



Mobility as a Service in a multimodal European cross-border Corridor (MyCorridor)

Deliverable 2.2

MyCorridor interoperable, open and seamless architecture and MyCorridor subsystems and modules specifications

Athanasios Salamanis, CERTH/ITI



MyCorridor	D2.2
Dissemination level:	PU
Work package:	WP2
Lead beneficiary:	Athanasios Salamanis, CERTH/ITI
Other beneficiaries involved:	Dionysios Kehagias (CERTH/ITI), Theodoros Ioakimidis (CERTH/ITI), Vasilis Mizaras (SWARCO Hellas), Giulia Dovinola (SWARCO MIZAR), Aimilia Bantouna (WINGS), Fanis Sklinos (VivaWallet), Filip Kvaček (CHAPS), Vaio Kakavas (AMCO), Nikos Kanakaris (UPAT), Nikos Karacapilidis (UPAT), Despina Meridou (WINGS), Ioannis Stenos (WINGS), Kostas Tsoumanis (WINGS), Xaris Kourogorgas (WINGS), Evagelia Tzifa (WINGS), Stefania Stavropoulou (WINGS), Panagiotis Demestichas (WINGS)
Date due to EC:	31/05/2019 (M24)
Date of Delivery to EC:	15/07/2019
Status (F: final; D: draft; RD: revised draft):	F
File Name:	MyCorridor_D2.2SystemArchitecture_Final.docx
Version:	Final

Document history

Version No.	Date	Details
0.1	10/05/2018	1 st draft version including the skeleton of the Deliverable and ToC with assignments for the partners involved
0.2	15/06/2018	2 nd draft version encompassing contribution of SWARCO for TM2.1
0.3	10/08/2018	3 rd draft version including the report of the system architecture design methodology and the system non-functional requirements
0.4	22/10/2018	4 th draft version including the report of the conceptual architecture, the logical architecture and the functional architecture
0.5	24/01/2019	5 th draft version including the system specifications, the review of the interoperability issues and the review of the cross-border security issues
0.6	14/02/2019	6 th draft version with refinements

Version No.	Date	Details
0.7	27/03/2019	7 th draft version including the updated Data Management Plan
0.8	08/05/2019	Refinement of the description of the TM2.0 and TM2.1 concepts
1.0	13/06/2019	Final draft version for Peer Reviewers
Final	15/07/2019	Final version submitted to the EC

Reviewers List

Name	Company
Gino Franco (External expert)	-
Laura Cocone (MyCorridor Quality Assurance Manager)	SWARCO MIZAR
Maria Gkemou	CERTH/HIT
Nikos Christodoulou	VivaWallet
Panos Marathokampitis	AMCO
Laura Franchi	TTS

This project is co-funded by the European Union under the Horizon 2020 Research and Innovation Programme. The content of this document reflects solely the views of its authors. The European Commission is not liable for any use that may be made of the information contained therein.

The members of the MyCorridor project Consortium shall have no liability for damages of any kind including, without limitation, direct, special, indirect, or consequential damages that may result from the use of these materials.

This deliverable is a draft document subject to revision until formal approval by the European Commission.

The MyCorridor project consortium consists of:

No.	Name	Short name	Country
1	NEWCASTLE UNIVERSITY	UNEW	UK
2	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	EL
3	OSBORNE CLARKE LLP	OC LLP	UK
4	WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES EPE	Wings ICT	EL
5	SWARCO MIZAR SRL	SWARCO MIZAR	IT
6	SWARCO HELLAS SYSTIMATA KYKLOFORIAS ANONYMI ETAIREIA	SWARCO Hellas	EL
7	CHAPS SPOL SRO	CHAPS	CZ
8	HACON INGENIEURGESELLSCHAFT MBH	HACON	DE
9	MAP TRAFFIC MANAGEMENT BV	MAPtm	NL
10	VIVA WALLET HOLDINGS - SOFTWARE DEVELOPMENT SA	VivaWallet	EL
11	AMCO OLOKLIROMENA SYSTIMATA YPSILIS TECHNOLOGIAS ANONYMI VIOMICHANIKI KAI EMPORIKI ETAIRIA	AMCO	EL
12	TOMTOM DEVELOPMENT GERMANY GMBH	TOMTOM	DE
13	ROMA SERVIZI PER LA MOBILITA SRL	RSM	IT
14	TTS Italia	TTS	IT
15	PANEPISTIMIO PATRON	UPAT	EL
16	IRU PROJECTS ASBL	IRU	BE
17	SALZBURG RESEARCH FORSCHUNGSGESELLSCHAFT M.B.H.	SFRG	AT

Table of Contents

Table of Contents	6
List of figures	11
List of tables	13
Abbreviation List	15
Executive Summary	18
1. Introduction	19
1.1 Purpose of the document.....	19
1.2 Intended audience	20
1.3 Interrelations	20
2 Towards TM2.1	21
2.1 TM2.0 Concept.....	21
2.2 TM2.0 Best practices.....	23
2.2.1 Social Traffic Management	23
2.2.2 C-ITS Verona (Italy).....	25
2.2.3 Mobimart	25
2.2.4 Regiomove	27
2.3 TM2.0: Enabler of MaaS	28
2.4 TM2.0 in MyCorridor - Evolution towards TM2.1	28
3 System Architecture Design Methodology	30
4 System Non-Functional Requirements	33
4.1 Look & Feel Requirements	34
4.2 Usability & Humanity Requirements	35
4.3 Performance & Scalability Requirements.....	40
4.4 Operational & Environmental Requirements	43
4.5 Maintainability & Support Requirements.....	44
4.6 Security & Data Privacy Requirements	46
4.7 Cultural Requirements	49
4.8 Legal Requirements	50
5 Conceptual Architecture.....	51

5.1	Architectural Styles.....	52
5.1.1	Layered architecture.....	52
5.1.2	Client-server architecture.....	53
5.1.3	Data-centered architecture	54
5.1.4	Data-flow architecture.....	55
5.1.5	Call-and-return architecture	56
5.1.6	Object-oriented architecture	57
5.1.7	Service-oriented architecture.....	57
5.1.8	Microservices architecture	58
5.2	Mapping requirements to architecture	59
6	Logical Architecture.....	64
6.1	Presentation Layer	64
6.1.1	Mobile Application	64
6.1.2	Web Application	65
6.2	Application Layer	68
6.2.1	Trip-Planner	68
6.2.2	Matchmaking Module	69
6.2.3	Multi-Criteria Search Module	70
6.2.4	MaaS Product Synthesis Module	71
6.2.5	Traveller Feedback Module	72
6.2.6	Big Data Management Module	73
6.2.7	Business Rules Implementer Module	74
6.2.8	Payment Module.....	75
6.3	Communication Layer - MaaS API.....	75
6.4	Data Layer	76
6.4.1	Travellers Data Repository.....	76
6.4.2	Services Data Repository	77
7	Functional Architecture	79
7.1	Traveller Use Cases.....	79
7.1.1	T1 - User Login/Register/Authentication.....	79
7.1.2	T2 - Static & semi-dynamic profiling.....	80
7.1.3	T3 - Personalized MaaS package configuration, purchase & redemption.....	81
7.1.4	T4 - Personalized Info Support (added value services, athletic, touristic, cultural, health push personalized notifications)	82
7.1.5	T5 - Modification/Cancelation.....	82
7.1.6	T6 - Traveller Feedback	83

7.1.7	T7 - Loyalty Scheme (encompassing incentivisation & rewarding)	83
7.2	Service Provider Use Cases	88
7.2.1	S1 - Service Provider Login	89
7.2.2	S2 - Service Registration	89
7.2.3	S3 - Service Provider Business Rules Editing	90
7.3	MaaS Aggregator Use Cases	93
7.3.1	B1 - Overall Business Rules Editing	93
7.3.2	B2 - Added Value Synthetic	93
7.4	Connected Use Cases	96
7.4.1	B3 - Clearance with the Traveller and the Service Providers (E-vouchers)	96
7.4.2	B4 - Mobility Token Issue and Redemption (Use/Validation)	96
7.4.3	B5 - Interactive Traffic Management Plan	97
8	System Specifications	98
8.1	Look & Feel Specifications	98
8.2	Usability & Humanity Specifications	99
8.3	Performance & Scalability Specifications	100
8.4	Operational & Environmental Specifications	102
8.5	Maintainability & Support Specifications	103
8.6	Security & Data Privacy Specifications	104
8.7	Cultural Specifications	105
8.8	Legal Specifications	106
8.9	MaaS Alliance Guidelines Compliance	106
9	Interoperability Issues	107
9.1	Service interoperability	107
9.1.1	Service interoperability barriers	107
9.1.2	Service interoperability solutions	108
9.2	Data interoperability	108
9.2.1	Data interoperability barriers	108
9.2.2	Generic data interoperability solutions	110
9.2.3	MaaS specific data interoperability solutions	110
10	Cross-Border Security Issues	112
10.1	Data encryption	113
10.2	Authorization and authentication	114
10.3	MaaS specific functionality	116
10.3.1	Data leakage/theft (packet sniffing)	117

10.3.2	Service behaviour manipulation	117
10.3.3	Service workflow manipulation.....	118
10.3.4	Pattern extraction.....	118
10.4	DoS attacks.....	119
10.5	Web services communication.....	119
11	Conclusions.....	120
	References.....	121
	Annex 1: Data Management Plan Update	126
1	Introduction	126
2	Data in MyCorridor	128
2.1	Mission related to Data Management	128
2.2	Clusters of data in MyCorridor	128
2.3	Dataset Description	128
3	FAIR data	129
4	Open Access approach.....	130
5	Key Data Management roles and assignment in MyCorridor	132
5.1	Key GDPR roles and assignment in MyCorridor.....	132
5.2	Data processed per entity & GDPR obligations	133
6	Data Security	137
7	Ethical aspects	139
7.1	Ethical and legal issues related to data sharing.....	139
7.2	Informed Consent	139
8	GDPR & Ethics related implications/obligations for MyCorridor	140
8.1	Research privilege and consent	140
8.1.1	Privacy by design	140
8.1.2	Data protection officer and GDPR roles and back-up mechanisms applied ...	141
8.1.3	Internal record keeping.....	141
9	Data Privacy Impact Assessment	141
9.1	Intro	142
9.2	Do I have to do a PIA?.....	142

9.3	Step 1: Identify the need for a DPIA	143
9.4	Step 2: Describe the processing	144
9.5	Step 3: Consultation process	161
9.6	Step 4: Assess necessity and proportionality	162
9.7	Step 5: Identify and assess risks	163
9.8	Step 6: Identify measures to reduce risk.....	165
9.9	Step 7: Sign off and record outcomes.....	166
Annex 2: MyCorridor GDPR compliant Informed Consent Form		167
Annex 3: Data processing - record keeping template		170

List of figures

Figure 1: TM2.0 membership [7]	22
Figure 2: The TM2.0 process [9]	23
Figure 3: Social Traffic Management approach	24
Figure 4: Example of collaboration between different traffic management operators to provide final information to MyCorridor app	30
Figure 5: Architecture Design Methodology of the MyCorridor platform	31
Figure 6: Layered architecture	53
Figure 7: An example of a system designed based on the client-server architecture pattern.	54
Figure 8: Data-centered architecture.....	55
Figure 9: Data-flow architecture.....	56
Figure 10: Main program/subprogram architecture	57
Figure 11: Object-oriented architecture	57
Figure 12: Service-oriented architecture	58
Figure 13: Typical microservices architecture pattern	59
Figure 14: MyCorridor conceptual architecture.....	61
Figure 15: Screens of the MyCorridor Android mobile application	65
Figure 16: SRT screen – Service provider registration.....	66
Figure 17: SRT screen – Service registration.....	66
Figure 18: SRT screen – Services view	67
Figure 19: MaaS Aggregator Dashboard home screen.....	68
Figure 20: UML component diagram of the Trip-Planner	69
Figure 21: UML Component diagram of the Matchmaking Module.....	70
Figure 22: UML component diagram of the Traveller Feedback Module	73
Figure 23: UML component diagram of the Big Data Management Module.....	74
Figure 24: UML component diagram of the Business Rules Implementer Module	75

Figure 25: UML component diagram of the MaaS API	76
Figure 26: UML entity relationship (ER) diagram of the Travellers Data Repository	78
Figure 27: UML entity relationship (ER) diagram of the Services Data Repository	78
Figure 28: UML sequence diagram of the traveller registration and login process	80
Figure 29: UML sequence diagram of the static and semi-dynamic process.....	81
Figure 30: UML sequence diagram of the configuration of the personalized MaaS package coupled with trip planning	84
Figure 31: UML sequence diagram of the configuration of personalized MaaS packages with multicriteria search and the ready to use MaaS packages.....	85
Figure 32: UML sequence diagram of the MaaS package modification/cancellation process.....	86
Figure 33: UML sequence diagram of the feedback provision process.....	87
Figure 34: UML sequence diagram of the process of viewing the platform's terms and conditions and the traveller's loyalty points	88
Figure 35: UML sequence diagram of the service provider's registration and log in processes.....	89
Figure 36: UML sequence diagram of the service registration process.....	90
Figure 37: UML sequence diagram of the service business rules editing process	92
Figure 38: UML sequence diagram of the overall business rules editing process.....	94
Figure 39: UML sequence diagram of the service synthesis process.....	95
Figure 40: UML sequence diagram of the checkout process	97
Figure 41: Traffic management services environment with the Traffic Management Services Aggregator and the MyCorridor platform	98
Figure 42: ENISA's generic model of cross-border authentication	115

List of tables

Table 1: Mobimart SWOT Analysis.....	26
Table 2: Look & Feel Requirements – LFR1	34
Table 3: Look & Feel Requirements – LRF2	35
Table 4: Usability & Humanity Requirements – UHR1	36
Table 5: Usability & Humanity Requirements – UHR2	37
Table 6: Usability & Humanity Requirements – UHR3	37
Table 7: Usability & Humanity Requirements – UHR4	38
Table 8: Usability & Humanity Requirements – UHR5	39
Table 9: Performance & Scalability Requirements – PSR1	40
Table 10: Performance & Scalability Requirements – PSR2.....	41
Table 11: Performance & Scalability Requirements – PSR3.....	42
Table 12: Operational & Environmental Requirements – OER1.....	43
Table 13: Maintainability & Support Requirements – MSR1	44
Table 14: Maintainability & Support Requirements – MSR2	45
Table 15: Security & Data Privacy Requirements – SDPR1	46
Table 16: Security & Data Privacy Requirements – SDPR2	47
Table 17: Security & Data Privacy Requirements – SDPR3	48
Table 18: Cultural Requirements – CR1	49
Table 19: Legal Requirements – LR1.....	50
Table 20: Matching of the define system architecture components with the use cases.....	61
Table 21: Look & Feel Specifications - LFS	98
Table 22: Usability & Humanity Specifications - UHS	99
Table 23: Performance & Scalability Specifications - PSS	101
Table 24: Operational & Environmental Specifications - OES	102
Table 25: Maintainability & Support Specifications - MSS.....	103

Table 26: Security & Data Privacy Specifications - SDPS	104
Table 27: Cultural Specifications - CS.....	106
Table 28: Legal Specifications - LS	106
Table 29: MyCorridor MaaS data models	111
Table 30. Dataset Description template.....	129

Abbreviation List

Abbreviation	Definition
API	Application Programming Interface
CAD	Computer-Aided Design
CCISS	Centro di Coordinamento Informazioni sulla Sicurezza Stradale
C-ITS	Cooperative Intelligent Transport Systems
CPU	Central Processing Unit
CR	Cultural Requirements
CS	Cultural Specifications
DMP	Data Management Plan
DoA	Description of Action
DOS	Denial-of-Service
DPI	Dots Per Inch
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ESB	Enterprise Service Bus
EC	European Commission
EFRE	European Fund for Regional development
EMP	Ethics Management Panel
ER	Entity Relationship
EU	European Union
FAIR	Findable Accessible Interoperable Reusable
FCD	Floating Car Data
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GBFS	General Bikeshare Feed Specification
GTFS	General Transit Feed Specification
GTFS-RT	General Transit Feed Specification - Real Time
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
ICT	Information Communication Technology
ICMP	Internet Control Message Protocol
IDE	Integrated Development Environment
IMEI	International Mobile Equipment Identity
IO	Input/Output
IT	Information Technology
ITS	Intelligent Transport System
Java EE	Java Enterprise Edition
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
KVV	Karlsruhe Verkehrsverbund
LDM	Local Dynamic Map
LER	Local Ethics Representative
LFR	Look & Feel Requirements
LFS	Look & Feel Specifications

Abbreviation	Definition
LGPL	Lesser General Public License
LR	Legal Requirements
LS	Legal Specifications
MaaS	Mobility as a Service
MSR	Maintainability & Support Requirements
MSS	Maintainability & Support Specifications
NABSA	North American Bike Share Association
NeTEx	Network Timetable Exchange
OER	Operational & Environmental Requirements
OES	Operational & Environmental Specifications
ORDP	Open Research Data Pilot
OTP	OpenTripPlanner
OWL	Web Ontology Language
PDF	Portable Document Format
PND	Personal Navigation Assistant
POI	Point of Interest
PSR	Performance & Scalability Requirements
PSS	Performance & Scalability Specifications
PT	Public Transport
PVD	Probe Vehicle Data
QoS	Quality of Service
RAM	Random Access Memory
RDF	Resource Description Framework
REST	Representational State Transfer
RMI	Remote Method Invocation
RMV	Rhein-Main-Verkehrsverbund
ROI	Return Of Investment
SASS	Syntactically Awesome Style Sheets
SDPR	Security & Data Privacy Requirements
SDPS	Security & Data Privacy Specifications
SLA	Service Level Agreement
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
Spring MVC	Spring Model-View-Controller
SP	Service Provider(s)
SPOF	Single Point Of Failure
SRT	Service Registration Tool
STM	Social Traffic Management
SWOT	Strengths Weaknesses Opportunities Threats
TM	Traffic Management
TM2.0	Traffic Management 2.0
TM2.1	Traffic Management 2.1
TMC	Traffic Management Control
TMS	Traffic Management System
UHR	Usability & Humanity Requirements

Abbreviation	Definition
UHS	Usability & Humanity Specifications
UI	User Interface
UML	Unified Modeling Language
UTF	Unicode Transformation Format
UTC	Universal Time Coordinated
VAO	Verkehrsauskunft Österreich
VBB	Verkehrsverbund Berlin-Brandenburg
VBN	Verkehrsverbund Bremen/Niedersachsen
VMS	Variable Message Signs
WP	Work Package
WSGI	Web Server Gateway Interface
W3C	World Wide Web Consortium
XML	Extensible Markup Language
3G	Third Generation Wireless Mobile Telecommunications
4G	Fourth Generation Wireless Mobile Telecommunications

Executive Summary

The current deliverable (D2.2) has been prepared in the context of WP2: “Open Cloud System Architecture” of MyCorridor project. The main objective of WP2 is to design an interoperable Open Cloud System Architecture for creating and growing an open ecosystem that acts as an enabler for a large scale implementation of MaaS services. The main challenges and objectives within this WP are:

- To integrate a big amount of data sources and services from different categories of stakeholders, while aiming at a fully interactive TM2.1.
- To obtain a detailed understanding of the envisaged cross-sectorial business scenarios.
- To enable seamless/roaming operability of MyCorridor services.
- To address the security risks of the electronic authentication in cross-border MaaS solutions.
- To provide a cloud-based platform for the delivery of orchestrated services to the users.
- To provide tools for the developer community, in order to enable an easy connection to MyCorridor platform.
- To provide interoperability with third-party platforms.
- To facilitate the exploitation of data according to the defined management plan and procedures, allowing MyCorridor to reach its full potential without imposing privacy risks.
- To address the general technological and systemic big data challenges that concern the entire MaaS value chain.
- To perform risk assessment on key technical, behavioral, legal and business related risks, suggesting also mitigation strategies for the most critical ones.

The activities of WP2 have been designed and executed in a way so as to respond to all the aforementioned objectives. In particular, the activity A2.1: “Towards TM2.1” explores how the TM2.1 concept can be integrated into the overall MyCorridor system architecture in order for the MyCorridor platform to provide enhanced traffic management services. Then, in the activity A2.2: “System architecture and technical specification” the overall system architecture of the MyCorridor platform is designed and implemented. This activity includes the definition of the overall non-functional requirements of the MyCorridor system, the design of all system components and their organization using a well-known and widely used architectural style, the definition of the interactions of the system components that will facilitate the implementation of the use cases defined in the deliverable D2.2, and the definition of the system specifications derived from the process of meeting the defined system non-functional requirements. Additionally, the activity A2.3: “Interoperability and cross-border security issues” refers to the several types of interoperability issues (e.g. function, data, business, payment, etc.) and the cross-border security issues that may arise during the operation of the MyCorridor MaaS platform, and how the designed system architecture handles them. Moreover, a full risk analysis of the system operation is conducted in the context of the activity A2.4: “Risk Assessment”. Finally, the activity A2.5: “Data management, reliability and QoS” provides a comprehensive data management plan for all the data entities involved in the operation of the MyCorridor platform, along with the definition of minimum Quality of Service (QoS) indicators for successfully overall service provision.

The deliverable D2.2: “MyCorridor interoperable, open and seamless architecture and MyCorridor subsystems and modules specifications” has consolidated the outcomes of activities A2.1-A2.3 and also the outcome of activity A2.5. Although the outcome of activity A2.5 has been reported in the deliverable D2.1: “Data management plan”, it is updated in this document. Finally, the outcome of activity A2.4 will be reported in a separate deliverable, namely D2.3: “Risk Analysis” (M30).

The deliverable is organized as follows. **Section 1** introduces the purpose of this document, the anticipated interrelations and the target audience. **Section 2** presents the Traffic Management 2.0

(TM2.0) concept, how it can be used as an enabler of MaaS, and how it is anticipated to work within the context of MyCorridor (i.e. evolution towards Traffic Management 2.1 (TM2.1)). **Section 3** describes the methodology followed for the design and implementation of the overall system architecture. **Section 4** presents the overall system non-functional requirements, namely those describing how the MyCorridor systems should be. **Section 5** describes the conceptual architecture of the system by introducing the several system architecture components, and how they are organized based on a specific architectural style. Then, **Section 6** briefly analyzes the functionality and characteristics of the various components (i.e. logical architecture), while **Section 7** describes how the components interact with each other in order to implement the use cases defined in the deliverable D1.1 (i.e. functional architecture). Afterward, **Section 8** presents the several technical specifications of the overall MyCorridor system derived by the necessity of meeting the non-functional requirements presented in Section 4. Then, **Section 8** and **Section 9** describe the several interoperability and cross-border security issues, respectively, that can occur during the operation of a MaaS platform, and how these issues are handled by design in the MyCorridor platform. **Section 10** concludes this deliverable by summarizing the main elements of the presented system architecture. Finally, **Annex 1** includes the updated data management plan, while **Annex 2** and **Annex 3** present the MyCorridor GDPR compliant Informed Consent Form and the Data processing - record keeping template, respectively.

1. Introduction

1.1 Purpose of the document

This deliverable is prepared in the context of WP2: “Open Cloud System Architecture” of MyCorridor project and describes in detail all elements of the system architecture. In particular, the document initially introduces the concept of Traffic Management 2.0 (TM2.0) by describing its main functionalities and how it can act as an enabler of MaaS. Also, it describes how this concept is considered by the system architecture design process of the MyCorridor platform, leading to its evolution towards Traffic Management 2.1 (TM2.1). Then, the methodology used for the design of the system architecture is presented, by stating its main steps, like the transformation of the use cases defined in the deliverable D1.1 into the system conceptual architecture. After that, the main steps of the system architecture design process, namely the conceptual architecture that defines the several system components and how they are organized into an integrated system, the logical architecture that describes the characteristics and the functionalities of the several system components, the functional architecture that describe the way in which the several system components interact with each other in order to implement the use cases, and the physical architecture that includes the several technical requirements of the system and the corresponding specifications, are described in detail. The document is completed with the presentation of the main interoperability and security issues that may arise during the operation of a MaaS platform, and how these issues are handled within the context of MyCorridor.

The development of the system architecture follows the principles of the Unified Modelling Language (UML) [1] system architecture methodology. Although UML cannot be considered as a formal software development methodology in the strict sense of the term “methodology”, it provides a set of tools and techniques that help software architects to design and implement the architecture of large scale software projects, in a formal and easily understandable way. Based on the UML methodology, initially, the several system components are defined, based on the identified use cases, and organized using a specific architectural style (i.e. conceptual architecture). Then, the characteristics and the functionalities of the defined system components are presented defining the system logical architecture, and after that, the system functional architecture describes the way in which the defined components interact with each

other in order to implement the use cases. In the final step, i.e. physical architecture, the several technical requirements and the corresponding specifications of the system are documented using a formal specifications template, i.e. the Volere Requirements Specifications Template [2].

In the deliverable D1.1 it is documented that, according to MyCorridor ecosystem definition, the identified users of the system are namely the Government/Authorities, the Cities/Regions, the Mobility/MaaS operator/aggregator/Issuer, the Transportation Service Provider/Operator (supplier of mobility products), the Infomobility, added value and Mobile Service / Technology Providers and the Travellers. In the context of the deliverable D2.2, the Transportation Service Providers/Operators and the Infomobility, added value and Mobile Service/Technology Providers are referred to as Service Providers, while for the rest of the users the nomenclature of deliverable D1.1 is used. Throughout the document, all the system functions are presented in correspondence with the users of the system.

The outcome of this deliverable, namely the overall system architecture of the MyCorridor platform, is the basis for the development of the whole MyCorridor platform whose detailed description will be presented in the deliverable D3.1.

1.2 Intended audience

The nature of this deliverable is public, meaning that it will be finally (upon approval by the EC) available through the web site of the project ("Library" section). Due to its various content layers, the interested audience may vary respectively, as follows:

- Internally to the project:
 - MyCorridor developers, encompassing all those dealing with the specifications and implementation work of the one-stop-shop (WP2 & WP3), the services to be integrated (WP4) and the personalisation work of WP5, for whom the competitive market and the definition of the Use Cases and their justification from the stakeholders' needs and priorities side are crucial for their work.
 - MyCorridor partners dealing with the business modelling and exploitation aspects of the project (in the context of WP7 and WP8) that need to take into account the priorities and restrictions imposed by the different stakeholders, as a basis for their respective work, as well as the competitive market and the approaches adopted in similar schemes.
 - MyCorridor partners dealing with demonstration and testing (in the context of WP6).
- Externally to the project:
 - Researchers working in transport, mobility, Information Communication Technology (ICT) and Intelligent Transport Systems (ITS) sectors (and combination of them) who seek to find MaaS specific information about user/stakeholder needs and priorities, overview of the market, strategic priorities and policies, key MaaS success and failure factors and discussion on expected impact.
 - Developers that are keen on understanding the way of MaaS operation and MaaS related solutions.
 - Technology, content and service providers as well as transport operators that are potentially interested in joining MyCorridor one-stop-shop and benefit from a proof of concept of their service/technology/content operating in a MaaS context.
 - TM2.0 Consortium, as deployment of example TM2.0 services will take place in the project.

1.3 Interrelations

The main objective of this deliverable is to present in detail the overall open and seamless architecture of the MyCorridor platform and the corresponding system specifications. This architecture was derived

based on the goal to implement, as much as possible, the use cases defined in the deliverable D1.1. Therefore, there is a clear and direct connection between the work presented in this deliverable, and the one took place in WP1. Additionally, the system architecture is the basis for the actual development of the MyCorridor service delivery platform, which is the subject of work in WP3. Moreover, the work presented here can be considered as enabler of the work that will be conducted in the context of WP4, WP5 and WP6 that refer to the services incorporated into the platform, the design and implementation of the user interfaces, and the pilot realization, respectively. Based on the above, the work reported in this deliverable is the cornerstone for the overall development and successful deployment of the MyCorridor MaaS platform.

2 Towards TM2.1

The Mobility as a Service (MaaS) concept can be defined as the ability of transport products/services to allow travellers for continuous travelling within a geographic region independently of the transport mode, while offering integrated payment options. Therefore, MaaS can be considered as a tool for building sustainable communities across three pillars: environment, quality of life and social welfare.

However, MaaS schemes frequently omit smooth transition from private vehicle ownership towards car sharing/usage. Moreover, the existing MaaS schemes focus more on the integration of services for travellers, and less on the optimization of mobility operations through traffic and multimodal transport management. This logical gap can be filled by the concept of Traffic Management 2.0 (TM2.0).

TM2.0 builds upon the deployment of connected vehicles and travellers in order to achieve convergence of mobility services and traffic management, combining actions of the individual travellers with the collective mobility objectives. The traffic management industry offers well-proven Intelligent Transport System (ITS) solutions for improving traffic flow and safety using a large diversity of sensors along the roads. Traditional traffic data collection, monitoring and control represent mature technologies with clear business models. Still, an efficient traffic management integration into multimodal MaaS has not been attempted.

The recent growth of cities is facing some criticalities, which are greatly affecting daily urban mobility. The car density with respect to the surface of the city, the urban structure that prevents radical viability transformation, the tourism flow (although usually concentrated in specific periods of the year), the inefficient use of the vehicles, and the daily people flows from the suburbs to downtown and vice versa, are some of the factors that contribute to the rise of environmental, mobility and social costs which are becoming difficult to sustain for today's cities. Cities, in their attempt to address these issues, are beginning to outline clear targets across the aforementioned three pillars of sustainability.

Finally, an interesting example of a TM2.0 best practice is *Social Traffic Management (STM)* [3]. Social Traffic Management builds on a personalized traffic information service and traffic management platform, that is based on mainstream social media, and aims to best match demand and supply with the intend to improve travellers' comfort and ease road congestion. However, the combination of TM2.0 and multimodal MaaS is still an open issue, and therefore, an effort has been made to address it within the framework of the MyCorridor project.

2.1 TM2.0 Concept

The TM2.0 platform was launched in 2011 by SWARCO [4] and TomTom [5] and formally established in 2014 under the ERTICO [6] umbrella of activities. It now comprises 40 members from all ITS sectors (from

public authorities to service providers) to focus on new solutions for advanced interactive traffic management.

Members



Figure 1: TM2.0 membership [7]

The objective of TM2.0 is to provide a discussion forum on interactive traffic management for stakeholders in the entire traffic management procedure value chain. Basic aims are to [8]:

- Use a set of common interfaces, principles and business models to facilitate the exchange of data between vehicles and Traffic Management and Control (TMC).
- Improve entire value chain for consistent traffic Management and mobility services with the aim to avoid conflicting guidance information on the road and in-vehicles.

The future of traffic management is to build upon deployment of connected vehicles and travellers in order to [8]:

- Achieve convergence of mobility services and traffic management.
- Create synergies between actions of the individual travellers with the collective mobility objectives.
- Bridge the innovative developments in the vehicle and in the traffic management.
- Give value to the legacy and create new business opportunities.

TM2.0 stands for a new proven collaborative concept for Traffic Management and Control (TMC), in which the travellers and goods, by using new technologies and sensors, become entirely part of the data supply chain. It offers great new opportunities for traffic management and control making it, on one side, cheaper and more efficient for the road operators, and, on the other side, more custom, friendly and acceptable for the users. This is accomplished by combining effectively data collected by the infrastructure and from the mobility services in the vehicles and smartphones.

The TM2.0 process is organized according to the following steps:

- **Collect data** from all available sources feeding into the traffic management.
- Data is fed into the statistics and modelling exercises performed by the public authorities when managing traffic (**Data Processing**).
- **Implementation** of traffic management under the concept of TM2.0 involves all means of information transmitters working towards informing and guiding the driver. All the actors involved in traffic information provision show the same data and follow the coherence principle.

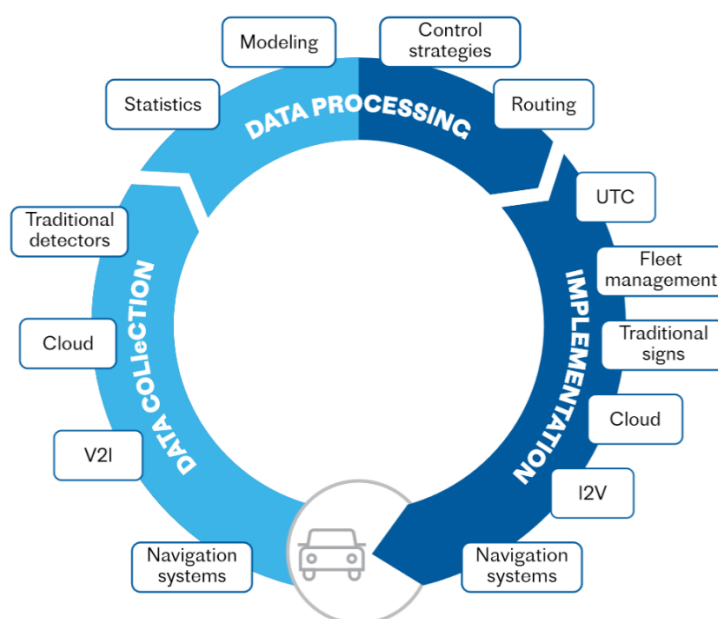


Figure 2: The TM2.0 process [9]

Modern navigation systems use traffic information to provide individual route advice to drivers. However, information related to traffic circulation strategies, traffic regulations or prioritized routes put in place by the TMCs, are not being fed to these systems. This is especially the case when extraordinary events are in place (planned or unplanned), such as important sport or cultural events, demonstrations, constructions or public transport strikes, but also when specific plans need to be enforced, e.g. in cases of smog warnings, evacuation alerts, or low-emission zones. Therefore, according to the vision of TM2.0, the future of traffic management is to combine intelligently the individual driver objectives (individual users' optimization) together with network wide management strategies (system optimization and equilibrium) in a win-win scenario.

