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

D2.3

First Implementation, Test and Validation of the Airport and Train (AT) Pilot

WP2 – AT Pilot

E-CORRIDOR

Edge enabled Privacy and Security Platform for Multi Modal Transport

Due date of deliverable: 31/07/2022
Actual submission date: 31/07/2022

31/07/2022
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, Riccardo Orizio, Piotr Sobonski, Hubertus Wiese (UTRC), Koussaila Moulouel, Seyed Modaresi, Mohamed Arbane, Abdelghani Chibani (PEC), Christian Plappert, Roland Rieke (FhG), Gianpiero Costantino, Ilaria Matteucci, Giacomo Iadarola (CNR), Thanh-Hai Nguyen, Jean-Paul Bultel (CEA), Olivier Mercier (ADP)

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

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	09-Feb-2022	S. Sebastio	UTRC	Initial table of content
0.2	06-Jul-2022	S. Sebastio	UTRC	Intro (Sec 1), architecture, deployment and UTRC components (Sec 2)
0.3	13-Jul-2022	S. Sebastio	UTRC	Contribution to goals and objectives (Sec 6) and improvements in Sec 1 and 2
0.4	13-Jul-2022	R. Orizio	UTRC	Workflow and test cases for the passenger localization
0.5	18-Jul-2022	S. Sebastio, P. Sobonski, H. Wiese	UTRC	Workflow and test cases for the camera feed analysis, multi-factor, and federated authentication
0.6	25-Jul-2022	S. Sebastio	UTRC	Executive summary, structure of the doc, conclusion
0.7	27-Jul-2022	S. Sebastio	UTRC	Requirements traceability matrix
0.8	27-Jul-2022	C. Plappert	FhG	Status, Workflow, test cases for trusted service manager
0.9	28-Jul-2022	G. Costantino, G. Iadarola	CNR	Status, workflow, test cases for interest-case of airport services and gait analysis
0.10	29-Jul-2022	A. Chibani, K. Moulouel, S. Modaresi, M. Arbane	PEC	Pilot environment and input for facial recognition
0.11	31-Jul-2022	T.-H. Nguyen, J.-P. Bultel	CEA	Contribution to the fully homomorphic encryption solution
1.0	31-Jul-2022	S. Sebastio, R. Orizio	UTRC	General fixes

Executive Summary

This document, along with the released software components and demonstration videos, reports on implementation, test and validation activities performed in the AT pilot until month 26 (M26). Such activities are meant to test and validate the performance of the E-CORRIDOR framework once integrated in the pilot environment. The designed system architecture and components identified in D2.2 are considered as reference.

As the "experimental validation and evaluation" (Task 2.3) started at M24, this report details the architecture, comprising the connected external sensors and systems, and discusses the application of the selected E-CORRIDOR components to the AT pilot scenarios through detailed workflows. For each component, status, first experimental results, data used (and planned to be used) are described. Whereas D2.1 described the acceptance tests with the end users (*evaluation phase*) by means of user stories and use cases, here test cases refer to how the key functionalities and aspects of each of the considered solution are going to be validated (*validation phase*).

Travel and lab access restrictions imposed by the COVID-19 pandemic have forced many of the partners to re-schedule and re-arrange their test and validation activities. Nevertheless, all the partners have progressed in their implementation and integration efforts, that are on track. It should also be considered that the application of some of the proposed components is deemed more experimental (see e.g., the gait analysis or the attribute-based encryption). Detailed workflows for the interaction of the components with the E-CORRIDOR framework and the pilot environment have been designed. Notably, (i) the workflow of the camera feed analysis has been validated with public datasets, (ii) the facial recognition is under integration but already validated in the AT pilot environment as standalone service, and (iii) the interest-cast tested in a distributed setting resembling the final deployment. In the next few months, the effort will be oriented towards the finalization of the integration with the E-CORRIDOR framework and the deployment in the pilot. More attention will be devoted to the validation and evaluation in the pilot environment as well as to any refinement needed according to the feedback collected during the experiments.

Table of contents

1. Introduction

1.1. *Overview*

Many travels are nowadays inherently multimodal. The Airport-Train (AT) pilot aims at providing solutions supporting both passengers and transportation service providers. The designed solutions span from authentication to passenger processing, access to the airport's and train station's services, to mechanisms for enhanced security and situational awareness. A fil rouge connects all such solutions with privacy and controlled data sharing enabled through the integration of the E-CORRIDOR framework.

The AT pilot is characterized by the presence of different stakeholders, the main ones recalled here:

- passengers: accessing the services offered by the transportation service providers, including ancillary ones (such as restaurants).
    - person with reduced mobility (PRM): are passengers requiring special assistance. In the pilot, a particular attention is devoted to the PRM considering the rising demand for assistance in the larger airports.
- PRM assistants: contractors working either for the carriers (airline or train) or the station (airport or train) that take care of the PRM passengers, to ensure a smooth transition among modes of transport.
- airport and train station operators: managing the facilities and the performed operations.
- carriers and service providers: taking care of ticket reservation, passenger movement and ancillary services (such as restaurants and shops) offered in the airport and train station premises.

Two main scenarios have been defined in the AT pilot considering the point of view of the passengers and the one of the transportation service providers.

- in the passenger process (represented in Figure 1), the steps are as follows:

1. the passenger books a ticket
2. the passenger's preferences for service access are expressed
3. check-in is performed:
    a. at home through mobile enrollment
    b. once reaching the first mode of transportation through a self-service kiosk
4. localization and direction information about the next touchpoint could be received on the passenger's smartphone
    a. in case of PRM passengers, the wheelchair is localized and the PRM assistants can exchange their positions to better support the passengers when switching from one mode of transport to the following one
5. during the waiting time, services matching the passenger's preference may be suggested
6. different travel documents and authentication procedures could be requested in different security domains

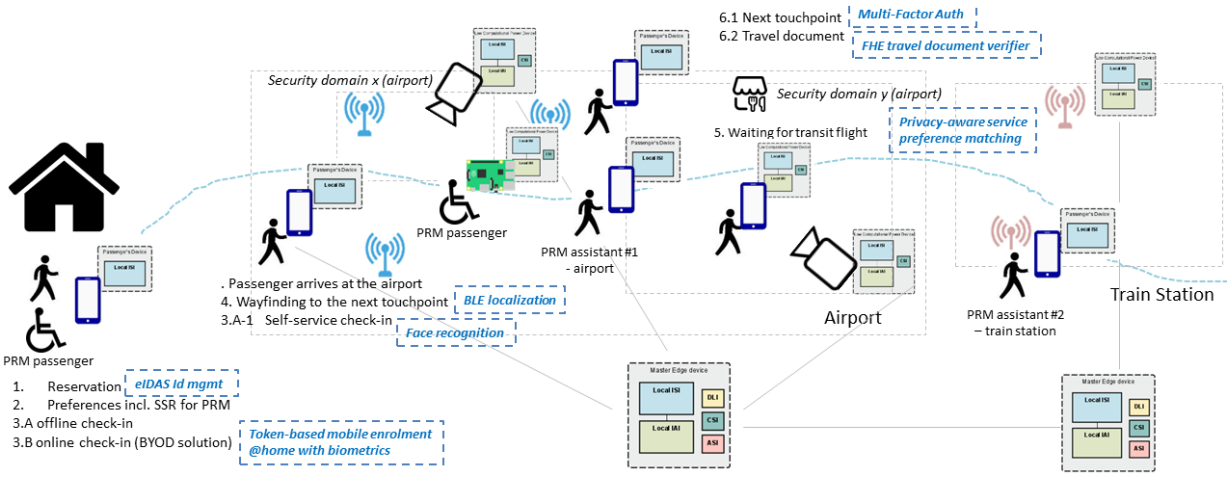

Figure 1 AT pilot services for the passenger process

- the analysis and security mechanisms put in place by transportation service providers (represented in Figure 2) are the following:
    - cameras deployed in the environment are used for performance analysis, activity recognition and identification of potential security issues (e.g., a left luggage)
    - authenticity of the sensors is protected through the hardware Root of Trust (RoT)
    - a Domain Name System (DNS) blacklist protects against malicious or illegitimate Internet addresses
    - threats and potential vulnerabilities related with the infrastructure of the airport and train station are exchanged with the ISAC pilot (Information Sharing and Analysis Center).

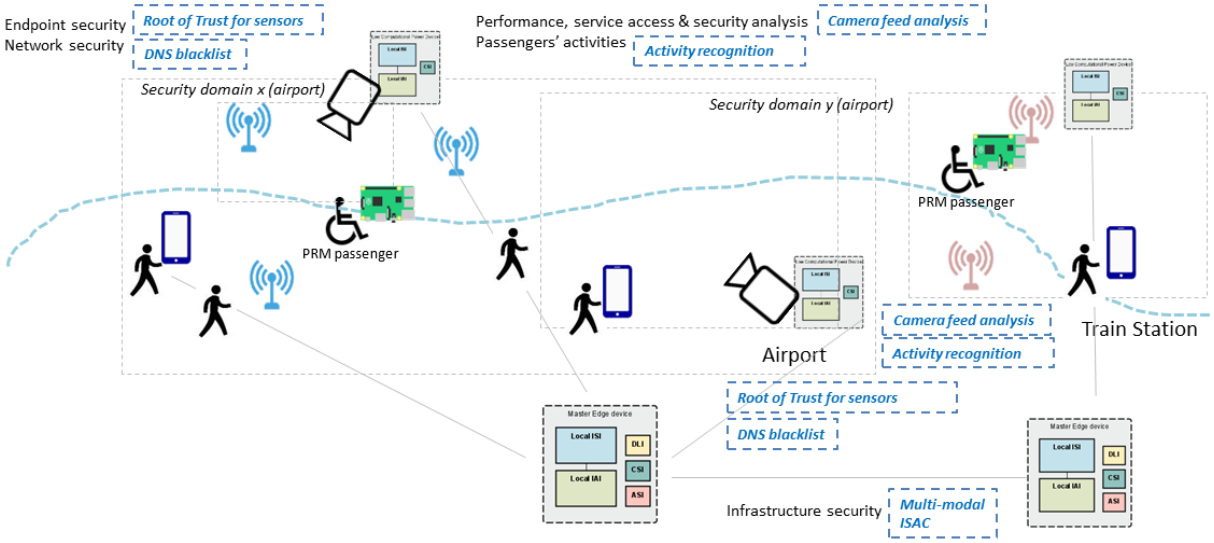

Figure 2 Security-related services for the Transportation Service Providers in the AT pilot

1.2. *Goals*

A few goals (and the corresponding solutions) related to the above scenarios and the AT pilot instantiation have been identified:

- Goal 1: achieve a frictionless passenger experience
    - Adopting the Bring Your Own Device (BYOD) solution for passenger enrollment and localization, as well as biometric-based mechanisms
- Goal 2: improve the quality of the assistance provided to the PRM passengers
    - Localization of the available wheelchairs and the PRM assistants can allow a smoother transition among mode of transport
- Goal 3: enable privacy-preserving, continuous and context-aware authentication of passengers
    - Multi-factor authentication, context analysis, and credentials recognized by EU states allow transportation entities to verify the passengers' credentials in a more robust and seamless manner
- Goal 4: improve operations management through collective privacy-aware analytics on the data shared in a secure way
    - Reviewing videos shared in a controlled and privacy-aware manner for performance analysis, activity recognition and security purposes
- Goal 5: provide multi-modal services and location-aware services respectful of the passenger privacy
    - Bluetooth-based localization and privacy-preserving preference matching can extend use and reach of the offered services
- Goal 6: ensure infrastructure security in the multi-transportation processes
    - By means of network protection, sensor validation and connection with the multi-modal ISAC

1.3. *Structure of the Deliverable*

The remaining of this deliverable is structured as follows. Section 2 details the refined AT pilot architecture, with a special emphasis on the adopted deployment models and the connected external solutions and sensors. Moreover, the different analytics and security services to be used in the pilot environment are recalled with a highlight on the motivation for the choice of each solution. Details on the (emulated) pilot services used for the validation are provided in Section 3. The same section provides a description of the status of the components and their integration in the pilot architecture. Type of data and test cases for the validation of each component are instead reported in Section 4. The requirements traceability matrix is reported in Section 5. Contributions of the identified solutions to the pilot and project objectives are discussed in Section 6. Conclusions are in Section 7. List of references (in Section 8), acronyms, and figures included in this document (in the Appendix) close the document.

Note to the reader: This deliverable reports on the first iteration of the implementation test and validation of the AT pilot solutions following requirements and architecture design presented respectively in D2.1 and D2.2. Despite the effort in keeping the document self-contained, it is assumed that the reader is already familiar with the E-CORRIDOR architecture, the sharing and analytics infrastructures as well as the analytics and security services described in D5.4, D6.2, D7.2 and D8.2.

2. Pilot Architecture and E-CORRIDOR Framework Integration

2.1 *Architecture*

The AT pilot setup foresees the presence of multiple external services, actors and sensors that need to interact with the E-CORRIDOR framework (please refer to Figure 3). Examples of the sensors deployed in the AT pilot environment are cameras, Bluetooth beacons and Lidar installed in the premises of the transportation service providers. These also act as data producers for our system. Moreover, services such as travel reservation system, assistance request, flight information, value-added services, shops and dining offers available in the airport and train station would need to exchange information with the E-CORRIDOR framework through the use of appropriate connectors.

The Information Sharing Infrastructure (ISI) API (Application Programming Interface) will be used by the above-mentioned sensors and solutions by means of code scripts, webpages, or mobile apps. Data sharing agreements (DSA) will instead be specified by airport and train station managers, experts of the domain, in collaboration with the related legal and privacy officers to ensure that legitimate interests and privacy regulations are respected. All the services offered by the Information Analytics Infrastructure (IAI) and the Advanced Security Infrastructure (ASI) are then exposed and offered to both passengers and operators of the transportation services.

Moreover, a bi-directional information exchange is established with the multi-modal transportation ISAC (Information Sharing and Analysis Center) to receive targeted news about threats and vulnerabilities affecting the two connected transportation sectors constituting this pilot. Additionally, private data related to the adopted hardware and software solutions can be shared upon proper anonymization.

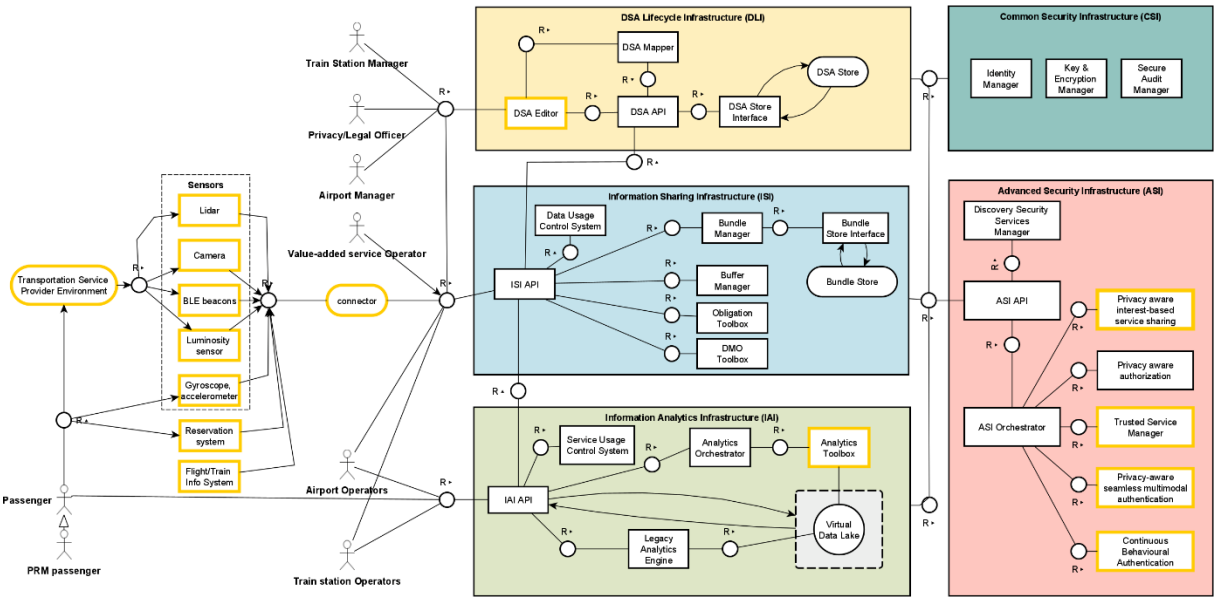

Figure 3 Instantiation of the E-CORRIDOR framework in the AT pilot environment

The main external components connected to the different nodes are:

- Sensors:
  - Lidar (Light Detection and Ranging): uses light pulses and measures the reflection time to estimate distance. Through the generated point cloud, a 3D

representation of the area can be generated. Solutions based on such sensors are deployed in delimited areas of the airport (e.g., where the baggage carousel is) to analyze them with an inherent privacy (as only the shape of the detected objects is captured). Unfortunately, Lidar-based solutions are expensive and therefore their use is still limited. In the AT pilot, we will explore the connection of the Lidar solutions with the E-CORRIDOR framework to support other analysis methods (e.g., the context analysis with information such as people counting).

