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

D3.2

Design and Architecture for the S2C Pilot

WP3 – Car Sharing Pilot (S2C)

E-CORRIDOR

Edge enabled Privacy and Security Platform for Multi Modal Transport

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

31/05/2021

Version 1.0

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

Project 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	
RE	Restricted to a group specified by the consortium (including the	
CO	Confidential, only for members of the consortium (including the	

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

Authors: M. Ammara (CLEM’), B. Flinois (CLEM’), S. Soufflet (CLEM’), M. Restrepo Sanchez (CLEM’), C Plappert (FhG), S. Paniagua (PLD), E. Consegal (AMTU), M. Jofre (FC), V. Moyano (FC), R. Han (WIT), J. O’Rourke (WIT)

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

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	16-Mar-2021	M. Ammara	CLEM’	Initial ToC and 1st Draft
0.2	19-Mar-2021	R. Han J O’Rourke	WIT	Trip planning and Carbon footprint analytics
0.3	25-Mar-2021	M. Ammara	CLEM’	Section 2
0.4	30-Apr-2021	M. Ammara	CLEM’	Section 4.4
0.5	1-Apr-2021	M. Ammara S. Soufflet	CLEM’	Section 2, 3, 5
0.6	2-Apr-2021	M. Ammara B. Flinois	CLEM’	Overall updates
0.7	9-Apr-2021	C. Plappert	FhG	Section 3 : eWallet architecture and authentication
0.8	14-Apr-2021	M. Ammara	CLEM’	Section 4 : Block Design and Component design Section 7 and 8
0.9	19-Apr-2021	V. Moyano M. Jofre	FC	4.1.2 and 4.3 : Micro-subsidies analytics
0.10	07-May-2021	M. Ammara	CLEM’	Merging, formatting, Executive summary and conclusion.
0.11	10-May-2021	M. Restrepo S. Soufflet B. Flinois	CLEM’	General revision
0.11	13-May-2021	R. Han	WIT	Internal review and comments
	28-May-2021	S Paniagua	PLD	Formatting
0.12	28-May-2021	F. Martinelli	CNR	General Revision
0.13	28-May-2021	M. Ammara	CLEM’	Security model update, Section 3 update
0.14	31-May-2021	F. Martinelli	CNR	General revision
0.15	31-May-2021	M. Restrepo	CLEM’	Addressed comments from F. Martinelli.
1.0	31-May-2021	M. Ammara	CLEM’	Addressed comments from reviewers. All sections involved.

Executive Summary

The deliverable presents the Smart city and Car Sharing (S2C) Pilot design and architecture in the E-CORRIDOR project. This architecture is designed to fulfil the requirements expressed in the previous deliverable D3.1 and to act as a reference for the next steps of the Pilot in the E-CORRIDOR project: implementation, deployment, tests, experimental validation, and evaluation.

First, a reminder of the pilot objectives and a presentation of the different concepts developed or used within the pilot to fulfil these objectives are provided. Then, the eWallet concept and architecture are presented, and eWallet is the central concept behind this pilot consisting of a digital unique shared identity of the mobility services users (denoted in the deliverable as “travellers” for clarity). The pilot combines various innovative concepts that will improve the multi-modal mobility experience for all the stakeholders thanks to secure data-sharing.

Next, the FMC modelling language is used to break down and describe the different blocks and components interacting in each use case, customizations of the components required for the pilot as well as the pilot specific analytics are presented. Finally, we present the data and security models, the deployment model and the subsequent hardware and software requirements.

Conclusively, this deliverable is the basis of the future works related to the next milestones MS3 “Setup of the running pilots” and MS4 “First Version of integrated platform and Pilots.” leading to the next deliverable D3.3 “First implementation, test and validations of the S2C Pilot”.

Table of contents

Executive Summary 3

1. Introduction 6

1.1. Overview....6

1.3. Definition and Abbreviations 6

2. System Overview....7

3. System Architecture....10

3.1. The eWallet 11

3.2. System Architecture for the eWallet....11

3.3. eWallet authentication mechanisms Alternatives 13

3.4. High-Level Protocol Overview for the eWallet Use Case 14

3.4.1. Adaptations for Backend Authentication.... 15

3.4.2. Adaptations for the OAuth2.0 Token Binding Extension 17

4. Component Architecture 19

4.1. Block Design 19

4.1.1. S2C-BD-01: Block diagram for S2C-UC-01 Sign in.... 19

4.1.2. S2C-BD-02: Block diagram for S2C-UC-02 Micro-subsidies.... 19

4.1.3. S2C-BD-03: Block diagram for S2C-UC-03 Trip planning and carbon footprint analytics.... 21

4.1.4. S2C-BD-05: Block diagram for S2C-UC-06 Security analytics services.... 22

4.1.5. S2C-BD-06: Block diagram for S2C-UC-07 Privacy-aware interest-based sharing.... 23

4.1.6. S2C-BD-07: Block diagram for S2C-UC-08 Driving behavioural recognition.... 24

4.2. Components Design 24

MSP web service backends customization.... 24

Central E-CORRIDOR customization 24

4.3. Analytics 25

4.3.1. S2C Pilot specific analytics.... 25

4.3.1.1. S2C-AF-01: Micro-subsidies.... 25

4.3.1.2. S2C-AF-02: Privacy-aware interest-based sharing 26

4.4. Data model 26

5. Integration with E-CORRIDOR 27

6. Security Model 28

6.1. Confidentiality 29

6.2. Data Integrity....29

6.3. Authentication 30
6.4. Authorisation 30
7. Deployment Model 30
7.1. Hardware requirements 30
7.2. Software requirements 31
8. Requirements Matrix 31
9. Conclusion 34
10.References 35

List of figures

Figure 1: High-level architecture 11
Figure 2: System Architecture for the eWallet Use Case 13
Figure 3: eWallet Backend Authentication 16
Figure 4: eWallet OAuth2.0 Token Binding 18
Figure 5: S2C-BD-01: Block diagram for S2C-UC-01 Sign in 19
Figure 6: S2C-BD-02: Block diagram for S2C-UC-02 Micro-subsidies 21
Figure 7: S2C-BD-03: Block diagram for S2C-UC-03 Trip planning and Carbon footprint 21
Figure 8: S2C-BD-05: Block diagram for S2C-UC-06 Security analytics services 23
Figure 9: S2C-BD-06: Block diagram for S2C-UC-07 Privacy-aware interest-based sharing 23
Figure 10: S2C-BD-07: Block diagram for S2C-UC-08 Driving behavioural recognition 24
Figure 11: Deployment model for the S2C Pilot 28

List of tables

Table 1: eWallet Alternative Comparison 14
Table 2: Data types and formats 27
Table 3: Mapping Use Cases and User Stories to architecture diagrams 33

1. **Introduction**

1.1. Overview

The main purpose of this deliverable is to describe the architecture of the S2C Pilot and its integration with the E-CORRIDOR framework, a main part of the Task 3.2 of WP3 "S2C Pilot design and Integration".

First, we will present a high-level view of the architecture and the pilot goals and scenarios, and then a more detailed presentation of each of the architecture's blocks and components. This architecture is designed with the goal of fulfilling the requirements defined in the first deliverable D3.1 [CLEM'2020]. Finally, we will present the integration/deployment model within the E-CORRIDOR Framework and its standards components as well as the security model in place.

1.3. Definition and Abbreviations

Term	Meaning
ASI	Advanced Security Infrastructure
API	Application Programming Interface
AF	Analytic Function
Authorization	The right or a permission that is granted to a system entity to access a system resource
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system
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
FMC	Fundamental Modeling Concepts
FHE	Fully Homomorphic Encryption
GDPR	General Data Protection Regulation
GPS	Global Positioning System

IAI	Information Analytics Infrastructure
ISAC	Information Sharing and Analysis Centre
ISI	Information Sharing Infrastructure
JSON	JavaScript Object Notation
MaaS	Mobility as a Service
MSP	Transportation Service Provider = Mobility service provider
OBD	On Board Diagnostics
S2C	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
UID	Unique Identifier
UUID	Universally Unique Identifier

2. System Overview

The purpose of the S2C Pilot is to demonstrate E-CORRIDOR framework's data sharing capabilities and effectiveness in making multi-modal transportation secure and more seamless in the context of carsharing and Demand-Responsive Transit (DRT) multimodality, capitalizing on the privacy-preserving data sharing and analytics services and the security infrastructure provided by the E-CORRIDOR framework.

First, a brief listing of the goals of the S2C Pilot:

- Allow single registration of travellers at multiple mobility service providers through a shared eWallet containing the traveller's information.
- 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 smart privacy-preserving itinerary planning and carbon footprint analytics service.
- Enable behavioural driver identification analytics.

The main two actors of the S2C Pilot are the traveller and The mobility service providers (MSPs). In this project we have two MSPs, the carsharing operator Clem' and the DRT (bus-on-demand) service provider Nemi. Through data sharing using the E-CORRIDOR framework, they will make the traveller experience more seamless and guarantee a high level of cybersecurity and data governance and privacy.

The main concepts behind the pilot are presented as follows:

eWallet: the eWallet is the shared storage of unique digital identities of travellers (user profile), it serves as a reference for The mobility service providers and the E-CORRIDOR ecosystem entities alike. The travellers (mobility services users) will register only once by providing the needed documents and information. The data will be stored directly in the eWallet that is stored in the central Cloud of E-CORRIDOR, and then The mobility service providers will fetch the traveller's data from the eWallet to get the necessary information and create user profiles for the travellers. If a mobility service provider validates the authenticity of the information, the latter can mark this fact in the eWallet so that other mobility service providers can trust it and avoid doing the same work, as a result the registration process much faster thanks to collaboration and data sharing. This enables a seamless registration process for both the travellers and The mobility service providers. The second major advantage is having a central reference where mobility service providers can save and share relevant information in a unique eWallet.

