D2.1

Requirements for 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: 30/11/2020
Actual submission date: 30/11/2020

27/11/2020

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)	

Authors: Stefano Sebastio (UTRC), A. Chibani (PEC), O. Mercier (ADP)

Approved by: Gianpiero Costantino (CNR)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	27-Jul-2020	M. Manea	HPE	Initial table of content
0.2	29-Sep-2020	S. Sebastio	UTRC	First draft of the user stories - Sec 1.5
0.3	13-Oct-2020	S. Sebastio	UTRC	Improved user stories (Sec 1.5), plus content up to Sec 1.6 included
0.4	27-Oct-2020	S. Sebastio	UTRC	Improved AT-US-02, AT-US-04, AT-US-06 and motivation (in Sec 1.3 current practice), first version of the use cases and catalogue (Sections 2.2-2.3), non-functional requirements (Sec 3)
0.5	04-Nov-2020	S. Sebastio	UTRC	UML use case diagram (Sec 2.1) and storyboard (Sec 2.4)
0.6	06-Nov-2020	S. Sebastio	UTRC	Sec 1.7 Pilot evaluation and Conclusion. Reference to cross-pilot link to the user stories. 1st Complete version of the deliverable
0.7	10-Nov-2020	A. Chibani, O. Mercier	PEC, ADP	Draft of: a new user stories and two additional use cases. Introduction of two stakeholders: contractors and PRM assistant
0.8	20-Nov-2020	S. Sebastio	UTRC	Integration of the draft from PEC and ADP. Additional references to current practice and scenario. Version ready for internal review
0.9	24-Nov-2020	A. Chibani, O. Mercier, S. Sebastio	PEC, ADP, UTRC	Minor changes to the used terminology
1.0	27-Nov-2020	S. Sebastio	UTRC	Integration of the reviewer's suggestions

Executive Summary

This document contains the requirements elicitation for the Air Train (AT) pilot. This pilot is one of the three pilots in E-CORRIDOR (alongside the Car Sharing, and the Information Sharing and Analytics Centre pilots). The AT pilot aims at simplifying the airport-train link, improving security analytics and operations management, and enhance the passenger experience throughout her journey. To achieve such goals novel federated (analytics and identity management) mechanisms need to be designed and adopted, to preserve data/analysis control and ownership while leveraging all the information collected by each stakeholder. Furthermore, considering sensitivity and nature of the passenger information (that could include biometric and personal device data), privacy-aware mechanisms must be enforced. All in all, a co-optimization of user experience, security and privacy is deemed advisable to reach the target of the AT pilot.

In this document, main stakeholders, user stories and use cases for the AT pilot are described. Additionally, the relevance of the pilot requirements with respect to the E-CORRIDOR objectives and means of validation are discussed.

While discussing the benefits of bringing the E-CORRIDOR concepts and its framework in the AT pilot, this document assumes that the reader is already familiar with the main pillars of its infrastructure namely, Information Sharing Infrastructure (ISI), Information Analysis Infrastructure (IAI) and Data Sharing Agreement (DSA). These were introduced in the project proposal and will be further developed in the Work Packages 6, 7 and 8.

Table of contents

1. High Level Requirements

The AT pilot considers the application of the E-CORRIDOR concepts to a multi-modal transportation ecosystem consisting by air and train transportations. Characteristic traits of such pilot are its special requirements with respect to data protection and passenger experience. Therefore, the pilot will be able to evaluate the privacy-preserving data sharing and analytics of the E-CORRIDOR framework. The E-CORRIDOR framework will unleash yet untapped synergies between modes of transportation with respect to security, identity management and authentication, and optimization. Cascading beneficial effects will be perceived by all the pilot stakeholders and ultimately by the passenger.

This section discusses the requirements for the AT pilot. It begins (Section 1.1) with an overview of the current scenario in order to establish a baseline for the subsequent discussion. The main stakeholders are identified and described in Section 1.2. Then, benefits brought to the AT pilot by the E-CORRIDOR framework are reported in Section 1.3 contrasting with the current practice. A few user stories, looking at the requirements from the point-of-view of the different involved stakeholders, and their mapping to the E-CORRIDOR objectives are described respectively in Section 1.4 and 1.5. The section ends discussing how the pilot will be evaluated (Section 1.6).

Use cases and non-functional requirements are detailed respectively in Section 2 and Section 3. Final remarks are in Section 4 whereas in the Appendix A are reported: a list of the adopted abbreviations, data types that will be considered during the execution of the use cases and our requirements elicitation process.

1.1. Scenario

The AT pilot is devoted to the passenger employing a multi-modal transportation. Indeed, the passenger journey is usually not confined between departing and destination airports. More often the passenger adopts multiple modes of transportation during her journey. E.g., the passenger could use a car sharing service to reach the closest train station, and from there she could take a train connecting to the airport. Sometimes there is also the need to take connecting flights. And the multimodal scenario continues at destination as well e.g., by taking a train to reach the desired city and then using the car sharing to reach the hotel. The lack of an adequate support in these connections during the journey produces a fragmented trip for the passenger. These disruptions are generally perceived more severely in the case of people requiring assistance.

An example of multi-modal transportation in the AT pilot including the passenger checks is depicted in Figure 1. In such a scenario, only an adequate interoperability among the different identification and authentication systems deployed by each stakeholder can enable a frictionless end-to-end multi-modal passenger journey. The AT pilot focuses in particular on the railway-airport connection.

A closer look at the activities performed in the airport reveals further source of disruption. Indeed, the passenger needs to pass through several identification/authentication/authorization checks for check-in, manual desk for baggage drop-off and checking, security, boarding gate, and custom border and baggage claim at the destination airport. In several of these checks, the passenger needs to provide multiple times her identity document (e.g., passport) and travel

ticket. Moreover, many of these operations are performed semi-manually by ground personnel with an unavoidable generation of waiting queues.

Some efforts in modernizing manual procedures in the airport have produced the automated physical access control (in place of manual desks) and the travel authorizations electronically linked to a traveller's passport e.g., ESTA (Electronic System for Travel Authorization) in US, ETA (Electronic Travel Authorization) in Canada and Australia and ETIAS (EU Travel Information and Authorization System) in Europe.

In light of the unfortunate COVID-19 pandemic, in addition to regulations and restrictions issued by several governments, the presence of waiting queues, public touch surfaces and the need to keep physical distance have discourage passengers from using the air transportation in particular.

To improve the passenger experience, context-aware multi-factor authentication, sensing technologies and robust identity management are advocated. These have the power of speeding up all the passenger-related procedures while improving the security and at the same time protecting the privacy of passengers, and railway and airport personnel.

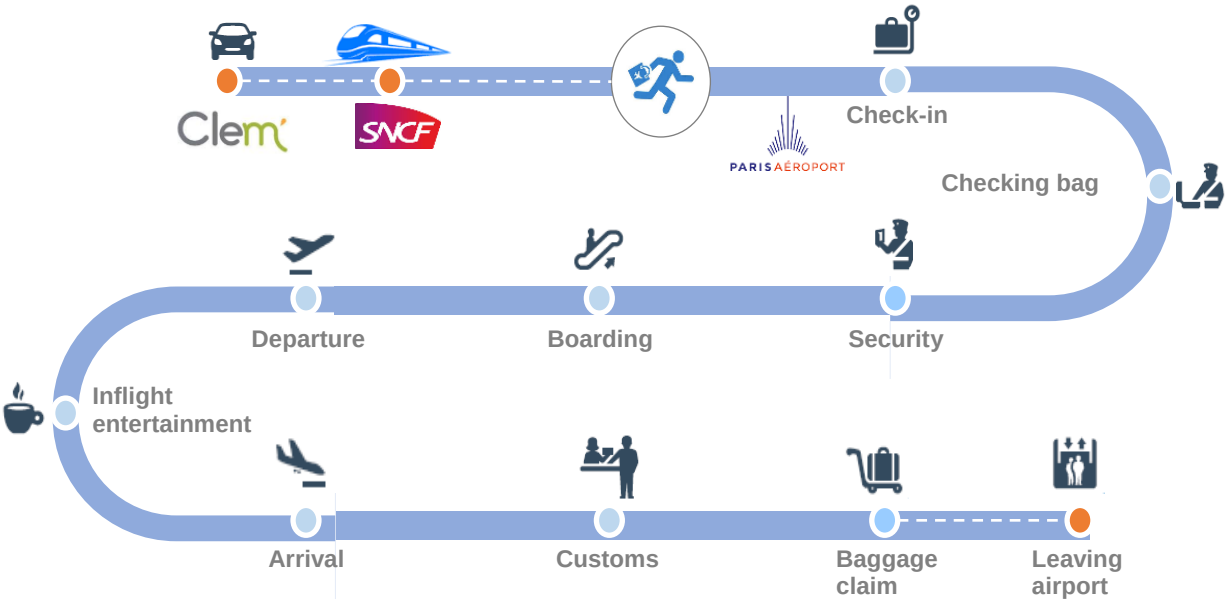

Figure 1 Multi-modal transportation and airport checks [from the E-CORRIDOR project proposal]

While respecting the privacy, data about passengers, operations and services are collected at different points by all the stakeholders. Unfortunately, it is not possible to take advantage of the information contained in such data due to the presence of isolated systems and data silos owned by each stakeholder.

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

In line with the depicted scenario, recently, the air transport of the future has been envisioned by the NEXTT (New Experience Travel Technologies)[1] industrial initiative whose main points revolve around passenger identification and her experience, and data sharing and processing.

1.2. Stakeholders

From the aforementioned scenario, a few stakeholders stand out. Their participation to the AT pilot is different, as well as their role as information *prosumers* (i.e., producer and consumer) while interacting with and through the E-CORRIDOR framework. Namely:

1. Passenger:
    a. People with Reduced Mobility (PRM) – any person whose mobility, when using transport, is permanently or temporarily reduced and therefore needs appropriate attention (e.g., disabled or elderly)[2],
    b. Accompanying person or PRM assistant,
2. Airport:
    a. Airport Managing Body (AMB) – body that, under national legislation, administers and manages the airport infrastructures, and coordinates and controls the activities performed in the airport,
    b. Airport services - aviation and non-aviation services,
3. Train station:
    a. Station manager – the organizational entity responsible for the management of the railway station,
4. Carriers:
    a. Air carrier,
    b. Train carrier,
    c. Potentially, any other carrier reaching/connecting with the airport.