2.2 TM2.0 Best practices

2.2.1 Social Traffic Management

As mentioned above, Social Traffic Management (STM) is an example of a TM2.0 best practice which builds on a personalized traffic information service and traffic management platform, based on mainstream social media, that aims to best match demand and supply and improve travellers' comfort and ease road congestion. One of the tools of the Social Traffic Management approach is to actively connect to target groups, often through existing social media communities and platforms, which are generally related to a specific location or event. This approach was successfully applied to the ArenaPoort area in Amsterdam, which includes a football stadium and several concert venues. In particular, by acting as a service provider, STM pro-actively informed the visitors about travel options, traffic flow,

accessibility, timetables, parking options, etc. Reversely, visitors were able to contact the STM service centre by using their preferred social media channel (e.g. WhatsApp, Facebook Messenger, Twitter, etc.) to ask for specific information related to their mobility needs [3]. No additional application download is ever required. An important added value of the traffic centre is that detailed knowledge of the traffic system of the area is available and continuously monitored in real-time. This allows to immediately anticipate to any type of delay or disruption and provide pre- and on-trip information to travellers. This goes for a range of scenarios, including public transport options considering occupancy, preferred walking routes, dynamic Kiss&Ride locations and approach routes, parking recommendations considering accessibility next to availability, etc.

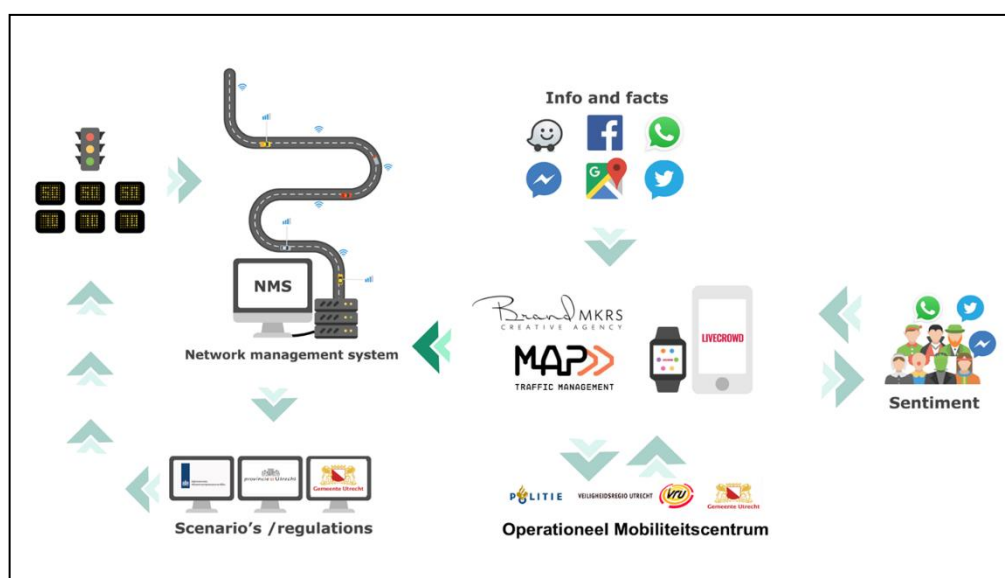


Figure 3: Social Traffic Management approach

In 2017, during a concert series on three consecutive nights, a little more than 64.000 unique visitors were reached by the aforementioned system, mainly through WhatsApp, Facebook, for one-on-one communication and Twitter for common messaging towards a larger audience [3]. The feedback received was very positive. The unique service of STM at large events helped people who were unfamiliar with the area around the event. Most questions were routing and traffic related, whether by car or public transport. After the event, the subject of the STM channel shifted back to routing and traffic information. People were asking for information on issues like the quickest route home, where to pay their parking ticket, what to do when a ticket is lost or the ticketing machine is not working correctly, etc. Finally, STM was also targeted by partners and friends who were coming to the venue to pick up relatives.

In March 2017, STM was deployed as the primary communication tool for road works that had a great impact on traffic during one specific weekend [3]. The original plan was to deploy STM for the duration of the road works, i.e. from Friday until the next Monday morning. Accordingly, the road operator communicated the availability of STM during these 3 days one week before, with the strict notice that it would be available from Friday. However, from the moment the notice was published questions were coming in. Most of these questions were coming from people planning their trip to Schiphol Airport and who were in need of clarification and/or assurance of the impact of the road works on their trip. Some of the questions were coming from people in need of more local route information, not even passing the road works but anticipating the effect on the local road network. Also, a group of people were interested in the road layout after the road works which was passing from 3 to 6 lanes through some complex interchanges at certain points. By providing up-to-date and personal travel information before and during the road works, STM was able to help users avoid traffic and delays. During this STM deployment, it also

became apparent that the STM community was very much engaged with the information given via Twitter, and it distributed even more information, resulting in engagement rates of well over 15% on Twitter.

The evaluation of the above STM deployments showed that most users are pleased to get a personal and quick response to any question they make. Moreover, it became evident that travellers with a higher rated user experience are more likely to comply to travel recommendations. This offers a huge potential to traffic management, and adding more traffic management orientated features is expected to further strengthen the effects of STM on traffic networks.

2.2.2 C-ITS Verona (Italy)

Another example of a TM2.0 best practice is C-ITS (Cooperative Intelligent Transport Systems) in Verona (Italy), which has the purpose of optimize traffic flows and reduce road transport induced CO2 emissions within the entire area of the city. The C-ITS systems deployed, with technological support of SWARCO and Telecom Italia, include:

- Traffic Light Assistant (broadcast t of SPAT/MAP messages at intersections)
- Real Time Traffic Information (broadcast of DENM messages)
- Road Works Warning (broadcast of DENM messages)
- Public Transport Prioritization

The services rely on ETSI G5 and LTE telecommunications technologies, while data and information exchange is realized with the use of standardized C-ITS messages (SPAT/MAP, DENM, CAM) and the DATEX II [10] protocol.

Results currently available indicate that at technical performance level the Traffic Light Assistant service is active on all intersections in the city, both centralized and isolated. In-vehicle information reaches the driver with a delay of < 3s and event information is being transmitted in-vehicle through DENM messages. C-ITS Verona is an enabler of the TM2.0 concept, as it supports the direct involvement of the vehicle in the Traffic Management Loop. The trade-off between information regarding the traffic lights represents a basic exchange of traffic management plans.

As far as impacts are concerned, safety levels are increasing due to more and more fluid and better distributed journeys along the network and thus the risk of accidents becomes lower, efficiency is improved as all services used allow easier travel. Environmental pollution is reduced because reducing Stops/Starts contributes to reducing CO2 emissions, while at socio-economic level better mobility management will contribute to improving the quality of life. At the level of user acceptance, the results are positive, especially with regard to professional drivers.

2.2.3 Mobimart

Mobimart is a “cross-border project” of the “Interreg” [11] EU initiative started in 2014. Mobimart partners are eleven Italian and French Public Authorities situated in the coastal Mediterranean area. The objective of Mobimart is to consider the transport services as “journeys” from origin to destination, independently from the transport mode and the morphological characteristics of the territories.

It involves two types of partners, or “nodes”:

- Regional transport offices – Tuscany (IT), Sardinia (IT), Liguria (IT), Provence-Alpes-Côte d'Azur – PACA (FR)

- Other public transport offices – North-Thyrrhenian Sea Port Authority – AdSP MTS (IT), Sardinian Sea Port Authority – AdSP MS (IT), Province of Livorno (IT), Province of Sassari (IT), Municipality of Pisa (IT) and Municipality of Genoa (IT)

MaaS opportunities should be something suitable and convenient for the environment and for users. Mobimart, in MaaS concepts, should represent a cheaper alternative to the car ownership. Travelling by bus reduces city congestion and people stress, so users should get economic benefits by travelling using public transport. In this way, Mobimart will help commuters using public transport.

The output of Mobimart project will be a digital platform that will act as a matchmaker between user preferences and available services. It will provide an integrated and intermodal travel-plan. Disposing of all the public transports open data, including the real-time state of the resources, is the fundamental precondition for implementing a MaaS offer atop. Public transport offices will collect mobility data from local public and private transport operators, including the real-time status of all resources. They will set up a tracking option in order to follow the status of the digital service (i.e. “Active”, “Down”, “In maintenance” etc.). Data will be sent to the regional transport office which the organization belongs to. If not in the correct standard format, regional transport offices will convert data in a common format, such as GTFS (General Transit Feed Specification), in order to keep a mutual platform that will collect all the transport data from all the eleven partners.

Mobimart project leader is the Tuscany Regional Authority, which has always been committed in innovation and sustainable mobility at national and European levels. All the transport data from all the Tuscan transport offices is full available on the “datiToscana” web platform [12]. The standard used is GTFS. The Region has set up the Regional transport observatory [13], a full open-data repository with details about road graphs, traffic sensors, free-parking availability and real time information about traffic and real-time transport status. The “Firenze – Pisa – Livorno Highway” has a DATEX II node and a traffic control centre which can monitor the real-time traffic status. The Highway control centre is connected with CCISS (Centro di Coordinamento Informazioni sulla Sicurezza Stradale, the Italian Highway TM agency) which provides traffic information at any time.

Currently CNIT, on behalf of AdSP MTS, is involved in the implementation of a service-oriented architecture (SOA) at the port of Livorno (encompassing and integrating information into the Port Communicating and Port Monitoring platforms) that could be used in order to retrieve useful information regarding both sea side (ETA, ETD, Passengers Forecast, etc.) and passengers’ mobility via C-ITS. CNIT could provide either a high integration level with the needed ICT component or the proper level of connectivity. In Mobimart, it will be possible to include C-ITS and Traffic Management information (using DATEX II standard) in order to increment road safety. It is also possible to calculate routes upon the occurrence of dangerous situations like accidents and roadworks. CNIT is actually developing vehicular communication in the perspective of “smart cities”.

It’s important to focus on all the positive and negative, internal and external facts which may impact Mobimart and its outputs. SWOT (Strengths Weaknesses Opportunities Threats) analysis [14] can help us to examine them.

Table 1: Mobimart SWOT Analysis

	Helpful	Harmful
Internal origin	STRENGTHS	WEAKNESSES
	Mutual platform;	Sometimes data transport is not up-to-date;

	Helpful	Harmful
	Standard common open data format.	Weak availability of open real-time data information.
External origin	OPPORTUNITIES Transport data and travel-plans will be useful to offer “one-ticket” services.	THREATS Strong competition among MaaS companies; Changes in data-privacy legal aspects.

Mobimart represents the first step for building a MaaS platform: data from these five regions will match together and people will obtain an integrated travel-plan, preliminary requirement to offer a single-ticket solution. There, you can find information about trains, buses and ferries with details concerning the status of the service. Seaports will become similar to airports: information about the real-time status of the service will fill “variable message panels”, which are so useful to the passengers. Integrated service are the fundamentals of MaaS: it’s necessary to re-engineer all the public transport timetables, in order to offer an available integrated service. E.g.: passengers who have just arrived in a seaport should take a bus or a train in a few minutes, car-rental and bike-sharing information will be integrated in the platform.

Mobimart will offer a mobile-friendly service too: user will be able to download the iOS/Android apps which will be useful to send service feedbacks too. MaaS puts users at the core of transport services: they will become part of the info-mobility system.

It’s impossible to ensure a MaaS service provision without reliable data. Mobimart will provide an integrated platform which will collect anonymized and aggregated data. Public governments have to monitor how data are processed and anonymized according to the European Union’s (EU) new data privacy regulation GDPR (General Data Protection Regulation).

Best practices have to be shared between partners, in order to reach innovative MaaS services based on high-quality and complete data. Mobimart platform will be an OTP (Open Trip Planner) service, so it will work on OpenStreetMap layers. Data has to be open and fully available without any restrictions. Standardizing data will be the first step for implementing a future “single-ticket” solution. Almost all the transport companies are already sharing their data and information using GTFS structures. That will not represent an obstacle for MaaS Alliance’s [15] outputs, because it will ensure a complete transparency and it will be possible to convert data in other eligible formats, such as NeTEx (Network Timetable Exchange). Sharing best-practices is strictly important because passengers should be able to switch between different services. With single-ticketing, if the service is unavailable, people should take another mean of transport or vehicle without purchasing additional tickets.

2.2.4 Regiomove

The three-year RegioMOVE [16] research project has been commissioned by the Karlsruhe Verkehrsverbund (KVV) and funded by the German state of Baden-Wuerttemberg and the European Fund for Regional development (EFRE), with a budget of around €5m. RegioMOVE will develop a new mobility concept that combines different mobility services to ensure easier access to transport. The project aims to lay the foundation for the development of a multimodal network using Mobility on Demand-driven transport services.

Actual transport demand from end users becomes the pivotal issue when developing appropriate mobility schemes, so as well as the traditional modes of transport, such as walking, cycling and motorized private

and public transport, MaaS concepts will also include car- and bike-sharing, as well as ride-pooling services.

To obtain the operational data on vehicle fleets required for the implementation of innovative and climate-friendly service concepts, system- and service-related specifications, such as maximum waiting times, detours and pick-up/drop-off concepts, will be collated, and a transport model will be used to simulate these concepts, including intermodal routes.

2.3 TM2.0: Enabler of MaaS

As described in previous works [17], the scope of TM2.0 includes business models, deployment steps, public-private cooperation concepts, organisational architecture, and data exchange principles related to the interaction of the following services:

- Mobility services (individual routing, individual information and advice, high quality real time and reliable services, interfaces to other modes of transport).
- Road traffic management (traffic management and control strategies, collective routing, adaptive and dynamic traffic control, traffic management procedures, interfaces to other modes of transport).
- Data collection (privacy, security and data collection, journalistic, static and dynamic data, probing, dynamic location referencing, update of the Local Dynamic Map (LDM)).
- Legacy and evolution of current systems (integration of traditional and Probe Vehicle Data (PVD)).

The traffic management industry offers well-proven ITS solutions for improving traffic flow and safety using a large diversity of sensors along the roads. Traditional traffic data collection and monitoring (e.g. flow, speed, acceleration, floating car data (FCD), etc.) is a mature technology with a clear business model. Nevertheless, today, traffic management plans are not part of the dynamic traffic information delivered to the vehicles. At the same time, the individual vehicle behaviour (intended, in relation to the route guidance system plans) is not made available to the traffic management system.

An efficient TMC integration into multimodal MaaS has not been attempted yet. The concept of Traffic Management 2.0 builds upon the deployment of connected vehicles and travellers in order to achieve convergence of mobility services and traffic management, combining actions of the individual travellers with the collective mobility objectives. This way, TM2.0 connects the innovative developments in the vehicle and on the road, while improving the value to the legacy systems and, at the same time, creating new business opportunities. For example, a new business paradigm shall be deployed in which TM becomes part of the multimodal service offering of a MaaS product. The TM2.0 approach is based on the view that integration produces amplified impact through the enabled synergies.

2.4 TM2.0 in MyCorridor - Evolution towards TM2.1

Nowadays, MaaS is one of the most important trend in mobility industry. However, some gaps can be identified, that is:

- There is a tendency to mainly create local **MaaS communities at city level** with agreements among different mobility providers (e.g. public transport, bike and car sharing, taxi, train, etc.), whose services are integrated in a single local platform or application.
- **Actual interoperability** among different “city” platforms is often **missing**.
- Smooth **transition from vehicle ownership to vehicle usership** is often omitted.

- Most of the existing MaaS schemes focus mainly on the integration of services for travellers, and less on the optimization of mobility operations through traffic and multimodal transport management.

MyCorridor aims to extend TM2.0 at its borders by providing a solution that incorporates multimodal, seamless, flexible, reliable, user-friendly, all inclusive, price-worthy and environmentally sustainable travelling at cities and regions and most importantly across all Europe. Specifically, the activity A2.1 – Towards TM2.1, included in the WP2 – Open Cloud System Architecture, has been set-up with the aim to explore how the TM2.0 concept can be integrated into the overall MyCorridor Open Cloud System Architecture. The key outcome of this activity is the conclusion that the interconnection between the MaaS paradigm and the TM2.0 concept can be implemented by integrating key traffic management services into the MaaS offerings and products. A traffic management service provider is viewed by the MyCorridor platform as any other service provider, meaning that s/he is registered to the platform and registers his services as any other service provider. The types of traffic management services that can be registered to the MyCorridor platform are the following:

- Parking availability information.
- Route planning.
- Real time traffic state and forecast information.
- Events (e.g. accidents, incidents, road works, etc.) information.
- Advanced traffic forecast information.
- Zone access control information.
- Traffic light forecast information.
- Traffic events information.

These services are offered to the traveller in two phases, namely in the pre-trip and in the on-trip phase. In the pre-trip phase, the traffic management services are presented to the travellers as part of the result of the matchmaking process, provided that the traveller has chosen in his profile that s/he wishes to receive traffic management services as MaaS offerings, and that the registered traffic management services meet the requirements of the traveller's input (e.g. trip request). It should be pointed out here that there is a differentiation in the way the traffic management services are presented to the traveller (i.e. in terms of UI presentation), compared with the other types of services. For example, in the case of event information, a textual description of the service is presented to the user (as for any other type of service), but also, the events that have occurred up to the present time are depicted on the map view as points of interest. The traveller can choose any of them on the map, and see relevant information of the event (e.g. type of the accident, severity, etc.). Other traffic management services are presented in similar ways.

Regarding the on-trip phase, the traveller can receive push notifications on his mobile phone that refer to the state of the traffic network. In particular, the system automatically identifies the traveller's mobility status (i.e. if s/he is moving or not), and starts tracking its position. Based on the position information, the traveller receives information regarding the state of the traffic network. For example, the traveller may receive a message notifying him for an accident that has happened very close to him, accompanied by an appropriate recommendation (e.g. to turn in the next exit). In this way, MyCorridor system associates the recommendation event for the real travel of the individual user, and use method(s) to influence the user's behaviour; there are two scenarios:

- *Virtual Variable Message Signs (VMS)*: When the user's car enters pre-defined geo-fence, pre-defined message is presented to the user proposing re-routing if such an action has been proposed by the Traffic Management System (TMS).
- *Park and drive message*: When the user's car enters a pre-defined geo-fence, and if there is parking available based on real-time occupancy data, then an in-vehicle, default message is presented to

the user proposing nearby parking and public transport information from a designated parking lot & ride place.

The information provided in the above phases, is the combination of multiple information from several traffic management operators (Figure 4), which provide different types of traffic management services in different areas. Therefore, it becomes evident that there is a need of a specific module that will act as an orchestrator of this traffic management services integration process. In the context of the MyCorridor project, we introduce the concept of *Traffic Management Services Aggregator*, which is a module responsible for gathering information from several, different traffic management services, unifying them, and offering them to the MaaS platform through one common interface (i.e. an API). This module is defined as external to the MyCorridor MaaS platform, but it directly collaborates with it.

The above are tangible examples of the collaboration between the MaaS paradigm and the TM2.0 concept in the context of MyCorridor project. These functionalities can go one step further towards the implementation of the TM2.1 concept. In particular, there should be a mechanism that will allow the traffic management operators to ask the assistance of the MaaS platform in order to improve the state of the traffic network. For example, the traffic management operators could indicate a capacity drop within the network, which they cannot solve using only traffic management measures. Thus, they ask the MaaS operator to switch travel demand onto a different travel mode or modes provided by the service providers, based in capacity and pricing, with respect to the user's business role in order to avoid the capacity drop. The switch can be achieved through push notifications, and/or incentives (e.g. discounts) to the travellers. One example is park and ride information and discount offer. It is the intention of the project partners to explore the feasibility of such scenarios during the final phase of the project.

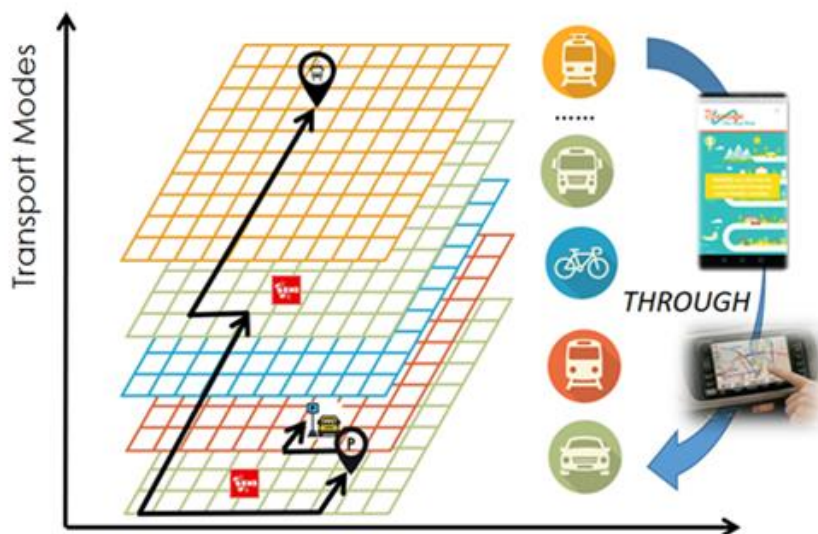


Figure 4: Example of collaboration between different traffic management operators to provide final information to MyCorridor app

3 System Architecture Design Methodology

Figure 5 below shows the methodology that was adopted in the context of MyCorridor project for defining the overall system architecture. This overall process includes the following subprocesses:

- Identification and recording of the initial needs of the users.

- Transformation of user needs into use cases.
- Definition of the specific system architecture components that can implement the identified use cases.
- Organization of the components in a particular architectural structure, selected based on its advantages compared to other structures.
- Description of sub-components, mode of operation, and technical characteristics for each of the defined components.
- Description of the interconnection between the components, so that the overall system can deliver the identified use cases.
- Identification and recording of the overall technical requirements that the system must satisfy.
- Definition and recording of the system specifications that satisfy, in the best possible way, the identified requirements.

These subprocesses can be described in a more documentary way using the principles of the Unified Modeling Language (UML) [18] system architecture methodology. Although UML cannot be considered as methodology in the strict sense of the term, it provides a set tools and techniques to software architects that help them to provide a clear and concise approach for the design of the architecture a large scale software project. UML is mainly expressed by a set of appropriate diagrams (e.g. use case diagrams, sequence diagrams, etc.) that schematically describe each of the aforementioned subprocesses (and more).

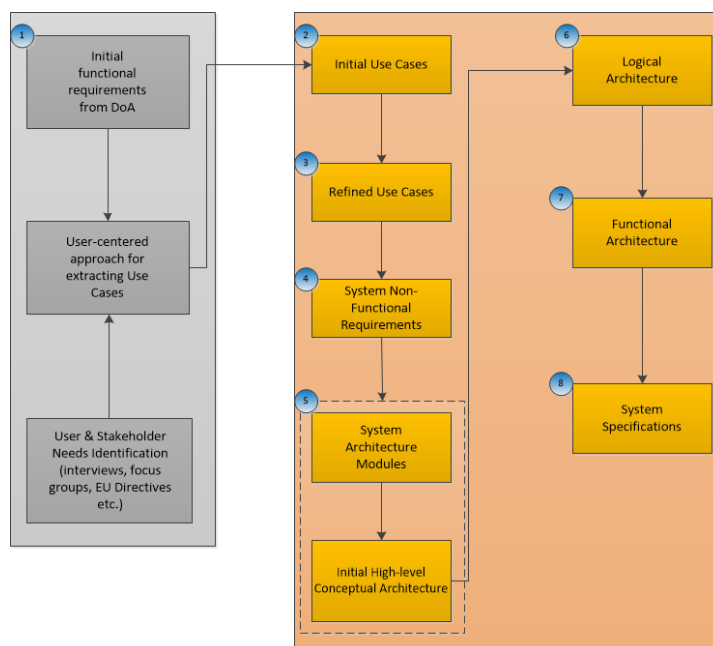


Figure 5: Architecture Design Methodology of the MyCorridor platform

The overall proposed methodology for designing the overall architecture of the MyCorridor platform includes the following distinct, but interactive steps:

Step 1: Identification and recording of initial user needs

In the first step of the proposed approach, the needs of the users and stakeholders are identified through various channels, such as literature and market surveys, on-line surveys, focus groups and workshops, EU Directives and policy documents review, etc. The overall process that takes place as part of the user-

centred approach for extracting use cases, according to the methodology defined in the deliverable D1.1, takes also into account the initial requirements from DoA.

Step 2: Transformation of user needs into use cases

The objective of this step is to transform the identified user needs (step 1) into a set of meaningful and descriptive use cases. This step is very important because, on one hand, the commonly unclear needs of users are translated into concrete, real-world scenarios, and on the other, all the subsequent steps of the process of designing the system architecture are driven by the requirement to meet these needs. The defined use cases are schematically described by the UML use case diagrams (as reported in the deliverable D1.1), whereas the user and market driven requirements checklist of D1.1. Chapter 11 has served as a clearance list for the use cases.

Step 3: Refinement of use cases

This is a repetitive step which includes the refinement of the initial use cases based on the review of the current state-of-the-art technologies that can implement them. This step has been repeated many times until the final, pragmatic set of use cases is produced.

Step 4: System non-functional requirements

The objective of this step is to define the non-functional requirements of the MyCorridor system. These requirements essentially describe how the system should *be* (in contrast with the functional requirements that describe what the system should *do*), and specify the criteria that can be used to judge the operation of a system. The system non-functional requirements emerged from the work conducted in the deliverable D1.1, namely the definition of the use cases and the user and market driven requirements. Finally, the system non-functional requirements are presented based according to a specific software system requirements specification template.

Step 5: Conceptual architecture

As soon as the final set of use cases and the system non-functional requirements are in place, we proceed with design of the system conceptual architecture. This step includes the first definition (in an abstract level) of the specific system architecture components that can implement the identified use cases. These components can implement either specific business logic (i.e. algorithmic process that produce a specific result), or ancillary functions that are equally important with the business logic (e.g. communication protocols, data transformation, etc.). Since these modules are defined, they are organized into a specific architectural structure. The choice of the particular structure to be used depends on the benefits it can offer to the overall system, compared to the benefits offered by other architectural structure. The final outcome of this step is the first version of the *high-level conceptual architecture* of the system, which is depicted by the corresponding conceptual architecture diagram.

Step 6: Logical architecture

This step describes the functions, the structural sub-components and the characteristics of each of the system architecture components. The descriptions are supplemented with appropriate UML component diagrams wherever useful, i.e. when a component is complex enough to contain sub-components, and therefore requiring a graphical description through a UML component diagram.

Step 7: Functional architecture

This step describes how the system architecture components communicate with each other in order to materialize the defined, in the deliverable D1.1, use cases. Each description is provided in a per use case

fashion, and it is supplemented with appropriate UML sequence diagrams. The descriptions provided in this step are essentially the functional requirements of the system (i.e. what the system should do).

Step 8: System specifications

This final step of the overall system architecture design process describes in detail the technical specifications of the overall system defined based on the need to meet the system non-functional requirements.

The following sections describe in detail the steps 4 to 7.

4 System Non-Functional Requirements

In the deliverable D1.1 a set of user and market driven requirements as identified through the consolidation of the collected information through a) the literature and the current MaaS landscape (competition), b) the online survey conducted by MyCorridor project, c) the focus groups and d) the feedback during and after the 1st Pan-European MyCorridor workshop, have been documented. These requirements formed the basis for the definition on the non-functional requirements of the MyCorridor system, presented in this section.

The non-functional requirements of the MyCorridor system are presented here according to the Volere Requirements Specification Template [2] (referred as Volere template from this point onwards). Volere [19] is the name given to a collection of requirements resources (e.g. courses, templates, books, processes, etc.) that were developed by the Atlantic Systems Guild (referred as Guild from this point onwards) in 1995 in order to be a common and easily accessible way of discovering requirements, communicating them and connecting them to solutions. The Guild is a London, Aachen and New York think tank, consultancy and training organisation with the objective of remaining at the forefront of systems development and engineering. The Guild includes the Volere Requirements Specification Template authors, Suzanne Robertson and James Robertson, together with Tom DeMarco, Peter Hruschka, Tim Lister and Steve McMenamin. The Volere approach to system requirements and specifications has been used by thousands of projects, which range from the conventional commercial domains such as banking, insurance, and so on, to more exotic areas such as air traffic control, aviation, automotive engineering, real-time control of appliances, telephony, and many more. The Volere template was utilized for the documentation of the non-functional requirements of the system developed in the context of the SocialCar H2020 European Research Project [20], in which CERTH/ITI was again the leading partner responsible for the overall system architecture design and implementation.

Based on the Volere template, the non-functional requirements of a large-scale software project can be divided into the following categories:

- Look & Feel Requirements (LFR)
- Usability & Humanity Requirements (UHR)
- Performance & Scalability Requirements (PSR)
- Operational & Environmental Requirements (OER)
- Maintainability & Support Requirements (MSR)
- Security & Data Privacy Requirements (SDPR)
- Cultural Requirements (CR)
- Legal Requirements (LR)

The Volere template provides a detailed structure for writing a rigorous and complete requirements specification. In particular, it provides sections for each of the requirements types appropriate to today's

software systems. In the following subsections, the non-functional requirements of the overall MyCorridor system, belonging to each of the above categories, are presented in tabular form based on the Volere “requirements shell”.

4.1 Look & Feel Requirements

The Look & Feel Requirements (LFR) are related to the appearance of the product and specify the mood, style and feeling of it. Such requirements are the colours, the fonts and the graphics to be used and can influence the way a potential customer will see and perceive the product. Moreover, these requirements will determine precisely how the product shall appear to its intended consumer and guide the designers to create a product as envisioned by the client. In the case of the MyCorridor system, these requirements are mainly related to the front-end interfaces, namely the mobile applications and the web applications, and are presented in Table 2 and Table 3.

Table 2: Look & Feel Requirements – LFR1

ID	LFR1
Name	Familiar appearance
Requirement type	LFR - Appearance
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#6, #7
Description	The system should support UI metaphors that are commonly used to general mobile applications
Rationale	To increase user acceptance of the MyCorridor system
Fit Criterion (Measurable)	User interface should look familiar to existing systems
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	4 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	1 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers, Service Providers
Author	Theodoros Ioakeimidis

ID	LFR1
Revision	V03, 12/06/2019

Table 3: Look & Feel Requirements – LRF2

ID	LFR2
Name	Attractive UI
Requirement type	LFR - Style
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#6, #7
Description	The UI should appear pleasant to use and not boring for the eye
Rationale	To increase user acceptance of the application
Fit Criterion (Measurable)	User should feel comfortable when looking at the application and browsing through it
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	4 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	1 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers, Service Providers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

4.2 Usability & Humanity Requirements

The Usability & Humanity Requirements (UHR) include the non-functional requirements that make the product usable and ergonomically acceptable to the end users. These requirements describe how easy it is for the intended users to operate the product, as well as the way in which the product can be altered or configured to take into account users' personal preferences. The Usability & Humanity Requirements of the MyCorridor system are presented in Table 4 - Table 8.

Table 4: Usability & Humanity Requirements - UHR1

ID	UHR1
Name	Ease of use
Requirement type	UHR – Ease of Use
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#6, #7, #8, #10, #22, #34, #24, #25, #26, #27
Description	Even people who are not familiar with the MaaS concept should be able to use the MyCorridor system
Rationale	Ease of use and better adaptability
Fit Criterion (Measurable)	To be understandable by users who are not familiar with mobility products
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	2 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers, Service Providers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 5: Usability & Humanity Requirements – UHR2

ID	UHR2
Name	Personalization
Requirement type	UHR – Personalisation and Internationalisation
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#1, #2, #3, #4, #5, #13, #15, #19
Description	The system should be adaptable to traveller's preferences
Rationale	To provide tailor-made mobility solutions that fit traveller's preferences requirements
Fit Criterion (Measurable)	Include a profiling mechanism
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	n/a
Constraints (Attainable)	n/a
Difficulty	2 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 6: Usability & Humanity Requirements – UHR3

ID	UHR3
Name	Internationalisation
Requirement type	UHR – Personalisation and Internationalisation

ID	UHR3
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#9, #30, #31
Description	The system should be adaptable to country-specific languages, measurement units and currencies, including symbols and decimal conventions
Rationale	To keep the users away from getting confused by the different conventions applying to each country
Fit Criterion (Measurable)	Support for all conventions within EU
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	4 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	3 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	Some functionalities that are not supported by existing systems should be hidden
Difficulty	2 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers, Service Providers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 7: Usability & Humanity Requirements – UHR4

ID	UHR4
Name	Easy to learn
Requirement type	UHR – Learning
Relevant User & Market Driven Requirement(s)	#29, #35, #36, #37, #38

ID	UHR4
(reported in the deliverable D1.1)	
Description	Even non-IT experts should be able to learn easily how to use the system. Also the system should train the users (i.e. travellers and services providers) regarding new concepts of MaaS (e.g. environmental friendly mobility, discounts for travellers that choose environmental friendly mobility solutions, etc.)
Rationale	Ease of use
Fit Criterion (Measurable)	To be understandable by users who are not familiar with PND devices
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	n/a
Constraints (Attainable)	n/a
Difficulty	2 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 8: Usability & Humanity Requirements – UHR5

ID	UHR5
Name	Use common symbols and words
Requirement type	UHR – Understandability and Politeness
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#6, #7, #8, #34

ID	UHR5
Description	The system should use words and symbols that are generally understandable by users and unambiguous
Rationale	To allow wide acceptance and usability
Fit Criterion (Measurable)	The UI includes only naturally understandable symbols
Customer satisfaction	4 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	4 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	3 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	2 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers, Service Providers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

4.3 Performance & Scalability Requirements

The Performance & Scalability Requirements (PSR) refer to aspects such as the product's ability to operate at a speed suitable for the intended environment, the quantification of the desired accuracy of the results produced by the product and the expected availability of the product. For instance, system response times, allowable time between failures and the expected increases in size that the product must be able to handle belong to this type of non-functional requirements. The Performance & Scalability Requirements of the MyCorridor system are presented in Table 9 - Table 11.

