



D3.3

First Implementation, Test and Validation of the Smart city and Carsharing (S2C) Pilot

WP3 – S2C Pilot

E-CORRIDOR

Edge enabled Privacy and Security Platform for Multi Modal Transport

Due date of deliverable: 31/07/2022

Actual submission date: 30/09/2022

31/07/2022

Version 1.0

Responsible partner: CLEM'

Editor: Mohammed AMMARA

E-mail address: mohammed.ammara@clem-e.com

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:

Mohammed Ammara, Stanislas Soufflet, Bruno Flinois (CLEM), Pedro Coutinho, Stefania Pesavento (FC), Eloi Martin (PLD), Henry Gadacz, Christian Plappert (FhG), James O'Rourke (TSSG), Thanh Hai Nguyen (CEA)

Approved by:

James O'Rourke (TSSG), Claudia Zago (HPE)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	09-Feb-2022	Mohammed Ammara	CLEM'	Initial table of content
0.2	11 th July 2022	Mohammed Ammara	CLEM'	Table of content synchronization with other Pilots and first content inputs
0.9.2	12 th august 2022	Alejandro Camacho	CLEM'	Review
0.9.3	30 th august 2022	James O'Rourke	TSSG	Final Review
0.9.3	30 th august 2022	Claudia Zago	HPE	Final Review
1.0	02 sept 2022	Mohammed Ammara	CLEM'	Merge reviews remarks and final touches

Executive Summary

This deliverable along with the software repositories and demonstration videos, presents, the implementation the tests and the first experimental evaluation accomplished at Month 26 (M26) for the Smart city and Carsharing Pilot (S2C Pilot). For reminder, The Pilot is the evaluation of the E-CORRIDOR Framework capabilities and the E-CORRIDOR analytics toolbox and the edge-enabled deployment features in the context of multimodal mobility in urban and peri urban settings.

The current implementation shows a fully functioning main scenario from registration to trip planning to booking with the usage of different analytics services from the E-CORRIDOR analytics toolbox. Additionally, the current implementation integrates intrusion detection analytics, FHE-based fact checking and behavioural driving identification into the Pilot which fulfils all the scenarios and use cases. The aforementioned integrations are features answering the requirements as expressed in D3.1 in a designed architecture in D3.2.

Most of the acceptance tests were performed and succeeded, especially for the main scenario. In the remaining months, full integration of ISI and IAI using finalized Data Sharing Agreements for data governance will be finalized with the goal of readiness for the subsequent final evaluation and experimentation in the real-world production environment.

Table of contents

- Executive Summary 3
- 1. Introduction 5
 - 1.1. Overview 5
 - 1.2. Goals 8
 - 1.3. Structure of the Deliverable 8
- 2. Pilot Architecture and E-CORRIDOR Framework Integration 9
 - 2.1. Architecture 9
 - 2.2. Deployment model 9
 - 2.3. Integrated components 10
 - 2.3.1. eWallet 10
 - 2.3.2. TSM (Trusted Service Manager)..... 10
 - 2.3.3. Fleet data sharing 10
 - 2.3.4. Privacy-preserving trip planner 10
 - 2.3.5. Carbon footprint analytics 11
 - 2.3.6. Micro-subsidies analytics 11
 - 2.3.7. Intrusion detection analytics & security services 11
 - 2.3.8. FHE-based checker analytics 12
 - 2.3.9. Secure routine for driver identification - Driver DNA..... 12
- 3. Implementation, Test and Validation Environment 13
 - 3.1. Environment 13
 - 3.2. Pilot Status 14
 - 3.3. Workflows 24
- 4. First Experimental Evaluation..... 27
 - 4.1. Data Sources 27
 - 4.2. Acceptance Testing..... 27
- 5. Requirements Traceability Matrix 36
- 6. Contribution to pilot and project objectives 38
- 7. Conclusion..... 39
- A. Appendix 40
 - A.1 Definitions and Abbreviations..... 40
- 8. References 42

1. Introduction

1.1. Overview

Multimodality is at the heart of sustainable mobilityⁱ. Promoting sustainable alternative modes of transportation, in lieu of personal car usage, is hindered by the fact that multiple modes are required to do a door to door trip compared to using a personal car. The path to sustainable multimodality is removing friction and obstacles for the traveller as well as for the mobility service provider.

Multimodality poses several challenges. For the travellers; it is the interaction with multiple entities (MSPs (Mobility Service Providers), public transport authorities, ticketing systems, user interfaces ... etc), most notably the fact that the traveller needs to register multiple times and manage data privacy in a complex and obscure way through different interfaces, in addition, the traveller needs to manage availabilities, bookings and pricing seeking this information from different sources. For the mobility service providers, it is the data governance, personal information data exchange, managing cybersecurity and Trust in the data sharing system and in the “partners” with whom the data is exchanged. Identity management and verification (notably in services where the traveller is the person driving). Furthermore, the integration into data sharing systems poses a cost of integration and technological risks as each mobility service provider has already made their own in-house information systems that are incompatible with one another without substantial modification.

The E-CORRIDOR Framework offers: Edge-enabled, flexible, privacy-aware, secure data sharing, a rich toolbox of analytics and the ISAC-MMT (Multimodal transportation Information Sharing Analysis Center). These capabilities will be exploited to offer a secure and frictionless multimodal experience in the S2C Pilot answering the requirements defined in D3.1.

We present the following scenarios involving multiples stakeholders (In this context all of them are data prosumers):

Scenario 1 (Main scenario): *S2C-UC-01 S2C-UC-02 S2C-UC-03 eWallet + trip planning + micro-subsidies*

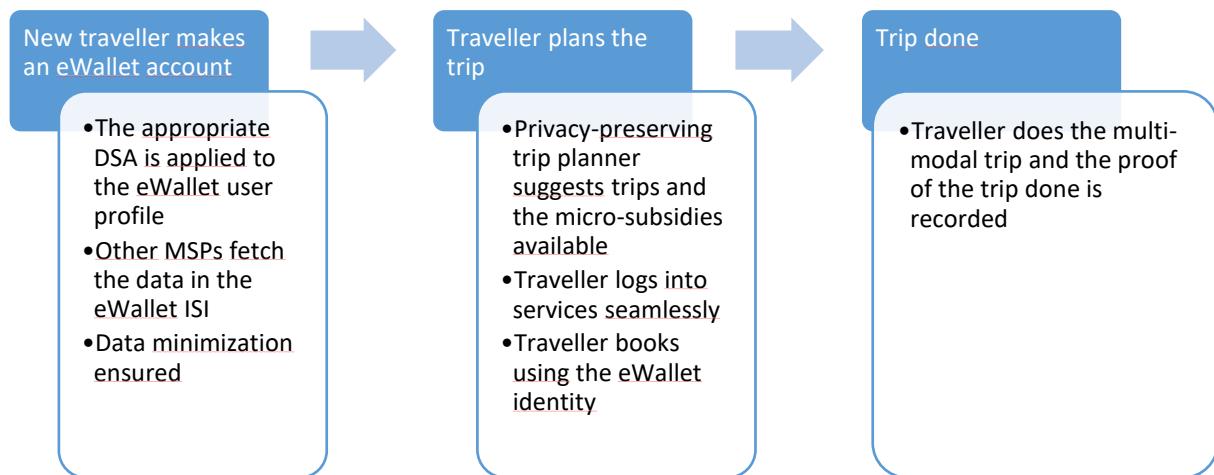


Figure 1 : Scenario 1 (Main scenario)

The first scenario describes the main three main user cases of the S2C Pilot:

The traveller registers only once and chooses the mobility services he or she wants to use. The traveller's personal data are stored in the eWallet's ISI and its data sharing is regulated thanks to the DLI which defines and enforces the DSAs (Data Sharing Agreement). DSA ensure that the least amount of data is shared to each MSP. The authentication and authorization mechanisms are managed by the TSM component (Authentication web service).

The traveller logs in using the eWallet identity, plans the trip using the privacy-preserving trip planner, carbon footprint analytics and the micro-subsidies analytics.

The trip request involves 3 analytics and thus different data sources from different ISIs:

- The fleet data about the shared cars availabilities and about the bus lines.
- The traveller's personal data.
- The trip request: time and location of the origin. Location of the destination. Preferred modes of transportation.

Multiple trips are suggested encompassing the different steps of each trip with details and redirections to each MSP's platform, the SSO (Single Sign-on) is ensured thanks to the TSP component and its OpenID Connect implementation. This way the traveller only registers once and only logs in once, the redirections to the MSP's respective platforms are done seamlessly without the need to type in the credentials (username & password).

The traveller preselects and books each segment of the trip. Once the traveller has completed the entirety of the trip, the Mobility service provider records into the eWallet a summary of the concluded trip and bookings.

Scenario 2 : S2C-UC-04 Cyberthreat management and intrusion detection

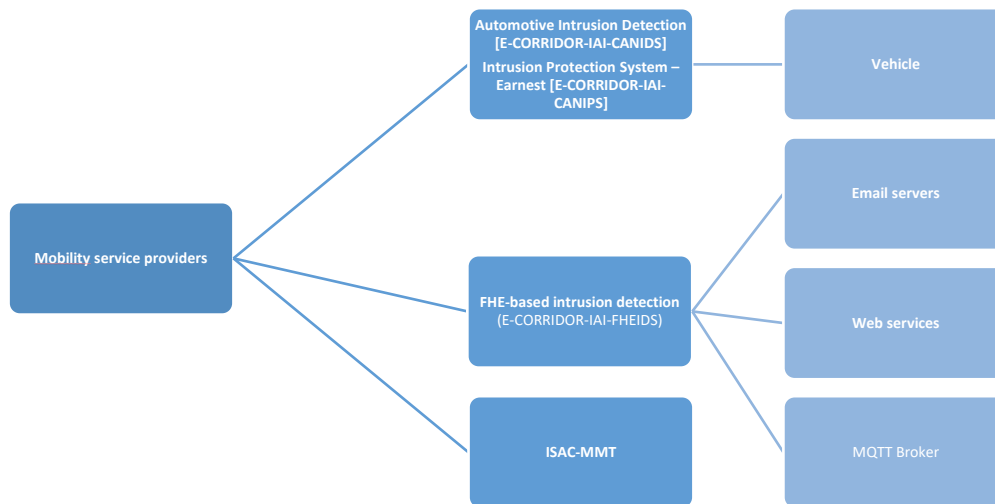


Figure 2 : Scenario 2

Thanks to intrusion detection analytics offered in the E-CORRIDOR framework and thanks to the multimodal transportation ISAC, Mobility Service Providers are alerted about intrusion and malicious files. The intrusion detection analytics and the multimodal transportation ISAC use data from different sensitive sources such as the vehicles, the e-mail servers, various web services and MQTT Broker (centrale node in a network of IoT embedded hardware on the vehicles that controls the access to the vehicle)