The passenger is the driving force for the AT pilot. Her willingness to visit the airport and use the connecting carriers is tightly dependent on the perceived experience. A friction experience due to long waiting lines, discontinued travel flow, manual and tedious procedures, or slow response/understanding of her needs are all factors potentially frustrating the passenger. A special case is represented by the People with Reduced Mobility (PRM) whose needs require the adoption of appropriate policies and the enabling of different services to ensure a non-discriminatory treatment.

In the multimodal transportation scenario envisioned in the AT pilot, the airport is the key node between airline and railway services. The airport aims at providing safety, security, a better passenger experience, and aviation and non-aviation services to both airlines and passengers. Moreover, airports are a crucial connection point in the passenger journey which starts even before reaching the airport. Data silos and manual procedures create reduced visibility on the

[1] https://nextt.iata.org/en_GB/ [Accessed: 12 Oct 2020]

[2] "Consolidated text: Regulation (EC) No 1107/2006 of the European Parliament and of the Council of 5 July 2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air" available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02006R1107-20060815 and "Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations" available online at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32007R1371 [Accessed: 18 Nov 2020]

available knowledge and a limited service optimization. Within the airport the Airport Managing Body (AMB) administers and manages the airport facilities and it is in charge of ensuring that security checks on passengers and baggage respect the applicable regulations. The airport services encompass all the additional (e.g., ticket sales, transit handling) and leisure services (e.g., shops, airport lounges) available to the passengers.

Carriers involved in the AT pilot are mainly airline and railway. But potentially other carriers are connected with the airport. Their goals are oriented toward improving the service operations and increasing the passenger satisfaction. Any optimized procedure has the potential to reduce costs hand in hand with a better passenger experience. Crucial aspects are owed to the screening checkpoint and to the baggage handling. But a smooth access to the services (even during the travel) can further rise the passenger satisfaction.

1.3. Comparison to current practice

Current travel practice foresees that passenger and baggage are identified and re-authenticated at each stop. Moreover, often more than a single mode of the transportation is used by the passenger during her journey and the same documents needs to be provided multiple times (e.g., ticket and passport). Indeed, the original Hub & Spoke (H&S) model focused around the (hub) airport where passengers transfer between different flights, has been later extended to railway services integrated as spokes and not only to reach the closest city centre. These multimodal integrated services have already been adopted by some carriers in a few airports (e.g., Lufthansa "Express Rail"[3], Finnair "Rail & Fly"[4] or Air France "Train + Air"[5]) but are mainly limited to selling combined tickets.

The potential poor experience is even exacerbated in case of people with reduced mobility (PRM). Fragmented regulations (e.g., between EU and US) concerning the responsibility among airport managing body (AMB) and air carrier for the PRM[6], generate frequent malfunctions and disruption for the passenger since her arrival in the airport terminal.

All this causes discontinuities in the passenger journey with repercussion in the overall passenger experience. The context-aware privacy preserving federated authentication mechanisms of the E-CORRIDOR framework will allow a seamless passenger journey while moving among different carriers and using in-flight and airport services.

Multiple transport modes have 'points of contacts' not only while transporting passengers but even goods. Despite the natural need for continuity in the data flow, nowadays carriers do not have any common platform to exchange data and often the communication relies on legacy processes. This scenario brings strong limitations with respect to security and performance in the transportation ecosystem and a frictionless multimodality is still elusive. The International

[3] https://www.lufthansa.com/us/en/lufthansa-express-rail [Accessed: 19 Nov 2020]

[4] https://www.finnair.com/us/gb/allegro [Accessed: 19 Nov 2020]

[5] https://www.airfrance.fr/FR/en/common/resainfovol/avion_train/reservation_avion_train_tgvair_airfrance.htm [Accessed: 19 Nov 2020]

[6] Often the PRM service is sub-contracted. But for the purpose of this document we consider the sub-contractor as part of the entity in charge of providing the service according the applicable regulation.

Air Transport Association (IATA) has joined[7] two recent efforts of the EU through the Digital Transport & Logistics Forum (DTLF)[8] and the FEDeRATED[9]. Through these consortiums, also with respect to the transportation domain, best practice and guidelines for an interoperable data sharing infrastructure will be developed.

The E-CORRIDOR platform is in line with the above mentioned efforts but perform a step forward. Data sharing agreements (DSAs) in E-CORRIDOR will allow the definition of sharing and analysis rights while preserving data ownership. Moreover, federated and distributed edge-enabled analytics will usher in new multi-stakeholders security services and operations data co-optimization.

Airline passengers need to traverse checkpoints: check-in, checking bag, passport security, boarding gate, and customs and baggage claim at destination. In all of these points, the passenger has close interactions with airport personnel and other passengers waiting in line. With the COVID-19 pandemic, to avoid proximity with other people and the touch of public surfaces many passengers have avoided as much as possible to travel.

The capability of the E-CORRIDOR platform of providing robust identification (and identity management), behavioural analysis and context-aware services will reduce the waiting time and provide a frictionless passenger experience while being compliant with the applicable regulations with respect to security and privacy.

Digital technologies are largely adopted by the airports in day-to-day operations for both aviation and non-aviation services. This scenario has brought airport to become more vulnerable to attacks and data breaches involving information on passengers and airport personnel. The EU agency EASA (European Aviation Safety Agency)[10] estimated that aviation systems face an average of 1000 cyber-attacks each month. Increased connectivity and network opening to stakeholders and users have further stressed the cyber infrastructure with respect to security issues. Cyber vulnerabilities across operational technology systems in the airport have already been proved to be able to potentially affect[11] baggage handling, aircraft tugs, de-icing systems and fuel pumps. But there are also public reports of ransomware, data breaches, attacks to the wi-fi network, and personal data leakage in major international airports. A recent research[12] on cybersecurity, compliance and privacy found that 97 of the world's top 100 airports are vulnerable. Initiatives such as Cyber Resilience in Aviation Industry promoted by the World Economic Forum[13] and the European Centre for Cyber Security in Aviation

[7] https://www.iata.org/contentassets/a1b5532e38bf4d6284c4bf4760646d4e/one_record_project_insight_multimodal_data_sharing.pdf [Accessed: 8 Oct 2020]

[8] https://www.dtlf.eu/ [Accessed: 8 Oct 2020]

[9] http://www.federatedplatforms.eu/index.php [Accessed: 8 Oct 2020]

[10] https://www.easa.europa.eu/domains/cyber-security/overview [Accessed: 22 Oct 2020]

[11] https://www.darkreading.com/vulnerabilities---threats/airports-and-operational-technology-4-attack-scenarios-/a/d-id/1334282 [Accessed: 22 Oct 2020]

[12] https://www.immuniweb.com/blog/state-of-cybersecurity-top-100-airports.html [Accessed: 23 Oct 2020]

[13] https://www.weforum.org/whitepapers/advancing-cyber-resilience-in-aviation-an-industry-analysis/ [Accessed: 23 Oct 2020]

(ECCSA)[14] aim to rise the cybersecurity situational awareness and develop a trusted network of collaboration with a multi-stakeholder community.

The information sharing and analysis capabilities of the E-CORRIDOR platform will ease the collaboration among the stakeholders while preserving the privacy of the exchanged data and analysis result.

1.3.1. Support to PRM passenger at the Charles de Gaulle Airport (CDG), Paris

The Paris Charles de Gaulle Airport (CDG) is the second busiest European airport according to the total number of passengers per year, and it is operated by ADP.

Passengers reach or leave CDG through different modes of transportation such as train, bus, taxi or private car. Within the E-CORRIDOR project, and the AT Pilot working group in particular, the airport-railway connection is exemplified by ADP on the airport side and by SNCF on the railway station (both the companies are partners of the E-CORRIDOR consortium). In the busiest airports, PRM support is requested by millions of passengers each year and will therefore receive special attention in this document.

Currently, the PRM passengers are managed by agents of the two companies at the endpoints of this link through a simple messaging system. Agents of the PRM department at CDG collect information about new PRM support requests from the airline carrier (thanks to the ADP flight management system). Such requests specify the kind of support needed at the train station including the need for a PRM assistant. Then, thanks to a dedicated electronic messaging system linking the PRM departments at ADP and SNCF, the ADP agent forwards the collected request. This message includes identity information, the Special Service Request (SSR) code, status, mobility needs, pick-up and drop-off areas, and information about the baggage. Unfortunately, this message does not contain enough information to authenticate the passenger. Therefore, this operation is manually performed by the two human agents.

All the private information is retained in a secure area and solely for a limited time (e.g., in the event of complaints or incidents) to comply with the GDPR and the French National Commission on Informatics and Liberty (CNIL).

1.4. User Stories

1.4.1. AT-US-01: Passenger Management and Operations

As a

Air carrier/airport managing body (AMB),

Railway station manager

I want to

Be able to support disabled passengers and passengers with limited mobility (people with reduced mobility, PRM)

So that

[14] https://www.easa.europa.eu/eccsa [Accessed: 23 Oct 2020]

Passenger, assistant and assistive device are identified, authenticated and properly treated while accessing to airport and train station, moving around the airport, and making their way to the aircraft.

1.4.1.1. Discussion

Main stakeholders:

1. Passenger - people with reduced mobility (PRM)
2. Air carrier
3. Train carrier
4. Airport managing body (AMB)
5. Railway station manager

Referenced stakeholders:

6. Airport services
7. PRM assistant

This scenario helps in assuring that PRM are not discriminated because of their disability – U.S. Department of Transportation 14 CFR Part 382 (Non-discrimination on the Basis of Disability in Air Travel) and EU Regulation 1107/2006. Responsibilities and duties are divided between airport managing body (AMB) and air carriers in the European Union. Whereas according to the U.S. regulations the air carrier is the sole responsible from the moment PRM enter the airport terminal.

Upon her arrival at the airport (if not already during the booking process), the PRM passenger asks travelling assistance to the air carrier and/or airport. The entity in charge of the PRM passenger assigns the most appropriate Special Service Request (SSR) code[15] and organizes the needed assistance. From this moment on, the passenger is assisted while moving around the airport, using airport services and facilities without any need to re-identify herself and her special needs.

It requires that in their way to the aircraft, passenger, assistant and assistive device (if any, e.g., wheelchair, crutch, cane, walker) will be properly identified, authenticated and treated at: check-in, baggage drop-off, security, any airport service (e.g., shops, toilets, lounges) and departure/arrival gate. This includes the automatic triggering of the corresponding policy and the subsequent authorization to use special routes, preferential gates and services (e.g., the elevator).