- Cameras can be embedded in other devices (e.g., a kiosk) for authentication purposes but are also largely used in the airport and train station for monitoring, analysis, security, and safety applications. In the AT pilot we foresee the presence of IP-connected (Internet Protocol) cameras deployed in the premises of the transportation service providers (e.g., in the terminals). For some of the AT pilot applications, RGB-D (Red Green Blue-Depth) cameras need to be installed. The additional depth sensor working along with the regular color/RGB sensor can enrich the conventional captured image with a per-pixel depth information (useful for the activity recognition).
- BLE beacons (Bluetooth Low Energy): are devices used to broadcast a codified universally unique identifier. By picking up the messages, a device in proximity of the beacon can determine its position in indoor environments or trigger pre-defined actions. Compared to other indoor localization solutions, a BLE-based one has a significant lower energy impact, a wide support from devices with different formats and a generally lower cost.
- Luminosity sensors: ambient light sensors have a wide set of uses spanning from mobile, to consumer, indoor and outdoor applications. In our context, such sensors will be used to assess the luminosity of the environment in which a video-based authentication solution operates and evaluate the potential impact on the quality of the collected data and executed process. We plan to implement ambient light sensors by CLEODE adopting the ZigBee protocol. A set of light sensors deployed in the lab and connected by means of a Zigbee network will collect and share the light intensity (in Lux) through Python or Java code.
- Gyroscope and accelerometer sensors are nowadays largely deployed in the smart phones and watches. User-related information collected by such sensors can be exploited to identify the user, the performed activity and potentially enabling a continuous authentication. In the AT pilot, users willing to use their own smartphones to collect and locally analyze these data (through an app running the E-CORRIDOR framework) may adopt such an additional authentication mechanism for some of the touchpoints.

- Reservation systems are used by airline and train carriers for booking tickets. A Passenger Name Record (PNR) is issued for each passenger or group of passengers travelling together. It is identified through an alpha numeric code and contains information such as itinerary (useful e.g., in case of connecting flights), name of the passenger(s) and ticket details. Additional optional attributes are also associated such as frequent flyer data, seat allocation, special service requests (SSR) and optional

service information (OSI) for assistance (e.g., wheelchair) or meal requirements, age, or disability. Nowadays, the same systems are also used to collect additional travel related information such as hotel accommodation, car rental, transfers and even suggest sightseeing and other value-added services. In the AT pilot, the reservation system will be integrated by means of an emulator to evaluate the overall workflow from the travel booking, to the access to airport and train station services.

- Flight and train information systems are databases used to timely share information about flight, baggage checkout, departing platform (for the train). Usually, this information is shared through large display boards. Nowadays, the same information is accessible through websites. In the AT pilot, information pertaining a particular passenger can be extracted from the information system and then used to better support the passenger in her travel, e.g., estimating the waiting time in the airport before the passenger needs to reach her next touchpoint, and enable wayfinding.

2.2. *Deployment Model*

The flexibility offered by the E-CORRIDOR framework will be exploited for its integration in the AT pilot environment. In particular, the *edge-only deployment model* (please refer to D5.2 for a detailed description and discussion of other deployment models for the framework) will be considered. As many personal data are collected and processed, it is generally not possible to transmit data among different security domains or to the cloud, due to performance and regulatory constraints. Moreover, to accommodate the heterogeneity of the hardware configurations considered in the scenarios only the required subsystems of the framework will be deployed. We assume the presence of the following nodes (represented in Figure 4):

- Master node: one for each mode of transport, it is constituted by a server implementing the whole E-CORRIDOR framework.
- Smartphone: according to the services the passengers may want to use, it may include only the IAI to perform local computation (e.g., in case of the localization or gait analysis) or also the ISI for sharing data with the AT pilot environment.
- Low power devices (e.g., RaspberryPi) are attached to the sensors deployed in the environment (e.g., IP-cameras), and generally include only the ISI. Such a configuration is used to allow a controlled data sharing and perform any anonymization required by the DSA (through Data Manipulation Operations, DMOs). In the case of the devices attached to kiosks or wheelchairs the device may run also the IAI subsystem for performing local computation.

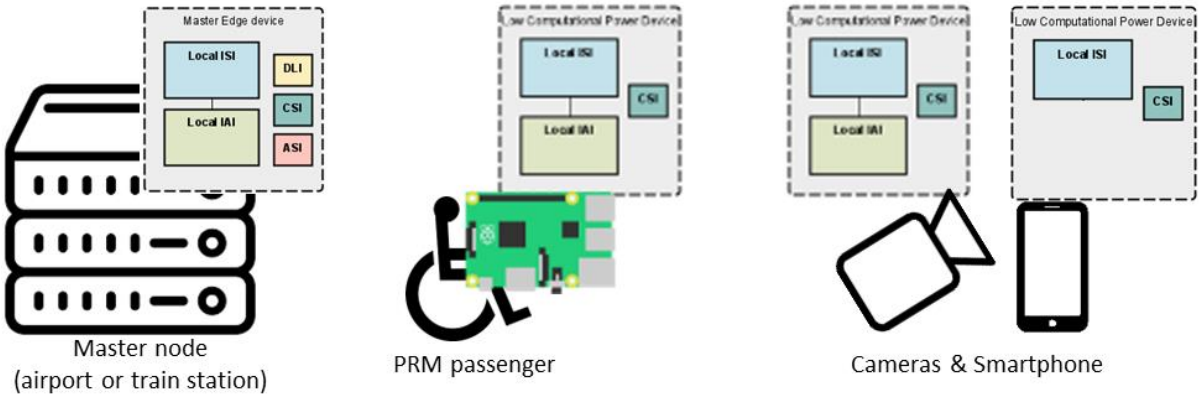

Figure 4 Examples of deployment for different types of devices in the AT pilot

By connecting the master node and the ISAC, a controlled data sharing about threats and vulnerabilities is enabled through the presence of the ISI subsystem on both.

2.3. *Integrated Components*

To achieve the AT pilot goals several analytics and security service components designed in E-CORRIDOR and made available through the IAI, and ASI are required. These will allow different authentication mechanisms, passenger-oriented services, and security and performance analysis. In the following, the main features of the components and their use in the pilot are recalled.

2.3.1. **Passenger Localization**

Bluetooth Low Energy (BLE) beacons, deployed in the airport and train station premises will transmit a codified message containing information about their position. By picking up these messages and measuring the received signal strength (RSS), a mobile app running on the passenger's smartphone can estimate its position in the terminal (so messages will flow only from the beacon to the smartphone to preserve the passenger's privacy). When such information is coupled with the itinerary information in the PNR (saved locally on the phone) and the travel information from the digital Flight Information Display System (FIDS), it is possible to provide passenger with directions to reach her next touchpoint. Another application scenario is related to the PRM where the component runs on a small device attached to wheelchairs and smartphones property of the airport or train station and made available to the passengers and assistants. These devices will also share the position with the infrastructure to ease the connections among operators and to better manage the available assets. Any other passenger using the app will need to explicitly request the sharing of her position.

2.3.2. **Camera Feed Analysis**

Cameras are largely deployed in the airport terminal and train station. The video collected by these cameras are often routed to the control rooms for visual inspection. Automated analysis can support security officer and operators while providing additional analysis functionalities to the airport and station managers. The designed analytics is able to perform automated crowd monitoring extracting metrics related to performance (e.g., passengers in a specific area or asset monitoring), safety and security (e.g., the respect of social distancing rules or to identify a left luggage). Running in the E-CORRIDOR framework, the component offers opportunities not only for cost reduction, and increased quality of service (due to the automated analysis) but also the respect of the privacy. As videos may contain sensitive data, potentially used for identifying

the passengers, the station managers along with legal and privacy officers, will need to specify an appropriate DSA. Other than defining the data access and usage (e.g., limiting the kind of analysis performed and metrics extracted from the video) a face redaction DMO can be imposed to preserve the privacy of the passengers.

2.3.3. Gait Analysis

Passengers are more and more prone to manage and control their journey from their mobile devices. Transportation service providers are therefore offering solutions supporting the BYOD (Bring Your Own Device) paradigm, including authentication mechanisms. Authentication solutions based on personal devices can reduce the queues (for some services) in the airport and train station (like kiosks) and at the same time improve the passenger experience. The proposed solution exploits the data collected from the sensors installed in the smartphones, smartwatches, and other wearable devices. This approach allows a continuous biometric authentication based on gait analysis. A classifier based on the Recurrent Neural Network (RNN) processes the data from the inertial sensors and models the unique features of the walking style of each passenger. The solution can also be considered in conjunction of more classic (biometric) authentication mechanisms for scenarios requiring a higher security level or a multi-factor authentication.

2.3.4. Face Recognition

The face recognition analytic is a biometric-based security solution to verify the identity of the passenger largely adopted in airports (and now also under test in a few train stations). Cameras are installed in specific kiosks for a seamless authentication: the passengers can pass through a checkpoint and be authenticated in few seconds. When the face recognition analytic is invoked, first the face detection and liveness identify the presence of a real person (i.e., not a picture). Additionally, to preserve the privacy of other passengers accidentally moving near the camera, the background can be blurred. Then, the facial recognition is performed against a ground-truth knowledge, e.g., a photo with the passenger holding her identity card. This ground-truth may also be collected by means of the E-CORRIDOR mobile application (see section 3.2.4).

2.3.5. Activity Recognition

The activity recognition aims at identifying the action performed by the passenger and exploiting this information as a context attribute to enhance a biometric-based authentication. Examples of activities identified by the component are standing, sitting, moving with a suitcase, talking on the phone, running. Such analysis can be performed in a privacy preserving fashion considering the way a person moves and a few physical characteristics (the latter not pertaining biometric measurements). In contrast to methods based on the full image, we extract and record only some key points from each camera, and some general attributes such as hair color, presence of moustache, kind of clothes (e.g., with short or long sleeves), and related objects such as glasses, suitcase, and bag with their shape features. Moreover, a model of the human skeleton is built by extracting the spatial position of the joints in the human body. Figure 5 shows the skeletal representation of a human body from data collected from different sensors (including depth information form cameras such as the Intel RealSense): the joints are represented by a circle. The model is then build considering movements over time, pose and activity of the person.

Figure 5 Skeletal representation of the human body used by the activity recognition to build the model

2.3.6. Analysis of Sensitive Passenger Data

Several use-cases in the multimodal transport domain need to process sensitive passenger data. The adoption of techniques able to preserve the privacy of such data also at computation time is therefore highly advisable. We thus adopt a fully homomorphic encryption (FHE). Such an approach encrypts the data in a way that allows the server to perform computations on it without the need of a prior decryption.

In the pilot, fully homomorphically encrypted passenger data are available from a QR code in the boarding pass. When scanning this QR code, the device gets the ciphered URL and sends the request to E-CORRIDOR framework to check whether it is valid or not. This URL is disabled after the travel ends.

2.3.7. Multi-Factor Authentication

As multiple authentication methods, often based on biometrics, are made available to the passengers, this service aims at combining them. On one hand, the multi-factor authentication can increase the robustness of the system. On the other hand, having different authentication mechanisms combined can also offer more authentication choices to the passengers while accommodating the security requirements of a given touchpoint. This security service is meant to orchestrate different biometric-based authentication solutions available in the E-CORRIDOR framework, in particular the IAI toolbox. It is constituted by two main subcomponents: the engine and the reasoner. The first is in charge of defining, executing and controlling the correct progress of a workflow where tasks correspond to the individual authentication solutions. The latter is instead described in the following subsection.

2.3.8. Context Reasoning

In the AT pilot, multiple components such as facial recognition, activity recognition and gait analysis are possibly exploited for passenger authentication. These components, being based on machine-learning models, are highly dependent on the quality of the data in input which are subject to different imperfections (such as imprecision, and ambiguity). Consequently, the generated output may be incorrect or more in general include a certain degree of uncertainty. For example, one ambient setting that may affect the analysis of video-based authentication mechanisms is the luminosity. Indeed, a low level of luminosity can significantly affect the ability of the facial recognition component. Consequently, the authenticator should not fully trust on the process in such circumstances. The context reasoning can exploit multiple sources and context information and provide a high-level decision to authorize or not the passenger. The component relies on an ontology that guides commonsense reasoning rules. An example of the information provided in input is: localization, identifier and confidence value from activity and facial recognition, luminosity level.

2.3.9. Federated Authentication

From the moment passengers book their ticket until the travel ends, many stakeholders are involved, and each stakeholder may require to re-authenticate the passenger. In case of multi-modal travels, passengers may even have different accounts or need to re-issue their credentials. Federated authentication solutions are a mean of improving the user experience while authenticating in different security domains. Indeed, federated authentication establishes agreements and allow authentication in different domains with a single digital identity. In the transportation sector, other related issues are the cross-border interoperability and compatibility, and the quality of the self-declared identities. Incorrect data and operational incompatibility in the passengers' files are estimated to cost hundreds of million to the airlines [1]. The adopted security services will be based on the EU eIDAS (electronic Identification, Authentication, and trust Services) framework and connected to the reservation or check-in system adopted in the AT pilot to ensure correctness and pan-European compatibility in the passenger's entries.

2.3.10. Trusted Service Manager

The Trusted Service Manager (TSM) is part of the ASI subsystem. It utilizes the Trusted Platform Module (TPM) as hardware Root of Trust (RoT) to strengthen the security of upper layer security services and provide an edged security layer to the E-CORRIDOR framework. Instantiated in the AT pilot use case, it strengthens the security among the different sensor platforms in both the train and airport domain with the help of a TPM 2.0 as hardware trust anchor in the system. This approach improves the overall system security against advanced cyberattacks that may tamper with the sensor platforms. It enables to establish strong trust

relationships between the sensor platforms and the E-CORRIDOR edge server by bootstrapping integrity-protected systems and reporting their status via an implicit platform attestation mechanism. This allows for example to detect trustworthy data input, like video streams, and mitigate against cyberattacks where an attacker may modify firmware and introduce compromised data input. We instantiate the system according to the *Host-based Integrity Verification System* described in our recent publication [2]. As a very high-level description, the system consists of the TSM-enabled sensor platforms and the E-CORRIDOR edge server. The TSM will measure the platform state of the sensor platform and unlock a corresponding TLS-key only if the platform is in a correct state. This is an implicit attestation mechanism, where the E-CORRIDOR edge server can trust a sensor platform if a TLS-session could be established successfully.

2.3.11. **Interest-Cast of Airport Services**

The goal of the interest-cast for airport services is to provide a way to run analytics that will use passengers' private information, without disclosing those private details to the other party. It uses the Two-Party Computation (2PC)-based service sharing part of the ASI subsystem, described in detail in T8.3 of D8.2. The relevant aspect is that the data exchanged by passengers and provider are kept private. We recall that in a secure two-party computation, two parties exist (Alice and Bob), each holding some private data: x and y, respectively. By adopting the 2PC, Alice and Bob can jointly compute the outcome of a function g(x, y), without disclosing to the other party their own input. In the AT pilot scenario, when a passenger uses this service, she can obtain specific information with respect to her interests in a privacy-preserving way.

2.3.12. **Services Offered Through the ISAC, Under Evaluation and/or Refinement**

- *Network Intrusion Detection*: an FHE-based solution to identify any connection with malicious IP addresses included in the Domain Name System blacklist (DNSBL). This service will be offered through the ISAC.
- *Encryption of ticketing information*: the access to some of the services available in the airport may be restricted according to some attributes of the passenger, such as nationality or other information part of her PNR. The attribute-based encryption (ABE) can be used to allow transactions only for passengers matching a given policy.