Scenario 3 : S2C-UC-05 : Privacy-preserving interest-based sharing

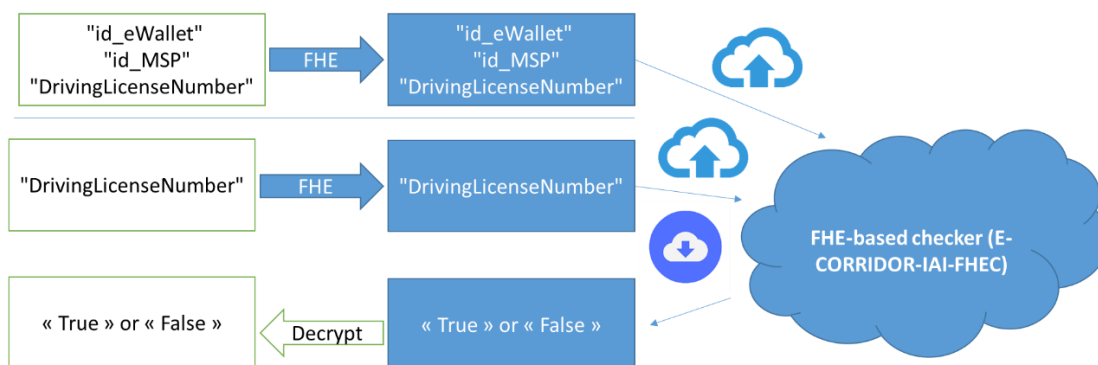


Figure 3 : scenario 3

A list of banned driving licenses is populated by multiple sources under a Fully Homomorphically encrypted format. This encryption ensures that the multiple sources cannot know each other’s respective inputs, neither can the FHE-based checker analytics.

A Mobility Service Provider needs to understand if a driving license number exists on the list, the FHE-based checker receives the driving license number to check in an encrypted format, the FHE-based checker compares the input to the list of banned driving licenses (encrypted format) without any decryption. The Mobility Service Provider receives the result “True” or “False” encrypted, it gets decrypted locally and thus only the Mobility Service Provider knows the result.

Scenario 4 : S2C-UC-06 : Driving behavioral recognition

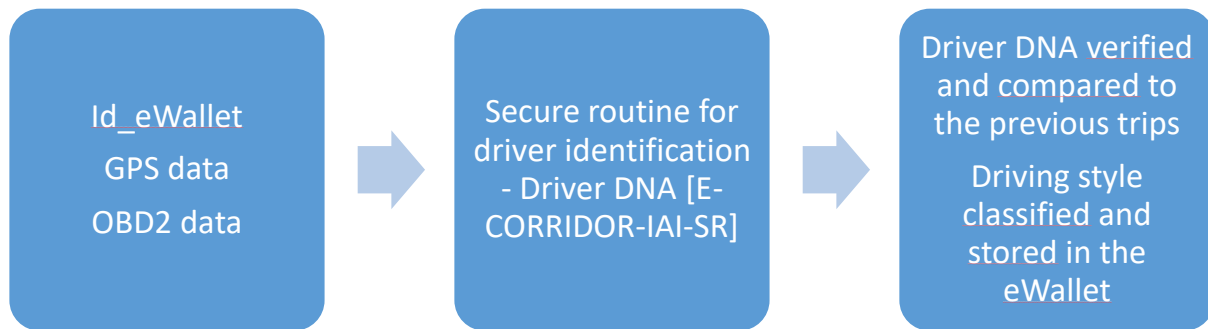


Figure 4 : scenario 4

Data from the OBD2 connector and from a GPS tracker in the car. Secure routine for driver identification - Driver DNA uses the data to determine the identity of the driver compared to previous data from the same driver, also to classify the driving style such as the eco-driving aspect, the goal is to run these analytics locally.

1.2. Goals

The requirements defined in D3.1 can be summarized into the following list of practical goals:

- Allow single registration of travellers at multiple mobility service providers through a shared eWallet containing the traveller's information and manage data sharing in a privacy preserving and flexible way.
- Enable micro-subsidies for multimodal trips that are based on trip characteristics and on driver profile characteristics stored in the eWallet.
- Share data of multiple types and sources using homomorphic encryption techniques for mobility analytics use cases and for cyberthreats management and intrusion detection.
- Deliver a privacy-preserving itinerary planning and carbon footprint analytics service.
- Enable behavioural driver identification analytics.

1.3. Structure of the Deliverable

The following chapters of the deliverable will follow three steps:

- We will present the built architecture of the Pilot; the deployment model and we will unpack and explain each of the Integrated components functioning and interactions.
- In section 3, the environment and the technologies used will be presented explaining the reasoning behind these choices. The current Pilot status will be presented and the remaining work to do. The workflows representing the Pilot scenarios as data sharing regulated with the Data Sharing Agreements.
- Section 4 summarizes the experimental evaluation of this first implementation and suggests steps towards final evaluation due by the end of the programme.

To conclude, the link between the requirements and the Acceptance tests will be formed by a matrix [Section 5], then the link between the Pilot and the E-CORRIDOR objectives will be explored [Section 6].

Note to the reader: Despite the effort in keeping the document self-contained, it is assumed that the reader is already familiar with the E-CORRIDOR architecture, the eWallet, the micro-subsidies concept, the OpenID Connect protocol and the previous WP3 deliverables.

2. Pilot Architecture and E-CORRIDOR Framework Integration

2.1. Architecture

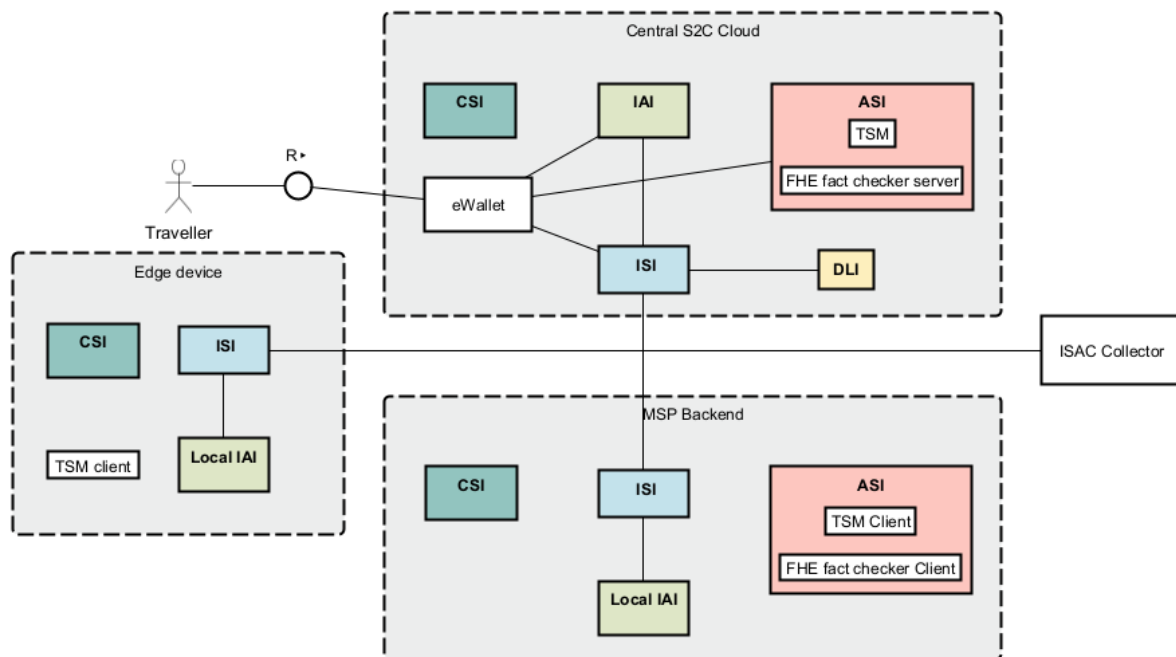


Figure 5 : S2C Pilot architecture

The architecture has 4 entities that we consider data prosumers: the Traveller, the Mobility Service Provider, the ISAC and the device on the vehicle.

The S2C Pilot architecture is hybrid, it combines central elements and elements running on mobility service providers' premises, while other elements are exceptionally running on edge devices on vehicles. All of them have a link to the ISAC collector.

The element facing the travellers directly is the eWallet web app from the eWallet component. The latter interacts with the travellers to register them using the TSM, to manage their trip requests using fleet data, the request and user profile stored in the ISI. The data exchange is regulated with rules written in CNL in the DSAs and enforced thanks to the DLI. The DSAs preconfigured are chosen according to the traveller's preferences as expressed in the registration step.

Micro-subsidies, trip planning and Carbon footprint analytics are located in the Central S2C Cloud and interact directly with the eWallet. FHE-based fact checker has two components distributed between the Central S2C Cloud and the MSP. Intrusion detection analytics and FHE based intrusion detection are running at the MSP's premises this is different from the vehicle intrusion detection analytics and the driver behavioural identification analytics that are running at the edge device.

TSM clients are available at every entity to ensure secure communication.

2.2. Deployment model

The S2C Pilot's deployment model is hybrid, thus exploiting E-CORRIDOR's edge-enabled capabilities. In fact, the eWallet, the TSM (and its authentication webservice) are centrally deployed on the cloud since they are central and unique elements in the Pilot.

Most of the components are deployed centrally in the cloud except for the following:

- The FHE-based checker’s deployment model is hybrid: the verification function runs centrally in the cloud. The Input to populate the list of the driving licenses and the output of the analytics are respectively encrypted and decrypted in the Mobility Service Provider’s premises (Locally).
- The Secure routine for driver identification - Driver DNA is deployed locally in the car in order to ensure the privacy of the behavioural data.

2.3. *Integrated components*

2.3.1. **eWallet**

The eWallet is the central component of the S2C Pilot, it is composed of 3 elements:

- **eWallet web app:** the user interface allowing the traveller to search for a multimodal trip, the eligibility for micro-subsidies and the redirections to the Mobility Service Provider’s platforms.
- **eWallet backend:** it manages the storage and sharing of the registered traveller’s personal information through the ISI and the DLI.
- **eWallet authentication server:** it is based on the TSM component from the ASI, it allows for:
 - the registration and the authentication to the eWallet web app
 - The Single-Sign on between the eWallet and the Mobility Service Providers’ platforms.

It has its own web user interface, the design of this interface and of the eWallet web app interface are similar so the redirections necessary through the OpenIdConnect workflow are done smoothly from the User Experience point of view.

2.3.2. **TSM (Trusted Service Manager)**

In addition to the integration of the TSM into the eWallet authentication server, the TSM will be deployed in the intrusion detection device and in the driver identification - Driver DNA device in the vehicles, it will be also deployed in the fleet data sharing ISIs in each of the Mobility Service Providers premises.