The micro-subsidies: The micro-subsidies analytics toolkit considers the following factors:

- Traveller's profile (e.g., senior citizens, occupation, etc.).
- Trip characteristics (modes of transportation used, time of departure/arrival, origin/destination and whether it passes through a geographical zone).
- Number of trips subsidized in the past.

Based on these factors, it determines the eligibility for a micro-subsidy (1€ or so) of a trip. The information regarding these factors will be shared through E-CORRIDOR's ISI as well as the attribution of micro-subsidies.

FHE enabled analytics: The FHE (fully homomorphic encryption) is an encryption technology allowing analytics on data without decryption. This is a very useful technology for third-party privacy preserving analytics. In a use case, The mobility service providers will share their rating on the users to the FHE analytics service, and the latter will calculate an average and share it back to the mobility services. This way the analytics services cannot access the data but still provide a result, and at the same time, the mobility services cannot know the traveller's rating on each of the mobility services. More use cases could be considered, such as checking if the traveller's documents are validated by other mobility service providers, or if a traveller's account is suspended at one or more mobility service providers.

The trip planning and carbon footprint: The mobility service providers will share through the E-CORRIDOR framework the available service information for bus-on-demand trips and car sharing, also the vehicle characteristics (i.e., carbon footprint profiles of vehicles). The IAI will access this shared data, and the trip planning tool in IAI will use it to suggest (upon request) the best multi-modal itinerary according to the traveller's preferences.

Cyberthreat management and intrusion detection: The mobility service providers in the Pilot will share server connection logs, files, emails, and data from the vehicles to the central E-CORRIDOR cloud. The security analytics services will conduct their analytics on the data, and in case of threats or intrusions detection it will notify the concerned mobility service providers.

Driver identification: The mobility service will share the available driver behaviour data about the driver in pseudonymized data. In the case of a stolen car for example or someone using someone else's user credentials, the driver identification analytics will detect it and alert The mobility service providers.

Global scenario:

We can imagine a scenario involving all these concepts during the pilot from the point of view of a traveller: a new user selects both MSPs (seeking multimodal trips) in the E-CORRIDOR registration form and submits his/her documents and information. This creates an eWallet with its associated Data Sharing Agreement (DSA) [CNR2020] [MPS2010] and is stored in the central E-CORRIDOR Cloud. It is accessible to the MSPs that are authorised to do so according to the DSA. The MSPs use this accessible eWallet to create an account in each one respectively. The most time-consuming task of the account creation process is the validation of the documents (most of the time done manually by a person). Thanks to data sharing, the first MSP to validate the documents will mark in the eWallet if the document is valid (by whom and when etc.), and the other MSPs can trust this information and validate the account without rechecking the documents. The traveller then can access and use all E-CORRIDOR mobility services.

One can use the privacy-preserving trip planning developed in WP7 (Task 7.2 and Task 7.4) to plan his/her trips according to his/her preferences (among them the carbon footprint of the trip) and these preferences can be also stored in the eWallet. His/her trip can be accorded a micro-subsidy (~ -2€) if the micro-subsidies analytics consider the trip characteristics and the user profile eligible.

The Trusted Service Manager TSM [CEA2020] developed in WP8 Task 8.5 is the component that manages and secures identities using roots-of-trusts based authentication and authorization mechanisms, the role that this component plays in the scenario is clarified in the following Section 3: System Architecture.

During all the steps of this scenario:

The threat information such as data from the virtual machines (VMs) connection logs, emails, uploaded files (mainly into the eWallet) and data from vehicles is a rich source of information for the Advanced Security Infrastructure (ASI) and the analytics used for intrusion detection, cyberthreat intelligence, driver behavioural identification. Some of the data will be fully homomorphically encrypted for highly sensitive data sharing, in this case, the Information Analytics Infrastructure can conduct analytics on data without decrypting it, this proves useful in cases where the third party is not fully trusted or if giving sharing this data involves complicated legal procedures and regulations. Another very useful use case is when multiple parties want to share data for collaborative analysis but at the same time want to keep each individual party inputs private and disseminate only the final result.

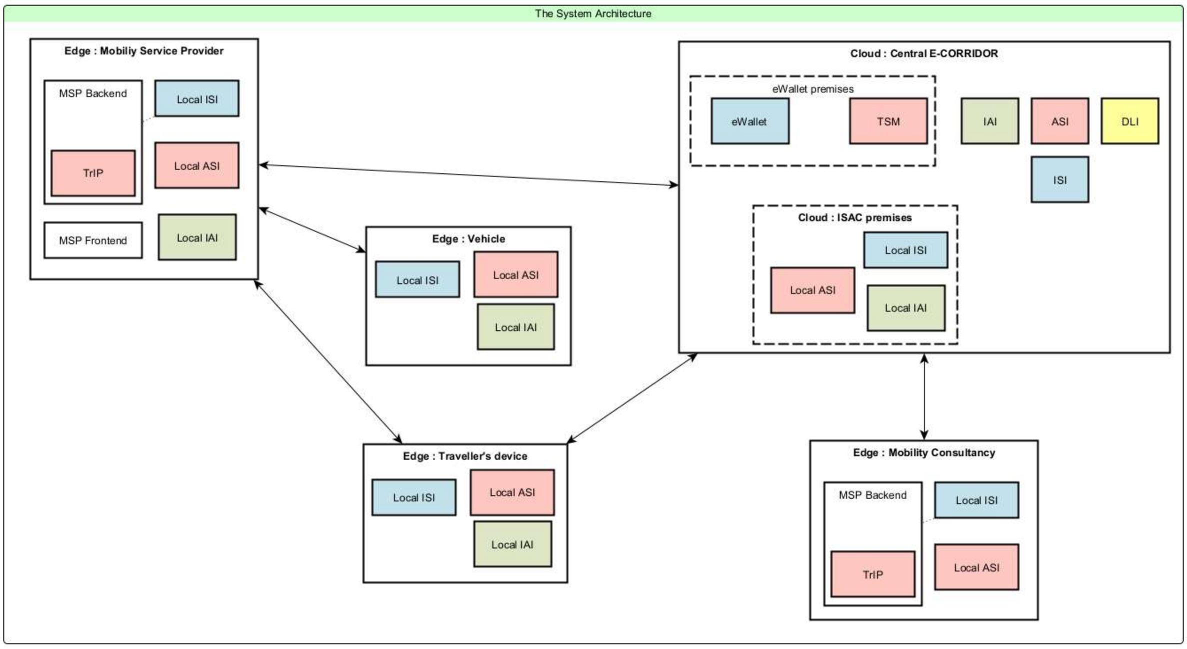
The data governance is ensured by DSAs, which are sticky policies linked to the data objects enforcing rules on authorisation (who can do what) and obligations (what should be done before which actions).

3. System Architecture

The S2C Pilot scenario involves multiple entities who act towards E-CORRIDOR as data prosumers, namely:

- The mobility service providers: they aspire to offer a seamless user experience and ensure their respect for the data protection obligations and a high level of cybersecurity and threat management.
- The analytics and security service providers using data from multiple sources according to predefined DSAs (micro-subsidies analytics toolkit, privacy preserving itinerary-planning and carbon footprint, the cyberthreat management analytics, the intrusion detection, and driver behavioural identification).
- The travellers.

The following graph presents the high-level architecture. In the following sections of the document, we describe the architecture in more details: first the eWallet and then the rest of the use cases.



.

Figure 1: High-level architecture

3.1. The eWallet

Currently, if a user wants to use a multi-modal mobility service, he/she needs to make accounts for each service provider. Furthermore, The mobility service providers cannot coordinate their services to ensure the complementarity and interoperability between the services without a unique digital identity of the traveller, nor can the public authorities subsidize particular parts of a multi-modal trip of the same user based on trusted unique identity.

To overcome the shortcoming of the cumbersome registration and authentication process, an eWallet system is proposed. With eWallet, a user will store his/her data in a virtual wallet that stores all necessary information to authenticate with all participating service providers. The advantage for the user is that he/she only has one single unique identity and can log into any participating mobility app without making multiple accounts. Moreover, The mobility service providers can save data related to the identity of the traveller within the eWallet that is accessible to other mobility service providers and partners for share, analytics, and later usage. Finally, all of this is protected thanks to the advanced security infrastructure and the framework's security by design principles.

3.2. System Architecture for the eWallet

The system architecture for the eWallet is depicted in Figure 2. It shows the most prominent entities with two exemplary service providers: A car sharing service (Clem') and a Bus-on-demand service (Nemi by Pildo labs).

In particular, the system architecture consists of the User with his/her Personal Device (1.1) and also his/her Browser (1.2), the car sharing and bus-on-demand service backends (2.1 and 3.1 respectively) with their resources, e.g., the car and the bus terminal (2.2. and 3.2. respectively), and finally the eWallet Provider (4). The car is divided into the car (2.2.2) (as a physical asset) and the so-called Car Access Proxy (CAP) (2.2.1) that acts as communication broker between the car and the car sharing service backend.

As seen in Figure 2, the relevant system entities may implement some edge components of the E-CORRIDOR framework, for example Edge ISI, Edge IAI and the Edge ASI to carry out advanced security services of E-CORRIDOR. For the eWallet use case, especially the Trusted Identity Provider (TrIP, Task 8.5) of the ASI component is used to securely distribute credentials and establish strong identities across the participating entities.

