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

D3.1

Requirements for the Smart city and Car Sharing Pilot (S2C)

WP3 – Smart city and Car Sharing Pilot (S2C)

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

30/11/2020
Version 1.0

Responsible partner: CLEM'
Editor: Mohammed Ammara
E-mail address: mohammed.ammara@clem-e.com

E-CORRIDOR is 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: M. Ammara (CLEM'), A. Lancelot (CLEM'), B. Flinois (CLEM'), S. Soufflet (CLEM'), S. Paniagua (PLD), E. Consegal (AMTU), M. Jofre (FC), V. Moyano (FC), R. Han (WIT)

Approved by: R. Han (WIT), M.Manea (HPE)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	27-Jul-2020	M. Manea	HPE	Initial ToC
0.2	09-Oct-2020	M. Ammara	CLEM'	1st draft
0.8	19-Nov-2020	M. Manea	HPE	Review
0.8	21-Nov-2020	R. Han	WIT	Review
1.0	27-Nov-2020	B. Flinois	CLEM'	Improved after reviews
1.0	27-Nov-2020	S. Soufflet	CLEM'	Improved after reviews
1.0	30-Nov-2020	M. Ammara	CLEM'	Improved after reviews

Executive Summary

The Car Sharing Pilot (S2C) of the E-CORRIDOR project's purpose is validating the E-CORRIDOR framework applications in multimodal transport in a smart city context where the traveller is involved with many different mobility operators at once.
The platform's secure data sharing and analytics capabilities will be leveraged to improve multimodality with a focus on simplicity, effectiveness and cybersecurity.

This document describes the main stakeholders involved in the pilot and their different interactions in the scenario showcasing E-CORRIDOR's capabilities. The document also describes in details the user stories and use cases expressing the requirements of the Pilot.

Executive Summary 3
1. High Level Requirements 5
1.1. Scenario 5
1.2. Stakeholders 6
1.3. Comparison to current practice 7
1.4. Definitions and Abbreviations 8
1.5. User Stories 8
1.5.1. S2C-US-01: eWallet 8
1.5.2. S2C-US-02 Socio-geographic dependant micro-subsidies 10
1.5.3. S2C-US-05 Trip planning and Carbon footprint. 12
1.5.4. S2C-US-04 Transport authority: access to Bus-on-demand data. 14
1.5.5. S2C-US-05 Informing the traveller about his/her data and how it is used. 15
1.5.6. S2C-US-06 Cybersecurity notifications: communicate about threats 16
1.5.7. S2C-US-07 Secure sensitive data that would be shared from end to end 17
1.5.8. S2C-US-08 Privacy aware interest-based service sharing 18
1.5.9. S2C-US-09 : Driving behaviour recognition 19
1.6. Relevance to E-CORRIDOR objectives 20
1.7. Pilot Evaluation 21
2. Use Cases 24
2.1. Use Case Diagram 24
2.2. Use Case Descriptions 25
2.2.1. S2C-UC-01: eWallet: Sign in/Log in 25
2.2.2. S2C-UC-02: Socio-geographic dependant micro-subsidies 26
2.2.3. S2C-UC-03: Trip planning and carbon footprint analysis 27
2.2.4. S2C-UC-04: Sharing service data with Transport authority 29
2.2.5. S2C-UC-05: Informing travellers about data usage and privacy. 30
2.2.6. S2C-UC-06: Security analytics: Notifications and threat/attack management 31
2.2.7. S2C-UC-07: Security analytics: Privacy aware interest-based service sharing 32
2.2.8. S2C-UC-08: Driving behaviour recognition 33
2.3. Catalogue of Use Cases 35
2.4. Storyboard 35
2.4.1. S2C-SB-01: storyboard for User Story S2C-US-01 eWallet 35
2.4.2. S2C-SB-02: storyboard for User Story SC-US-03 Trip planning and carbon footprint analysis 36
2.4.3. S2C-SB-03: storyboard for User Story S2C-US-06 Cybersecurity: notifications 37
3. Non-functional Requirements 38
3.1. Security 38
3.2. Performance 38
3.3. Usability 38
3.4. Operational 38
4. Conclusions 39

1. High Level Requirements

1.1. Scenario

With the advent of smartphone applications and IoT technologies, mobility in urban areas has experienced a significant leap in the past few years than it has in decades. There has never been as many choices for getting around the city, whether on a shared car, on bus or bike, and as much information about public transport services available in real time as right now. With all, it is becoming easier for users to find the most convenient mobility solution for every trip. However, a solution usually involves burdensome interchanges and authentications from one mobility service to another, which plays a negative role to the development of multimodal transportation.

Multimodality allows us to tailor the most convenient mobility solution by combining different modes of transportation and getting the best of each one. Each mode has its specific characteristics, which are more adapted to a particular situation (demand, geography, Origins-Destinations, other available modes, etc.).

However, there still are barriers to an efficient multimodality:

- From the traveller's point of view, it is painful to register in each of the mobility services, and their need is to plan ahead and search for the availabilities/arrival time of each mode with an acceptable customer experience. Also, today during the trip one needs to carry many tickets or proof of payment. All these factors and lake of trust on security of each of these services, make multimodal trips using mobility services less attractive compared to the use of a personal vehicle.
- From the operator's and the public authorities' point of view, it is difficult to adjust the routing and the scheduling of trips and also the maintenance in order to adjust the capacity to the demand. Moreover, it is complicated to guarantee and enforce the privacy and the safety of the data shared when trying to coordinate different mobility services. Furthermore, without an effective data sharing and analytics infrastructure, there is no effective way to have a shared open data that guarantees privacy but also the ability to conduct big data analytics and real-time optimization.

Indeed, E-CORRIDOR can remove these barriers and make multimodal trips as seamless and secure as single-mode trips.

Three concepts will be tested within this pilot:

- Offering access to different mobility services with one single registration/authentication process via an eWallet that will use E-CORRIDOR's secure data sharing and data analytics capabilities. The eWallet will allow for a much simpler one-step authentication using the shared user data (more details in the user stories below).
- Implementing a micro-subsidies system in multimodal trips based on socio-geographical information, through which travellers benefit from reduced prices when combining sustainable modes of transport. An analytics service will collect shared information through the E-CORRIDOR framework, calculate the micro-subsidies for

multi-modal trips and communicate to the concerned parties the result (mobility service provider or public authorities).

- Participating in a collaborative approach between multiple data prosumers for Cyber Threat Management.

The mobility services to which the project's e-Wallet will give access are a DRT service offered by Pildo Labs, and a carsharing service operated by Clem'. To allow multimodal trips combining both services, Clem' will deploy one vehicle in a town where Pildo's DRT service, called Nemi, is currently operating.

(The location of the carsharing station, the administrative documents for the parking space, the vehicule choice have been chosen but need to be confirmed)

DRT: Bus lines that are optimized according to the demand (expressed through the app Nemi) in real time in time and space (Dynamic schedules and bus stops).

The eWallet: a Digital Pocket containing traveller profile data shared between different services in a secure and privacy preserving manner, allowing for seamless multimodality starting by the seamless authentication.

