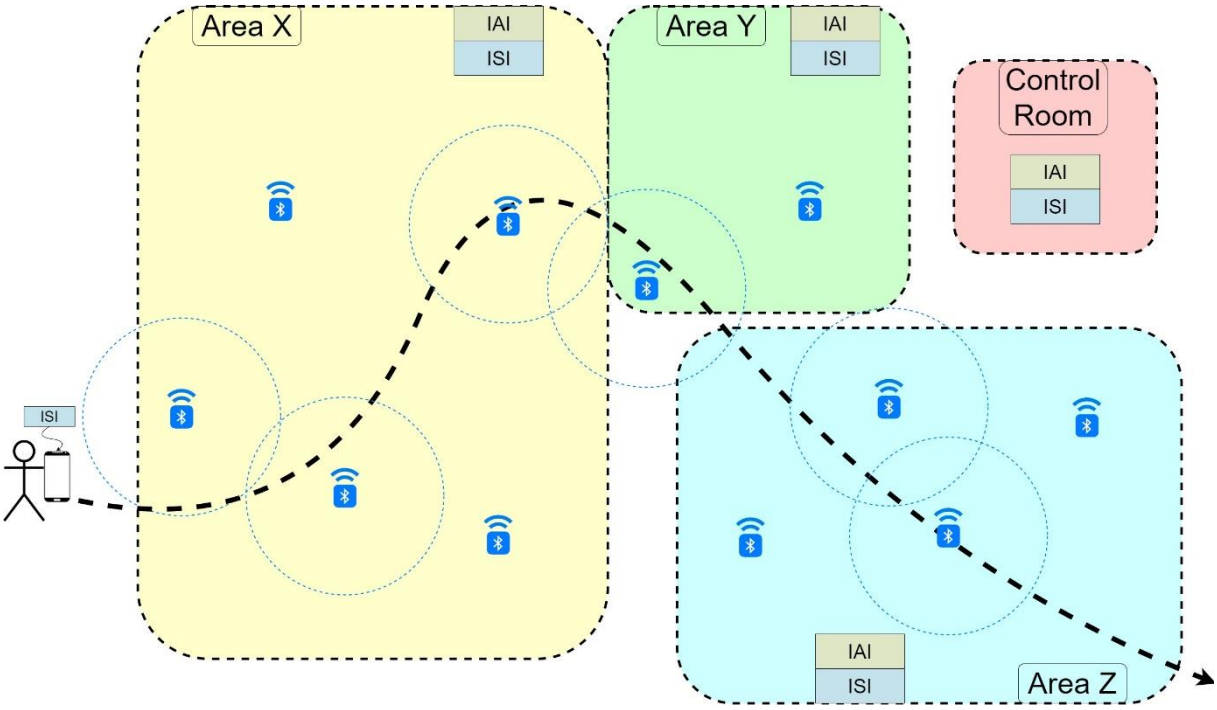

Figure 4 Adoption of the E-CORRIDOR-IAI-PL in the AT pilot

Through the privacy-aware information sharing, the overall information on the passengers' location will be used to build a passenger flow model and optimize the services in the airports and train stations (e.g., opening an additional service desk).

4.1.2 AT-AF-02: Passenger Identification, Behavior and Contextual Analysis (E-CORRIDOR-IAI-PBI)

Cameras are installed in airports and train stations for monitoring the passengers for security and safety reasons. Through a continuous and automatic monitoring of the environment the E-CORRIDOR-IAI-PBI component can perform: (i) passengers identification, (ii) characterize their behavior, and (iii) contextual analysis. This information can be exploited for authentication and to provide novel services.

People moving together in the airports may belong to the same group or family and have a unique Passenger Name Record (PNR) linked to the same reservation. This characteristic behavioral information may be exploited during the authentication but for instance also to deliver additional services specified at reservation time (e.g., to get a luggage cart).

The context is represented by the passenger's baggage and position in the terminal. The baggage can indeed be linked with the identified passenger and transmitted throughout the different touch points of the passenger journey. Her position in the terminal can instead be exploited with respect to the terminal topology and the position of the cameras (see Figure 5) to identify any security and safety issues, e.g., passengers dwelling in front of a self-service kiosk could reveal some problems in using the machine.

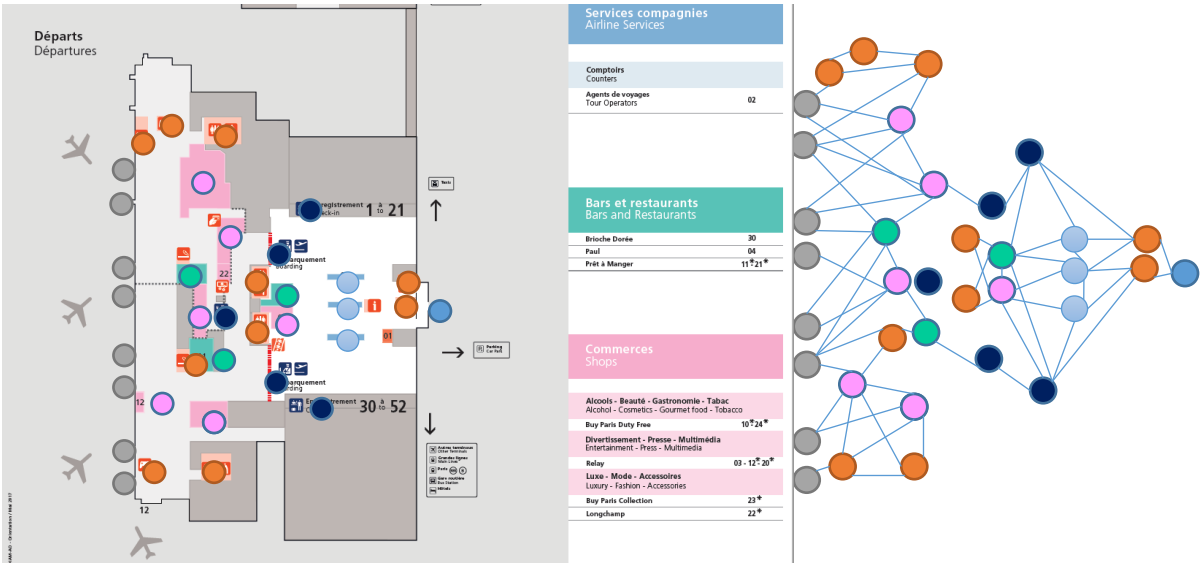

Figure 5 The plan of an airport terminal (on the left) and an exemplified deployment of the cameras (on the right) to support the re-identification performed by the E-CORRIDOR-IAI-PBI

4.1.3 AT-AF-03: Passenger Authentication through Gait Analysis (E-CORRIDOR-IAI-GA)

Through a Bring Your Own Device (BYOD), passengers can use their own smartphones and wearable devices, and the sensors available on the same as an additional source of biometric data. A seamless authentication can be performed by analyzing the walking pattern of the person and building a gait model.

In the AT-pilot scenario, passengers running an instance of the E-CORRIDOR framework on their devices, by accepting a DSA, can choose to be enrolled in the gait-based authentication, e.g., while booking the flight. Features of the passenger gait will be stored in the ISI. Then at the arrival at the train station or airport terminal, the passenger is encouraged to go in a "smart tunnel" that basically collects new biometric data from the passengers walking through pre-defined paths. The authentication is performed by comparing the gait characteristics collected during the enrolment and the ones in the smart tunnel (see Figure 6).

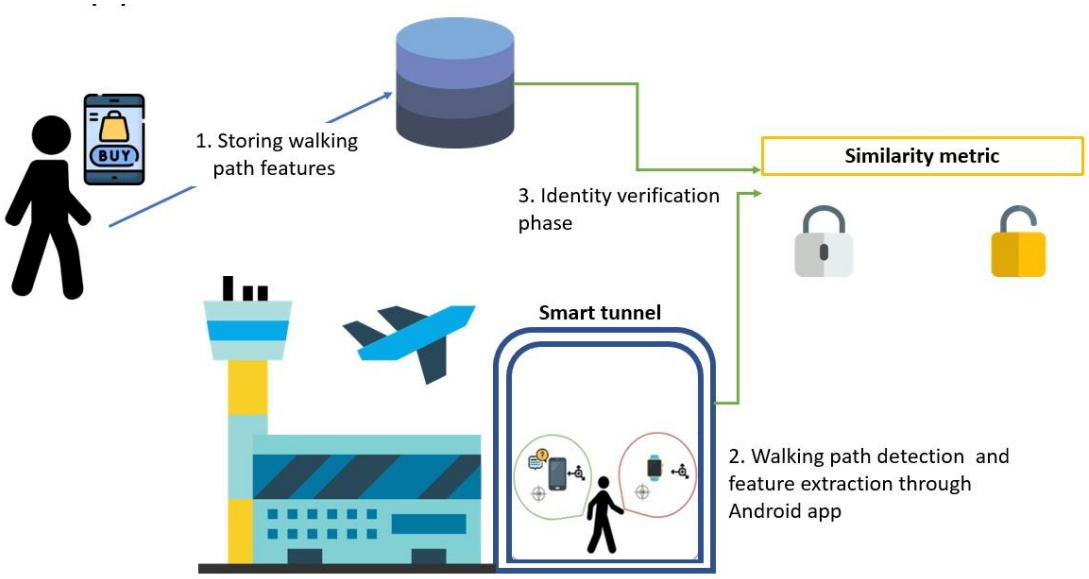

Figure 6 E-CORRIDOR-IAI-GA for gait-based authentication in the AT pilot

4.1.4 AT-AF-04: Face Recognition – Passenger authentication (E-CORRIDOR-IAI-FR)

In the AT pilot, the face recognition component is designed for verifying if the face of a passenger detected in the current touch point is similar (i.e., has at least a x% of similarity) to the photos of the face of the same passenger captured in previous touch points of the passenger journey. In light of the privacy restrictions, the component does not link the passenger face with any other personal information of the passenger such as name and ticket number. To further guarantee the privacy for the passenger data, the face recognition takes as input only the template of the previous detection (and not the actual photo), compares the latter with the current photo and provides a matching score. The updated model and the associated score are propagated to the next touch points through the ISI, and then the local memory is emptied by following a pre-specified DSA (e.g., once the passenger reaches the subsequent transportation domain).

A set smart video cameras installed in the airport and train station touch points are in charge of collecting and mapping facial features (e.g., described with the Histogram of Oriented Gradients (HOG)). The default configuration encompasses the presence of a single camera but it can be extended to combine information coming from multiple cameras. The component is designed to work at the edge (therefore the passenger photos are never transferred to the cloud for processing), according to four main steps: (i) capturing, (ii) extracting, (iii) comparing, and (iv) matching, explained in more detail in D7.1. The face recognition component learns new faces incrementally with three main phases: (i) collecting a face data at the first touch point, (ii) training the face recognition model using the collected face data, and (iii) updating the model at the next touch point.