The overall idea is that the user creates an eWallet account and later on authenticates with the eWallet to authorize all the services participating in the E-CORRIDOR eWallet system.

In the scope of the project, different variants to implement the eWallet are analyzed. The different alternatives are presented and analyzed in the following.

N.B: TSM : Trusted Service Manager

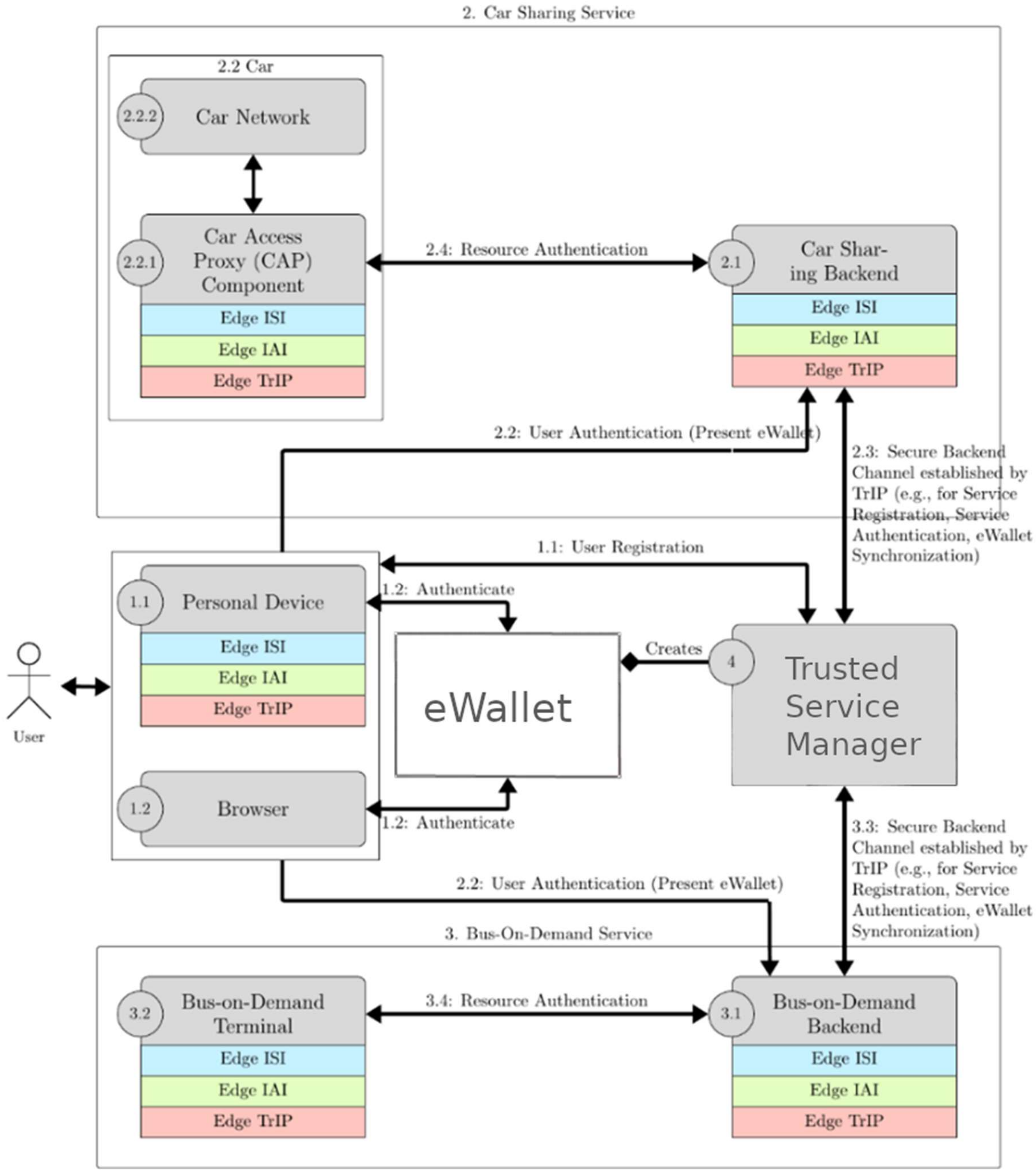

2. Car Sharing Service
2.2 Car
2.2.2 Car Network
2.2.1 Car Access Proxy (CAP) Component
Edge ISI
Edge IAI
Edge TrIP
2.4: Resource Authentication
2.1 Car Sharing Backend
Edge ISI
Edge IAI
Edge TrIP
2.2: User Authentication (Present eWallet)
2.3: Secure Backend Channel established by TrIP (e.g., for Service Registration, Service Authentication, eWallet Synchronization)
1.1: User Registration
1.2: Authenticate
1.1 Personal Device
Edge ISI
Edge IAI
Edge TrIP
User
eWallet
Creates
4 Trusted Service Manager
1.2 Browser
1.2: Authenticate
3.3: Secure Backend Channel established by TrIP (e.g., for Service Registration, Service Authentication, eWallet Synchronization)
2.2: User Authentication (Present eWallet)
3. Bus-On-Demand Service
3.2 Bus-on-Demand Terminal
Edge ISI
Edge IAI
Edge TrIP
3.4: Resource Authentication
3.1 Bus-on-Demand Backend
Edge ISI
Edge IAI
Edge TrIP

Figure 2: System Architecture for the eWallet

3.3. eWallet authentication mechanisms Alternatives

First, two definitions:

- Authorization: The right or a permission that is granted to a system entity to access a system resource.

- Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

To realize the eWallet system, many alternative approaches can be proposed and analyzed regarding their feasibility within the project. Table 1 below shows a comparison of two alternatives.

In the first alternative, the OAuth2.0 authorization protocol [HARDT2012] is enhanced with a token binding mechanism [BHNPGMM2012] that is carried out by the TrIP. The second alternative focuses on securing the backend communication between the Service Provider Backends and the E-CORRIDOR backend. Here, TrIP is only implemented in the backends of the Service providers.

Since in the mobility market there are already many actors with different interests and characteristics, each one having its established proprietary information system, and since the open standards are limited to public transit timetables [GITHUB2021]. The path towards multi-modality can take one of two directions : one dominant mobility actor imposes its standards on all the other actors which takes a lot of spending and effort from all mobility actors to adapt their information systems to standards that are not ideal for each mode of transportation, the other direction is to establish an “eWallet” that is flexible enough to be highly scalable, highly interoperable and doesn’t create barriers to entry or limiting dependencies. Two alternatives will be explored in the pilot, one with the minimal impact and the other one with low impact yet it allows for Single Sign-On (SSO) Support: backend authentication only and OAuth2.0 extension.

Alternative	Advantage	Disadvantage
OAuth2.0 extension	• Extension of a Standard (Token Binding) • SSO Support	• Need a parallel central TrIP (E-CORRIDOR)
Backend Authentication (only)	• Better Acceptance/ Faster integration with Industry partners	• Still accounts for every Service (no SSO)

Table 1: eWallet Alternative Comparison

3.4. High-Level Protocol Overview for the eWallet Use Case

The general eWallet system consists of the generic protocols Service Registration, Service Profile Update, User Registration, User Profile Update, User Authentication, and eWallet Sharing. They are explained in general here and the specific adaptation for the two approaches are detailed in the following sections.

During the service registration protocol, each service provider that wants to participate in the eWallet sharing registers with the eWallet provider and, among other things, transmits the list of data he/she will need from the future users in the eWallet. This needs to be done once. However, if the required data changes in the future, the service provider can transmit the updated required data via Service Profile Update protocol.

During user registration, the users register with the eWallet provider and creates his/her eWallet credentials. Based on the transmitted data during the Service Registration protocol, the eWallet provider can tell the user which data he/she needs to enter to later use which particular service. Moreover, according to the mobility services chosen by the traveller, the DSA will be defined accordingly for the eWallet e.g., which service provider can access which data or how many times can a service provider use a later created token before another user authentication is necessary. This protocol typically needs to be done once. However, if new services join the eWallet system or some data becomes outdated, e.g., driver license validity period, the user may need to update the eWallet profile. This is done with the Profile Update protocol.

The authentication protocol varies depending on the chosen alternative. This and other adaptations are detailed in the following.

3.4.1. Adaptations for Backend Authentication

Figure 3 shows an instantiation of the eWallet system for the Backend Authentication approach.

Once the registration process is completed, the eWallet provider triggers the legacy account creation for all participating service providers. They will notify the users to complete their profile with a password, e.g., via Email.

The authentication is then done as follows: The user authenticates with the credentials of the distinct service provider he/she wants to use (legacy authentication). If he/she authenticates successfully, the service provider requests the necessary data from the eWallet profile of the eWallet Provider (eWallet Sharing) via a secure channel, e.g., TLS. He verifies the profile and depending on the result grants access or not.

In this approach, TrIP is only used to establish secure channels between the backends, e.g., during Service registration and eWallet Sharing during the legacy authentication.