Nemi: is a tool which enables the operation of demand-responsive public transport services. It makes mobility in low-density areas feasible by providing a software solution that enables flexible bus routes. Consisting on a system back-end —which hosts the routing algorithm—, a mobile user app, a driver app, and a web back-office, it allows citizens to book seats on vehicles which are operating different demand-responsive lines by indicating origin, destination and time of their desired trip. The available options are shaped by the virtual stops and schedule previously defined by the competent public authority.[1]

1.2. Stakeholders

Mobility is a complex subject involving so many stakeholders, pursuing multimodality adds another layer of complexity, the E-CORRIDOR framework is at the centre of all the different interactions involving data sharing between these stakeholders, we will list the principal ones:

- Travellers: The main stakeholder of this pilot. To address their need to go from point A to point B 2 options : using multimodal transport or the single-mode one. However, for multimodal transport, they need to sign/log into each service, plan ahead (seeking different information from different sources about trips and fees), synthetize and decide on a trip considering multiple criteria. The current initiatives towards multimodality involving data sharing triggers concerns about data security and privacy for the travellers. These factors are barriers to the multimodal trips that are more sustainable compared to the personal vehicle.

[1] http://www.nemi.mobi/
https://www.linkedin.com/company/ne-mi/

- Mobility service provider (carsharing and bus-on-demand): (Also called Transportation service providers TSP), each one has the mission to provide a sustainable mobility solution. Multimodality is one of the powerful levers in improving the sustainability of mobility, multimodality is using for each part of the trip, the most adapted mode of transportation (both economically and environmentally). However, enabling multimodality requires a collaboration between the Mobility service providers, and with the other stakeholders.
- Data Protection Authorities[2]: E-CORRIDOR framework has the ambition of being pan-european and highly scalable, hence why this pilot needs to be compliant with the GDPR.
- Public transport authorities: With the goal of achieving a more sustainable and inclusive transportation system for the needs of the citizens, they coordinate the different efforts according to public policies aiming for the previously mentioned goals. They plan and tender for transportation projects. They also fund, subsidize, and control the quality of service of the mobility service providers. They contribute to the enforcement of legislations.
- Mobility consultancies: they provide advice to the public authorities and the mobility service providers, as well as innovative solutions for better answering the mobility demand, for instance: the socio-geographic dependent micro subsidies.

1.3. Comparison to current practice

Building on E-CORRIDOR framework functionalities, the pilot will demonstrate an innovative multimodal and seamless trip solution, offering a single registration and enabling an innovative method for micro subsidizing specific segments of the trip. It will offer a different perspective compared to current multimodal mobility schemes, with some aspects to highlight:

1. **Data sharing**: the current mobility services perform in a separate way without sharing data that is relevant for having the most suitable and adapted trip. Although the large list of benefits for users that sharing data among service operators can provide, aspects like privacy concerns and data security arise as the main reasons to not share the data. Access to data is essential to run a good mobility service and to implement the needed corrections to it on the go with the main objective to have a continuous improvement strategy regarding the offered trips. The framework proposed by E-CORRIDOR solves these data privacy issues by ensuring secure data sharing among mobility providers.
2. **Personalized mobility**: based on the shared data among the different mobility services and users' experience, a more personalized mobility can be offered to the citizens. Adapting trip suggestions to traveller's particular needs, recognizing the driving behavior, adaptative micro-subsidies… Nowadays, we are suffering the constraints of non-personalized mobility, causing some of the problems that cities are facing, such as traffic jam or congestion in public transport at rush hours and a strong preference to the personal vehicle. For sure, obtaining personalized mobility implies working on reliable data and data shared by different mobility providers and running analytics without compromising the privacy and the cybersecurity.

[2] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

3. **One registration, seamless authentication**: as there are no data shared nor a multimodal platform including the different mobility offers, today there is no single registration for the different services composing a multimodal trip. When using different modes of transport, this aspect becomes very inconvenient for users as they need different tickets and bookings, and they have to be logged in several platforms.
4. **Micro subsidies and dynamic incentives**: these are the most innovative aspects compared to the current mobility offer. The public subsidies for mobility are currently done in a flat rate by ticket or temporary pass, independently of the real mobility situation in a city in a concrete moment of the day, either supply side subsidies or demand side subsidies. Having micro subsidies in a dynamic way, taking into account the travellers' geo-position, the traveller's personal information, the trip's information and ensuring the privacy of the data shared by third parties will allow having a better impact on travellers' behavior (mobility decisions) to ease the general mobility situation.

1.4. Definitions and Abbreviations

Table 1 : Definitions and Abbreviations

Term	Meaning
NFR	Non Functional Requirement
S2C	Smart city and Car Sharing Pilot
MoSCoW	Must have, Should have, Could have, and Won't have but would like
DRT	Demand-Responsive Transit
DSA	Data Sharing Agreement
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.
DMO	Data Manipulation Operation (anonymisation, pseudonymisation, encryption, obfuscation…)
MaaS	Mobility as a Service
GDPR	General Data Protection Regulation
TSP	Transportation Service Provider = Mobility service provider
ISAC	Information Sharing and Analysis Centre
FHE	Fully Homomorphic Encryption
Data prosumer	Data consumer and producer
Traveller	Passenger, mobility service user, driver… While the term user includes travellers and the E-CORRIDOR framework and services users.

1.5. User Stories

1.5.1. S2C-US-01: eWallet

As a

S2C pilot traveller

I want to

be able to use multiple services and combine services with only one created account

So that

I can use all E-CORRIDOR-enabled mobility services seamlessly without needing multiple accounts.

1.5.1.1. Class: Data sharing

1.5.1.2. Discussion

Main stakeholders: All data prosumers and all who store travellers' data: (mobility service providers, transport authority, third party analytics, security analytics…).
Referenced stakeholders: -

The main actor of this user story is the **Traveller**. To use any service, they usually needs to register ("sign in") to each mobility service, in this situation we have to do as many registrations as the number of mobility services we intend to use.

To enhance multimodality, in this pilot the traveller will only need to create a new account once, in one given mobility provider's platform (participating in the E-CORRIDOR-enabled eWallet). Once this account created, the relevant information collected during the sign-in process will be made accessible to all other mobility providers in the ecosystem if they need to access it for user-related purposes. If the user (traveller) is interested in using one of the other services, he/she will find him/herself able to access all mobility services with his/her previously created account, without any need to create individual accounts on said platforms.

The digital wallet (eWallet) is the name of this feature, it will enable end users (travellers) to access services from multiple transport service providers irrespective of region or geography from a single unique digital identity. This wallet will be adapted specifically for the purpose of mobility and will therefore contain necessary and validated information such as driver's licence, proof that the driving licence has been validated by a mobility provider, proof of address, mobility profil etc. as required by various transport providers and national regulations for each traveller.

Some of the information will need to be accessible at any time to the operators, while other pieces of information can be provided only for the validation phase and later be made accessible only upon request.

For instance, for Clem' the information that needs to be accessible in all cases will be the following:

- Email
- First name
- Last name
- Address
- Mobile phone number
- Driving licence number
- Validation status (Driving licence, Payment history status)
- Validation date (Can be Null between subscription/validation and Validation status)
- An ID linking this profile to the other mobility partners

An issue that comes to mind is that different mobility services may require different information. For example, Clem needs to check a traveller's driving licence before allowing the traveller or driver to book a vehicle, whereas a DRT service will not need the driver's license in any way.

This is the information that Nemi needs to access in different stages of the service provision:

- National ID number
- An ID linking this profile to the other mobility partners
- Email
- First name
- Last name

This means that when a traveller completes a sign-in process, the data provided upon subscription needs to be made accessible to other operators, who may need it to sign him/her in other mobility services. If one's data is not complete enough to give the traveller access to the whole extent of some mobility service, the traveller may be asked to complete his/her user data on that mobility service platform. This update is then shared with other mobility services.