Table 9: Performance & Scalability Requirements – PSR1

ID	PSR1
Name	Fast response
Requirement type	PSR – Speed and Latency
Relevant User & Market Driven Requirement(s)	#20, #32

ID	PSR1
(reported in the deliverable D1.1)	
Description	The system performance should be as close as possible to the real-time response level
Rationale	Potential travellers are not willing to wait for more than 60 seconds for a set of personalized MaaS packages to appear. Therefore, the response of the system should not exceed this time limit
Fit Criterion (Measurable)	Time from the submission of the request to the response
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	3 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	4 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 10: Performance & Scalability Requirements – PSR2

ID	PSR2
Name	Accurate Suggestions
Requirement type	PSR – Precision or Accuracy
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#1, #2, #4, #11, #12, #14, #15, #16, #17, #18, #19, #21, #32
Description	The system should provide accurate MaaS offerings

ID	PSR2
Rationale	Potential travellers might quickly lose interest in the platform in the event that they experience a lot of bad suggestions that do not fit their preferences
Fit Criterion (Measurable)	User relevance feedback
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	4 (Scale from 1=low difficulty to 5=extreme difficulty).
Actors	Travellers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 11: Performance & Scalability Requirements – PSR3

ID	PSR3
Name	System Availability
Requirement type	PSR – Reliability and Availability
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#11, #12, #14, #16, #32
Description	The system shall be available for use 24 hours a day, 365 days a year (except maintenance periods), and also to be able to support adequate number of users in terms of performance and data storage
Rationale	Potential travellers might quickly lose interest in the platform in the event that the system is often down when they want to use the application
Fit Criterion (Measurable)	The system is up and running all the time (except maintenance periods)

ID	PSR3
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	3 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

4.4 Operational & Environmental Requirements

The Operational & Environmental Requirements (OER) refer to the physical environment in which the product will operate, the interface with adjacent systems and the distribution of the product. These requirements will ensure that the product fits to its intended environment and will help quantify the clients' expectations about the amount of money and resources they will need to allocate in order to install and use the product. The Operational & Environmental Requirements of the MyCorridor system are presented in Table 12.

Table 12: Operational & Environmental Requirements – OER1

ID	OER1
Name	Network conditions
Requirement type	OER
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#11, #12, #14, #16, #20, #24, #31, #32
Description	Potential travellers shall be able to use the product while being on the move and there is an enabled wireless Internet connection (3/4G or Wi-Fi)

ID	OER1
Rationale	For enabling all of the foreseen functionalities on the go and real-time updates
Fit Criterion (Measurable)	Device communication accuracy and low latency
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	Wireless Internet connection on the go (3/4G or Wi-Fi)
Difficulty	1 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

4.5 Maintainability & Support Requirements

The Maintainability & Support Requirements (MSR) contain the requirements that refer to the quantification of the time necessary to make specified changes to the product, the level of support that the product requires, and the adaptability of the product. The Maintainability & Support Requirements of the MyCorridor system are presented in Table 13 and Table 14.

Table 13: Maintainability & Support Requirements – MSR1

ID	MSR1
Name	Automatic updates
Requirement type	MSR
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#32, 34
Description	The system should be able to automatically update to the latest version

ID	MSR1
Rationale	To guarantee stability in performance
Fit Criterion (Measurable)	Relevant functionality to allow automatic updates
Customer satisfaction	4 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	4 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	4 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	Internet access
Difficulty	1 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	Travellers
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 14: Maintainability & Support Requirements – MSR2

ID	MSR2
Name	Regular checks and maintenance sessions
Requirement type	MSR
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#32, #34
Description	The overall health of the MyCorridor system should be regularly checked, and scheduled maintenance periods should be established
Rationale	Ensure the seamless functionality of the overall MyCorridor system
Fit Criterion (Measurable)	Regular checks and maintenance periods should be established
Customer satisfaction	4 (Scale from 1=uninterested to 5=extremely pleased)

ID	MSR2
Customer dissatisfaction	4 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	4 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	-
Difficulty	1 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	MaaS aggregator, service provider
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

4.6 Security & Data Privacy Requirements

The Security & Data Privacy Requirements (SDPR) help to understand the expectations for the confidentiality aspects of the system, such as who is authorized to access the system and to what extent, as well as the expectations for the integrity of the system's data. Moreover, this type of requirements specifies what actions the system has to take in order to ensure the privacy of individuals for whom it stores information. The Security & Data Privacy Requirements of the MyCorridor system are presented in Table 15 - Table 17.

Table 15: Security & Data Privacy Requirements – SDPR1

ID	SDPR1
Name	Traveller/service provider/MaaS aggregator authentication
Requirement type	SDPR - Access
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#23, #28, #33
Description	The system shall support traveller/service provider/MaaS aggregator authentication
Rationale	To prevent malicious users from getting access to the system and jeopardising the quality of the provided services

ID	SDPR1
Fit Criterion (Measurable)	The system asks for traveller's/service provider's/MaaS aggregator's credentials in order to allow access
Customer satisfaction	3 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	3 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	4 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	The traveller/service provider/MaaS aggregator must be authenticated by a trusted authority
Difficulty	1 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	All users
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 16: Security & Data Privacy Requirements – SDPR2

ID	SDPR2
Name	Data privacy
Requirement type	SDPR - Privacy
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#23, #28, #33
Description	No personal data must be revealed or stored on the cloud in any unprotected way
Rationale	In order for MyCorridor to conform to EU personal data and ethics requirements
Fit Criterion (Measurable)	Access of personal data should be restricted to the device
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)

ID	SDPR2
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)
Conflicts	-
Constraints (Attainable)	User should be aware of any privacy issues
Difficulty	2 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	All users
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

Table 17: Security & Data Privacy Requirements – SDPR3

ID	SDPR3
Name	User awareness of information practices
Requirement type	SDPR - Privacy
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#3, #23, #24, #25, #27, #28, #33
Description	The system shall make its users aware of its information usage practices before collecting data from them
Rationale	Protection of sensitive personal data. System makes use of user data in a protected (e.g. anonymized) way and only under user consent
Fit Criterion (Measurable)	User should be notified and confirm before the system will be allowed to collect data
Customer satisfaction	5 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	5 (Scale from 1=low priority to 5=highest priority)

ID	SDPR3
Conflicts	-
Constraints (Attainable)	User should be aware of any privacy issues
Difficulty	3 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	All users
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

4.7 Cultural Requirements

The Cultural Requirements (CR) include requirements that are specific to the sociological factors that affect the acceptability of the product. Such requirements will help developers to discover and take into account aspects that can be beyond their cultural experience. The Cultural Requirements of the MyCorridor system are presented in Table 18.

Table 18: Cultural Requirements – CR1

ID	CR1
Name	Localization
Requirement type	CR
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#9, #11, #12, #20, #24, #30
Description	The system should be able to support localized information
Rationale	Easier user interaction with the system
Fit Criterion (Measurable)	The system should support the language, currency and metric system of the country of use as well as the native language of the user
Customer satisfaction	4 (Scale from 1=uninterested to 5=extremely pleased)
Customer dissatisfaction	5 (Scale from 1=hardly matters to 5=extremely displeased)
Priority	4 (Scale from 1=low priority to 5=highest priority)

ID	CR1
Conflicts	Inaccurate information may sometimes become available due to potential translation errors
Constraints (Attainable)	The scope of countries in which the system will operate should be defined in advance (e.g. EU). The different country codes should be taken into account for all the countries to be included
Difficulty	2 (Scale from 1=low difficulty to 5=extreme difficulty)
Actors	All users
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

4.8 Legal Requirements

The Legal Requirements (LR) specify the legislation context under which the product shall operate in order to avoid future delays, lawsuits, and legal fees, and also to ease the identification of any copyrights or other intellectual property that has to be protected. The Legal Requirements of the MyCorridor system are presented in Table 19.

Table 19: Legal Requirements – LR1

ID	LR1
Name	Conform to GDPR [21]
Requirement type	LR
Relevant User & Market Driven Requirement(s) (reported in the deliverable D1.1)	#28, #33
Description	The system should conform to the GDPR regulation and to provide transparent, viable and beneficial Service Level Agreements (SLAs)
Rationale	To comply with the law so as to avoid lawsuits and legal fees
Fit Criterion (Measurable)	The system should manage personal data according to regulations imposed by GDPR, and to provide the registered services to the travellers based on clear SLAs

ID	LR1
Customer satisfaction	<i>5 (Scale from 1=uninterested to 5=extremely pleased)</i>
Customer dissatisfaction	<i>5 (Scale from 1=hardly matters to 5=extremely displeased)</i>
Priority	<i>5 (Scale from 1=low priority to 5=highest priority)</i>
Conflicts	-
Constraints (Attainable)	-
Difficulty	<i>2 (Scale from 1=low difficulty to 5=extreme difficulty)</i>
Actors	All users
Author	Theodoros Ioakeimidis
Revision	V03, 12/06/2019

5 Conceptual Architecture

The system architecture design process is a multi-level process in which representations of data structures and system components are combined in a specific structure in order to provide the implementation path of the final system. This process provides an abstract view of the system, along with a way information is exchanged between its structural elements, and therefore, it is considered as a fundamental part of the development process. The following key design principles should be carefully considered when building the architecture of a large scale software project:

- Requirements are very likely to evolve throughout the development process. Hence, an architecture should be able to embrace this kind of change and be traceable to the user requirements within the system development lifecycle.
- Each component of the system should be in charge of a single system functionality. This principle, known as the single responsibility principle, enhances the better understanding of the system and prevents responsibilities from becoming coupled, which eventually leads to a fragile design difficult to adapt to changes.
- Components and modules should be divided into distinct sections so that there is no functionality overlap. Each section is responsible for a specific concern, which leads to high cohesion and low coupling among components.
- In many cases, application requirements could be unclear or there may be a need for further planning over time. Large upfront design of the whole system makes it hard to embrace evolving requirements and decreases scalability.
- The cost effectiveness of the proposed solution should be taken into account. Considering the estimated budget, a complete and in depth analysis regarding development and maintenance cost of the proposed solution should be conducted in order to estimate whether it meets the needs of the software development process.

Software architecture consists of system representations that enhance communication and understanding among stakeholders. It provides a level of abstraction that enables broader comprehension of the structure and interactions between the various system components. Moreover, the earliest design decisions are the most significant part of the system's development process and have a great impact on all the following stages. Therefore, carrying out a thorough analysis regarding the selection of the most suitable architectural style is a fundamental process at the early stages of the system design. The following subsection presents the most widely used software architecture styles, summarizing their strengths and weaknesses.

5.1 Architectural Styles

Architectural styles define the basic characteristics and behaviour of a system. They refer to particular patterns used in order to establish a structure for all system components and modules, define the way these software elements communicate with each other and form a set of constraints about the way they relate and integrate to form the system. Architectural styles can also provide a view of the overall properties of the system through conceptual and implementation models. Some of the most commonly used architectural styles are summarized below.

5.1.1 Layered architecture

The most common software architecture pattern is the layered architecture, also known as the n-tier architecture pattern. In this pattern, the overall system is organised into separate layers, with each layer performing a specific function within the application. Each layer relies only on the features and services offered by the layer immediately beneath it. Therefore, the layered architecture pattern provides isolation and independence. The number and types of the existing layers may vary based on the nature of the application. Thus, smaller applications may have only three layers, whereas larger and more complex business applications may contain five or more layers.

One of the major advantages of the layered approach is *the separation of concerns* among the components of the system. Components within a specific layer are only associated with the logic that pertains to that layer, thus making it easy to add new layers with additional functionality or replace an existing one without affecting other parts of the system. In addition, the layered architecture pattern supports the incremental development of software systems, since during the development of a layer, some of its services can be made available to users as soon as they are ready.

Apart from the advantages, there are some shortcomings as well. Separating a system into different independent layers is a non-trivial task that requires expertise. Moreover, performance issues may arise, because a single request shall pass through multiple tiers in order to reach its final destination.

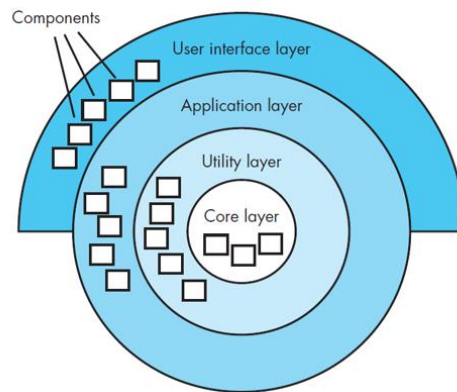


Figure 6: Layered architecture

The overall concept of the layered architecture is depicted in Figure 6. As shown in this figure, there are different layers accomplishing operations that progressively become closer to the machine instruction set. Components in the outer layer service user interface operations, whereas components in the inner layer perform operating system interfacing. Intermediate layers provide utility services and application software functions.

5.1.2 Client-server architecture

In the context of the client-server architecture pattern, clients request and receive services delivered from different servers. The main components of a client-server system are:

- A set of servers that offer services to other components. The servers are considered as individual software components, so several servers may run on the same computer.
- A set of clients that access the services offered by the servers. Several instances of a client program can be executed concurrently on the same or different computers.
- A network that allows the clients to communicate with the servers. The client-server systems are usually implemented as distributed systems connected using Internet protocols.

A server computer can manage several clients simultaneously, whereas one client can be connected to multiple servers at a time, each providing a different set of services. Services and servers can change without affecting other parts of the system, allowing for easy component replacements and upgrades. In addition, as servers have better and more effective control over the resources, the security ensured by this architecture is also quite stringent. An example of a system designed based on the client-server architecture pattern is presented in Figure 7.

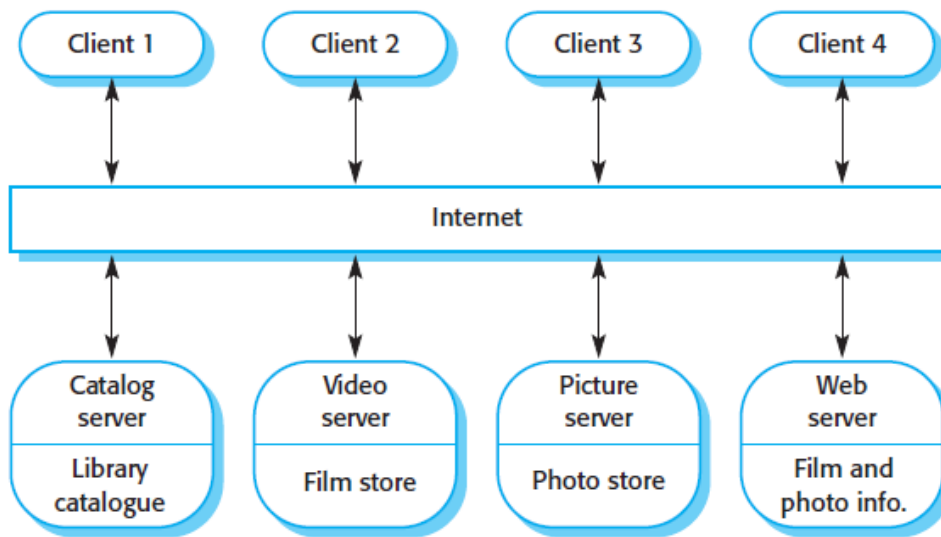


Figure 7: An example of a system designed based on the client-server architecture pattern.

5.1.3 Data-centered architecture

In the data-centered architecture, the data is centralized and frequently processed by the several system components. A data store (e.g. a file or a database) resides at the center of the architecture, and it is frequently accessed by other system components that update, add, delete, or modify data within that store. This approach is suitable for systems in which the primary objective is the frequent processing of large volumes of data. Some examples of software systems that commonly adopt this model of architecture are:

- Command and control systems
- Management information systems
- Computer-Aided Design (CAD) systems
- Interactive Development Environments (IDEs)

One of the main advantages of the data-centered architecture is the efficiency in data sharing. Organizing components around a data repository constitutes an efficient way of sharing large amounts of data that eliminates the need for transmitting information explicitly from one component to another. Another advantage of these architectures is that they promote integrability, meaning that the client components can function independently of each other. Thus, existing components can be changed and new components can be added to the architecture without affecting any other components.

However, there are also some shortcomings related to this architectural style. Firstly, there is a high dependency between the data structure of the data store and its agents. The system components must operate around an agreed data model for the shared repository and this means that it may be difficult or even impossible to integrate new components, if their data models are different from the agreed schema. Moreover, the data repository is a *single point of failure (SPOF)* for the whole system, and therefore, problems that may arise in it, may affect the availability and the dependability of the overall system.

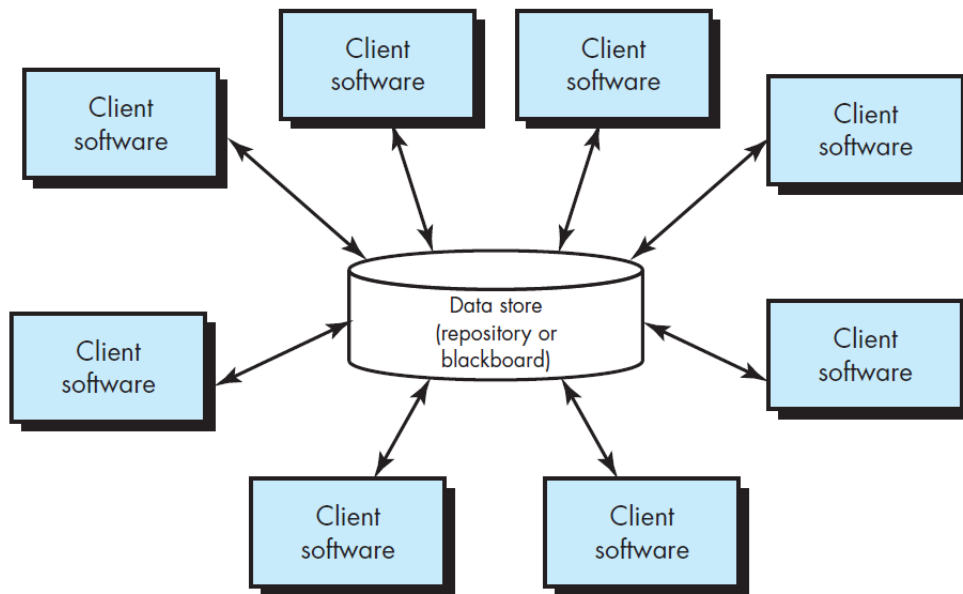


Figure 8: Data-centered architecture

A data-centered software system, in which the several components share data only through the data store without interacting directly with each other, is depicted in Figure 8. Data stores can be either passive, where a client accesses the data regardless of any changes to the data or actions performed by other clients, or use a “blackboard” model that notifies a client when particular data become available, or when data of interest to a client change.

5.1.4 Data-flow architecture

This architectural style is employed when input data has to be transformed through a series of computational or manipulative components into output data. In data-flow architecture, the data enters into the system and flows through the modules one at a time until they are assigned to some final destination (output or a data store). The whole software system can be seen as a series of transformations on consecutive pieces or sets of input data, where data and operations are independent of each other.

The main objective of this approach is to achieve reusability and modifiability. There are three types of execution sequences between modules:

- Batch sequential
- Pipe and filter or non-sequential pipeline mode
- Process control

Figure 9 demonstrates a pipe and filter execution sequence, where the data flows (as in a pipe) from one discrete processing component (filter) to another, and each component carries out a specific type of data transformation. Systems that adhere to this model can be implemented by combining UNIX commands, using pipes and the control facilities of the UNIX shell. Variants of this pattern have been in use since computers were first used for automatic data processing.

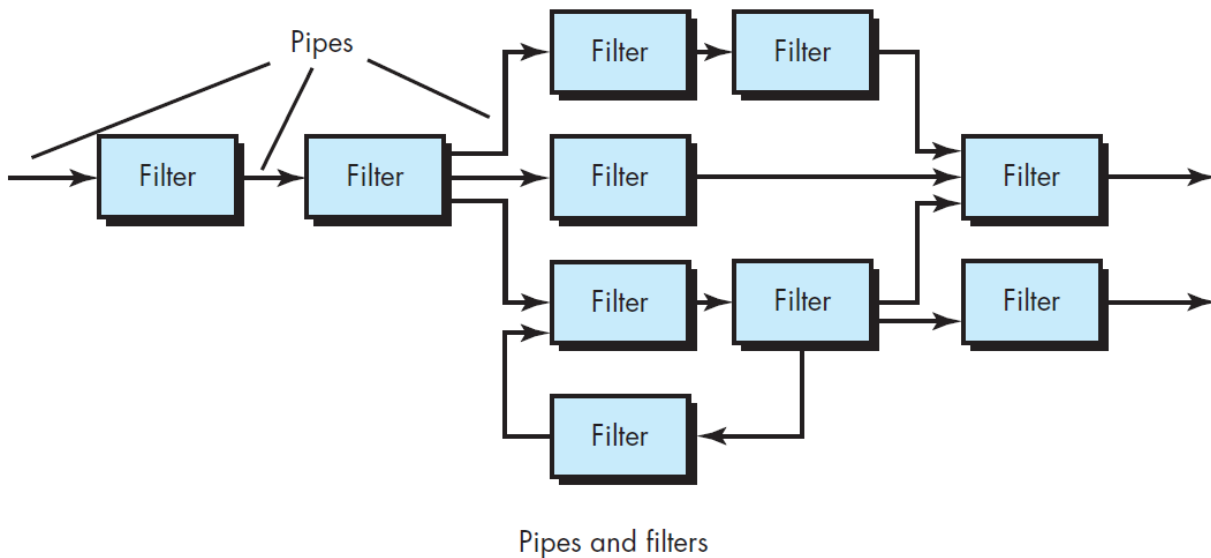


Figure 9: Data-flow architecture

When transformations are sequential with data processed in batches, this pipe and filter architectural model becomes a *batch sequential* model, a common architecture for data-processing systems such as billing systems. In the batch sequential style, the processing steps are independent programs and there is the assumption that each step runs to completion before the next step starts. Each batch of data is transmitted as a whole between the steps. The architecture of an embedded system may also be organized as a process pipeline.

Data-flow systems are easy to understand and maintain because their workflow style matches the structure of many business processes. In addition, reusing or adding transformations is simple and straightforward. Poor performance though is an issue in such systems, as there is no way to make filters interact cooperatively to solve a problem. Moreover, they support limited user interaction. For instance, it is difficult to implement graphical user interfaces, which have more complex Input/Output (IO) formats than simple textual input and output and are based on events such as mouse clicks or menu selections, using the data-flow architecture.

5.1.5 Call-and-return architecture

The call-and-return architecture has been the dominant architectural style in large software systems for the past 30 years. The primary objective of this approach is to build systems that are relatively easy to modify and scale. A number of sub-types of this style have also emerged including:

- Main program/subprogram architectures (Figure 10): the classical programming paradigm where the objective is to hierarchically decompose a program into smaller pieces in order to achieve modifiability. There is typically a single thread of control and each component in the hierarchy gets this control (optionally along with some data) from its parent and passes it along to its children.
- Remote procedure call systems: they are main-program-and-subroutine systems that are decomposed into parts that live on computers connected via a network. The computations are distributed to multiple processors in order to improve performance. The actual assignment of parts to processors is deferred until runtime, so that it can change easily to accommodate performance tuning. A remote procedure call is practically indistinguishable from standard main

program and subroutine systems, except that subroutine calls may take longer to accomplish if it is invoking a function on a remote machine.

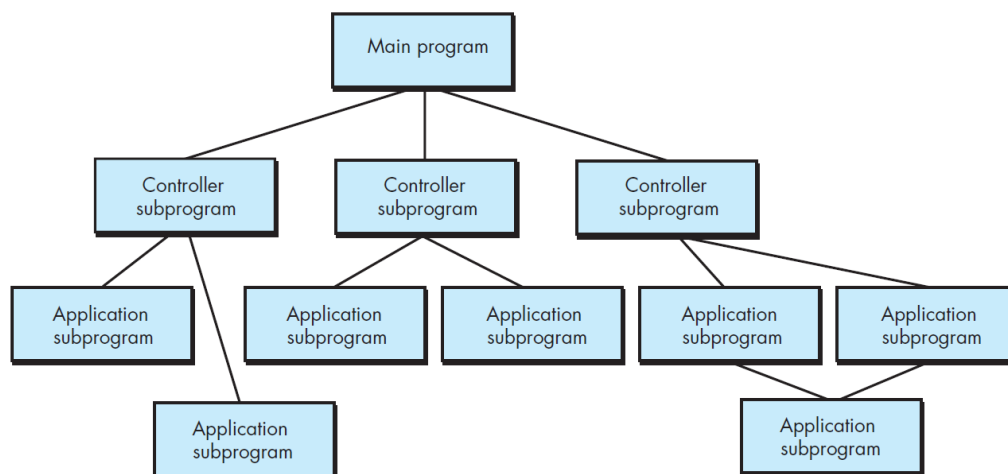


Figure 10: Main program/subprogram architecture

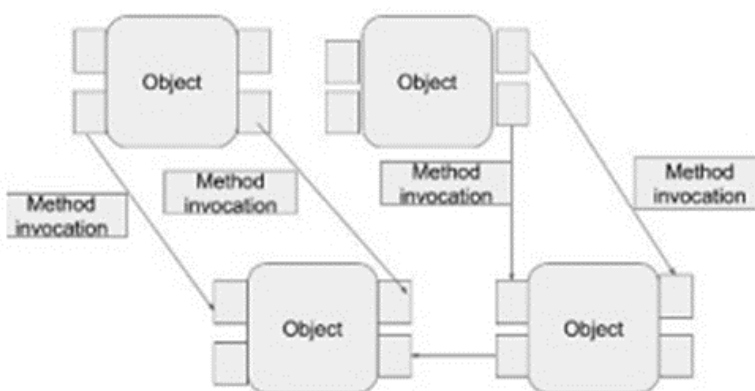


Figure 11: Object-oriented architecture

5.1.6 Object-oriented architecture

The object-oriented architecture is the modern version of the call-and-return architecture, focusing mainly on the bundling of data and methods to manipulate these data. It is a design paradigm based on the division of responsibilities for an application or system into individual reusable and self-sufficient components (objects). The components of a system provide black-box services that the other components can request for, trying to achieve modifiability. The internal functionality of an object is unknown to its environment (encapsulation) and the object can be accessed only through provided operations, typically known as methods, which are constrained forms of procedure calls. This encapsulation promotes separations of concerns, reusability and extensibility. As Figure 11 depicts, access to the objects is allowed only through specific methods.

5.1.7 Service-oriented architecture

The service-oriented architecture (SOA) is an architectural style that supports service orientation and makes application functionality to be provided as a set of services (Figure 12). A service is a discrete unit of functionality that can be accessed remotely and acted upon independently. A service has the following properties:

- It is self-contained.
- It logically represents a business activity with a specified outcome.
- It is a black box for its consumers.
- It may consist of other underlying services.

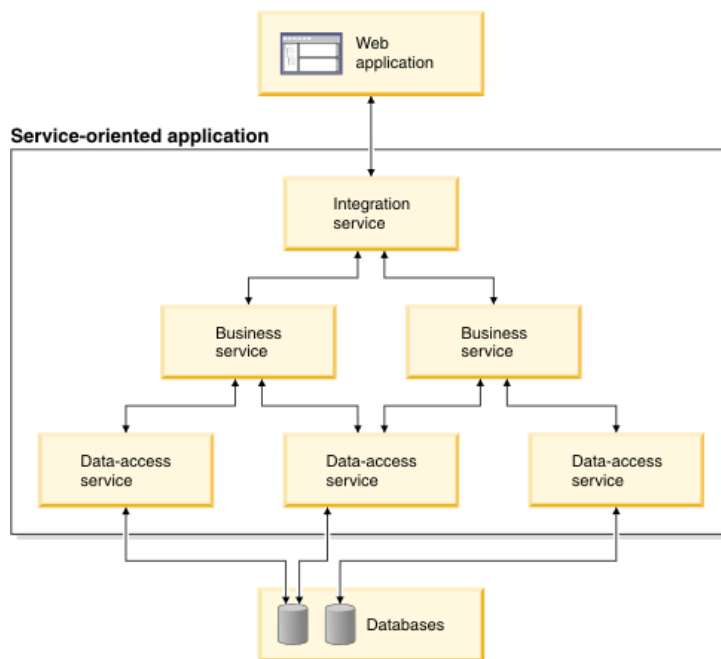


Figure 12: Service-oriented architecture

Services are self-directed and accessed through a formal contract, which promotes loose coupling and abstraction. SOA provides interoperability, since the provider and the consumer of the service can be built and deployed on different platforms. Moreover, the SOA approach includes greater ease of maintaining and updating the system, since it is easier to fix or replace elements without affecting the other system components. However, in the SOA pattern issues may arise in the communication between services. SOA is typically associated with the Enterprise Service Bus (ESB), as the central means of communication between services, which often does not respond well to change and it typically results in more complexity, and makes it harder to understand where a service begins and ends.

5.1.8 Microservices architecture

The microservices architecture pattern is based on the notion of service components. It has evolved from issues associated with other common architecture patterns, such as the service-oriented architecture pattern (SOA), and focuses on building systems that are as modular as possible. Microservices are not bound by the same communication frameworks, protocols, and specifications that ultimately limit SOA. Service components can vary in granularity from a single module to a large portion of the application. All the components are fully decoupled from one another and accessed through some sort of remote access protocol (e.g., REST, SOAP, RMI, etc.). Figure 13 depicts the typical microservices architecture pattern.

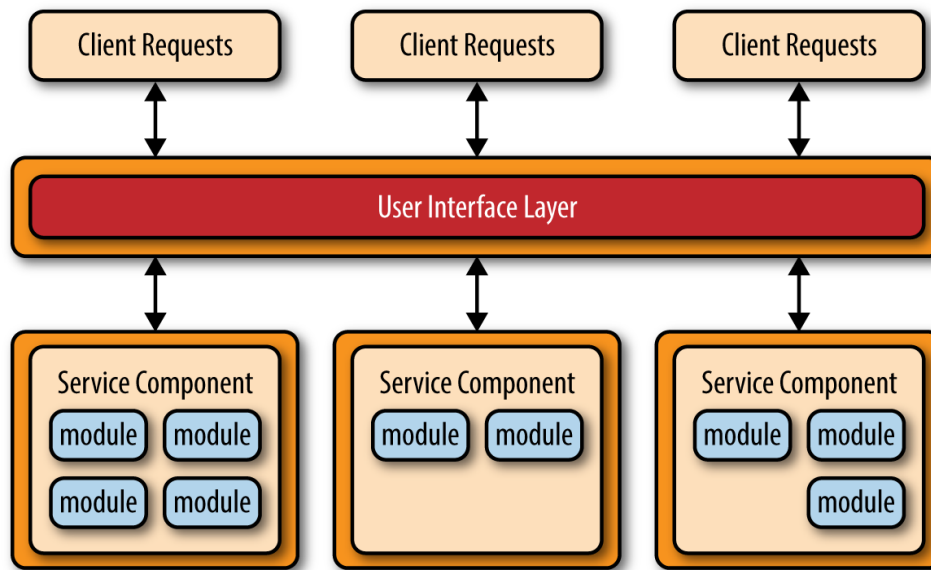


Figure 13: Typical microservices architecture pattern

The microservices architecture pattern provides scalability, robustness and decoupling. If a service goes down, it will not take out the entire application. Additionally, the services can be scaled independently. Moreover, this architectural style provides the capability of real-time production deployments, thereby significantly reducing the need for the traditional monthly or weekend “big bang” production deployments. Finally, it should be stated that one of the major challenges in this architecture pattern is to determine the correct level of granularity for the service components. In particular, too coarse-grained or too fine-grained service components may eliminate the benefits that come with this architecture pattern and increase complexity.