3. Status of the Testing Environment and Components

In this section the status of the pilot environment planned to be used during the validation and evaluation stages is described. Moreover, an updated status for each of the component expected to be used in such environment is described.

3.1. *Environment*

For the evaluation and validation, the AT pilot environment will be constituted by services deployed (mostly through virtual machines) in two distinct and interconnected security domains representing the airport and train station. More in detail we will consider:

1. Devices: (i) passenger's smartphone running the E-CORRIDOR solutions, (ii) low-power devices running the ISI and IAI components connected to the sensors (as described in Section 2.1 and 2.2), (iii) edge server running all the subsystems of the E-CORRIDOR framework
2. Airport information system emulator connected to a few touchpoints (e.g., registration, bag drop)
3. Airport booking server – connected with a database compliant with the Amadeus environment [3]
4. Train station information system emulator connected to a few touchpoint (e.g., gate access and PRM service)
5. Train booking server – connected with a database compliant with the Amadeus or Sabre Rail [4] environments
6. E-CORRIDOR kiosk (one at the train station and a second on the airport) – managing the multimodal transport registration.

All the emulated services will be exposed through web applications (by adopting Flask [5] as web framework).

3.2. *Pilot Status*

In the following sub-sections, the status of each component part of the AT pilot is discussed, remarking the remaining steps in terms of development and integration.

3.2.1. **Passenger Localization**

As of month 26 of the project, we are able to create personalized BLE beacons sending messages to advertise their position (on x, y, z axis). Examples of the generated beacon message with two different protocols under evaluation (i.e., iBeacon and Eddystone) are reported in Figure 6. These messages are going to be analyzed by the currently under development Android app that, through trilateration, will estimate the position of the passenger (from the received signal strength) and localize her in the train station-airport premises.

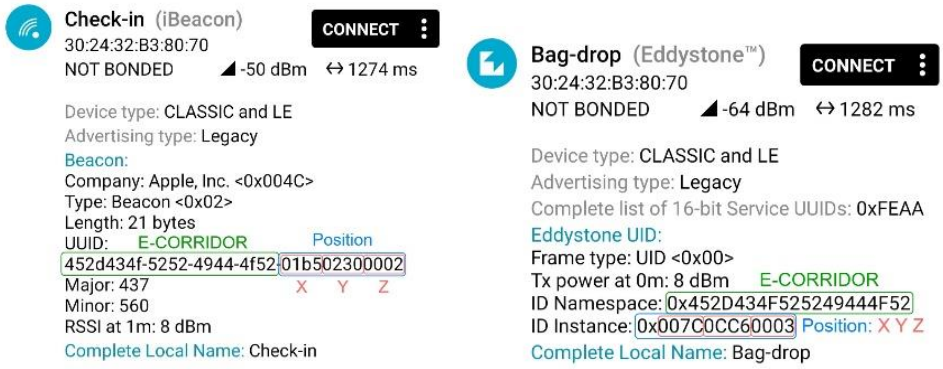

Figure 6 Beacon messages as received by a mobile device: on the left from the iBeacon installed on the check-in and on the right from the Eddystone on the bag-drop desk.

Once the localization algorithm has been finalized and properly tested, the app will be enhanced by integrating the information coming from the PNR and FIDS to generate ad-hoc paths related to each passenger journey. While the PNR will provide information related to the specific journey on which the passenger is on (e.g., flight number for the bought ticket), the FIDS will provide information on the flight and its status (e.g., airline name, expected time of arrival, check-in and gate numbers). Such information will be merged to generate the path that the passenger should follow to easily reach all her relevant Points of Interest (PoIs), e.g., baggage drop, check-in kiosk, gate. As final step, we will evaluate the integration of this service with the interest-cast service to improve the passenger experience while on the train station-airport premises.

3.2.2. Camera Feed Analysis

The component can analyze the videos collected by the cameras installed in the airport terminal and train station. The domain expert can identify the areas of interest for extracting metrics through a graphical interface (Figure 7). It allows the drawing of quadrilaterals on a reference image for the area. The zones corresponding to the quadrilaterals are saved and stored on a JSON file.

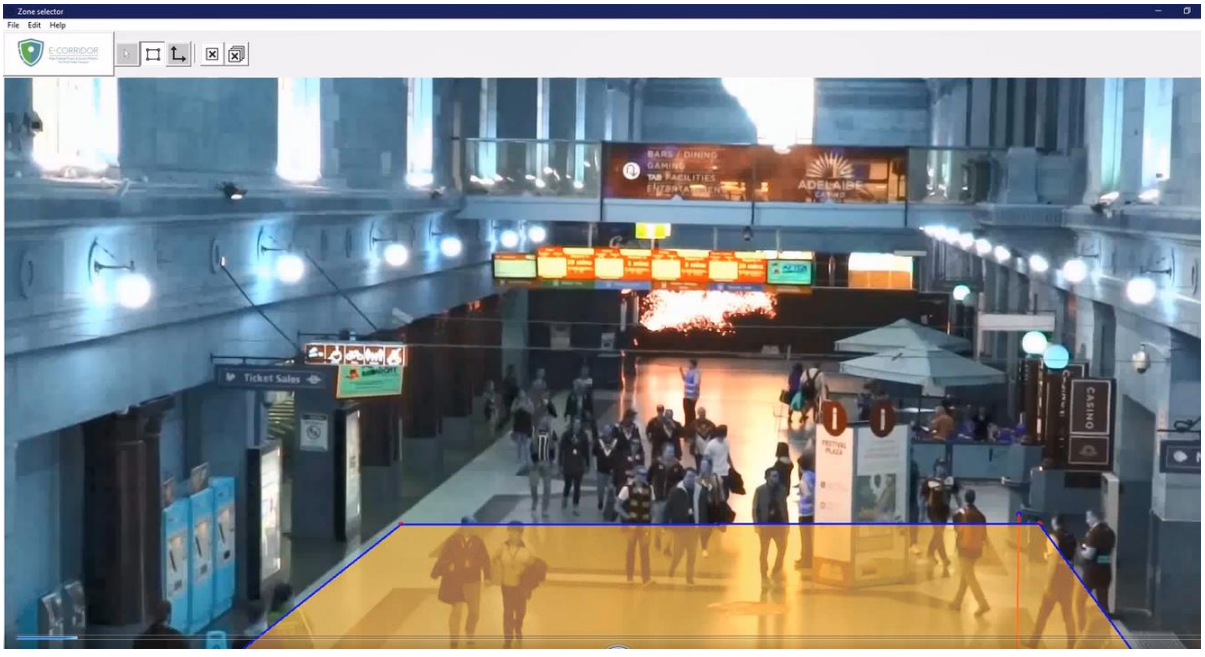

Figure 7 E-CORRIDOR app for the zone selector of the camera feed analysis

In output a few metrics are currently provided (see Figure 8), such as distance among passengers (to check the respect of the COVID-19 safe distance), the number of passengers in a given area (e.g., to open a new desk or install an additional kiosk if the area is often populated, see Figure 9), and an alert if a luggage is far from the corresponding passenger (e.g., to summon the security guard, see Figure 10).

```
(m): 5.9
(m): 1.34
(m): 1.49
(m): 1.26
(m): 1.29
(m): 1.35
7 11:04:05.938 DEBUG  Number of People In Zone 0: 4
7 11:04:05.943 DEBUG  Number of People In Zone 1: 5
7 11:04:05.943 DEBUG  Number of People In Zone 2: 4
7 11:04:05.943 DEBUG  ----------------------------------------
7 11:04:06.109 DEBUG  Number of People In Zone 0: 4
7 11:04:06.114 DEBUG  Number of People In Zone 1: 5
7 11:04:06.116 DEBUG  Number of People In Zone 2: 4
7 11:04:06.116 DEBUG  ----------------------------------------
(m): 0.93
(m): 1.01
(m): 6.61
(m): 7.05
(m): 5.9
(m): 1.34
```

Figure 8 Camera feed analysis example of two output metrics: number of people and distance (in meters)

Figure 9 Camera feed analysis – annotated and anonymized video with the overlay of the zones of interest

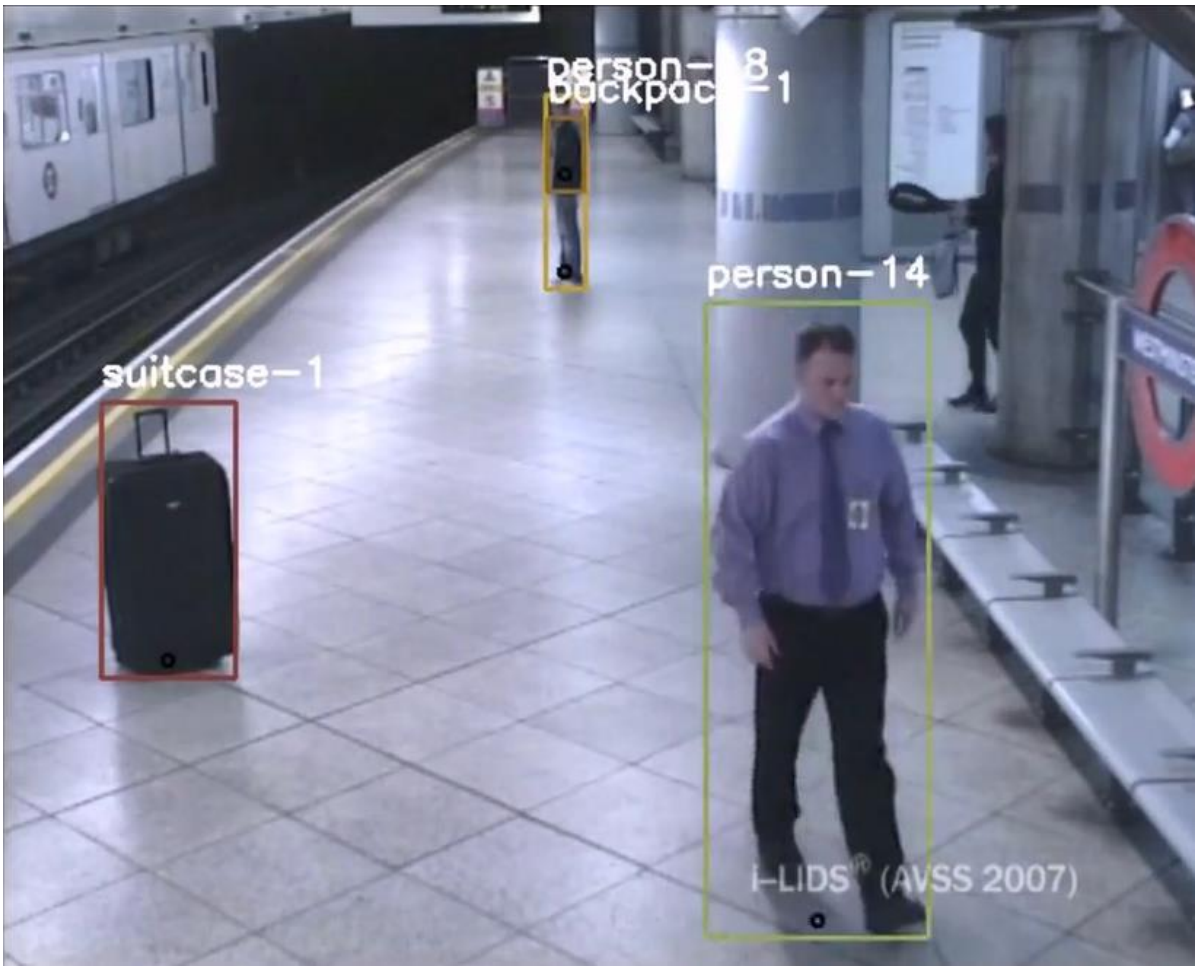

Figure 10 Camera feed analysis - identification of a left luggage

The component is fully integrated in the E-CORRIDOR framework and has been tested in conjunction with the face anonymization DMO and a realistic DSA. The experiments have been limited to a few publicly available videos, but a realistic setting emulating the presence of an IP camera has been recreated with a RaspberryPi, and the ZeroMQ library [6].

3.2.3. Gait Analysis

We developed a solution for continuous user authentication based on data collected from mobile devices. The component perform a gait analysis exploiting data from inertial sensors and a model built with a recurrent neural network (RNN) for a deep-learning based classification. At the current stage of implementation, the component is able to handle all the continuous authentication stages, starting from data collection to data pre-processing, classification, and policy enforcement. Also, we performed a set of real experiments to demonstrate the effectiveness and efficiency of the proposed framework. Currently, we are working to integrate this component into the E-CORRIDOR framework.

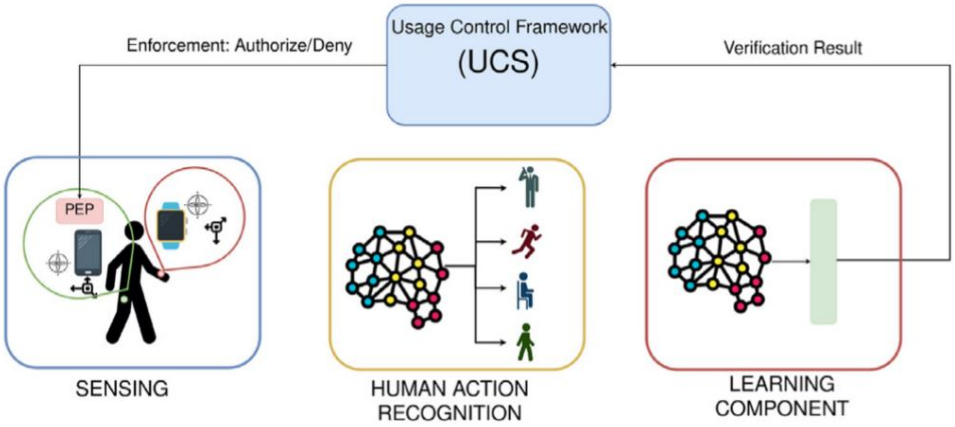

Figure 11 Overview of the gait analysis component

The component is composed of four modules (represented in Figure 11):

- sensing component: an Android application that gather inertial data information related to the user's movement.
- human activity recognition component (HAR): a deep learning network based on an RNN, able to analyze the data provided by the preprocessing components and infer the specific movement or action that the user is performing.
- user verification component (learning component): it performs an analysis on the data provided by the HAR to predict if the user performing the action is authorized.
- usage control component (UCS): implement the access control policy and evaluate the data coming from the user verification component to enforce the device control and authorization.

3.2.4. **Facial Recognition**

The component is constituted by a mobile app and a kiosk service. The first version of the currently deployed mobile application is designed using the Cordova framework [7] (based on HTML, CSS, and JavaScript) and supports different operating systems such as Android and iOS, even if the latter is not planned to be evaluated during the project execution. The communication between the applications and the servers is encrypted using TLS v1.3. On the mobile, the self-generated AES key is stored by using the Android keystore. The application displays the list of registered travels. At the time of writing this deliverable, the check-in can be performed online or offline through an encrypted QR-code to present to train-kiosk. The following subsections describe the two options in more details.

3.2.4.1. Offline data transfer

The offline data check-in foresees the encryption (with the RSA-OAEP, SHA-256 algorithm) of the user information with the public key of the kiosk. Figure 12 shows the generated encrypted QR-code.