The shared data about the traveller may include whether this traveller has been suspended by an operator or has unpaid trips or any problem with his/her account (Invalid driving license, fake identity, etc.

When a traveller needs to modify his personal data, he/she needs to be able to access it on any one of his/her accounts and modify it without repeating the modification on each account. The concerned parties will need to be informed by a log that there was a change in the data (without necessarily storing the pre-existing data). When a traveller wants to quit the service and expresses the need to have all his data erased, the data stored on the different mobility partners's data storage need to be treated accordingly.

Acceptance Tests:

- (with the consent of the traveller and intention for registering into Clem' and Nemi) A registration in one service registers in the other service.
- 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).
- 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.
- 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.
- The modification is notified to other operators, and the history of changes can easily be explored (dates of changes, not necessarily previous content)

1.5.2. S2C-US-02 Socio-geographic dependant micro-subsidies

As a

Public Authority / Employer / Mobility consultancy

I want to

be able to analyse data of each trip and the traveller's profile.

So that

I can identify the eligibility for a micro-subsidy and calculate its amount.

1.5.2.1. Class: Data analytics

1.5.2.2. Discussion

Main stakeholders: Subsidiser or subsidy controller (Public Authority / Employer / Retailer), traveller, Transportation Service Provider (TSP)
Referenced stakeholders: -

Our plan is to develop a micro-subsidy calculation engine, comprising a database with geographic information on eligible areas and a set of rules set by the platform to ensure micro-subsidies fill gaps in public transport and support wider policy objectives. It will be designed along open access standards to be available to MaaS or proprietary TSP platforms. It will allow subsidizers to micro-subsidise[3] certain first/last-mile journeys using commercial TSPs.

How it works: Currently, there is a myriad of subsidies being applied to urban transport. Supply-side subsidies are channelled to transport operators, while demand-side subsidies are directly channelled to beneficiaries. These subsidies, as they are set to target certain modes of transport or certain groups of population at large, are not granular enough to fully discriminate on the basis of need or of the policy goals being pursued. This is where our platform comes in: it allows to marginally target every person and every circumstance, learn about mobility patterns and set subsidies, different in each case and in each moment in time if needed, in order to maximize societal goals[4]. It takes a small investment in transit subsidies that are surgically targeted at specific gaps and turns that into additional ridership, and reduced vehicle km travelled.

For example, rather than subsidizing a bus to run every 30 minutes on a route with only five or six customers, a better option would subsidize a local taxi or ride-hail to take health-care worker Jaume to the train station 4 km away so he can get to the hospital where he works. Or, instead of funding a late-night bus, with unsustainably few riders, subsidize taxi use after a certain hour and within a specified zone to bring Celina home after her late shift as a security guard.

The increased transit ridership pays back the investment, and reduced vehicle km travelled contributes to the global effort to mitigate negative externalities caused by the private automobile (accidents, congestion, air pollution).

[3] micro-subsidy ("subsidy") — a very small (usually single-digit) subsidy targeted for a particular time, and place and purpose. Examples are 2€ for a 4€ bikeshare to the train station or 9€ for a pensioner to take a 17€ taxi to the hospital.

[4] This has some resemblance with what the aviation industry has managed to do very successfully over the last 20 years: by setting different prices; they have managed to increase the load factor of aircrafts and increase profits. In our case, by setting differentiated subsidies to the maximum level possible (i.e. personal subsidies), we want to maximize societal goals, including an increase in the average occupancy rate of Public Transport.

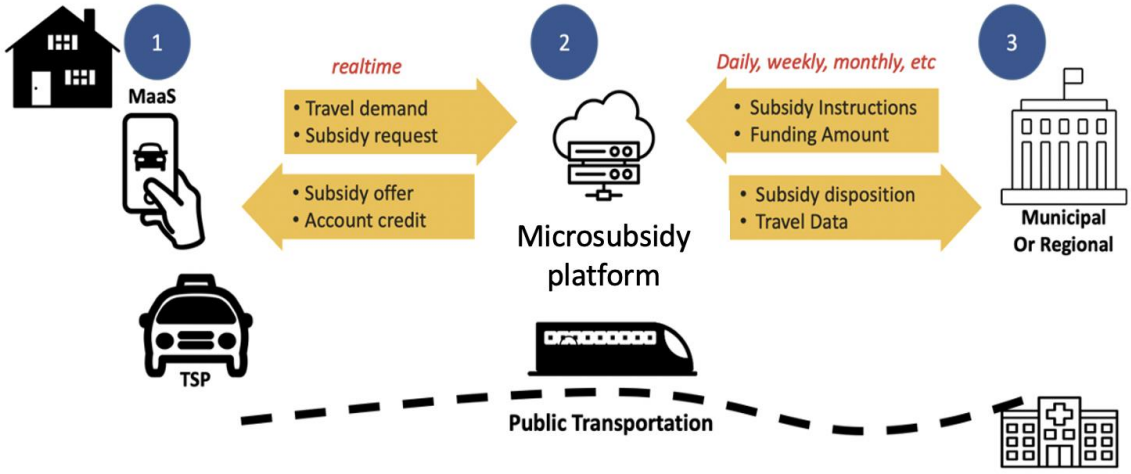


Figure 1 : Microsubsidy workflow

With this platform, cities will be able to generate public transport service improvements and cost savings while creating an open marketplace for mobility services and a control framework for managing future, new mobility fleets.

The E-CORRIDOR framework will enable to share data in a secure way among the micro-subsidies platform and the different entities involved (mobility providers, MaaS platforms). In order to assign a micro subsidy to a certain trip, the platform will require individual trip data such as origin, destination, time of trip, calculated trip cost before subsidies, or even traveller profile data (e.g. micro subsidies based on age).

1.5.2.3. Acceptance Tests

In order to develop a good performance of the micro-subsidy platform, a list of acceptance test will be implemented by E-CORRIDOR:

1. The Transport Service Provider (TSP) will send the travel request done by the traveller to the micro-subsidy platform.
2. The micro-subsidy platform will cross the travel request with the instructions provided by the correspondent public body
3. 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.
4. The TSP will show the micro-subsidy offer to the traveller for his/her acceptance and once it is accepted, the traveller will pay for the trip (taking into account the discount), and the micro-subsidy will be transferred to the TSP account.

1.5.3. S2C-US-05 Trip planning and Carbon footprint.

As a

S2C Travellers

I want to

be able to see multimodal trips and information about arrival time, total cost, carbon footprint, get suggestions/ranking according to my criteria.

So that

I identify the trip that suits my needs.

1.5.3.1. Class: Data analytics

1.5.3.2. Discussion

Main stakeholders:

- S2C travellers

Referenced stakeholders:

- S2C mobility service providers (mainly carsharing and bus-on-demand, other transport agencies can also be included)
- Transport authorities.