5.2 Mapping requirements to architecture

The combination of an early understanding of requirements (both functional and non-functional) along with an appropriate choice of the architectural style, that will most effectively satisfy these requirements, is a key factor for the successful deployment of a large scale software project. Mapping requirements to a system architecture refers to a formal procedure that takes as input both the functional (expressed by the defined use cases) and the non-functional requirements, and provides as output the system architecture components organized into a particular structure based on a specific architectural style. The choice of architectural style can often constrain certain requirements fulfilment, while practical and comprehensive mappings do not always exist. In addition, many proposed solutions for implementing this process focus mainly on the non-functional (e.g. quality), rather than the functional requirements of the system. In order to fulfil the defined requirements of the MyCorridor system, the following system architecture components were defined:

- **Mobile Application:** The front-end module of the MyCorridor system architecture used by the travellers. Through this application, the travellers get access to the MyCorridor platform.
- **Web Application:** Front-end applications through which both the service providers and the MaaS aggregators get access to the MyCorridor platform. In particular, the web application used by the service providers is the Service Registration Tool (SRT), and the one used by the MaaS aggregators is the MaaS Aggregator Dashboard.
- **Trip-Planner:** Hybrid multimodal trip-planner.

- **Matchmaking Module:** The system architecture component responsible for matching the traveller's requests with the MaaS offerings that exist in the MyCorridor platform, namely the several types of services.
- **Multi-criteria Search Module:** The system architecture component responsible for retrieving services according to different user search criteria (e.g. transportation module, type of mobility product, etc.).
- **MaaS Product Synthesis Module:** The system architecture component responsible for supporting the generation of new services from the MaaS aggregator as the result of synthesis/combination of two or more different services.
- **Traveller Feedback Module:** The system architecture component responsible for integrating the travellers' feedback, regarding either the individual services or the overall MaaS packages, into the MyCorridor platform.
- **Big Data Management Module:** The system architecture component responsible for the provision of data analytics services that produce useful insights regarding the usage of the MaaS services.
- **Business Rules Implementer Module:** The system architecture component responsible for providing the necessary functions to the service providers and the MaaS aggregator for viewing, modifying and validating the business rules of the individual services and the overall MyCorridor platform, respectively.
- **Payment Module:** The system architecture component responsible for the payment of the different service providers through VivaWallet's payment services, as well as, the integration with the back-office systems of the underlying service providers, in order for the traveller to be able to select, pay and receive the desired mobility service.
- **MaaS API:** The stable, robust, efficient and secure RESTful API that is responsible for the communication and interaction between all the system architecture components, as well as for the communication between the overall MyCorridor platform and external modules (e.g. Traffic Management Services Aggregator).
- **Travellers Data Repository:** The database that holds all data entities related to the traveller.
- **Services Data Repository:** The database that holds all data entities related to the services and the service providers.

The aforementioned system architecture components should be organized into a particular structure based on a specific architectural style. Considering the uses cases of the MyCorridor platform reported in the deliverable D1.1 and the system non-functional requirements reported in section 4, as well as the key design principles and the architectural styles that have been presented above, it was decided that the architectural style that best matches the needs of the MyCorridor platform is **the layered architecture**. Based on the presentation conducted in the previous subsection, the main advantages of the layered architecture pattern are:

- **Components within each layer deal only with the logic of their layer.** For example, components in the presentation layer deal only with the logic of the front-end interfaces, whereas components in the application layer consider only the back-end infrastructure of the system. This *separation of concerns* feature increases flexibility, maintainability and makes the system easily scalable.
- **Components can be reused by multiple applications.** For example, a mobile interface could be used instead of a web browser by simply replacing the user interface (UI) component in the presentation layer. Considering that layers are independent, there are no further changes required in the other layers.
- **Layered architecture allows different kind of development teams to focus on a specific layer with minimum dependency between them.** Hence, ease of development is enhanced,

making it easy to add new layers with additional functionality or replace existing ones without affecting other parts of the system.

- **Each layer relies only on the features and services offered by the layer that lies beneath it.** Therefore, each layer is isolated and can be tested regardless of the rest. In addition, different levels of security can be configured on different layers.

The architecture of the MyCorridor platform was designed taking into account all the aforementioned advantages of the layered architecture pattern and the result is presented in Figure 14. The matching between the use cases and the defined system architecture components is presented in Table 20.

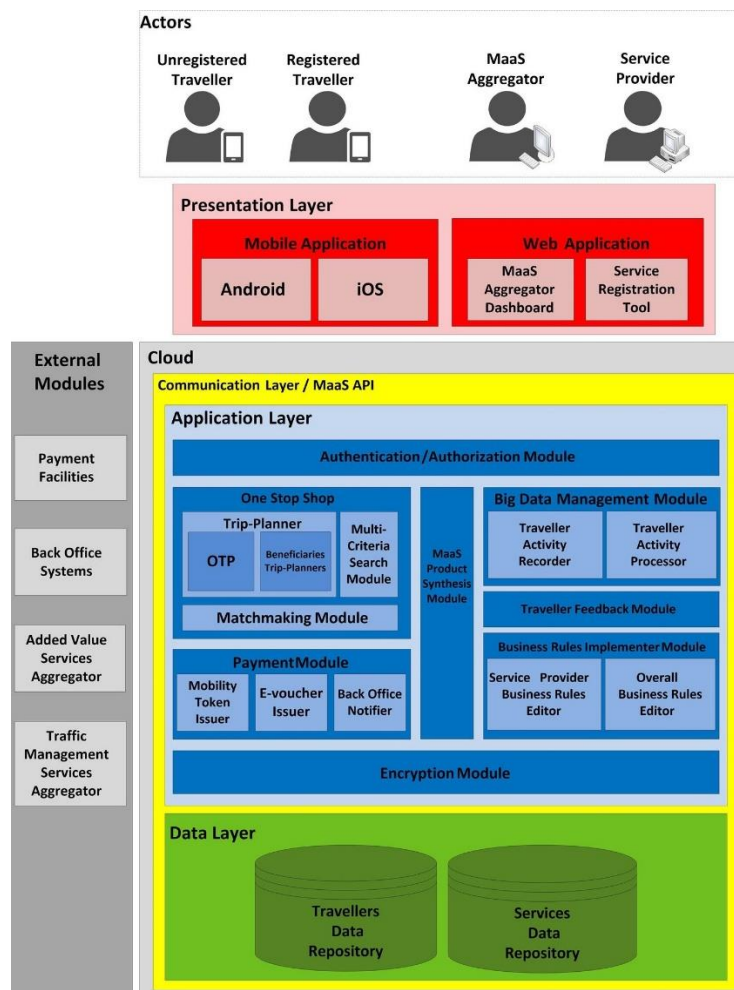


Figure 14: MyCorridor conceptual architecture

Table 20: Matching of the define system architecture components with the use cases

Use Cases	Layer/Module
T1. User Login/Register/Authentication	Presentation/Mobile Application Communication/MaaS API Application/Authentication-Authorization Module, Encryption Module

Use Cases		Layer/Module
		Data/Travellers Data Repository
T2. Static & semi-dynamic profiling		Presentation/Mobile Application Communication/MaaS API Data/Travellers Data Repository
T3. Personalized MaaS package configuration, purchase & redemption	Ad-hoc with trip planner (in case of trip planning selection)	Presentation/Mobile Application Communication/MaaS API Application/Trip-Planner, Matchmaking Module, Payment Module, Big Data Management Module, Traveller Feedback Module Data/Travellers Data Repository
	Ad-hoc without trip planner, MaaS Product Synthesis Module	Presentation/Mobile Application Communication/MaaS API Application/ Multi-Criteria Search Module, Matchmaking Module, Payment Module, Big Data Management Module, Traveller Feedback Module Data/Travellers Data Repository
T4. Personalized Info support (added value services – athletic, touristic, cultural, health push personalized notifications)		Communication/MaaS API Application/Matchmaking module
T5. Change/Cancellation		Presentation/Mobile Application Communication/MaaS API Data/Travellers Data Repository
T6. Traveller feedback		Presentation/Mobile Application Communication/MaaS API Application/Traveller Feedback Module Data/Travellers Data Repository
T7. Loyalty scheme (encompassing incentivisation & rewarding)		Presentation/Web Application Communication/MaaS API Application/Business Rules Implementer Module Data/Services Data Repository

Use Cases	Layer/Module
S1. Service provider logs in	Presentation/Web Application Communication/MaaS API Application/Authentication-Authorization Module Data/Services Data Repository
S2. Service registration	Presentation/Web Application - Service Registration Tool Communication/MaaS API Application/Business Rules Implementer Module Data/Services Data Repository
S3. Service provider business rules editing	Presentation/Web Application Communication/MaaS API Application/Business Rules Implementer Module Data/Services Data Repository
B1. Overall business rules editing	Presentation/Web Application - MaaS Aggregator Dashboard Communication/MaaS API Application/Business Rules Implementer Module Data/Services Data Repository
B2. Added Value Synthetic	
B3. Clearance with the traveller and the service providers (e-vouchers)	Presentation/Mobile Application Communication/MaaS API Application/Payment Module Data/Travellers Data Repository
B4. Mobility Token Issue and redemption (use/validation)	Presentation/Mobile Application Communication/MaaS API Application/Payment Module Data/Travellers Data Repository
B5. Interactive Traffic Management Plan	Communication/MaaS API

In section 6, the structural submodules and the characteristics of each of the system architecture components is presented, while in section 7 their interactions that implement the defined use cases are described.

6 Logical Architecture

This section presents the functions, the structural submodules and the characteristics of each of the modules of the MyCorridor platform. For each layer of the system architecture, a detailed description of the corresponding modules is provided.

6.1 Presentation Layer

The presentation layer is responsible for presenting the application content to the end users through appropriate interfaces (e.g. a mobile application, a web page, etc.). Essentially, the presentation layer of an application is the gateway through which the users get access to the services provided by the application. In the MyCorridor platform, the presentation layer contains the two following types of interfaces:

- Mobile application for the travellers. For a traveller, who is always on the move, this was a natural choice. There are two different versions of the mobile application, one for Android [22] and one for iOS [23] users, where both offer the same set of functionalities.
- Web applications for the service providers and the MaaS aggregator. A service provider can interact with the MyCorridor platform through the Service Registration Tool (SRT), which offers him all the necessary functionalities, e.g. service registration, service editing, service management etc. In addition, the MaaS aggregator dashboard is the interface through which the MaaS aggregator has the full supervision of the platform and can implement the several management functions, e.g. overall business rules editing, service synthesis, etc.

The aforementioned applications are described in the next subsections.

6.1.1 Mobile Application

A mobile application is the front-end module of the MyCorridor system architecture used by the travellers. It provides the user with all the functionality necessary to interact with the platform in an easy and secure way. The mobile application is an autonomous module in the overall MyCorridor system architecture, and communicates with modules in the application and the data layers via the MaaS API. Specifically, the mobile application offers the following functionalities:

- Traveller registration/login to the MyCorridor platform. The traveller can register to the platform by either providing an email and a password, or via social media accounts (e.g. Google, Facebook).
- Set up and modification of traveller profile. Within the MyCorridor platform, a registered traveller sets up a travel profile that contains several preferences like preferred mode of transport or routing preferences. The semi-dynamic parameters of the profile (described in the deliverable D1.1) are updated upon traveller's selection.
- Personalised MaaS package configuration, purchase & redemption. This is the core service of the MyCorridor platform that consists of the MaaS packages, i.e. MaaS&Go and MaaSPacks. The traveller accesses these packages through the mobile application.
- Personalised information (i.e. push notifications). During his trip, the traveller receives in the mobile application notifications regarding traffic management information (e.g. traffic state of

road, road works, incidents etc.) and added value information (e.g. approach to the venue of a concert, recommendation for a restaurant, etc.).

- Evaluation of services. The traveller can evaluate the services s/he selected of each leg of his trip, by providing feedback in the form of numerical value (from 1 to 5 stars) and a short text. In addition, s/he can view other travellers' feedback for the services available on the platform.
- Multiple languages. The mobile application supports many languages.
- Accessibility features. The mobile application was developed considering libraries and tips for providing accessibility support.

Figure 15 presents some screens of the Android mobile application.

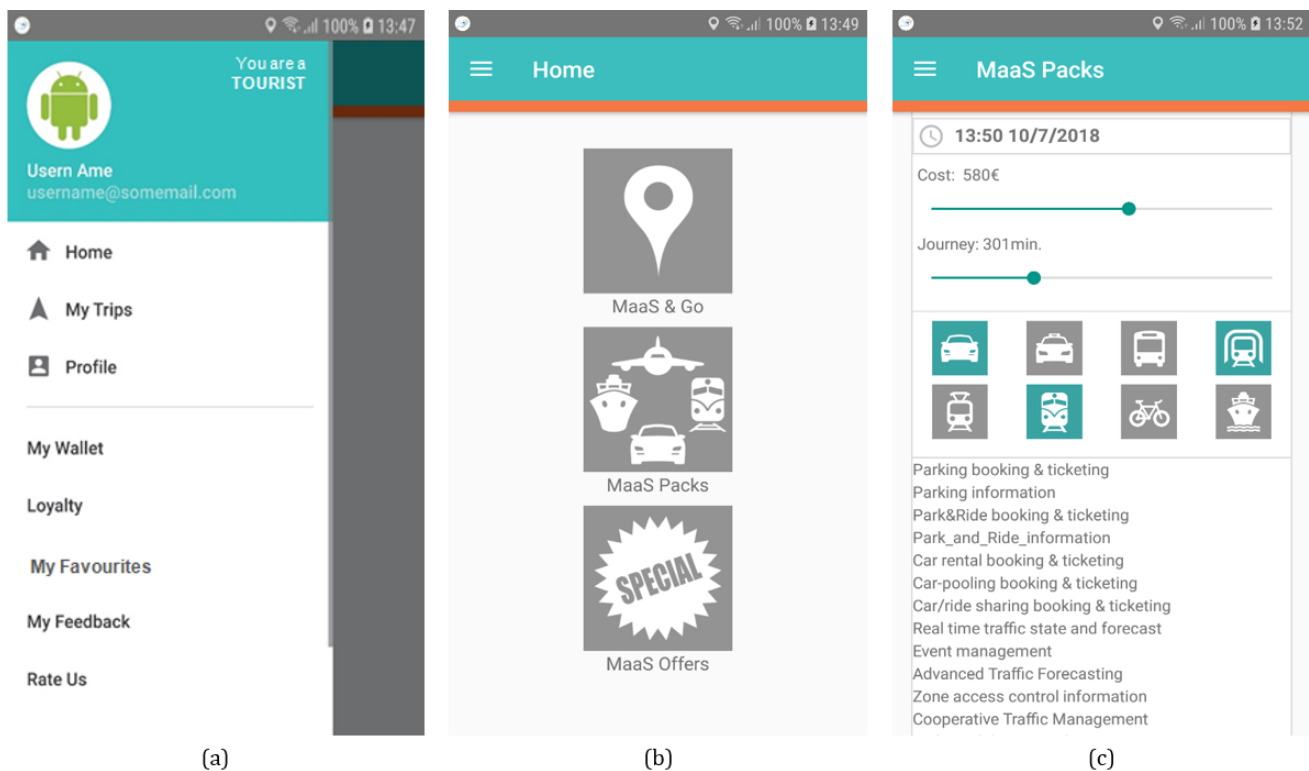


Figure 15: Screens of the MyCorridor Android mobile application

A detailed description of the implementation details of the MyCorridor mobile application has been provided in the deliverable D5.2.

6.1.2 Web Application

The presentation layer of the system architecture contains two separate web applications through which the service providers and the MaaS aggregator interact with the MyCorridor platform. In particular, the service providers interact with the platform through the Service Registration Tool (SRT), while the MaaS aggregator through the MaaS Aggregator Dashboard.

The SRT provides the following functionalities to the service providers:

- Service provider registration and log in.
- Registration of a new service.
- Editing of the attributes of a service.

- View of the registered services.

The SRT was designed with the objective of making the service registration process for the service providers as simple as possible. Some screens of the SRT are presented in Figure 16, Figure 17 and Figure 18.

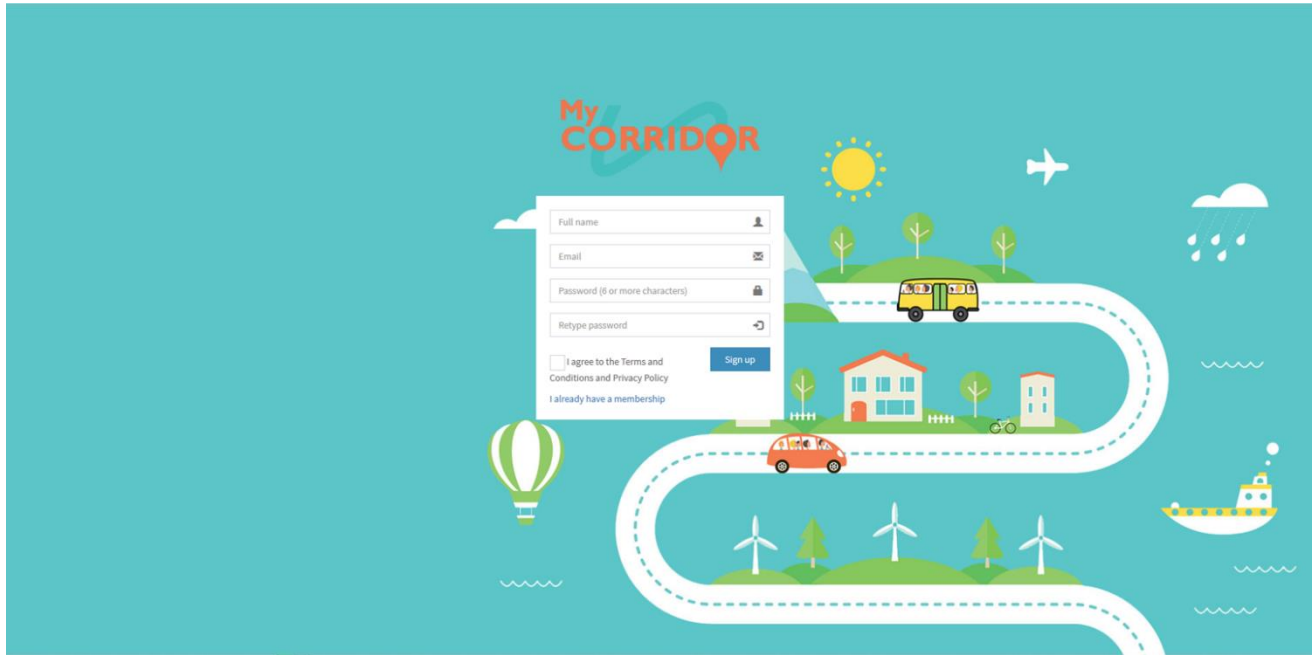


Figure 16: SRT screen – Service provider registration

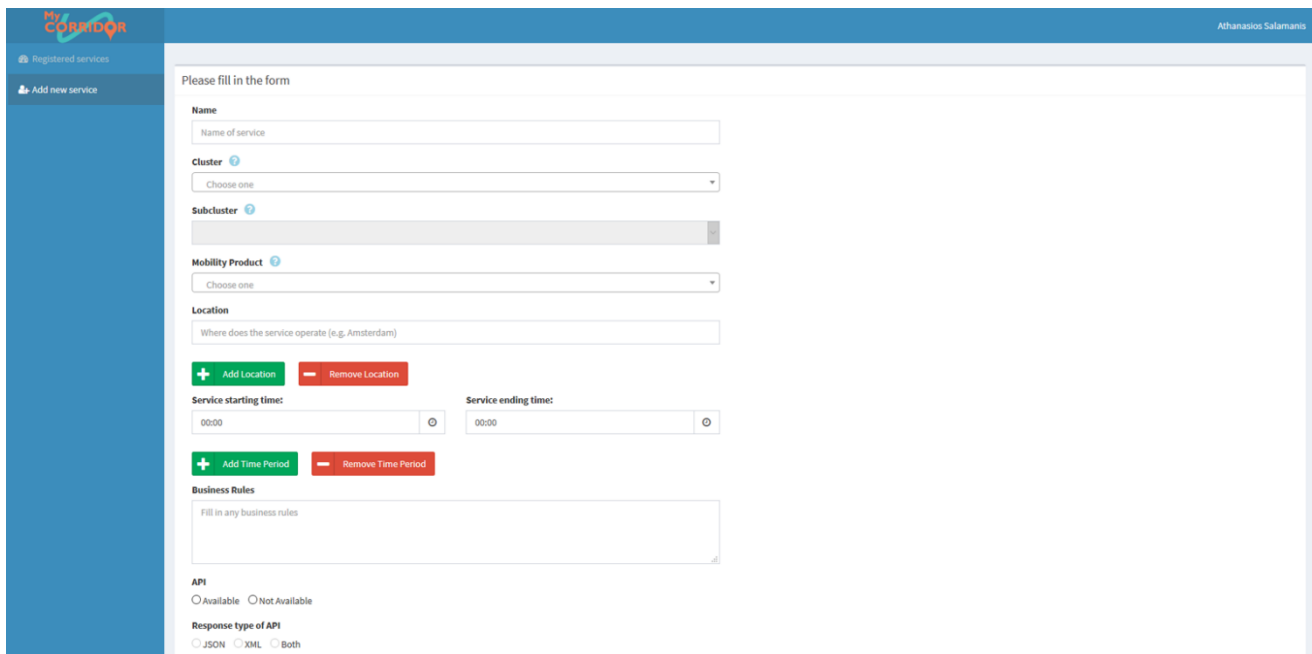
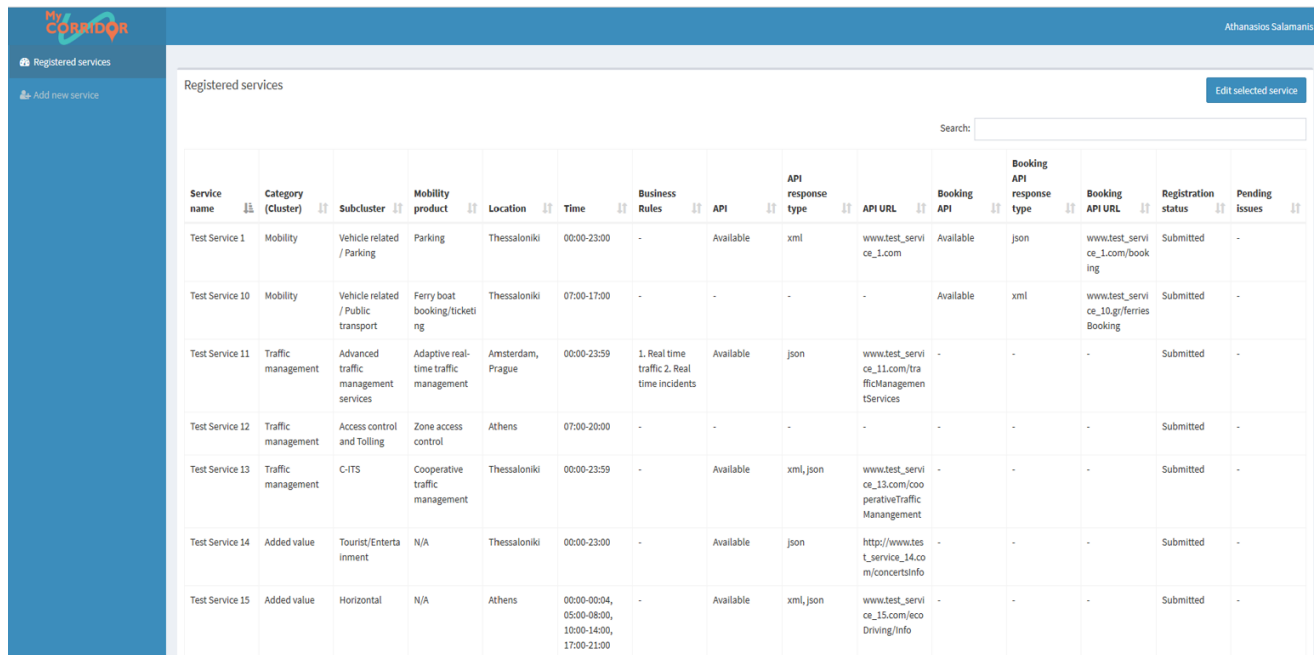


Figure 17: SRT screen – Service registration



Service name	Category (Cluster)	Subcluster	Mobility product	Location	Time	Business Rules	API	API response type	API URL	Booking API	Booking API response type	Booking API URL	Registration status	Pending issues
Test Service 1	Mobility	Vehicle related / Parking	Parking	Thessaloniki	00:00-23:00	-	Available	xml	www.test_service_1.com	Available	json	www.test_service_1.com/booking	Submitted	-
Test Service 10	Mobility	Vehicle related / Public transport	Ferry boat booking/ticketing	Thessaloniki	07:00-17:00	-	-	-	-	Available	xml	www.test_service_10.gr/ferriesBooking	Submitted	-
Test Service 11	Traffic management	Advanced traffic management services	Adaptive real-time traffic management	Amsterdam, Prague	00:00-23:59	1. Real time traffic 2. Real time incidents	Available	json	www.test_service_11.com/trafficManagementServices	-	-	-	Submitted	-
Test Service 12	Traffic management	Access control and Tolling	Zone access control	Athens	07:00-20:00	-	-	-	-	-	-	-	Submitted	-
Test Service 13	Traffic management	C-ITS	Cooperative traffic management	Thessaloniki	00:00-23:59	-	Available	xml, json	www.test_service_13.com/cooperativeTrafficManagement	-	-	-	Submitted	-
Test Service 14	Added value	Tourist/Entertainment	N/A	Thessaloniki	00:00-23:00	-	Available	json	http://www.test_service_14.com/concertsinfo	-	-	-	Submitted	-
Test Service 15	Added value	Horizontal	N/A	Athens	00:00-00:04, 05:00-08:00, 10:00-14:00, 17:00-21:00	-	Available	xml, json	www.test_service_15.com/ecoDriving/info	-	-	-	Submitted	-

Figure 18: SRT screen – Services view

The MaaS Aggregator Dashboard allows the MaaS aggregator to define the overall business rules under which the individual services of each service provider will be provided. In addition, it enables the MaaS aggregator to combine different services, so that they can be provided as a single synthesized service. Specifically, the MaaS Aggregator Dashboard provides the following functionalities to the MaaS aggregator:

- Overall supervision of the platform.
- Definition and modification of the overall business rules that govern the operation of the platform.
- Design and validation of synthesized services.

The home screen of the MaaS Aggregator Dashboard is presented in Figure 19.

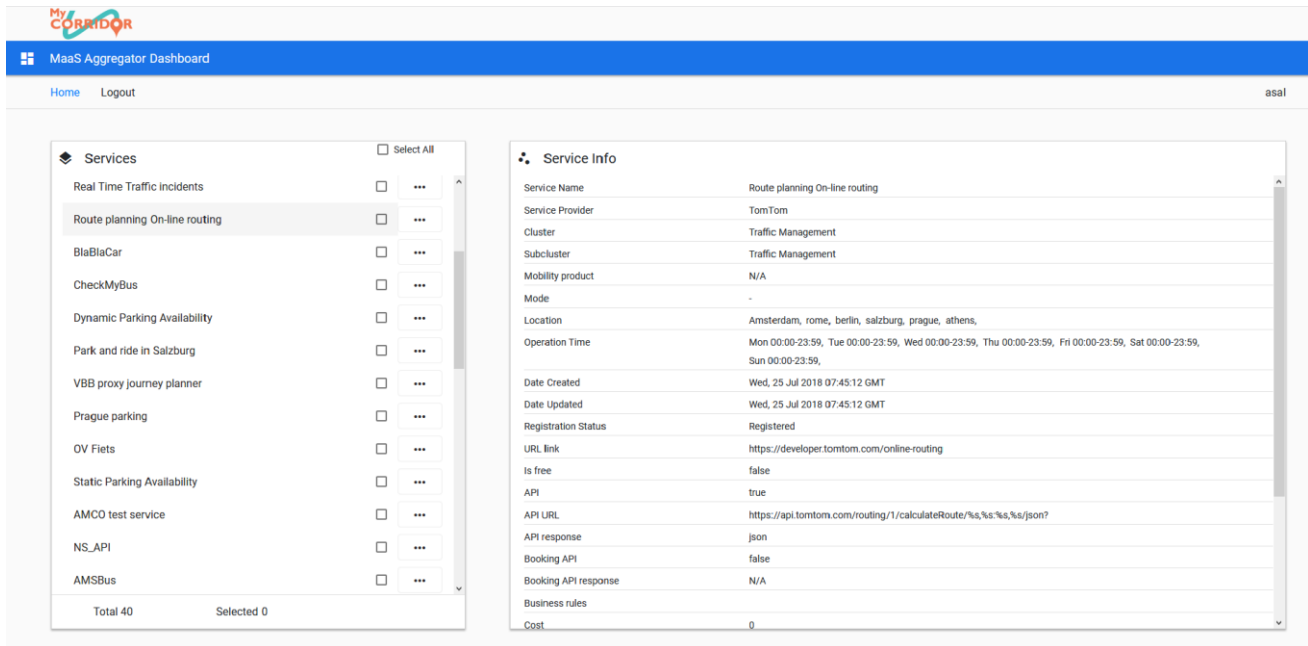


Figure 19: MaaS Aggregator Dashboard home screen

6.2 Application Layer

The application layer contains the business logic of the MyCorridor platform, meaning that the modules of this layer provide the core functions of the platform. A description of each of these modules is provided in the following subsections.

6.2.1 Trip-Planner

The Trip-Planner is responsible for providing itineraries for getting from point A to point B, by combining several transport modes, e.g. bus, car, metro, scooters, bicycles, etc. In the context of the MyCorridor platform, a hybrid trip planning solution was designed and implemented, combining the OpenTripPlanner [24] (OTP - an open source multimodal trip-planner) with commercial trip-planners. In particular, when a trip is requested for an area that is under the coverage of one of the commercial trip-planners, this trip-planner is used. On the other hand, the OpenTripPlanner is utilized for trips that fall out of any of the commercial trip-planners' range. It should be noted that the commercial trip-planners are offered to the MyCorridor platform by some of the partners of the consortium.

The OpenTripPlanner is a multimodal trip-planner, released under the Lesser General Public License (LGPL) [25] license. It is written in the Java programming language and runs on Linux, Windows, Mac, or potentially any platform with a Java Virtual Machine (JVM). OTP uses maps from the public OpenStreetMap [26] repository in order to build a representation of the road network, which is called a 'graph'. In addition, it can use public transport data in the General Transit Feed Specification (GTFS) [27] format to build a representation of the transit network, and adds this representation to the graph as an overlay. An OTP graph specifies every location in the region covered and how to travel between them. The multimodal trips are provided by the trip planning engine, which implements several (Dijkstra-based) trip planning algorithms. Moreover, OTP comes with a built-in web server and the trip planning functionality is provided as a RESTful web service that responds to journey planning requests with itineraries in either the JavaScript Object Notation (JSON) [28] or the Extensible Markup Language (XML) [29] format.

On the other hand, the set of MyCorridor commercial trip-planners comprises the following trip-planners:

- Verkehrsverbund Berlin-Brandenburg (VBB): it covers the Berlin-Brandenburg area.
- Verkehrsverbund Bremen/Niedersachsen (VBN): multimodal trip planner for the Niedersachsen area (Lower Saxony).
- Rhein-Main-Verkehrsverbund (RMV): trip-planner for the Greater Frankfurt area.
- Verkehrsankunft Österreich (VAO): it covers all Austria.
- IDOS leading Czech Republic trip-planner.

The VBB, VBN, RMV and VAO trip-planners are part of the HaCon systems and share a common interface. The VBB, VBN and RMV operate in Germany, while the VAO operates in Austria. Their trips are provided as RESTful services via the HAFAS REST API. The MyCorridor hybrid trip-planner implements read-only requests to this API with multiple get parameters in order to specify the requested journey planner information. The response of each request is delivered in either the XML or the JSON format.

The IDOS trip-planner is the leading trip-planner in Czech Republic, and it is offered to the MyCorridor platform by CHAPS. It includes public bus timetables covering approximately 85000 trips from 302 operators. In addition, it includes rail transport timetables covering approximately 10000 trips from 6 operators. Moreover, it includes urban transport timetables from 115 cities, and it covers approximately 478000 European trips from the MERITS exchange system.

The UML component diagram of the Trip-Planner is presented in Figure 20. A complete description of the MyCorridor Trip-planner will be provided in the deliverable D4.1.