The TSM protects the devices and the eWallet thanks to its usage of the hardware based TPM (Trusted Platform Module) 2.0 as Root of Trust (RoT) to verify the integrity of the firmware against tampering and in case of tampering, fails the TLS handshake.

2.3.3. **Fleet data sharing**

Real-time information about the fleets of each of the Mobility Service Providers such as the booking calendars of shared vehicles, the timetables of the bus lines etc are inputs to the Analytics functions that suggest the trips to the travellers and calculate the carbon footprint. The ISI and DLI from the E-CORRIDOR framework are used to manage this data sharing.

2.3.4. **Privacy-preserving trip planner**

Planning a multimodal trip is a complex task, it is a multi-criteria optimization problem. Thus, planning a trip is one of the barriers to multimodality. Travellers have an Origin and Destination, preferences about the expected duration of the trip, the price, the modes of transportation etc. The traveller needs to register at all the potential Mobility service providers, visit each platform to understand and memorize the availabilities and the origin-destination for

the different legs of the trip creating the desired traveller's Origin – traveller's Destination. Furthermore, the traveller manages his or her data privacy regarding each of the Mobility Service Providers.

The complexity of the tasks demonstrates the need of a fully integrated privacy-preserving trip planner. The analytics combine the eWallet (traveller's information and preferences), the fleet data shared from the Mobility Service Providers and the OpenStreetMap geographical data to suggest trips to the traveller on the eWallet web app using a unique eWallet identity.

2.3.5. Carbon footprint analytics

The traveller needs to know and understand the carbon footprint of the different suggested trips. To calculate the carbon footprint, the analytics need as an input the distance of each leg of the suggested trip, data about the Carbon intensity (Emissions per km travelled) of each mode of transportation from the Mobility Service Providers.

Combined with the privacy-preserving trip planner and the eWallet web app. The traveller is informed about the carbon footprint of each suggested trip and therefore can include this criterion.

2.3.6. Micro-subsidies analytics

Socio-geographic dependant micro-subsidies are very well targeted subsidies of a small amount, they can be attributed based on the mode of transportation, the origin-destination, and the time of departure for the whole trip or for just one leg of the trip, personal information from the eWallet profile or any combination of the listed items. Very well targeted subsidies allow Public Transportation Authorities to subsidise sustainable modes or groups of people while avoiding undesirable market distortions. The subsidies analytics allow also for collaboration between mobility service providers, for instance, a traveller is more likely to take a bus/train than a personal car, if a shared car is available at the bus station to use it for the "last mile".

2.3.7. Intrusion detection analytics & security services

Openness of Mobility Service Providers to data sharing improves the quality of service and makes possible seamless multimodal trips, however this openness increases the attack surface and proves the necessity for cyberthreat management and intrusion detection.

Leveraging E-CORRIDOR framework's edge-enabled deployment model, we can use multiple analytics from IAI and security services from the ASI on different premises, for instance:

- **On the vehicles level:**

Automotive Intrusion Detection [E-CORRIDOR-IAI-CANIDS] analyses data from the car IoT system and from the MQTT broker managing the IoT that gives/revokes access to the car.

Intrusion Protection System – Earnest [E-CORRIDOR-IAI-CANIPS] analyses data from the car's CAN BUS.

- **On the webservices level:**

FHE-based intrusion detection (E-CORRIDOR-IAI-FHEIDS) analyses data from the webservices logs, the e-mail server's logs, and also from the MQTT Broker to detect intrusions and anomalies. The Fully Homomorphic Encryption ensures the privacy of the shared data for analysis.

- **On a global level:**

ISAC-MMT fosters collaboration between different Mobility Service Providers from different modes of transportation and exploits public data sets and information about the latest vulnerabilities. This interaction provides MSPs with webservices (analytics) to conduct scans, verifications and tests on suspicious files or addresses. It keeps MSPs notified about the latest threats with personalized notifications, and it provides a visualization of labelled data to help better understand the results of the analytics.

2.3.8. FHE-based checker analytics

Mobility Service Providers need to verify documents (driving license, identity card ... etc) before allowing the traveller to use the service. A collaboration between Mobility Service Providers through data sharing about the travellers such as (Validity of documents, good drivers, bad drivers, eligibility for price reductions ... etc) is also needed, however, the issue with data sharing in the context of collaboration between multiple parties is the disclosure of information required.

The issue is solved thanks to Fully Homomorphic Encryption: the computation is done on encrypted data without decrypting it. Also, the multiple inputs to the central computation are not disclosed neither to the entity doing the calculation nor to the other multiple entities who send inputs for the computation.

This form encourages data sharing and collaboration to centralize or aggregate data.

2.3.9. Secure routine for driver identification - Driver DNA

Mobility Service Providers cannot identify when an unauthorized use of the vehicle through identity usurpation occurs. Behavioural data analytics using the driving style and other metrics from the car can help detect unauthorized uses.

This valuable yet very personal data can also be used to incentivize eco-friendly and safe driving.

3. Implementation, Test and Validation Environment

This section describes the Pilot environment and the technical choices/trade-offs, the status of the Pilot's components and their integration, and the workflow describing the interactions between the components and the usage of the DSAs (Data Sharing Agreements) defined and enforced thanks to the DLI (DSA Lifecycle Infrastructure).

3.1. Environment

As explained in Section 2 (and more extensively defined in D5.3), the components will run as web microservices in docker containers set up using the Ingress concept, all interactions between the docker containers will happen through exposed RESTful APIs and authenticated with the Identity Manager (Keycloak). The containers of the eWallet, ISI and the IAI containing Trip planning analytic and the Carbon footprint analytics will be deployed on the same Virtual machine.

We present the technologies selected to build the components and the influences on these choices. Mature and widely used technologies with regular security updates were preferred with the goal of TRL 7 in mind:

- The eWallet web app is built using React.js, it is one of the most popular web developments frameworks, it offers a rich web experience with efficient software development and easy testing.
- The eWallet authentication server is built using Flask, a python-based backend framework is preferred in this case since the TSM will be mostly Python based, data exchanged is signed by the server using the itsdangerousⁱⁱ package. MarkupSafeⁱⁱⁱ package is used for character escaping the user's inputs in the authentication server's web pages.
- The eWallet web app and eWallet authentication server's web interfaces use the same CSS to offer a smooth user experience and the same visual identity.

Mobility Service Providers often have proprietary and in-house made information systems. Usage of the most standardized data format available is therefore preferred and required for a successful exploitation of the E-CORRIDOR framework. That's why the carsharing operator in the pilot shares fleet data in the GBFS format, the DRT operator (demand-responsive transit) used GTFS format. The first version of the integration between the eWallet, the two MSPs, and the trip planning, carbon footprint and micro-subsidies analytics used the Paris geographical OpenStreetMap data. The real-world planned Pilot with real users is expected to operate in the city of Santa Suzanna. An update of the data but not the format is expected.

The intrusion detection input from the production webservices of the MSPs is adapted in this first implementation for Apache server logs since most partners of the consortium already use Apache. Apache is the 2nd most widely used webserver right behind Nginx. The two cover 60% of the web servers on the internet. An adaptation for Nginx will be developed to cover the two most widely used web servers.

The MQTT technology is widely used to communicate with IoT objects thanks to its lightweight and flexible characteristics (low usage of bandwidth, low latency, and high scalability), it is used by Meta in Instagram and Messenger for the chat functions. in the case of carsharing it is used by Clem' (but also by BMW and Volkswagen) to manage remotely the access to the vehicles.

The MQTT Broker is the central element of the architecture and the most sensible, hence the need to highly secure it. In fact, a DDoS or an intrusion can render a whole fleet inoperative. The AI-based intrusion and anomaly detection technology offered by E-CORRIDOR is very promising.

The single sign on (SSO) using the eWallet identity to log into the eWallet web app and then seamlessly into MSPs platforms is based on the OpenID Connect. It is a proven protocol, widely used and easy to integrate with existing OAuth 2.0 servers.

Among the 3 Authentications flows available in the OpenID Connect, we have chosen the Authorization Code Flow^{iv} since it is the most adapted to our requirements and the most secure. In fact, it offers a maximum of communication server-to-server which we can secure thanks to the TSM, and the browser does not get access to the exchanged token nor do we depend on a script running in the browser for authentication.

Some slight modifications in the MSP's platforms were necessary to enable the SSO (registration of the MSP as client for the eWallet) and the automatic selection of the suggested vehicle/bus stop in the eWallet web app, the latter has been implemented through a simple parameter in the redirection URI.

3.2. Pilot Status

S2C features	Short Description	Implementation	Testing	Contribute to UC
eWallet identity	Workflow for traveler subscription and authentication and central traveler data repository	✓	🔵	UC-01, UC-02, UC-03
Trip planning	Workflow for itinerary suggestions for a traveler registered in the eWallet according to multiple factors	✓	🔵	UC-01, UC-02, UC-03
Micro-subsidies	Workflow for trip request analysis and micro-subsidy attribution Workflow for justifying and accounting micro-subsidies	✓	🔵	UC-01, UC-02, UC-03
Cyberthreat management & intrusion detection	Workflow for security & integration with the ISAC pilot (WP4)	🔵	🟡	UC-04
Driving licence verification	Workflow for verifying driving license between MSPs through FHEncryption	✓	🔵	UC-05
Driving behavioural identification	Using an OBD reader to analyze data and share the result in order to identify the driver from the driving behavior	🟡	🟡	UC-06

Figure 6 : S2C Pilot status summary

- 🟡 *in progress*
- 🔵 *advanced*
- ✓ *completed*

Figure 7 : Legend

The table summarises the current progress of the S2C Pilot, in fact, the components necessary for the main scenario (eWallet + trip planning + carbon footprint analytics + socio-geographic dependent micro-subsidies + SSO with station automatically selected) are completed and integrated including the necessary modifications in the MSP's Platforms.



Welcome

This webapp is the user interface for the S2C Pilot of the E-Corridor project (<https://e-corridor.eu/>). It includes user registration on the E-Corridor eWallet and the integration of a Trip Planner that will allow the user to plan a trip that will use the electric carsharing service from Clem (<https://www.clem-e.com/>) and the bus-on-demand service from Nemi (<http://www.nemi.mobi/>).