Travellers usually need to use multiple modes of transportation for their journey and using trip planners for optimized travel experience. The figure below shows an example of multi-modal transportation for the trip of a traveller. To be specific, the traveller planning to go to take a flight may use transport tools such as public buses, shared cars, trains, and aeroplanes, and each leg of the trip will have different requirements such as the arrival time at bus stops or airports. A traveller may first use the trip planning tools provided by E-CORRIDOR to get a route suggestion (such as using car-sharing or on-demand bus service). Trip planning and carbon footprint analytics are data analytics tools developed and provided by WP7 of E-CORRIDOR and integrated into the E-CORRIDOR platform. After the traveller has made his/her choice, relevant service requests will be sent to appropriate service providers for seamless transportation service and experience. Transport agencies and operators should push the latest traffic information to the APIs of trip planning tools to keep travellers informed about the traffic state. Travellers may also have additional requirements such as arrival time, total cost, carbon footprint, and getting suggestions/ranking according to their criteria. Thus, trip planning and analytics tools should consider users' requirements and the available services in E-CORRIDOR. The available service refers to other data analytics services such as socio-geographic dependant micro-subsidies (since it may affect the estimation of fees) and data sharing services (since it may affect how to process and use the trip information generated by our tools)

Trip planning tools should be provided to infer or predict the best multi-modal travel itineraries for end-users. The analytics will consider travellers' interests and preferences, the CO_2 footprint of the possible itineraries, price, time and number of connections. The analytics should be able to use anonymized data to protect travellers' privacy. This means the trip planning and carbon footprint analytic tools don't need to use sensitive (personal) information in their services, and there is no need for travellers to worry about the disclosure of personal and trip information. Besides, they need to be self-adaptive, recomputing the itinerary at runtime, according to possible context change or critical situations on the initial itinerary. Moreover, the trip planning platform should be scalable to include other transport services from other transport operators, interact with other internal functional modules (such as the service for calculating socio-geographic dependant micro-subsidies), and deal with different computing scenarios.

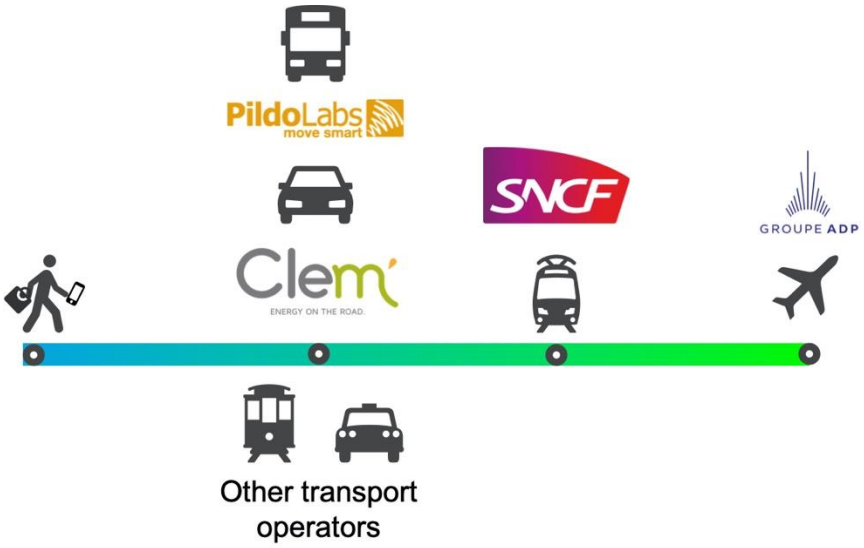


Figure 2. Multi-modal transportation in the trip planning.

1.5.3.3. Acceptance Tests

- The travellers can use trip planning tools provided by E-CORRIDOR to calculate the optimized routes for their trips.
- The trip planning and analytics tools will consider travellers' interests and preferences, the CO_2 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 traveller's privacy.
- 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 context change or critical situations on the initial itinerary);
- The results of the route calculated should be compared with other trip planners in the markets to ensure the performance, while the privacy and security aspects of the trip planning tools should be verified based on the security standards set by the project.

1.5.4. S2C-US-04 Transport authority: access to Bus-on-demand data.

As a

Transport authority

I want to

to have permanent access to information of the DRT service.

So that

I can oversee the quality of service and the KPIs.

1.5.4.1. Class: Data sharing

1.5.4.2. Discussion

Main stakeholders:

- Transport authority

Referenced stakeholders:

- DRT service provider
- Transport operator

The main actor of the user story is the transport authority. In order to oversee the performance of the DRT service, it needs to be able to access the following data from on-going services in real time, through a secured REST API:

- Bus geopositioning
- Bus speed
- Time of arrival of the bus at every stop

It also requires to have access to historical data of:

- Reservations (accepted and rejected)
- Kilometres travelled per expedition
- Aggregated data for kilometres travelled, segments used by the optimization algorithm to build the itinerary, speed, punctuality, occupation levels, and origin-destination matrices.
- Total number of expeditions per line, monthly and annually.
- Number of contingency expeditions per line (due to a malfunction of the software), monthly and annually.
- Kilometres travelled per line, monthly and annually.
- List of the segments used by the optimization algorithm to build the itinerary, per line, monthly and annually.
- Hours of operation per line, monthly and annually.
- Information about the service: stops, possible routes and schedule for the expeditions.

1.5.4.3. Acceptance Tests

- The requested operational data is made available through a secured API REST, which is then provided to the transport authority.
- The data shared through the REST API is in the format requested by the transport authority.
- The transport authority is able to retrieve real-time information about the service through the REST API.
- The transport authority is able to access historical data from the service through the REST API.

1.5.5. S2C-US-05 Informing the traveller about his/her data and how it is used.

As a

Traveller

I want to

be able to know which companies have access to my data, to which specific data and for which purposes.

So That

I can be sure that I approve the way my data is used and that I can keep control of it

1.5.5.1. Class: Data sharing

1.5.5.2. Discussion

Main stakeholders: S2C pilot traveller
Referenced stakeholders: mobility service providers, transport operators, E-CORRIDOR partners, GDPR regulators

S2C pilot travellers will not go through the hassle of having to sign up for each of the services they use in their multimodal trips. However, for this to be possible, their data must be handled in a different way than previously agreed. This will not be the case for new users (travellers) who decide to benefit from E-CORRIDOR-enabled mobility services from the beginning, but it will be for Clem's or Nemi's existing service users (travellers). Such users will be offered the possibility to sign in through E-CORRIDOR when they try to use the other service for the first time. It is essential that they are then informed about the changes in the data privacy policy that this action will trigger, in other terms, the DSA content explained simply (What data and shared with whom…) to the travellers to ensure consent.

When a traveller decides to sign in through E-CORRIDOR, his/her personal data is shared with all E-CORRIDOR partners. Before completing this action, the traveller must be clearly informed of which companies will have access to his/her personal data and for which uses, as well as his/her rights regarding the access, modification, and deletion of such data.

The data privacy policy applied by E-CORRIDOR can not only be shared with the traveller during the sign-in process, but it can also be published on a website referenced on the different mobility providers' platforms.

1.5.5.3. Acceptance Tests

- A user from Clem' tries to sign up for Nemi or vice versa, and is offered the possibility to do it through E-CORRIDOR
- 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.
- 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.

1.5.6. S2C-US-06 Cybersecurity notifications: communicate about threats

As a

Data prosumer

I want to

Be able to isolate inputs that could represent a security threat and alert other partners if I detect one.

So that

The other partners and the ISAC pilot can take action.

1.5.6.1. Class: Data sharing and data analytics

1.5.6.2. Discussion

Main stakeholders: Mobility service providers, Cybersecurity threats,
Referenced stakeholders: Advanced security services (WP8), Data analytics techniques (WP7), Travellers, ISAC (WP4).

This user story is in synergy with the WP4 tasks, it is a collaborative approach exploiting the E-CORRIDOR framework capabilities for a better Cyber Threat Management.