4.1.5 AT-AF-05: Activity Recognition for passenger authentication (E-CORRIDOR-IAI-AR)

The human activity recognition component aims at determining and naming activities using streams of data collected from vision sensors, such as cameras and/or Lidars. The component exploits a deep learning method for modeling sequences of human activities performed in a three-dimensional space. Standard Recurrent Neural Networks (RNNs) and Long Short-term

Memory Networks (LSTMs) classifiers are adopted. The combination of RNN with LSTM is proposed to model also long-term sequences of actions. The entire body's motion is modeled as interconnected parts. Indeed, in human actions joints in the body move in groups, and each group is mapped to a significant part of the body. The activity recognition module provide in output the activity performed (with higher probability) by the passenger. Such an information will be taken in input and exploited by the multi-biometric passenger authentication component.

4.1.6 AT-AF-06: OpenAPI for Fully Homomorphic Encryption (E-CORRIDOR-IAI-FHEC) on Sensitive Passenger Data

There are a lot of high sensitive data related to the passenger personal information (including biometrics) that are treated in the AT pilot scenario. The OpenAPI for Fully Homomorphic encryption provided by the E-CORRIDOR-IAI-FHEC allows the data scrambling in order to protect data confidentiality and perform privacy-preserving computations.
All in all the component is able to perform computation on encrypted data without the need of decrypting them in untrusted environments. In the AT pilot, the component can be used to support other components and different services, e.g., to check the passenger reservations or localize the touch point at which the passenger is located.

4.1.7 AT-AF-07: Full Homomorphic Encryption-based Network Intrusion Detection (E-CORRIDOR-IAI-FHEIDS)

Transportation entities largely adopt cyber-networks and systems in their operations. This opens up for the possibility of cyber threats e.g., due to malware or spam messages. While for some security analysis the AT pilot can rely on the functionalities of the MMT-ISAC, some sensitive information such as data on the structure of the cyber-infrastructure and the content of the email messages cannot be sent for external processing and analysis.
To preserve the data confidentiality, the E-CORRIDOR-IAI-FHEIDS provides IPv4 blacklisting functionalities and email spam filtering in a privacy-preserving fashion. Indeed, the fully homomorphic encryption is able to perform such checks to protect the network environment from intrusion in a privacy-aware manner.

4.1.8 AT-SF-01: Multi-Biometric and Multi-Factor Authentication

The multi-biometric and multi-factor authentication (MFA) component exploits the information from different environmental sensors available in the AT pilot and generated by the biometric-based analytics through a sensor fusion approach. By combining biometrics, contextual, behavioral and location information it is possible to improve robustness and security of the current authentication methods adopted in the transportation domain based on a single biometric or on a basic token (e.g., the bar-code available on the ticket).
Several biometric-based analytics are adopted in the AT pilot, and this component will leverage on these analytics (such as computer vision platform based on deep learning and multi-camera, a Bluetooth-based localization and gait analysis from sensors available in the user’s smartphone) to perform the passenger authentication. Other sensors and data sources (like the RFID data contained in the electronic passport) could be also included in the data fusion to provide one a stronger authentication mechanism.

4.1.9 AT-SF-02: Context reasoning

The context reasoning component is used for deducing higher-level context information by aggregating different sensors data together with the output of the predictive components. In the airport and train station the context includes environmental information of the touch point itself such as luminosity of the area and number of people waiting in the queues for baggage drop, registration kiosks or security screening. On the other hand, the context concerns the passenger as individuals and defined as any information that can be used to characterize the "state" of the passenger. The main objective of the reasoning component is to check the consistency of the predictions when they are used by the advanced security components (for instance the multi-biometric passenger authentication). Indeed, information inferred by data analytics components could include inaccuracies potentially leading to decision errors. The context reasoning component exploits a ground truth (composed of a set of rules describing relations and constraints of the passenger context attributes) to detect context inconsistency. These (probabilistic) rules are executed by an Answer Set Programming (ASP) reasoning engine. The ASP is a rule-based logic programming paradigm used to represent knowledge and solve combinatorial (NP-hard) problems where there is no optimal solution to reduce the solution space.

4.1.10 AT-SF-03: Federated Authentication Based on eIDAS

To ensure a seamless and a frictionless experience for passengers in the multimodal transportation scenario, a "continuous and token-based" authentication needs to be applied. Each transport entity collects over time passenger information to build a behavioral fingerprint (i.e., a token) used for the authentication in the local services. While progressing in her journey, approaching a new security domain or changing mode of transport, the passenger's token can be exchanged among stakeholders through the E-CORRIDOR framework. In such a way the passenger can be kept continuously authenticated with the transportation environment.
The AT pilot adopts standard and widely used protocols (such as SAML) and the EU eIDAS to achieve a pan-European identity management in multi-modal journeys. The sequence diagram presented in Figure 7 reproduces the interaction among different security domains (e.g., train station and airport) while adopting the eIDAS protocol for authentication. A passenger already authenticated in the security domain A (Service A, in the figure), can be re-authenticated and access to services in the second security domain (Service Provider in Service B, perhaps belonging to a different EU member state) thanks to requests following the EU identification system.

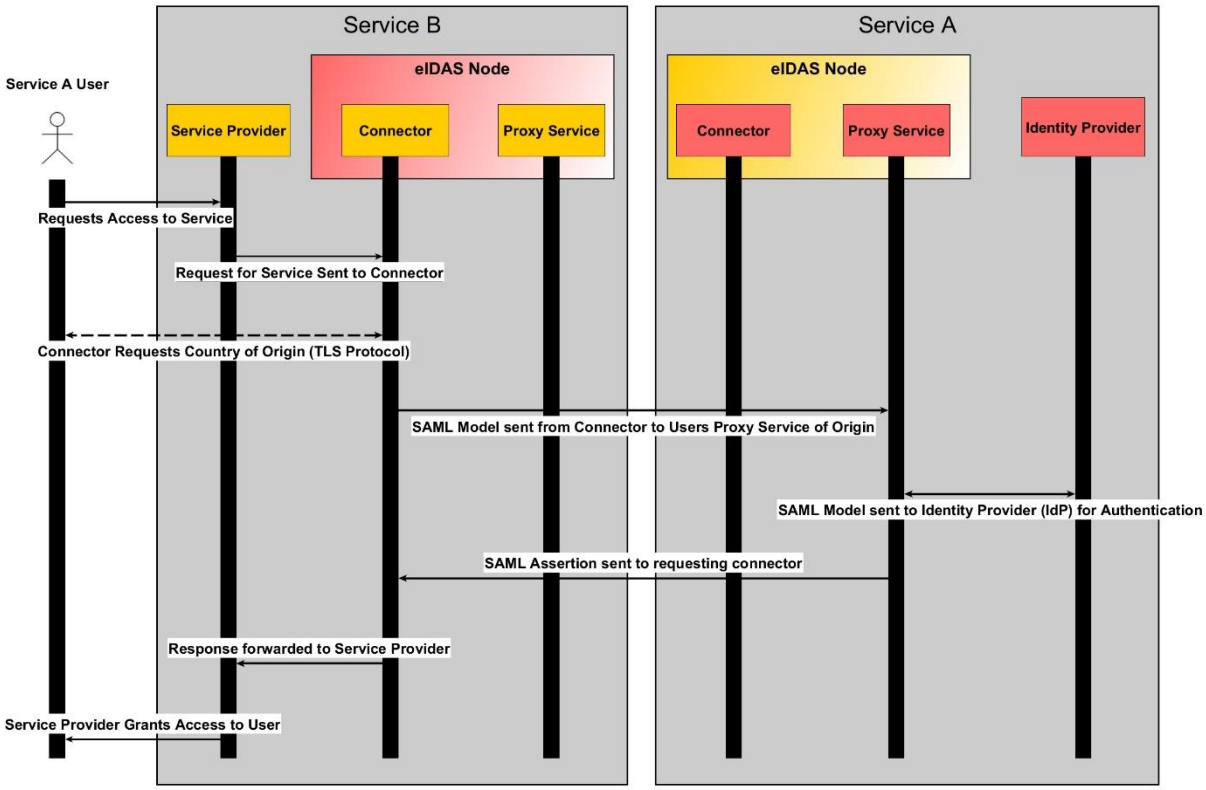

Figure 7 Sequence diagram of the eIDAS adoption for a pan-European authentication

4.1.11 AT-SF-04: Trusted Service Manager

Figure 8 shows the instantiation of the Trusted Services Manager (TSM) component for the AT Pilot. It is deployed as part of the ASI as an edge layer of the sensor platform that connects multiple environmental sensors, e.g., cameras, used for continuous authentication at the airport. It introduces a hardware-based isolation layer rooted from a Trusted Platform Module (TPM) into the platform that is used as shielded location to generate and use cryptographic keys and store them with other security-sensitive data, like integrity measurement values. Moreover, it is used to bootstrap a trustworthy system.

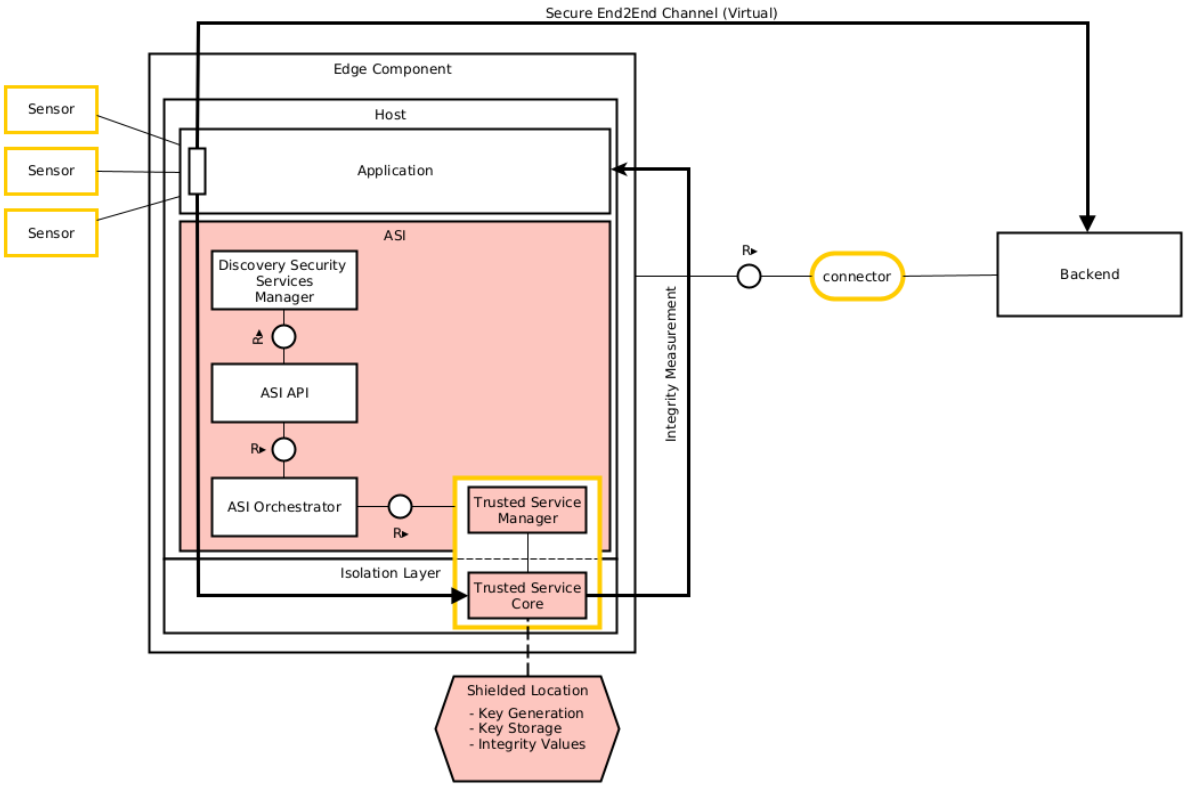

Figure 8 Trusted Service Manager Instantiation

From a higher level, the TSM enables the secure (re-)provisioning, distribution, and storage of credentials, e.g., in form of cryptographic keys, to establish secure channels among the entities exchanging sensor information and allows to verify the system state of the components to build strong trusted relationships across the entities.