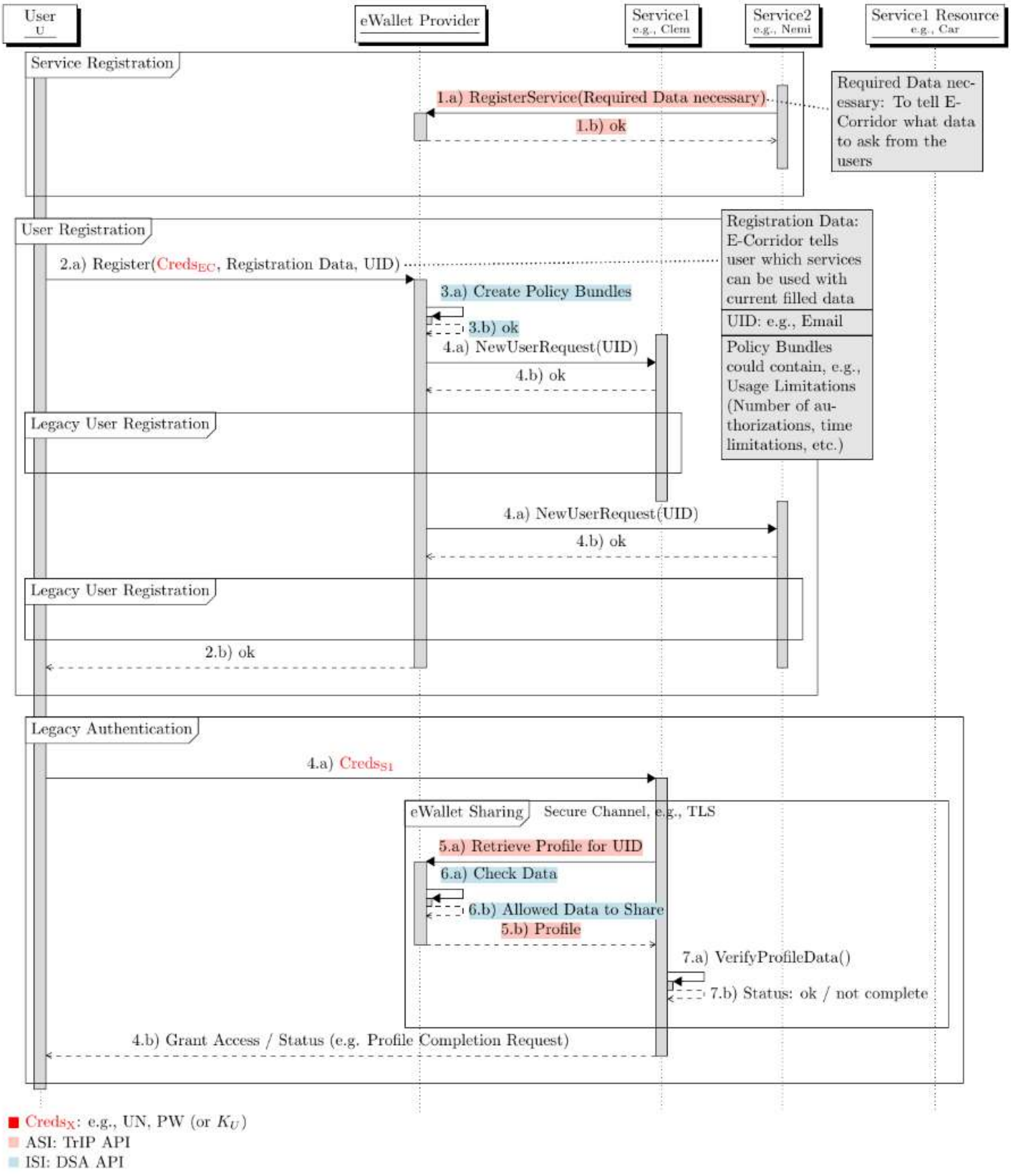

User
U
eWallet Provider
Service1
e.g., Clem
Service2
e.g., Nemi
Service1 Resource
e.g., Car
Service Registration
1.a) RegisterService(Required Data necessary)
1.b) ok
Required Data necessary: To tell E-Corridor what data to ask from the users
User Registration
2.a) Register(Creds$_{EC}$, Registration Data, UID)
Registration Data: E-Corridor tells user which services can be used with current filled data
UID: e.g., Email
Policy Bundles could contain, e.g., Usage Limitations (Number of authorizations, time limitations, etc.)
3.a) Create Policy Bundles
3.b) ok
4.a) NewUserRequest(UID)
4.b) ok
Legacy User Registration
4.a) NewUserRequest(UID)
4.b) ok
Legacy User Registration
2.b) ok
Legacy Authentication
4.a) Creds$_{S1}$
eWallet Sharing
Secure Channel, e.g., TLS
5.a) Retrieve Profile for UID
6.a) Check Data
6.b) Allowed Data to Share
5.b) Profile
7.a) VerifyProfileData()
7.b) Status: ok / not complete
4.b) Grant Access / Status (e.g. Profile Completion Request)
■ Creds$_{X}$: e.g., UN, PW (or K_U)
■ ASI: TrIP API
■ ISI: DSA API

Figure 3: eWallet Backend Authentication

3.4.2. Adaptations for the OAuth2.0 Token Binding Extension

Figure 4 shows an instantiation of the eWallet system for the OAuth2.0 Token Binding Extension approach.

During the authentication protocol, the user accesses the Website or (Web-) App of the service provider and states that he is an eWallet user, e.g., by selecting it in the login page of the service provider ("log in as eWallet user"). The user is then redirected to the eWallet authentication where the user authenticates. A token is created that contains among other things various policies and the service provider keys. The token can be used to establish a secure channel between Service Provider and eWallet to retrieve the necessary data.

In this approach, TrIP is used to establish secure channels between the backends, e.g., during Service and User registration and creates the Token for the eWallet Sharing.

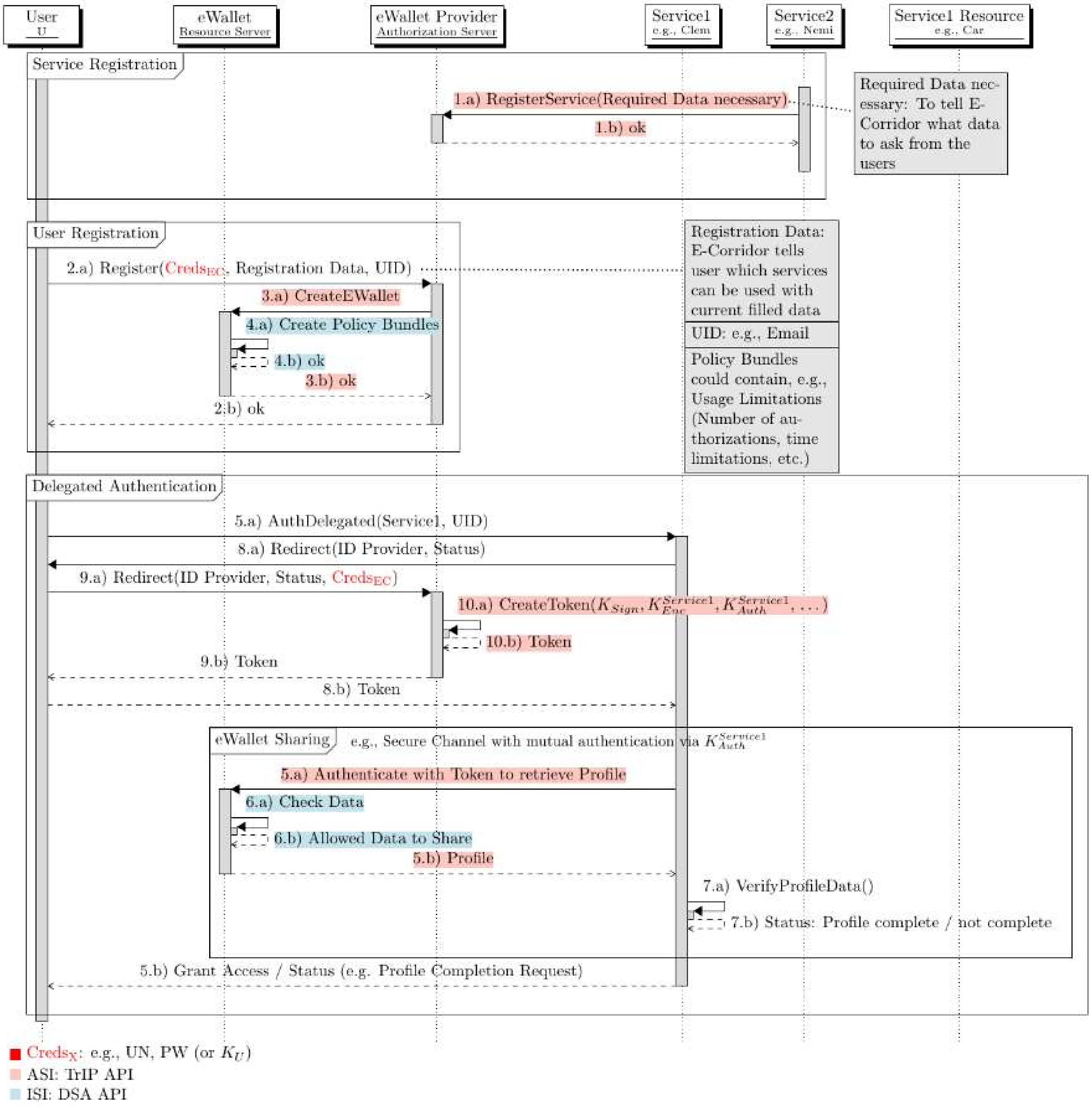

User
U
eWallet
Resource Server
eWallet Provider
Authorization Server
Service1
e.g., Clem
Service2
e.g., Nemi
Service1 Resource
e.g., Car
Service Registration
1.a) RegisterService(Required Data necessary)
1.b) ok
Required Data necessary: To tell E-Corridor what data to ask from the users
User Registration
2.a) Register(Creds_{EC}, Registration Data, UID)
3.a) CreateEWallet
4.a) Create Policy Bundles
4.b) ok
3.b) ok
2.b) ok
Registration Data: E-Corridor tells user which services can be used with current filled data
UID: e.g., Email
Policy Bundles could contain, e.g., Usage Limitations (Number of authorizations, time limitations, etc.)
Delegated Authentication
5.a) AuthDelegated(Service1, UID)
8.a) Redirect(ID Provider, Status)
9.a) Redirect(ID Provider, Status, Creds_{EC})
10.a) CreateToken($K_{Sign}, K_{Enc}^{Service1}, K_{Auth}^{Service1}, \ldots$)
10.b) Token
9.b) Token
8.b) Token
eWallet Sharing
e.g., Secure Channel with mutual authentication via $K_{Auth}^{Service1}$
5.a) Authenticate with Token to retrieve Profile
6.a) Check Data
6.b) Allowed Data to Share
5.b) Profile
7.a) VerifyProfileData()
7.b) Status: Profile complete / not complete
5.b) Grant Access / Status (e.g. Profile Completion Request)
🟥 Creds_X: e.g., UN, PW (or K_U)
ASI: TrIP API
ISI: DSA API