To ensure a smooth and safe journey, the authentication should provide a frictionless passenger experience to the user while preserving her privacy. Considering the special assistance scenario, alongside the passenger also the context (notably, assistive device and assistant) needs to be captured and analysed through the privacy-preserving analytics of the E-CORRIDOR framework to allow a continuous authentication.

Ideally, thanks to collaboration and information sharing (specified by means of DSAs) among train station, departing airport, airline and destination airport, the service support is carried out even at destination and thus follows the PRM passenger. Starting from the disembarking

[15] https://support.travelport.com/webhelp/uapi/Content/Air/Shared_Air_Topics/SSRs_(Special_Service_Requests).htm [Accessed: 5 Oct 2020]

procedure and up to the next mode of transportation chosen by the passenger (e.g., connecting flight, train, car sharing, shuttle, bus or taxi).

1.4.1.2. Acceptance Tests

1. The PRM passenger declares her needs only once (while arriving at the airport or during the booking process) to receive the required assistance.
2. Air or train carriers and/or AMB identify the PRM passenger and automatically arrange the corresponding special services.
3. All the spots visited by the PRM passenger throughout her journey are aware of the SSR code and put corresponding policies in place.

1.4.2. AT-US-02: Frictionless Multimodal Journey

As a

Passenger

I want to

Avoid any disruption while changing mode of transportation

So that

I can easily travel by using the mode(s) of transportation more suitable to my needs

1.4.2.1. Discussion

Main stakeholders:

1. Passenger

Referenced stakeholders:

2. Air carrier
3. Train carrier
4. Airport

Most often, the passenger needs to use multiple modes of transportation during her journey. Ideally, the passenger should not be required to provide the same information multiple times (e.g., boarding pass or identification card) while having a seamless authentication and identification of herself and her baggage between different stakeholders. The final aim is a frictionless experience for the passenger while changing mode of transportation and passing through the different authentication points, leveraging on the Single Sign-On (SSO) authentication schema.

To reach such a goal, carriers (e.g., air and train) share data by creating a digital corridor for information systems, while preserving confidentiality, control and ownership on the passenger data. These characteristics are provided by the DSAs attached to the shared data and by the Information Sharing Infrastructure (ISI) of the E-CORRIDOR framework. The same data sharing capabilities are required within the different identification/authentication spot present in the airport itself. Passenger information is captured at the boarding gate, verified at the Customs and Border Protection (CBP), and the analysis sent back to the airline for opening the

gate and registering the passenger as boarding. Potentially, the flow is not interrupted even during the travel while the passenger uses in-flight entertainment (IFE) and services. Thanks to federated authentication mechanisms and the adoption of a digital wallet (e-wallet) service, the passenger can take the mode of transportation of her choice without any need to stop at the ticket vending machine. Tickets are automatically purchased as soon as the passenger is identified and gains access to the next mode of transportation.

Carriers (airline and railway companies) and airport cooperate by means of pre-established or ad-hoc agreements and a robust identity management. To the same passenger a unique identifier is assigned throughout her whole journey. Passenger information must be proved and/or exchanged in a privacy preserving manner, be compliant with the specified DSA (Data Sharing Agreement) and regulations (e.g., GDPR) including the data retention policies. All the authorization delegations must be recorded in case of audit. Regulatory and privacy issues need to be taken into account and accommodated.

1.4.2.2. Acceptance Tests

1. The passenger does not provide the same identification documents multiple times.
2. The passenger is able to use a SSO authentication schema even while changing mode of transportation.
3. Carriers and airport are able to exchange passenger information in a privacy preserving manner.
4. Results of the authentication performed at one spot are made available to other authentication spots by means of delegation.
5. Data confidentiality is respected and all the analyses are compliant with the concerning regulations as specified in the DSA.

1.4.2.3. Cross-pilot user-story: reference D3.1 - S2C-US-01 Sign in eWallet

In the deliverable D3.1, the car sharing pilot (S2C) presents a user story (S2C-US-01) describing a traveller willing to access to multiple services with a single account and a single log-in. Similarly, the above user story (AT-US-02) considers a passenger accessing to multi-transportation systems without any need to re-authenticate herself and with the ability of automatically purchasing the required ticket. This is achieved thanks to the exchange of passenger information in a privacy preserving manner among carriers.

1.4.3. AT-US-03: Distributed and Combined Context Analysis in Sensor Network

As a

Airport managing body (AMB)

I want to

Coordinate the analysis performed by all the passenger-oriented sensors available in the airport

So that

The passenger is better identified and I can provide her a better experience in the airport.

1.4.3.1. Discussion

Main stakeholders:

1. Airport managing body (AMB)

Referenced stakeholders:

2. Passenger
3. Air carrier
4. Airport services

In the airport, a plethora of sensors (RFID reader, camera, lidar, kiosk etc.) are available to identify and authorize the passenger to perform different operations (baggage drop-off, check-in, security, etc.). Each authentication spot is potentially characterized by its own required level of accuracy and domain representation. Thanks to the distributed context and behavioural analysis capabilities of the E-CORRIDOR framework, pre-assessed low risk passengers can have an expedited passage going through controls.

The AMB can collect sensor information and, more importantly, aggregate analysis results to co-optimize user experience, (cyber-) security services and privacy also thanks to Machine to Machine (M2M) communications. Information could be subjected to specific data retention policies (e.g., see the Article 5(1)(e) of the GDPR), come from different kind of sensors, and be described in heterogeneous data formats. The E-CORRIDOR Information Sharing Infrastructure (ISI) framework, will be in charge of handling such data and present them to the Information Analysis Infrastructure (IAI) components in a common format.

The effectiveness of the distributed context analysis is evaluated also taking into account the interaction friction experienced by the passenger throughout her journey.

1.4.3.2. Acceptance Tests

1. The AMB is able to orchestrate the sensing and the automated recognition capabilities of the various sensors deployed in the airport.
2. Heterogeneous data formats are presented in a common fashion to the (security and authentication) analysis algorithms.
3. The passenger is identified in the airport with minimum disruption while preserving her privacy.

1.4.4. AT-US-04: Advanced Security Analytic Services

As a

Airport managing body (AMB)

I want to

Enhance my security analytics tools

So that

I can improve the security for all the passengers visiting my airport, the hosted airline companies, other carriers reaching the airport (e.g., train or car sharing) and the airport itself, and be less vulnerable to novel (cyber) security attacks.

1.4.4.1. Discussion

Main stakeholders:

1. Airport managing bodies (AMB)

Referenced stakeholders:

2. Passenger
3. Air carrier
4. Train carrier

Several activities are carried out in the airport. Thanks to novel analytic services, the AMB improves the airport security while providing both aviation (provision, maintenance and operation of equipment, and technologies required by the air carrier and handling services) and non-aviation services (e.g., commercial activities and business lounges).

Event log from the Industrial Internet of Things (IIoT), cloud computing and integrated systems deployed in the airport are collected. After the establishment of multi-party or Peer to Peer (P2P) agreements and the definition of an appropriate DSA, information from carriers (e.g., air and train carriers) and passengers is collectively analysed to improve the confidence level of the detection. Events contextual, internal and external to the airport are properly correlated and analysed.

To aim for advanced detection services the analysis should include operation, system and network events. Cyber, physical and cyber-physical threats must be identified and predicted through a continuous security monitoring system with the anomaly detection capabilities and Intrusion Detection System (IDS) provided by the IAI of the E-CORRIDOR framework. Once the analysis is concluded, the security analytic services of the AMB distribute the results to all the stakeholders according to the relative relevance through the ISI. At the reception of such results, each stakeholder is then able to customize, apply at runtime any novel security model/policy that should be needed and timely stop any attempt of breaking any service or the identification management. Mitigation actions are potentially performed proactively. Both data and analytics results have attached DSAs.

1.4.4.2. Acceptance Tests

1. The AMB is able to detect novel complex threat events that it would not be able to identify otherwise.
2. All the stakeholders are able to increase the knowledge about the threats, and to improve and adapt their own security tools.
3. Threats events are presented to the stakeholders with respect to the subjective relevance.

1.4.4.3. Cross-pilot user-story: reference D4.1 - ISAC-US-08 Aviation cyber threat information analysis; ISAC-US-09 Aviation cyber threat information sharing

In the deliverable D4.1, the Information Sharing and Analysis Centre pilot (ISAC) presents the user stories ISAC-US-08 and ISAC-US-09 respectively describing AMB willing to analyse sensor data collected in the airport locally or through the ISAC tools, and also willing to share the data itself or the analysis results with other aviation organization (airlines, airport operators and service provides). Similarly, the above user story (AT-US-04) considers the AMB willing to enhance the security analytics tools detecting and predicting cyber, physical, and cyber-physical threats. Moreover, D4.1 introduces the multi modal transportation ISAC (namely, the ISAC-MMT) in which operators belonging to different (but potentially) connected transportation sectors share data and analysis results with the aim of improving the overall view on the security threats. Privacy preserving information sharing and federated analysis can allow novel security services while preserving information ownership and confidentiality.

1.4.5. AT-US-05: End to End Safe-Contact/Contactless Journey

As a

Passenger

I want to

Feel safe and confident in the airport and in the airplane

So that

I can travel again during and after the COVID-19 pandemic minimizing the touch of public surfaces.

1.4.5.1. Discussion

Main stakeholders:

1. Passenger
2. Airport managing body (AMB)

Referenced stakeholders:

3. Air carrier
4. Airport services

Normally, in the airport, passengers are in close proximity to each other at numerous touch points. As reported by a passenger survey commissioned by IATA[16] on the impact of COVID-19, among the top three travellers' concerns at the airport there is queuing at check-in, security, border control and boarding gate. To address this, the IATA proposed the use of: self-service check-in, hands-free and automated processes, self-bag drop, and contactless boarding process.

[16] https://www.iata.org/en/publications/store/covid-passenger-survey/ [Accessed: 28 Sep 2020]

The AMB assures that long and slow-moving lines of passengers are not present, contact between passengers and airport personnel are reduced as well as the physical act of touching surfaces. Passenger takes advantage of her own device, through a BYOD (Bring Your Own Device) approach, or contactless stations to use both aviation and non-aviation services in the airport premises. The same approach is adopted in the airplane while ordering food, drinks and controlling the IFE system (potentially, even by paying through an e-wallet system). Also, this would support the fight against the COVID-19 by reducing the chance of infection. Distributed, edge-enabled and privacy-aware analytics of the E-CORRIDOR framework will enable secure and continuous authentication services.

1.4.5.2. Acceptance Tests

1. Passenger do not need to touch any public surface throughout her journey.
2. In-flight services can be requested by means of BYOD solutions.
3. AMB is able to provide contactless or BYOD solutions for authentication.