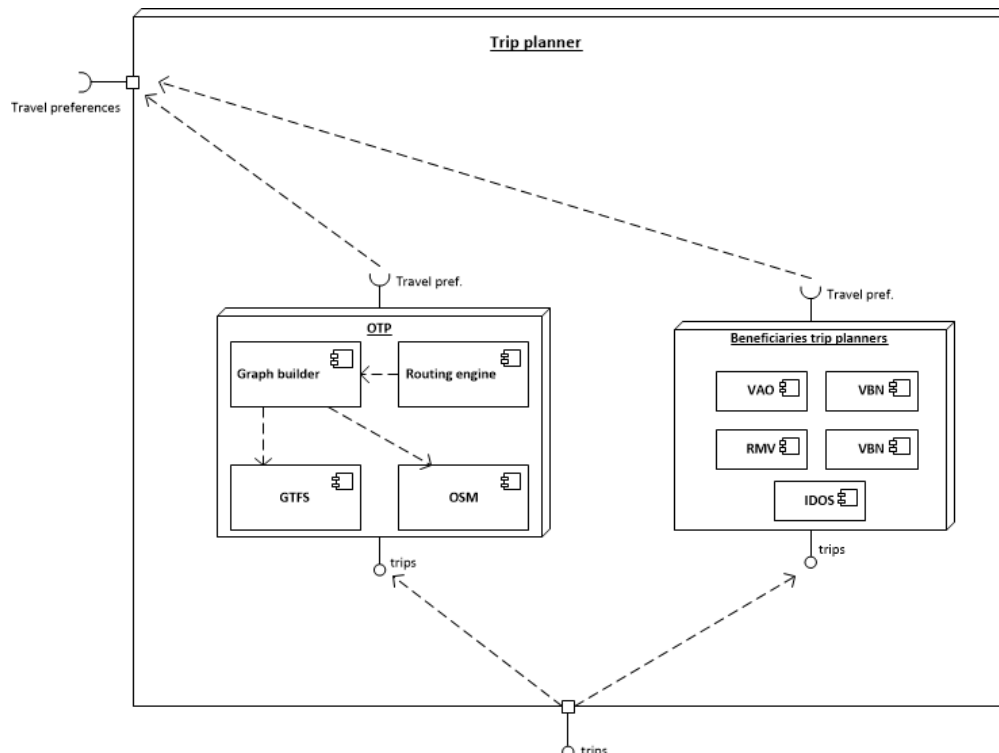


Figure 20: UML component diagram of the Trip-Planner

6.2.2 Matchmaking Module

The Matchmaking Module is responsible for matching the traveller's requests with the MaaS offerings that exist in the MyCorridor platform, namely the several types of services. In particular, the Matchmaking Module receives as input a traveller request (that may include a trip generated by the trip-planner, or not), and tries to identify those services that meet the characteristics of the request in the best possible way, based on the characteristics of the request itself (e.g. origin, destination, departure date and time, etc.), the characteristics of the traveller that submitted the request (e.g. preferred transportation mode(s), routing preference, possible accessibility issues, etc.), and the characteristics of the services that exist to the MyCorridor platform at the time of the request submission (e.g. mode, type, cluster, subcluster, etc.). The result of the matchmaking process is either a set of services for each leg of the traveller's trip in the MaaS&Go scenario, or one set of services in the MaaS Packs scenario.

The Matchmaking Module is composed of three major components as shown in the corresponding UML component diagram presented in Figure 22. The first component is the Data Receiver, which is responsible for making appropriate RESTful calls to the MaaS API in order to receive the necessary data for the matchmaking process. This component essentially implements a web service client by wrapping the widely used cURL library [30]. The second component is the Data Parser, which parses the data coming from the web services (which is in JSON format) and transforms them into appropriate data structures in order to be processed in the matchmaking process. This module utilizes the RapidJSON [31] library to parse the data. Finally, the third component of the Matchmaking Module, is the Matchmaker which implements the core matching functionality of the module. The Matchmaker is a typical rule-based system (or expert system) whose functionality is based on the specific set of rules (i.e. *rule base*) that specify the way in which the services are selected. For example, one rule of the matchmaker's rule base is that the origin and the destination points of the traveller should fall into the working area of a service, in order for this service to be selected. The choice for implementing the Matchmaker as an expert system, (rather than, for example, as a machine learning system) was derived, on one hand, by the desired flexibility that the matchmaking module should have in order to satisfactorily cover the characteristics of the different services, and on the other, by the lack of reliable ground truth regarding the way in which the MaaS offerings should be matched to the traveller's needs. The Matchmaker is implemented as a custom, native C++ application. A complete description on how the Matchmaking Module works will be provided in the deliverable D3.1.

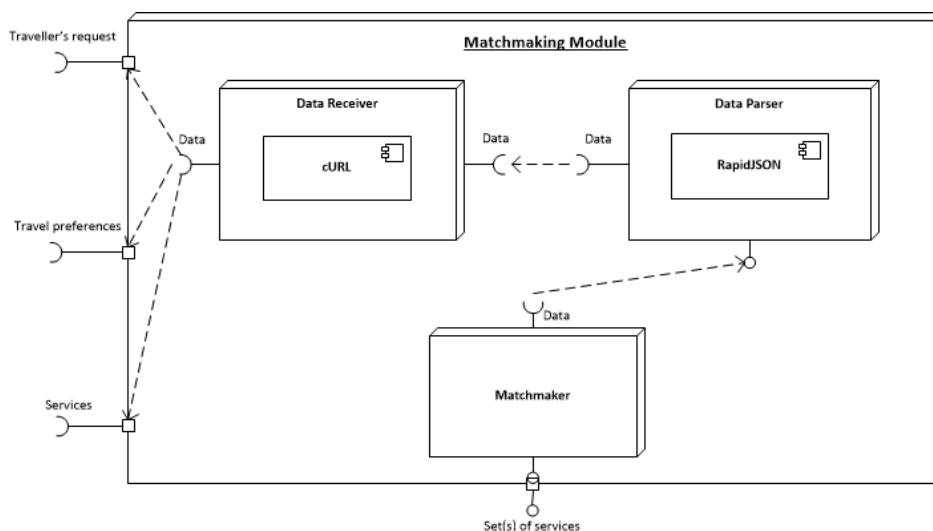


Figure 21: UML Component diagram of the Matchmaking Module

6.2.3 Multi-Criteria Search Module

The Multi-Criteria Search Module is responsible for retrieving services according to different user search criteria. These criteria encompass features such as transportation mode, type of mobility product and journey time. A traveller enters as input one or more of these values, and the Multi-Criteria Search Module finds the services that match the required characteristics. The Multi-Criteria Search Module essentially implements a set of filters, namely comparisons between the traveller's input and the characteristics of the services registered in the MyCorridor platform. This module is implemented as a custom, native Python application. A complete description of the Multi-Criteria Search Module will be provided in the deliverable D4.1.

6.2.4 MaaS Product Synthesis Module

The MaaS Product Synthesis module is responsible for supporting the generation of new services from the MaaS aggregator as the result of synthesis/combination of two or more different services, e.g. a parking availability information service combined with trip planning to motivate the traveller not to use his private car in places where there is no parking availability or parking products and vehicle sharing products in the same area bundled, providing specific advantageous conditions (i.e. on discount). The functionality of the service synthesis can be used by the MaaS aggregator for promotional activities and incentives such as combining less popular products with more popular ones (at lower cost), so as to promote the use of the first; or combination of products with higher green footprint at lower cost for promoting environmentally friendly behaviour/choices. The services that will be created through this process will be tagged as "synthetic added value services".

In particular, the MaaS aggregator can select pairs of registered services through the MaaS aggregator dashboard. At this point, the MaaS aggregator will be supported with analytics for mobility product popularity and usual combination of products by the users so as to have a better view of the use of the registered services in his platform. Accordingly, the MaaS Product Synthesis module will evaluate the compatibility of the business rules among the products (e.g. available services in a common area, common hours of availability, etc.) using the following set of rules (i.e. rule-based system):

For time compatibility, some of the operating hours need to overlap. In order to validate the time compatibility, the following conditions are checked:

- The starting time of the first service is before the ending time of the second service, and
- The ending time of the first service is after the starting time of the second service.

This formula is derived from DeMorgan's laws in boolean algebra.

Location compatibility is accordingly confirmed when the locations of the selected services overlap. In order to check location compatibility, for every possible pair of locations (when there is more than one locations that the service is available), overlapping areas of the bounding boxes (that are provided when fetching the services from the server) are investigated. If at least one overlapping area is identified, it is enough and the services are considered to have compatible locations. To do so, the following conditions are checked:

- The minimum latitude of location A is lesser than the maximum latitude of location B,
- The maximum longitude of location A is greater than the minimum longitude of location B,
- The minimum longitude of location A is lesser than the maximum longitude of location B and
- The maximum longitude of location A is greater than the minimum longitude of location B.

If all these conditions hold true, it means that the locations overlap.

Assuming that the services are compatible, the service registration form is provided to the MaaS aggregator pre-filled with the common (among the selected services) business rules. The MaaS aggregator may then re-fine the pre-filled information and proceed to the generation of the new synthetic added value service. The new service and the respective rules are accordingly stored in the Services Data Repository.

In terms of software development, service synthesis is based on Angular [32], i.e., a popular framework that utilizes HTML, CSS and TypeScript [33] (a JavaScript [34] superset), often used to create web applications. In the provided implementation, we are using Bootstrap [35], jQuery [36] libraries and the Google Places Autocomplete API [37]. The RESTful API under the link <http://83.212.109.136:4200/service-info> can be used in order to call for the specific functionality.

6.2.5 Traveller Feedback Module

The Traveller Feedback Module is responsible for integrating the travellers' feedback, regarding either the individual services or the overall MaaS packages, into the MyCorridor platform. In general, the module is responsible for:

- Providing other traveller's feedback options. This is because, a detailed screen per leg of the trip is shown to the traveller including information from other travellers regarding the MaaS services used in the past.
- Receiving traveller's feedback from the mobile application.
- Retrieving data from the data layer that are going to be used for computing the ranking values of the services.
- Validating and transforming the data received by the mobile application in a proper data format in order to be used for computation purposes and data exchange with the data layer.
- Compute the overall MaaS platform ranking values and/or the services ranking values, by taking into account the previous ranking values and the traveller's feedback and combining different factors (that are part of the feedback) like comfort, routing preferences etc.
- Sending the traveller's feedback and the corresponding service rankings to the data layer.

The module is composed of three major components as shown in the corresponding UML component diagram presented in Figure 22. The first component, entitled Feedback Input/Output Gateway, is a web service responsible for receiving the traveller's feedback. Moreover, this component is responsible for sending and retrieving data from the modules forming the data layer. More precisely, the module sends the computed service ranking that has been received by the service ranking component and the traveller's feedback to the data layer. The component is also responsible for providing other travellers' feedback to the service layer in order to be used by the traveller. The design and implementation of the web service is based on the REST architecture. The second component, entitled Feedback Assessment, is responsible for validating the data received by the mobile application. Moreover, this component transforms the data in a data format suitable for data exchange with the other components of the module and the modules of the data layer. Regarding the data exchange, the module uses the JSON format. The third component, entitled Service Ranking, contains an algorithm for computing the rankings of the services but also the ranking of the overall MaaS service experience. The algorithm is a weighted algorithm that uses the traveller's feedback, the traveller's preferences and the previous rankings in order to compute the new rankings. A complete description of the Traveller Feedback Module is provided in the deliverable D3.2.

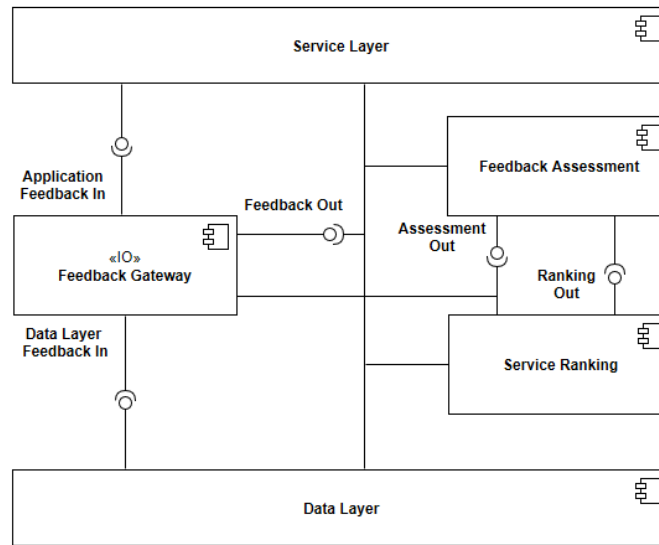


Figure 22: UML component diagram of the Traveller Feedback Module

6.2.6 Big Data Management Module

The Big Data Management Module is responsible for the provision of data analytics services that produce useful insights regarding the usage of the MaaS services. In particular, its main objective is to identify patterns of MaaS products usage by the travellers, within the MyCorridor platform. To this end, the module includes two submodules, namely the Traveller Activity Recorder and the Traveller Activity Processor.

The Traveller Activity Recorder collects all the necessary information needed for the calculation of statistics regarding the way travellers make use of the available services. Practically, this submodule is a set of callback functions, which are triggered right after a traveller completes the purchase of a set of services. These functions extract, collect and store all the data that are then fed into the Traveller Activity Processor.

The Traveller Activity Processor includes all the algorithmic solutions and applies the appropriate big data analytics techniques for the calculation and extraction of statistics and metrics that provide useful insight into travellers' trends towards MaaS products usage. The extracted knowledge can be shared to the service providers (upon agreement, and given the written consent of the travellers) in order to improve their services and adapt more to the user requirements.

The UML component diagram of the Big Data Management Module is presented in Figure 23.

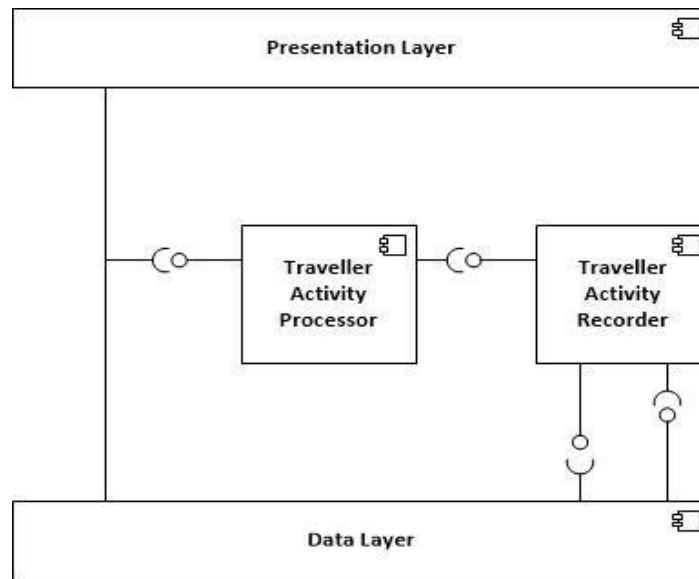


Figure 23: UML component diagram of the Big Data Management Module

6.2.7 Business Rules Implementer Module

The Business Rules Implementer Module is responsible for providing the necessary functions to the service providers and the MaaS aggregator for viewing, modifying and validating the business rules of the individual services and the overall MyCorridor platform, respectively. In particular, each registered service provider can log into the MyCorridor platform through the SRT, and view as well as modify the current business rules of his registered services. The business rules s/he can view and modify are the following:

- A short description of the service.
- Tariffs per service expressed in Euro (€).
- Tariffs covering multiple services of the same service provider expressed in Euro (€).
- Validity times or other special conditions for each tariff.
- Terms and conditions per service.
- Exclusive discounts per service.
- Disclaimer.
- Possible combination of a service with another service provider's mobility service.
- Strategy or promotional method that the service provider would like to allow or forbid to be used for some or all services.

In addition, the MaaS aggregator can log into the MyCorridor platform through the MaaS aggregator dashboard and view, as well as, modify the current business rules overall MaaS platform. Specifically, the MaaS aggregator can view and modify the following business rules:

- Overall business strategy. The MaaS aggregator can select a different overall business strategy in different periods. For example, a strategy that promotes the electric vehicles can be selected for a specific period, and one that promotes the cheapest mobility services for another. The way in which this multiple strategies are implemented within the MyCorridor platform is described in detail in the deliverable D3.1.
- Tariffs and discount policies. The MaaS aggregator can view and modify the rules that govern the tariffs and discount policies through which the services are provided, in order to ensure the fair

promotion and distribution of all services and avoid competition issues between the service providers.

- Loyalty scheme. The MaaS aggregator can view and modify the rules through which the users (travellers and service providers) are rewarded for their participation to the platform.
- Service synthesis rules. The MaaS aggregator can view and modify the rules through which different services (possibly from different service providers) are combined in order to generate a new service.

The Business Rules Implementer Module is composed of three components, as shown in the UML component diagram presented in Figure 24. The first component, entitled Business Rules Viewer, is responsible for retrieving from the data layer the business rules that currently apply to a service or the overall platform, and present them to the corresponding service provider or the MaaS aggregator, respectively. The second component, entitled Business Rules Editor, allows the service providers and the MaaS aggregator to modify the business rules of the services and the overall platform, respectively, and sends these changes back to the data layer for storage. Finally, before sending the data to the data layer, the modifications of the business rules are first passed to the third component, entitled Business Rules Assessor, that verifies their validity and applicability.

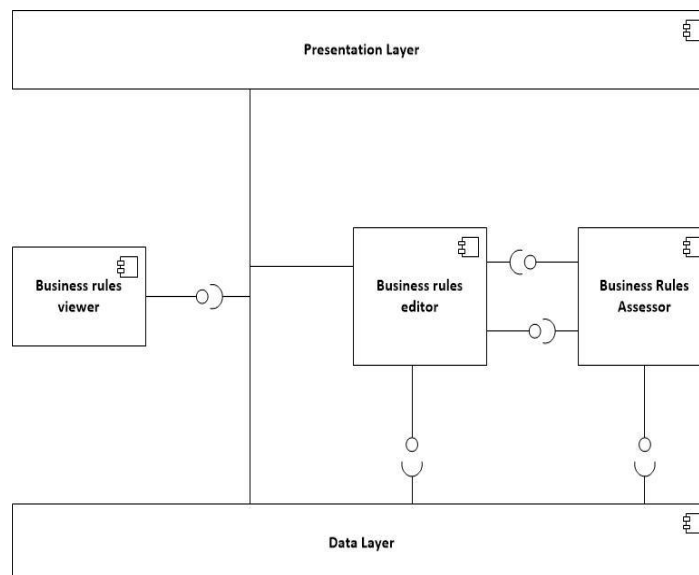


Figure 24: UML component diagram of the Business Rules Implementer Module

6.2.8 Payment Module

The Payment Module is responsible for the payment of the different service providers through VivaWallet's payment services, as well as, the integration with the back-office systems of the underlying service providers, in order for the traveller to be able to select, pay and receive the desired mobility service. The module is composed by three components, namely the E-voucher Issuer, the Back Office Notifier and the Mobility Token Issuer. The E-voucher Issuer provides functionality for payments of mobility services using credit and debit bank cards, through MyCorridor mobile application, while both the Back Office Notifier and the Mobility Token Issuer, implement the appropriate services required for the connection of the MyCorridor platform with the underlying back-office systems of the mobility service providers.

6.3 Communication Layer - MaaS API

The MaaS API handles the data flow within MyCorridor platform and is responsible for the communication between all the system modules, and between the platform and the external modules, e.g. the Traffic Management Services Aggregator. To this end, a well-defined and secure API was designed and implemented based on the REST architecture. As depicted in Figure 25, the MaaS API includes three components. The first component, entitled the Service Orchestrator, manages the data communication flow and maps incoming requests to services. In particular, the role of this component is to send each request, coming either from the presentation or from the application layer, to the appropriate system module. Moreover, it is responsible for sending and receiving data to and from the data layer, as well as for providing all the data required by the presentation layer in order to present information to the end users. All incoming requests from the presentation layer are first evaluated by the second component, namely the Authentication/Authorization Module, and only if they meet the specified authentication and authorization criteria they are passed to the service orchestrator. If a request does not meet the authentication and authorization criteria, it is rejected and an appropriate message appears on the end user's screen (either on the mobile application or on the web applications). Finally, all sensitive data, such as emails and passwords, are first encrypted by the third component of the MaaS API, i.e. the Encryption Module, before the service orchestrator sends them to the data layer.

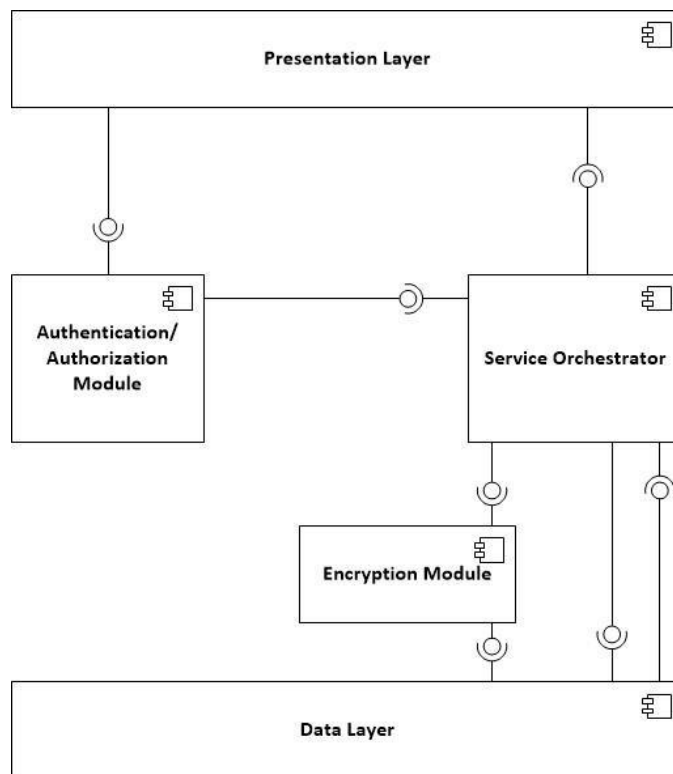


Figure 25: UML component diagram of the MaaS API

6.4 Data Layer

The data layer is the underlying database technology that manages the storage and retrieval of application data. It consists of the Travellers Data Repository and the Services Data Repository, which store data for the two main data entities in the MyCorridor platform, namely the travellers and the services. Moreover, the data layer holds all the other useful information needed by the system modules in order to perform their individual tasks.

6.4.1 Travellers Data Repository

The Travellers Data Repository is the database that holds the data entities of the traveller, the traveller statistics, the traveller picture, the trip and the position of the traveller, and it contains five data collections (i.e. the term collection is used here because this repository is implemented as NoSQL [38] database), respectively. In particular, the User collection contains the data entity of the traveller, the User_statistics collection contains the data entity of the traveller's statistics (namely the data that are related to the purchase activity of the traveller within MyCorridor platform), the User_picture collection contains the data entity of the traveller's picture, the trip collection contains the data entity of the traveller's trip, and the Positions collection contains the data entity of the position of a traveller when s/he is actually travelling (i.e. this information is essential for the integration of TM2.0 concept with MyCorridor platform).

It should be noted that the data entities of the traveller's statistics and picture could be defined within the User collection, but for performance and maintenance reasons it was decided to be defined as a separate collections. Additionally, the sensitive data of the travellers, such as emails and passwords, are encrypted using appropriate hashing algorithms before stored. Therefore, these data is not visible to anyone, not even to the system administrators.

Each traveller may perform one or more trips, while each trip is associated with only one traveller. Therefore, a one-to-many relationship exists between the User data entity and the Trip data entity. Additionally, a traveller can have only one personal picture to the platform, and a picture is associated with only one traveller. Hence, a one-to-one relationship exists between the User data entity and the User_picture data entity. Moreover, there is only one set of statistics for a traveller, and each set of statistics corresponds to a single traveller. This means that a one-to-one relationship exists between the User data entity and the User_statistics data entity. Finally, a traveller passes through many positions during a trip, while a specific position at a specific time is associated with only one traveller. Therefore, a one-to-many relationship exists between the User data entity and the Positions data entity. The UML entity relationship (ER) diagram of the Travellers Data Repository is presented in Figure 26.

6.4.2 Services Data Repository

The Services Data Repository is the database that contains the data entities of the registered services providers, the registered services, the statistics regarding the usage of the services within the MyCorridor platform, and the feedbacks (i.e. numerical ratings and textual comments) related to the services. In particular, the Service_provider collection contains the data entity of the registered service provider, the Service collection contains the data entity of the registered service, the Service_statistics collection contains the data entity that refers to the usage statistics of the corresponding services, and the Feedback collection contains the data entity of the feedback provided for a service. It should be noted that the sensitive data of the registered service providers, such as emails and passwords, are encrypted using appropriate hashing algorithms before stored. Therefore, these data are not visible to anyone, not even to the system administrators.

Each service provider is associated with one or more services, while a service has only one service provider. Therefore, a one-to-many relationship exists between the Service_provider data entity and the Service data entity. Additionally, for a registered service a single set of usage statistics exist, while each set of service statistics corresponds to only one service. This means that a one-to-one relationship exists between the Service data entity and the Service_statistics data entity. Finally, a registered service can receive one or more feedbacks (from the same or different travellers), while a single feedback is associated with only one registered service. Hence, a one-to-many relationship exists between the Service data entity and the Feedback data entity.

The UML entity relationship (ER) diagram of the Services Data Repository is presented in Figure 27.

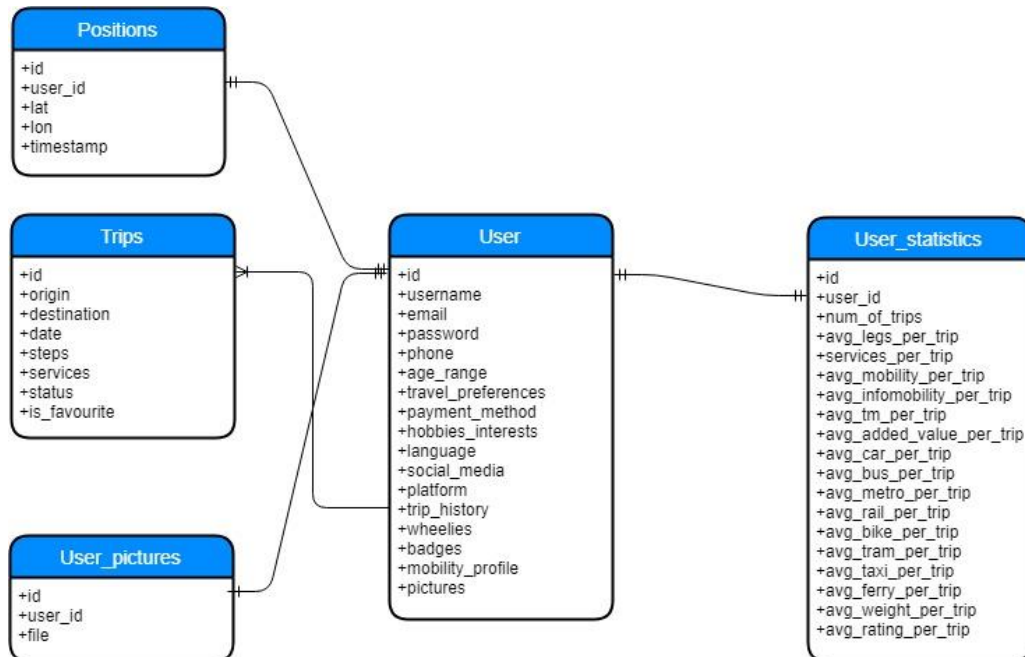


Figure 26: UML entity relationship (ER) diagram of the Travellers Data Repository

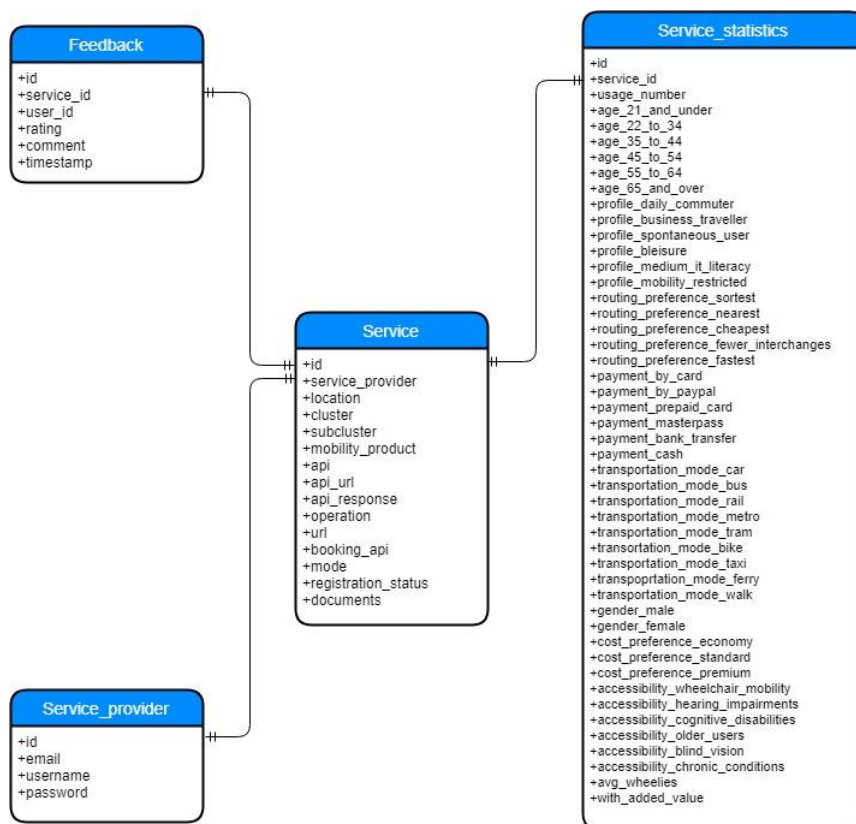


Figure 27: UML entity relationship (ER) diagram of the Services Data Repository

7 Functional Architecture

Since the several modules of the system architecture have been presented and described in section 5, this section presents the functional architecture of the system (i.e. functional requirements), namely the way in which the system modules interact with each other in order to implement the defined, in the deliverable D1.1, use cases. The description of these interactions is presented in a per-use-case fashion, supplemented with appropriate UML sequence diagrams.

7.1 Traveller Use Cases

This section presents the interactions between the system modules that implement the use cases that refer to the traveller, namely the uses cases T1-T7.

7.1.1 T1 - User Login/Register/Authentication

Based on the use case T1, the traveller registration process is carried out as follows. The traveller via his mobile device accesses the MyCorridor mobile application and enter his credentials (i.e. an email and a password). Then, these credentials are transferred from the Service Orchestrator to the Authentication/Authorization Module to be validated (e.g. check for unique email, check for minimum password length etc.). If the validation process is successful, the credentials are transferred to the Encryption Module to be encrypted, and then to the data layer in order to be stored in the Travellers Data Repository. If the validation process fails, a failure message is returned to the traveller.

The traveller login process is implemented as follows. The traveler uses his mobile device to access the MyCorridor mobile application, and enters his credentials. Then, the Service Orchestrator passes the credentials to the Authentication/Authorization Module, which in turn it communicates with the data layer in order to compare the provided credentials with those stored in the Travellers Data Repository. If the compared credentials are the same (i.e. the authentication process is successful), the traveller can access the platform. If the authentication process fails, an appropriate error message is returned to the traveller.

These two processes are depicted in the UML sequence diagram presented in Figure 28.

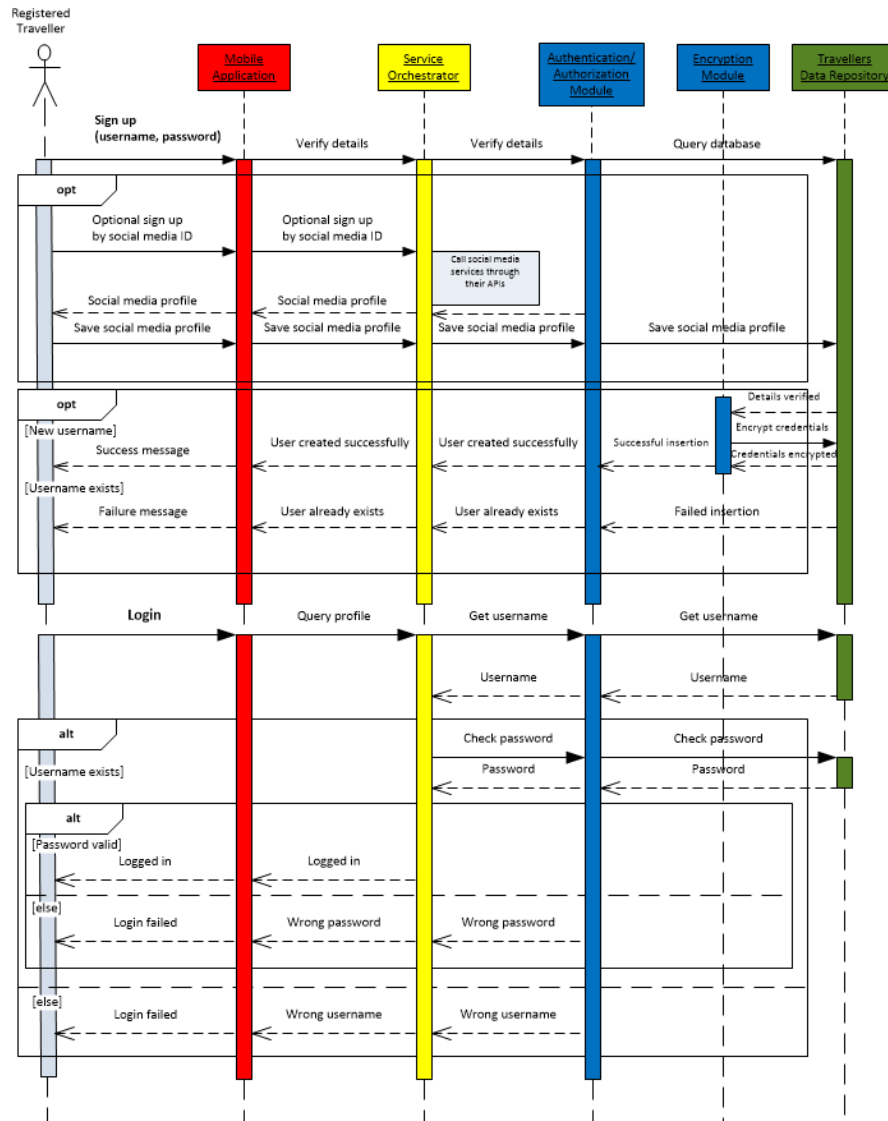


Figure 28: UML sequence diagram of the traveller registration and login process

7.1.2 T2 - Static & semi-dynamic profiling

The traveller can set up and modify his travel profile that includes his travel preferences (defined and reported in the deliverable D1.1). After successful registration, the traveller is able to create his profile by filling in his preferences. Then, s/he is able to view it and modify it further via the mobile application. The static part of the profile includes user information and accessibility preferences, while the semi-dynamic part includes general user preferences and travel preferences. Static information can be changed only by the user whereas semi-dynamic information can be updated while the user interacts with the MyCorridor platform. During this process, the information of traveller's profile are transferred from the mobile application to the Traveller's Data Repository and vice versa, through the MaaS API and in particular through the Service Orchestrator. The UML sequence diagram that describes the process of the static and semi-dynamic profiling is presented in Figure 29.