4.2 Component in Action

This section describes how the stakeholders interact with the AT pilot architecture. A special attention is devoted to the interactions with the E-CORRIDOR core framework, the data analytics components and the advanced security services, adopted by the pilot and mentioned in the previous Section 4.1. As one of the key feature of the E-CORRIDOR lies on the privacy-aware capabilities and on the controlled data sharing, for each scenario an exemplifying Data Sharing Agreement (DSA) is reported.

All in all, to achieve the use cases presented in D2.1 (“Requirements for the AT Pilot”), the AT pilot stakeholders (i.e., passengers, airport and train station operators and services) exploit the E-CORRIDOR framework deployed in the pilot. In the following, for ease of discussion, the use cases are grouped in four sets according to their contribution to the pilot goals (see Table 2).

In the discussion below, we assume that the use cases follow the normal flow of the events where the capabilities of the E-CORRIDOR are exploited. Indeed, the alternative flows generally consider reverting to manual procedures in case of problems, low confidence on the analytics results or lack of sensor coverage (see D2.1).

Table 2 Block diagrams and corresponding use cases for the AT pilot

AT-BD-01	PRM Passenger Assistance	✓					✓							✓
AT-BD-02	Multi-Biometric Passenger Authentication and Baggage monitoring in Multi-modal travels		✓	✓	✓	✓	✓						✓	
AT-BD-03	Frictionless access to Multi-modal services						✓	✓	✓					
AT-BD-04	Controlled Data sharing for Service prediction, optimization and security									✓	✓	✓	✓	
		Must	Must	Must	Should	Must	Must	Could	Could	Must	Could	Could	Should	Could
		AT-UC-01: PRM Passenger Assistance and Authorization	AT-UC-02: Passenger and Baggage Contextual Identification	AT-UC-03: Contactless Passenger Authentication and Authorization	AT-UC-04: Privacy-preserving Passenger Monitoring	AT-UC-05: Passenger Analysis Opt-In Opt-Out	AT-UC-06: Single Sign-On Authentication	AT-UC-07: Multi-Modal Ticketing	AT-UC-08: Service Access Through Bring Your Own Device	AT-UC-09: Sharing of Service Access Data	AT-UC-10: Run Collective Security Analytics	AT-UC-11 Notification of Service Disruption	AT-UC-12 Passenger Flow Overview and Prediction	AT-UC-13 Privacy-aware Behavioral Identification	AT-UC-14 Notification on PRM Passengers' Location

4.2.1 AT-BD-01: PRM Passenger Assistance - Block diagram for AT-UC-01, AT-UC-06, AT-UC-14

Use cases AT-UC-01, AT-UC-06, and AT-UC-14, aim at describing a seamless access to the multi-modal transportation for PRM passengers by taking into account a better travel experience and an easier management of the PRM special services (requested to the airport and or train station) with respect to the current practice. As remarked in D2.1 this scenario covers an important spectrum of the demands for large transportation hubs (please see Section 1.3.1 therein) and presents room for improvement with a clear direct impact on the passenger experience. The E-CORRIDOR framework has the opportunity of enhancing the current practice thanks to its advanced authentication mechanisms, and its collaborative and privacy-aware information sharing.

At the arrival of the PRM passenger, on the E-CORRIDOR framework deployed in the AT pilot, the following steps and interactions between the stakeholders and the framework take place (please see Figure 9):

1. Camera feeds (videos and pictures) are transmitted by the environmental sensors of the infrastructure (train station or airport) to the local ISI.
2. Data manipulation operations (DMOs), such as facial redaction or features described through a Histogram of Oriented Gradients (HOG), are performed to ensure the privacy of the passenger data.
3. The PRM passenger as well the PRM assistant (still at different places of the same transportation environment) are identified at the edge thanks to the face recognition. The context reasoning, behavior and activity analytics (AT-AF-02 and AT-AF-05) are used to make the identification robust and seamless at the same time.
4. The Special Service Request (SSR) code declared at the booking time and attached to its PNR along with the passenger preferences, are retrieved from the PRM database through the ISI.
5. A notification is sent to the PRM assistant which enables the required SSR in the corresponding domain (either airport or train station).
6. Thanks to the localization capabilities (of AT-AF-02 and AT-AT-01) of the E-CORRIDOR framework the position of the passenger is inferred with (various degree of) accuracy.
7. The PRM assistant can access to the position of the PRM passenger through the ISI and easily reach the passenger thanks to the indoor navigation provided by the AT-AF-01 component.
8. Assistive devices (if any) and baggage are handled by the assistant.
9. SSR code and policy are “propagated” (the information is saved in the ISI with an appropriate DSA to allow the access of those sensitive information only to the relevant personnel) even among different stakeholders
10. The assistant also helps the PRM passenger to configure and accept an appropriate DSA (from a set of predefined ones). This only in case the passenger is also willing to share its location (with a given granularity) e.g., with a relative.
11. The PRM assistant in the initial security domain (for instance at the arrival platform of the train station) can access to the information (e.g., contact and location) of the

PRM assistant in charge of handing the PRM services in the subsequent domain. Therefore the (train) PRM assistant can easily localize and reach the second PRM assistant waiting at the designated venue (e.g., the airport information point). Data among PRM assistants of different transportation entities are exchanged through the ISI according to a specified DSA.

12. The AT-AF-01 keeps inferring the passenger location throughout her own journey and save the information in the ISI.
13. The authenticated relative holding the needed attributes access to the location information according to the DSA specified before by the passenger.
14. The passenger does not need to go through the same steps again as bi- or multi-lateral agreements are in place among transportation companies and the "Federated authentication based on eIDAS" (AT-SF-03) ensures a frictionless access to the services of the next transportation domain within the EU.

In Figure 9 the interactions between the instances of the E-CORRIDOR framework deployed in the different domains is exemplified. In particular the PRM assistant in charge of the first transportation domain can localize the PRM passenger and then can also locate the assistant in the next transportation domain.

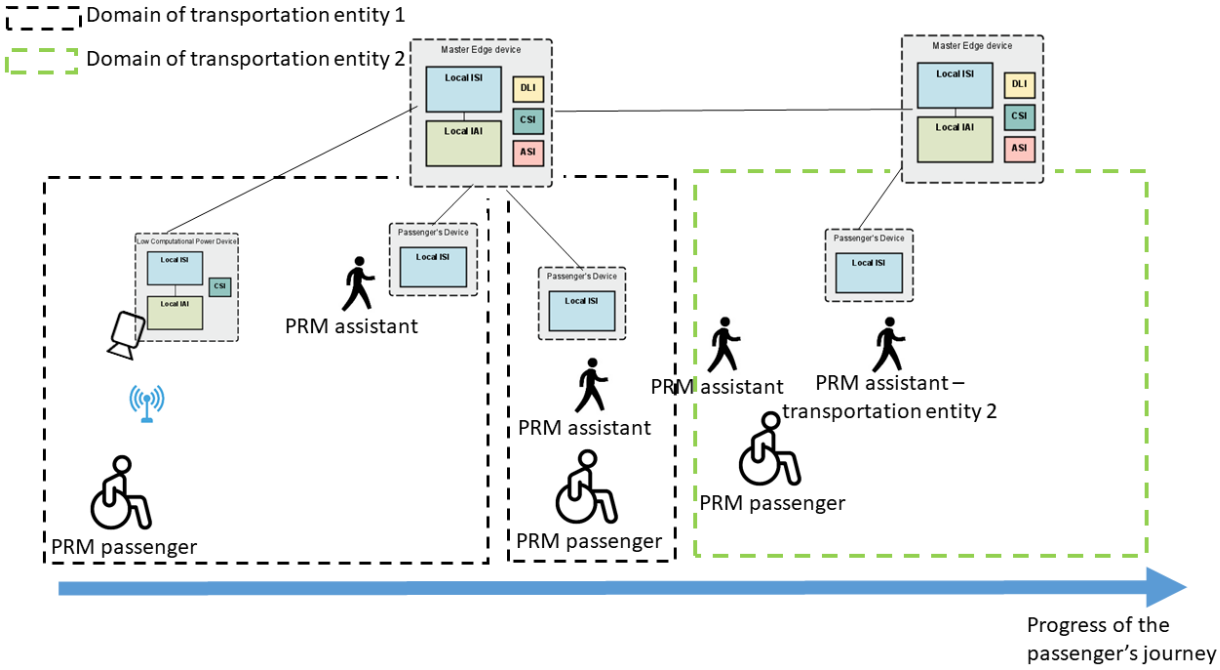

Figure 9. End to end multi-modal and privacy-aware for PRM passenger

4.2.1.1 AT-DSA-01: Data Exchange about PRM Assistants of Different Domains

The PRM assistants working at airport and train station need to cooperate to ensure a frictionless experience for the PRM passenger. In particular, their contact and location information are exchanged only for the duration of the transfer and then removed.

The corresponding authorization is expressed as:

Location and contact data of the actor having *Sector*=”train station” and *Role*=”PRM assistant” CAN be accessed by the actor having *Sector*=”airport” and *Role*=”PRM assistant”.

IF subject has (*Sector* =”Train station” AND *Role*=”PRM assistant”) it CAN access to “location data” of subject with (*Sector*=”Airport” AND *Role*=”PRM assistant”)

Similarly, for the case in which data of the PRM assistant at the airport are accessed by the one in the train station.