When a data input is received or a dangerous connection is attempted from an external source, there is a potential for a cybersecurity threat. As a mobility service provider that is connected to a data sharing infrastructure, i.e., E-CORRIDOR, I might be impacted by this threat. Other stakeholders might be as well. A need for secure data analysis exists to make sure that such threats are detected, identified and that the data is isolated so that other stakeholders do not suffer from this threat.

The advanced security services (WP8) and the intrusion detection analysis (WP7), as well as the ISAC (WP4) can provide alerts (by email and SMS), the content of this alert will help to assess the risk and to take the correct countermeasures. Moreover, the alert needs to respect the DSAs (the DSA needs to list the parties to be notified.)

For connections, the IP address is needed for including it in the IP Blacklist. For the DPOs, the concerned stakeholders (especially the ones storing it or a copy of it in the Edge) need to be able to identify the malicious DPOs.

1.5.6.3. Acceptance Tests

- A DPO, Data Protected Object, containing a malware, it needs to be detected and blocked at the upload, if not, if it is detected after sharing, the DPO needs to be identified and the concerned stakeholders need to be informed.
- Attacks need to be detected, the stakeholders are informed with the source, the level of risk, by email and SMS. Countermeasures to be taken by E-CORRIDOR and countermeasures advised to stakeholders are instructed.
- Spamming email addresses.

1.5.7. S2C-US-07 Secure sensitive data that would be shared from end to end

As a

Data prosumer

I want to

Have the sensitive data or data that is always shared (ideally all data) encrypted from end-to-end from its source to E-CORRIDOR, instead of from our storage to E-CORRIDOR

So that

We ensure the cybersecurity of the data prosumers.

1.5.7.1. Class: Data sharing

1.5.7.2. Discussion

Main stakeholders: Travellers, mobility providers, E-CORRIDOR framework (especially the Cloud)
Referenced stakeholders: None

Mobility providers in this Pilot will share sensitive data:

- Traveller profiles and personal documents
- Traveller status and ratings
- Information from the GPS trackers from the vehicles (and behavioral data (to be confirmed))
- Charging points information flux: Remote control and data about the electrical consumption
- IOT: Remote control by our servers for the Car sharing key access systems and for the charging station remote control and electricity consumption monitoring.
- Data from third party APIs

That is why we would like the shared data to be encrypted with well managed keys.

1.5.7.3. Acceptance Tests

- Shared data is encrypted from end-to-end (Earliest possible)
- In case the cloud is accessed by an intruder, the data is not exploitable
- The key management respects the DSAs

1.5.8. S2C-US-08 Privacy aware interest-based service sharing

As a
Mobility service provider
I want to
Be able to conduct analytics about Connection sources (IP addresses, email addresses) and about Driver profiles, without compromising their privacy.
So that
We ensure the cybersecurity of E-CORRIDOR and the quality of service of mobility providers

1.5.8.1. Class: Data sharing

1.5.8.2. Discussion

Main stakeholders: Advanced security services (WP8), Mobility service providers, service users (travellers).
Referenced stakeholders: None

The FHE technology allows for privacy-preserving analytics, and this would allow mobility providers to share information about the traveller profiles (Fake identities, payment history,

driving history etc.). The traveller profiles encrypted and shared contain information about the profiles.

Other mobility providers could do tests (result=True or False) about profiles. The FHE technology allows also for testing if emails and IP addresses are in the Blacklist.

1.5.8.3. Acceptance Tests

- Test if Traveller A is using a fake driving licence (or one driving licence that is used by multiple accounts) = Driving license number, date, and place of issue, receives an answer (True or False)
- Test if Traveller B has a high payment default risk = Validation status, receives an answer (True or False)
- 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)

1.5.9. S2C-US-09 : Driving behaviour recognition

As a

Mobility service provider

I want to

Be able to recognize whether the current driver is the real account owner

So that

We receive alerts in case of doubt.

1.5.9.1. Class: Data analytics

1.5.9.2. Discussion

Main stakeholders: Data analytics techniques (WP7), Mobility service provider, Drivers
Referenced stakeholders: None

The current state of driver authentication is by username and his password, however a user could give his credentials to someone else and allow him/her to use the service and drive the cars.
Problem : another person could still use the account.
Using behavior data, E-CORRIDOR analytics services could identify if it is the usual driver using FH encrypted data.

1.5.9.1. Acceptance Tests

- After training the model by 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.

1.6. Relevance to E-CORRIDOR objectives

Table 2 : Correlation between the user stories of the S2C pilot and the objectives of the E-CORRIDOR project.

	Objective 1	Objective 2	Objective 3	Objective 4	Objective 5	Objective 6
US-S2C-01	x		x	x	x	x
US-S2C-02	x	x		x	x	x
US-S2C-03	x	x		x	x	x
US-S2C-04	x	x		x	x	x
US-S2C-05	x			x	x	x
US-S2C-06	x			x	x	x
US-S2C-07	x	x	x	x		x
US-S2C-08	x	x	x	x		x

We remind the E-CORRIDOR objectives here:

- 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 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 three pilot products for Car Sharing in smart cities (S2C).
- Objective 7: E-CORRIDOR will be promoted and ease the exploitation, communication, standardization.

The E-CORRIDOR is pilot driven since it is the application of a secure and privacy-aware framework on multimodal transport, in our case the Smart city and Carsharing Pilot. This

application will prove the innovative and much-needed capabilities of E-CORRIDOR explained in the objectives (see above).

Therefore, this pilot's requirements are an embodiment of the E-CORRIDOR's objectives. (**see table above**). Indeed, the eWallet is a step in the direction of seamless multimodality as it saves travellers time and offers them seamless usage of multiple services using secure and privacy-aware data sharing between mobility partners through E-CORRIDOR. Furthermore, the analytics and security services provided by E-CORRIDOR, using data from multiple sources in our pilot, will offer functions needed for enabling multimodality, such as informing the traveller about his itinerary choices, about the estimated durations of trips and about his carbon footprint, and other functions for improving the quality of service like data sharing with transportation authorities, the travellers, and between mobility service providers. E-CORRIDOR will also exploit these data from the pilot in a collaborative and privacy aware manner in order to ensure high levels of cybersecurity for the concerned pilot partners, ensure and encourage trust in the framework's capabilities, and provide valuable analytics results like alerts and protective measures in case of attacks/intrusions. The success of the pilot will prove the E-CORRIDOR framework and provide factual results for reaching **objective 7**.