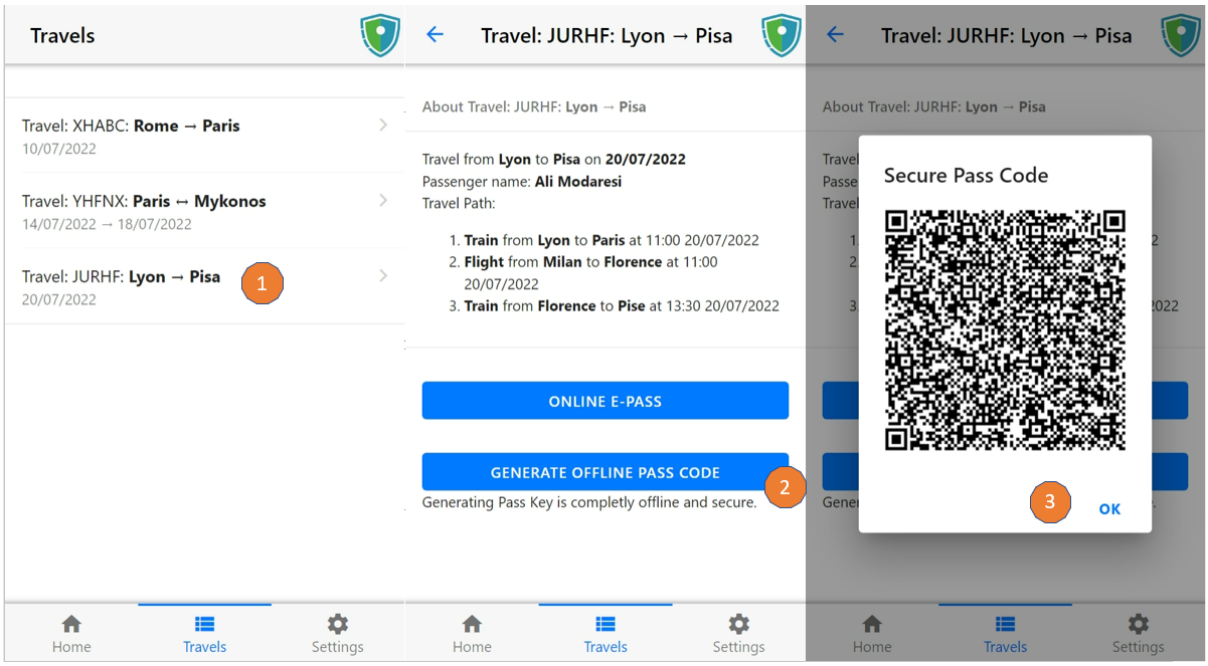

Figure 12 Offline check-in with secure QR-code

3.2.4.2. Online data transfer

To use the online check in, the passenger takes a picture of herself (specifically her face) while clearly holding her passport (or identity card), as presented in Figure 13. Finally, the passenger needs to agree on sharing this information with the infrastructure.

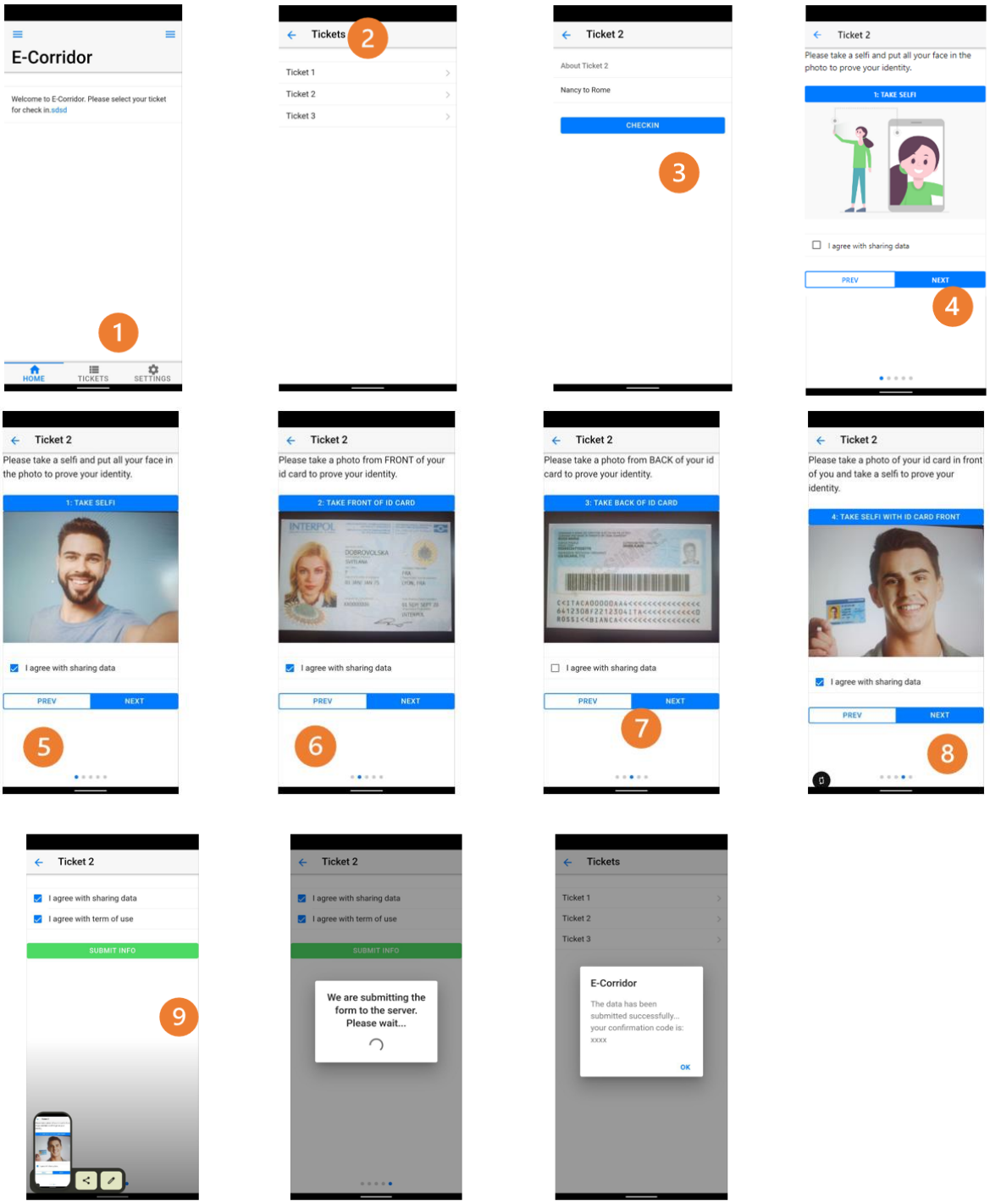

Figure 13 Online check-in

3.2.4.3. Kiosk Application at Train Station

In the train station an image of the passenger is collected for reference in subsequent recognitions. Therefore, we designed a kiosk interface that can read the information from the QR code generated by the mobile application (see Section 3.2.4.1). Then, the kiosk interface will capture a photo of the passenger and save it, in encrypted form on the local ISI of the kiosk. Figure 14, Figure 15 and Figure 16 briefly describe this workflow.

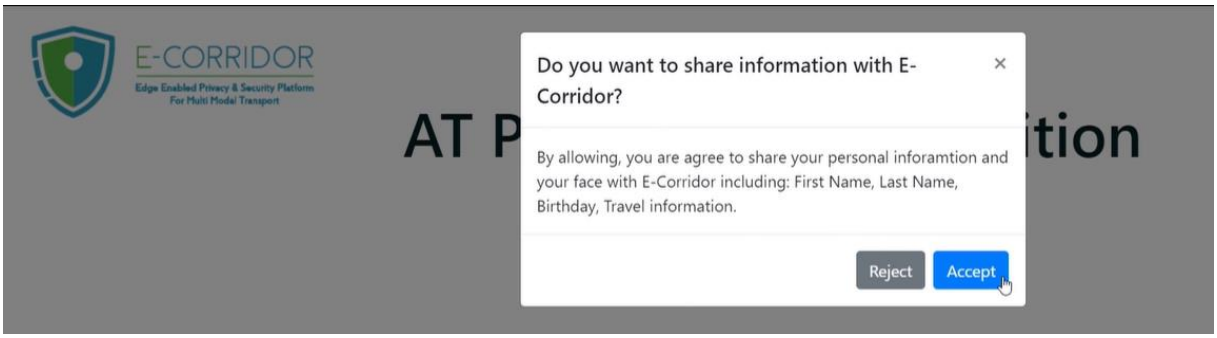

Figure 14 Consent form for sharing the passenger information with the train station kiosk

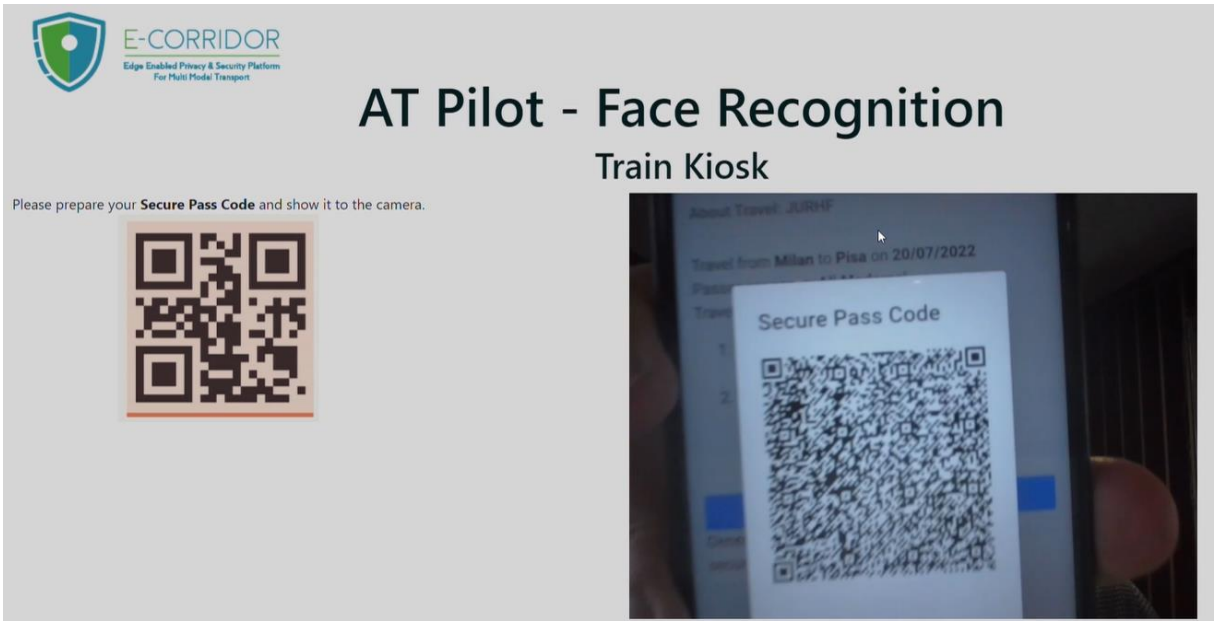

Figure 15 The train kiosk reading the passenger information from the QR code

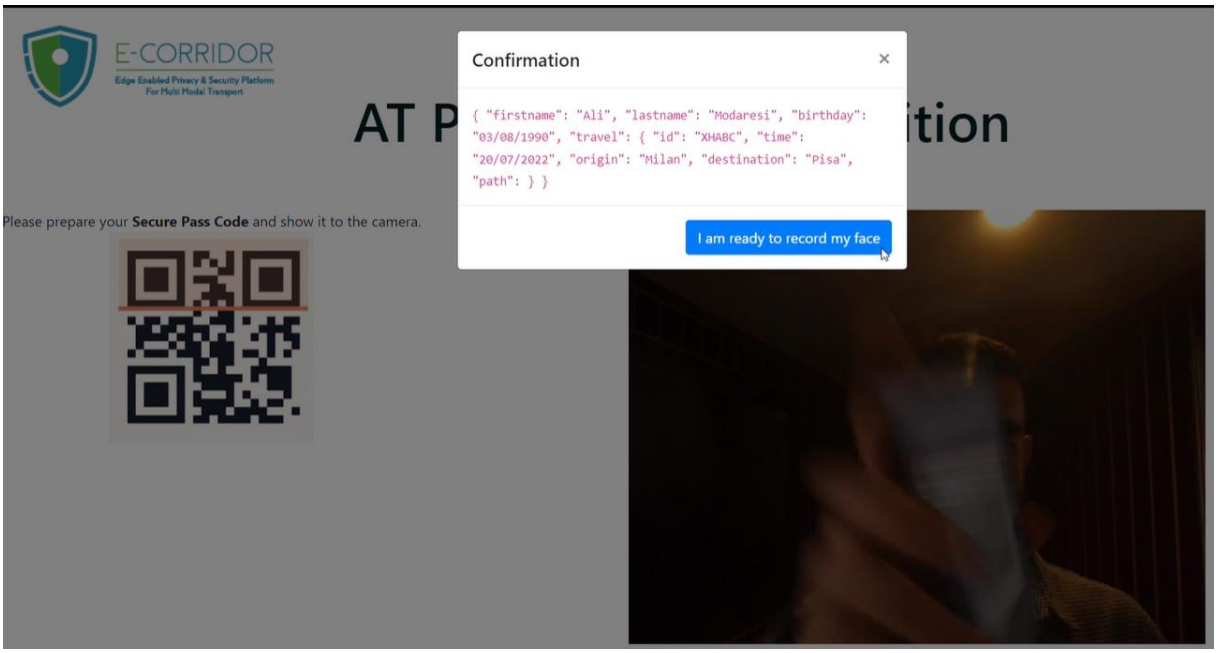

Figure 16 A message showing to the passenger the information read from the QR code

3.2.4.4. Kiosk Application at Airport Terminal

At this point, the passenger is enrolled and can use the kiosk in the airport terminal to perform the authentication based on the facial recognition. To preserve the privacy of other passengers accidentally passing in front of the camera, we blur the background. Examples are presented in Figure 17 and Figure 18.

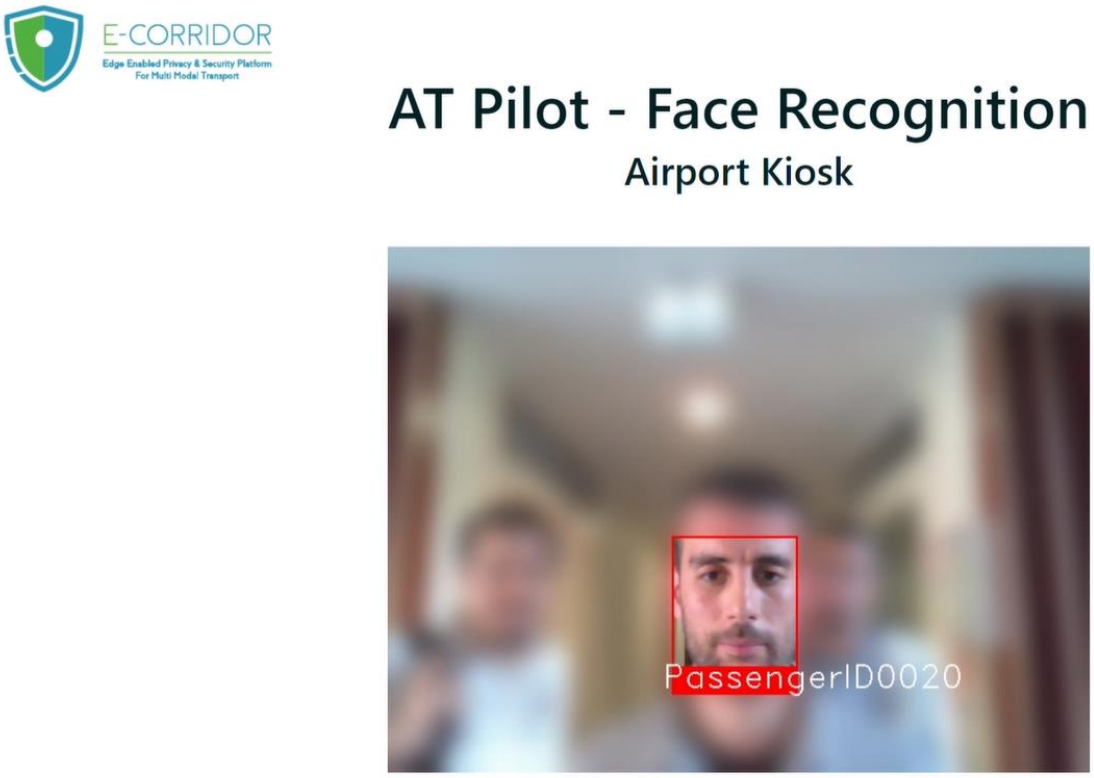

Figure 17 Passenger identification at the airport kiosk

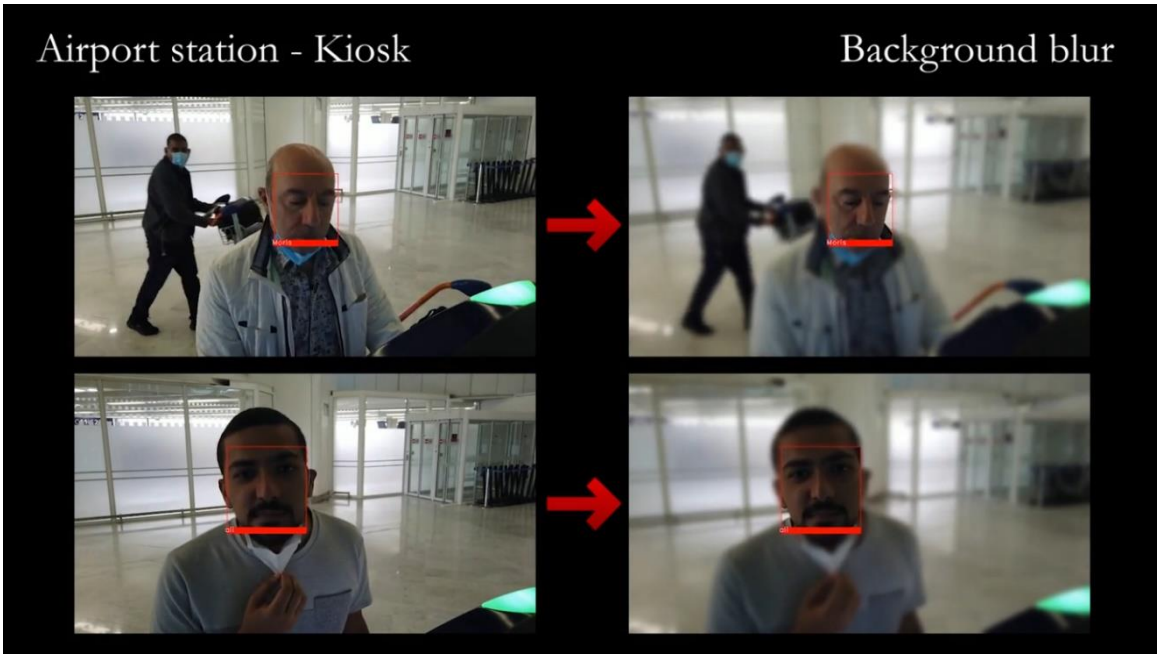

Figure 18 With and without the background blurring in the airport

3.2.5. Activity Recognition

The component has been implemented in Python and works connected with Intel RealSense RGB-D cameras. Tests have been performed in a lab setting recreated with a few cameras and researcher acting as passengers. The component can extract some features, e.g., clothes, to discern the different participants of the test. Moreover, by exploiting the depth information, the joints of the human body can be recognized and used to build a virtual skeleton. The set of activities currently considered include walking, walking with a bag, walking with a suitcase, sitting and standing.