SIGN IN

REGISTER



Figure 8 : eWallet welcome page

Street address
Coimbra

City
Coimbra

Postal code
54321

Country
Portugal

Maximum walking distance in meters
1500

Driver license expiry date
30 / 06 / 2022

Driver license identifier
54321

I accept the following services access my data:
NEMI
CLEM

I accept the [terms and conditions](#)

Register

Already have an account? [Log in.](#)

Figure 9 : eWallet registration page



Homepage of authServer

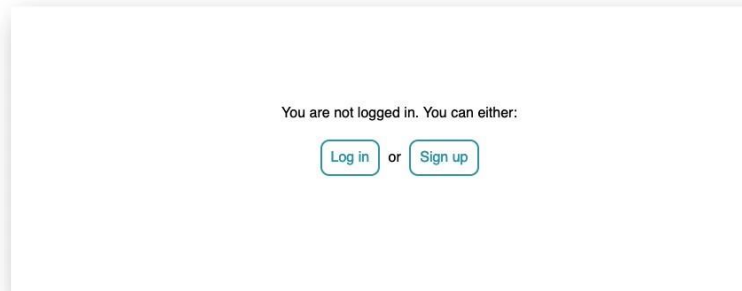


Figure 10 : TSM (authentication server) web page



Log In

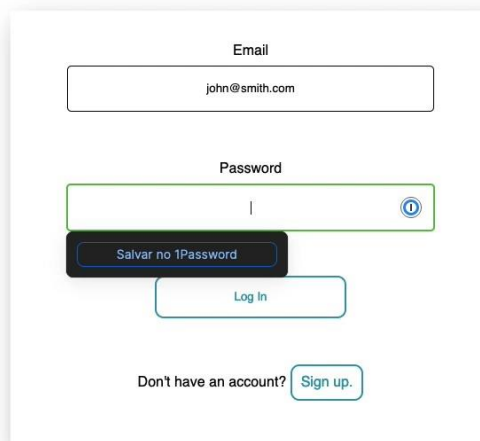


Figure 11 : eWallet login page



Authorize access

e-corridor-webapp is requesting access to: **openid email profile address phone user_preferences driver_license tickets**

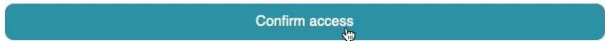


Figure 12 : Authorization step for the SSO

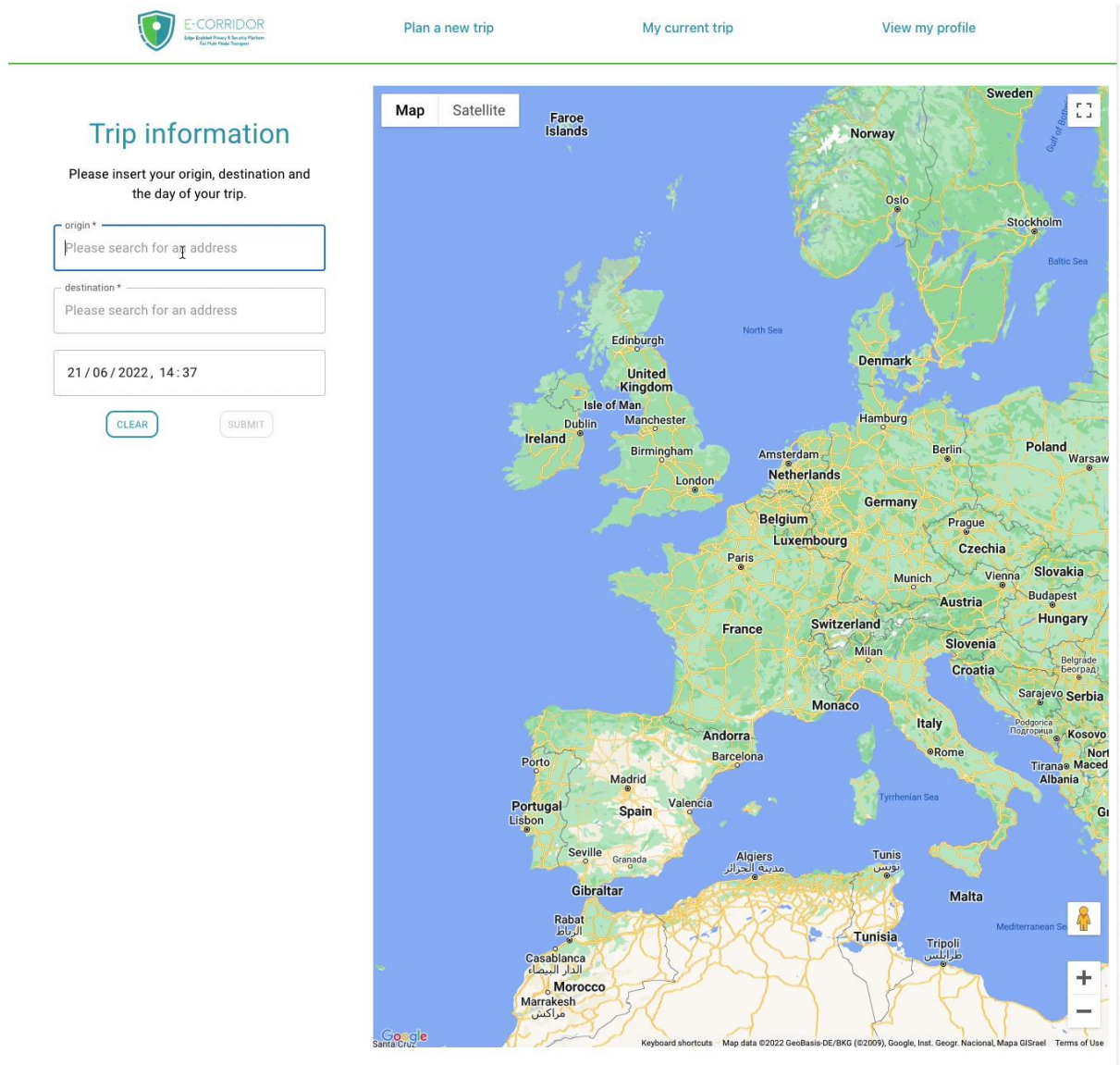


Figure 13 : eWallet Trip planning interface

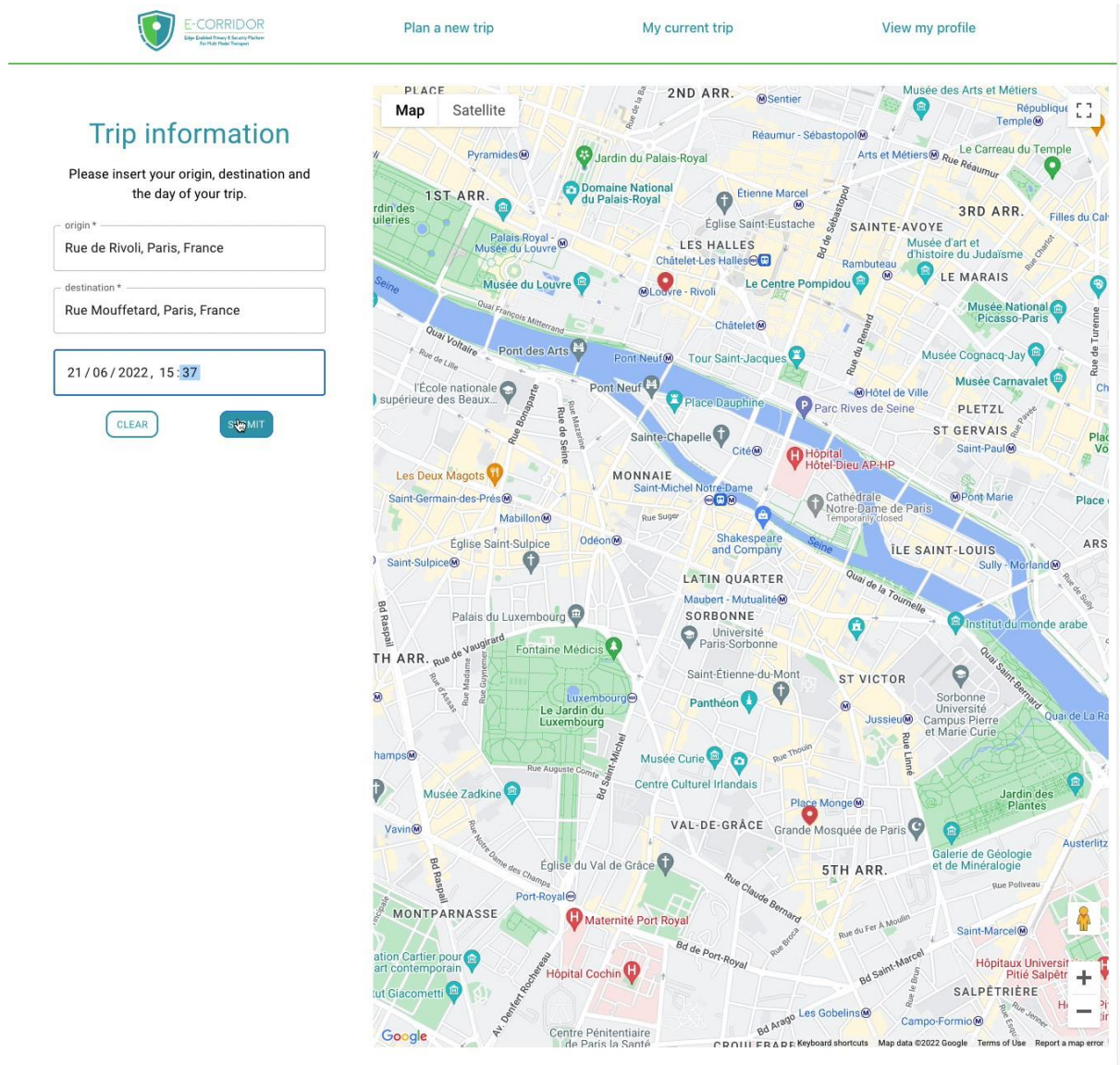


Figure 14 : eWallet Trip planning interface

```
toPlace=48.8204283539517%2C2.36480712890625&
time=3%3A35pm&
date=10-13-2021&
mode=BUS%2CWALK%2CBICYCLE_RENT&
maxWalkDistance=5000&
arriveBy=false&
wheelchair=false&
debugItineraryFilter=false&
locale=en ````

### Example return