Figure 4: eWallet OAuth2.0 Token Binding

4. Component Architecture

4.1. Block Design

4.1.1. S2C-BD-01: Block diagram for S2C-UC-01 Sign in

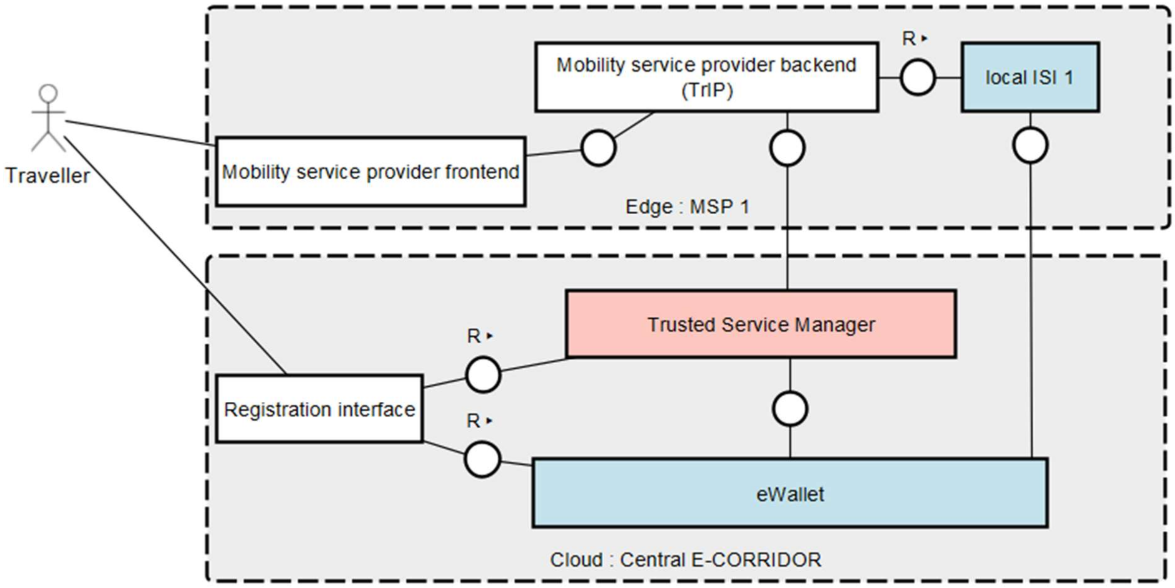

Mobility service provider backend (TrIP)
R ▸
local ISI 1
Traveller
Mobility service provider frontend
Edge : MSP 1
Trusted Service Manager
R ▸
Registration interface
R ▸
eWallet
Cloud : Central E-CORRIDOR

Figure 5: S2C-BD-01: Block diagram for S2C-UC-01 Sign in

The sign in process (registration) for a new traveller starts by a simple registration through a web form where one submits his/her personal data and information. This data is stored then in the Central E-CORRIDOR ISI in the eWallet. The mobility service providers regularly synchronize the traveller's profiles in their respective local ISIs taking for a reference the data in the Central E-CORRIDOR ISI. The mobility service providers then have to fetch the traveller's profile data from the local ISI, adapt its format and make the user account at their backends respectively.

In the graph, for readability, only one Mobility Service Provider is presented.

4.1.2. S2C-BD-02: Block diagram for S2C-UC-02 Micro-subsidies

Factual's micro-subsidies analytics toolkit calculates the eligibility and the amount of a micro-subsidy to accord to a traveller using one's metadata and one's trip attributes such as the departure time, job location, age, origin-destination, among others. The solution is flexible, at the configuration level, to use different types of criteria, depending on the real use case scenario of the pilot.

The use case happens at two stages:

1. The user requests a trip price and gets the information, including the promised micro-subsidy.

2. A verification that the trip done is compliant with the micro-subsidy conditions and application of the micro-subsidy at the billing and finally saving everything in the eWallet in the central E-CORRIDOR.

Case 1: Using a trip planner interface

Stage 1: Requesting a trip price.

The traveller will request the trip from location A to location B through the trip planner interface, and if the mobility service provider station is located between, the itinerary planning tool can suggest it. This request is forwarded to Factual's micro-subsidies analytics toolkit to calculate the amount of subsidy and then, the final trip price is suggested to the traveller. Once the traveller accepts it, he/she can be directed to relevant mobility service providers to make necessary bookings.

Stage 2: The verification phase.

The mobility service providers gather proofs that the trips are done and send them back to the micro-subsidies analytics toolkit to verify post-trip eligibility. After the verification, the micro-subsidies analytics toolkit stores this data to make the required reporting by the transportation authorities regarding the spending of the micro-subsidies.

The proofs in case of a multimodal trip (in this case, between Nemi bus on demand and Clem' carsharing) will contain several verification proofs:

-QR code screened on the bus, to verify that this part of the trip has been done.

-GPS data from the car, to confirm that the user has arrived at the destination, and the booking data for the car sharing trip.

Case 2: Not requiring the trip planner interface.

In this case, both stages (requesting a trip price and the verification phase) work in a similar way to those Case 1, but with a direct contact between The mobility service providers and the micro-subsidies analytics toolkit, The mobility service providers can share the trip requests and user metadata with the micro-subsidies analytics toolkit, and the latter verifies the eligibility and accords the micro-subsidy to the trips with the further step of verification of trips.

For the architecture enabling these scenarios through the E-CORRIDOR framework, it is represented hereinafter:

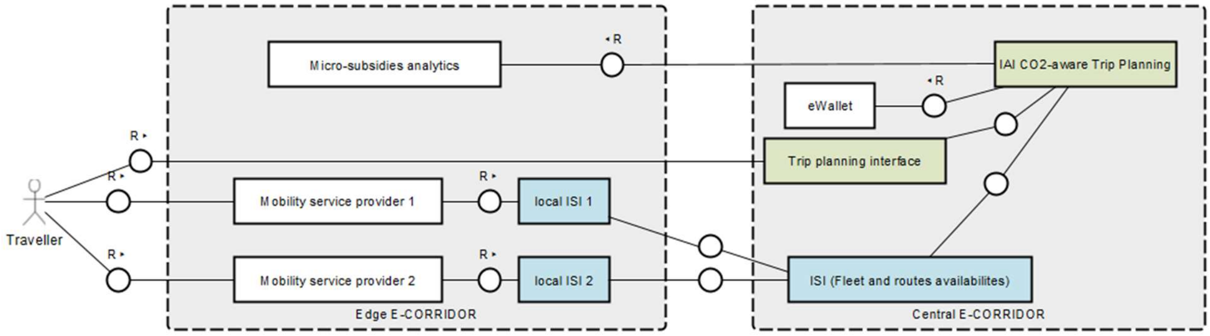

Micro-subsidies analytics
R
IAI CO2-aware Trip Planning
eWallet
R
Trip planning interface
R
R
R
Traveller
Mobility service provider 1
R
local ISI 1
Mobility service provider 2
R
local ISI 2
ISI (Fleet and routes availabilites)
Edge E-CORRIDOR
Central E-CORRIDOR

Figure 6: S2C-BD-02: Block diagram for S2C-UC-02 Micro-subsidies

4.1.3. S2C-BD-03: Block diagram for S2C-UC-03 Trip planning and carbon footprint analytics

The use case *S2C-UC-03 Trip planning and carbon footprint analysis* defined by Deliverable 3.1 concerns travellers (e.g., passengers, mobility service users, drivers), who plan to calculate optimised routes for their multimodal trips according to certain criteria and estimate the carbon footprint information of their trips both before and after the trips. This use case targets the pre-trip scenarios since most travellers care about the duration, distance, and traffic condition of a trip before starting it to enhance the travel experience or satisfy specific demands (arriving at a specific time or generating the least CO2 emission). The following figure shows the FMC block diagram of this use case.