4.2.2 AT-BD-02: Multi-Biometric Passenger Authentication and Baggage Monitoring - Block diagram for AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-05, AT-UC-06, AT-UC-13

The use cases AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-05, AT-UC-06 and AT-UC-13 refer to the (biometric) identification and authentication solutions aiming at improving the passenger experience. This scenario is mainly focused at the exploitation of the ISI and ASI components adopted in the AT pilot architecture.
Without loss of generality, in the following, it is assumed that all the operations are performed in a single domain:

1. At the initial touch point (e.g., train departure area or airport terminal entrance), the passenger provides her travelling documents (i.e., ticket, passport, visa) to a self-service kiosk. The OCR and QR code readers extract the name of the passenger and the flight information from the ticket.
2. The kiosk and the environmental sensors collect also some biometric information of the passenger (through videos and pictures). Such information is transmitted to the local ISI and appropriate DMOs, such as facial redaction or transformation to HOG, are performed to ensure the privacy of the passenger.
3. The passenger is then enrolled in the system thanks to the ISI and ASI components. In particular with passenger localization, identification, gait analysis, and face and activity recognition (AT-AF-01, AT-AF-02, AT-AF-03, AT-AF-04 and AT-AF-05). A passenger model from multi-biometric and behavioral data is then built by the ASI components AT-SF-01 and AT-SF-02. Such a model constitutes the “token” used for multi-factor authentication and it is stored in the ISI.
4. In case of passengers travelling together with the same PNR and localized at the same touch point, the corresponding tokens are linked as well as with their belonging (e.g., baggage and assistive device).
5. The local ISI of the following touch point visited by the passenger in her journey accesses to the identification token. Environmental sensors collect new data and the above mentioned components performs privacy-preserving comparison with the model included in the token. The corresponding model can be updated and it is used to perform a robust authentication. Notably, the context reasoning component (AT-SF-02) will be in charge of evaluating the confidence of the authentication process and possibly request the rollback to manual procedures (if the confidence is below the threshold specified for the current security domain).

Sensors, analytics and security service components involved in this scenario are reported in Figure 10.

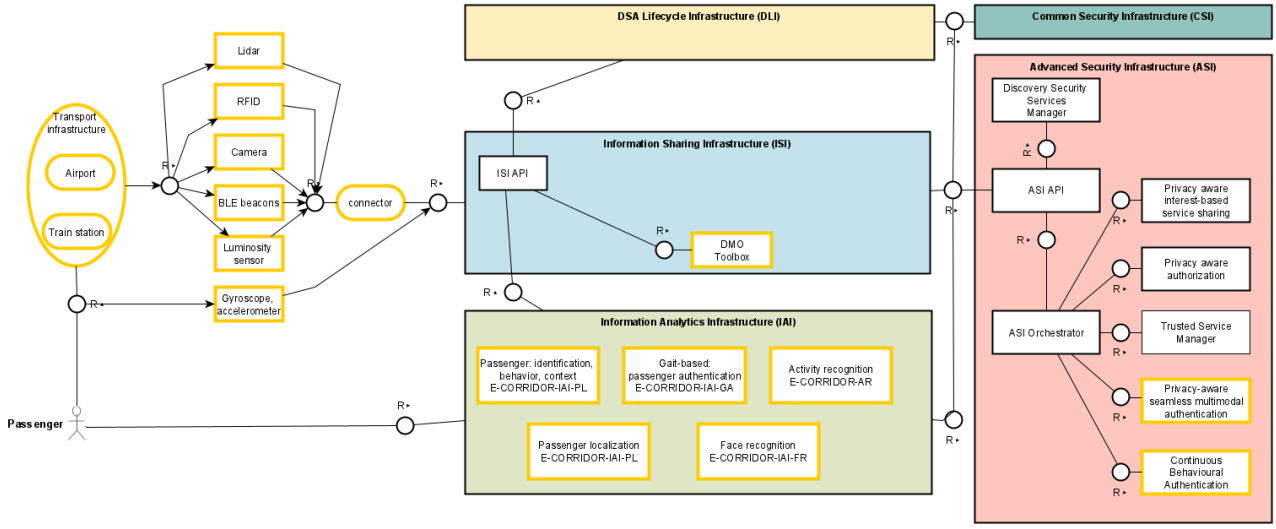

Figure 10. Multi-Biometric Passenger Authentication biometric authentication

4.2.2.1 AT-DSA-02: Anonymization and Access to Sensitive Data

In the discussed scenario, several highly sensitive data are collected. It is therefore required that appropriate DSAs regulate their anonymization and access.

Passenger data captured by the airport's device_X, need to be (pseudo-)anonymized with the function XYZ. Later on, these data can be accessed and processed only by devices located in area_Y.

This DSA is constituted by two main parts: an obligation and an authorization.

Obligation:
AFTER a data item having *Producer*=”device_X” is collected THEN the data item MUST be pseudo-anonymized with the DMO “XYZ”.
Authorization:
IF the accessing device (subject) has *PhysicalPosition*=”area_Y” it CAN access to the same data.

Then, the two parts are simply concatenated:
Obligation; authorization

4.2.3 AT-BD-03: Frictionless Access to Multi-Modal Services - Block diagram for AT-UC-05, AT-UC-06, AT-UC-07, AT-UC-08

The overarching scenario depicted in the AT pilot envisions an improved passenger experience in multi-modal journeys. Use cases AT-UC-05, AT-UC-06, AT-UC-07 and AT-UC-08 have the final goal of providing a frictionless and seamless access to all the transportation services used by the passengers in their trips. In particular, the focus is on the passengers’ preferences and on collection and use of personal data stored in a secure digital wallet (eWallet) held by the same passenger through the Bring Your Own Device (BYOD) technology.

1. The passenger is authenticated at the beginning of her journey (please refer to the previous Section 4.2.2).
2. The passenger opts for using the BYOD option therefore her personal device runs an instance of the E-CORRIDOR core framework.
3. An appropriate DSA is accepted by the user to share, in a privacy-preserving fashion, personal and biometric data with the ISI subsystem. These set of date along with personal preferences constitutes the eWallet.
4. Security domains even belonging to different transportation entities are within the same Circle of Trust (CoT) and therefore their identity and access management systems cooperate.
5. The federated domain established by the CoT (AT-SF-03) allows a continuous authentication and authorization to the passenger.
6. The passenger can request to any of the next transportation domain services personalized with the information stored in her eWallet.

In Figure 11 are represented the main stages of the scenario: (i) data collection, (ii) authentication, (iii) sharing of the authentication token within the CoT.

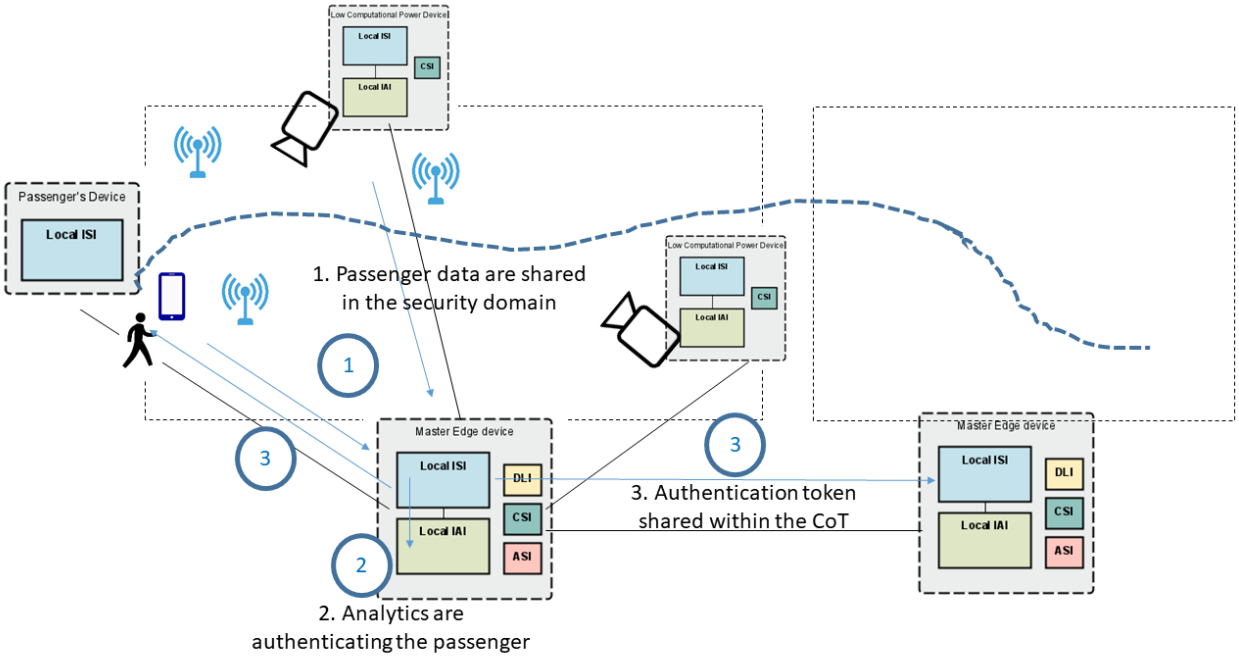

Figure 11. Frictionless Access to Multi-Modal Services Block diagram

4.2.3.1 AT-DSA-03: Sharing of Data Collected in Different Domains

In the depicted scenario it is required that while the passenger moves in different security domains, some of her data are made available to the other security domain with the aim of customizing the required services.

Data of *type*=”type_Z”, of *producer*=”Passenger_X” and produced at *physical position*=“area_W” are elaborated by the *subject*=”X” (e.g., the train station). These are later made available for access to subjects (members) of *organization*=”Y” (e.g., an airport service).

IF (*Producer* is Passenger_X AND *PhysicalPosition* is area_W AND *dataType* is type_Z) THEN *Organization* (X OR Y) CAN access to the data

4.2.4 AT-BD-04: Controlled Data Sharing for Service Prediction and Optimization and Security - Block diagram for AT-UC-09, AT-UC-10, AT-UC-11, AT-UC-12, AT-UC-13

The use cases AT-UC-09, AT-UC-10, AT-UC-11, AT-UC-12 and AT-UC-13 aim at describing a scenario in which, thanks to a collaborative and controlled data sharing environment, it is possible to overcome the current limitations in sub-optimization and features of the provided services due to the presence of data silos. The ISI subsystem of the E-CORRIDOR framework covers the dual role of privacy enforcement in the shared data (through DMOs, e.g., able to perform pseudo-anonymization) and controlled data access (through the DSAs). Collective analytics for enhanced security services and optimized operations can be achieved.

In the following, a scenario in which train station and airport improve their services thanks to the above mentioned features of the E-CORRIDOR framework is exemplified. In the same scenario, with respect to the security services, the presence of the MMT-ISAC (pilot of the E-CORRIDOR project implemented in WP4) is exploited.