1.7. Pilot Evaluation

This table recapitulate all the acceptance tests:

Table 3 : Summary of the Acceptance Tests

S2C-AT-01	A registration in one service registers in the other service.
S2C-AT-02	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).
S2C-AT-03	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.
S2C-AT-04	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.
S2C-AT-05	The modification is notified to other operators, and the history of changes can easily be explored (dates of changes, not necessarily previous content).
S2C-AT-06	The Transport Service Provider (TSP) will send the travel request done by the user to the micro-subsidy platform.
S2C-AT-07	The micro-subsidy platform will cross the travel request with the instructions provided by the correspondent public body
S2C-AT-08	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.
S2C-AT-09	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.
S2C-AT-10	The passengers can use trip planning tools provided by E-CORRIDOR to calculate the optimized routes for their trips.
S2C-AT-11	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.
S2C-AT-12	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 context change or critical situations on the initial itinerary);
S2C-AT-13	The results of the route calculated should be compared with other trip planners in the markets to ensure the performance, while the privacy and security aspects of the trip planning tools should be verified based on the security standards set by the project .
S2C-AT-14	The requested operational data is made available through a secured API REST, which is then provided to the transport authority.
S2C-AT-15	The data shared through the REST API is in the format requested by the transport authority.
S2C-AT-16	The transport authority is able to retrieve real-time information about the service through the REST API.
S2C-AT-17	The transport authority is able to access historical data from the service through the REST API.
S2C-AT-18	A user from Clem' tries to sign up for Nemi or vice versa, and is offered the possibility to do it through E-CORRIDOR
S2C-AT-19	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.
S2C-AT-20	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.
S2C-AT-21	A DPO , Data Protected Object, containing a malware, it needs to be detected and blocked at the upload, if not, if it is detected after sharing, the DPO needs to be identified and the concerned stakeholders need to be informed.
S2C-AT-22	Attacks need to be detected, the stakeholders are informed with the source, the level of risk, by email and SMS. Countermeasures to be taken by E-CORRIDOR and countermeasures advised to stakeholders are instructed.
S2C-AT-23	Spamming email addresses detected.
S2C-AT-24	Shared data is encrypted from end-to-end (earliest possible)
S2C-AT-25	In case the cloud is accessed by an intruder, the data is not exploitable.
S2C-AT-26	The key management respects the DSAs.

S2C-AT-27	Test if User A is using a fake driving licence (or one driving licence that is used by multiple accounts) = Driving license number, date, and place of issue, receives an answer (True or False)
S2C-AT-28	Test if User B has a high payment default risk = Validation status, receives an answer (True or False)
S2C-AT-29	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)
S2C-AT-30	After training the model by 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.

2. Use Cases

2.1. Use Case Diagram

In this diagram, the mobility service B could have the same interactions as the mobility service A, the lines aren't drawn here for the sake of graph clarity.

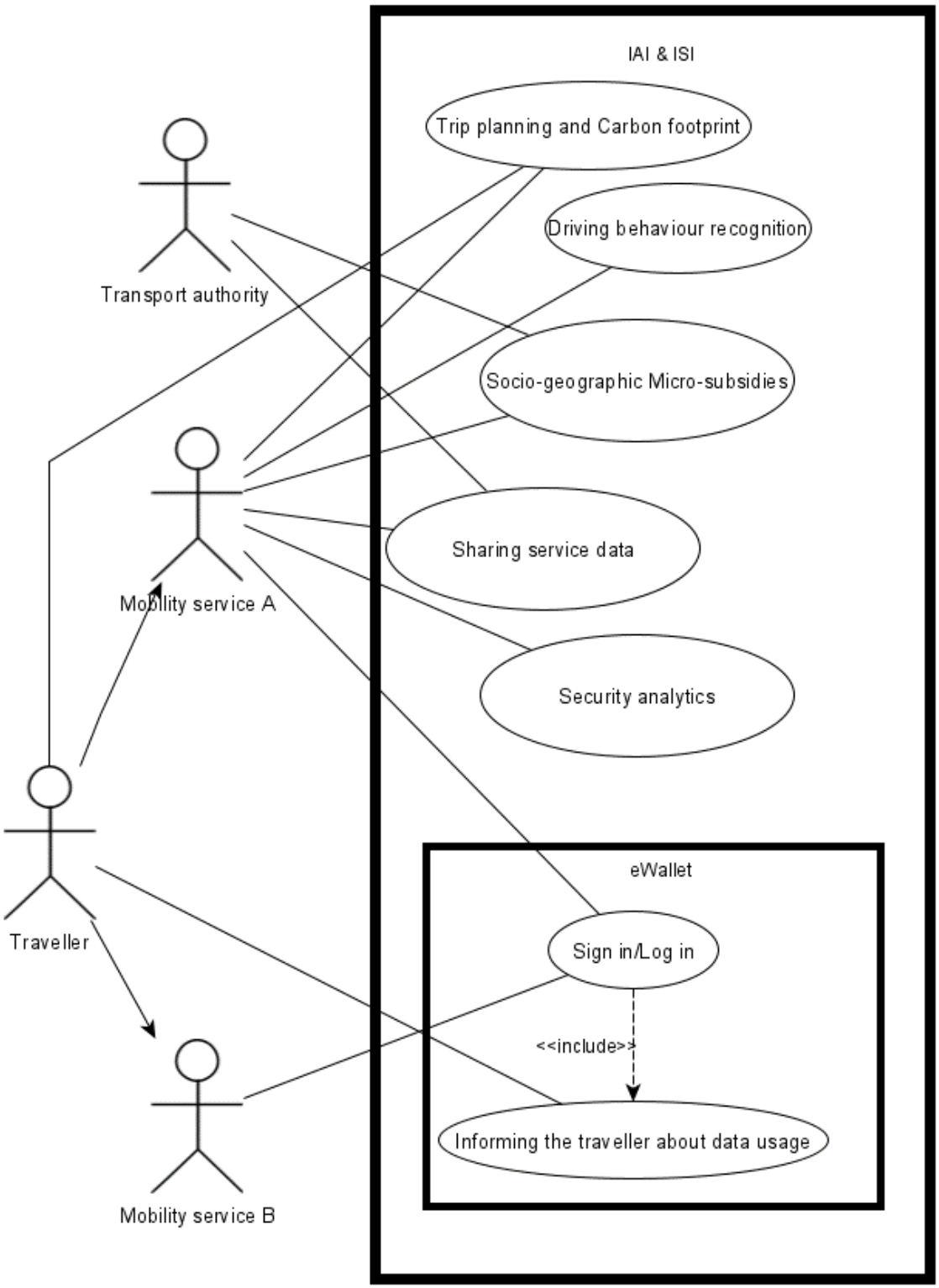


Figure 2: Pilot Use Cases

2.2. Use Case Descriptions

2.2.1. S2C-UC-01: eWallet: Sign in/Log in

Use Case Name	Shared mobility eWallet
Participating actors	Clem', Pildo, AMTU
Purpose	Allowing travellers to connect seamlessly to different mobility services with only one created account on any of these services
Priority	Must
Flow of events: Normal flow	1. Traveller has an account in one mobility service 2. Traveller wants to use another mobility service, and clicks on a button "Log in with E-CORRIDOR" 3. Traveller chooses the mobility service he/she is logged already signed in. 4. Traveller is logged in and can use.
Flow of events: Alternative flow	• Traveller's data is not enough or not validated to allow him/her to use the service. • Traveller's data is used to sign in, and he/she is invited to complete the account profile in the concerned mobility service.
Pre-condition	• Traveller is not logged in, but registered in only one mobility service.

Post-condition	• Traveller logged in seamlessly.

Table 4. S2C-UC-01 use case description

2.2.2. S2C-UC-02: Socio-geographic dependant micro-subsidies

Use Case Name	Micro-subsidies platform
Participating actors	Factual, Clem, AMTU, Pildo
Purpose	Enable multimodal trip planning for travellers and single registration/authentication via an eWallet and, a socio-geographical based method for micro subsidies for multimodal trips.
Priority	Must
Flow of events: Normal flow	1. The traveller has an account in the mobility service. 2. The traveller wants to use this mobility service for a specific trip. 3. The traveller books a trip, with a specific origin and destination, for this mobility service. 4. The mobility service provides a price for this trip, based on the analysis carried out by the micro-subsidies platform. 5. The traveller accepts the price for this trip. 6. The user performs the trip. 7. The micro-subsidy system validates that the trip has been performed and is validated for subsidy.