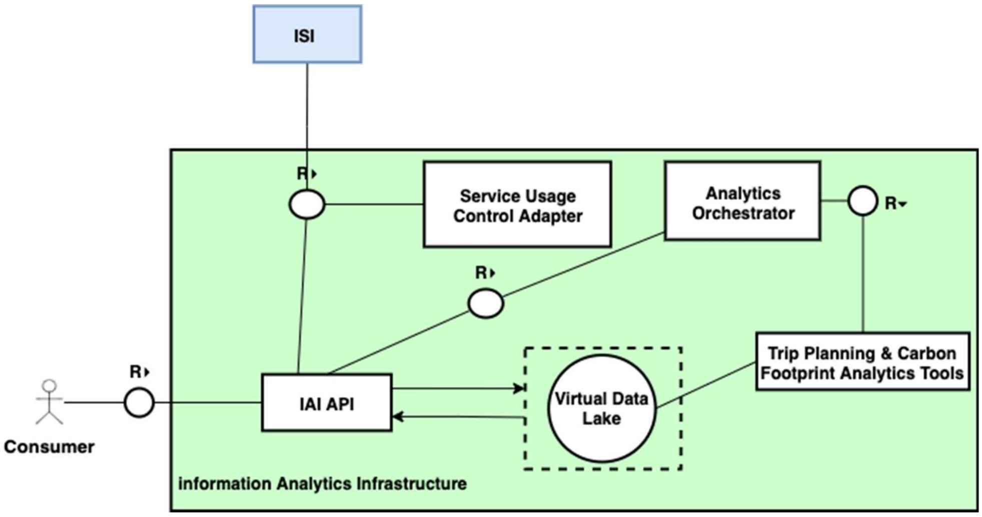

ISI
R
Service Usage Control Adapter
Analytics Orchestrator
R
R
Trip Planning & Carbon Footprint Analytics Tools
R
IAI API
Virtual Data Lake
Consumer
information Analytics Infrastructure

Figure 7: S2C-BD-03: Block diagram for S2C-UC-03 Trip planning and carbon footprint analytics

The traveller, who is the information consumer in this case, uses a web browser or a client to access the Information Analytic Infrastructure (IAI) API to request the trip planning and carbon footprint analysis service. If the request succeeds, the IAI will return potential trip and carbon footprint information to the end-users.

This API will deal with the requests for the service by calling the analytics orchestrator. To be specific, the Service Usage Control Adapter and Analytics Orchestrator are standard parts of the IAI component of the E-CORRIDOR framework. The Service Usage Control Adapter is an instance of the Continuous Authorization Engine provided by the framework and is integrated within the IAI subsystem, to control the usage of the analytics services exposed by the framework. This is a security mechanism for enforcing the usage control policy paired with the analytics services both at access request time and continuously. Last, Analytics Orchestrator orchestrates multiple analytics services if an application involves using more than one analytics service.

Mobility service providers need to periodically share their transport service information (such as vehicle locations and availability) with the E-CORRIDOR framework through ISI. Then, when consumers trigger the trip planning and carbon footprint calculation through IAI, the transport service information stored in ISI will be checked against their DSA policies and copied to a virtual data lake in IAI for further data analysis. Due to the time-variant characteristics of their transport service, mobility service providers such as Clem' and Pildo need to publish their latest service information to the framework regularly, to ensure passengers and drivers can get up-to-date and optimized trip suggestions.

Besides, the trip planning and carbon footprint analytics tools in IAI should also be able to call the APIs of the micro-subsidies analytics toolkit to enable the calculation and display potential micro-subsidies information.

4.1.4. S2C-BD-05: Block diagram for S2C-UC-06 Security analytics services

The mobility service providers have multiples inflows of data under different formats, sharing the relevant server logs (URLs and IP addresses), email addresses, files from eWallet and data from the vehicles will detect threats and intrusions.

The bigger the amount of data and the number of sources, the richer the intrusion detection analytics resources are. To guarantee the privacy of the data and their owners, the data will be manipulated (anonymisation, pseudonymisation, FHE, or obfuscation) before sharing.

The mobility service providers can invoke the IAI API for punctual analytics (in addition to the regular periodic analytics). They will also receive notifications and alerts in case of cyberattacks or intrusion detection.

The ISAC Pilot, using these shared cyberthreat data in addition to data from other sources, will perform pilot-specific (also mode of transportation specific) analytics to accurately label cyberthreat information and to generate security reports.

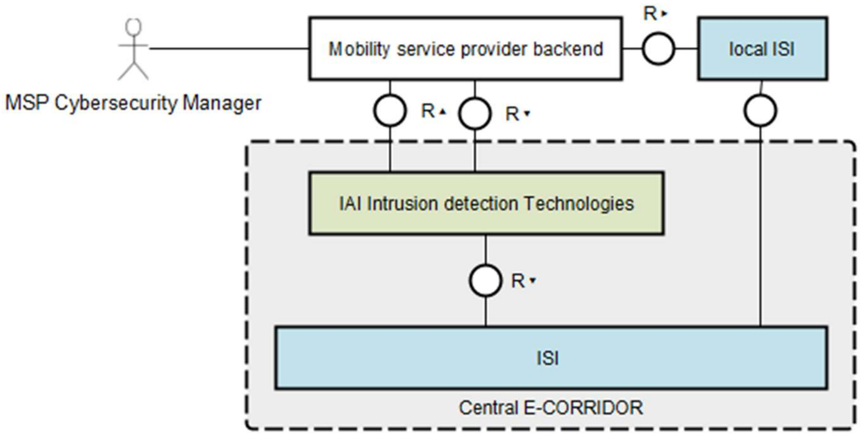

R▸
Mobility service provider backend
local ISI
MSP Cybersecurity Manager
R▴
R▾
IAI Intrusion detection Technologies
R▾
ISI
Central E-CORRIDOR

Figure 8: S2C-BD-05: Block diagram for S2C-UC-06 Security analytics services

4.1.5. S2C-BD-06: Block diagram for S2C-UC-07 Privacy-aware interest-based sharing

This use case exploits two characteristics of the Privacy-aware interest-based sharing:

- Data is Fully Homomorphically Encrypted, so third-party analytics can be conducted on data without decrypting it.
- The ability to conduct analytics combining multiple sources of information in a privacy-aware manner and disseminating only the final result.

The mobility service providers can edit the traveller’s profile on the central ISI (accessible to other mobility service providers or not, this will be defined through the DSA). They can invoke privacy-aware interest-based sharing analytics such as traveller’s preferences for modes of transportation, traveller’s notation, traveller’s usage of micro-subsidies or other price reductions etc. One mobility service provider can therefore get the results of the analytics without needing to trust the third party and without disclosing each data inputs, in our pilot with 2 MSPs it is easy to guess the other MSP’s input if you know the analytics results and your own input, however, in an E-CORRIDOR ecosystem full of MSPs, this will prove useful and effective.

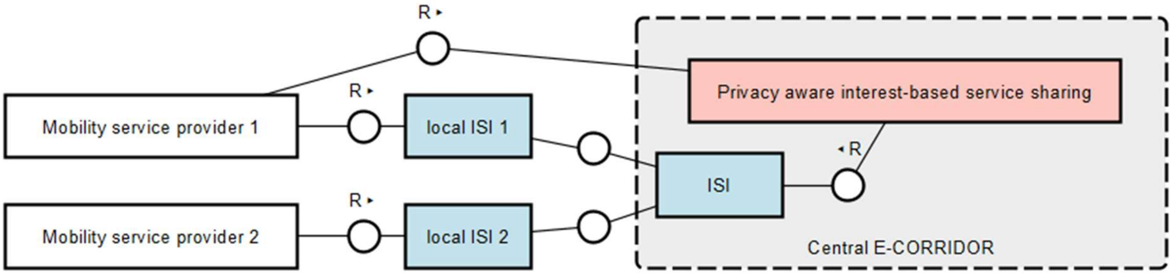

R▸
Privacy aware interest-based service sharing
R▸
Mobility service provider 1
local ISI 1
◂R
ISI
R▸
Mobility service provider 2
local ISI 2
Central E-CORRIDOR

Figure 9: S2C-BD-06: Block diagram for S2C-UC-07 Privacy-aware interest-based sharing

4.1.6. S2C-BD-07: Block diagram for S2C-UC-08 Driving behavioural recognition

The mobility service providers will share data about the driving behaviour the driver through the ISI, this way the data becomes accessible for the IAI, the latter contains the "Secure routine: driver identification" component.

The mobility service can then invoke the IAI API in order to get a reporting on the results of the analytics.

An alert by email is sent by the IAI to the mobility service provider in case of a driving behaviour that does not match the usual driver's driving.

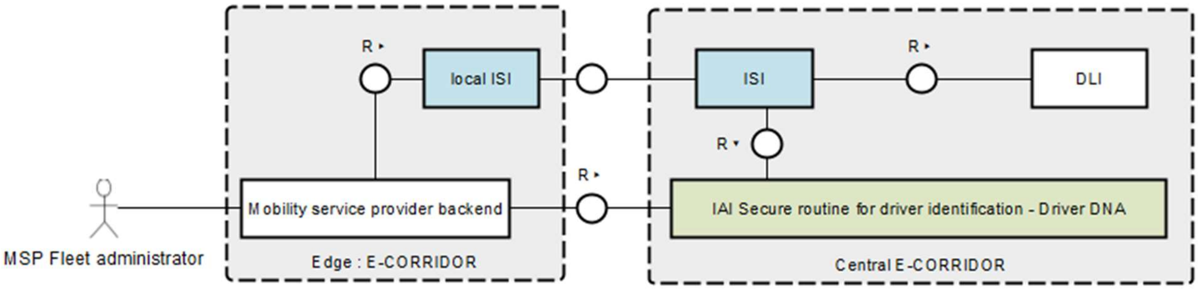

R
local ISI
ISI
R
DLI
R
R
Mobility service provider backend
IAI Secure routine for driver identification - Driver DNA
MSP Fleet administrator
Edge : E-CORRIDOR
Central E-CORRIDOR

Figure 10: S2C-BD-07: Block diagram for S2C-UC-08 Driving behavioural recognition

4.2. Components Design

The E-CORRIDOR framework's components are flexible and adapted to the pilot's data sharing requirements [CNRS2020]. However, some customization is needed:

MSP web service backends customization

The mobility service providers as well as the mobility consultancies and all the future members of the E-CORRIDOR ecosystem who will use the eWallet need to establish a data format converter between the local ISI and the backends of their services, the data format converter converts the user profile from the Mobility Service Provider's proprietary format to the eWallet unique format, it is basically a data mapping process. They also need to deploy a TrIP (trusted identity providers) to get registered with the Central E-CORRIDOR Trusted Service Manager TSM.