3.2.6. Analysis of Sensitive Passenger Data

At M26, the APIs for FHE-based services have been implemented and their functioning tested. The integration in the E-CORRIDOR framework is in progress. We have implemented the authorization protocol, which is available at https://ecorridor-asi.iit.cnr.it:8443/swagger-ui.html. This protocol, described in Section 3.3.6, will make FHE-based services available in pilot environment.

In Figure 19, we encrypted the boarding pass number. When scanning this QR code, the device will get a ciphered URL and send the request to the E-CORRIDOR framework to check whether it is valid to access or not. This ciphertext is homomorphically encrypted.

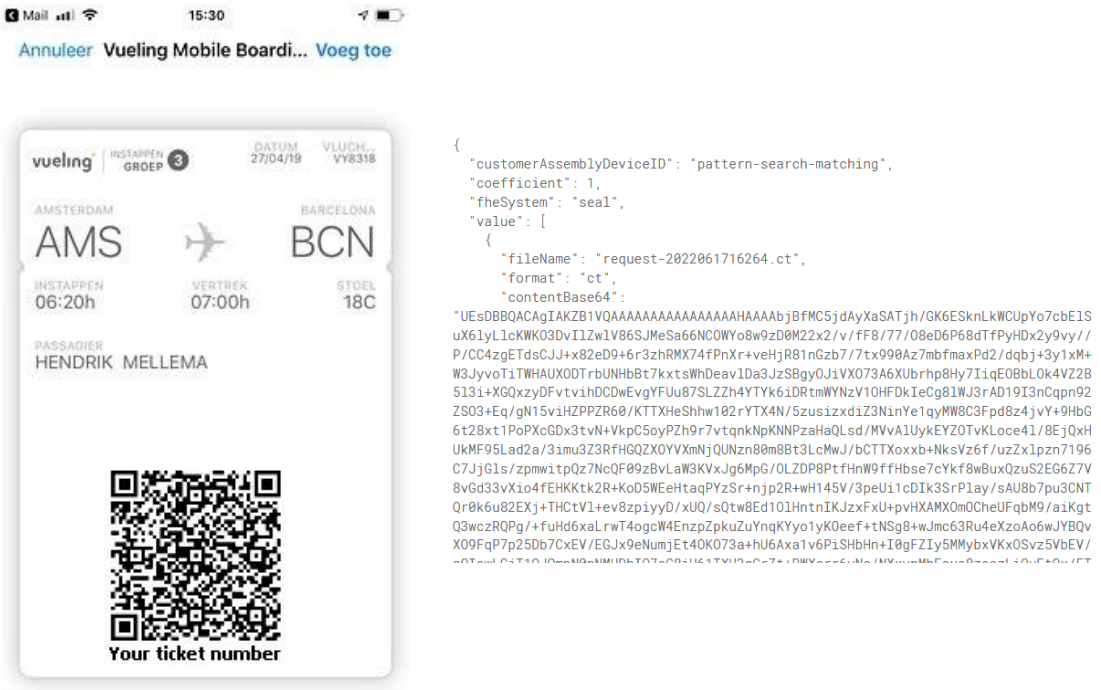

Figure 19 Ticket number encrypted with FHE, the content in the QR is the ciphered link

3.2.7. Multi-Factor Authentication

To perform the multi-factor authentication two main components are required: the engine and the context reasoner. The engine is in charge of composing the authentication analytics available in the IAI toolbox and has therefore been built starting from the IAI orchestrator API. It requires in input the definition of the authentication mechanisms used as part of the multi-factor process and shares the output of those with the context reasoning for further processing.

Currently we are able to run some test authentications and compose them by means of a simple JSON file. As not all the authentication solutions planned to be adopted in the AT pilot are integrated in the E-CORRIDOR framework yet, the communication interface has still to be refined and with it the API exposed by the engine and the format of the messages to/from the context reasoner.

3.2.7.1. Context Reasoning

The context reasoning will be used in conjunction with the multi-factor authentication to infer at runtime the quality of the performed process. Attributes that are currently considered by the reasoner include: body movement, attributes of clothing and baggage, luminosity, and current property of the environment (e.g., crowded area). All in all, the component will process the output of several other components such as the camera feed analysis, the activity recognition, the facial recognition and possibly the passenger localization. Once exposed in a common format, we will parse the output provided by each of these components and define an ontology for the exploited attributes.

3.2.8. **Federated Authentication**

The eIDAS-based federated authentication solution requires the deployment of all the components foreseen in the eIDAS framework (namely, service provider, identity provider and node). This extra effort is needed as only the member states can cover the role of integrator in a production environment. Moreover, as the information in the eIDAS platform includes sensitive data related to the digital identity of the European citizen, for the purpose of this project it would not be possible to work with the real environment.

Currently, we have re-created in our environment a setting with two member states able to exchange an authentication message. Next steps will require the extension of the basic attributes with some optional ones required by the pilot (e.g., the passport number) and the design of an eIDAS compatible service provider mimicking the passenger registration.

3.2.9. **Trusted Service Manager**

The TSM is a low-level security service providing strong security to upper layer services. In the AT pilot, we use it to instantiate the Trusted Sensor Network (TSN) to establish trust in the different sensor platforms of the various trust domains part of train station and airport. Being offered as a low-level security service, some of its features are in common with the already available eWallet solution instantiated for the S2C (smart cities and car sharing) pilot. The TSM is containerized, deployed in the E-CORRIDOR framework, and already configured with the respective TPM software libraries and TPM interfaces. These TPM interfaces are easily interchangeable and provided for: the TPM software simulator (in case a platform does not have the TPM hardware) and the TPM hardware device. Moreover, the current implementation can store the measured integrity values and has the correct Platform Configuration Register (PCR) policy templates ready.

Next steps foresee the deployment of the container on the sensor platforms of the AT pilot and their provisioning with keys, certificates, and policy instantiations for the correct integrity values. Moreover, a lightweight Public Key Infrastructure (PKI) between the sensor platforms and the E-CORRIDOR edge server will be built and the TPM-enabled TLS channel integrated.

3.2.10. **Interest-Cast of Airport Services**

At month 26 of the project, the application scenario in the AT pilot foresees passengers involved in a multimodal travel moving from, for instance, the train station to the airport. While waiting for her connecting flight, the passenger has some free time to spent to go to a restaurant. The

passenger can use her smartphone to run the *Interest-Cast of Airport Services* application, which uses the 2PC technique, to keep her data private. The app works considering two main actors:

- A service provider that advertises the services available in the airport.
- A prosumer that is represented by a passenger during his/her multimodal travel.

When running the service, both parties involved wish to keep their data private. In particular, the offered service will make use of the prosumers' interests. Considering the above scenario, the service provider hosted at the airport side will allow the passenger to know all the restaurants matching the passengers' interests while keeping all data used in the service totally private.

At the current state, a passenger can run this service using the dedicated app available for Android smartphones. On the airport side, a kiosk has been emulated through a RaspberryPi 4 running Android OS in which all information related to the restaurants is available.

3.3. *Workflows*

The workflows describing the interaction of the components with the E-CORRIDOR framework and the AT pilot environment are presented. In case of the camera feed analysis, being the component already fully integrated in the framework, a DSA policy invoking a privacy preserving DMO is also briefly described.

3.3.1. Passenger Localization

This component aims at helping the passenger reaching her relevant PoIs merging the information gathered from the PNR and the FIDS. Once the environment will be equipped with conveniently placed BLE beacons, the mobile app on the passenger's device will be able to estimate her position and generate a path to reach the next PoIs. Furthermore, if the passenger agrees, she may receive suggestions considering time-constraints and preferences, interacting with the businesses present on the airport and train premises.

While the localization is computed on the analytics locally installed on the smartphone, the information about the passenger journey and the related flight status (i.e., the above-mentioned PNR and FIDS) will be collected through the E-CORRIDOR framework.

The scenario is similar in case of PRM passenger, but since the passenger will be using equipment provided by the airport, the localization process will be bi-directional, i.e., the device installed on the wheelchair will receive information from the beacons as well as transmit messages to the beacons with the dual purpose of improving the position estimation and informing the PRM assistants.

Moreover, by using the same solution the transport operator can let the beacons scan its surrounding for active Bluetooth devices and, without collecting any data from any of these devices, estimate the amount of people under its coverage and therefore provide a rough estimate of the passenger flow in the airport.

An example of these scenarios and the related communications between passengers and beacons is presented in Figure 20.

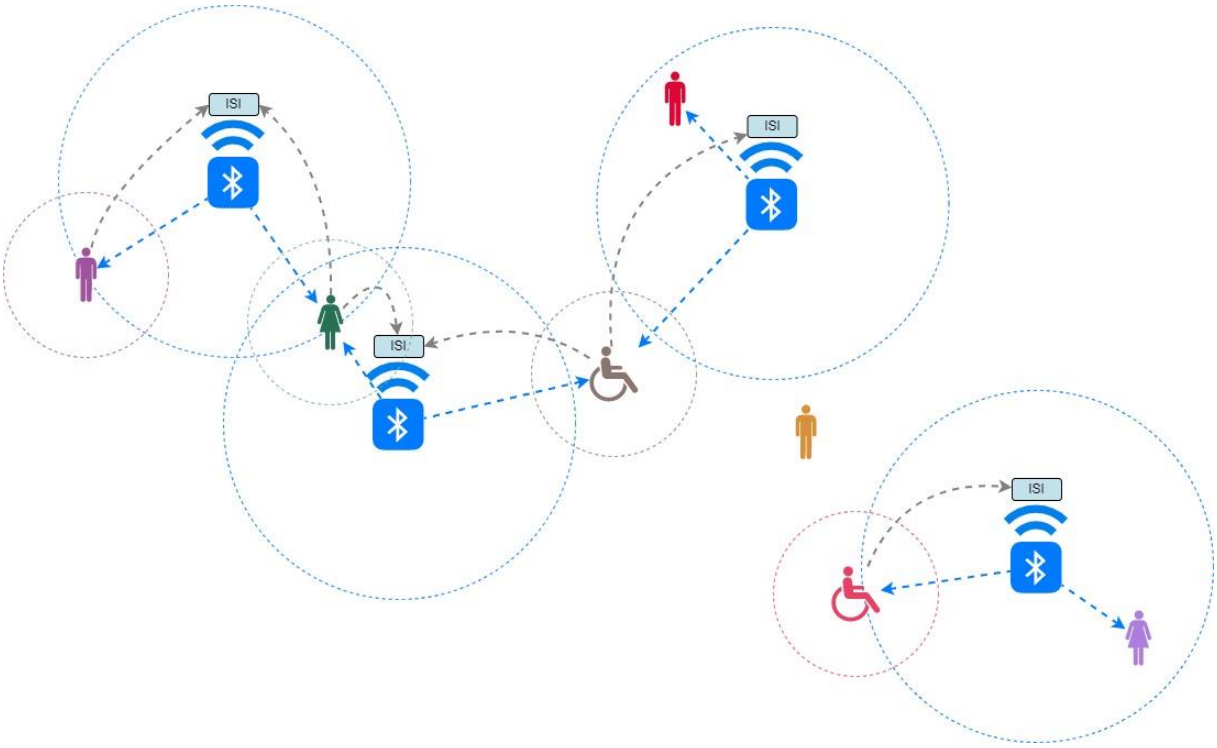

Figure 20 Example of messages exchanged between passengers and BLE beacons.

As no extra personal information about the passenger is collected or shared with the infrastructure, at the time of writing this deliverable, we don't foresee the need of any DMOs. A DSAs will be instead used by the transport service operators to connect and share the information about the FIDS and the reservations in the ISI.

3.3.2. Camera Feed Analysis

To let the analytics perform the analysis, IP-based cameras deployed in the train station and airport terminals are connected to the E-CORRIDOR framework. The connector is in charge of chunking the video stream and storing each block in the ISI. As the video may contain information that are sensitive (i.e., that could potentially identify a passenger) and not needed for the purpose of this analytics, it is required that domain expert along with privacy and legal officers define an appropriate DSA. In such a DSA are specified, among the others, rules about data creation, access, use and retention. In particular, the data access can exploit the face anonymization DMO designed to preserve the privacy of the passengers while allowing the correct execution of the analytics. An example of the DSA designed by means of the DSA editor and enforced through the ISI is reported in Figure 21. To avoid storing the not anonymized video in a central node some pre-processing can be executed locally.

Figure 21 Camera feed analytics DSA

Once the data are stored in the ISI, the analytics can be executed making its results available as regulated by the DSA. At the time of writing this report the workflow has been deployed with the support of a RaspberryPi for the local processing and connected to the AT pilot testing Virtual Machine (*ecorridor-at.iit.cnr.it*). The "move" operation has been currently emulated as not yet fully supported by the E-CORRIDOR framework. Figure 22 pictorially represents the workflow of the camera feed analytics.

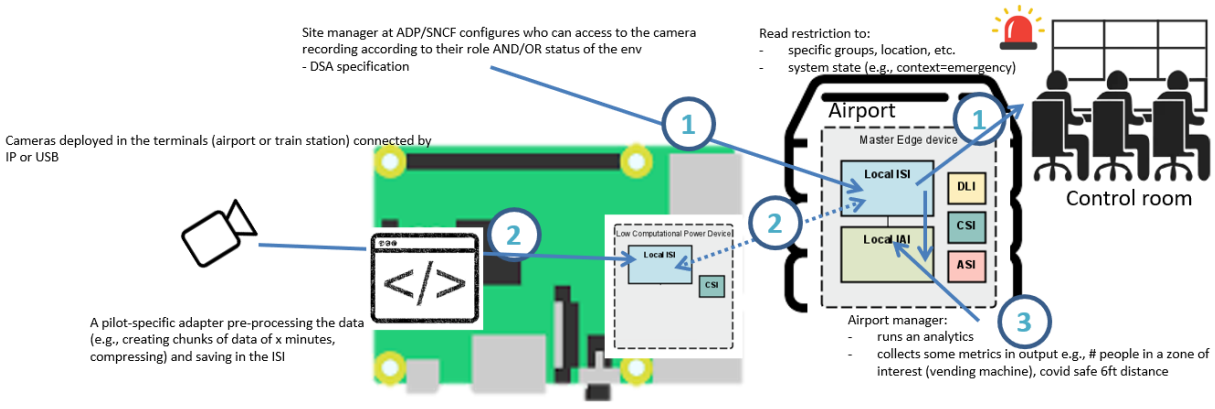

Figure 22 Camera feed analytics workflow

3.3.3. Gait Analysis

The continuous authentication allows to verify a user's identity continuously and in real-time, allowing a seamless access to the service for authorized users. Once integrated in the E-CORRIDOR framework, the gait analysis will contribute to analyze data coming from the passengers' smartphones opting to use the E-CORRIDOR app for such a kind of authentication process. The gait model built during the enrollment will be securely stored in the ISI. Once the

passenger is in the airport and train station, he/she will be prompted to walk in a "smart tunnel". Thus, the gait analysis will be able to retrieve the original model and compare it against the runtime data.