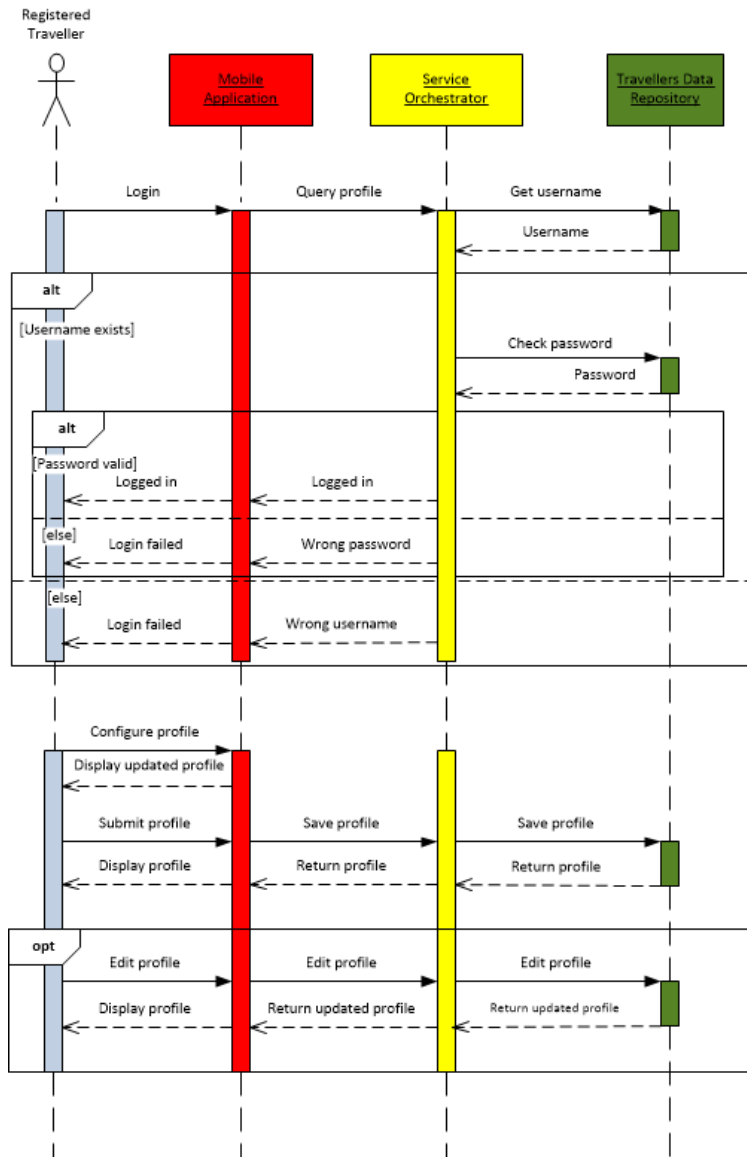


Figure 29: UML sequence diagram of the static and semi-dynamic process

7.1.3 T3 - Personalized MaaS package configuration, purchase & redemption

The use case T3 states that after the traveller has been registered to the MyCorridor platform and set up his profile, s/he can select one of the offered MaaS packages. The two following MaaS packages have been specified:

- **Personalized MaaS package coupled with trip planning (MaaS&Go).** In this case, the trip-planner is used and an ad-hoc matchmaking process provides the applicable mobility products for each leg of the returned trips, based on the availability of services in the one-stop-shop and the traveller profile and preferences.
- **Personalized MaaS package with multi-criteria search (MaaSPacks).** In this package, the traveller selects mobility products by specifying values for different search criteria, while the trip-planner is not used.

In the case of the personalized MaaS package coupled with trip planning, the traveller initially logs into the platform by providing his credentials, and after s/he has been authenticated, s/he makes a trip request that includes a set of requirements (i.e. origin, destination, departure date, mode of transport, etc.). This request is forwarded through the MaaS API to the application layer, and specifically to the Matchmaking Module. The Matchmaking Module initially calls the Trip-Planner to generate multimodal trips. The Trip-Planner receives the trip request from the Matchmaking Module, processes it, and generates a set of multimodal trips that satisfy the traveller's trip requirements. This set of trips includes an optimal trip, in the sense that it is the one that satisfies the requested trip requirements in the best possible way. The set of generated trips is then returned to the Matchmaking Module. After that, the Matchmaking Module requests and receives the traveller's preferences from the Travellers Data Repository via the MaaS API, and the matchmaking process initiates. In particular, a set of services (i.e. mobility, infomobility, traffic management or added value) is assigned to each leg of each of the multimodal trips. The selection of the services is based on the trip requirements, the traveller's preferences and the services' attributes (a complete description of the matchmaking process will be documented in the deliverable D3.1). The generated trips along with the matched services are returned to the traveller's mobile application through the MaaS API. Finally, the traveller chooses the desired combination of trip and services and proceeds with the checkout process.

Regarding the personalized MaaS package with multi-criteria search, the traveller makes again a trip request with specific requirements (e.g. origin and destination), but this time the request is delivered (from the MaaS API) directly to the Matchmaking Module, bypassing the Trip-Planner. Then, the Matchmaking Module identifies the services that satisfy the requirements of the traveller's request with the aid of the Multi-Criteria Search Module. The set of services that best satisfy the traveller's request is delivered to the traveller's mobile application through the MaaS API. Finally, the traveller chooses the desired services and proceeds to the checkout process.

7.1.4 T4 - Personalized Info Support (added value services, athletic, touristic, cultural, health push personalized notifications)

Along with the mobility, infomobility and traffic management services, the travellers can also select added value services (e.g. cultural, touristic etc.) during the MaaS package configuration process. These services are not directly associated with mobility itself and their role is to enhance the overall travel experience. These services are offered to the traveller in two ways. The first is during the MaaS package configuration process, where they are offered in the same way as the other types of services (pre-trip phase). The second way is during the trip itself (on-trip phase) where, provided that the traveller selected added value services during the MaaS package configuration process, s/he receives push notifications in his mobile application that provide information about the selected added value services (e.g. update for the location of a concert, new dinner offer at a restaurant, etc.). These push notifications are triggered either automatically (e.g. when the traveller's distance from the venue of an event becomes less than 3 kilometers) or manually by the traveller through an appropriate selector in the main menu of the mobile application. It is important to stress that the added value services are optional, meaning that the traveller should have given his consent to accept such services (by an appropriate choice in his profile).

The MaaS package configuration process described in the previous section, including the added value services support that described in this section, is schematically depicted in the UML sequence diagrams presented in Figure 30 and Figure 31.

7.1.5 T5 - Modification/Cancelation

After the configuration of the MaaS package, and before proceeding to the checkout process, the traveller has a last chance to modify or cancel it. In particular, the traveller is provided with the option to add or

remove individual services from the MaaS package, and even cancel the selection of the whole package. This process is depicted in the corresponding UML sequence diagram presented in Figure 32.

7.1.6 T6 - Traveller Feedback

The use case T6 refers to functionality of the MyCorridor platform through which the traveller can provide feedback for purchased MaaS packages and individual services included therein. A traveller can provide feedback for a MaaS package either immediately after using it (i.e. after the trip has been completed), or at a later time after having stored the trip information.

In the first case, at the end of the trip a suitable form is presented to the traveller's mobile application, through which the traveller can provide his feedback (a star value and free text) for the MaaS package s/he has just consumed. This feedback is received by the MaaS API that communicates with the data layer in order to store it to the Services Data Repository. Then, the MaaS API delivers the feedback to the Traveller Feedback Module where it is used for updating the ranking values of the services included in the MaaS package to which the feedback refers. Finally, the updated ranking values of these services are stored to the Services Data Repository after being transferred through the MaaS API.

In the second case, at the end of the trip the traveller chooses to ignore the feedback form, and save the trip information instead. The trip information are received by the MaaS API and delivered to the data layer in order to be stored to the Travellers Data Repository. Then, at a later time, the traveller decides to provide feedback for a trip that has taken place in the past. To do this, s/he selects the desired trip from the list of the saved trips in the mobile application and loads the corresponding feedback form (which is the same as the one being presented to the traveller at the end of a trip). The traveller provides his feedback and from this point onwards the process is the same as described above. Finally, it should be noted that the process of viewing the feedbacks of other travellers for particular services is included in the MaaS package configuration process and it does not have its own use case.

The feedback provision process is schematically depicted in the UML sequence diagram presented in Figure 33.

7.1.7 T7 - Loyalty Scheme (encompassing incentivisation & rewarding)

In the context of use case T7, the traveller will be able to get and view the current terms and conditions of the operation of the MyCorridor platform, as well as his loyalty points and rewarding schemes.

In particular, after the traveller has been authenticated and logged into the platform, s/he can select to view the platform's terms and conditions from a suitable selector in the main menu of the mobile application. This request is received by the MaaS API, which communicates with the data layer in order to fetch the terms and conditions data from the MaaS Aggregator Data Repository. These data are then forwarded back to the traveller and presented to the mobile application.

With regard to loyalty points, after the traveller has been authenticated and logged into the platform, s/he can select to view them from a suitable selector in the main menu of the mobile application. This request is received by the MaaS API, which communicates with the data layer in order to fetch the loyalty points from the Travellers Data Repository. These points are then forwarded back to the traveller and presented to the mobile application.

The aforementioned procedures are presented in the UML sequence diagram in Figure 34.

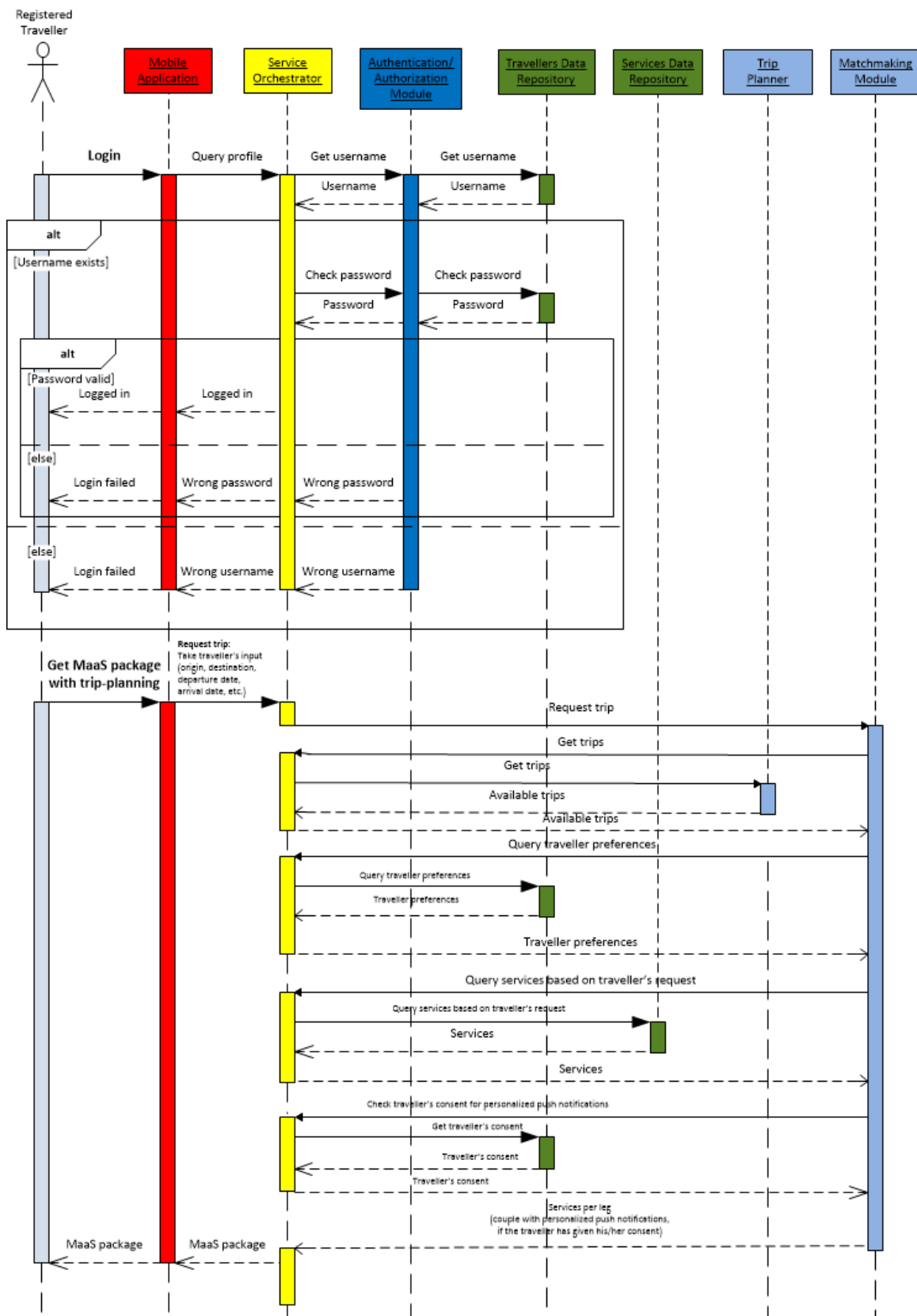


Figure 30: UML sequence diagram of the configuration of the personalized MaaS package coupled with trip planning

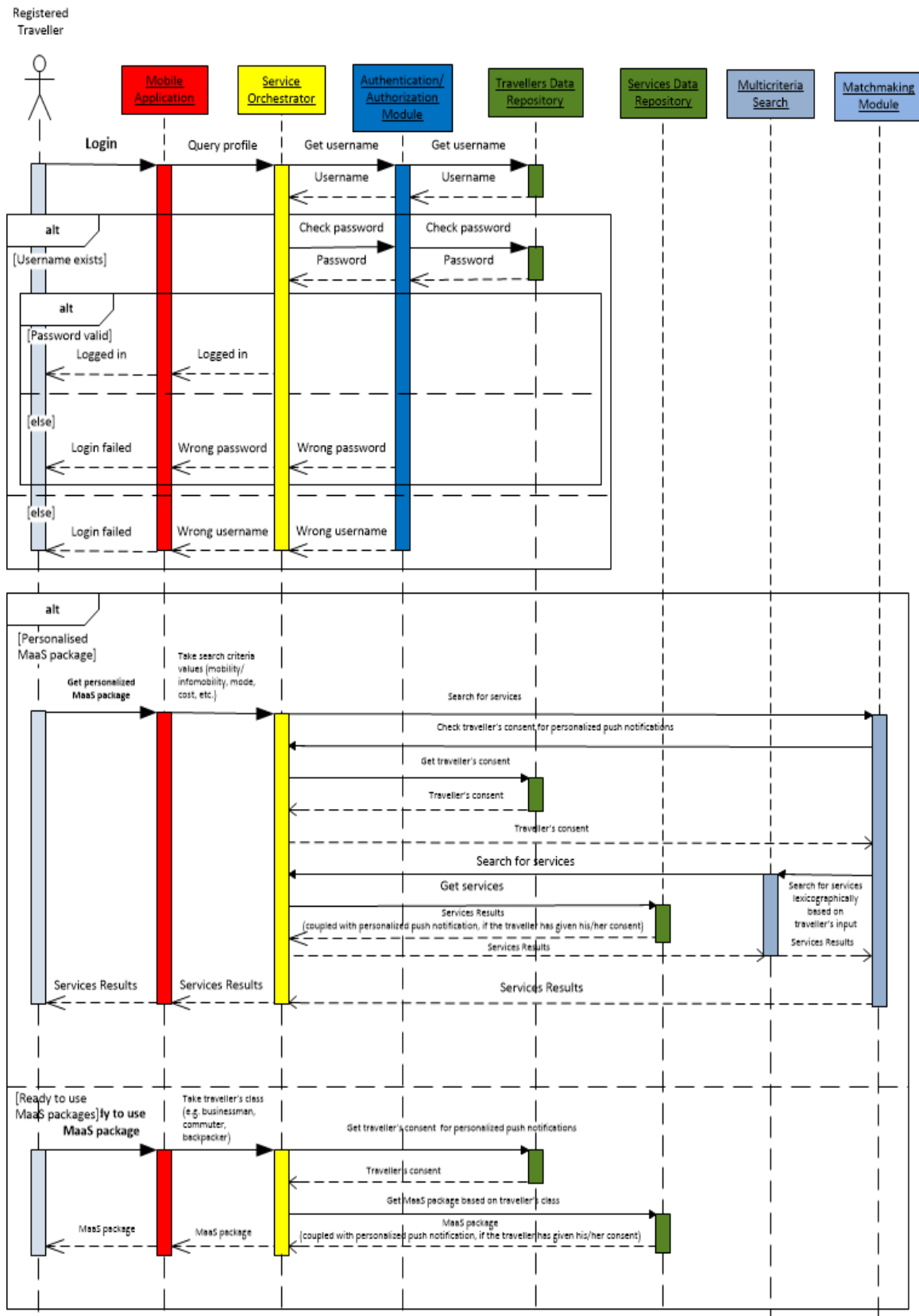


Figure 31: UML sequence diagram of the configuration of personalized MaaS packages with multicriteria search and the ready to use MaaS packages

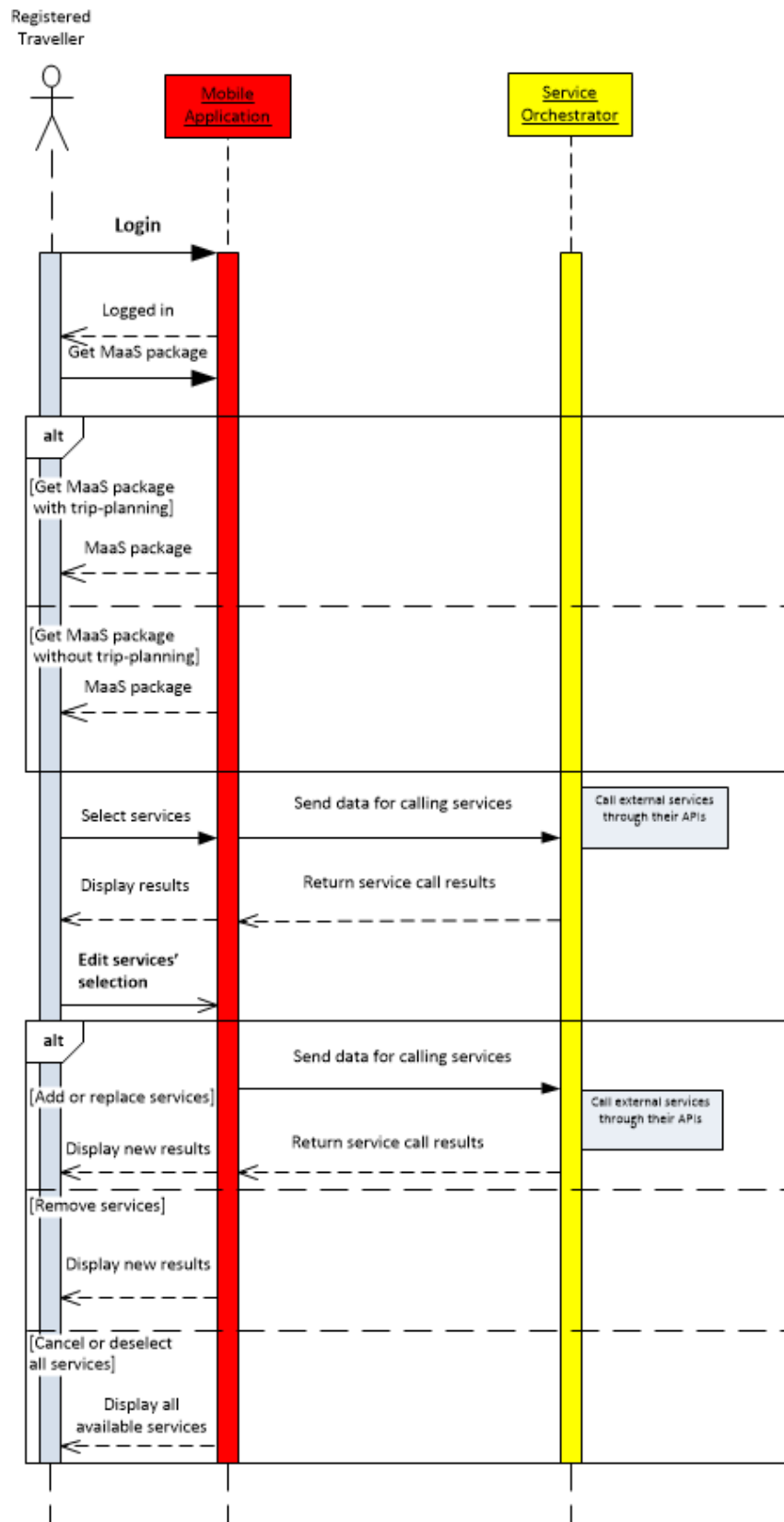


Figure 32: UML sequence diagram of the MaaS package modification/cancellation process

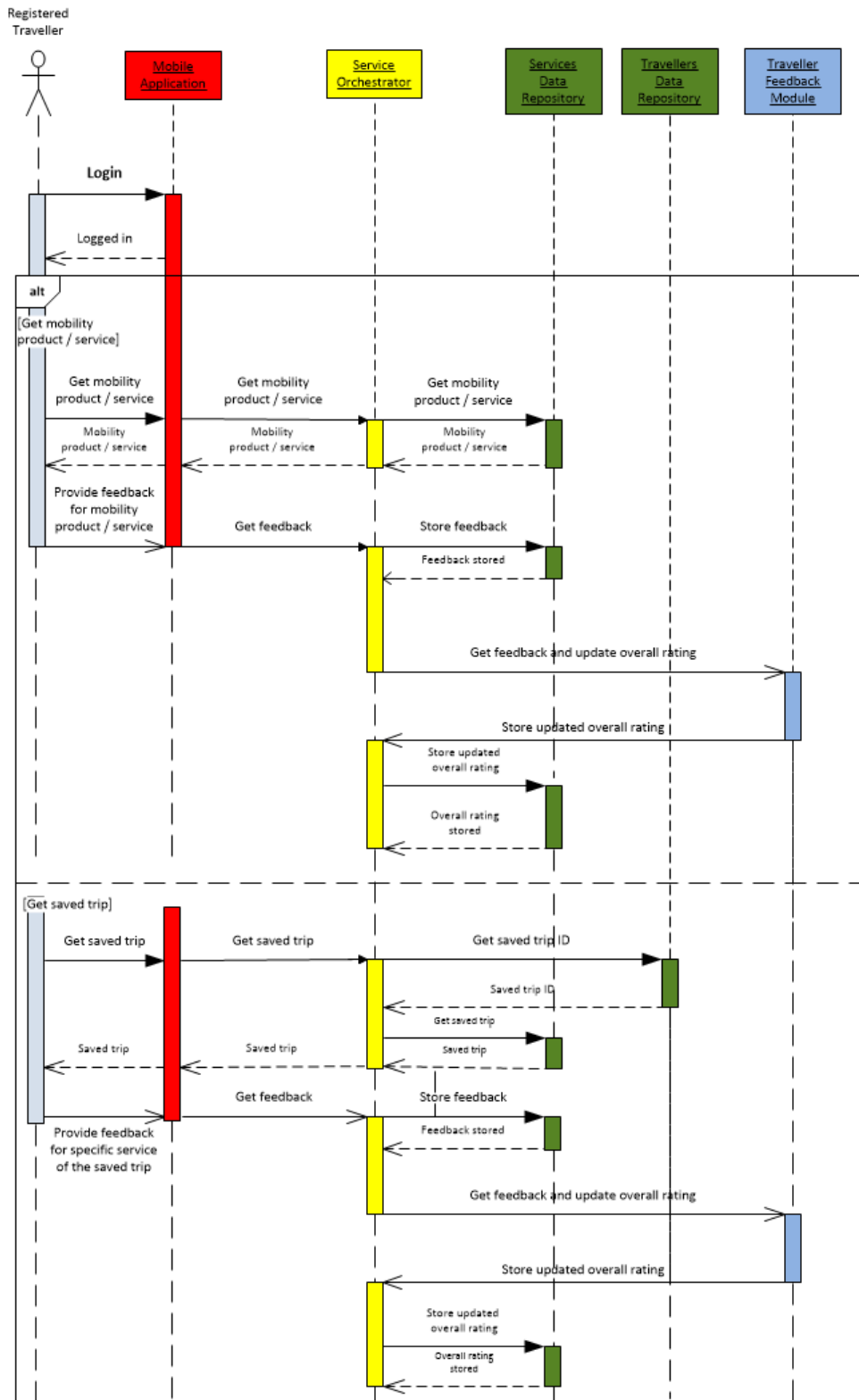


Figure 33: UML sequence diagram of the feedback provision process

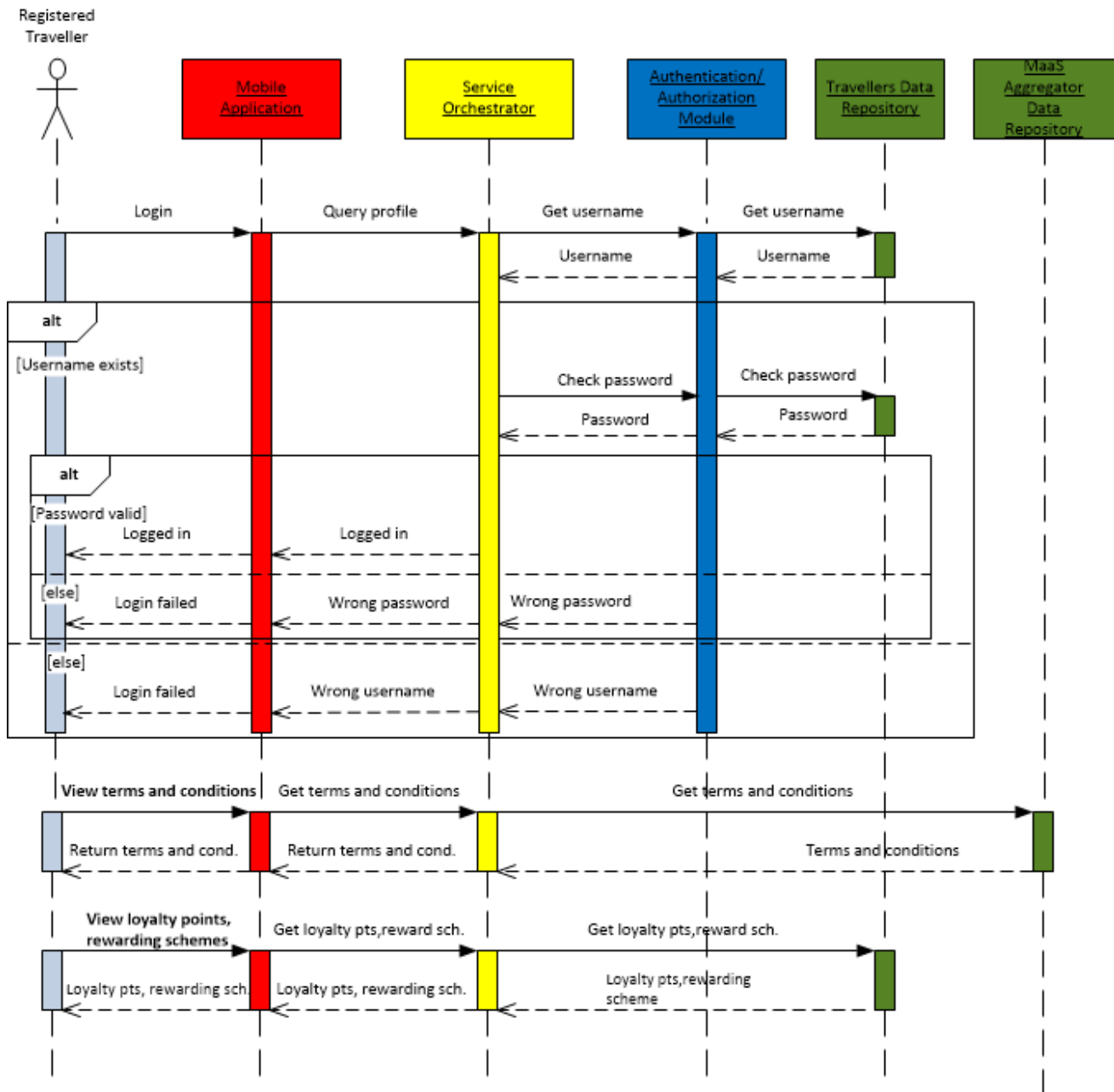


Figure 34: UML sequence diagram of the process of viewing the platform's terms and conditions and the traveller's loyalty points

7.2 Service Provider Use Cases

This section presents the interactions between the system components that implement the use cases referring to the service provider, namely the uses cases S1-S3.

7.2.1 S1 - Service Provider Login

The service provider can access the MyCorridor platform through the SRT, using any device with an Internet connection. In order to register to the platform, s/he gives his credentials (i.e. an email and a password) by completing a suitable form. These credentials are received by the Service Orchestrator and transferred to the Authentication/Authorization Module to be validated (e.g. check for unique email, check for minimum password length etc.). If the validation process is successful, the credentials are transferred to the Encryption Module to be encrypted, and then to the data layer in order to be stored in the Services Data Repository. If the validation process fails, a failure message is returned to the service provider.

After the service provider has been registered to the platform, s/he can log in by providing his credentials. Again, this is done through an appropriate form in the web application, which can be accessed from any device with an Internet connection. The credentials are received by the Service Orchestrator, which passes them to the Authentication/Authorization Module. The Authentication/Authorization Module communicates with the data layer in order to compare the provided credentials with those stored in the Services Data Repository. If the compared credentials are the same (i.e. the authentication process is successful), the service provider can access the platform. If the authentication process fails, an appropriate error message is returned to the service provider.

The service provider's registration and log in processes are depicted in the UML sequence diagram presented in Figure 35.

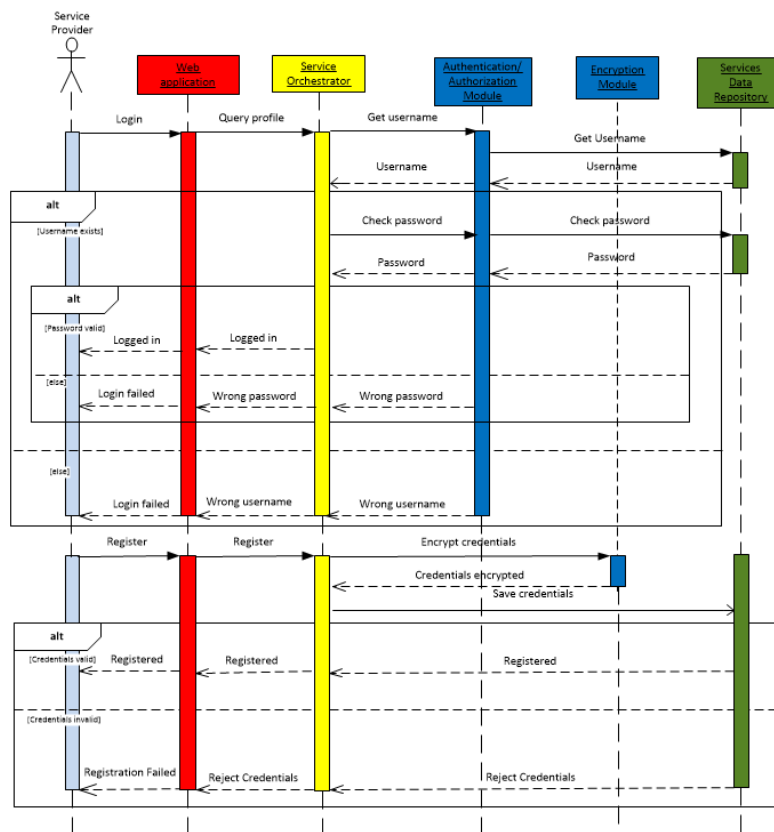


Figure 35: UML sequence diagram of the service provider's registration and log in processes

7.2.2 S2 - Service Registration

The service provider can register a new service (i.e. mobility, infomobility, traffic management or added value) through the SRT. In particular, after logging in to the platform, the service provider registers a new service by filling out a form with the attributes of the service. The completed form is submitted to the platform and received by the Service Orchestrator, which in turn sends it to the data layer in order to be stored in the Services Data Repository. The new service is stored in the Services Data Repository and a success message is returned to the SRT via the Service Orchestrator. This process can only fail if there is already a service in the Services Data Repository (belonging to the same service provider) with exactly the same attribute values. In this case, the service registration process fails and a failure message is returned to the service provider.

The service registration process is schematically depicted in the UML sequence diagram presented in Figure 36.