Central E-CORRIDOR customization

It is noteworthy to mention that a microservice within the Central E-CORRIDOR for hosting an independent (from MSPs) registration interface to the eWallet microservice is required. This latter will host the web forms and the creation of eWallet profiles directly into the Central E-CORRIDOR ISI. Also, the micro-subsidies analytics toolkit is a legacy analytics, thus, it will be deployed in Factual's backend, however it will be invoked by the IAI in the Central E-CORRIDOR Cloud. Last but not least, the TrIP and a central storage solution (e.g: NoSQL database such as MongoDB) will be deployed within the eWallet which is deployed in the Central E-CORRIDOR Cloud.

4.3. Analytics

4.3.1. S2C Pilot specific analytics

4.3.1.1. S2C-AF-01: Micro-subsidies

As mentioned above, the micro-subsidies engine has the responsibility to decide whether or not a certain trip is subsidised. This functionality can be customised to a number of different subsidy scenarios – named in the system as subsidy programmes. The criteria can be:

1. Geographical: can include different geographical polygons and rules to apply different subsidy values depending on the origin, destination, or passthrough zones of the trips.
2. Time based: the programmes can include these criteria if it makes sense to apply different subsidy values depending on the time and date of the trip. For example: only subsidise trips that happen on a weekday in the morning.
3. Traveller metadata: trips taken by certain travellers may be eligible to receive subsidies, but not everyone. Although this data is totally anonymous to the subsidy toolkit because the user identity is not shared, the trip planning tool or mobility service provider makes subsidy requests sending data that is used as a criterion for a certain programme (e.g., age, working company, etc.).
4. Limits: the entity responsible for the subsidy programme may decide to impose limits on the amount of a subsidy or on the number of subsidies that can be applied to a certain traveller. Another interesting option with this criterion is to allow the programme to have a certain budget burn-rate like, for example, if there is a monthly cap to spend.

After deciding on the details of the pilot, these criteria will be configured on the subsidy toolkit, and The mobility service providers will send a subsidy request for each trip, including the required data that is used on the subsidy calculation.

This input data is evaluated in real-time, and, on the same integration interface (API), the result is sent back to the mobility service provider app so that the user is informed of the available subsidy. At the end of the trip (or on a different timeframe to be agreed), the trips can become confirmed, and the financial deductions are then finalised.

As output data from the toolkit, different data analytics are available like, for example: available budget, daily burn-rate, monthly burn-rate, most popular origins/destinations subsidised, etc.

The flexibility is high, and the integration is easy. The specifics of the pilot analytics are totally dependent on what subsidy criteria will be used.

4.3.1.2. S2C-AF-02: Privacy-aware interest-based sharing

To enable communication using Fully Homomorphic Encryption between the MSPs and the IAI, The MSPs first will invoke its local ISI API which will then invoke the Local FHE API which is a Subsystem Integrated into the local ISI that encrypts data before sharing (FHE is one of the DMOs available in the ISI and enforced thanks to the DSAs).

We have two applications:

- Each MSP will share the eWallet ID and the number of the usage of the MSP's service, these data protected objects will be then stored in the IAI Virtual data lake available for analytics, the privacy-aware interest-based sharing toolkit will calculate the sum by each eWallet ID and send back the result FHEncrypted.
- Each MSP shares a list of suspended driving licences, in the same way, the MSPs can invoke the IAI API to check whether a driving licence is already suspended by one of the MSPs.

4.4. Data model

This table from D5.2 is a reminder of the data and its format generated and exchanged in the S2C Pilot.

Data Type Class	***Data Format***	***Standard***	***Pilot Use Case ID***
Bus geo-positioning	*GPX*	*Proprietary*	*S2C-US-06*
Bus speed	*Proprietary*	*Proprietary*	*S2C-US-06*
Time of arrival of the bus at every stop	*Proprietary*	*Proprietary*	*S2C-US-06*
User profile	*JSON*	*Proprietary*	*S2C-US-01*
			S2C-US-06
			S2C-US-06
			S2C-US-07
			S2C-US-08
Trip data	*JSON*	*Proprietary*	*S2C-US-02*
			S2C-US-06
			S2C-US-03

Micro-subsidies calculation results data	*JSON*	*Proprietary*	*S2C-US-02*
Connection logs	*Structured Text*	*Proprietary*	*S2C-US-06*
			S2C-US-07
E-mails	*EML*	*Open Standard*	*S2C-US-06*
			S2C-US-07
DRT (bus-on-demand) service and usage data	*JSON*	*Proprietary*	*S2C-US-06*

Table 2: Data types and formats

5. Integration with E-CORRIDOR

This section explains how each S2C Pilot partner is deploying different E-CORRIDOR components (such as ISI, IAI, ASI, and CSI), and how they are interacting with the centralised E-CORRIDOR components. The communication between the different microservices will be over Internet using mainly RESTful APIs, hence the need for establishing reliable and secure communications, the security model is discussed in the following section 6.

The E-CORRIDOR deployment model suited for the S2C Pilot is "E-CORRIDOR edge-to-cloud distributed". In the following, we will explain the reasons behind this choice and describe the deployment.

The S2C Pilot unites different mobility service providers around a unique single digital identity of the travellers that is what we define as eWallet. Another central element of the pilot is the Trusted Service Manager TSM that manages authorisation and authentications towards the eWallet. Having these two central entities requires a central E-CORRIDOR cloud. The mobility service providers and the mobility consultancy (with their Micro-subsidies analytics toolkit) will deploy the ISI and the ASI on the Edge respectively that would allow the communication between the mentioned entities and the central eWallet. The behavioural identification and some of the intrusion detection analytics need to be conducted locally (considering data protection obligations, computational power, and data bandwidth limitations). Thus, some of the Edges will deploy a local IAI containing the concerned local analytics while the rest of the analytics developed within the WP7 used in the S2C Pilot will be deployed in the central cloud.

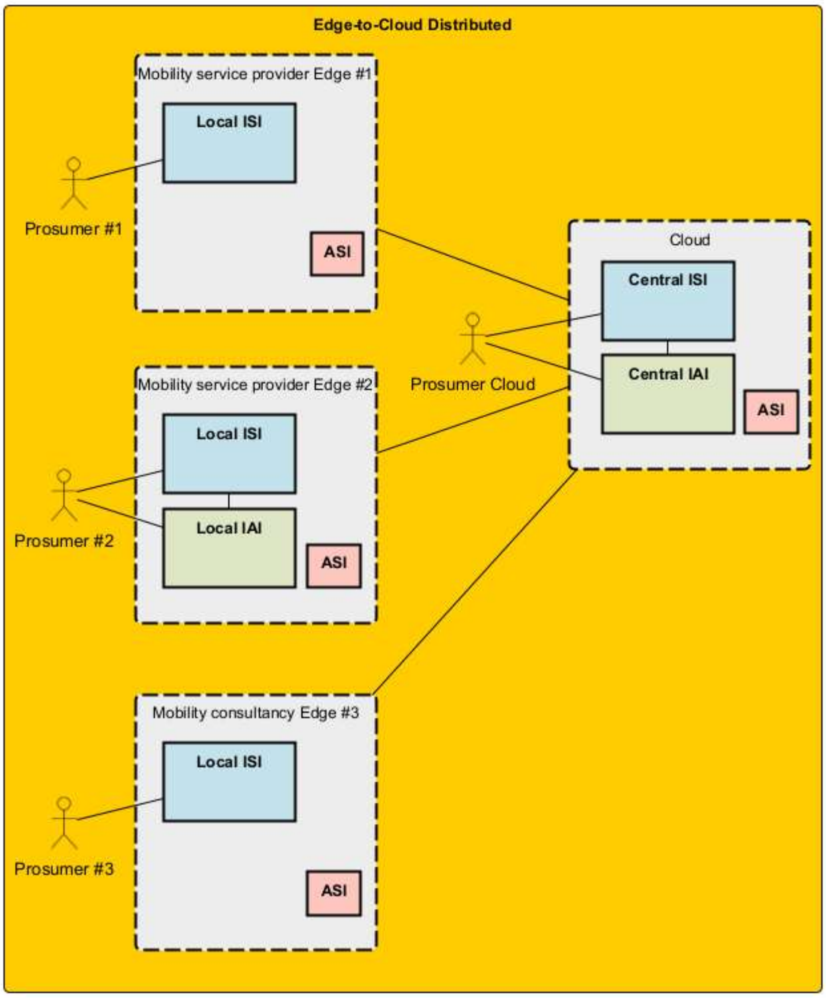


Figure 11: Deployment model for the S2C Pilot

6. Security Model

Lack of Trust is a major barrier to data-sharing, especially when it concerns personal data. Guaranteeing a secure data-sharing framework is essential for building trust among all mobility stakeholders [WBCSD2020] and onboarding more members into the E-CORRIDOR ecosystem: travellers, mobility service providers, the security services, and the analytics services.