3.3.4. Facial Recognition

This component aims at authenticating the passenger in a seamless manner despite the heterogeneity of the access control environments adopted by the train station and airport terminals (even using different paper-based identity verifications). We consider an environment with cameras placed strategically in the path performed by the passengers. Examples of these touchpoints are the physical gate to enter in the train platform area or the baggage drop desk in the airport. The cameras can record a short video of the passenger and transmit this to the edge server for processing according to the defined DSA. A DMO related to this component, blurring the image behind the close-up face, can be included in the DSA to improve the privacy of all the passengers. By executing the same process at different touchpoints, it is possible to re-identify the passenger without affecting her/his normal crossing.

3.3.5. Activity Recognition

This component aims to anonymously recognize the activity of the passenger when crossing the different touch points. The workflow is similar to the one discussed for the face recognition. At a given touch point, the cameras will record a video of the passenger walking towards the touch point. This video is automatically transformed to a set of moving skeleton frames and stored in the ISI. The activity recognition component will retrieve each segment of these "skeleton frames" in order to recognize the passenger activity and its quality. A high-level representation of the workflow while the passenger moves around the different touchpoint and the extracted information are reported in Figure 23.

Figure 23 High-level representation of the workflow in the activity recognition

3.3.6. Analysis of Sensitive Passenger Data

The ciphertext containing the sensitive passenger data is available from a QR code in the boarding pass of a passenger. Also, a list of valid boarding passes is stored in encrypted format as soon as passengers book their flights. When the passenger scans the QR code, the device will get the ciphered URL and send the request to the E-CORRIDOR framework to check whether it is valid to access or not. A Boolean answer is returned by the component.

3.3.7. Multi-Factor Authentication

Transportation service providers are expected to define a set of multi-factor authentication mechanisms they want to make available to their passengers to cover the security requirements of different touchpoints as well as to provide more flexibility to the passengers for their authentication. Interactions with several single-factor authentication analytics are therefore expected such as gait analysis and facial recognition.

Initially, the providers will define the set of allowed authentication schemas in a simple JSON format. Then the passengers will invoke and make use any of those schemas. On the backend, and transparently to the passenger, the engine will invoke each analytics and interact with the context reasoner. As final step the transportation service provider and the passenger are informed about the result of the overall authentication process.

3.3.8. Federated Authentication

Once integrated, it is expected that a service requiring the passenger authentication in the AT pilot (e.g., the booking service) will be exposed as a service provider in the eIDAS framework. Thanks to such a solution the transportation service provider will be able to get the information related to the passenger's identity validated by a member state.

As this will be exposed as a service by the ASI, the addition of further service provider offers will be simplified.

3.3.9. Trusted Service Manager

The TSM-enabled Trusted Sensor Network (TSN), its workflow, and how it is integrated into the E-CORRIDOR framework are depicted in Figure 24. The system consists of the sensor platforms of the different mobility providers, e.g., train and airport, that send their sensor data to the platform (1) and the E-CORRIDOR edge server. The sensor platforms are equipped with the TSM and its TPM that instantiates a hardware isolation layer to the potentially untrusted host (2). It stores identity keys and measures the platform integrity during the boot of the platform (3). The integrity measurements are stored in the Platform Configuration Registers (PCRs) of the TPM. The identity keys are asymmetric keys used to establish secured TLS channels between the sensor platform and the E-CORRIDOR edge server (4). The identity keys are bound to the platform state via a specific authorization policy (*TPM2_PolicyPCR*) and are only unlocked if the platform state represented by the PCRs is benign. Thus, implicit attestation is implemented since a TLS channel can only be established successfully if the sensor platform is trusted. No additional overhead is created for integrity value transmission and verification.

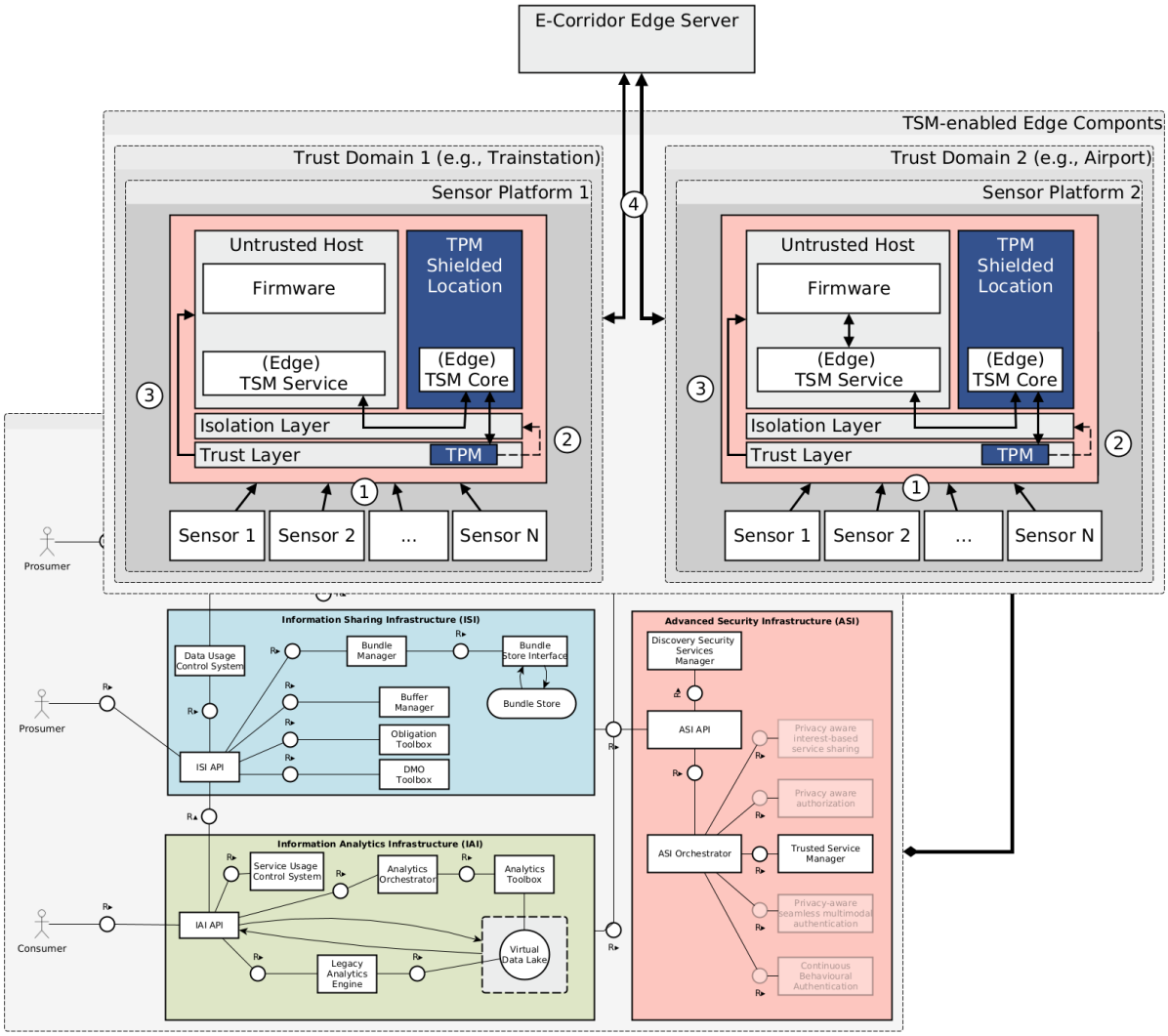

Figure 24 TSM instantiation for the Trusted Sensor Network

3.3.10. Interest-Cast of Airport Services

The interest-cast of airport services and, in particular, its application for the restaurant scenario involves the parameters reported in Table 1.

Table 1 Set of interests that a passenger can consider, with examples

Parameter	Description	Value types (examples)
Menu	It considers the type of restaurant	Italian, American, Indian, Japanese
Location	How far from the passenger position	In a range of 200 meters
Cost	It expresses the type of restaurant in terms of costs. For instance, a fast-food or an expensive restaurant	Cheap, expensive
Time to wait	It approximately indicates the maximum amount of time to wait until the passenger is served	Less than 10 minutes

If interested in adopting the service, the passenger has to set up those parameters before running the service. For each interest, a passenger can provide her preferences, and these will be matched in a private manner with the offers available in the kiosk.

In Figure 25, we show an interaction between a self-service kiosk in the airport and the passenger's smartphone. All data related to the passenger's interests and the available restaurants are first stored in the local ISI. Then, when the analytics that involves the 2PC–based service sharing component is running, the 2PC module available in the ASI subsystem is triggered.

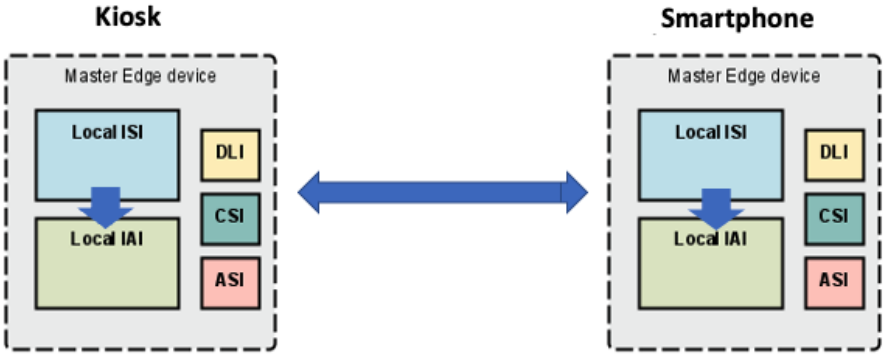

Figure 25 Interest-based 2PC service between a Kiosk and Smartphone

At the time of writing this document, the analytics works as a standalone component and its integration with the AT Pilot and the E-CORRIDOR framework is in progress. The current implementation is written in Java, and it is based on CBMC-GC tool [8]. It is composed of two main parts: the compiler that translates functions written in C language into garbled circuits, and the interpreter that can execute compiled functions [9]. Thus, CBMC-GC offers a very flexible high-level language that allows developers to express a wider range of functions compared to simpler techniques, which for instance only focus on simple private matching operations. To work with passengers' smartphones, we have extended and adapted CBMC- GC to work on the Android operating system (OS).

In Figure 26 and Figure 27, we show the app customized to work in a standalone fashion for the AT pilot. With the app, a passenger will be able to get a list of restaurants based on his/her preferences customized through the app itself. Once the passenger has indicated the preferences, he/she will get the list of restaurants that will be selected according to the preferences in a complete privacy-preserving manner, i.e., the passengers' preferences will not be disclosed with the service provider and vice versa.

Figure 26 2PC – based service main window

Figure 27 2PC– based service price customization

Figure 28 and Figure 29 refer to the app running at the kiosk side and, in the specific case Figure 29 shows the restaurants that matches the interests expressed by the passenger with the values available at the kiosk side. The restaurants are ranked considering the number of matches that the restaurants have with the passenger's interests. So, the two restaurants showed in Figure 29 are the ones that have the highest number of matches considering the parameters reported in Table 1.

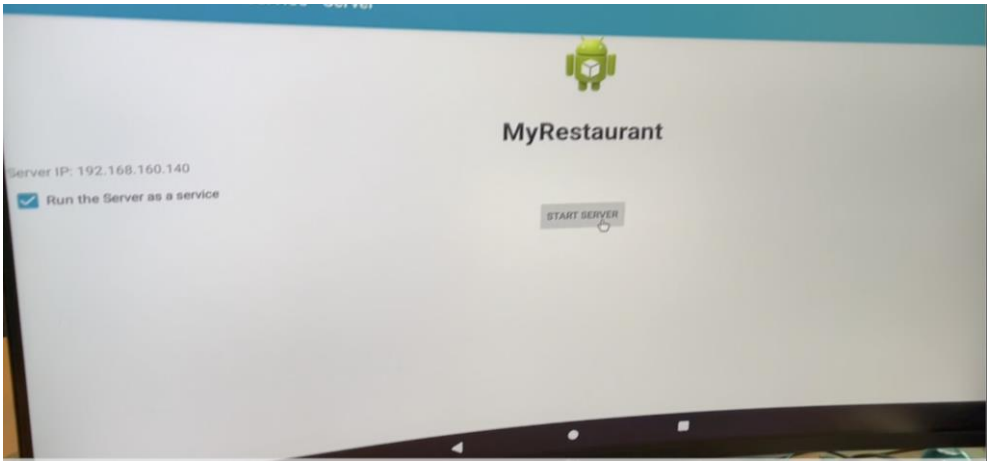

Figure 28 Interest-Cast of Airport Services on the kiosk

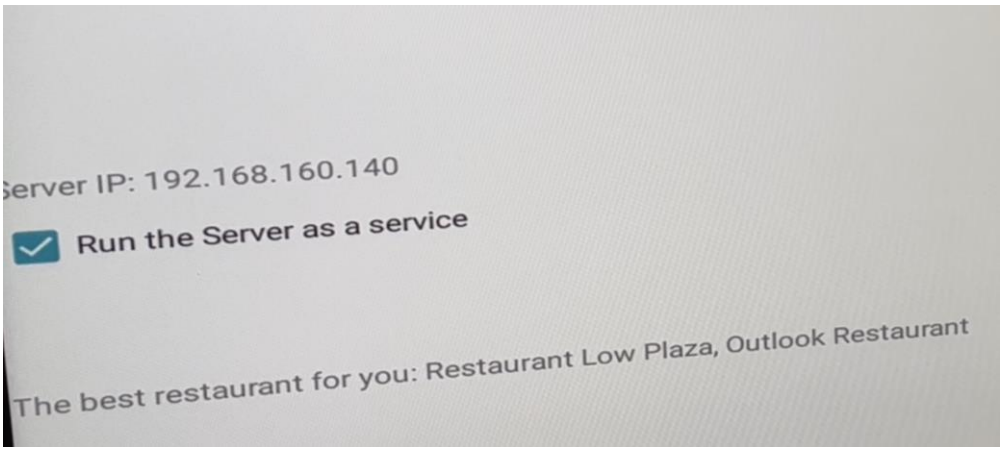

Figure 29 Interest-Cast of Airport Services result on the kiosk

4. First Experimental Evaluation

This section first describes the data used (or planned to be used) for the test and validation phases, and then defines a few test cases useful to validate the functioning of each component.

4.1. *Data Sources*

4.1.1. Passenger Localization

As previously mentioned, this component will only leverage data shared by the transport service providers through connectors with their reservation and information systems. The only additional data processed by the component will be the messages shared by each beacon with the related signal strength (RSSI). In testing phase, we will also collect the correct position of the passengers (from researchers working in the lab) to better refine the localization algorithm. This additional information on the real position will be used only for testing purposes and not be part of the component that will be deployed on the E-CORRIDOR framework.

Passenger localization data		Source
Test	*[beacon_id, beacon_message, RSSI, real_position]*	*Data collected in the lab from researchers with ground truth*
Validation	*[beacon_id, beacon_message, RSSI]*	*Real data from researchers' smartphones in a confined space of the AT pilot*

4.1.2. Camera Feed Analysis

During this testing phase, we considered the presence of different publicly available datasets collected from a setting similar to ours. The public videos (from the Multiple Object Tracking Benchmark – MOT20 [10] and the Advanced Video and Signal based surveillance IEEE AVSS 2007 [11]) contain passengers moving around in a train station. Potentially, additional public videos will be included in the test suite. For the final validation, we will evaluate the possibility of using the Genetec Omnicast solution [12] adopted in the AT pilot and designing a connector for the corresponding API. If that will be realized, the video will come only from a restricted environment set-up by the pilot for validation purposes and the role of the passengers will be performed by researchers and collaborators in the E-CORRIDOR project.