```json
{
 "requestParameters": {
 "date": "10-13-2021",
 "mode": "BUS,WALK,BICYCLE_RENT",
 "arriveBy": "false",
 "wheelchair": "false",
 "debugItineraryFilter": "false",
 "fromPlace": "48.897678169122194,2.34832763671875",
 "toPlace": "48.8204283539517,2.36480712890625",
 "time": "3:35pm",
 "maxWalkDistance": "5000",
 "locale": "en"
 }
}
```

**Figure 15 : Trip planning analytics request and response sample**



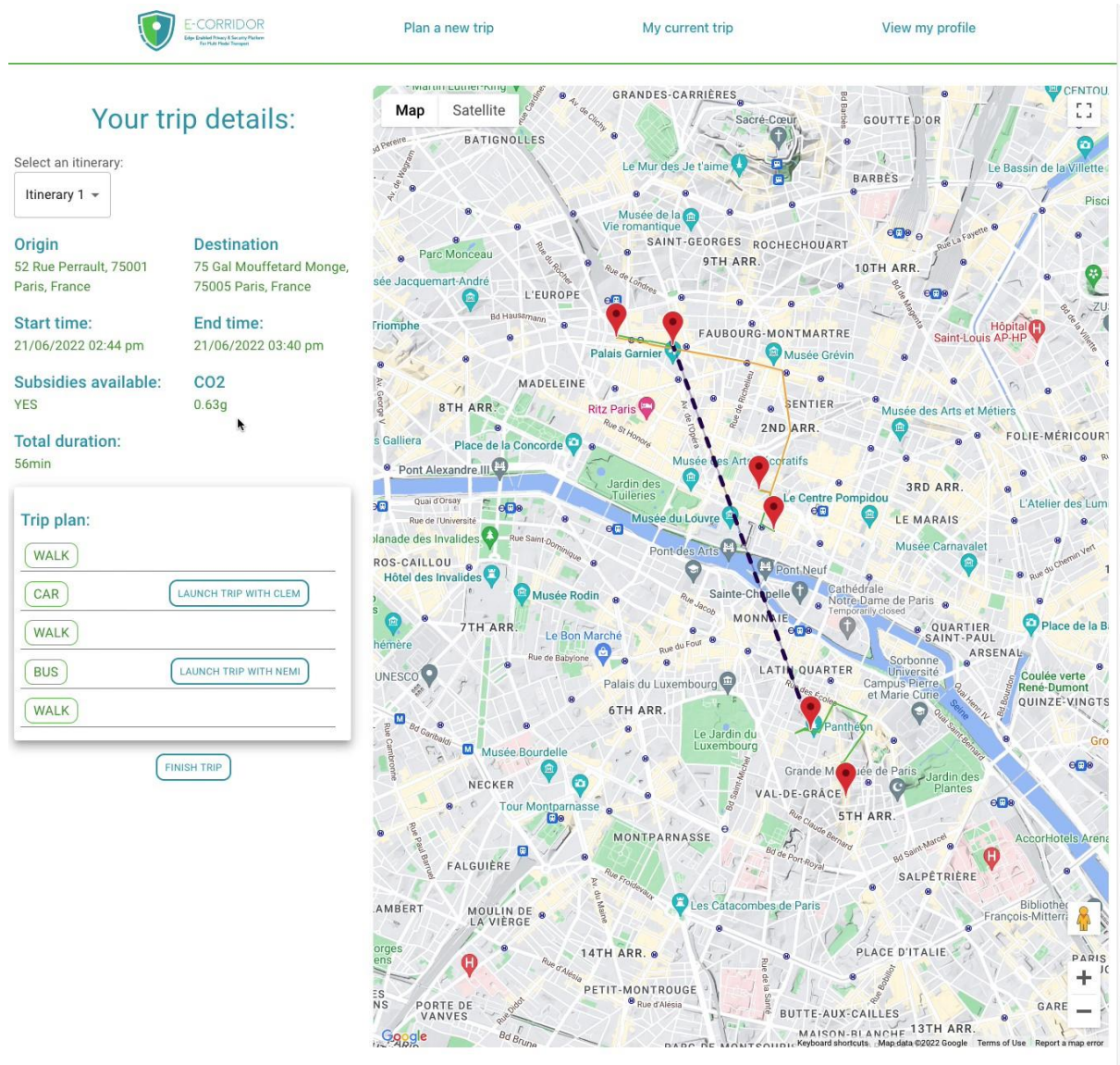
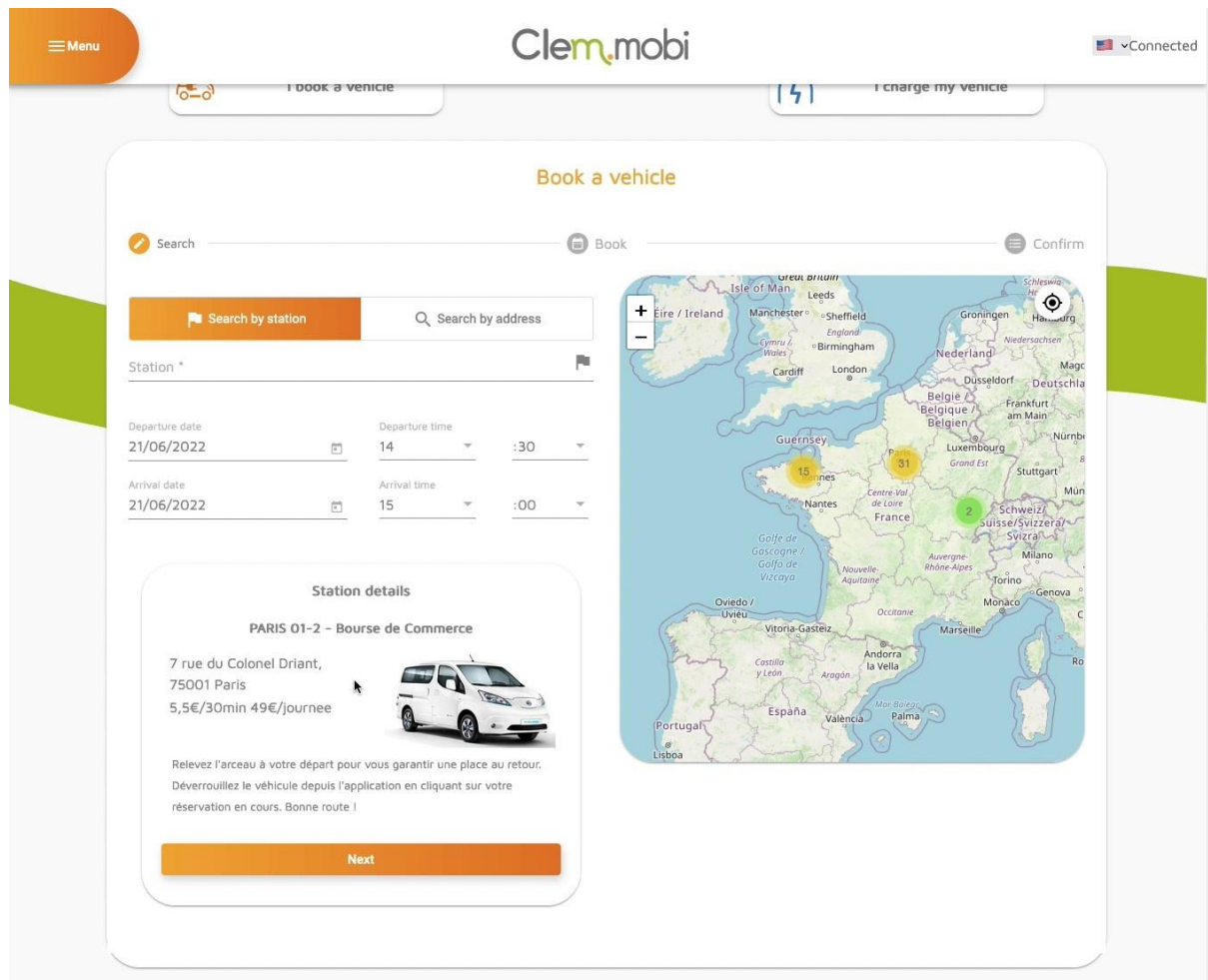


Figure 16 : eWallet trip planning



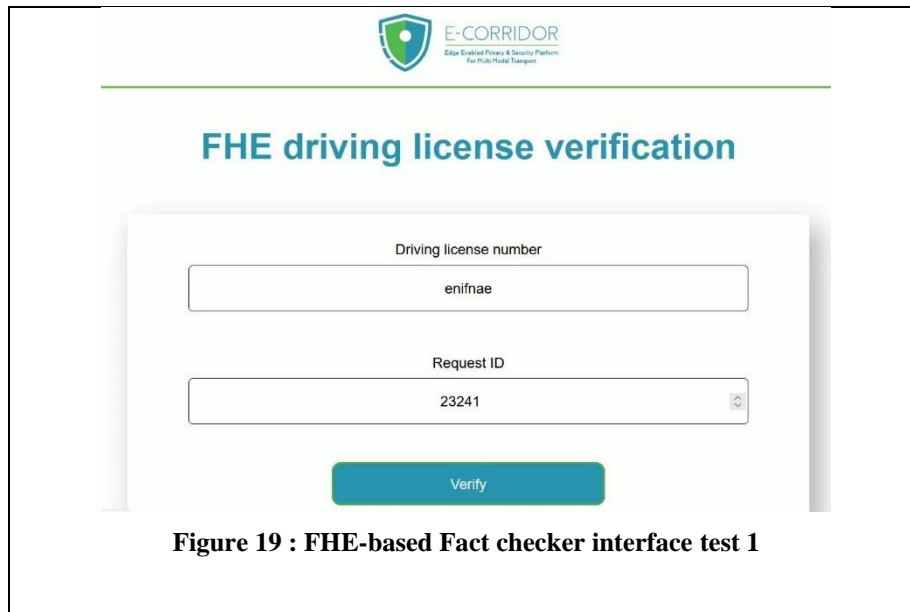
Figure 17 : Authorisation for MSP to access eWallet id



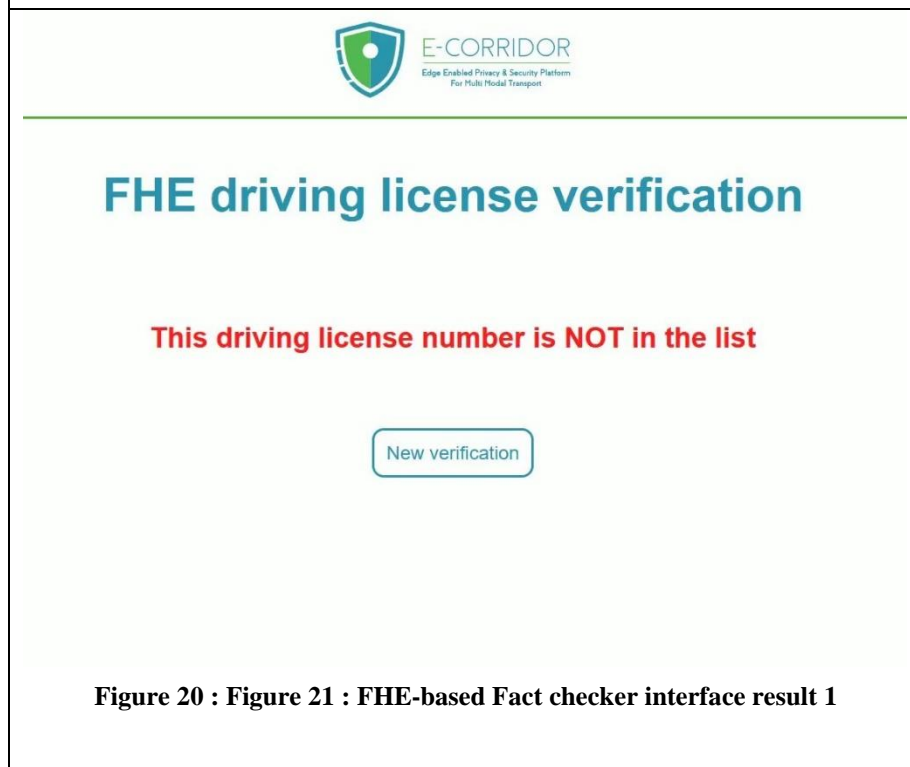
**Figure 18 : Seamless redirection into Clem' website with the station automatically selected**

The “Pilot connector” component which aggregates different input (Server Logs, MQTT Broker logs etc) to share with the central ISI for intrusion detection analytics is completed. An additional function will be added to the Pilot connector to use the ISAC-MMT webservices periodically to run scans.


The Driving licence verification webservice (also based on Flask) and its testing with the FHE based fact checker are completed. Behind the interface, the webservice interacts with 3 endpoints of the FHE-based checker analytics (send value, invoke analysis, decrypt, and retrieve analysis result), the next step is to have the FHE based fact checker accessible through one unique IAI API endpoint and the IAI Orchestrator manages sequence of invoking the 3 API endpoints of the FHE based fact checker.



**Figure 19 : FHE-based Fact checker interface test 1**



**Figure 20 : Figure 21 : FHE-based Fact checker interface result 1**



**FHE driving license verification**

Driving license number  
license-number-03

Request ID  
3424

Verify

**Figure 22 : FHE-based Fact checker interface test 2**



**FHE driving license verification**

This driving license number is in the list

New verification

**Figure 23 : FHE-based Fact checker interface result 2**

The implementation of the Secure routine for driver identification - Driver DNA within the S2C Pilot is still in progress.

Tasks to be finished:

- Integration of the S2C Pilot components with E-CORRIDOR's Common Security Services
- Switch from MongoDB to ISI data storage for the eWallet
- TPM 2.0 deployment in production environment
- Finalize and refine DSAs
- Integration of S2C Pilot with ISAC-MMT webservice and automation of periodic analyses

### **3.3. Workflows**

The workflows stem from the scenarios of the pilot:

The first event is the registration of the MSPs and analytics services into the eWallet authentication server through a server-to-server request over HTTP. Each MSP or analytics service now has a client id and a client secret and a list of fields from the eWallet user (traveller) profile to retrieve.

The travellers register into the eWallet thanks to the sign in page in the eWallet authentication webservice. The travellers express the list of MSPs with whom the personal data shall be shared.

The appropriate Data Sharing Agreement (DSA) is automatically selected according to the traveller's choice and the traveller's personal information is stored in the ISI.

The DSA are predefined and ensure that the data minimization principle is respected, for example, the carsharing operator needs access to the driving licence number but the Demand Responsive Transit (Bus-on-demand) does not. When the Demand Responsive Transit requests a traveller's personal information from the eWallet ISI, the field anonymization DMO (Data Manipulation Operation which is a function of the framework) is applied on the driving licence number field.

The traveller logs into the eWallet web app, credential is verified against those in the eWallet ISI. The traveller requests a trip (Origin-Destination and datetime), the trip request with the eWallet id is sent to the trip planning analytics. The latter fetches mode of transportation preferences from the eWallet ISI, fleet data (Carbon intensity, Shared vehicles availabilities and bus timetables) and performs the analytics. The trips suggestions are then sent to the micro-subsidies analytics to verify eligibility for micro-subsidies, the full result is returned to the eWallet web app to display.

The legs of the chosen trip are displayed in detail with the Carbon emissions and micro-subsidies of each leg of the trip. The user clicks on book, the user is then redirected and seamlessly logged (0 action from the traveller) into the Mobility Service Provider platform with the relevant station or bus stop selected, the travellers make the booking and gets back to the eWallet web app to book for the remaining legs of the trip the same way.

At each of the redirections to the MSP's platform, the OpenID Connect Authorisation code flow is performed. When access to additional information about the traveller is needed by the MSP, the latter can fetch the information if allowed in the eWallet ISI.



The screenshot shows a web interface for configuring a Data Subject Access (DSA) policy. At the top, there is a 'Back' button. The 'Title' field contains 'S2C - eWallet - Traveller's personal data accessible only to CLEM' and the 'Status' is 'CUSTOMISED'. Below this are three expandable sections: 'Purpose\*' (Contractual Obligations), 'Application domain\*' (S2C), and 'Data Classification' (Confidential). The 'Description' and 'Additional Information' sections are collapsed. The 'Validity' section shows a date range from 'June 18, 2021' to 'June 18, 2024'. Under 'Parties', a table lists 'Name' as 'CLEM'. The 'Policies' section contains a table with two rows: one for 'AUTHORIZATION' allowing data creation and another for 'AUTHORIZATION' allowing data reading for the 'CLEM' organization. A 'General Policies' link is at the bottom.

Figure 24 : DSA allowing only Clem' to access data

The screenshot shows a web interface for configuring a Data Subject Access (DSA) policy. At the top, there is a 'Back' button. The 'Title' field contains 'S2C - eWallet - Traveller's personal data accessible only to PLD' and the 'Status' is 'CUSTOMISED'. Below this are three expandable sections: 'Purpose\*' (Contractual Obligations), 'Application domain\*' (S2C), and 'Data Classification' (Confidential). The 'Description' and 'Additional Information' sections are collapsed. The 'Validity' section shows a date range from 'June 18, 2021' to 'June 18, 2024'. Under 'Parties', a table lists 'Name' as 'PLD'. The 'Policies' section contains a table with three rows: one for 'AUTHORIZATION' allowing data creation, one for 'AUTHORIZATION' allowing data reading for the 'PLD' organization, and one for 'OBLIGATION' requiring data anonymization. A 'General Policies' link is at the bottom.

Figure 25: DSA allowing only Pildo labs to access data

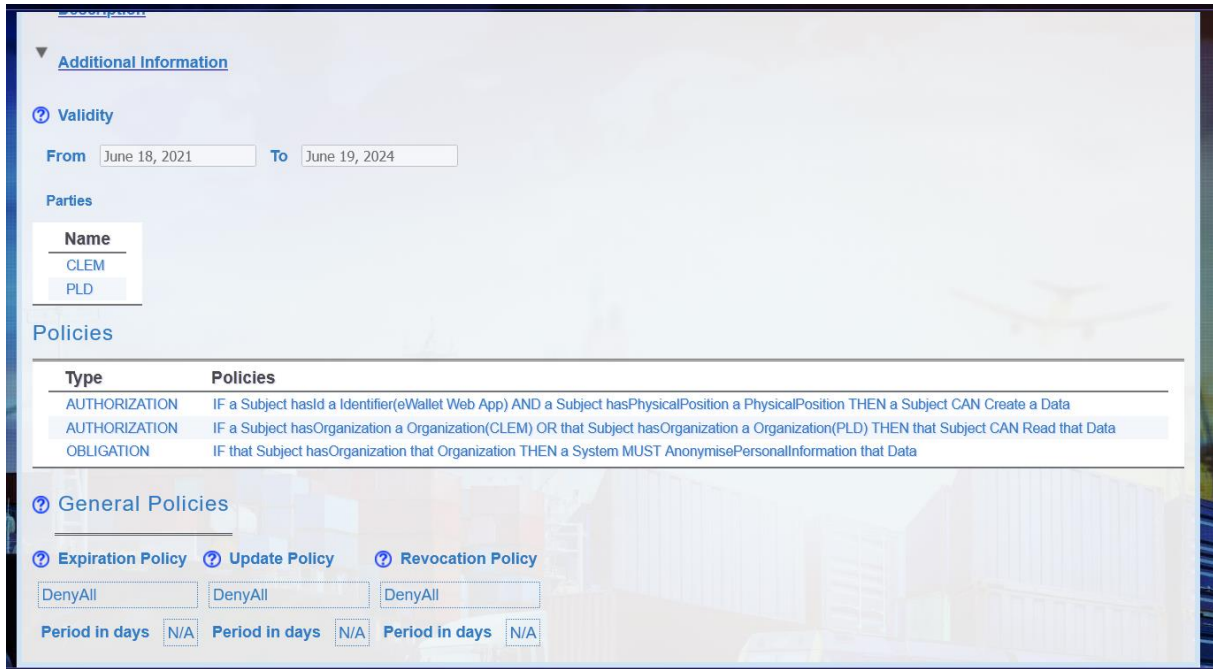


Figure 26 : DSA allowing both Clem' and Pildo labs to access data

With regards to the Intrusion Protection System – Earnest [E-CORRIDOR-IAI-CANIPS] the following DSA is applied for data creation (collected from the CAN BUS) and for conducting analytics on the created data.

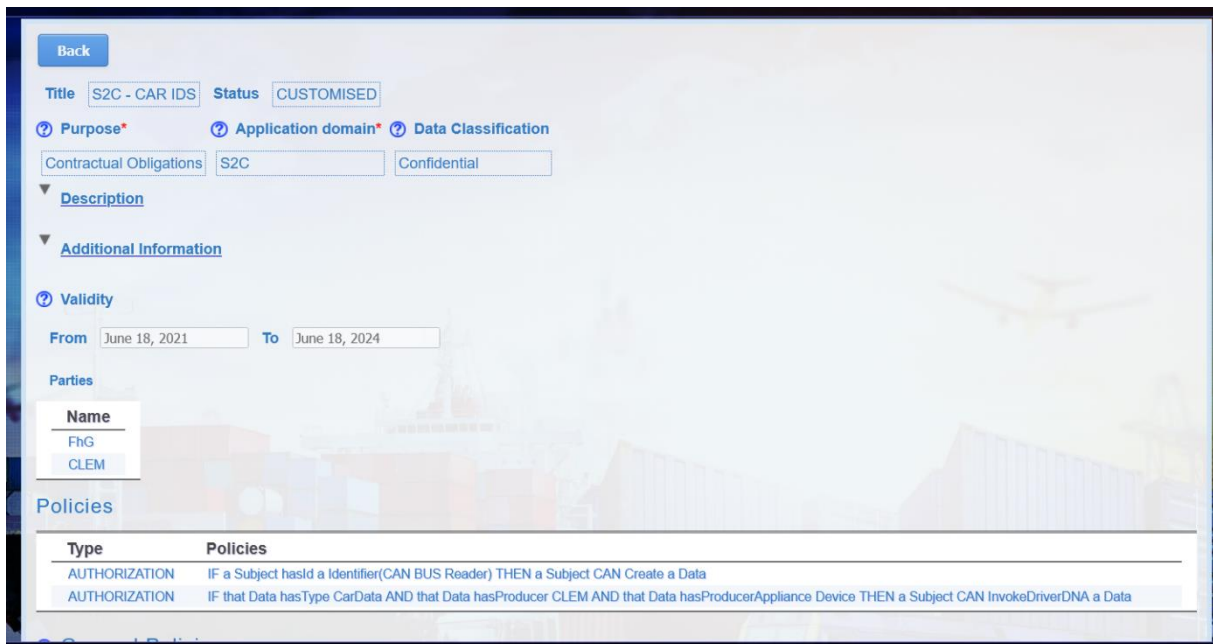


Figure 27 : DSA for data creation and Intrusion detection analytics on the vehicle device

## 4. First Experimental Evaluation

The Experimental Evaluation took the shape of usability testing<sup>1</sup> since it revolves on the traveller and their multimodal journey. The participants of the testing are employees from the consortium. The next experimentation during the 3<sup>rd</sup> year of the programme would be in a real-world environment with real travellers.

### 4.1. Data Sources

- The user profile data used to create eWallet accounts is synthetic data.
- The fleet data from the two MSPs (Clem' and NEMI (Pildo labs)) are real data.