1.4.6. AT-US-06: De-silo and Co-optimize Operations Data

As a

Airport managing body (AMB)

I want to

Leverage on all the data generated by the travellers (from reservation to security and on the aircraft), by the air carriers and in the airport

So that

I can connect all the data silos and co-optimize the operations.

1.4.6.1. Discussion

Main stakeholders:

1. Airport managing body (AMB)

Referenced stakeholders:

2. Air carrier
3. Train carrier
4. Passenger

A deluge of data is generated in the overall airport related services, starting from the reservations placed by travellers, to ground services and airplane logs. Data are also created as the airports manage the flow of people, aircraft, turnarounds and passenger experience. Also, airlines generate data while scheduling, operating and maintaining their fleets. This scenario requires the exchange of (operational) information between different stakeholders: airlines, airport operators, ground handlers and other partners.

The AMB would connect all these information silos through a privacy-preserving and controlled solutions to usher in a new generation of intelligent analytics (respectively through

the ISI and IAI of the E-CORRIDOR framework). Better services and enhanced knowledge are provided to airports, airlines and passengers. Knowledge and forecasting on the passenger behaviour will be improved as well as and how she interacts with processes and services. This will allow better planning decisions by matching capacity with demand, identify bottlenecks, and an improved passenger flow management and engagement. E.g., a high number of passengers in the train reaching the airport could suggest the opening of additional baggage drop-off desks. Signs of disruption (such as bad weather or traffic congestion around the airport) will be communicated to the affected stakeholders.

Due to regulatory and commercial reasons it is not possible to simply persuade all the involved stakeholders to move on a common computing platform (e.g., cloud computing). Limitations extend to performance aspects while moving large amount of data.

To solve these issues, collaborative edge-enabled solutions and appropriate DSAs are adopted in the E-CORRIDOR framework. In a federated setting, the data transfer is reduced and the enforced DSAs allow to keep control and ownership on data and analysis results.

1.4.6.2. Acceptance Tests

1. AMB is able to de-silo and co-optimize the collected data
2. Data privacy is ensured through appropriate privacy-preserving algorithms
3. DSAs regulate data access and analysis
4. Stakeholders collaborate and co-optimize services while retaining control over data and analysis results.

1.4.7. AT-US-07: Document-free Secure Multimodal Travel Credential

As a

Airport managing body (AMB),

Railway station manager

I want to

Reduce the data exchange burden for (re-)authenticating and route the passenger, letting the same passenger to collect and carry tamper-proof information useful for her authentication.

So that

Airports and railway stations can cooperate to ease the authentication process.

1.4.7.1. Discussion

Main stakeholders:

1. Passenger
2. Airport managing body (AMB)
3. Train station manager

Referenced stakeholders:

4. Air carrier
5. Train carrier

Just after having booked the ticket, the passenger can start collecting the travel credentials needed throughout her journey. This information vault will initially include tickets and passport but later on the airport or railway station the same will be enriched with contextual, biometrical and behavioural data. Such a tamper-proof vault will allow a token-based authentication for the passenger and be limited to a single journey. Its access will be restricted according to an authorized-to-know basis.

Behavioural and context analysis of the E-CORRIDOR framework will support a robust authentication mechanism. Any anomaly detected by the IAI will represent a potentially risky situation for safety and/or security of the airport and railway station operations. In case of anomaly events, the authentication procedure will be rolled-back to a normal manual process and different alarm levels may be raised towards the airport and railway station personnel. At the end of the journey, the information vault will be emptied by the behavioural and contextual data, and available only for a limited time and for the sole access by the border control and security authorities.

In line with this scenario, the IATA envisions to improve the identity management by 2035 through the One ID program[17]. One of the key point is the extension of the ‘check-in’ performed in the airport with the 'ready to fly' terminology extending some elements of the check-in process. Also, One ID aims at facilitating the “sharing of the passenger’s biographical, biometric and travel document information between the various public and private stakeholders that interact with the passengers across the journey and have a valid reason to access certain data in order to process passengers correctly, safely and securely”, and at providing services in the most efficient way. Thanks to a real-time visibility of the passengers’ location in the airport it is possible to provide them a personalized customer experience and anticipate their demand.

1.4.7.2. Acceptance Tests

1. The travel credential includes and replaces all the other travel documents (e.g., ticket, passport)
2. AMB security procedures are enhanced while easing and speeding up the processes for the passenger
3. The passenger privacy is preserved thanks to privacy-preserving analysis and by handing over the control of the travel credentials to the same passenger

[17] https://www.iata.org/en/programs/passenger/one-id/ [Accessed: 19 Nov 2020]

1.5. Relevance to E-CORRIDOR objectives

The AT pilot aims at providing enhanced intra-modal and multi-modal services to all the above mentioned transportation stakeholders and ultimately to the passenger. The user stories discussed in the previous sections represent different facets of the pilot, and are highly and completely relevant to the E-CORRIDOR objectives, and in some aspects also related to the Car Sharing (S2C) and the Information Sharing and Analytics Centre (ISAC) pilots.

In particular, the AT pilot focuses on distributed analysis and identity management, to co-optimize privacy, security and passenger experience and therefore contribute to the following E-CORRIDOR objectives (here reported for the sake of completeness):

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

The correlation between the User Stories presented in Section 1.4 and the above-mentioned E-CORRIODR objectives are as follow.

The *AT-US-01: Passenger management and operations, AT-US-02: Frictionless Multimodal Journey*, *AT-US-03: Distributed and Combined Context Analysis in Sensor Network*, *AT-US-05: End to End Safe-Contact/Contactless Journey*, and *AT-US-07: Document-free Secure Multimodal Travel Credential* are linked to the *Objective 1* of the project. The information treated in and shared among the stakeholders of these user stories is confidential. It is therefore required to consider appropriate DSAs to preserve ownership and control over such sensitive information to be compliant with data storage, processing and retention regulations.

The *AT-US-02: Frictionless Multimodal Journey, AT-US-03: Distributed and Combined Context Analysis in Sensor Network, AT-US-04: Advanced Security Analytic Services*, *AT-US-06: De-silo and Co-optimize Operations Data,* and *AT-US-07: Document-free Secure Multimodal Travel Credential* are linked to the *Objective 2* of the project. Data are collected and owned by different stakeholders in these user stories. Moving data or stakeholders services on a common platform (e.g., could computing) could not be feasible. Privacy-aware federated analytics are advocated in such scenarios.

The *AT-US-03: Distributed and Combined Context Analysis in Sensor Network, AT-US-04: Advanced Security Analytic Services, AT-US-06: De-silo and Co-optimize Operations Data,* and *AT-US-07: Document-free Secure Multimodal Travel Credential* are linked to the *Objective 3* of the project. Current data analysis systems are extensive and multifaceted, and inevitably exposed to a multitude of attacks. Complex attack analysis is able to reveal advanced and novel

threats by correlating set of events that when analysed in isolation could not rise the attention up to an alert level. Collaborative security analytics will benefit all the involved stakeholders.

The *AT-US-01: Passenger Management and Operations*, *AT-US-02: Frictionless Multimodal Journey*, *AT-US-03: Distributed and Combined Context Analysis in Sensor Network*, *AT-US-05: End to End Safe-Contact/Contactless Journey*, and *AT-US-07: Document-free Secure Multimodal Travel Credential* are linked to *Objective 4* of the project. Tools and approaches for identity management, analytics and security already available in the AT pilot will be enhanced thanks to the E-CORRIDOR platform and its ability to provide privacy-aware distributed analytics and identity management.

The *AT-US-01: Passenger Management and Operations*, *AT-US-02: Frictionless Multimodal Journey*, *AT-US-05: End to End Safe-Contact/Contactless Journey*, and *AT-US-07: Document-free Secure Multimodal Travel Credential* are linked to the *Objective 5* of the project. Thanks to privacy-aware, continuous behavioural mechanisms it would be possible to provide a frictionless passenger experience while using intra- and inter- modality services.

The *AT-US-01: Passenger Management and Operations*, *AT-US-02: Frictionless Multimodal Journey*, *AT-US-03: Distributed and Combined Context Analysis in Sensor Network*, *AT-US-04: Advanced Security Analytic Services*, *AT-US-05: End to End Safe-Contact/Contactless Journey*, and *AT-US-06: De-silo and Co-optimize Operations Data* are linked to the *Objective 6* of the project in which privacy-aware distributed services of the E-CORRIDOR framework will be validated at the AT pilot site. The evaluation will be carried out in a purposely designed test environment (disconnected from the production systems of airport and train station) but able to simulate the AT pilot site.

Table 1 summarizes the links between user stories and objectives of the E-CORRIDOR project.

Table 1 Correlation between user stories of the AT pilot and objectives of the E-CORRIDOR project

	Objective 1	Objective 2	Objective 3	Objective 4	Objective 5	Objective 6
AT-US-01	✓			✓	✓	✓
AT-US-02	✓	✓		✓	✓	✓
AT-US-03	✓	✓	✓	✓		✓
AT-US-04		✓	✓			✓
AT-US-05	✓			✓	✓	✓
AT-US-06		✓	✓			
AT-US-07	✓	✓	✓	✓	✓	

1.6. Pilot Evaluation

The user stories introduced in the previous sections define actions and operations deemed relevant for the AT pilot. Integration, execution and evaluation of the pilot scenarios in the E-CORRIDOR framework will follow the acceptance tests defined at the end of each user story. To assess the fulfilment of the key requirements, the following set of questions can be used during the pilot evaluation.

- 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?
- Will the passenger understand how her data are analyzed and shared to provide her seamless authentication mechanisms?
- 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?
- Will the sensor-based identification and authentication mechanisms actually allow a frictionless experience while preserving the passenger privacy?
- 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?
- Will the airport, air and train carriers perceive real benefits form sharing the data in terms of situation awareness, prediction and optimization?
- 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?
- Will the proposed passenger identification and authentication solutions be tamper-proof?

2. Use Cases

In this section, use cases for the AT pilot are represented in Section 2.1 and discussed in details in Section 2.2. These use cases have a priority assigned according to the MoSCoW (Must have, Should have, Could have, and Won't have but would like) method. A matching of the use cases with the user stories described in the previous section (see Section 1.4) is reported in Section 2.3. Story boards representing some user stories and non-functional requirements are respectively reported in Section 2.4 and Section 3. Then the document concludes with some final remarks in Section 4.

2.1. Use Case Diagram

Figure 2 reports the UML use case diagram for the AT pilot.