Camera feed analysis data		Source
Test	*[video]*	*Data from public sources*
Validation	*[video]*	*Real data with researchers acting as passengers in a confined space of the AT pilot validation environment.*

4.1.3. Gait Analysis

We performed several experiments to verify effectiveness and efficiency of the solutions. In particular, we considered three public activity recognition datasets, namely UCI-HAR, HMOG and WISDM.

The UCI-HAR dataset [13] contains data provided by 30 volunteers within an age range of 19-48 years. Each person performed six different activities, walking, walking upstairs and

downstairs, sitting, standing, and laying. The activities are measured through a smartphone located on the waist. The HMOG dataset [14] [15] includes recordings from the accelerometer, gyroscope, and magnetometer from 100 smartphone users within 24 different sessions. The activities considered for our experiments are related to reading and writing when the user is walking. Also, the WISDM dataset [16] collect data from the accelerometer and gyroscope sensors of a smartphone but also from a smartwatch. The data comes from 51 users who performed 18 diverse daily activities such as walking, jogging, typing and various eating activities.

It is worth to remark that this component proposes a more experimental solution than other biometric-based authentication mechanisms considered in the project (e.g., the facial recognition).

4.1.4. Face Recognition

Face recognition analytic exploits two main input: (i) an image as a ground-truth, and (ii) a video recorded during the passenger at a kiosk. The image used for ground-truth is constituted by a selfie of the passenger with his/her identity document. The processing at the edge compares the face of the passenger with the one included in the identity document. The video recorded at the train station or airport are checked for liveness and used for the re-identification.

Facial recognition data		Source
Test	*[video, image]*	*Real data with researchers acting as passengers in the lab, including some stress scenarios (e.g., multiple passengers near the camera, picture in place of the real person)*
Validation	*[video, image]*	*Real data with researchers acting as passengers in a confined space of the AT pilot validation environment.*

4.1.5. Activity Recognition

As we are not aware of any publicly available dataset useful for our scenario, we will record videos with researchers part of the project performing the role of the passengers. The following test and the corresponding video recordings are planned to be used:

- laboratory test, single user: in this test, we consider only one user in the video stream in all our user identification systems. This test will be repeated with three different users in three different locations.
- laboratory test, multiple user: we consider multiple users (e.g., three and five) in video streams collected in our research lab. This test will be repeated with three different groups of users in three different locations.
- airport test, multiple user: as in the previous test but repeated with three different groups of users in three areas of the airport.

4.1.6. Analysis of Sensitive Passenger Data

The component handles sensitive data, such as passenger name and surname and possibly information related to the PRM passenger and the expressed SSR. Therefore, all the experiments will include synthetic data generated in the lab for testing and validation purposes. Further tests will consider the time needed to execute our FHE-based solution in the travel process to verify that the solution will be accepted when deployed in a realistic setting.

Analysis of Sensitive Passenger data		Source
Test	*Passenger details including personal details and ticket info*	*Synthetic data generated to mimic the dataset collected by the airlines*
Validation	*Passenger details including personal details and ticket info*	*Synthetic data generated to mimic the dataset collected by the airlines*

4.1.7. Interest-Cast of Airport Services

At month 26, the main goal of the evaluation step is to verify the correctness of the app and its first integration with the AT Pilot and its requirements. Thus, the Interest-Cast of Airport Services app was evaluated in the lab using synthetic data to show the correct working of the service. At the provider side, data were generated in the lab to express the values for the restaurants. Instead, for the passenger role, data were randomly generated, to express the preference of the passenger.

Interest-Cast of Airport Services		Source
Test	*Passengers' interests and restaurant values*	*Synthetic data generated in the lab from researchers*
Validation	*Passengers' interests and restaurant values*	*Data collected in the lab from researchers and from the emulated reservation system*

4.1.8. ASI components

Components part of the ASI do not directly process data but are rather meant to provide the building blocks for advanced security solutions.

- Multi-factor Authentication: it is configured through a simple JSON file. To ensure the privacy, the output generated by the single authentications are in the form of tokens rather than raw data.
- Context Reasoning: only attributes extracted and exposed by other components will be processed.
- Federated Authentication: a set of test/not-real identities will be added to the identity provider and used for validating the workflow (motivations for not using real identities were discussed in Section 3.2.8).
- Trusted Service Manager: it is a security module not processing the data. Keys are generated for the deployment/validation.

4.2. *Tests Cases for Validation*

4.2.1. Passenger Localization

Test Id: TC_PL_1 – Beacon messages	Component: Passenger localization
Description	Ensure the correct generation and broadcasting of the beacon messages.
Input	Set of parameters to correctly configure the beacon (coordinates and beacon tag).

Expected Output	The correctly generated BLE beacon and the related shared message.
Status & Results	[Test successful]: In the lab with smartphone and RaspberryPis configured as beacons. The beacons generate and send correct BLE messages based on their position. We are currently able to generate both iBeacon and Eddystone beacons.
Final Validation	Using the specific beacons deployed on the airport premises.

Test Id: TC_PL_2 - Localization	**Component: Passenger localization**
Description	Ensure the correct localization estimation of the passenger based on different BLE beacon configurations. The same test can be used for the PRM scenario, augmented with the localization messages shared by the PRM-supporting equipment.
Input	Set of messages coming from a different number of BLE beacons.
Expected Output	The estimated position of the passenger.
Final Validation	Setup with beacons in the airport premises and representing a few points of interest.
Status & Results	[Not performed yet at M26]

Test Id: TC_PL_3 - Path generation	**Component: Passenger localization**
Description	Ensure the path generation for the passenger by knowing the information related to her journey.
Input	Set of messages coming from different BLE beacons, PNR and FIDS-related information.
Expected Output	A path the passenger may follow to reach her next touchpoint based on travel details and current location.
Final Validation	Integration with the PNR and FIDS information from simulated systems deployed in the airport.
Status & Results	[Not performed yet at M26]

Test Id: TC_PL_4 - Flow estimation	**Component: Passenger localization**
Description	Flow estimation based on the number of devices in the proximity of each BLE beacon.
Input	Set of RSSI values in the proximity of BLE beacons.
Expected Output	An estimate of the passengers in the proximity of the BLE beacon.
Final Validation	Using the specific beacons deployed on the airport premises.
Status & Results	[Not performed yet at M26]

4.2.2. Camera Feed Analysis

Test Id: TC_CFA_1 – Passenger identification	Component: Camera feed analysis
Description	Ensure the tracking of the passengers.
Input	Videos with passengers moving in the airport/train station.
Expected Output	Annotated video with bounding boxes around each passenger while moving.
Status & Results	[Test successful]: with the public videos we are able to identify and (anonymously) track the passengers in the scene.
Final Validation	Setting recreated in the AT pilot labs.

Test Id: TC_CFA_2 – Object identification	Component: Camera feed analysis
Description	Identify the different relevant objects in the scene (e.g., luggage).
Input	Videos with passengers carrying their luggage.
Expected Output	Annotated video with the kind of luggage (e.g., backpack, trolley).
Status & Results	[Test successful]: with the public videos we are able to identify several kinds of luggage.
Final Validation	Setting recreated in the AT pilot labs.

Test Id: TC_CFA_3 – Metrics extraction	Component: Camera feed analysis
Description	Extract relevant metrics from the analyzed video.
Input	Videos with passengers moving in the station carrying their luggage and area of interest(s).
Expected Output	Number of people in each area along with their distance from each other.
Status & Results	[Test successful]: with the public video we are able to extract and print on the console the corresponding metrics.
Final Validation	Setting recreated in the AT pilot labs and output metrics saved in the ISI (e.g., in JSON format).

4.2.3. Gait Analysis

Test Id: TC_GA_1 – Deep Learning model evaluation	Component: Gait Analysis
Description	Evaluate the accuracy of the Deep Learning (DL) models when provided users data
Input	Inertial sensors data collected from smartphones and smartwatches, describing the movements of the users

Expected Output	DL model able to identify the users, and classify correctly the samples
Status & Results	[Test successful]: we achieved 96-98% of accuracy on the different test sets
Final Validation	Integrating the framework and test on real-time data

Test Id: TC_GA_2 – Verification time	**Component: Gait Analysis**
Description	Evaluate the computation time to prove the feasibility of the real-time authorization control
Input	Sensor measurements and time information
Expected Output	The time required to provide the authorization decision
Final Validation	With framework integrated and real-time (emulation) of data.
Status & Results	[Not performed yet at M26]

4.2.4. Facial Recognition

Test Id: TC_FR_1 – Offline Registration of Multimodal Journey	**Component: Facial recognition**
Description	This test is used to evaluate if the user is able to generate a QR code from the mobile app. This will be used in the offline check-in when the passenger arrives at train station or airport terminal
Input	Valid booking data
Expected Output	QR code
Status & Results	[Test successful]: test in the lab with the QR code used by the kiosk web app emulator.
Final Validation	QR code read in a setting recreated in the AT pilot labs.

Test Id: TC_FR_2 – Face Video Automatic Recording	**Component: Facial recognition**
Description	Automatic recording of the video on the touchpoint only if relevant for the facial recognition (i.e., not recording when there is no passenger or when the passenger is not looking at the camera)
Input	Video
Expected Output	Video useful for the facial recognition analytics
Final Validation	Using the kiosk emulators deployed in the airport premises.
Status & Results	[Not performed yet at M26]

Test Id: TC_FR_3 – Fake Faces Detection	Component: Facial recognition
Description	Detect the presence of a real person in front of a camera. It tests the functioning of the liveness module used in the component.
Input	Video
Expected Output	Boolean value representing the presence of a person
Final Validation	Using the kiosk emulators deployed in the airport premises.
Status & Results	[Not performed yet at M26]

4.2.5. Activity Recognition

Test Id: TC_AR_1 – Classification of the activity	Component: Activity recognition
Description	Identify the person and classify the performed activity against a set of actions relevant for the domain (e.g., walking with some luggage, standing)
Input	Video
Expected Output	String describing the performed activity
Final Validation	Setting in the lab.
Status & Results	[Not performed yet at M26]

Test Id: TC_AR_2 – Multi-camera setting	Component: Activity recognition
Description	Classify the performed activity from multiple camera streams covering the same area from different points of view.
Input	Multiple video streams
Expected Output	String describing the performed activity
Final Validation	Multi-camera setting in the lab and airport premises.
Status & Results	[Not performed yet at M26]

4.2.6. Analysis of Sensitive Passenger Data

Test Id: TC_SD_1 – Homomorphic encryption	Component: Analysis of sensitive passenger data
Description	Verify the presence of the booking in the set of valid entries
Input	A set of strings describing the passenger information entered for the booking
Expected Output	Boolean value describing if the entry was present in the list stored in the ISI
Final Validation	Call the FHE service offered in the ASI with an encrypted booking information and compute over the data in the ISI

Status & Results	[Not performed yet at M26]

Test Id: TC_SD_2 – Performance impact	**Component: Analysis of sensitive passenger data**
Description	Understand the performance impact of the FHE solution
Input	Multiple passengers verifying their data in parallel
Expected Output	Processing time
Final Validation	Data processed on a central node potentially supporting multiple instances of the FHE service.
Status & Results	[Not performed yet at M26]

4.2.7. Multi-Factor Authentication

Test Id: TC_MFA_1 – Composition of authentication solutions	**Component: Multi-factor Authentication**
Description	Combine multiple authentication analytics in the IAI toolbox.
Input	Configuration file with the desired composition of the analytics.
Expected Output	Correct execution of the specified analytics while respecting the defined serial/parallel execution.
Status & Results	[Test successful]: only with test authentication analytics.
Final Validation	With the final version of the authentication analytics integrated in the AT pilot.

Test Id: TC_MFA_2 – Quantitative analysis of the final authentication process	**Component: Multi-factor Authentication**
Description	Evaluate the results of the MFA.
Input	MFA schema, single-factor authentication results and passenger performing the MFA.
Expected Output	Message describing the quality of the resulting MFA.
Final Validation	With the final version of the authentication analytics integrated in the AT pilot and the running contextual analysis.
Status & Results	[Not performed yet at M26]

4.2.8. Federated Authentication

Test Id: TC_FA_1 – Instantiation of eIDAS	**Component: Federated authentication**
Description	Evaluate the deployment of the eIDAS framework with two member states.
Input	Digital identities included in the identity provider.

Expected Output	SAML message describing the performed authentication.
Status & Results	[Test successful]: two member states emulated on the same machine
Final Validation	Two different member states simulated hosted on different server (distributed deployment).

Test Id: TC_FA_2 – Attribute extension	**Component: Federated authentication**
Description	Test the exchange of the optional attributes related to the travel domain.
Input	Digital identities included in the identity provider with additional attributes (e.g., passport number).
Expected Output	SAML authentication message including the optional attributes.
Final Validation	Two different member states simulated.
Status & Results	[Not performed yet at M26]

Test Id: TC_FA_3 – Service provider integration	**Component: Federated authentication**
Description	Evaluate the integration of the eIDAS with a service offered to the passenger by the transportation service provider.
Input	Form requiring the passenger authentication for accessing the service.
Expected Output	Attributes returned by the eIDAS framework and authentication completed.
Final Validation	Two different member states simulated.
Status & Results	[Not performed yet at M26]

4.2.9. Trusted Service Manager

Test Id: TC_TSM_1 – Correct Provisioning	**Component: Trusted Service Manager**
Description	Ensure the correct provisioning and distribution of keys and certificates between the components.
Input	-
Expected Output	A successfully established trust relationship between sensor platforms and E-CORRIDOR edge server based on a lightweight PKI.
Status & Results	[Not performed yet at M26]
Final Validation	Using the sensor platforms in the airport and possibly train station.

Test Id: TC_TSM_2 – Correct Reporting	Component: Trusted Service Manager
Description	Ensure the correct reporting of a benign and a modified software state via implicit attestation.
Input	-
Expected Output	A successfully established TLS channel between sensor platform and E-CORRIDOR edge server or the denial of such a connection in case of a compromised platform state.
Status & Results	[Not performed yet at M26]
Final Validation	Using the sensor platforms in the airport and possibly train station.

4.2.10. **Interest-cast of Airport Services**

Test Id: TC_IC_1 – App evaluation	Component: Interest-cast of Airport Services
Description	Evaluate the deployment of the two-party computation-based data sharing service
Input	Passenger's interests and provider info related to restaurants
Expected Output	Matching between the inputs
Final Validation	Setting recreated in the lab for the AT Pilot using a smartphone, for the passenger, and RaspberryPi 4, for the kiosk (provider)
Status & Results	[Test successful]: the passenger is able to know the best matches depending on her inputs in a privacy-preserving way

Test Id: TC_IC_2 – Interests setting for user	Component: Interest-cast of Airport Services
Description	Evaluate the possibility that a passenger can set up the parameters based on her interests.
Input	Passenger's value for each interest reported in Table 1
Expected Output	The desired value is set for the interest
Final Validation	Setting recreated in the lab for the AT Pilot using a smartphone, for the passenger
Status & Results	[Test successful]: the passenger is able to set the desired value

Test Id: TC_IC_3 – Options setting for service provider	Component: Interest-cast of Airport Services
Description	Evaluate the fact that data at provider side are fed by a central reservation system, e.g., Amadeus, at the airport side

Input	Value for each restaurant is automatically fed into the provider app
Expected Output	Values for each restaurant is inserted and updated automatically and stored in the local ISI
Final Validation	Setting recreated in the AT pilot labs
Status & Results	[Not performed yet at M26]

5. Requirements Traceability Matrix

Table 2 reports the requirements traceability matrix considering the end user evaluation that will be performed in the next period (following the use cases defined in D2.1) and the functionalities of the involved components (through the test cases defined in Section 4.2).