- For the Intrusion detection analytics: Logs from the MQTT Broker of Clem's carsharing service were shared with the partners for the models training.
- The driving licence list for the FHE-based checker analytics is synthetic. (List of random alphanumeric chains of characters)

### 4.2. Acceptance Testing

In the deliverable D3.1 we have defined the requirements for the S2C Pilot, in the same document at the section 1.7. Pilot Evaluation we list the Acceptance Tests in the Table 3 : Summary of the Acceptance Tests.

At M26, we have conducted the test scenarios with the following outcomes:

Test ID: S2C-AT-01	
<b>Description</b>	A registration in one service registers in the other service.
<b>Input</b>	The user's personal information through
<b>Expected Output</b>	One unique identity used for all Mobility Services
<b>Status &amp; Results</b>	[Test Successful]: One unique identity stored in the eWallet and shared to the MSPs, furthermore, the identity is verified.
<b>Final Validation</b>	Managing the identity during its lifecycle (modification, update, erasure, and access revocation)

Test ID: S2C-AT-02	
<b>Description</b>	A successfully registered account by the previous test, when it logs in one service, it is automatically logged into the other service (or at least the log in needs one click).
<b>Input</b>	Traveller logged in the eWallet
<b>Expected Output</b>	Traveller logged in the other MSPs's platforms. (1 or 0 clicks required from the user)
<b>Status &amp; Results</b>	[Test Successful]: A traveller logged in the eWallet webapp is redirected to the MSPs and authenticated automatically using the eWallet identity

<sup>1</sup> <https://www.nngroup.com/articles/usability-testing-101/>

<b>Final Validation</b>	Enable MSP to MSP redirection the same way. This part requires modifications from MSPs
-------------------------	----------------------------------------------------------------------------------------

**Test ID: S2C-AT-03**

<b>Description</b>	The data submitted during subscription for a traveller on one of the participating platforms can be downloaded in the operator's system when the traveller joins the new operator using the eWallet connection option.
<b>Input</b>	A new MSP joins the eWallet AND the MSP is authorized to access a certain traveller's data.
<b>Expected Output</b>	Data retrieved by the MSP from the eWallet ISI
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	Verify all functions work equally for the preexisting MSPs as for the newly joined MSPs

**Test ID: S2C-AT-04**

<b>Description</b>	A change in the personal information in one account triggers a change after a reasonable time in the data stored on the other services's data storage.
<b>Input</b>	Update in the eWallet profile, preconfigured DSA to alert the MSPs
<b>Expected Output</b>	Notification by the ISI to the MSPs
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	Automatic notification at each update

**Test ID: S2C-AT-05**

<b>Description</b>	The modification is notified to other operators, and the history of changes can easily be explored (dates of changes, not necessarily previous content).
<b>Input</b>	Update in the eWallet profile, preconfigured DSA to alert the MSPs
<b>Expected Output</b>	Auditable logs conserved for changes
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	Automatic logs update

**Test ID: S2C-AT-04**

<b>Description</b>	The Mobility Service Provider (MSP) will send the travel request done by the user to the micro-subsidy platform.
<b>Input</b>	Trip request from the traveller on the eWallet web app

<b>Expected Output</b>	Transfer of the request and the eWallet id to the micro subsidies platform
<b>Status &amp; Results</b>	[Test Successful]: Thanks to the eWallet, the trip request is done through the eWallet web app which makes the request by each MSP redundant.
<b>Final Validation</b>	

**Test ID: S2C-AT-07**

<b>Description</b>	The micro-subsidy platform will cross the travel request with the instructions provided by the correspondent public body
<b>Input</b>	Trip request and eWallet profile
<b>Expected Output</b>	Micro-subsidy eligibility and amount calculated
<b>Status &amp; Results</b>	[Preliminary test successful]: The test using only the trip characteristics is successful
<b>Final Validation</b>	Testing using multiple and complex rules including eWallet profile attributes

**Test ID: S2C-AT-08**

<b>Description</b>	Once it is verified by the micro-subsidy platform that the trip requested has a corresponding offer, the platform will send the subsidy offer and the funding amount to the TSP.
<b>Input</b>	Trip request and eWallet profile
<b>Expected Output</b>	Eligibility and amount are suggested and transferred in a secure way through the redirection
<b>Status &amp; Results</b>	[Preliminary test successful]: The eligibility and amount are suggested, the secure discount token is not yet integrated/tested
<b>Final Validation</b>	The discount is safely applied through the redirection and accepted by the MSP

**Test ID: S2C-AT-09**

<b>Description</b>	The TSP will show the micro-subsidy offer to the user for his/her acceptance and once it is accepted, the user will pay for the offer (including the discount), and the micro-subsidy will be transferred to the TSP account.
<b>Input</b>	Trip itinerary chosen; micro-subsidy applied
<b>Expected Output</b>	The traveller benefits from the micro-subsidy
<b>Status &amp; Results</b>	[Not yet performed at M26] ; an improvement thanks to the seamless flow will automatically apply the micro-subsidy (however, an

	adaptation from the MSP is required) This feature is to be implemented in year 3 of the project.
<b>Final Validation</b>	The traveller benefits from the micro-subsidy seamlessly

**Test ID: S2C-AT-10**

<b>Description</b>	The passengers can use trip planning tools provided by E-CORRIDOR to calculate the optimized routes for their trips.
<b>Input</b>	Trip request (Origin-Destination, datetime of departure, user identity)
<b>Expected Output</b>	Multimodal trip suggestions
<b>Status &amp; Results</b>	[Test successful]: Multimodal trips are suggested for the Trip requests over Paris geographical data.
<b>Final Validation</b>	Real world tests with real users

**Test ID: S2C-AT-11**

<b>Description</b>	The trip planning and analytics tools will consider users' interests and preferences, the CO2 footprint of the possible itineraries, price, time and number of connections. Also, the tools designed for trip planning should be able to use anonymized data, to not hinder the user's privacy.
<b>Input</b>	Trip request (Origin-Destination, datetime of departure, user identity)
<b>Expected Output</b>	Multimodal trip suggestions
<b>Status &amp; Results</b>	[Test successful]: Multimodal trips are suggested for the Trip requests over Paris geographical data.
<b>Final Validation</b>	Real world tests with real users

**Test ID: S2C-AT-12**

<b>Description</b>	Trip planning tools should be scalable (using APIs to interact with other services and being adapted to different computing scenarios), and self-adaptive (recomputing the itinerary at runtime, according to possible changes in context or critical situations on the initial itinerary);
<b>Input</b>	Changes during the trip of the request
<b>Expected Output</b>	Updated results according to the latest data
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-13	
<b>Description</b>	The results of the route calculated should be compared with other trip planners in the markets to ensure performance, while the privacy and security aspects of the trip planning tools should be verified based on the security standards set by the project.
<b>Input</b>	Comparative tests with Google Maps, Citymapper and equivalents
<b>Expected Output</b>	Similar results of trips suggestions, Outperformance with regards to personalization and privacy
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-14	