Consequently, the E-CORRIDOR framework and its implementation in the pilots are designed with a security model in place to attain the cybersecurity and data privacy objectives of the project, in particular, 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.”

The eWallet is secure and shared between mobility service providers, it contains sensitive personal data of the travellers, therefore, an emphasis is given to the eWallet authentication and authorization using Root(s)-of-Trust, it provides many benefits which are explained in the following sections.

The editing of the eWallet is secure and auditable thanks to the Common Security Infrastructure and the DSA Lifecycle Infrastructure.

The confidentiality of data shared with the IAI is maintained by the different complementary levels of the security model as explained in the following sections in the document, but in addition to that, the data is pseudonymised before sharing. And in some use cases, the data is homomorphically encrypted, which means that the analytics toolkit will not decrypt the data when performing the analytics.

The security model has three complementary main levels:

- The authentication and authorisation between the different microservices based on the Root of Trust of each component and managed by E-CORRIDOR's Trusted Service Manager TSM.
- The authorisations and the obligations of the entities based on the DSAs predefined and enforced through E-CORRIDOR's ISI and associated to each shared data object.
- The secure communication protocols.

6.1. Confidentiality

The Trusted Service Manager TSM stores secret keys and protect it from unauthorized access. In case of tampering, by design, the device becomes untrustworthy to the other devices and therefore it does not get unauthorized privileges.

The DSAs define and enforce the confidentiality of data, it also applies the anonymisation/pseudonymisation operations before sharing if requested in the DSA. This way we can control not only who can access the data, but also if they must apply some Data Manipulation Operations before a certain action to guarantee the confidentiality.

The confidentiality of the communication between the microservices is secured using TLS protocol.

6.2. Data Integrity

The TSM and the TrIP protect public information (public keys and certificates) from tampering by securing the authentication and the authorisation.

Thanks to the Root(s)-of-Trust technology, the integrity of the system is verifiable at each communication establishment, consequently, the devices integrity and e.

The DSAs defines the data manipulations operations obligations, the resulting object from these DMOs and from E-CORRIDOR analytics inherit the DSAs from the original data protected object (Also a specific DSA different than the one that would be inherited one could be defined) and the Secure Audit Manager in the CSI keeps digitally signed logs of the operations for integrity and transparency.

The secure communication protocols (namely the TLS) protect from attacks that have the goal of tampering the data.

6.3. Authentication

The authentication for the DSA Editor as well as for invoking the IAI API are managed by the Identity Manager in the Common Security Infrastructure, it is also used for logging the activity of the users of the two mentioned services.

For the eWallet, the authentication will be based on the Trusted Service Manager TSM which is a part E-CORRIDOR's Advanced Security Infrastructure (Task 8.5). This identity manager offers an additional layer of security compared to the state-of-art authentication protocols.

In fact, it establishes trusted communication between the entities interacting with the eWallet by verifying the certified Root(s) of Trust stored on the edge (VMs, PCs, IoT devices, Smartphone etc). This avoids the exchange and thus leakage of the vulnerable classic credentials (username and password), the Root of Trust also allows for verification that the device has not been tampered to give access to sensitive data such as the encryption keys stored within. Thanks to this Trust by design approach, the integrity and authenticity of the device is continuously verifiable.

6.4. Authorisation

The access to the data protected objects and the ability to read or edit them is defined and enforced by the DSAs, in certain cases the DSA enforces obligations (actions such as pseudonymisation, automatically sending an email etc) at or prior to some actions, this too is defined in the DSAs.

The subsystem responsible for managing DSAs is the DLI (DSA Lifecycle Infrastructure), its DSA editor is accessible via a webpage for the data prosumers, the security and the auditability of the DLI is ensured by the CSI (Common Security Infrastructure), The DSA Editor allows data prosumers to define DSAs using CNL (Controlled Natural Language), this way the data prosumers have an accessible way to ensure their respect for the data sharing regulation in a fool-proof manner and without having coding expertise. Also, it enables them to have a clear understanding of how their data is accessible to the other data prosumers and under what conditions. Finally, the data prosumers, thanks to the clear understanding and control over the data, are able to establish and communicate to the travellers the conditions of the data-sharing.

More information about the DLI is available in the deliverables D6.1 and D5.2.

7. **Deployment Model**

7.1. Hardware requirements

- Processors: 4 Intel/AMD 64-bit (8 cores, if provided as Virtual Core).
- Minimum RAM: 4GB.
- Hard Disk: 500 GB.
- OBD2 Reader.
- Car.

- Smartphone.
- Tablet Android 9.0+.

7.2. *Software requirements*

- Debian 10.
- Gitlab.
- MySQL.
- MongoDB.
- Laravel.
- Postman.
- WebSocket Python.
- PostgreSQL 10+.
- Java, Spring Boot Framework.
- Python3.
- Kubernetes Cloud.
- Libraries from The Trusted Computing Group for the Trusted Service Manager and Trusted Identity Provider implementation:
    - Tpm2-tss.
    - Tpm2-tools.
    - Tpm2-pkcs11.
    - Tpm2-abrmd.
    - Tpm2-tss-engine.
    - Tpm2-openssl.
    - Tpm2-simulator.
    - Libssh.

8. Requirements Matrix

The following matrix summarises how the Use Cases (and the associated User Stories) presented in Deliverable D3.1 can be implemented adopting the design presented in the previous sections.

Use case	User Story	Block design	Description
S2C-UC-01	S2C-US-01	S2C-BD-01	A traveller registers through a web form by submitting his/her personal data; this data is then stored in the Central E-CORRIDOR ISI in the eWallet. Mobility service providers fetch the traveller's profile data from the local ISI.
S2C-UC-02	S2C-US-02	S2C-BD-02	Mobility service providers share the trip

			requests and user metadata with the micro-subsidy analytics toolkit; the latter verifies the eligibility and accords the micro-subsidy to the trips with the further step of verification of trips.
S2C-UC-03	S2C-US-03	S2C-BD-03	The traveller uses a web browser or a client to access the Information Analytic Infrastructure (IAI) API to request the trip planning and carbon footprint analysis service; if the request succeeds, the IAI will return potential trip and carbon footprint information to the end-users.
S2C-UC-06	S2C-US-06 S2C-US-07	S2C-BD-05	Mobility service providers can request the IAI API for intrusion detection analytics. They will also receive notifications and alerts in case of cyberattacks or intrusion detection.
S2C-UC-07	S2C-US-08	S2C-BD-06	Mobility service providers can edit the traveller's profile on the central ISI and invoke privacy-aware interest-based sharing analytics without needing to trust the third party and without disclosing each data inputs.
S2C-UC-08	S2C-US-09	S2C-BD-07	Mobility service providers will share data about the driving behaviour through the ISI API, this way the data becomes accessible for the IAI; they can then

			invoke the IAI API in order to get a reporting on the results of the analytics.

Table 3: Mapping Use Cases and User Stories to architecture diagrams

9. Conclusion

This deliverable presented the design and architecture for the S2C (Smart City and Car Sharing) Pilot fulfilling the requirements set in the previous deliverable D3.1.

First, it explains the main concepts and the global pilot scenario. Then, the architecture of the pilot and the different interactions between the components developed for the pilot as well as the components belonging to the E-CORRIDOR Framework and tailored to this pilot use cases. Last, it presents the security and the deployment models.

This document will act as a reference for the next steps: implementation, deployment, tests, experimental validation, and evaluation.

10. References

Here we provide bibliography references used in the document:

[CLEM'2020] CLEM'. Requirements for the Smart city and Car Sharing Pilot (S2C). In E-CORRIDOR WP3, Deliverable D3.1, 2020.

[CNR2020] CNR. Sharing and Analytics Infrastructure Architecture. In E-CORRIDOR WP6, Deliverable D6.1, page 11, 2020.

[MPS2010] I. Matteucci, M. Petrocchi, and M. L. Sbodio. CNL4DSA: a Controlled Natural Language for Data Sharing Agreements. In SAC '10: Proceedings of the 2010 ACM Symposium on Applied Computing, pages 616–620, March 2010.

[CEA2020] CEA. Advanced Security Services Requirements and Architecture. In E-CORRIDOR WP8, Deliverable D8.1, page 29, 2020.

[HARDT2012] D. Hardt, Microsoft. The OAuth 2.0 Authorization Framework. In Internet Engineering Task Force (IETF), October 2012. https://datatracker.ietf.org/doc/html/rfc6749

[BHNPGMM2012] D. Balfanz, J. Hodges, M. Nystroem, A. Popov, Google Inc., Kings Mountain Systems, Microsoft Corp. The Token Binding Protocol Version 1.0. In Internet Engineering Task Force (IETF), October 2018. https://datatracker.ietf.org/doc/html/rfc8471

[GITHUB2021] Open Data Standards Directory, Transportation category: https://datastandards.directory/Transportation

[CNRS2020] CNR. Sharing and Analytics Infrastructure Architecture. In E-CORRIDOR WP6, Deliverable D6.1, pages 30 and 34-35, 2020.

[WBCSD2020] WBCSD. Enabling data-sharing: Emerging principles for transforming urban mobility. 2020.

[MAAS2018] MaaS Alliance. Data makes MaaS happen. November 2018.

[MAAS2017] MaaS Alliance. White paper: Guidelines & Recommendations to create the foundations for a thriving MaaS Ecosystem. September 2017.