Table 2 Requirements traceability matrix

Use Case ID	Use Case Name	Priority	Test Cases	Status	Comment
AT-UC-01	PRM passenger Assistance and Authorization	Must	TC_FR_1 TC_FR_2 TC_FR_3 TC_SD_1 TC_SD_2	In progress	Face recognition already running, but not yet integrated with the processing of sensitive data of PRM
AT-UC-02	Passenger and baggage contextual identification	Must	TC_CFA_1 TC_CFA_2 TC_AR_1 TC_AR_2	In progress	Videos from the cameras can identify passengers and their luggage. To integrate with the activity recognition and contextual analysis
AT-UC-03	Contactless Passenger Authentication and authorization	Must	TC_FR_1 TC_FR_2 TC_FR_3 TC_GA_1 TC_GA_2	In progress	Evaluate if the facial recognition can be combined in a multi-factor authentication
AT_UC-04	Privacy-preserving Passenger Monitoring	Must	TC_CFA_1 TC_CFA_2 TC_CFA_3 TC_PL_4 TC_AR_1 TC_AR_2	Advanced	Camera feeds can be analyzed following the final deployment and metrics can be extracted
AT-UC-05	Passenger Analysis Opt-in Opt-Out	Must	TC_FR_1 TC_IC_1 TC_IC_2 TC_GA_1	In progress	The face recognition explicitly ask consent before sharing the data
AT-UC-06	Single Sign-On Authentication	Must	TC_FA_1 TC_FA_2 TC_FA_3	Advanced	The eIDAS based solution is run in a test environment, integration with a service provider is in progress

AT-UC-07	Multi-modal ticketing	Could	TC_SD_1 TC_SD_2	Not started	Evaluate the possibility of using the attribute-based encryption solution discussed in Sec 2.3.12
AT-UC-08	Service access through Bring Your Own Device	Could	TC_FR_1 TC_PL_2 TC_PL_3 TC_IC_1 TC_IC_2 TC_GA_1 TC_GA_2	In progress	Evaluate the passenger experience while using the different solutions
AT-UC-09	Sharing of service access data	Must	TC_CFA_3 TC_PL_4	In progress	Adopt a common format for sharing the data
AT-UC-10	Run collective security Analytics	Could	TC_AR_1 TC_AR_2 TC_CFA_3	In progress	Exploit the interaction with the ISAC pilot
AT-UC-11	Notification of service disruption	Could	TC_CFA_3	Advanced	Currently only through camera feed analysis
AT-UC-12	Passenger flow overview and prediction	Should	TC_PL_4 TC_CFA_3	In progress	The Bluetooth-based estimation to be integrated and shared in a common format
AT-UC-13	Privacy-aware behavioral identification	Should	TC_AR_1 TC_AR_2 TC_MFA_1 TC_MFA_2	Not started	It requires the integration of all the components before starting the evaluation
AT-UC-14	Notification on PRM passenger's location	Could	TC_PL_2 TC_PL_3	In progress	In lab

6. Contribution to the Pilot and Project Objectives

All in all, the benefits brought by the E-CORRIDOR project in a multi-modal setting like the AT pilot, are related to the controlled and privacy-preserving data sharing enabling authentication and security services. Recalling the project objectives, current progress and next steps regarding the AT pilot activities are summarized in Table 3.

Table 3 Contribution of the AT pilot activities to the E-CORRIDOR objectives at M26

Objective	Current progress	Next steps
1. E-CORRIDOR will build a flexible, confidential, and privacy-preserving framework for managing data sharing	DSAs related to the shared data support the analytics execution, accommodate data ownership requirements, and respect the privacy of the passenger (e.g., facial blurring DMO).	Additional DMOs (e.g., the background blurring for the kiosk facial recognition) that are under development will be integrated.
2. E-CORRIDOR will define edge enabled data analytics and prediction services in a collaborative, distributed and confidential way	The analytics in the framework can leverage the shared data. At M26 one is fully integrated (the camera feed analysis) and a second is under integration (the facial recognition). Analytics are executed on the central node (e.g., security services), on resource constrained devices (e.g., for the kiosk services), on the smartphone (e.g., for the localization or interest-cast) on in a hybrid fashion according to the requirements of the specific scenario.	Finalize the integration of all the services in the framework. Test and evaluate the solutions in their deployment configuration (e.g., smartphone, RaspberryPi).
3. E-CORRIDOR will define a secure and robust platform in holistic manner to keep the communication platform safe from cyber-attacks and ensure service continuity	To ensure the cyber-security of the AT pilot infrastructure, DNS blacklist and root of trust for the sensors are adopted. Moreover, a connection with the ISAC pilot will enable the collection of relevant threats and vulnerabilities.	Integration, test, and validation of the security components as well as the connection with the ISAC pilot regarding events relevant to the aviation and railway sectors.
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	Solutions adopted in the AT pilot are the result of a co-design with the technology/solution providers.	Test and validation in the pilot environment to collect feedback and further mature the solutions

5. E-CORRIDOR will provide mechanisms for seamless access to multimodal transport	Different authentication mechanisms are provided. Moreover, solutions to enhance/simplify the access to the services available in the AT pilot domain such as localization and interest-cast are offered.	Once integrated in the framework, there will be an effort in evaluating the interactions among the solutions to offer a better passenger experience in the corresponding scenario.
6. The framework and the services developed will be used to deliver three pilot products	All the components will contribute to the two main scenarios of the AT pilot (from the point of view of the passengers and of the transportation service providers).	Solutions will be evaluated against the use cases defined in D2.1 (and summarized by the two pilot scenarios in Sec 1.1), and the test cases in Sec 4.2.

In D2.2, we identified a few key questions considering the suitability of the AT pilot solutions (that were still under design at M12) as a product (ref. to the above-mentioned project Obj. 6). Here we review those questions considering the completed design and implementation results.

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?*

   An in-depth evaluation would require an assessment with the appropriate authorities (e.g., the Data Protection authority CNIL as both ADP and SNCF operate in France) and the EU GDPR (General Data Protection Regulation). Considering the scope of the project, in E-CORRIDOR we limit our consideration to the technical aspects only, despite the regulation requires also legal and operational analysis. At M26, two Data Manipulation Operations (DMOs) have been designed (the face redaction/blur already integrated, and the background blurring under integration). The DMOs are expected to cover the purpose and data limitation principles of the GDPR. Along with DSAs and the ISI subsystem, storage limitation (specifying a data retention policy), integrity and confidentiality principles (by means of encrypted bundle) are considered in the pilot solution.

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

   When the AT pilot solutions will collect data from the passenger a consent form will be prompted explaining the kind of data collected and the use that will be done. These messages are a way of representing the corresponding DSA that is written in a controlled natural language as a way of eliminating ambiguity and easing the automatic processing. For instance, the screenshot in Figure 30 from a live experiment of the facial recognition solution shows the consent form that the passenger must accept to allow any further collection and processing of her data.

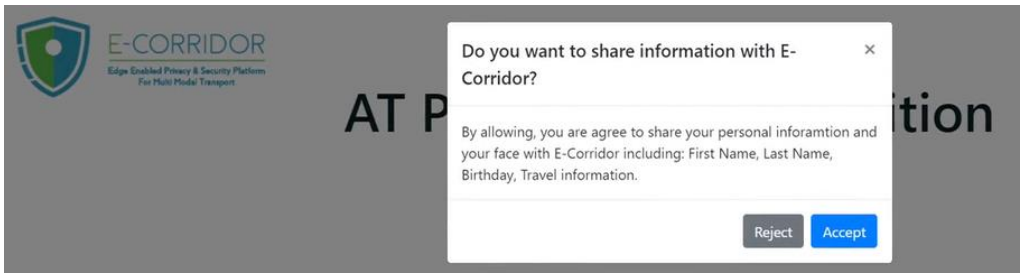

Figure 30 A screenshot of the data sharing form of the facial recognition solution

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?*

   At M26 the overall workflows for the designed solutions have not yet been validated in the pilot environment. Therefore, it is not possible to draw a conclusion about the performance impact of some of the privacy-preserving solutions. However, current tests for instance with the interest-cast of airport services (implemented on an Android phone and a RaspberryPi), adopting the secure two-party computation protocol to ensure privacy over the passenger's preferences, show a response time not affecting the user experience. Also, edge computation is expected to keep high performance while adopting privacy-preserving solutions.

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

   In the AT pilot, different authentication mechanisms are provided. In particular, the BYOD-related solutions are aligned with current trends where the passengers have a general preference in using their own devices to manage the travel. Other authentication mechanisms such as facial recognition will adopt a background blurring DMO (currently under integration) to ease the check-in process while preserving the privacy of any other passenger passing by the kiosk.

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 access to the services offered in the airport terminal or train station are expected to be improved by the adoption of localization and preference matching solutions. Current practices foresee the passengers wandering in the terminal or accessing to the info kiosks searching for the desired restaurant or directions to the next touchpoint. The localization and preference matching solutions deployed in the AT pilot aim at providing to the passenger a way to receive suggestions and directions for the services while moving in the terminal. This is expected to bring benefit to both transport service providers (e.g., better managing the passenger flow and reducing the queues) and passengers (e.g., better spending the waiting time).

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

   &

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?*

   The analysis of the camera feeds and the data sharing among different areas can enable a situation awareness (e.g., recognizing a left luggage, the respect of social distance or crowd management), and predictive and prescriptive analytics (e.g., identifying upcoming bottlenecks and suggest mitigations). In the AT pilot,

exchanging output metrics about the passenger flow can help managing the passenger flow and build a comprehensive view of the environment and of the connection between the two modes of transport. The DSAs can regulate the data exchange in such a way that only the expected information is exchanged.

8. *Will the proposed passenger identification and authentication solutions be tamper-proof?* The adopted authentication mechanisms will adopt some solutions to avoid an improper use. e.g., the facial recognition will be able to detect the presence of a live person (checking eye-blink) or the use of face masks (by using a camera with depth sensors). Moreover, the multi-factor authentication and the context reasoning will enrich the authentication procedure with additional information to increase the robustness of the process.

A summary of the E-CORRIDOR solutions applied in the AT pilot and the contribution to the pilot's goals (recalled in Section 1.2) is reported in Table 4.

Table 4 Components integrated in the AT pilot and contribution to the AT pilot's goals

Solutions of the E-CORRIDOR framework applied in the AT pilot	Goal 1	Goal 2	Goal 3	Goal 4	Goal 5	Goal 6
Passenger localization	✓	✓			✓	
Camera feed analysis				✓		✓
Gait analysis	✓		✓			
Facial recognition	✓		✓			
Activity recognition			✓	✓		✓
Analysis of sensitive passenger data		✓	✓			
Network intrusion detection						✓
Multi-biometric and multi-factor authentication with context analysis	✓		✓			
Federated authentication	✓	✓	✓			
Trust Identity management						✓
Interest-cast of the airport services	✓	✓			✓	
Encryption of ticketing info		✓				

7. Conclusion

This document reported the current setup of the AT pilot as well as the ongoing test and validation activities. All the E-CORRIDOR components considered for application in the AT pilot have a clear workflow and contribution to the pilot's goals (as summarized in Table 4). For each component, the described test cases define the ongoing validation (to verify that the targeted purpose is achieved). For the evaluation in the field, the acceptance tests (from end users) will follow the use cases already defined in D2.1.

With respect to the AT pilot architecture designed at M12, one additional component has been adopted by the pilot. The interest-cast service contributes to a few of the pilot goals related to the frictionless passenger experience and to the privacy-aware service access and matching. All the components planned to be used for the final demonstration of the pilot activities currently run stand alone and have detailed workflows describing the interaction between the pilot environment and the E-CORRIDOR framework. Notably, three of these solutions (i.e., the camera feed analysis, the facial recognition, and the interest-cast) have been validated in their final edge deployment configuration with smartphones and/or RaspberryPi. Components have been so far tested through publicly available datasets and lab settings.

The next months will be devoted to the integration and testing of all the services adopted in the pilot. In the final phase, each component will be validated in the AT pilot environment for acceptance by potential passengers (whose role will be covered by researchers and collaborators working in the project) and transportation service providers (i.e., ADP and SNCF).

8. References

[1] CEF DIGITAL, "Business Proposition of eIDAS-based eID in Aviation sector," 2018. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Studies+and+supporting+documents

[2] C. Plappert, F. Fenzl, R. Rieke, I. Matteucci, G. Costantino and M. De Vincenzi, "SECPAT: Security Patterns for Resilient Automotive E / E Architectures," in *30th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, 2022.

[3] Amadeus IT Group SA, "Amadeus Ticketing Platform," [Online]. Available: https://amadeus.com/en/portfolio/airlines/ticketing-platform. [Accessed 2022].

[4] 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].

[5] Pallets, "Flask web development, one drop at a time," [Online]. Available: https://flask.palletsprojects.com/en/2.2.x/. [Accessed 2022].

[6] ZeroMQ, "An open-source universal messaging library," ZeroMQ, [Online]. Available: https://zeromq.org/. [Accessed July 2022].

[7] Apache, "Apache Cordova," [Online]. Available: https://cordova.apache.org/. [Accessed 2022].

[8] D. Kroening and E. Clarke, *CBMC Bounded Model Checker - https://www.cprover.org/cbmc/,* Carnegie Mellon, 2016.

[9] S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Multi Level Security Problem," in *Advances in Cryptology*, 1982.

[10] P. Dendorfer, H. Rezatofighi, A. Milan, J. Shi, D. Cremers, I. Reid, S. Roth, K. Schindler and L. Leal-Taixé, "MOT20: A benchmark for multi object tracking in crowded scenes," arXiv:2003.09003.

[11] AVSS 2007, "2007 IEEE International Conference on Advanced Video and Signal based Surveillance," [Online]. Available: http://www.eecs.qmul.ac.uk/~andrea/avss2007_d.html. [Accessed July 2022].

[12] Genetec, "Software development kit and DAP (Development Acceleration Program)," [Online]. Available: https://www.genetec.com/. [Accessed 2022].

[13] D. Anguita, A. Ghio, L. Oneto, X. Parra and J. L. Reyes-Ortiz, "A Public Domain Dataset for Human Activity Recognition Using Smartphones," in *21th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, ESANN*, Bruges, Belgium, 2013.

[14] Z. Sitová, J. Šeděnka, Q. Yang, G. Peng, G. Zhou, P. Gasti and K. S. Balagani, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," *IEEE Transactions on Information Forensics and Security*, vol. 99, 2015.

[15] Q. Yang, G. Peng, D. T. Nguyen, X. Qi, G. Zhou, Z. Sitová, P. Gasti and K. S. Balagani, "A Multimodal Data Set for Evaluating Continuous Authentication Performance in Smartphones," in *12th ACM Conference on Embedded Network Sensor Systems (SenSys '14)*, New York, NY, 2014.

[16] G. M. Weiss, K. Yoneda and T. Hayajneh, "Smartphone and Smartwatch-Based Biometrics Using Activities of Daily Living," *IEEE Access*, vol. 7, pp. 133190-133202, 2019.

A. Appendix

A.1 Definitions and Abbreviations

Term	Meaning
ABE	Attribute-based encryption
ASI	Advanced Security Infrastructure (subsystem of the framework)
AT	Airport-Train (E-CORRIDOR pilot)
BLE	Bluetooth Low Energy
BYOD	Bring Your Own Device
CNIL	Commission nationale de l'informatique et des libertés (French regulatory body for data privacy)
CSS	Cascading Style Sheets
DMO	Data Manipulation Operation
DNS	Domain Name System
DNSBL	DNS blacklist
DSA	Data Sharing Agreement
EU	European Union
eIDAS	Electronic Identification, Authentication, and trust Services
eWallet	Electronic Wallet
FHE	Fully Homomorphic Encyption
FIDS	Flight Information Display System
GDPR	EU General Data Protection Regulation
HTML	HyperText Markup Language
ID	Identifier
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center (E-CORRIDOR pilot)
ISI	Information Sharing Infrastructure (subsystem of the framework)
JSON	JavaScript Object Notation
M*x*	Month *x* of the E-CORRIDOR project
OIDC	OpenID Connect
OSI	Optional Service Information
PCR	Platform Configuration Register
PNR	Passenger Name Record

PoI	Point of Interest
PRM	People with Reduced Mobility
QR-code	Quick Response Code
RGB-D	Red Green Blue-Depth
RNN	Recurrent Neural Network
RoT	Root of Trust
RSA-OAEP	Rivest–Shamir–Adleman Optimal Asymmetric Encryption Padding (encryption algorithm)
RSSI	Received Signal Strength Indicator
SAML	Security Assertion Markup Language
SHA	Secure Hash Algorithm (cryptographic hash function)
SSO	Single Sign-On
SSR	Special Service Request
S2C	Smart Cities and Car Sharing
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSM	Trusted Service Manager
TSN	Trusted Sensor Network
URL	Uniform Resource Locators
WP	Work Package

A.2 List of Figure