Flow of events: Alternative flow	• There is no alternative flow.
Pre-condition	• The micro-subsidies platform knows the traveller's location and profile and the expected trip (origin and destination). • The public authority informs the micro-subsidies platform over the discounts that can be offered to the travellers. • The public authority allocates a budget to the micro-subsidies, and it has the means to transfer the funds to each TSP involved in the micro-subsidies system.
Post-condition	• The user have a micro-subsidy for using a sustainable mobility service.

Table 5. S2C-UC-02 use case description

2.2.3. S2C-UC-03: Trip planning and carbon footprint analysis

Use Case Name	Trip planning and carbon footprint analysis
Participating actors	WIT, Clem', Pildo, AMTU
Purpose	Allowing travellers to calculate optimized routes for their multimodal trips according to their criteria and check relevant trip information, and calculate and track carbon footprint info of their trip both before and after the trips
Priority	Could

Flow of events: Normal flow	• The travellers provide the origin and destinations locations of their trips and relevant preferences data such as carbon footprint, price, time and number of connections. • Trip planning and carbon footprint analysis tools provided by E-CORRIDOR will calculate the optimized routes for their trips, along with the estimated carbon footprint info for each route. • The travellers check the route and carbon footprint info and choose their preferred route. • The travellers will be directed to relevant multi-modal transport service provided by E-CORRIDOR (e.g., car-sharing service provided by Clem') or external transport services. • After the trip, the travellers can check their trip information including the actual carbon emission.
Flow of events: Alternative flow	• If travellers have changed their trip info (e.g. destination locations) or relevant traffic info have been updated (e.g. traffic jam or extreme weather) during their trips, the trip planning will recompute the itinerary at runtime considering the context changes and inform the travellers about changes made for their routes. • Travellers can gain suggestions from carbon footprint analytics tools and choose routes with least carbon emission and check their real-time trip info including the emission during their trips.
Pre-condition	• Travellers know the origin and destinations of their trips, but want to learn about the details of possible routes and relevant multi-modal transport service, or want to check the carbon footprint of their past trips.
Post-condition	• Travellers have learned about the detailed route suggestions or the information of finished trips (including carbon footprint) through the tools provided by E-CORRIDOR and have been seamlessly directed to relevant transport service.

Table 5. S2C-UC-03 use case description

2.2.4. S2C-UC-04: Sharing service data with Transport authority

Use Case Name	Sharing data with Transport authority
Participating actors	Pildo
Purpose	Ensuring that the transport authority has access to the operational data from Pildo's DRT service that it requires
Priority	Could
Flow of events: Normal flow	1. The transport authority makes use of a REST API to access real-time and historical data from the service's operation
Flow of events: Alternative flow	• The data from the service's operation is shared with the transport authority via their data management portal[2]
Pre-condition	• A REST API that gives access to the operational data from Pildo's DRT service is setup • The data is stored in the format required by the transport authority
Post-condition	• The transport authority keeps track of the service's performance successfully

Table 6. S2C-UC-04 use case description

2.2.5. S2C-UC-05: Informing travellers about data usage and privacy.

Use Case Name	Informing travellers about data usage and privacy
Participating actors	Clem', Pildo
Purpose	Keeping the traveller informed about the usage of his/her data
Priority	Could (can be done by just a generic text in the general conditions (to be evaluated))
Flow of events: Normal flow	1. A traveller registered in Clem' tries to use Nemi for the first time, or vice versa 2. During the sign-up process, the traveller is shown the possibility to sign-up through E-CORRIDOR 3. When choosing this option, the traveller is shown a message that informs him/her of the new data privacy policy that applies 4. If the traveller wants to read it before accepting, he/she is shown a link or a button which leads to a text which includes, at least, the companies that are granted access to the traveller's personal data and the purposes for which they access and use the data 5. The traveller accepts the new data privacy policy
Flow of events: Alternative flow	1. A traveller who is not registered in Clem' nor in Pildo tries to use one of the two mobility services for the first time 2. During the sign-up process, the traveller is shown the possibility to sign-up through E-CORRIDOR 3. When choosing this option, the traveller is shown a message that informs him/her of the data privacy policy that applies 4. If the traveller wants to read it before accepting, he/she is shown a link or a button which leads to a text which includes, at least, the companies that are granted access to the traveller's personal data and the purposes for which they access and use the data 5. The traveller accepts the new data privacy policy

Pre-condition	• There is a legal text that includes exhaustive information regarding data management of travellers who benefit from E-CORRIDOR's technology • E-CORRIDOR partners which offer this possibility (Clem' and Pildo in the case of this pilot) feature this information through their platforms (mainly, app and website)
Post-condition	• The traveller makes use of E-CORRIDOR's technology being aware of the way his/her data is accessed and used

Table 7. S2C-UC-05 use case description

2.2.6. S2C-UC-06: Security analytics: Notifications and threat/attack management

Use Case Name	Cybersecurity: threat/attack management
Participating actors	Data owners (Mobility service providers); Passengers; ISAC; Security and analytics services
Purpose	Guarantee a high level of Cybersecurity and threat management
Priority	Should
Flow of events: Normal flow	1. The data owners share data to cloud encrypted by FHE 2. The data is analyzed 3. Threats are identified 4. A notification is sent (type of threat, source, risk level, advice)

Flow of events: Alternative flow	Breach of a DSA: 1. Analysis stopped 2. Files quarantined (if necessary) 3. Data owner informed
Pre-condition	• Threats undetected • Data containing the threat source or the information about the threat and its source
Post-condition	• Threats detected or a pattern is recognized • Concerned parties are notified

Table 8. S2C-UC-06 use case description

2.2.7. S2C-UC-07: Security analytics: Privacy aware interest-based service sharing

Use Case Name	Privacy aware interest-based service sharing
Participating actors	Mobility service providers; Travellers; Security and analytics services
Purpose	Conducting analytics about shared data without compromising their privacy
Priority	Could

Flow of events: Normal flow	1. The mobility service provider shares traveller profiles data encrypted by FHE. 2. The mobility service provider asks if one traveller's data is validated by the other mobility service providers (statues of driving license, being banned, or having unpaid bookings) 3. The mobility service provider receives and answers (true or false)
Flow of events: Alternative flow	• No information about the traveller available.
Pre-condition	• Malicious traveller undetected (fake driving license, or one driving license used on multiple accounts, Risky IP or email addresses).
Post-condition	• Warning about certain travellers or sources of external connections

Table 9. S2C-UC-07 use case description

2.2.8. S2C-UC-08: Driving behaviour recognition

Use Case Name	Driving behaviour recognition
Participating actors	Mobility service providers; Travellers; driver, analytics services
Purpose	Recognizing the driver's identity from the driving behaviour
Priority	Could

Flow of events: Normal flow	• Driver books a car and logs in. • Driving behaviour is matched with the usual driving behaviour of that account.
Flow of events: Alternative flow	• Driving behavior is different, an alert with a level of certainty metric sent to the mobility service provider.
Pre-condition	• Driver is only identified by a log in id and password.
Post-condition	• Driver's identity verified

Table 10. S2C-UC-08 use case description

2.3. Catalogue of Use Cases

Table 12: Mapping of Use Cases to User Stories

Use Case	User Stories
S2C-UC-01	S2C-US-01
S2C-UC-02	S2C-US-02
S2C-UC-03	S2C-US-03
S2C-UC-04	S2C-US-04
S2C-UC-05	S2C-US-05
S2C-UC-06	S2C-US-06
	S2C-US-07
S2C-UC-07	S2C-US-08
S2C-UC-08	S2C-US-09