<b>Description</b>	The requested operational data is made available through a secured REST API, which is then provided to the transport authority.
<b>Input</b>	Data from the eWallet web app and from the integrity of the framework
<b>Expected Output</b>	Operational anonymized statistics data from the eWallet accessible
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-15	
<b>Description</b>	The data shared through the REST API is in the format requested by the transport authority.
<b>Input</b>	Data from the eWallet web app about the trip requests, the trips choices and the micro-subsidies applied
<b>Expected Output</b>	Accessible anonymized reports
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-16	
<b>Description</b>	The transport authority is able to retrieve real-time information about the service through the REST API.
<b>Input</b>	Data from the eWallet web app about the trip requests, the trips choices and the micro-subsidies applied
<b>Expected Output</b>	Accessible anonymized reports



<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

**Test ID: S2C-AT-17**

<b>Description</b>	The transport authority is able to access historical data from the service through the REST API.
<b>Input</b>	Data from the eWallet web app about the trip requests, the trips choices and the micro-subsidies applied
<b>Expected Output</b>	Accessible anonymized reports
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

**Test ID: S2C-AT-18**

<b>Description</b>	A user from Clem' tries to sign up for Nemi or vice versa, and is offered the possibility to do it through E-CORRIDOR
<b>Input</b>	User seeking to register at the MSP
<b>Expected Output</b>	Also suggesting also the possibility of registering through the eWallet
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	Redirection to the eWallet from the registration pages of the MSPs

**Test ID: S2C-AT-19**

<b>Description</b>	When choosing this option, the user is informed about the new data privacy policy that applies, which must at least contain complete information about the companies which are granted access to his/her personal data and for which purposes.
<b>Input</b>	User seeking to register at the MSP
<b>Expected Output</b>	Also suggesting the possibility of registering through the eWallet AND presenting the data privacy policy
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	Redirection to the eWallet from the registration pages of the MSPs



Test ID: S2C-AT-20	
<b>Description</b>	The user has access to E-CORRIDOR's data privacy policy not only when completing the sign-in/up process, but also through E-CORRIDOR's partners platforms and the project's website.
<b>Input</b>	Data privacy policy
<b>Expected Output</b>	Shared DSA with the user
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-21	
<b>Description</b>	A DPO, Data Protected Object, containing malware, needs to be detected and blocked at the upload, if it is only detected after sharing, the DPO needs to be identified and the concerned stakeholders need to be informed.
<b>Input</b>	Sharing a DPO with the ISAC-MMT webservices
<b>Expected Output</b>	Malware detected (acceptable level of false positives and false negatives)
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-22	
<b>Description</b>	Attacks need to be detected, the stakeholders are informed of the source, the level of risk, by email and SMS. Countermeasures to be taken by E-CORRIDOR and countermeasures advised to stakeholders are communicated.
<b>Input</b>	Breach of DSA, Intrusion on the level of vehicle or MQTT Broker or webservices
<b>Expected Output</b>	Intrusions and breaches detected, and stakeholders informed. (acceptable level of false positives and false negatives)
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-23	
<b>Description</b>	Spamming email addresses detected.
<b>Input</b>	Spamming the email server
<b>Expected Output</b>	Spams detected (acceptable level of false positives and false negatives)
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-24	
<b>Description</b>	Shared data is encrypted from end-to-end (earliest possible)
<b>Input</b>	Components (docker containers)
<b>Expected Output</b>	TPM 2.0 based TLS connections between the components, TLS handshake refused when firmware is tampered with
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-25	
<b>Description</b>	In case the cloud is accessed by an intruder, the data is not exploitable.
<b>Input</b>	DSA breach
<b>Expected Output</b>	DSA revocation in case of breach
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-26	
<b>Description</b>	The key management respects the DSAs.
<b>Input</b>	
<b>Expected Output</b>	
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-27	
<b>Description</b>	Test if User A is using a fake driving licence (or one driving licence used by multiple accounts) = Driving license number, date, and place of issue, receives an answer (True or False)
<b>Input</b>	Behavioural driving data from the OBD2 and GPS data
<b>Expected Output</b>	Acceptable level of false positives and false negatives
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

Test ID: S2C-AT-28	
<b>Description</b>	Test if User B has a high payment default risk = Validation status, receives an answer (True or False)
<b>Input</b>	Banned driving licence numbers list
<b>Expected Output</b>	Verify if a driving licence number (or eWallet id) is on the list or not
<b>Status &amp; Results</b>	[Test Successful]: Tested with the FHE-based fact checker

<b>Final Validation</b>	Final version testing with IAI
-------------------------	--------------------------------

**Test ID: S2C-AT-29**

<b>Description</b>	Test if IP address by which the user was connected to validate the general conditions of use and email address is blocked by other stakeholders, receives an answer (True or False)
<b>Input</b>	Banned IP addresses and emails list
<b>Expected Output</b>	Verify if an IP addresses and emails is on the list or not
<b>Status &amp; Results</b>	[Test Successful]: Tested with the FHE-based fact checker
<b>Final Validation</b>	Final version testing with IAI

**Test ID: S2C-AT-30**

<b>Description</b>	After training the model with different users on their real accounts, in different conditions (traffic ... etc), one of them uses another person's account, the model should detect and notify.
<b>Input</b>	Behavioural driving data from the OBD2 and GPS data
<b>Expected Output</b>	Acceptable level of false positives and false negatives
<b>Status &amp; Results</b>	[Not yet performed at M26]
<b>Final Validation</b>	

## 5. Requirements Traceability Matrix

Recalling the Use Cases identified in D3.1 and the test cases defined in Section 3.2, we summarized the contribution of each Test case with regard to the Use cases in the next Table.

Use Case ID	Use Case Name	Case Priority *	Test Cases	Status	Comment
S2C-UC-01	Shared mobility eWallet	Must	S2C-AT-01 S2C-AT-02 S2C-AT-03 S2C-AT-04 S2C-AT-05	Advanced	The full user journey (registration-trip planning-booking) is accomplished and functional, the update of the eWallet user profile and the workflow that follows are yet to be finished
S2C-UC-02	Micro-subsidies platform	Must	S2C-AT-06 S2C-AT-07 S2C-AT-08 S2C-AT-09	Advanced	The Micro-subsidies analytics are integrated with the eWallet web app through the Trip planning analytics
S2C-UC-03	Trip planning and carbon footprint analysis	Could	S2C-AT-10 S2C-AT-11 S2C-AT-12 S2C-AT-13	Advanced	The trip planning and carbon footprint analytics are integrated into the eWallet web app. Further personalisation in relation to the eWallet profile is yet to be improved
S2C-UC-04	Sharing data with Transport authority	Must	S2C-AT-14 S2C-AT-15 S2C-AT-16 S2C-AT-17	Not Started	This use case is part of the Evaluation process. Extracting operational data from the eWallet and the trip planner requests will be performed and shared with high attention to data privacy (For the case: Transport authority is external to E-CORRIDOR)