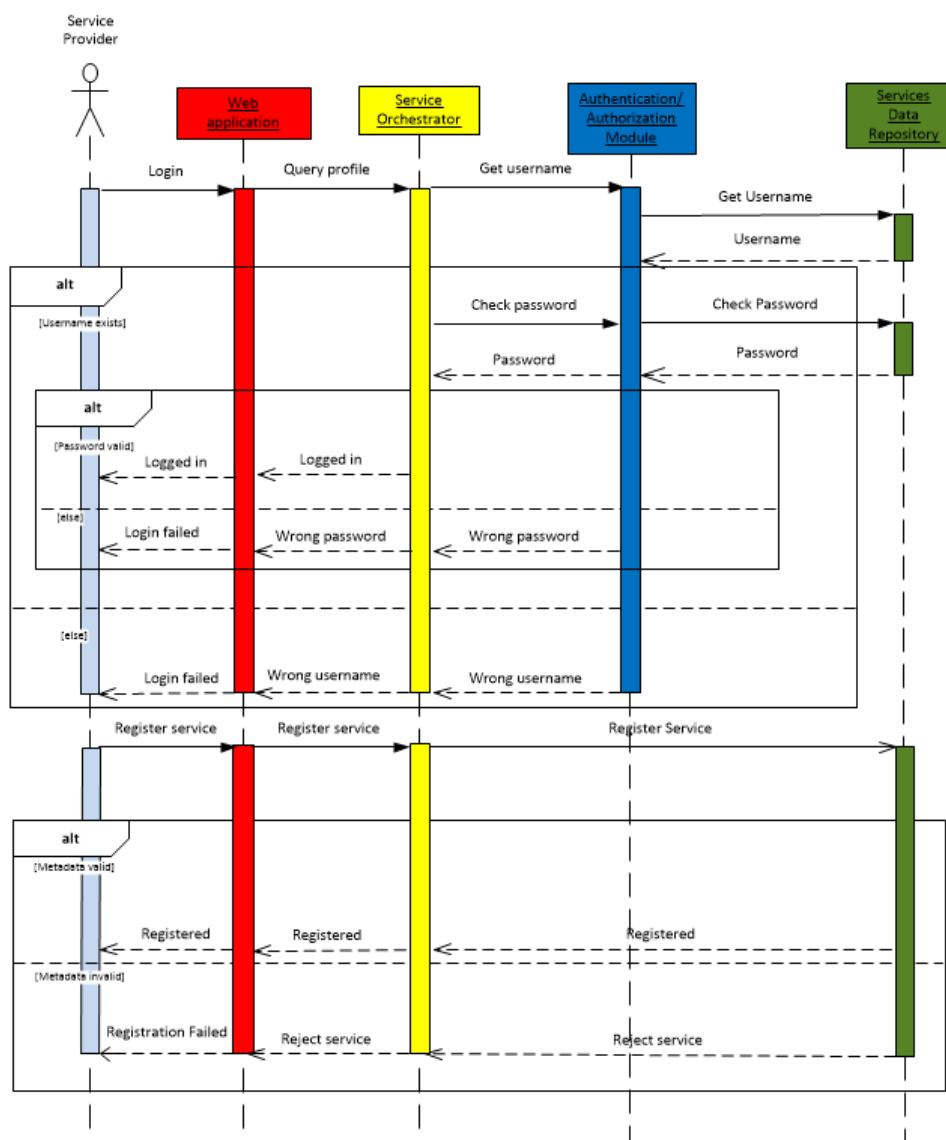


Figure 36: UML sequence diagram of the service registration process

7.2.3 S3 - Service Provider Business Rules Editing

The service provider can modify the business rules of his registered services. To do this, the service provider initially logs in to the MyCorridor platform through the SRT by providing his credentials. Then, s/he browses the list of the registered services and selects the one whose business rules s/he wants to modify. An appropriate form containing the attributes of the service pops up, and the service provider modifies the business rules s/he wants. These business rules include tariffs, offers and discounts for specific types of travellers, working hours, alerts for abnormal events in the typical operation of the service, etc. A complete list of the service business rules set by the service provider will be documented in the deliverable D3.1.

After the modification of the service's business rules, the service with the modified business rules is transferred to the Service Provider Business Rules Editor through the Service Orchestrator. The Service Provider Business Rules Editor evaluates the new business rules and checks if they are compatible with the overall business rules set by the MaaS aggregator. If this is the case, the new business rules are accepted and the modified service is transferred to the data layer through the Service Orchestrator in order to be stored in the Service Data repository. Also, an appropriate success message is returned to the service provider. If the new business rules do not comply with the overall business rules of the platform, the changes are rejected and a failure message is returned to the service provider.

The service business rules editing process is presented in the UML sequence diagram of Figure 37.

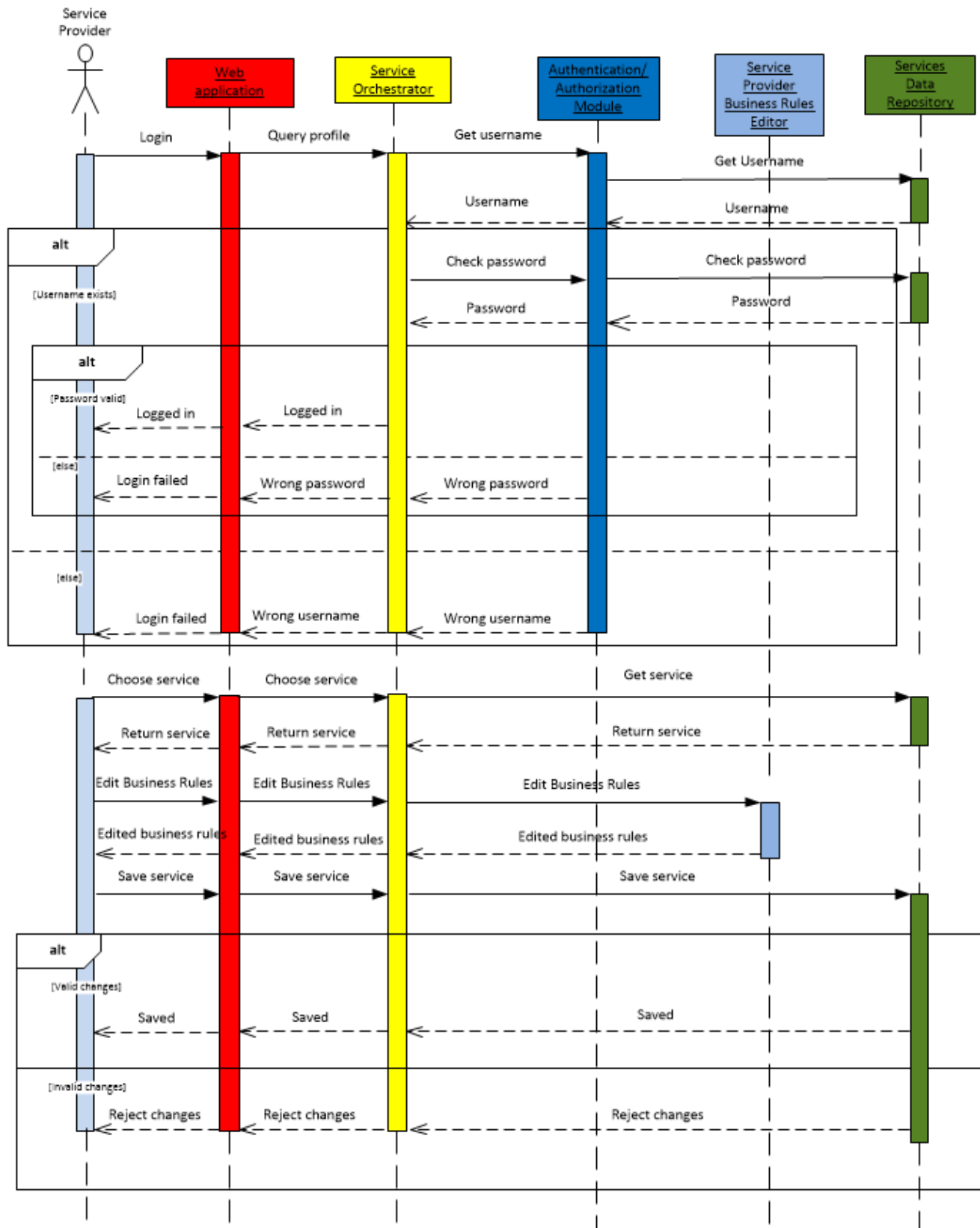


Figure 37: UML sequence diagram of the service business rules editing process

7.3 MaaS Aggregator Use Cases

This section presents the interactions between the system components that implement the use cases referring to the MaaS aggregator, namely the uses cases B1-B2.

7.3.1 B1 - Overall Business Rules Editing

The MaaS aggregator logs into the MyCorridor platform by providing appropriate credentials (i.e. an email and a password) in the web application that corresponds to him, namely the MaaS Aggregator Dashboard. These credentials are transferred from the Service Orchestrator to the Authentication/Authorization Module to be validated. If the credentials are valid, the MaaS aggregator is logged into the platform, and a complete set of all registered services from all service providers is presented to him.

The MaaS aggregator can modify the overall business rules that govern the operation of the platform. In particular, s/he makes changes to the business rules s/he wants (e.g. privacy policy, pricing policy, taxation policy, and promotional strategy) and submits these changes to the platform. The changes are received by the Service Orchestrator and delivered to the Overall Business Rules Editor for validation. The Overall Business Rules Editor checks if the changes on the overall business rules of the platform can be applied based on the existing registered services and their corresponding business rules, and if this is the case it applies them to all system components. Also, a success message is returned to the MaaS aggregator. Finally, it should be noted that the changes of the overall business rules should not heavily violate the business rules of a large proportion of the registered services. In this case, the changes should be rejected.

The overall business rules editing process is presented in the UML sequence diagram of Figure 38.

7.3.2 B2 - Added Value Synthetic

The MaaS aggregator can generate new services by synthesizing existing registered services. To do this, the MaaS aggregator first logs into the platform by providing appropriate credentials (i.e. an email and a password) in the web application that corresponds to him, namely the MaaS Aggregator Dashboard. These credentials are transferred from the Service Orchestrator to the Authentication/Authorization Module to be validated. If the credentials are valid, the MaaS aggregator is logged into the platform, and a complete set of all registered services from all service providers is presented to him. Then, the MaaS aggregator selects the services s/he wants to combine. The set of selected services is transferred from the Service Orchestrator to the Added Value Services Synthesis Module where the synthesis process is conducted.

If the services selected by the MaaS aggregator can be combined, the service synthesis process is successful and the resulted new service is returned to the MaaS aggregator. The MaaS aggregator can evaluate, and possibly modify, the attributes values of the new service. Finally, the new service is received by the Service Orchestrator that transfers it to the data layer in order to be stored to the Services Data Repository. However, if the services selected by the MaaS aggregator cannot be combined, the service synthesis process cannot be completed and a failure message is returned to the MaaS aggregator.

The service synthesis process is presented in the UML sequence diagram of Figure 39.

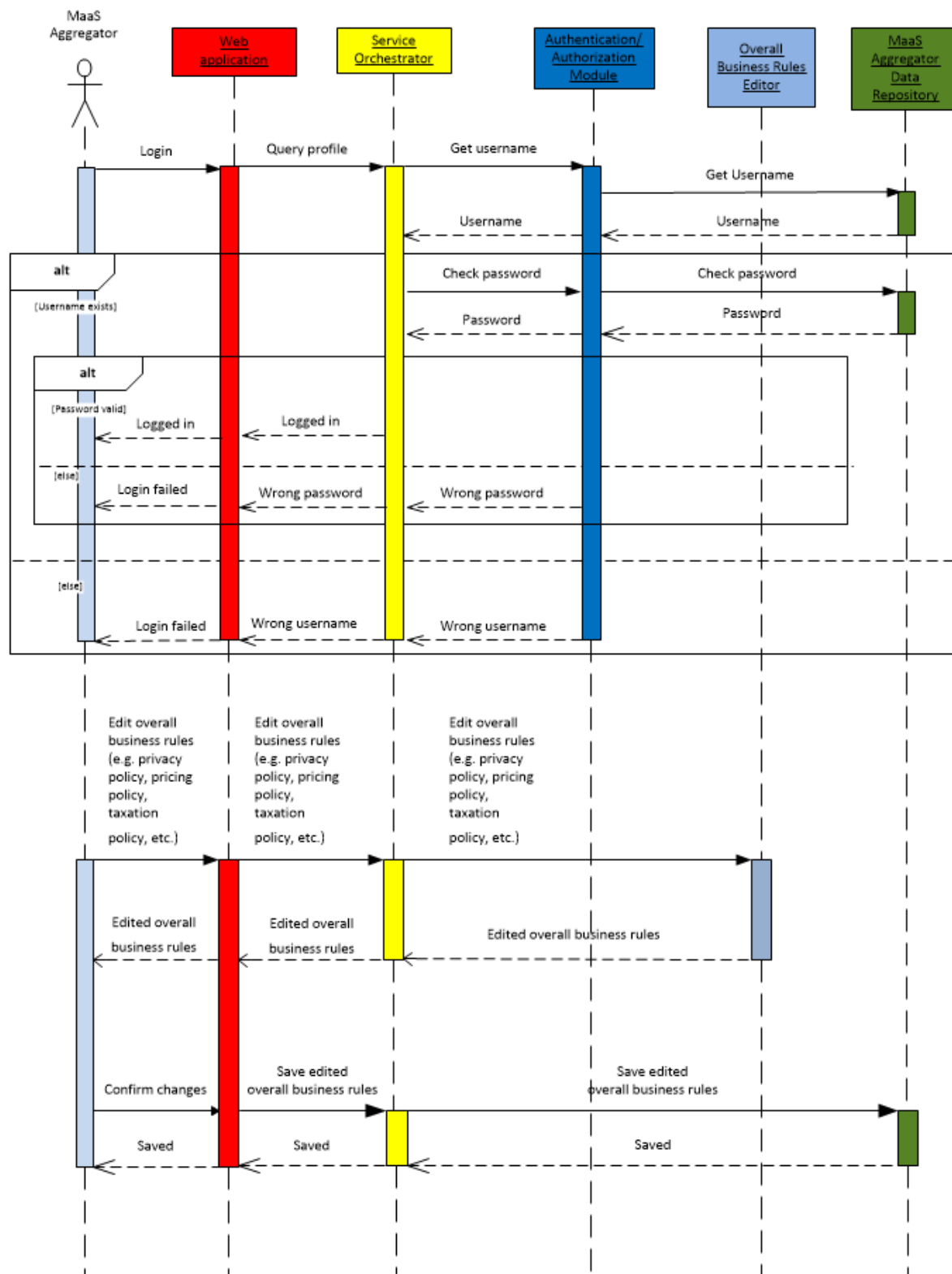


Figure 38: UML sequence diagram of the overall business rules editing process

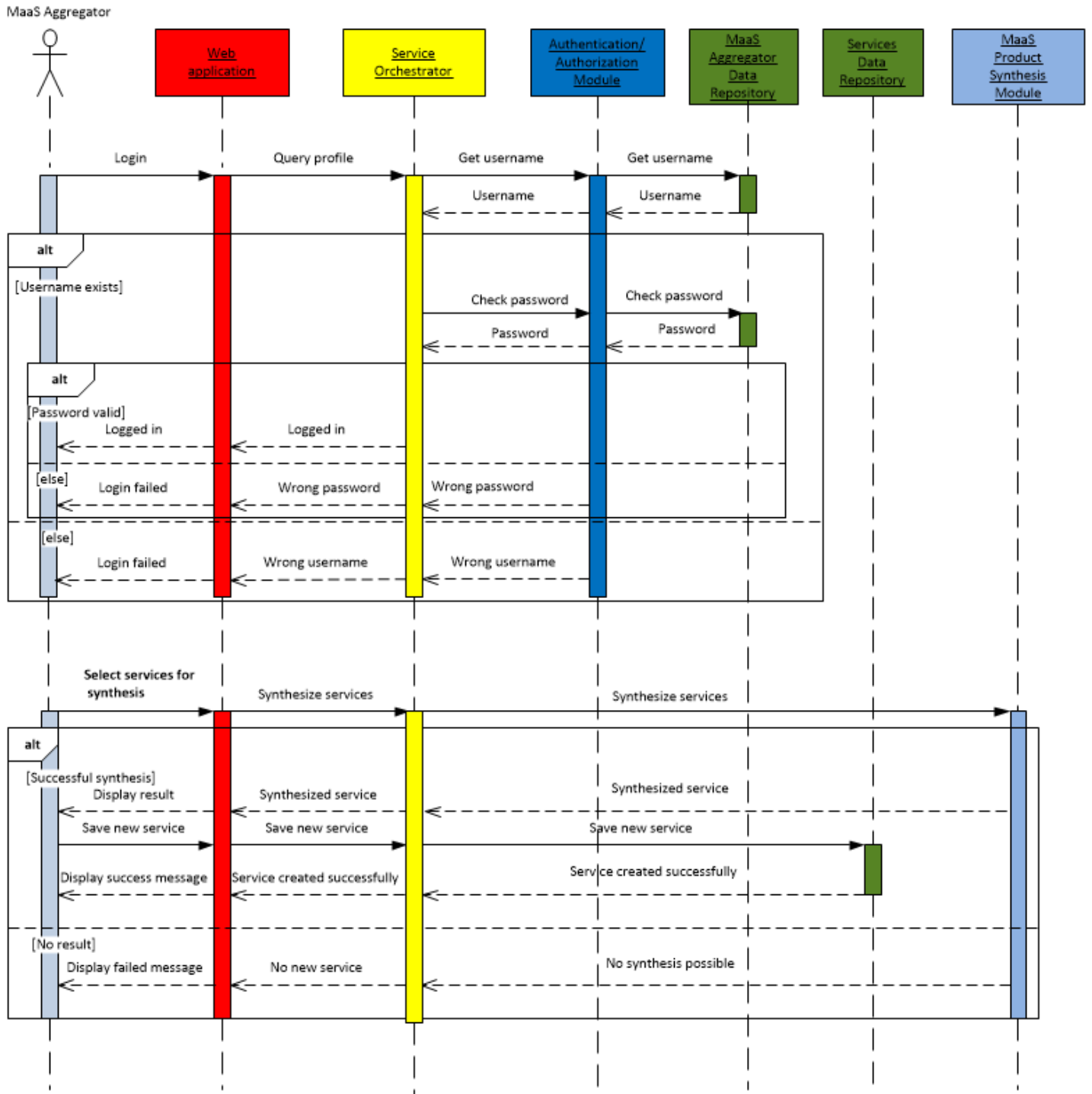


Figure 39: UML sequence diagram of the service synthesis process

7.4 Connected Use Cases

7.4.1 B3 - Clearance with the Traveller and the Service Providers (E-vouchers)

The use case B3 refers to the payment of the purchased services and the issuing of e-vouchers (i.e. receipts). These functionalities are implemented by the Payment Module that lies in the application layer. In particular, when a traveller proceeds to the checkout process, the Payment Module is invoked by the MaaS API to handle this process. Initially, the E-Voucher Issuer submodule implements the payment of the services using VivaWallet's infrastructure. After the successful completion of the payment process, the E-Voucher Issuer invokes the Back Office Notifier submodule, which in turn communicates with the back-office systems of the service providers in order to inform them for the purchase of the corresponding mobility services, and the successful payment of them. After these purchases are validated by the back-office systems of the service providers, the Back Office Notifier submodule communicates with the E-Voucher Issuer to issue the receipt of the transaction. Finally, the issued e-voucher is delivered to the mobile application of the traveller through the MaaS API.

7.4.2 B4 - Mobility Token Issue and Redemption (Use/Validation)

The use case B4 refers to the processes of issuing and redemption of mobility tokens (i.e. tickets). As described in the previous subsection, after the MaaS products purchases are validated by the back-office systems of the service providers, the Back Office Notifier submodule communicates with the E-Voucher Issuer (both submodules of the Payment Module) to issue the receipt of the transaction. At the same, the Back Office Notifier submodule communicates with the Mobility Token Issuer to issue the mobility token. The issued mobility token contains ticket information regarding all the purchased mobility services, in the ticketing format used by each service provider (e.g. QR codes, Aztec codes, etc.). Finally, the issued mobility token is delivered to the mobile application of the traveller through the MaaS API.

The above process, along with the process of clearance with the traveller and the service providers described in the previous subsection, are presented in the UML sequence diagram of Figure 40.

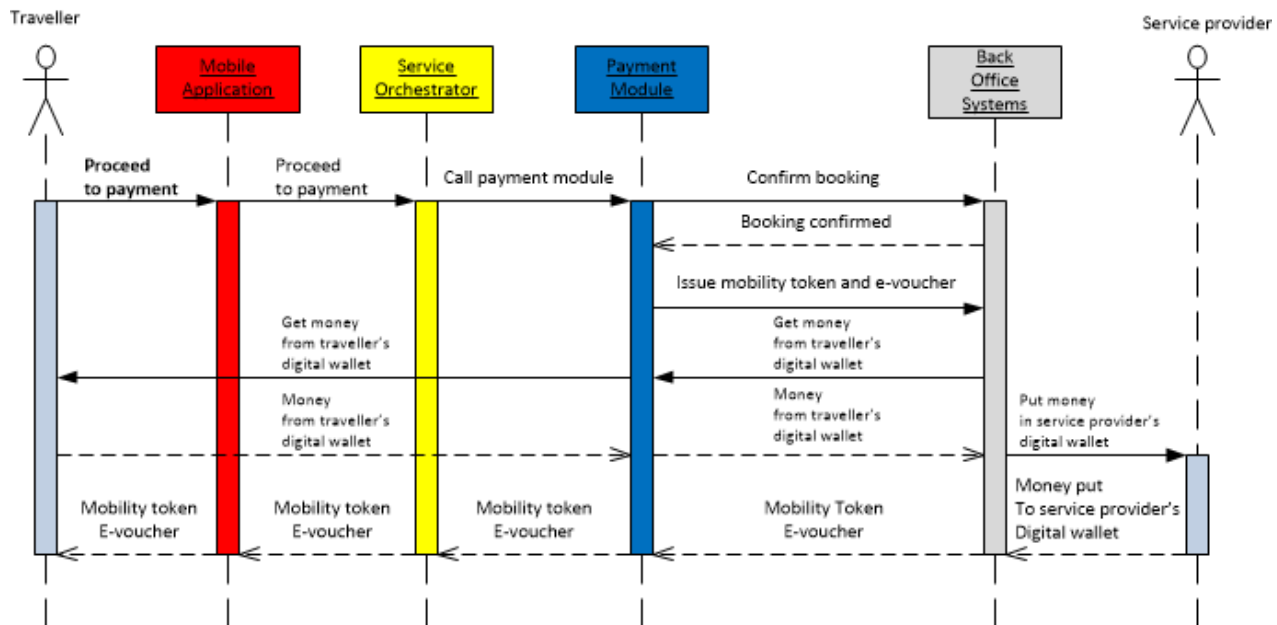


Figure 40: UML sequence diagram of the checkout process

7.4.3 B5 - Interactive Traffic Management Plan

The use case B5 refers to the interaction and cooperation of different actors involved in the integration process of the TM2.0 functionalities into the MyCorridor platform. Most of the functionalities of this use case take place outside the bounds of the overall MyCorridor platform, and involve mainly the Traffic Management Services Aggregator and the several sources of traffic management information. The environment of the several traffic management services, along with the Traffic Management Services Aggregator and the MyCorridor platform is presented in Figure 41.

The raw traffic management data coming from the several infrastructure managers are collected by the Traffic Management Services Aggregator, where they are pre-processed and fused into unified data structures. Once these data structures are ready, they are fed into the MyCorridor platform through their integration into the MyCorridor MaaS API. The data related to the traffic management services that are fed into the MyCorridor platform in this way are the following:

- Real time/scheduled traffic events
- Current travel times
- Travel time forecasts
- Current level of services
- Level of services forecasts
- Traffic light forecasts
- Zone access control information
- Speed recommendations
- Virtual Variable Message Signs (VMS)
- Park & Ride recommendation

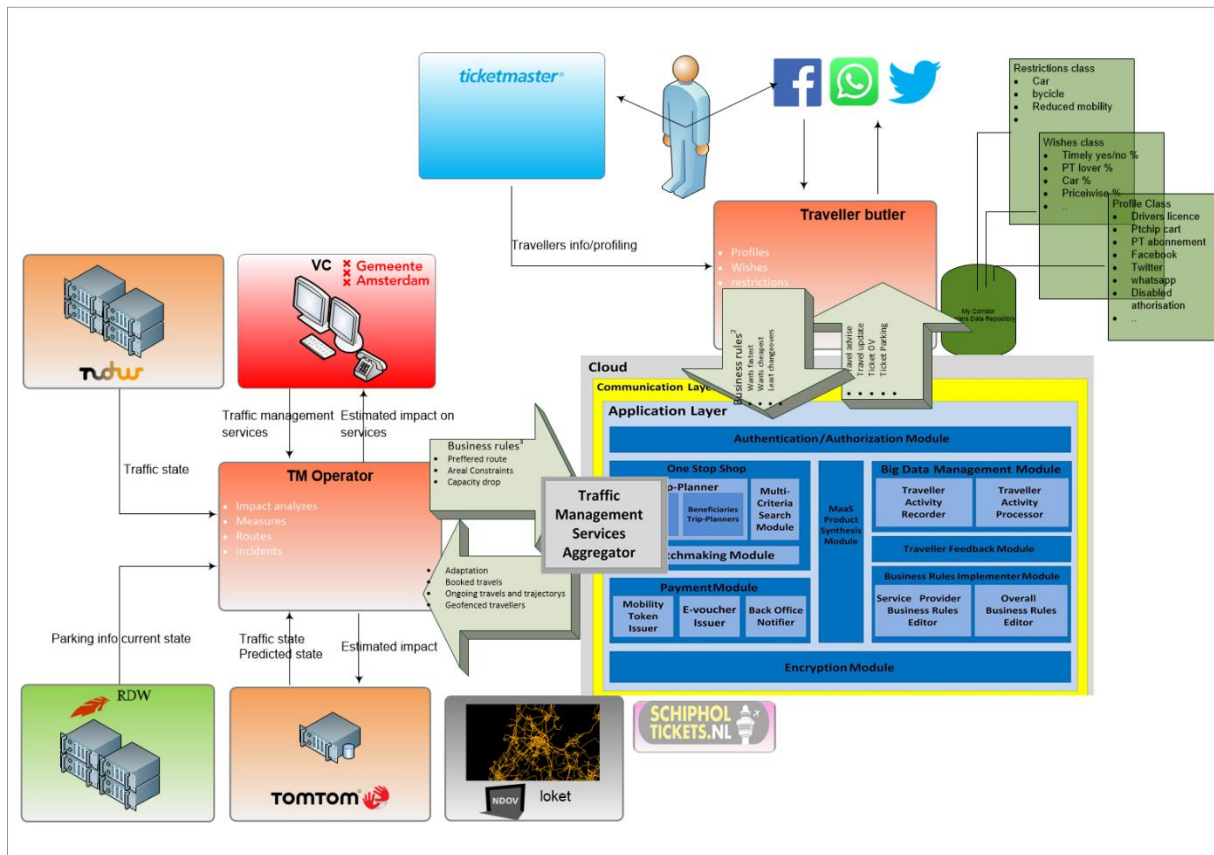


Figure 41: Traffic management services environment with the Traffic Management Services Aggregator and the MyCorridor platform

8 System Specifications

This section presents the MyCorridor system specifications, namely those defined by the need to meet the system non-functional requirements presented in section 4. The specifications are organized in the same categories used for reporting the non-functional requirements, and they are presented in tabular form along with their matching requirements.

8.1 Look & Feel Specifications

The Look & Feel Specifications (LFS) of the MyCorridor system were defined to meet the LHR, and are presented in Table 21.

Table 21: Look & Feel Specifications - LFS

Specification Name	Specification ID	Requirement Type	Description
Look & Feel Specification - 1	LFS1	LFR1, LFR2	The UI components (i.e. screens, menus, buttons) of the mobile app follow the look & feel paradigm of

Specification Name	Specification ID	Requirement Type	Description
			well established State of the Art MaaS apps (i.e. the Whim app) [39].
Look & Feel Specification - 2	LFS2	LFR1, LFR2	The mobile app utilizes light colors and shades.
Look & Feel Specification - 3	LFS3	LFR1, LFR2	The web applications (i.e. SRT and MaaS aggregator dashboard) utilize established web development technologies.
Look & Feel Specification - 4	LFS4	LFR1, LFR2	The web applications (i.e. SRT and MaaS aggregator dashboard) have minimalistic look & feel.
Look & Feel Specification - 5	LFS5	LFR1, LFR2	The web applications utilize light colors and shades.

8.2 Usability & Humanity Specifications

The Usability & Humanity Specifications (UHS) of the MyCorridor platform defined by the need to meet the UHR requirements are presented in Table 22.

Table 22: Usability & Humanity Specifications - UHS

Specification Name	Specification ID	Requirement Type	Description
Usability & Humanity Specification - 1	UHS1	UHR1, UHR4, UHR5	Task Completion Rate (rate of tasks successfully completed by the users): ≥ 75%
Usability & Humanity Specification - 2	UHS2	UHR1, UHR4, UH5	Effectiveness (rate of users successfully completed a particular task): ≥ 60%
Usability & Humanity Specification - 3	UHS3	UHR1, UHR4, UH5	Average Task Completion Time (average time required by a user to complete a task): ≤ 120 sec.
Usability & Humanity Specification - 4	UHS4	UHR1, UHR4, UH5	Average Time to Failure (average time a user spends on a task before give up or complete the task incorrectly): ≥ 60 sec.
Usability & Humanity Specification - 5	UHS5	UHR2, UHR3, UHR4, UHR5	Use of the HTML lang and XML xml:lang language attributes to identify the text processing language

Specification Name	Specification ID	Requirement Type	Description
Usability & Humanity Specification - 6	UHS6	UHR2, UHR3	Use of BCP 47 (not RFC 5646) template for language declarations and language tag matching
Usability & Humanity Specification - 7	UHS7	UHR2, UHR3	Blocks of content inherit any text-processing language set for the resource as a whole
Usability & Humanity Specification - 8	UHS8	UHR2, UHR3, UHR4, UHR5	Indication for a change in language for blocks of content when the language changes
Usability & Humanity Specification - 9	UHS9	UHR2, UHR3, UHR4, UHR5	Default base text direction is left-to-right
Usability & Humanity Specification - 10	UHS10	UHR2, UHR3, UHR4, UHR5	Base text directions include left-to-right, right-to-left, and auto
Usability & Humanity Specification - 11	UHS11	UHR2, UHR3, UHR4, UHR5	Text uses Unicode encoding form (i.e. UTF-8, UTF-16 or UTF-32)
Usability & Humanity Specification - 12	UHS12	UHR2, UHR3, UHR4, UHR5	Digit shaping (non-ASCII digits) for numeric values parsing and formatting for display
Usability & Humanity Specification - 13	UHS13	UHR2, UHR3, UHR4, UHR5	UTC date and time formats: YYYY/MM/DD hh:mm:ss
Usability & Humanity Specification - 14	UHS14	UHR2, UHR3, UHR4, UHR5	Users receive text in the language they prefer, based on user explicit choice
Usability & Humanity Specification - 15	UHS15	UHR1	User friendly MaaS API to allow 3rd parties to input their content
Usability & Humanity Specification - 16	UHS16	UHR4	Promotion of environmental friendly mobility solutions
Usability & Humanity Specification - 17	UHS17	UHR1, UHR3, UHR4, UHR5	W3C compliant interfaces

8.3 Performance & Scalability Specifications

The Performance & Scalability Specifications (PSS) of the MyCorridor system defined by the need to meet the PSR requirements are presented in Table 23.

Table 23: Performance & Scalability Specifications - PSS

Specification Name	Specification ID	Requirement Type	Description
Performance & Scalability Specification - 1	PSS1	PSR1	UI components response time: ≤ 2 sec.
Performance & Scalability Specification - 2	PSS2	PSR1	Average time for MaaS package generation: ≤ 6 sec.
Performance & Scalability Specification - 3	PSS3	PSR1	Average time for map loading: ≤ 2 sec.
Performance & Scalability Specification - 4	PSS4	PSR1	Average time for payment process completion: ≤ 10 sec.
Performance & Scalability Specification - 5	PSS5	PSR2	Acceptance rate of returned MaaS&Go services: ≥ 70%
Performance & Scalability Specification - 6	PSS6	PSR2	Acceptance rate of returned MaaSPacks services: ≥ 70%
Performance & Scalability Specification - 7	PSS7	PSR3	Average server uptime: ≥ 99.59%
Performance & Scalability Specification - 8	PSS8	PSR3	Number of simultaneous user requests supported: ≥ 1000
Performance & Scalability Specification - 9	PSS9	PSR3	Number of travellers whose data are stored: ≥ 10000
Performance & Scalability Specification - 10	PSS10	PSR3	Size of stored travellers data: ≥ 200 MB
Performance & Scalability Specification - 11	PSS11	PSR3	Number of services whose data are stored: ≥ 1000

Specification Name	Specification ID	Requirement Type	Description
Performance & Scalability Specification - 12	PSS12	PSR3	Size of stored services data: ≥ 50 MB
Performance & Scalability Specification - 13	PSS13	PSR2	Accuracy/Reliability: ≥ 90% (regarding the accuracy of the informatory part of the products the MyCorridor platform will return upon user profiling)
Performance & Scalability Specification - 14	PSS14	PSR2	Validity: ≥ 80% (MyCorridor platform products comply with the overall business rules policy)
Performance & Scalability Specification - 15	PSS15	PSR2	Relevance: ≥ 95% (MyCorridor platform products configured relevance to the user)
Performance & Scalability Specification - 16	PSS16	PSR3	Completeness: ≥ 90% (seamless experience when applicable, i.e. in trip planning)
Performance & Scalability Specification - 17	PSS17	PSR1, PSR2, PSR3	Use of RESTful services
Performance & Scalability Specification - 18	PSS18	PSR1, PSR2, PSR3	Use of the JSON format for data exchange
Performance & Scalability Specification - 19	PSS19	PSR2	Use of typical data mining and machine learning tools and algorithms for extracting useful MaaS usage patterns

8.4 Operational & Environmental Specifications

The Operational & Environmental Specifications (OES) of the MyCorridor system defined by the need to meet the OER requirements are presented in Table 24.