1. Being airport and train station used by many travelers as connections in their journeys, the two transportation entities consider the presence of bi-lateral agreements and the establishment of a CoT.
2. Sensors and data collected at the edge in all the security domains of the two transportation environments are saved in the ISI after having been processed by the appropriate DMOs (e.g., to anonymize some records of the passenger data).
3. Appropriate DSAs are defined along the shared data in such a way that the other transportation entity can exploit the collective data but only respecting the limitation imposed by the data producer, including the list of analytics available in the toolbox of the IAI deemed trusted for operating over those data.
4. The collaborative analysis takes place, respecting the DSAs, also through a federated analytics approach (i.e., the raw data may not be shared but only the intermediate results generated by the edge analysis).
5. Analyses for a global optimization of the services can take place (service disruption, security vulnerability, passenger flow, etc.). For instance, the train station can inform the airport about a strike, a delay or an interruption for some of its trains, then the passengers arrived at the airport can be timely informed of alternative options.
6. Security alerts generated by the Security information and event management (SIEM) deployed in the transportation entities can be shared with the MMT-ISAC through the same approach.
7. The MMT-ISAC will in turn process those alerts and make such information available to other transportation entities potentially affected by the same vulnerability or threat.
8. Additionally, the MMT-ISAC will share to the interested parties, according to the specified topics of interest, any threat or vulnerability collected from public sources (in D4.2 a deeper discussion on the services provided by the MTT-ISAC is provided).

In Figure 12, the different instances of the E-CORRIDOR framework deployed on the passenger's device, transportation environments and MMT-ISAC are presented. Passenger's information is collected from personal devices and while interacting with the infrastructure (e.g., with the airport services). Transportation entities can leverage on the collaborative environment enabled by the E-CORRIDOR framework to optimize their services and operations. Security analysis and threat information sharing are performed exploiting the interaction with the MMT-ISAC.

Please refer to D4.2 for a more detailed discussion on the services provided by the MMT-ISAC.

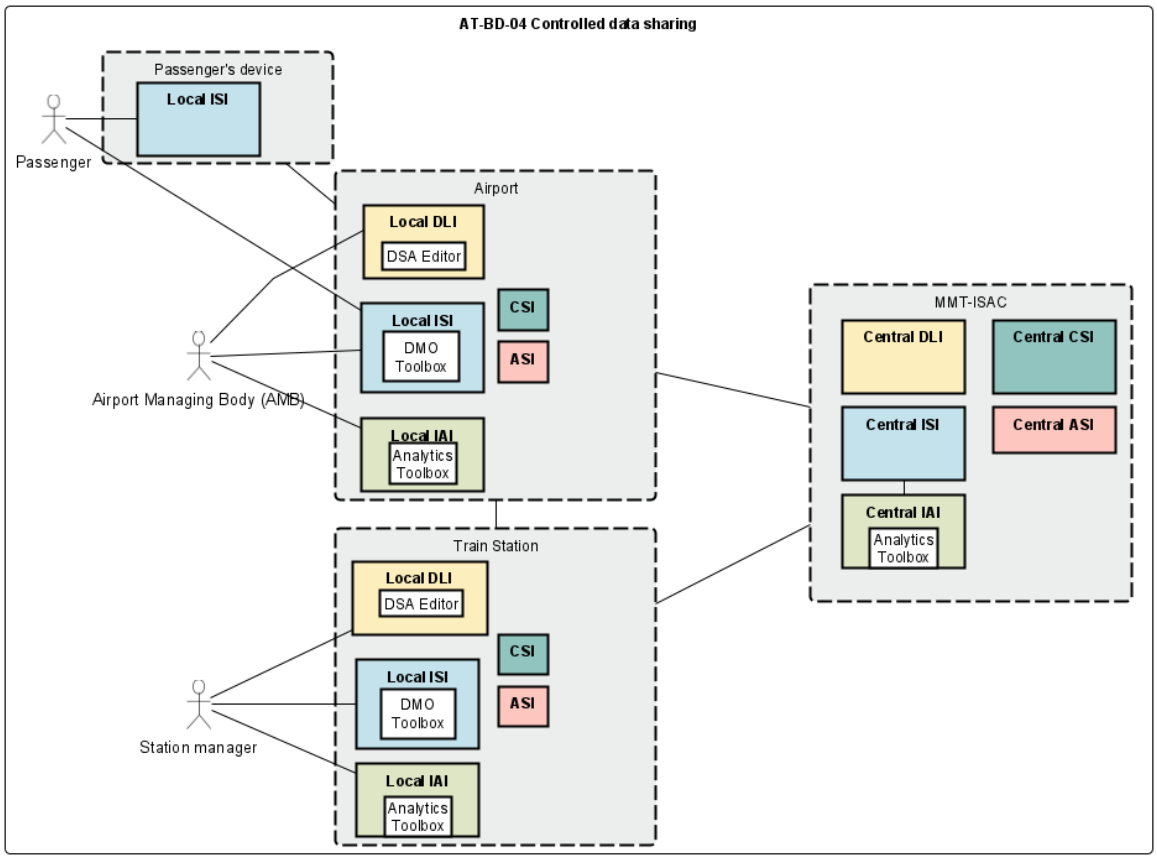

Figure 12. Controlled data sharing for Service Prediction and Optimization and Security

4.2.4.1 AT-DSA-03: Data Retention Policy on Passenger Data

To comply with the applicable regulations, some data collected by the transportation entities must be deleted after the passenger journey (if no special request is made by the authorities).

Data captured by airline_X at boarding_gate are encrypted and will be deleted after a period of Y (if no special request from relevant authorities is received).

Obligation:
AFTER a data item having (*ProducerAppliance*="boarding_gate" AND *ProducerApplianceOwner*="airline_X" is collected) THEN it MUST be encrypted.

AFTER obligation (if NO 'auth_req' THEN delete).

4.2.4.2 AT-DSA-04: Notification on Special Events

The analytics can identify the presence of specific events that require the attention of the transportation personnel or of the passengers.

The analytics_X works on data from devices A, B, C. After the analysis, if the analytics_X identifies the presence of the contextual attribute 'service disruption' (e.g., due to an emergency event, air/train delays or high flow of passengers) the analytics_Y is called to define an appropriate countermeasure (e.g., inform the passenger of another travel option, open an additional bag-drop desk) and a notification is sent to the passenger.

AFTER the subject belonging to *Organization*=”entity_S” calls the analytics_X on the *DataType*=”A,B,C” THEN (IF the context *EmergencyState* is present THEN (MUST call the analytics_Y))

5 Data Model

The following table reports all the data models (types and classes) that are expected to be consumed as input or provided as output by the E-CORRIDOR components that are relevant to this pilot:

Table 3 Data formats expected to be used in the AT pilot

Data type class	Data format	Sensor and system (in case of connected) - source	Components (analytics or connector)	Reference to the BD
Indoor Location and Mapping data	GeoJSON	Connector - Indoor location Web API	E-CORRIDOR-IAI-PL	AT-BD-01, AT-BD-03
GPS data from Smartphone	NMEA 0183/GPRMC sentence: <Time, Status, Latitude, Longitude, Speed, Angle, Date, Variation, Integrity, Checksum>	Smartphone GPS Receiver	E-CORRIDOR-IAI-PL	AT-BD-01, AT-BD-03
Passenger QR Code identifier	QR Code	RGB Camera	AT pilot connector	AT-BD-01, AT-BD-03
Baggage QR Code identifier	QR Code	RGB Camera	AT pilot connector	AT-BD-01, AT-BD-03
Boarding pass	BCBP (bar-coded boarding pass)	Optical Barcode Reader	AT pilot connector	AT-BD-01, AT-BD-03
Image (for facial, fingerprint, or iris recognition) in passport	JPEG, JPEG2000	Camera	E-CORRIDOR-IAI-FR	AT-BD-01, AT-BD-02
Accelerometer	JSON <time, x, y, z> in m/s^2	Smartphone IMU Sensor	E-CORRIDOR-IAI-GA	AT-BD-02
Gyroscope	JSON: <time, x, y, z>	Smartphone IMU Sensor	E-CORRIDOR-IAI-GA	AT-BD-02
Magnetometer	JSON: <time, x, y, z> in uT	Smartphone IMU Sensor	E-CORRIDOR-IAI-GA	AT-BD-02
Bluetooth RSSI (received signal strength indication)	JSON: <time, station id, RSSI>	Smartphone	E-CORRIDOR-IAI-PL	AT-BD-01, AT-BD-03

Passenger Activity and Posture	JSON Activity Streams 2.0. Multi-lingual representation of activities. Compatible with JSON-LD	RGB-D Camera	E-CORRIDOR-IAI-AR	AT-BD-02, AT-BD-03
Lidar	LAS (LASer) file format for the interchange and archiving of lidar point cloud data	LIDAR SDK	E-CORRIDOR-IAI-AR	AT-BD-01, AT-BD-03
RFID Data	JSON <time, Tag IS, Reader ID, tagSeenCount, memoryBankDat, XPC, Signal Power, accessStatus, relativeDistance, firstSeenTimeStamp>	RFID Reader SDK	Smart sensor – edge device available in the AT pilot	AT-BD-01, AT-BD-03
Rail Booking passenger data	Sabre Rail GDS XML Schema	Sabre Rail GDS Web Service API	Connector/Simulator used in the AT pilot environment	AT-BD-01, AT-BD-03
Airline Booking passenger data	JSON Amadeus REST Schema	Amadeus Web API	Connector/Simulator of the AT pilot environment	AT-BD-01, AT-BD-03
Operating System and Processes log	Syslog standard format	Log files	E-CORRIDOR-IAI-FHEIDS	AT-BD-04
Security event log	Common Event Format (CEF) normalizing security events.	Log files	E-CORRIDOR-IAI-FHEIDS	AT-BD-04

6 Security Model

As discussed in detail in Section 3.1, in the AT pilot several sensitive data are processed. These data are related to personal and biometric information of the passengers and to the cyber infrastructure of the transportation entities (e.g., information on the structure of the cyber network, the characteristics of the adopted assets). The access to these data must be restricted, be ensured that no confidential information is leaked, that the data integrity is preserved, and that the access to those are controlled and logged. In the following, some security attributes are considered with respect to the AT pilot and the characteristics of the E-CORRIDOR framework.

6.1 Confidentiality

Confidentiality (a component of privacy) guarantees that information is kept secret and inaccessible to any unauthorized entity. As already mentioned, in the AT pilot, sensitive data related to passengers and the cyber infrastructure of the transportation operators are processed. A confidentiality breach could result in severe fines and legal action (e.g., by breaking the GDPR, General Data Protection Regulation), damages to the reputation of the responsible stakeholders, and exposure to cyber-security threats. Indeed, confidential information on the cyber-infrastructure has value and systems are often under attack as criminal hackers hunt for vulnerable systems to exploit.