S2C-UC-05	Informing travellers about data usage and privacy	Could	S2C-AT-18 S2C-AT-19 S2C-AT-20	In Progress	Selected DSA is dependent on the Mobility Services selected by the traveller, improvements are being made with regards to transparency and clarity

S2C-UC-06	Cybersecurity: threat/attack management	Should	<b>S2C-AT-21</b> <b>S2C-AT-22</b> <b>S2C-AT-23</b> <b>S2C-AT-24</b> <b>S2C-AT-25</b> <b>S2C-AT-26</b>	In Progress	Data formats of the different inputs for the analytics and Pilot connector communicating the input into the analytics' ISI and the ISAC collector are implemented, examples of data are shared with partners for models training. Full integration is in progress with attention to the analytics to be ran on the edge.
S2C-UC-07	Privacy aware interest-based service sharing	Could	<b>S2C-AT-27</b> <b>S2C-AT-28</b> <b>S2C-AT-29</b>	Advanced	Webservice and UI are accomplished and functional with FHE-based fact checker APIs. Usage of IAI APIs is in progress
S2C-UC-08	Driving behaviour recognition	Could	<b>S2C-AT-30</b>	In Progress	Examples of OBD2 data are shared with partners to help develop and test their analytic. Full integration is in progress with attention to the analytics to be ran on the edge.

\*Priority is defined using the MoSCoW method as in D3.1

## 6. Contribution to pilot and project objectives

Recalling the project objectives, current progress, and next steps regarding the S2C pilot activities are summarized in the next Table.

Objective	Current Progress	Next Steps
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).	Data sharing for several purposes was performed in a flexible, confidential and privacy preserving manner performed with the goal of offering a seamless multimodal user journey involving different data prosumers.	Full implementation of ISI and DSAs for all the steps of the workflows and scenarios. Validation in real world environment
Objective 2: E-CORRIDOR will define edge-enabled data analytics and prediction services in a collaborative, distributed and confidential way.	ISI and IAI edge versions are available for low computation power devices. With DSA enforced locally	Deploying on a device on the car the IAI and ISI, apply intrusion detection and driving behaviour analytics locally.
Objective 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.	Implementation and integration of multiple intrusion detection technologies on different levels, model training by realistic data and integration with ISAC are improving the cybersecurity of E-CORRIDOR communication capabilities	Finalization of TPM 2.0 secured webservices and secure TLS channels secured by TPM 2.0. Full utilization of DSA capabilities in real world environment
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.	Tools developed in the S2C Pilot such as the eWallet, trip planner, carbon footprint analytics in addition to tools developed in other work packages are being implemented, integrated and evaluated. Slight modifications were necessary in MSP's platforms to integrate them with E-CORRIDOR tools	Full evaluation in real world environment is the best way to mature the tools provided by E-CORRIDOR partners.
Objective 5: the framework and the services developed will be used to deliver a pilot product for Centre of information sharing for multimodal transportation (ISAC).	Integration with ISAC-MMT is in progress.	Testing of all ISAC webservices and attack simulations.

## 7. Conclusion

The D3.3 deliverable presented the First Implementation, Test and Validation of the Smart city and Carsharing (S2C) Pilot until Month 26.

The E-CORRIDOR framework components and the Pilot specific components were developed as designed in the previous deliverable D3.2. The full integration using ISI and IAI is in progress. The software currently offers a full user experience from single registration, single sign on, to multimodal trip suggestions with Carbon footprint analytics and micro-subsidies analytics. All with seamless redirections into the Mobility Service Providers platforms.

The integration, the Data Sharing Agreements and the workflows transforming the traveller's experience into steps of highly regulated data sharing between the components have progressed to an advanced level of maturity. A first validation step was performed and shed the light on the necessary work to finalize the Pilot and to prepare it for the real-world environment and users.

Finalization of the full integration of the ISI/IAI with all the components and workflows, the deployment of the TPM 2.0 modules and the deployment on the edge of the concerned analytics will be completed in the following months to have a finished Production-level Pilot and to finally present it to real users. Final evaluation of the pilot will use real user's feedbacks to evaluate usability and performance. From the point of view of Mobility Service Providers, the potential cost of integration of additional Mobility Service Providers will be studied to improve the exploitation of E-CORRIDOR framework.

## A. Appendix

### A.1 Definitions and Abbreviations

Term	Meaning
AF	Analytic Function
AT	Acceptance test
API	Application Programming Interface
ASI	Advanced Security Infrastructure
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system
Authorization	The right or a permission that is granted to a system entity to access a system resource
CTI	Cyber Threat Information
Data prosumer	Data consumer and producer
DMO	Data Manipulation Operation (anonymization, pseudonymization, encryption, obfuscation...)
DPO	Data Protected Object (not to be confused with Data Protection Officer): it is a data object stored in one of the data storage infrastructure within the E-CORRIDOR partners.
DRT	Demand-Responsive Transit (in the pilot, it is the bus-on-demand service called Nemi operated by Pildo labs)
DSA	Data Sharing Agreement
eIDAS	Electronic Identification, Authentication and trust Services
EU	European Union
FHE	Fully Homomorphic Encryption
FMC	Fundamental Modeling Concepts
GDPR	EU General Data Protection Regulation
GPS	Global Positioning System
IAI	Information Analytics Infrastructure
IDS	Intrusion Detection System
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centre
ISI	Information Sharing Infrastructure
JSON	JavaScript Object Notation
M2M	Machine to Machine



MaaS	Mobility as a Service
MoSCoW	Must have, Should have, Could have, and Won't have but would like
MSP or TSP	Transportation Service Provider = Mobility service provider
OBD	On Board Diagnostics
OIDC	OpenID Connect
S2C Pilot	Smart City and Car Sharing Pilot
SSO	Single Sign-On
Traveller	Passenger, mobility service user, driver... While the term user includes travellers and the E-CORRIDOR framework and services users.
TrIP	Trusted Identity Provider
TSM	Trusted Service Manager (D8.1 page 9)
UC	Use Case
US	User Story

## 8. References

---

- <sup>i</sup> [https://transport.ec.europa.eu/transport-themes/mobility-strategy\\_en](https://transport.ec.europa.eu/transport-themes/mobility-strategy_en) A fundamental transport transformation: Commission presents its plan for green, smart and affordable mobility
- <sup>ii</sup> <https://itsdangerous.palletsprojects.com/en/2.1.x/>
- <sup>iii</sup> <https://palletsprojects.com/p/markupsafe/>
- <sup>iv</sup> [https://openid.net/specs/openid-connect-core-1\\_0.html#CodeFlowAuth](https://openid.net/specs/openid-connect-core-1_0.html#CodeFlowAuth) OpenID Connect Core 1.0 incorporating errata set 1

D3.1 Requirements for the S2C Pilot  
D3.2 Design and Architecture for the S2C Pilot  
D5.3 First version of E-CORRIDOR platform and test bed  
D5.4 Final Reference Architecture  
D6.2 Sharing and Analytics Infrastructures first maturation  
D7.2 Data Analytics techniques first maturation  
D4.3 First implementation, test and validations of the ISAC Pilot