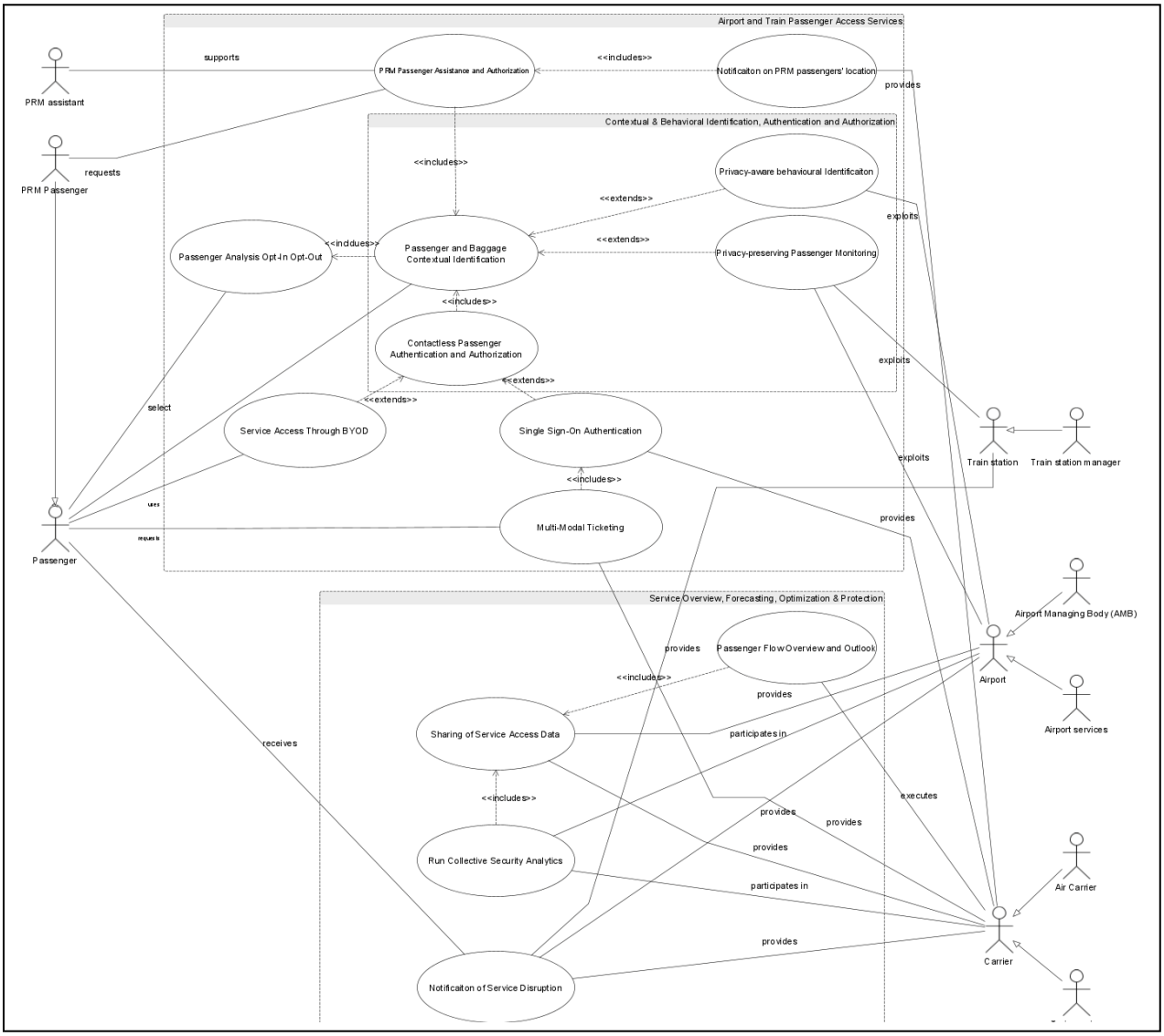

Figure 2: Overall AT Pilot UML Use Case diagram

For the sake of readability, the next two figures present magnified versions of the previous diagram by focusing on: the "Airport and Train passenger Access Services" system, including the "Contextual and Behavioural Identification, Authentication and Authorization" subsystems

(in Figure 3), and on the "Service Overview, Forecasting, Optimization and Protection" (in Figure 4).

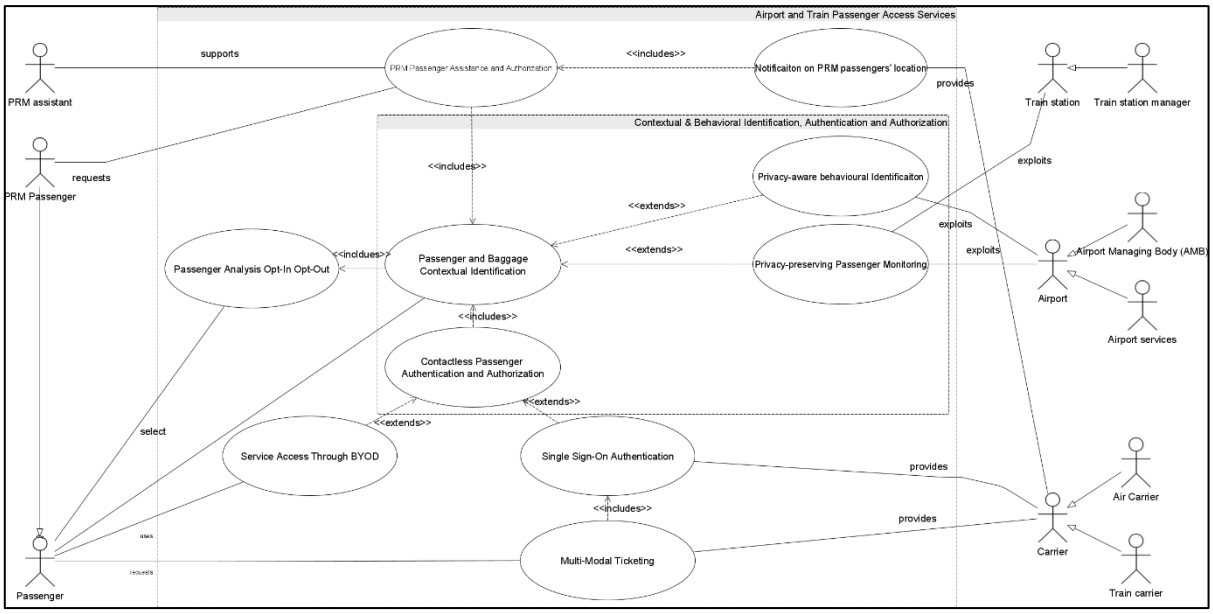

Figure 3 Airport and Train Passenger Access Services - UML Use Case diagram

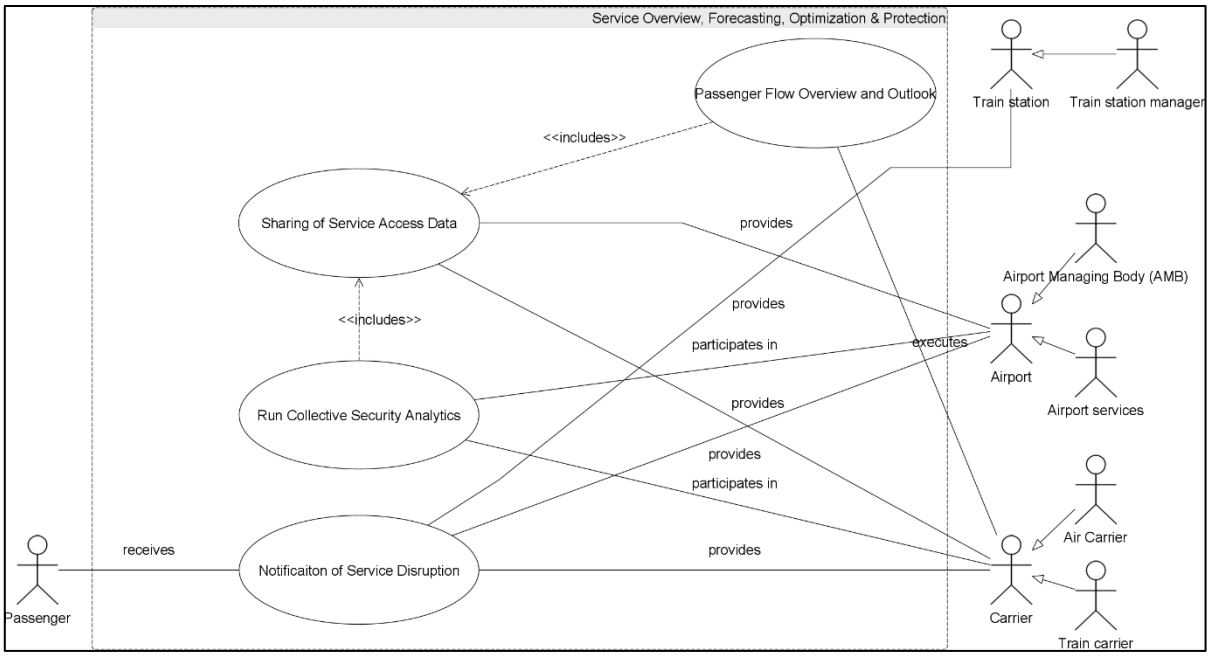

Figure 4 Service Overview, Forecasting, Optimization and Protection - UML Use Case diagram

2.2. Use Case Descriptions

2.2.1. AT-UC-01: PRM Passenger Assistance and Authorization

Use Case Name	PRM Passenger Assistance and Authorization
Participating actors	• PRM passenger • Air carrier • Train carrier • Airport managing body (AMB) • Train station manager
Purpose	The PRM passenger has declared her needs (during the booking process, or as soon as she reaches the airport, the train station or takes the first mode of transportation) and wants to receive the required assistance.
Priority	Must
Flow of events: Normal flow	1. The PRM passenger is identified and authorized thanks to the IAI 2. A SSR code is assigned 3. Appropriate policies are enabled 4. Policies and SSR code are propagated to all the relevant stakeholders through the ISI
Flow of events: Alternative flow	5. The SSR code is self-declared by the passenger during the booking process, so step 2 must be skipped
Pre-condition	• Train, air carriers and AMB have established agreements for managing PRM passengers • All the carriers and the AMB can map policies to their own format or a standard format is chosen
Post-condition	• All the services required by the PRM passenger are automatically and (as much as possible) proactively enabled and provided