Ensuring confidentiality on the shared data represents a critical requirement for the AT pilot. One of the main goals of the E-CORRIDOR project, reflected in the features of its framework, is privacy. To respect data confidentiality, techniques of the E-CORRIDOR framework such as DMOs and DSAs ensure that data are properly treated (e.g., anonymizing confidential passenger records, performing facial redaction on feeds collected from environmental cameras) and accessed only to the desired entities. Moreover, obligations enforced in the ISI ensure that appropriate *data retention policies* are adopted, i.e., if there are no different auditing requirements from the regulatory entities, sensitive data are deleted soon after the original analysis goals are fulfilled.

In addition to the common features provided by the E-CORRIDOR framework, having highly sensitive information, the AT pilot will adopt a *token-based* authentication while transferring credentials among multiple security domains. Thanks to such an approach no confidential information needs to be transferred but only the proof that the identity is deemed trusted (i.e., the biometric information are not sent from the train station to the airport, and vice versa, while the multimodal access to the services can still be offered).

6.2 Integrity

Integrity ensures that data preserve their accuracy and completeness from creation to deletion. In the AT pilot, this corresponds to avoid that any data shared in the collective infrastructure is changed (in an uncontrolled manner) before or after being analyzed. By monitoring passengers in the transportation premises and processing their records, any data alteration can affect the quality of the analyses (up to being ineffective) and therefore cause the inability to timely deliver the requested (customized) services or lower the quality of the security checks and identification procedures. In the E-CORRIDOR framework, the data bundles managed by the ISI contains the Data Protected Object (DPO). Basically, a signed hash-based summary of the data (referred to as singed bundle integrity check) guarantees that the whole data bundle has not been corrupted either by chance or purpose (please see Section 4 of D5.2 for a detailed description of the ISI subsystem in E-CORRIDOR).

6.3 Authentication, Authorization and Auditing

An optimal access control and identity management is required to achieve the seamless access to multi-modal transportation. Authentication and authorization follow the identification step by verifying that the issued identity information is genuine and that appropriate access to the service is provided.
In the AT pilot, one of the key goals is the provisioning of a frictionless passenger experience while accessing to the services of multiple transportation entities throughout the journey. In the E-CORRIDOR, the trusted identity provider component (AT-SF-04, see D8.1 for a detailed description of the ASI subsystem) is in charge of providing cryptographic keys and verification of the participating entities (e.g., connected environmental sensors collecting biometric information useful for the passenger identification).
The access to the information shared in the ISI is then regulated by DSAs. This authorization is performed at both user and analytics levels. Therefore, some services can be restricted to some users, and the analytics can perform their operations on pieces of data only if the first are able to meet the trust requirements expressed by the data producer.
For regulatory compliance the delegation authorization and data access needs also to be logged and available for auditing by competent authorities. The Common Security Services Infrastructure (CSI) subsystem of the E-CORRIDOR framework provides the needed secure auditing facilities.

To ensure that the above properties are respected, in the AT pilot, an application of the SecRAM [6] methodology proposed by SESAR JU for risk identification, analysis and assessment will be also considered.

Please refer to D6.1 for a more detailed discussion on the features of the ISI subsystem of the E-CORRIDOR framework, and to D5.2 for an overall description of the same framework.

7 Deployment Model

This section lists deployment requirements for the AT pilot. First, the deployment of the E-CORRIDOR architecture in the pilot is illustrated. Then specific hardware and software requirements are considered (in Sections 7.1 and 7.2). Finally, in Section 7.3, connectors with components and devices peculiar to the AT infrastructures are presented.

It is important to note that the requirements described below are subject to change as the design of the pilot will continue to evolve in the next months of the project with the final aim of ensuring an efficient and effective integration of the E-CORRIDOR framework for its subsequent validation and evaluation. Moreover, feedback and improvements collected throughout the maturation of the E-CORRIDOR framework will be reported also in the pilot architecture.

The AT pilot is characterized by the presence of a multitude of sensitive data and multiple security domains either belonging to the same or different stakeholders. This situation turns out in the existence of data silos and self-contained and sub-optimization of the systems. Thanks to its privacy-aware analytics and controlled data sharing, the E-CORRIDOR framework can hold a privileged position in enhancing the current scenario allowing the creation of a collaborative multi-modal transportation sector where data ownership is preserved and novel and improved services can be delivered to passengers and transportation entities.

Sensitive data concerning passengers (e.g., biometric, passport and travel documents) need to be kept in the same security domain that has originally collected them due to performance and regulatory reasons. On the performance side to perform a timely identification of the passengers and allow the exploitation of more sensors (e.g., the ones available in wearable and mobile devices of the same passengers), some components of the E-CORRIDOR framework may need to be deployed at the edge. In such a way the delay introduced transferring the data to the cloud node is avoided. According to resource constraints (in terms of both power and computation) and scenario, some subsystems can be omitted, e.g., if the device does not have enough resource, only the ISI can be deployed on the edge. The DMOs will be performed on the edge before sharing the data. Other nodes running also the IAI subsystem will be in charge of performing the analytics. In case of environmental sensors deployed in the airport and train station premises (cameras with associated single board computers), thanks to Machine-to-Machine (M2M) communications, a distributed and combined contextual analysis can be performed to support seamless authentication.
Moreover, to really achieve a frictionless experience for the passenger, the same edge computation and communication needs to be performed even while the passenger changes mode of transportation. Being in presence of multiple and independent stakeholders (airport and train station) in the AT pilot, the deployment of the infrastructure on a single cloud environment could be unfeasible to be achieved in practice. Instead, through bi-lateral agreements, the confidential exchange of data to improve the services of both infrastructures and customers would receive a more favorable adoption. The edge execution would thus fulfil both regulatory and performance needs. Figure 13 represent the designed deployment model.

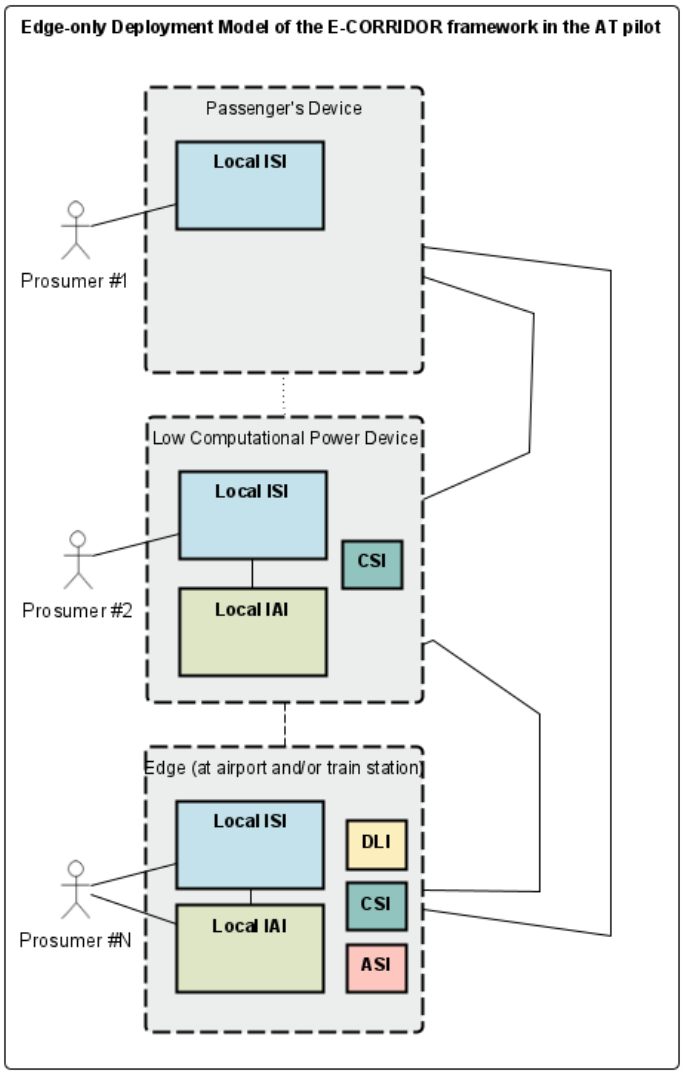

Figure 13 Deployment model of the E-CORRIDOR framework in the AT pilot

Nevertheless, the controlled data sharing enabled by the E-CORRIDOR framework opens up to the inclusion in the AT pilot of a cloud node managed by a third party, to support more demanding analytics. In the latter case the deployment model would correspond to the "mixed distributed deployment model" (presented in Section 3.3 of D5.2). Some notification on security threats and request for analyses can also be performed on the MMT-ISAC (see deliverable D4.2 on the architecture of the ISAC pilot).

7.1 Hardware Requirements

7.1.1 Edge devices of the touch points in the transportation infrastructure

RGB-D Video Cameras

Stereo video cameras able to capture RGB video streams with high quality and equipped with depth sensing capabilities (D), such as the Intel® RealSense™ RGBD camera series. These cameras offer wide field of view and a vision range up to ten meters, which is compliant with scene capturing requirements of activity and face recognition in the airport and train station touch points. The RGB-D camera can be integrated, e.g., into the check-in or baggage drop kiosks of the airport or at the passenger access control of the train platform. An SDK is available for implementing the data analytics algorithms required by the pilot.

Active RFID Readers and Tags
Active RFID reader can detect and decode RFID signals from any active RFID tag in a range up to 100m, e.g., the Wavetrend's RX50. The reader decodes the received tag identifier, signal strength (RSSI) and the associated metadata. It can be connected to a (single-board) computer either through USB or Ethernet, and some API are offered.

Zigbee® or Z-Wave Light Sensors
Light sensors measure the quantity of light in the ambient space. Such an information is used as context by the face recognition and activity recognition cameras installed at the touch point. The device operates wirelessly and communicates via the radio frequency standard Zigbee® or Z-Wave such as Cleode™ ZLum. This kind of sensors consumes a limited amount of electrical energy and can run on a cell battery. Moreover, it can be installed easily on any surface type: wood, plastic, etc.

BLE Beacons Transmitters
BLE Beacons are small wireless transmitters based on the Bluetooth low-energy technology to send their identification signals to the passengers' device while moving in the airport and train station indoor premises. The transmission range is usually of tens of meters but can be extended depending on the beacon hardware implementation. The BLE beacon transmitters as well as the readers implement the Generic Attribute Profile (GATT) Specification of Bluetooth technology that is built on top of the Attribute Protocol (ATT). The latter establishes common operations and a framework for the data transported and stored by the ATT. GATT provides profile discovery and description services for the BLE devices supporting *Airtag (Apple) or Eddystone (Google Eddystone-EID*) technologies.