2.4. Storyboard

The following storyboards recall some of the user stories introduced in Section 1.5

2.4.1. S2C-SB-01: storyboard for User Story S2C-US-01 eWallet

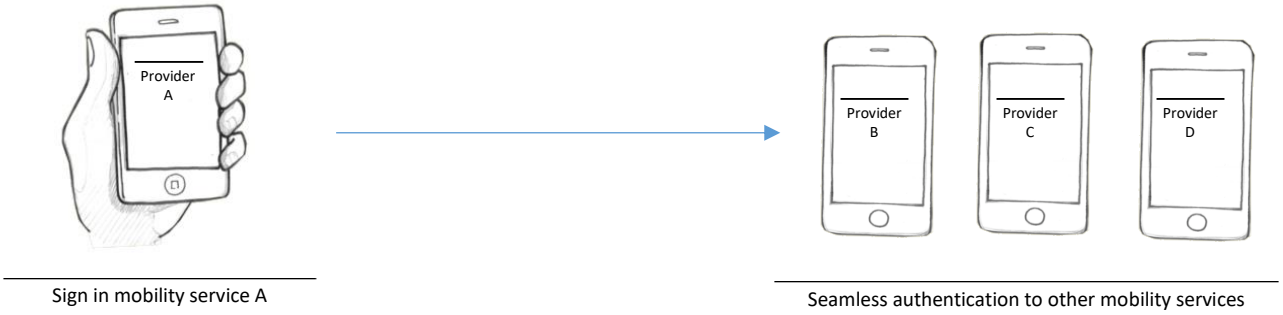
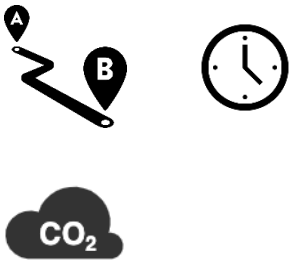


Figure 3: Storyboard for User Story S2C-US-01

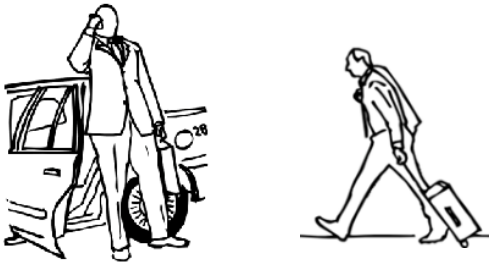
2.4.2. S2C-SB-02: storyboard for User Story SC-US-03 Trip planning and carbon footprint analysis

1) A traveller/user aims to plan a trip using any of the available systems in the E-CORRIDOR platform.



2) the E-CORRIDOR Trip Planning tool suggests possible routes according to the origin, destination, arrival time and other user preferences (such as carbon footprint).

3) The user decides which transportation option suits him/her the best and proceeds with the journey. Suggested trips include multimodal transport ones.



4) The user will be directed the multimodal transport service and information service provided by E-CORRIDOR and enjoy his/her trip.

5) The user can check the relevant trip information (such as time and carbon footprint) after trips.

6) If trip information is shared with transport authorities and transport service operators by the user, they can use the information to improve the transport operation and policies.

Figure 4: Storyboard for User Story S2C-US-03

2.4.3. S2C-SB-03: storyboard for User Story S2C-US-06 Cybersecurity: notifications

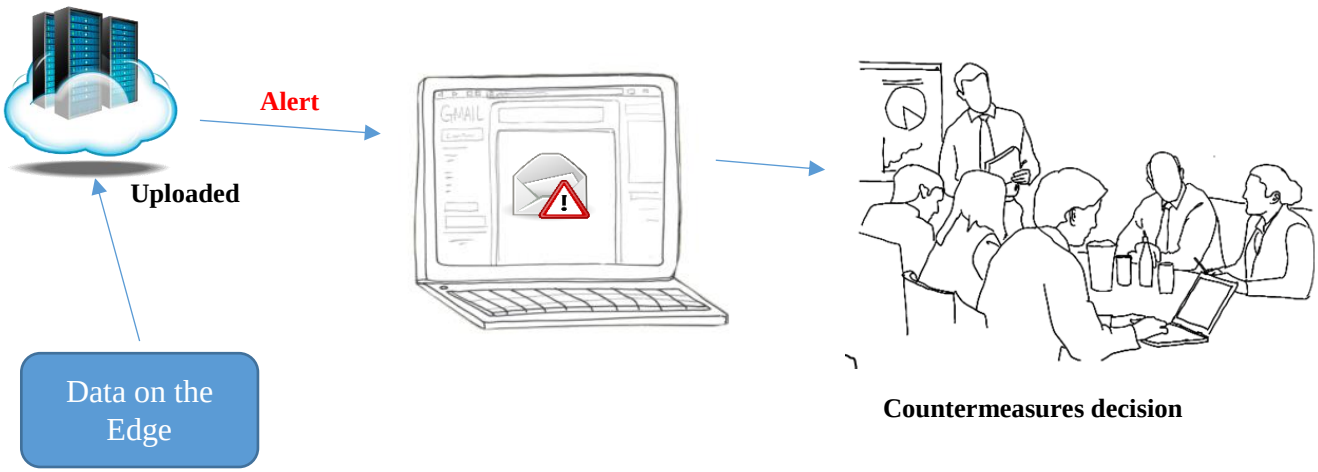


Figure 5: Storyboard for User Story S2C-US-06

3. Non-functional Requirements

Table 13: List of Non Functional Requirements

3.1. Security

S2C-NFR-01	Flexible and interoperable Identity management schemes.
S2C-NFR-02	Compliant to GDPR data sharing.
S2C-NFR-03	Anonymize sensitive usage and personal data that would be shared, from end to end. (DMO (Data Manipulation Operations such as anonymization, pseudonymisation, FHE, other Encryption …) prior to the sharing will be defined for each data object in the excel file joined to this document)
S2C-NFR-04	Secure identity management: the authentication mechanisms for the eWallet need to be secure and reliable.
S2C-NFR-05	Secure identity management: the seamless authentication needs to be privacy aware. (the flows for logging into one account having logged into to the account before needs to not include personal data)
S2C-NFR-06	A central log for the operations done need to be saved.
S2C-NFR-07	The shared data must be encrypted by a standard encryption for the data shared where both parties need to access the content of the data. (US-S2C-01 02 05 06) FHE for where data analytics must not be able to access the content of the data. (US-S2C-03 04 07 08)

3.2. Performance

S2C-NFR-08	The time for the updates within DPO to all concerned prosumers should be reasonable.
S2C-NFR-09	Upload/download time, response time
S2C-NFR-10	The local hardware performance needed to operate needs to be reasonable

3.3. Usability

S2C-NFR-11	The DSA definition interface needs to be clear and easy to use (low possibility of making errors).
S2C-NFR-12	The time for the updates within DPO should be reasonable.
S2C-NFR-13	A notification or a status follow up for the DPO updates.
S2C-NFR-14	A dashboard for the status of the different components (OK, down).

3.4. Operational

S2C-NFR-15	Hybrid deployment model (a local ISI in order to sanitize the data before sharing)

4. Conclusions

This pilot will contribute to advancing mobility into a new level, where data sharing and collaborative approaches are conducted with security and privacy. These new capabilities will make travelling easier and more convenient as well as guaranteeing a higher quality of service of multimodal transportation.