Table 2. AT-UC-01 use case description

2.2.2. AT-UC-02: Passenger and Baggage Contextual Identification

Use Case Name	Passenger and Baggage Contextual Identification
Participating actors	• Passenger • Air Carrier • Train Carrier
Purpose	Thanks to contextual analysis, passenger and baggage are automatically identified at each touch point involved in a passenger's journey.
Priority	Must
Flow of events: Normal flow	1. Passenger provides the required documents and identify herself at the beginning of her journey (disregarding the chosen mode of transportation) 2. The passenger declares her baggage 3. Passenger and baggage are linked even if different routes are taken 4. Carriers share data (thanks to the ISI) and are able to identify passenger and her baggage thanks to contextual information
Flow of events: Alternative flow	5. Some security checks may require additional information or a higher confidence on the identification. Therefore manual operations must be put in place
Pre-condition	• Carriers are able to collect contextual information through sensors • Contextual information is shared among carriers in a privacy-preserving manner
Post-condition	• Thereafter, the passenger is automatically identified • Carriers and passenger are aware of the baggage location

Table 3. AT-UC-02 use case description

2.2.3. AT-UC-03: Contactless Passenger Authentication and Authorization

Use Case Name	Contactless passenger authentication and authorization
Participating actors	• Passenger • Air Carrier • Train Carrier

	• Airport
Purpose	Authenticate and authorize the passenger through contactless mechanisms and biometrical data.
Priority	Must
Flow of events: Normal flow	1. The passenger consents to share her biometrical data along the travel documents 2. Biometrical data are collected from the passenger and a DSA is attached 3. Carriers and airport are able to verify and match the biometrical data against the travel documents and booking information 4. The passenger gets her access granted to the gate or the requested service
Flow of events: Alternative flow	5. If the collected information does not reach the required confidence, additional requests may be issues or manual checks may be put in place 6. The authorization may be denied if the passenger does not have the credentials needed for the requested service (e.g., a valid ticket)
Pre-condition	• The passenger is travelling with and provides the required documents (e.g., passport and ticket) • Carriers and airport have the required tools to collect biometrical data from the passenger with the required confidence/quality.
Post-condition	• Passenger gains access to the requested service.

Table 4. AT-UC-03 use case description

2.2.4. AT-UC-04: Privacy-preserving Passenger Monitoring

Use Case Name	Privacy-preserving Passenger Monitoring
Participating actors	• Passenger • Airport managing body (AMB) • Airport services • Train station manager

Purpose	Passenger movements in the airport are monitored in a privacy-preserving way to support identification, security and optimization operations
Priority	Should
Flow of events: Normal flow	1. Passenger is identified at her arrival 2. Environmental sensors are able to monitor her movement in the airport and train station and have visibility over the passenger's location 3. Data are collected and analyzed in a privacy-preserving manner by airport and train station with the IAI deployed at the edge
Flow of events: Alternative flow	4. For some analytics (e.g., passenger flow), the monitoring could be performed in an aggregated form
Pre-condition	• Environmental sensors have the capability of recognizing people and their contextual attributes (e.g., location, performed activities) in areas with a high density of passengers • The passenger consents to be identified through sensor-based mechanisms and have her behavior modeled in exchange for better services
Post-condition	• Data generated by the analysis are available to the airport for service optimization, forecasting and security • Monitoring the passenger at key steps of her journey can support passenger identification if data are shared among stakeholders in a secure and confidential way (through the ISI)

Table 5. AT-UC-04 use case description

2.2.5. AT-UC-05: Passenger Analysis Opt-In Opt-Out

Use Case Name	Passenger Analysis Opt-In Opt-Out
Participating actors	• Passenger • Airport • Air carrier • Train carrier

Purpose	The passenger can understand and select the analysis that can be performed with the data collected from her
Priority	Must
Flow of events: Normal flow	1. Passenger requests any service to the airport or the carriers 2. A human intelligible Data Sharing Agreements (DSA) is provided to the passenger 3. The passenger can opt-in or opt-out to the different kinds of analysis and therefore customize the DSA 4. The analyses respect the DSA and access to the services is provided accordingly
Flow of events: Alternative flow	5. The passenger opt-out from all the analysis, therefore contextual identification and authentication services cannot be performed. In many steps, it would be required to revert to manual procedures
Pre-condition	• Alongside the DSA, the analysis services and benefits/consequences for opt-in/opt-out are described • The passenger has a basic knowledge on the analysis described in the DSA
Post-condition	• The DSA accepted by the user is saved, in case of auditing • The DSA is propagated to the corresponding services and the involved stakeholders

Table 6. AT-UC-05 use case description

2.2.6. AT-UC-06: Single Sign-On Authentication

Use Case Name	Single Sign-On Authentication
Participating actors	• Air carrier • Train carrier • Passenger
Purpose	The passenger needs to provide her travel documents and tickets only once
Priority	Must

Flow of events: Normal flow	1. The passenger provides all the required identification documents and tickets at the start of her journey 2. Carriers exchange the authentication data through standard and secure protocols 3. The passenger is automatically authenticated while approaching her next service or carrier
Flow of events: Alternative flow	4. When needed, delegation authorizations can be issued to provide details on the passenger identity. These authorizations must be logged in case of audits
Pre-condition	• Carriers and services have established bilateral or multilateral agreement • Identity management systems of each stakeholder can map the format of each other in their Circle of Trust (CoT)
Post-condition	• The passenger is authenticated through her home identity provider (where information and tickets were originally collected)

Table 7. AT-UC-06 use case description

2.2.7. AT-UC-07: Multi-Modal Ticketing

Use Case Name	Multi-Modal Ticketing
Participating actors	• Passenger • Air carrier • Train carrier
Purpose	Through the adoption of an e-wallet system and thanks to agreements between carriers, tickets for the corresponding carrier are automatically sold
Priority	Could
Flow of events: Normal flow	1. The passenger tries to access to a new mode of transportation for which she does not have the ticket 2. The carrier authenticates the passenger thanks to the continuous authentication of the IAI and pre-established agreements with the source carrier

	3. The carrier requests the e-wallet service to charge the passenger for the requested ticket 4. The passenger receives the ticket for the requested carrier
Flow of events: Alternative flow	5. The passenger does not have enough money in her e-wallet. In this case, her information could be automatically loaded in the vending machine but an alternative mode of payment must be used
Pre-condition	• Carriers have agreements for selling tickets in their Circle of Trust • The passenger has an e-wallet with enough money to buy the ticket for the requested service
Post-condition	• The ticket is bought by the passenger • An amount corresponding to the ticket price is charged on the e-wallet of the passenger

Table 8. AT-UC-07 use case description

2.2.8. AT-UC-08: Service Access Through Bring Your Own Device

Use Case Name	Service Access Through Bring Your Own Device
Participating actors	• Passenger • Airport • Air carrier
Purpose	The passenger can access to airport and In-Flight Entertainment (IFE) services through a BYOD (Bring Your Own Device) approach.
Priority	Could
Flow of events: Normal flow	1. The passenger opt for the BYOD approach 2. The service provider verifies the compatibility of the passenger device for the required service 3. Inputs are provided by the passenger through her own device 4. Multi-biometrics and travel data are used by the IAI to create a secure digital record useful for the passenger authentication

Flow of events: Alternative flow	5. The device used is not compatible, alternative service request mechanisms must be adopted
Pre-condition	• The device adopted by the passenger respect the hardware and software specifications requested by the service provider
Post-condition	• The passenger gets the requested services without any need to interact with any public device

Table 9. AT-UC-08 use case description

2.2.9. AT-UC-09: Sharing of Service Access Data

Use Case Name	Sharing of service access data
Participating actors	• Airport • Air carrier • Train carrier
Purpose	Stakeholders can share data about access to their services in a privacy-preserving manner while preserving data ownership
Priority	Must
Flow of events: Normal flow	1. Stakeholders express the kind of data they might be interested to 2. A Data Sharing Agreements (DSAs) is proposed by the data producer and accepted by the data consumer 3. Data are obfuscated or pseudo-anonymized before being shared
Flow of events: Alternative flow	4. If the preprocessing operations performed by the data producer are not compatible with the operations the data consumer is willing to perform, or if there is not an agreement on the DSA, the data sharing does not take place.
Pre-condition	• Stakeholders have established agreements and belong to the same Circle of Trust (CoT)
Post-condition	• Data are sent to the data consumer for processing

Table 10. AT-UC-09 use case description

2.2.10. AT-UC-10: Run Collective Security Analytics

Use Case Name	Run Collective Security Analytics
Participating actors	• Airport • Train station • Air carrier • Train carrier
Purpose	IDS (Intrusion Detection Systems) and security operations are collectively performed on the edge
Priority	Could
Flow of events: Normal flow	1. Stakeholders accept a common Data Sharing Agreement (DSA) 2. Data are converted in a commonly accepted format 3. Analysis are performed on the edge, and model and results exchanged
Flow of events: Alternative flow	4. The security operation interests a single stakeholder, and therefore the analytics are performed locally 5. If one of the stakeholders does not have the required computational power can also choose to share the data but do not join the analysis
Pre-condition	• Stakeholders have established agreements and belong to the same Circle of Trust (CoT)
Post-condition	• Security analytics are performed and results are shared with the interested stakeholders

Table 11. AT-UC-10 use case description

2.2.11. AT-UC-11 Notification of Service Disruption

Use Case Name	Notification of service disruption
Participating actors	• Passenger

	• Air carrier • Train carrier • Airport • Train station
Purpose	Passengers are informed by any disruption (e.g., service strike, delay, weather alerts, emergency state) they may incur during their journey
Priority	Could
Flow of events: Normal flow	1. The passenger provides information about her whole journey 2. Stakeholders register this request 3. Contextual/environmental disruptions affecting any of leg of the journey are notified to the passenger (through the ISI) alongside possible solutions or workaround
Flow of events: Alternative flow	4. In case of disruption, carriers can build alternative solutions and suggest these to the passenger
Pre-condition	• Carriers and airport must be able to register and distribute information about any disruption affecting the access to their services
Post-condition	• The passenger is informed on the service disruption and receives alternative solutions (if available)

Table 12. AT-UC-11 use case description

2.2.12. AT-UC-12 Passenger Flow Overview and Prediction

Use Case Name	Passenger flow overview and prediction
Participating actors	• Airport • Air carrier • Train carrier
Purpose	Dashboard for monitoring and predicting the passenger flow
Priority	Should