Fanless Single Board Computer
This hardware will be used to connect RGB-D cameras, light sensors and RFID and perform analysis at the edge. Raspberry Pi and Nvidia Jetson are alternative for the edge computation of some of the data analytics adopted in the pilot.

Registration or Baggage drop Hardware
It is 4 CPU Intel/AMD 64-bit computer that is used to simulate passenger registration and baggage drop. It is connected to a USB camera to read QR code, capture user face, and print and read boarding pass or baggage drop receipt.

Edge Server
In each transportation entity of the AT pilot, there is the need for running the complete E-CORRIDOR framework and locally executing all the learning and analysis required by the analytics. A computer equipped with a high-performance GPU and high-speed network is required.

7.1.2 Passengers' device

Any smartphone or tablet equipped with the Android mobile operating system able to execute the E-CORRIDOR core framework. The execution of local analytics on the mobile device could pose additional constraints related to the specific functionality requested.

7.2 Software Requirements

Touch point software infrastructure

- Debian 10 or Ubuntu 14 Linux
- Python3
- Windows 10 Virtual Machine (Registration or Babbage drop Kiosk)
- Java, Spring Boot Framework

Edge infrastructure for IAI

- Debian 10 or Ubuntu 14 Linux Virtual Machine
- Python3
- NVIDIA VGPU
- Nvidia EGX Stack
- Docker
- MongoDB
- Mysql
- Java, Spring Boot Framework
- WebSocket
- Nginx HTTP
- Tomcat

Passengers and PRM Assistant Mobile devices

- Android mobile operating system
- WebSocket
- Python 3

7.3 Pilot Connectors

To ease the subsequent integration and validation of the AT pilot architecture, some connectors with the infrastructure currently available in the pilot premises are considered.

Indoor Mapping
In the AT pilot, the Indoor Mapping connector is needed for the visualization of the output of the analytics component Passenger Localization and Flow Optimization (E-CORRIDOR-IAI-PL). Through the connector the indoor map of the pilot premises will be represented and populated with the information of the location of the PRM passenger and assistant.
There are many APIs available to represent indoor maps and point of interest in structured way. Indoor map data are represented by using the standard IMDF (Indoor Mapping Data Format). The latter is a data model that is used to describe an indoor space. It is constituted by a set of JSON collections, in GeoJSON format.

Sabre Rail GDS Web API
A Web API connecting to the Global Distribution Systems (GDSs) is used to check passenger booking and the status of the transportation. Several GDS systems exist today, which provides

consolidated data from a wide range of rail transportation providers. The Sabre GDS allows to get passenger ticket information from over 50 railway carriers including SNCF (partner of the E-CORRIDOR project). In the pilot, an emulation of the Sabre GDS Rail Web API will be used as trustable source of information of the passenger identity when the first touch point in the multi modal journey is the train station. An example of the message received by interacting with the API is reported in Figure 14.

```
<RailManageBookingRQ MarketingCarrier="2C" PrimaryLangID="en">
  <ProcessType>Modify</ProcessType>
  <ProcessStep>Preview</ProcessStep>
  <BookingDetails>
   <BookingRef ID="UJFYLR" ID_Context="2C" Type="14" />
   <Contacts>
    <Contact ID="1">
     <Name>
      <PersonName>
       <NamePrefix>M</NamePrefix>
       <GivenName>Name</GivenName>
       <Surname>Surname</Surname>
      </PersonName>
     </Name>
     <Telephones>
      <Telephone
       ID="1"
       Operation="Add"
       PhoneNumber="111111999"
       Remark="Office phone"
      />
     </Telephones>
     <Emails>
      <Email>RAILTESTMAIL@GMAIL.COM</Email>
     </Emails>
     <Addresses>
      <Address>
       <AddressLine>15 Rue de Paris</AddressLine>
       <CityName>Paris</CityName>
       <PostalCode>75000</PostalCode>
       <CountryName>France</CountryName>
      </Address>
     </Addresses>
    </Contact>
   </Contacts>
  </BookingDetails>
 </RailManageBookingRQ>
```

Amadeus DCS Web API

Figure 14 Example of informaiton retrieved from the Sabre Rail GDS API

The connector to the departure control system (DCS) handles the following operations:

- Check-in from mobile and web apps as well self-service kiosks
- Baggage weights verification at self-service kiosks

- Generating and printing of boarding passes and baggage tags;
- Reporting and sharing information with security and flight management services.

As it will not be possible to interface the AT pilot architecture under evaluation directly with the DCS used by the air carriers an instance of the Amadeus will be simulated.
As soon as passengers are captured and recognized at any touch point a call to the Amadeus web API will be performed. This call is used to verify if the passenger is eligible to the flight, if she is located in the right terminal or if at the boarding counter for the right flight, and if the passenger needs assistance according to the specified SSR code.

8 Requirements Matrix

The E-CORRIDOR framework, its components and features are able to cover requirements and needs in the airport and train multi-modal travels as expressed by the AT pilot. Here we summarize the contribution of the main characteristics of the E-CORRIDOR towards the goals of the AT pilot (see Table 4). It is worth remarking that the characteristics of the ISI subsystem provide a transversal contribution towards all the goals of the pilot. In particular, the controlled and privacy-aware data sharing covers a pivotal role in ensuring that the sensitive data are treated properly while letting the data producers retain the control over their data assets.

Table 4 Features of the E-CORRIDOR framework and their contribution to the goals of the AT pilots

		AT-BD-01 PRM: Passenger Assistance	AT-BD-02: Multi-Biometric Passenger Authentication and Baggage monitoring in Multi-modal travels	AT-BD-03: Frictionless access to Multi-modal services	AT-BD-04: Controlled Data sharing for Service prediction, optimization and security
Data analytics for driver and passenger identification - IAI	E-CORRIDOR-IAI-PBI: Passenger: Identification, Behavior, Context	✓	✓	✓	
	E-CORRIDOR-IAI-GA: Gait analysis – passenger authentication		✓	✓	
	E-CORRIDOR-IAI-PL: Passenger location	✓	✓	✓	✓
	E-CORRIDOR-IAI-FR: Face recognition		✓	✓	✓
	E-CORRIDOR-IAI-AR: Activity recognition	✓	✓		✓
Privacy preserving (Security) analytics - IAI	E-CORRIDOR-IAI-FHEC: FHE – based checker				✓
Intrusion detection technologies (IDS) - IAI	E-CORRIDOR-IAI-FHEIDS: FHE - based intrusion detection				✓
ASI components	Multi-biometric and multi-factor authentication	✓	✓	✓	
	Federated authentication based on eIDAS	✓		✓	✓

	Trusted Identity Provider	✓		✓	
Features of the E-CORRIDOR core framework	Data manipulation operations (DMOs) of the ISI subsystem (e.g., facial redaction, (pseudo-) anonymization)	✓	✓	✓	✓
	Human readable and configurable DSA	✓	✓	✓	✓
	DSA-regulated access to information shared in the ISI subsystem (restricted access to the information)	✓	✓	✓	✓
	Edge-based deployment of the E-CORRIDOR framework		✓	✓	✓

9 Impact and Innovation of the E-CORRIDOR framework in the AT pilot

The E-CORRIDOR project, its framework and the innovation brought by the latter have the potential to enhance the multi-modal transportation from what concerns the airport-rail link, as well as the services and security offered to the passengers of both modes of transport. The AT pilot represents a noticeable example of such scenario.

In the following, we discuss how the AT pilot contributes to the E-CORRIDOR goals and in particular how the airport rail multimodal transport has the potential to be impacted by the adoption of the E-CORRIDOR framework. Then, some important innovations considered in the AT pilot are discussed.

9.1 Expected Impact of E-CORRIDOR in the AT Pilot

Toward the fulfilment of its own requirements and needs, the AT pilot contributes to the following E-CORRIDOR objectives (reported here for the sake of completeness):

- Objective 1: E-CORRIDOR will build a flexible, confidential and privacy-preserving framework for managing data sharing, for several purposes, by different prosumers (i.e., information producer and consumer);
- Objective 2: E-CORRIDOR will define edge enabled data analytics and prediction services in a collaborative, distributed and confidential way;
- Objective 3: E-CORRIDOR will define a secure and robust platform in a holistic manner to keep the communication platform safe from cyber-attacks and ensure service continuity;
- Objective 4: E-CORRIDOR will improve, mature and integrate several existing tools provided by E-CORRIDOR partners and will tailor those to the specific needs of the E-CORRIDOR platform and Pilots;
- Objective 5: E-CORRIDOR will provide mechanisms for seamless access to multimodal transport;
- Objective 6: the E-CORRIDOR framework and the services developed will be used to deliver a pilot product.

In the following we discuss how such contribution is realized.

With respect to Objective 1, in the AT pilot the prosumers are represented by the two transportation entities (train station and airport), their personnel and passengers. The data are collected through a multitude of sensors deployed in the transportation premises (e.g., cameras, Bluetooth beacons) and available in the personal devices of the same passengers (e.g., smartphone sensors). Thanks to the ISI subsystems of the E-CORRIDOR framework, data can be shared while respecting data privacy (DMOs can anonymize data before saving them in the data bundle), ownership and retaining control. All the four Block Diagrams discussed in Section 4.2 leverage on the privacy-preserving data sharing capabilities of the E-CORRIDOR framework as, even within the infrastructure of a single transportation entity (e.g., AT-DB-02 in Section 4.2.2), multiple security domains exists and the privacy while transferring sensitive data must be ensured.

The AT-BD-04 (see Section 4.2.4) is a prominent example of a distributed, collaborative and confidential way of performing edge analytics in the AT pilot, as targeted by the Objective 2. Therein, multiple stakeholders are able of de-siloing their data and achieving a global optimization, currently hindered by the lack of privacy-preserving means for sharing and analyzing data. The E-CORRIDOR framework can be deployed at the edge where analyses can be performed, and thus be compliant with applicable regulations in the transportation domain expressed by the AT pilot. Indeed, sensitive data of the passengers must not leave the security domain that has originally collected such information. Additionally, the presence of a single cloud for multiple transportation stakeholders could be a scenario hard to be put in place (e.g., for business and control reasons), while an edge-enabled analysis can be easily adopted. Moreover, the DSA-based data sharing is able to retain data ownership and enforce accessing and usage rules for the shared information contained in the data bundles.

Improving the security of the transportation entities, especially toward a multi-modal transportation, ensuring the cyber-security of the platform and the validity of all the authentication procedures in the different touch points (Objective 3) are of primary importance in the AT pilot. Several analytics and advanced security services are able to provide a robust continuous multi-biometric and multi-factor authentication (see Section 4.1). The context-aware and behavioral analyses are able to enhance the security of the current practices where a single factor or biometric are used to authenticate the passenger. Cyber-security events and alerts can be exchanged among transportation entities through the MMT-ISAC (see deliverable D4.2 for a more detailed discussion) which can also disseminate topic-based security information.