Flow of events: Normal flow	1. Sensors deployed in the areas managed by each stakeholder collect data 2. Stakeholders agree on Data Sharing Agreement (DSA) 3. Passenger flow are analyzed and used for prediction
Flow of events: Alternative flow	4. Contextual information regarding external events may be included in the analysis
Pre-condition	• Carriers and airport have sensors deployed in their environments • Stakeholders have established agreements and belong to the same Circle of Trust (CoT)
Post-condition	• Overview and prediction data are prompted in a dashboard and can be further used for optimizing the operations

Table 13. AT-UC-12 use case description

2.2.13. AT-UC-13 Privacy-aware Behavioural Identification

Use Case Name	Privacy-aware Behavioural Identification
Participating actors	• Passenger • Airport managing body (AMB) • Airport services
Purpose	Build a behavioural model of the passenger useful for her identification
Priority	Should
Flow of events: Normal flow	1. Sensors deployed in the areas managed by each stakeholder continuously collect data 2. Thanks to the collected data and privacy-aware analyses the passenger behavior is modeled (e.g., through a gait analysis) in the IAI and associated to her travel credentials 3. Such credentials are used to identify the passenger at each touch point
Flow of events: Alternative flow	4. Some analysis could also rely on aggregated data (i.e., how the passenger flow is behaving) and contextual knowledge (e.g., if a

	flight is late it is expected to observe a deviation on the passenger behavior)
Pre-condition	• Environmental sensors have the capability of recognizing people and their contextual attributes (e.g., location, performed activities) in areas with a high density of passengers • The passenger consents to be identified through sensor-based mechanisms and have her behavior modeled in exchange for better services
Post-condition	• The behavioral passenger identification can be used to provide a robust authentication mechanism • Services in the airport are able to analyze and share data in a privacy-preserving manner according to a DSA

Table 14. AT-UC-13 use case description

2.2.14. AT-UC-14 Notification on PRM Passengers' Location

Use Case Name	Notification on PRM Passengers' Location
Participating actors	• Passenger • PRM assistant • Airport • Air carrier • Train carrier
Purpose	Notify (pre-authorized) relatives about the location and status of the PRM passenger
Priority	Could
Flow of events: Normal flow	1. The PRM passenger inform the carrier services how and which information about herself should be shared with the indicated relative. The request is limited to the specified journey 2. The PRM assistant searches over a predefined set the appropriate DSA according to the properties specified by the passenger (including granularity of the status updates and notification policy)

	3. The relative is informed about specific events (push notification, e.g., "boarding process completed") or requests the current status (pull notification, i.e., under explicit request of status update)
Flow of events: Alternative flow	4. There is no DSA ready for use, therefore the PRM assistant will be in charge of creating the appropriate DSA to accommodate the passenger requests
Pre-condition	• The PRM passenger explicitly requests to share location and status concerning her journey with a relative
Post-condition	• The relative is informed about status and location of the PRM passenger

Table 15. AT-UC-14 use case description

2.3. Catalogue of Use Cases

Table 16: Mapping of Use Cases to User Stories

Use Case	User Stories
AT-UC-01	AT-US-01
AT-UC-02	AT-US-02 AT-US-03 AT-US-07
AT-UC-03	AT-US-01 AT-US-02 AT-US-05 AT-US-07
AT-UC-04	AT-US-03 AT-US-04 AT-US-06 AT-US-07
AT-UC-05	AT-US-01 AT-US-02 AT-US-03 AT-US-05 AT-US-07

AT-UC-06	AT-US-01 AT-US-02 AT-US-05 AT-US-07
AT-UC-07	AT-US-02 AT-US-07
AT-UC-08	AT-US-03 AT-US-05 AT-US-07
AT-UC-09	AT-US-02 AT-US-04 AT-US-06 AT-US-07
AT-UC-10	AT-US-04 AT-US-06
AT-UC-11	AT-US-02 AT-US-06
AT-UC-12	AT-US-06
AT-UC-13	AT-US-02 AT-US-03 AT-US-05 AT-US-07
AT-UC-14	AT-US-01 AT-US-03

2.4. Storyboard

The following storyboards recall some of the user stories introduced in Section 1.4 and use cases reported in Section 2.2.

2.4.1. AT-SB-01: Passenger Authentication in an End-to-End Safe-contact Journey

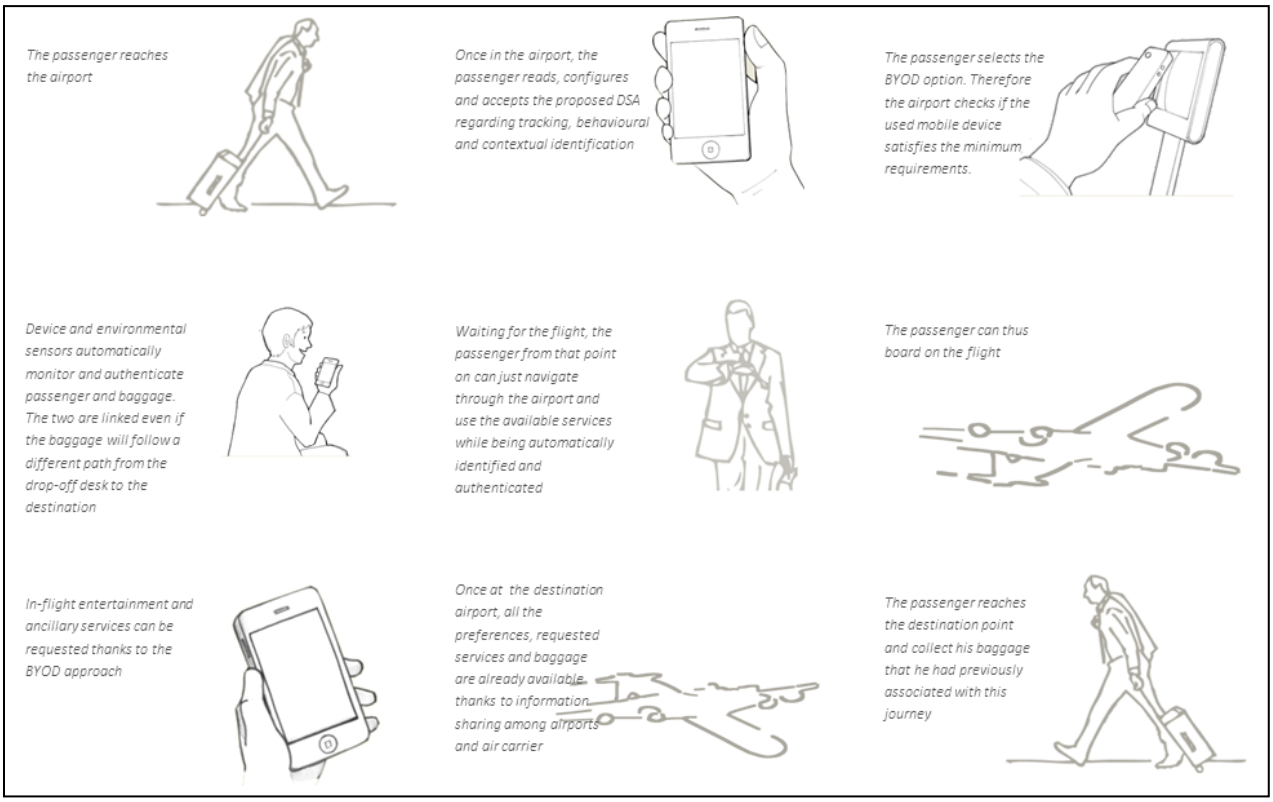

Figure 5: Passenger Authentication in an End-to-End Safe-contact Journey

The storyboard in Figure 5 represents the end-to-end safe contact/contactless journey (AT-US-05) enabled by BYOD (AT-UC-08), passenger and baggage identification (AT-US-01), monitoring (AT-UC-04), and contextual and behavioural authentication (AT-US-03).

2.4.1. AT-SB-02: Frictionless and Flexible Multimodal Journey

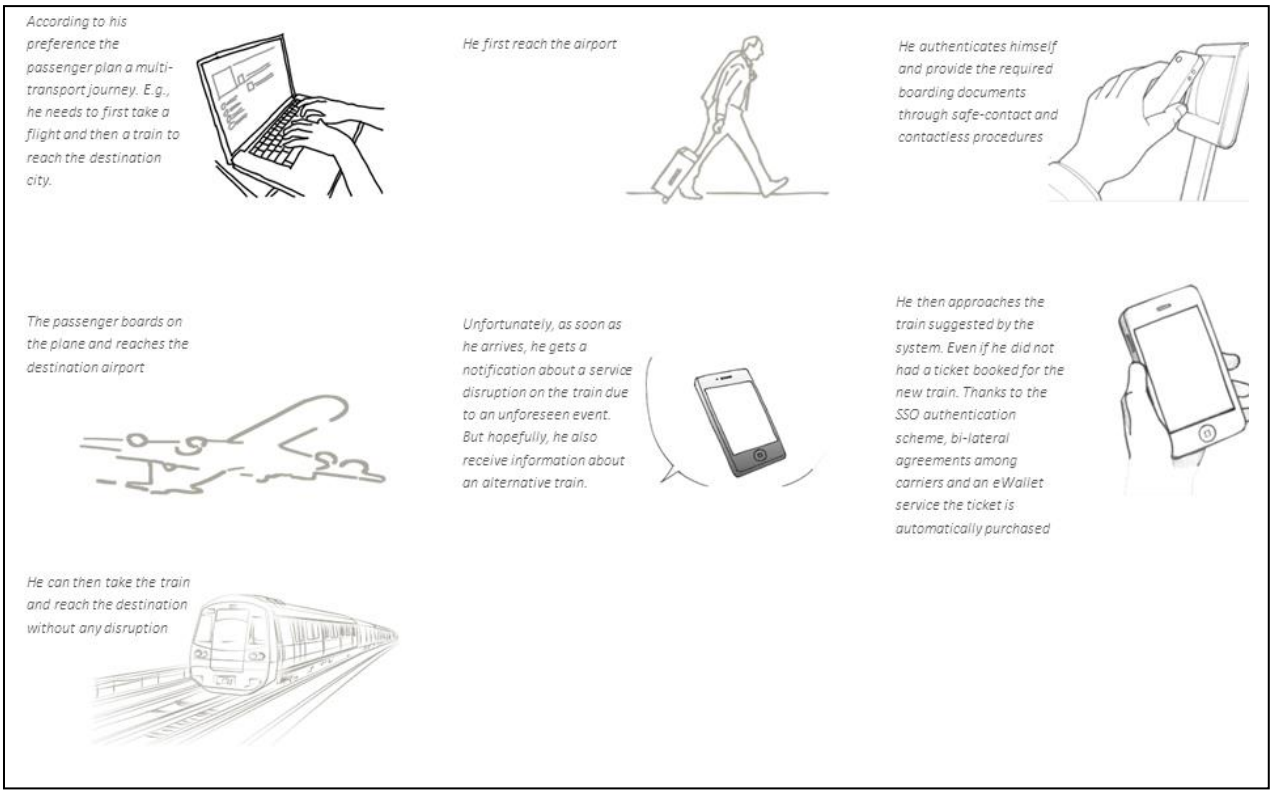

Figure 6 Frictionless and Flexible Multimodal Journey

The storyboard in Figure 6Figure 5 represents a flexible (AT-UC-07) and frictionless multi-modal journey (AT-US-02) enabled by the E-CORRIDOR framework in presence of service disruption (AT-UC-11), in which the passenger takes advantage of the document-free secure multimodal travel credential (AT-US-07).

2.4.1. AT-SB-03: Collective Intelligence for Performance Optimization and Protection

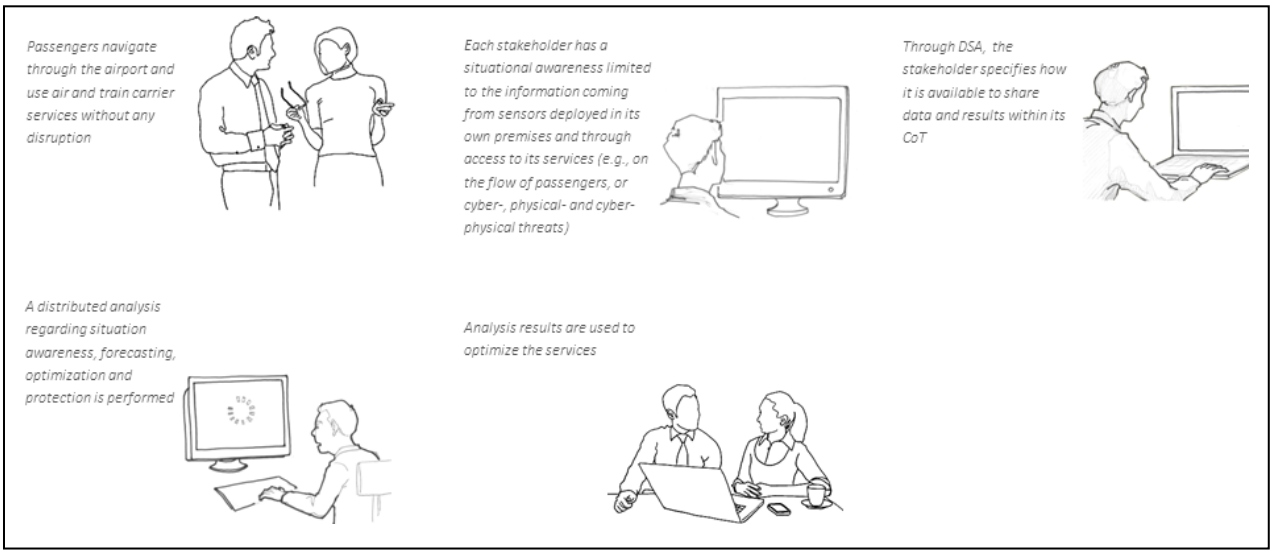

Figure 7 Collective Intelligence for Performance Optimization and Protection

The storyboard in Figure 7Figure 5 represents analysis, forecasting, optimization (AT-US-06) and security services (AT-US-04) enabled by the data sharing and collective analysis provided by the E-CORRIDOR framework.

3. Non-functional Requirements

Identifier	Description	Category
AT-NFR-01	Delegation authorization must be logged and available for auditing	Security
AT-NFR-02	All the collected passenger-related biometrical data must be obfuscated or encrypted before being further processed or shared	Data manipulation operation
AT-NFR-03	All passenger-related biometrical data must be processed in a confidential and privacy-preserving way	Security
AT-NFR-04	Data retention policy must be compliant with the applicable regulations (e.g., Article 5(1)(e) of the GDPR)	Security
AT-NFR-05	Passenger-data must be stored in encrypted format or pseudo-anonymized	Data manipulation operation
AT-NFR-06	The transfer of analysis results from the E-CORRIDOR platform to the AT Pilot should be secure with respect to confidentiality and integrity	Security
AT-NFR-07	Communication between stakeholders must be protected	Security
AT-NFR-08	Data and analysis results are shared on a need-to-know basis	Operational
AT-NFR-09	Data pertaining to the same type of sensor must be translated to a common format	Operational
AT-NFR-10	Collection of biometrical information should not disrupt the normal actions performed by the passenger	Usability
AT-NFR-11	Passengers should be able to understand by whom her biometric data are processed	Usability
AT-NFR-12	The processing time of passenger data should be compatible with a seamless authentication	Usability
AT-NFR-13	Stakeholders should be able to specify agreements for data sharing and analysis	Operational
AT-NFR-14	Analysis should be performed as much as possible on the edge to allow stakeholders an independent deployment, development and evolution of their tools	Operational
AT-NFR-15	Identity providers must share information respecting multilateral or (Peer-to-Peer) P2P agreements	Security
AT-NFR-16	Identity management systems must follow standard protocols (e.g., SAML, OAuth, OIDC, eIDAS)	Security

Table 17: List of Non Functional Requirements

4. Conclusions

This document described some of the challenges and opportunities in the next generation multi-modal passenger transportation with a focus on the air-train connection. Starting with an overview on the considered scenario and the current practices, present limits and opportunities to improve operations and passenger experience have been highlighted. Then functional and non-functional requirements to achieve the envisioned frictionless passenger experience and enhanced services and operations have been formalized by means of user stories and use cases.

The main challenges lying ahead in the air-train transportation involve privacy-aware data sharing and collective analysis. The E-CORRIDOR project envisioning a flexible, secure, robust, collaborative and confidential framework for information sharing and analytics will be able to ensure safety and security of multimodal transport systems while keeping the communication platform safe from cyber-attacks and ensuring service continuity. The edge and collective analytics paired with privacy-preserving data sharing will be able to preserve data ownership and comply with the applicable regulations while providing superior passenger experience and services in multi-modal transportation.

A. Appendix

A.1 Definitions and Abbreviations

Term	Meaning
AMB	Airport Managing Body
BYOD	Bring Your Own Device
CBP	Customs and Border Protection
CoT	Circle of Trust
DSA	Data Sharing Agreement
EASA	European Aviation Safety Agency
ECCSA	European Centre for Cybersecurity in Aviation
ESTA	Electronic System for Travel Authorization - US
ETA	Electronic Travel Authorization – Australia and Canada
ETIAS	EU Travel Information and Authorization System
EU	European Union
eIDAS	Electronic Identification, Authentication and trust Services
e-wallet	Digital wallet
GDPR	EU General Data Protection Regulation
H&S	Hub and Spoke
IATA	International Air Transport Association
IDS	Intrusion Detection System
IFE	In-Flight Entertainment
IIoT	Industrial Internet of Things
ISI	Information Sharing Infrastructure
M2M	Machine to Machine
MoSCoW	Must have, Should have, Could have, and Won’t have but would like
NEXTT	New Experience Travel Technologies
NFR	Non Functional Requirement
OIDC	OpenID Connect
P2P	Peer-to-Peer
PRM	People with Reduced Mobility
RFID	Radio-frequency identification
SAML	Security Assertion Markup Language
SSO	Single Sign-On

SSR	Special Service Request
UML	Unified Modelling Language
US	United States of America

A.2 Data types

Data type class	**Data format**	**Standard**	**Pilot UC id**
GPS data	GPX (GPS Exchange Format)	Open Standard	AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-09, AT-UC-11, AT-UC-12, AT-UC-13, AT-UC-14
GPS data from smartphone	NMEA 0183/GPRMC sentence: <Time, Status, Latitude, Longitude, Speed, Angle, Date, Variation, Integrity, Checksum>	Industry Standard	AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-06, AT-UC-08, AT-UC-13, AT-UC-14
boarding pass	BCBP (bar-coded boarding pass)	Industry Standard (IATA)	AT-UC-03, AT-UC-06, AT-UC-07, AT-UC-08
Passport	ICAO9303	Industry Standard	AT-UC-03, AT-UC-06
image (for facial, fingerprint, or iris recognition) in passport	JPEG, JPEG2000	Open Standard	AT-UC-03, AT-UC-06, AT-UC-08, AT-UC-13
accelerometer	JSON <time, x, y, z> in m/s^2	Open Standard	AT-UC-03, AT-UC-08, AT-UC-13
gyroscope	JSON: <time, x, y, z>	Open Standard	AT-UC-03, AT-UC-08, AT-UC-13
magnetometer	JSON: <time, x, y, z> in uT	Open Standard	AT-UC-03, AT-UC-08, AT-UC-13
Bluetooth RSSI (received signal strength indication)	JSON: <time, station id, RSSI>	Open Standard	AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-08, AT-UC-12, AT-UC-13, AT-UC-14
WiFi RSSI (received signal strength indication)	JSON: <time, station id, RSSI>	Open Standard	AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-08, AT-UC-12, AT-UC-13, AT-UC-14
camera	H.264, .mp4	Open Standard	AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-08, AT-UC-12, AT-UC-13, AT-UC-14

Lidar	LAS	Open Standard	AT-UC-02, AT-UC-03, AT-UC-04, AT-UC-08, AT-UC-12, AT-UC-13, AT-UC-14
RFID	raw bits	No standard	AT-UC-06
passenger data	JSON <name, surname, date of birth, place of birth, nationality>	Open Standard	AT-UC-06, AT-UC-14
network log	syslog-ng	Open Standard	AT-UC-09, AT-UC-10
event log	CEF	Open Standard	AT-UC-09, AT-UC-10
network log	NetFlow	Industry Standard (CISCO)	AT-UC-09, AT-UC-10
airplane tracking	ADS–B (Automatic dependent surveillance-broadcast)	Industry Standard	AT-UC-09, AT-UC-10, AT-UC-11

A.3 Requirements elicitation process

The pilot requirements collected in this document are the results of several (web call) discussions with three influential actors in the multimodal airport-train scenario namely, ADP, SNCF and Collins IMS. The first two are partners of the E-CORRIDOR project whereas the latter has been reached by UTRC through the Raytheon Technologies network.

Collins Information Management Services (IMS), part of the Collins Aerospace, is a leader in technologically advanced and intelligent solutions for aerospace, airport, rail, defence, and critical infrastructure industries.