Several tools for analytics and security services (listed in Section 4.1) provided by the E-CORRIDOR partners have been adopted into and tailored for the AT pilot (Objective 4). Some of those tools have been actually co-designed thanks to the interactions with the AT pilot (e.g., AT-SF-01 and AT-SF-02). A direct integration in the pilot demonstration is expected with the dual goal of helping the maturation of the corresponding technologies (in accordance with the project goal of reaching a Technology Readiness Level up to level 6 or 7) and ease their integration in the AT pilot.

Multi-biometric and multi-factor authentication and the context-reasoning are able to support a seamless access to multi-modal transport in the AT pilot (Objective 5). Through a sensor fusion approach these components are able to combine several sources of information, either sensors or generated as output of other prediction analytics (e.g., face recognition, behavioral analysis, passenger location) with the final aim of supporting a robust passenger authentication, avoid any decision error and request the intervention of manual procedures only when needed. Such a vision can speed-up the processing of all the passenger checks and enable novel customized services for the passengers (e.g., notification of service disruption in multi-modal journeys).

As remarked in Section 4, several components and features available in the E-CORRIDOR framework are able to fulfil the requirements of the next-generation journey where novel services are provided to the passengers and a frictionless experience is perceived while accessing to a pan-European multi-modal transport. Privacy-aware data sharing and analysis will build the needed foundations for a collaborative environment where airport and train station can share token-based identities of the passengers and provide the needed customized services targeted to their journey. The E-CORRIDOR framework and its components have a privileged position to be considered for inclusion in an AT pilot product (Objective 6) as their features are refined thanks to the input collected from the pilot itself. The high-modularity and flexibility of

the E-CORRIDOR framework create also the possibility that multiple pilot products will be derived according to specific use cases.

Table 5 summarizes the contribution to the project objectives of the E-CORRIDOR framework as it is deployed in the AT pilot.

Table 5 Main features of the E-CORRIDOR framework in its application to the AT pilot and contribution to the project objectives

Features the E-CORRIDOR framework as applied to the AT pilot	Obj. 1	Obj. 2	Obj. 3	Obj. 4	Obj. 5	Obj. 6
Biometric-based analysis: Passenger localization, contextual analysis, gait analysis, activity analysis, face recognition	✓	✓		✓	✓	✓
Multi-biometric and multi-factor authentication and context reasoning		✓	✓		✓	✓
Intrusion detection based on fully homomorphic encryption	✓		✓	✓		✓
Federated authentication			✓		✓	✓
Trust Identity management	✓		✓	✓		✓
Deployment model: Edge-enabled architecture		✓	✓			
Information Sharing Infrastructure supporting Data Protected Objects	✓	✓				✓
DSA-based data sharing	✓	✓				

9.2 Expected Innovation Brought by the AT Pilot

The AT pilot architecture is expected to bring the following innovations to the current practice and state of the art where an integrated multimodal transportation is not yet mature and discontinuities are reflected in the perceived passenger experience.

- Privacy-aware multi-modal journey supporting a connected experience and BYOD technology.
- Single-token identity based on biometrics and context-aware analysis, created by a trusted identity provider in the CoT on the first transportation entity and propagated to the subsequent transportation domains to enable a seamless re-identification and re-authentication of the passenger.
- Exploit passenger location to customize services, for keeping passengers connected and informed of all events of interest to her journey.

- Transportation systems involved in multi-model trips will be connected not only physically but also operationally through collaborative data analytics and privacy aware data sharing.
- Maturate the state of the art solutions for multi-factor authentication and multi-biometric.
- Optimize passenger routing and transit and reduce waiting time at touch points.

10 Evaluation Metrics

In D2.1 we identified a set of questions that will constitute a guideline for the pilot evaluation and its harmony with the established goals. Here, we report those questions and the corresponding answers in light of the proposed AT pilot architecture. The same answers will be revised in the next months of the project execution with respect to the actual results achieved during the pilot evaluation.

1. *Will the data masking and encryption techniques adopted on the passenger data respect privacy and the applicable regulations for the airport, air and train carriers?*

   A compliance check with the GDPR and a successful assessment of the French Data Protection authority CNIL (as the pilot partners ADP and SCNF operate in France) will guarantee the respect of the relevant regulations.

2. *Will the passenger understand how her data are analyzed and shared to provide her seamless authentication mechanisms?*

   DSAs are expressed in a controlled natural language, which helps to ease their writing but also increase their understandability when shown to the passenger for approval before being used by the analytics in the AT pilot.

3. *Will the (pseudo-)anonymization and encryption techniques needed to satisfy the privacy requirements allow to achieve the target analytics goal? Or a performance-privacy trade-off will need to be considered?*

   DMOs performed by the ISI are in charge of applying the required anonymization processes. Moreover, before storing the data in the ISI the "bundles" are encrypted. The performance-privacy trade-off will be evaluated at testing time by considering the time required to perform those operations and the potential delay introduced in the passenger operations. Here it is worth to remark that the architecture foresees an edge execution of the analytics, also to cope with the performance requirements of some services.

4. *Will the sensor-based identification and authentication mechanisms actually allow a frictionless experience while preserving the passenger privacy?*

   The AT pilot aims at improving the passenger experience, therefore all the analytics and security services executed in the framework should be transparent to the passenger and able to work without requiring any additional input from the passengers. E.g., the face recognition should be able to quickly detect the face and the gait analysis should not require to perform any abnormal activity in the enrollment stage to perform the aimed authentication.

5. *Will the proposed solution allow a seamless access to multi-modal transportation enhancing the current practice from the point of view of both passenger and transportation carriers?*

   The single token authentication mechanism should guarantee the access to multi-modal transportation services. It will be evaluated by comparing the information that the passengers have to manually re-issue to perform the same activities in the solutions currently adopted and during the evaluation of the AT pilot architecture (e.g., if the passenger does not need to provide her passport multiple times).

6. *Will the airport, air and train carriers perceive real benefits form sharing the data in terms of situation awareness, prediction and optimization?*

   AT-BD-04 discussed potential optimizations for the airport and train station as well as for what concerns the improved security. Passenger flow optimization depends on the passenger localization, and a dedicated analytics is included in the

architecture. The same component can also be used for sharing customized messages related the queues (e.g., at the check-in or baggage drop desk). Data sharing with the MMT-ISAC can increase the security of the infrastructure through targeted and sectorial threat notifications.

7. *Will the airport, air and train carriers perceive a benefit in performing collective analytics in terms of quality of the results and data ownership/control?*

   As discussed in Section 3.1, the ISI subsystem of the E-CORRIDOR core framework is able to fulfill all the control, access and privacy requirements and regulations applicable to the scenario depicted in the AT pilot. The benefit of collective and at the edge analytics are evaluated according to the passenger experience. If the latter is improved (e.g., thanks to touchless and single-token solutions), it is also likely that a higher number of trips will be performed by the passengers trough the same transportation entities.

8. *Will the proposed passenger identification and authentication solutions be tamper-proof?*

   The multi-factor and multi-biometrics solutions included in the design of the AT pilot architecture aims at providing a robust authentication solution. Additionally, the context reasoning component will be able to assign scores to the quality of the detections and check the consistency of the predictions.

11 Conclusion

In this deliverable, we described the design of the AT pilot architecture according to the requirements specified in the deliverable D2.1. The document has discussed how the required pilot activities leverage on the E-CORRIDOR core framework and features to fulfill all the pilot requirements. In particular the adoption of the analytics and security services available in the ISI and ASI, and the DSA have been discussed with respect to different block-diagrams corresponding to the previously identified use-cases. Data, security and deployment models have been introduced along with some hardware and software requirements (collected at M12). Contribution to the project objectives and expected innovation brought by the AT pilot activities have been highlighted. Finally, an initial refinement of the evaluation metrics to be considered during the pilot demonstration has been presented.

This document will act as a reference for ongoing implementation and deployment efforts and for the experimental validation and evaluation expected to start in the last year of the project in M24.

References

[1] Amadeus IT Group SA, "Amadeus - Departure control system," [Online]. Available: https://amadeus.com/en/portfolio.airlines.operations.departure-control-system. [Accessed 27 May 202].

[2] SABRE GLBL INC, "Sabre Departure Control Suite," [Online]. Available: https://www.sabre.com/products/suite/departure-control/?orderby=title&order=ASC. [Accessed 27 May 2021].

[3] IATA, "NEXTT Passenger Journey," [Online]. Available: https://nextt.iata.org/en_GB/the-journey/passenger. [Accessed 27 May 2021].

[4] European Commisison, "GDPR - What data can we process and under which conditions?," [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_en. [Accessed 28 May 2021].

[5] Google, "Eddystone protocol," 2018. [Online]. Available: https://github.com/google/eddystone.

[6] SESAR Joint Undertaking, "SecRAM 2.0 - Security Risk Assessment methodology for SESAR 2020," SESAR JU, 2017.

[7] A. K. Jain, A. A. Ross and K. Nandakumar, Introduction to Biometrics, Boston, MA: Springer, 2011.

[8] M. Singh, R. Singh and A. Ross, "A comprehensive overview of biometric fusion," *Information Fusion*, vol. 52, pp. 187-205, 2019.

A. Appendix

A.1 Definitions and Abbreviations

Term	Meaning
AMB	Airport Managing Body
API	Application Programming Interface
ASI	Advanced Security Infrastructure – E-CORRIDOR framework subsystem
ASP	Answer Set Programming
BYOD	Bring Your Own Device
CoT	Circle of Trust
CSI	Common Security Infrastructure – E-CORRIDOR framework subsystem
DMO	Data Manipulation Operation
DSA	Data Sharing Agreement
EU	European Union
eIDAS	Electronic Identification, Authentication and trust Services
e-wallet	Digital or electronic wallet
GDPR	EU General Data Protection Regulation
GPS	Global Positioning System
HOG	Histogram of oriented gradients
IAI	Information Analysis Infrastructure E-CORRIDOR framework subsystem
IATA	International Air Transport Association
IdP	Identity Provider
IDS	Intrusion Detection System
ISI	Information Sharing Infrastructure – E-CORRIDOR framework subsystem
JSON	JavaScript Object Notation
LiDAR	Light and Detection and Ranging
LSTM	Long Short-term Memory Network
MFA	Multi-Factor Authentication
M2M	Machine to Machine
NEXTT	New Experience Travel Technologies
OCR	Optical character recognition
PRM	People with Reduced Mobility
PNR	Passenger Name Record
QR code	Quick Response code – two dimensional bar code
RFID	Radio-frequency identification
RGB-D	Red Green Blue – Depth – color model with depth information
RNN	Recurrent Neural Networks
RoT	Roots of Trust
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SSO	Single Sign-On
SSR	Special Service Request
TPM	Trusted Platform Module