Table 24: Operational & Environmental Specifications - OES

Specification Name	Specification ID	Requirement Type	Description
Operational & Environmental Specification - 1	OES1	OER1	Android Wi-Fi support

Specification Name	Specification ID	Requirement Type	Description
Operational & Environmental Specification - 2	OES2	OER1	Android 3G/4G support
Operational & Environmental Specification - 3	OES3	OER1	Android GPS support
Operational & Environmental Specification - 4	OES4	OER1	iOS Wi-Fi support
Operational & Environmental Specification - 5	OES5	OER1	iOS 3G/4G support
Operational & Environmental Specification - 6	OES6	OER1	iOS GPS support

8.5 Maintainability & Support Specifications

The Maintainability & Support Specifications (MSS) of the MyCorridor system defined by the need to meet the MSR requirements are presented in Table 25.

Table 25: Maintainability & Support Specifications - MSS

Specification Name	Specification ID	Requirement Type	Description
Maintainability & Support Specification - 1	MSS1	MSR1	Automatic updates of Android mobile app through Google Play (whenever a new version is available)
Maintainability & Support Specification - 2	MSS2	MSR1	Automatic updates of iOS mobile app through App Store (whenever a new version is available)
Maintainability & Support Specification - 3	MSS3	MSR2	Scheduled server maintenance: once in 2 months
Maintainability & Support Specification - 4	MSS4	MSR2	Logging CPU, RAM, network and storage utilization on the server: once a day
Maintainability & Support Specification - 5	MSS5	MSR2	Verify server backups: once a month
Maintainability & Support Specification - 6	MSS6	MSR2	Check hardware installation: once in 3 months

Specification Name	Specification ID	Requirement Type	Description
Maintainability & Support Specification - 7	MSS7	MSR2	Update of third-party software components (e.g. libraries): once a month
Maintainability & Support Specification - 8	MSS8	MSR2	Check for new releases of the service provider's API: once a week

8.6 Security & Data Privacy Specifications

The Security & Data Privacy Specifications (SDPS) of the MyCorridor system defined by the need to meet the SDPR requirements are presented in Table 26.

Table 26: Security & Data Privacy Specifications - SDPS

Specification Name	Specification ID	Requirement Type	Description
Security & Data Privacy Specification - 1	SDPS1	SDPR1	HTTP Basic authentication through Python Eve framework [40]
Security & Data Privacy Specification - 2	SDPS2	SDPR1	Endpoint-level Authentication through Python Eve framework [41]
Security & Data Privacy Specification - 3	SDPS3	SDPR2	Password encryption using bcrypt [42]
Security & Data Privacy Specification - 4	SDPS4	SDPR2	Email encryption using hashlib [43]
Security & Data Privacy Specification - 5	SDPS5	SDPR2	Support for HTTPS communication protocol
Security & Data Privacy Specification - 6	SDPS6	SDPR2	Use of MongoDB default security measures [44]
Security & Data Privacy Specification - 7	SDPS7	SDPR2	Use of RESTful services

Specification Name	Specification ID	Requirement Type	Description
Security & Data Privacy Specification - 8	SDPS8	SDPR2	Use of the JSON format for data exchange
Security & Data Privacy Specification - 9	SDPS9	SDPR3	Terms & Conditions in Android mobile app
Security & Data Privacy Specification - 10	SDPS10	SDPR3	Terms & Conditions in iOS mobile app
Security & Data Privacy Specification - 11	SDPS11	SDPR3	Terms & Conditions in SRT
Security & Data Privacy Specification - 12	SDPS12	SDPR3	Terms & Conditions in MaaS Aggregator Dashboard
Security & Data Privacy Specification - 13	SDPS13	SDPR2	Implementation of payments through the secure infrastructure of VivaWallet
Security & Data Privacy Specification - 14	SDPS14	SDPR3	The system informs the users regarding their history of trips, purchases of services, reviews and loyalty points
Security & Data Privacy Specification - 15	SDPS15	SDPR3	The users can view reviews of other users on the services
Security & Data Privacy Specification - 16	SDPS16	SDPR3	Service Level Agreements (SLAs) signed by registered service providers

8.7 Cultural Specifications

The Cultural Specifications (CS) of the MyCorridor system defined by the need to meet the CR requirements are presented in Table 27.

Table 27: Cultural Specifications - CS

Specification Name	Specification ID	Requirement Type	Description
Cultural Specification - 1	CS1	CR1	Language support of Android mobile app through the strings.xml file [45]
Cultural Specification - 2	CS2	CR1	Language support of iOS mobile app through the LaunchScreen.stroyboard [46] and Localizable.strings files [47]
Cultural Specification - 3	CS3	CR1	Use of Currency Converter Python library [48]

8.8 Legal Specifications

The Legal Specifications (LS) of the MyCorridor system defined by the need to meet the LR requirements are presented in Table 28.

Table 28: Legal Specifications - LS

Specification Name	Specification ID	Requirement Type	Description
Legal Specification - 1	LS1	LR1	The system conforms to GDPR [21]
Legal Specification - 2	LS2	LR1	Terms & Conditions in Android mobile app
Legal Specification - 3	LS3	LR1	Terms & Conditions in iOS mobile app
Legal Specification - 4	LS4	LR1	Terms & Conditions in SRT
Legal Specification - 5	LS5	LR1	Terms & Conditions in MaaS Aggregator Dashboard
Legal Specification - 6	LS6	LR1	DPIA [49]

8.9 MaaS Alliance Guidelines Compliance

The Mobility as a Service (MaaS) Alliance [15] is a public-private partnership creating the foundations for a common approach to MaaS, unlocking the economies of scale needed for successful implementation and take-up of MaaS in Europe and beyond. The main goal is to facilitate a single, open market and full deployment of MaaS services. The MaaS Alliance has published a set of guidelines [50][51] for the design of the key aspects needed to sustain a MaaS ecosystem. During the design phase of the MyCorridor system

architecture, and in particular during the design phase of the MaaS API, an effort has been made to follow these guidelines.

The MyCorridor MaaS API exposes an endpoint for retrieving door-to-door trips, as suggested by the MaaS Alliance Guidebook. In particular, in the request parameters, the starting and ending points of the trip are defined as latitude-longitude pairs, whereas the preferred travel modes are passed as a list of strings. Additionally, the date and time of the trip can be defined, and if they do not, the current date and time are used. Moreover, the MyCorridor MaaS API returns one or more trips based on the selected transportation modes. Each trip has its own departure and arrival date-time pairs and is composed of a number of segments (steps). For every segment, the starting and ending date-time are provided, as well as the transportation mode for the specific segment. Furthermore, as proposed in the MaaS Alliance Guidebook, the MyCorridor MaaS API exposes an endpoint for retrieving points of interest (POIs). Requests on that endpoint include the latitude and longitude coordinates of the location around which POIs should be returned, the search radius in meters and the categories of the preferred POIs. In the context of MyCorridor project, POIs are characterised as added value services and they are related to food, museums, weather, and live-music events. Finally, it should be mentioned that the MaaS Alliance Guidebook includes many suggestions regarding the booking and the payment processes involved in the context of a MaaS ecosystem, and these guidelines are planned to be followed in the second development phase of the project (i.e. after the end of the first pilots round).

9 Interoperability Issues

The activity A2.3 - “Interoperability and cross-border security issues” addressed a variety of issues concerning the enhancement of interoperability within the MyCorridor MaaS platform. In particular, the interoperability-related outcome of this activity includes, on one hand, the identification of the principal barriers that prevent service providers from exposing data that will facilitate the complete purchase of a multimodal trip from a single MaaS interface, and on the other, the recommendation of solutions to overcome some of these barriers, along with the degree in which these solutions can be implemented in the context of the MyCorridor project.

9.1 Service interoperability

The concept of service interoperability is related to the seamless provision of mobility solutions from a MaaS platform, in the case that the traveller requests a trip that crosses the border of a city or a country. In such cases, specific problems may arise which can be considered as barriers in the wider acceptance of the MaaS mobility paradigm. In this subsection, some of these problems (identified in the context of the MyCorridor project) are presented, along with possible ways of handling them.

9.1.1 Service interoperability barriers

When a traveller requests a trip whose origin and destination points are located in the two sides of a border, i.e. a city border or a country border, then it is likely that the part of the trip on one side of the border to be covered by the services registered in a MaaS platform, while the other part does not. Additionally, even in the case that a MaaS platform has registered services that can cover the whole trip, a problem with the validation of the tickets purchased for the different service providers may arise. This means that the traveller may be in the situation in which the ticket(s) s/he bought for a mobility service that serves the complete trip may be valid at one side of the border but not on the other. Such problems make it imperative for a MaaS platform to ensure the interconnectivity between the different registered services so as to be able to provide seamless mobility solutions to serve the travellers’ trip requests.

9.1.2 Service interoperability solutions

As explained in the previous subsection, service interoperability problems may arise during the operation of a MaaS platform, in cases that the request trips cross city or country borders. One obvious solution to these problems is for the MaaS platform to try have as many services as possible registered. This means not only different type of services (i.e. in terms of transportation mode, bus services, car services, etc.) but also as many options as possible for the same type of service provided by different service providers (e.g. 3 different intercity bus services within the same country). The second solution to the service interoperability problems may be the registration of services that, on one hand, cover very large geographical areas (e.g. whole countries, or whole Europe), and on the other, ensure that the same business policy applies to all areas they cover. Fortunately, nowadays, there are many mobility services covering very large areas in the European continent and operating with the same business policy in all areas (e.g. taxi.eu [52], Uber [53], CheckMyBus [54]), that can potentially be registered and operate in the context of the MaaS ecosystem.

Finally, from a technical point of view, an approach that can facilitate the process of handling the service interoperability problems is by splitting its trip into legs and serving its leg separately, as happening in the MyCorridor case. Based on the assumption that a service can serve a trip if it covers (geographically) both its origin and destination points, if we process a trip request in a leg-based fashion and match services in each separate leg (rather in the overall trip), we increase the locality of each matching as a service should cover the start and end points of a leg (that can be very close with each other) rather than a trip. In this way, the probability that the start and end points of a part of the trip being in different sides of a border is reduced, thus reducing the probability that the aforementioned service interoperability problems arise. However, this solution comes with the technical/computational cost that the matchmaking process should be conducted for each leg of each of the trips generated for a trip request. In the case of MyCorridor, this technical limitation is handled, in the implementation level, by the use of a high performance programming language (i.e. C++) which inherently offers appropriate tools (e.g. OpenMP [55], POSIX Threads [56], etc.) for easily parallelizing the matchmaking process taking place for the legs of a trip. This process can be considered as very close to embarrassingly parallel, as the consecutive legs of a trip share only one common point (i.e. the end point of a leg is the start point of the immediately next leg).

9.2 Data interoperability

The data interoperability issues of a MaaS platform refer to the several different data formats/templates/structures that exist in the transport industry for the representation of the same data entities that usually appear in the operation of a MaaS platform (e.g. trips, services, payments, etc.). This heterogeneity in the representation of the data creates difficulties mainly in the service registration and the services interconnection processes within a MaaS platform, both in technical and in business level. These difficulties along with some potential solutions are presented in the following subsections.

9.2.1 Data interoperability barriers

The MaaS paradigm includes the integration of several different types of mobility into one single interface. Therefore, the several data interoperability issues that may arise during the integration of these services into a MaaS platform, may be very different in both concept and severity. Hence, the presentation of the current data interoperability barriers that appear in a MaaS platform take place in a per-transportation-type fashion.

Regarding the public transport services (referred also as public transit services), like bus, rail, metro services etc., the definition and the wide acceptance of the GTFS format for exchanging data was a very important towards interoperable public transport services. Nowadays, the GTFS [27] format is utilized

by more than 6000 public transit authorities for generating and publishing public transport data feeds. Additionally, the GTFS-RT [57] format has been used in recent years from some public transit authorities for publishing real-time public transport data feeds (e.g. delays, cancellations, changed routes, vehicle positions, etc.), due to the fact that by design the GTFS format does not support real time information. However, data interoperability barriers in public transport services still exist. The most important of them is the cost and complexity for generating high quality public transport data feeds, either static or real-time. Many of the public transport authorities worldwide have neither the hardware infrastructure nor the software development expertise in order to be able to gather, organize and distribute high-quality data feeds. One remedy on this issue is the outsourcing of the data generation and distribution process to third-party hardware and software vendors. However, the level of professionalism and expertise of these vendors varies between cities, countries, etc., thus resulting in data feeds of different quality levels.

Another important barrier towards interoperability between public transport services is the conciseness of the existing public transport data formats. For example, there public transport authorities whose business model is very complex, and therefore, the generated data cannot be represented by the typical GTFS or the GTFS-RT format. For this reason, it is very important for the public transport services (at least the major ones) to be involved in the evolution process of the GTFS and the GTFS-RT data standards by constantly providing feedback to them regarding their needs data specifications.

Another major type of mobility integrated in a MaaS ecosystem is the private transit services that include taxis, services that connect travellers with the drivers their private vehicles for transporting people (e.g. Uber [53]), carsharing services, bikesharing services and carpooling services. Regarding the services like Uber, the principal barrier in data interoperability is the intense competition between the different services. For example, Uber can provide access to its services to third-party apps (e.g. MaaS apps) through its public Uber API[58], under the condition that no competitive service will be provided by the app. This fact is in complete contrast in the MaaS principle stating that a MaaS platform should provide to the travellers as many mobility services as possible, even if these services come from competitive providers. Regarding the taxi services, the major interoperability barrier is the technology adoption, meaning that most of the taxi services (even the major ones) lack of mature APIs and mechanisms in general for gathering and distributing data.

In the case of the carsharing services, the data interoperability barriers are formed as a combination of the lack of mature APIs for sharing data in the case of small- or medium-scale providers, and the intense competitive environment in the case of large-scale providers. For example, ZipCar [59], which is a leading carsharing service worldwide, offers static data (e.g. car type) to third-party mobility software vendors (e.g. MaaS apps) through an API, but to book or pay for a vehicle the traveller should be redirected to the ZipCar's own interface. ZipCar probably wants to have full control over the booking and payment process in order to ensure the promotion of its own service, compared to the usual policy of MaaS apps that try to provide competitive services in the most equitable way.

Regarding the bikesharing services, a major step towards data interoperability has been taken with the definition of the General Bikeshare Feed Specification (GBFS) [60] by the North American Bike Share Association (NABSA) in late 2015. This format allows bikesharing service providers to distribute both static (e.g. bikesharing stations locations) and real-time (e.g. capacity and availability of bikes) data. Although, the format has been adopted by many bikesharing providers in the United States, its penetration in other countries is still very low. Finally, the principal barriers regarding the larger integration of carpooling/ridesharing services in a MaaS platform are the lack of considerable mass of drivers and riders in one platform, and the lack of mature ridesharing APIs. Although there have been some efforts for the design and development of commercial-ready ridesharing APIs (e.g. Carma API [61], CarpoolWorld API [62], etc.), they are far from being characterized as standards or formats due to their very limited adoption by the market.

9.2.2 Generic data interoperability solutions

The data interoperability barriers presented above create difficulties in the overall operation of a MaaS platform, thus limiting the wider adoption of the MaaS paradigm. For this reason, in this subsection we present some generic solutions/recommendations in order to overcome (in some extent) these barriers.

Regarding the public transport services, a simplistic, yet very difficult in practice, way to overcome the interoperability barriers is the wider acceptance of the GTFS and GTFS-RT formats. The public transport authorities should not only generate static (or/and real-time) data, but also to format them using these standards. Also, the generated data should be as complete as possible in order to avoid the consequences of missing values as much as possible. The public transport authorities that will bear the costs of these processes, either in-house (by employing developers) or through outsourcing (by paying a third-party software vendor), is very likely to get a considerable Return of Investment (ROI) [63].

In the case of Uber-type services or taxi services, things are more complicated. In these cases, clear incentives and business models should be designed and proposed to the corresponding service providers to convince them to have their APIs open without restrictions to third-party mobility applications in general and to MaaS applications in particular. Regarding the bikesharing applications, the wider adoption of the GBFS standard from a large number of bikesharing service providers (possibly under collaboration with NABSA) can effectively strengthen the integration possibilities of such services into MaaS platforms. Finally, in the case of carpooling/ridesharing services, emphasis should be given at first in the design and implementation of both stable ridesharing APIs and data standards for the information exchanged during the operation of such services.

As it is evident, all the aforementioned guidelines mainly concern the service provider's side. A more MaaS specific approach (i.e. from the MaaS aggregator/designer/implementer side) to the interoperability issues is presented in the next subsection.

9.2.3 MaaS specific data interoperability solutions

Apart from the aforementioned generic solutions, a more holistic approach for addressing the interoperability issues is through MaaS specific technology advancement and data standardization. The first part of this proposition refers to the design and development of technologies/tools/systems that are exclusively suited for the operations of a MaaS platform. For example, the design and implementation of a module responsible for matching the travellers' requests with the existing registered services (e.g. MyCorridor Matchmaking Module) can be considered as an expression of the rationale behind the MaaS specific technology advancement. On the other hand, the second part of the proposition refers to the concept of designing a common format for representing all the information exchanged during the operation of a MaaS platform. This part can be considered more difficult than the first because it requires the collaboration of entities coming from completely different fields, e.g. universities, research entities, public authorities, private transit service providers, software companies, etc.

In the context of the MyCorridor project, an effort has been made to follow both parts of the aforementioned guideline. In particular, as already presented, the MyCorridor platform contains several modules that provide MaaS specific technology advancement. The Matchmaking Module, which is responsible for matching the travellers' requests with services registered in the platform, the MaaS API which handles all communications between as system architecture components, and the Payment module which is responsible for the realization of the actual booking, payment and ticket issuing processes, can clearly be considered as MaaS specific technology advancements.

Regarding the data standardization part, we consider that we made a first step towards the design of a complete data format for MaaS data, on top of which future projects and initiatives can build. In particular,

as will be thoroughly described in the deliverable D3.1, we designed a set of data models that represent many entities and roles involved in the operation of a MaaS platform. These data models are presented in Table 29.

Table 29: MyCorridor MaaS data models

Term	Description
User	A traveller who uses the MyCorridor system for planning his/her trips.
Travel preferences	The travel preferences of a user (traveller).
User picture	A picture (i.e. a media file) of the traveller.
Social media	It represents the online “presence” of the traveller in social media (i.e. Facebook and Twitter).
Type of services	It describes which types of services the traveller wants to receive as MaaS offerings, namely mobility, infomobility or non-mobility (i.e. traffic management and added value) services.
Trip	A multimodal trip that may include both private and public transport modes.
Location	A specific geographic location (i.e. a point)
Itinerary	An alternative itinerary for a specific instance of the Trip data model.
Step	A leg of an itinerary of a trip.
Leg geometry	Geographic representation of a leg as a polyline.
Service	A service that can be provided through MyCorridor platform. This can be mobility, infomobility, traffic management or added value service.
Service location	An operating area (i.e. a city or a country) of the service.
Bounding box	Geographic bounding box, namely an area enclosed by an imaginary rectangle.
Operation	A specific time period of operation of a service.
Service documentation	It represents a document (in PDF [64] format) that contains all details regarding the functionality of a service’s APIs (both basic API and booking API)
Service provider	A service provider that registers his/her services on the MyCorridor platform.
Feedback	A rating and a brief comment for a service.

Term	Description
Matchmaking product	The result of the matchmaking process. In the case of the MaaS&Go scenario, this is a complete trip with specific services matched on its legs (i.e. MaaS trip). In the case of the MaaSPacks scenario, it is a set of services (i.e. MaaS package).
Position	The location of a traveller at a specific time.
User statistics	The set of MaaS usage variables related to the travellers.
Service statistics	The set of MaaS usage variables related to the services.

A thorough description of all aforementioned data models will be provided in the deliverable D3.1. All data models were implemented as JSON schemas, resulting in collections of JSON documents (or specifically BSON [65] documents) in NoSQL [38] data repositories (MongoDB [66] data repositories in particular). Also, it is worth mentioning that, apart from the NoSQL-based implementation, the Service data model (that describes meta-information of mobility/infomobility/traffic management/added value services) was also implemented as an RDF [67] ontology using the OWL [68] ontology language. This parallel implementation of the Service data model was implemented in order to examine which of the two implementations, namely the NoSQL-based and the OWL-based, is more suitable for the MaaS ecosystem in terms of speed development, maintenance, flexibility, scalability and performance.

10 Cross-Border Security Issues

The second major subject addressed by the activity A2.3 - “Interoperability and cross-border security issues” is the security issues (both in-border and cross-border) that may arise during the operation of the overall MyCorridor MaaS platform. The outcome of this part of the activity comprise the identification of related issues, their elaboration aiming to decide which of them will be implemented in the context of the project and which not (in any case, the latter should to be taken into account during a real life operation of the MyCorridor platform), the definition of corresponding specifications that come along the proposed architecture, and the provision of guidelines and recommendations to the service developers and service integrators about the most reliable and sustainable technological solutions for the needs of the project.

From an overall point of view, the benefits of the layered architecture pattern in terms of security have been thoroughly reported in the literature [69]. Such a choice enables developers to secure each of the distinct layers separately, using different methods that are appropriate to each security issue. For instance, the MyCorridor platform can store sensitive or confidential information in its application layer, keeping it away from the presentation layer, thus making it more secure.

Potential security issues within the various blocks and connections of the MyCorridor architecture concern:

- Data encryption;
- Electronic authentication and authorization of actors involved;
- MaaS specific functionality, and
- Denial-of-Service (DoS) attacks.

The elaboration of these issues, together with a description of the methods to address them in the context of the MyCorridor project, is reported below. At the end of the report, we briefly elaborate the issue of web services communication, justifying the choice of the REST (Representational State Transfer) solution adopted in the project.

10.1 Data encryption

Data encryption is the process of encoding information in order to disable unauthorized users to access or decrypt it. Generally speaking, it aims at protecting the confidentiality of the related data. All types of sensitive data stored in the context of the project need to be “translated” to a new form so that only authorized personnel (having access to the encryption key) can read it. In other words, encrypted data appears scrambled to an unauthorized user. In case that encrypted information is stolen or copied, it will be unreadable and therefore of no value. Encryption is a preventive security control.

The two main approaches to perform data encryption are by using either a symmetric key or an asymmetric key. A symmetric key (also known as secret key) uses the same key to both encode and decode the information. This approach is commonly used to encrypt small amounts of data. On the other hand, asymmetric key (or public key cryptography) uses two linked keys, one private (for decryption) and one public (for encryption).

Commonly used libraries for encryption in Python programming language (which is the language used for the development of the MaaS API that implements the security requirements) include:

- **hashlib** [70]. This library provides a decent password and data hashing algorithm, updated at the schedule of Python versions; it can be used to generate hashed passwords for secure storage or checksums to confirm data integrity during transmission.
- **cryptography** [71]. This library provides cryptographic recipes and primitives. It supports Python 2.6– 2.7, Python 3.3+, and PyPy [72].
- **PyCrypto** [73]. This library provides secure hash functions and various encryption algorithms. It supports Python version 2.1+ and Python 3+.
- **bcrypt** [74]. This library implements the well-known bcrypt hashing function which is based on the Blowfish cipher.

According to the data schema and the analysis of the Use Cases (see deliverable D1.1) developed in the context of MyCorridor, entities that need to be encrypted are:

- the email of a traveller / service provider / MaaS aggregator;
- the password of a traveller / service provider / MaaS aggregator;
- the username of a traveller / service provider / MaaS aggregator;
- the social id of a traveller.

➔ For the needs of the project, the recommended encryption solution includes the utilization of **bcrypt and hashlib libraries** (for username, social id and email encryption). bcrypt is required for password encryption due to its robust and strong encryption capabilities. However, the encryption using bcrypt is considered as a CPU-intensive task. Hence, hashlib is suggested in order to hash data attributes where the level of encryption provided by bcrypt is assumed as an overhead; such attributes include the email, the password and the social id of a user.

10.2 Authorization and authentication

In the context of activity A2.3, generic models for domestic and cross-border electronic authentication have been considered, assessed and finalized. A variety of authentication methods exists in the literature, the most common of them being:

- **HTTP Basic authentication and authorization.** According to this method, the client provides its username and password in order to communicate with the server. This method does not utilize cookies or local storage techniques. The shortcoming of this method is that the credentials of the user are transferred through the network whenever the communication with the server is needed; hence, they can be easily accessible by malicious users.
- **OAuth 2.0 token-based authentication and authorization.** In this method, the server provides the client with a unique generated token. This unique key is used for user authentication and authorization. The shortcoming of this method is that it is admittedly slower than the HTTP Basic authentication method.

Attention was also paid to issues regarding cross-border authentication and authorization. For this purpose, we reviewed prominent solutions proposed by diverse EC Agencies, EU-funded projects, and academic researchers. Approaches that are of particular interest to the needs of MyCorridor have been described or elaborated in the following:

- The Risk Assessment Report titled “Security Issues in Cross-border Electronic Authentication”, produced by ENISA (European Network and Information Security Agency - www.enisa.europa.eu) [75].
- The NETC@RDS project (NETC@RDS service for the electrification of the European Health Insurance Card: a pan-European project supported by the EU’s eTEN Program) [76] that addressed a series of issues about security infrastructure, communication protocols, and secure network interconnection between the service portals.
- The STORK (Secure Identity Across Borders Linked) EU project that proposed a solution to make it easy for citizens to access the concerned public service online wherever they are located, whether using a smart card or a virtual ID number [77].
- The STORK 2.0 (Secure idenTity acrOss boRders linKed 2.0) project, involving 57 partners from 19 European Member and Associated States, which contributes to the realization of a single European electronic identification and authentication area. The project pilots the updated European eID interoperability platform in key areas like eBanking, eHealth, public services for business, and eLearning and academic qualifications [78].
- The publication titled “Middleware Architecture for Cross-Border Identification and Authentication”, by B. Zwattendorfer, I. Sumelong and H. Leitold, appearing in the Journal of Information Assurance and Security [79].
- The work done in the context of the CAVAL initiative, which aims at the development of an open standard for data interoperability in the travel and tourism industry [80]. Of particular interest are their Web Services Specifications for Travel Agents Interoperation.

The above approaches elaborate a series of issues including different types of adapter components, different user credentials that link the user’s identity with a token, reliability of each credential, token security levels, tokens issued by different operators, different technical infrastructure and equipment in use, alternative authentication protocols and procedures, different sets of personal data, as well as acceptance and trust of personal data from one country to another.

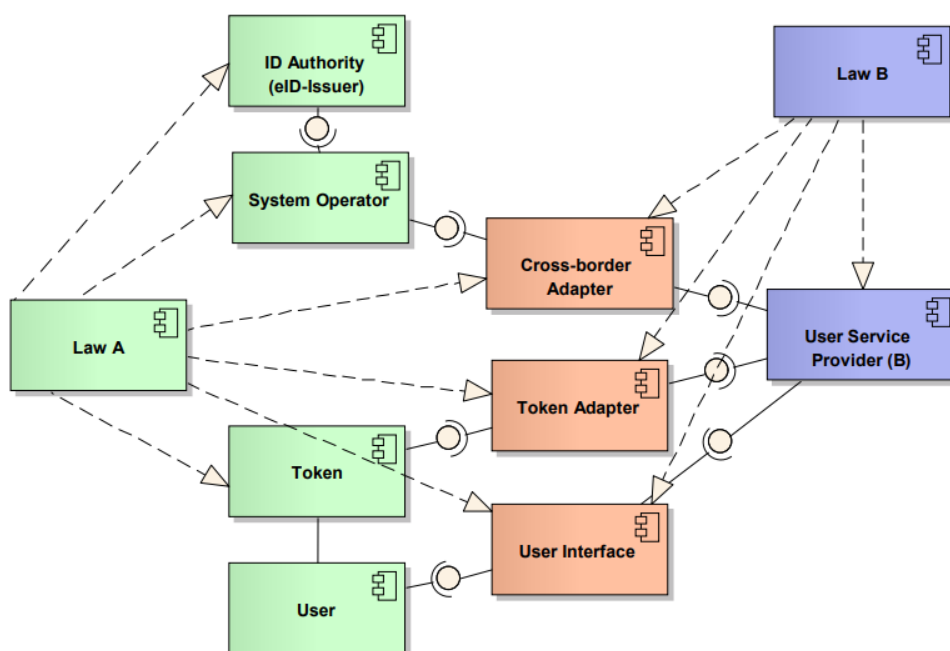


Figure 42: ENISA's generic model of cross-border authentication

Our consideration of the abovementioned approaches reveals that their implementation is based on models proposed by ENISA. As far as electronic cross-border authentication is concerned, their generic security model (Figure 42) has been broadly adopted, which suitably addresses a diversity of cross-border authentication requirements. Briefly, in order to achieve compatibility between the two systems to the point where a user of the first system may receive services from the second system, adapter components must be introduced into both systems. The two basic components are: (i) the **cross-border adapter**, which has the task of actually proxying an electronic authentication request from the local service provider (B) across the border between countries and systems to the system operator, and (ii) the **token adapter**, which is specific to the cross-border solution of the system and whose main task is the interfacing of a token from one country with the user service provider from another country [75].

As stressed by ENISA in their report, we mention here that for each specific cross-border system, the best and most appropriate implementation must be found; this is not so much a question of technology, but of considering possible solutions as these are defined by law and contractual agreements between the systems.

- ➔ For the needs of the project, taking into account both usability and security issues, we argue that the recommended solution for authentication and authorization is through the **HTTP Basic authentication and authorization method**. Compared to the OAuth 2.0 token-based method, it is faster as far as implementation efforts are concerned. In addition, with respect to its crucial shortcoming, i.e. that the user credentials can be intercepted, this can be largely overcome by relying on the HTTPS protocol. The integration of more sophisticated models, such as that proposed by ENISA, should be considered during the last year of the project, in case that the project's use cases impose token-based cross-border authentication and authorization requirements.

10.3 MaaS specific functionality

In a MaaS platform, such as the one being developed in the context of MyCorridor project, service correctness and data quality are not under the responsibility of a single actor. This certainly imposes a series of security issues. In any case, the platform should play an essential role in preventing system abuses, as well as in monitoring the correctness of transactions carried out. In other words, while it is unlikely to anticipate that the MyCorridor platform guarantees complete correctness of data sources and MaaS related services, it is necessary to define and adopt practices to prevent bad data quality and malicious service behaviour.

Extensively elaborated issues about data sources security include **data provenance** [81] and **data trustworthiness** [82]. Confirming data provenance means ensuring that the source of data is verifiable; in other words, that it corresponds to the one declared in the process of creation. In a MaaS setting, provenance protection is a defensive action against malicious actors claiming to expose data of a competitor aiming at gaining unfair advantage [83]. On the other hand, data trustworthiness concerns the ascertaining of the correctness of data provided by a specific source. In the setting under consideration, the data trustworthiness assessment is usually derived from the reputation of its creator (traveller, service provider).

→ For the needs of the project, the recommended solution to handle data provenance and data trustworthiness security risks is through a **basic authentication** mechanism that verifies the provider of data. The invocation and implementation of more sophisticated mechanisms [83] go out of the scope of the MyCorridor project.

As far as **service maliciousness** is concerned, it is broadly admitted that it is difficult to formalize and verify the concept of service trustworthiness in an open platform, like the one being developed in the context of MyCorridor project. In such a context, service trustworthiness can be linked with its compliance to a certain functionality. If a service creates aggregated data by processing various data sources, one needs to ensure that the aggregation algorithm is correct, as well as that it provides a complete list of results (not hiding useful ones from the user).

There are many cases of malicious actions to be performed by a registered service. For instance, a malicious trip-planner could suggest routes that favour or harm a certain travel service provider; GPS-based positioning combined with the identification of drivers may reveal sensitive information about drivers' behaviour, which certainly threatens their privacy; drivers may also represent an insider threat to a bus operator service, since they can disable the GPS device of their vehicles, thus compromising the reliability of services that depend on the GPS positioning system (a service that estimates bus arrivals and delays).

To the best of our knowledge, the most comprehensive analysis and assessment of security risks related to malicious threats has been performed by the developers of the *SMAll* (Smart Mobility for All) platform, a MaaS solution that builds on the concept of federated Cloud Computing to support the transportation market [84]. Their approach adopts a tiered view of MaaS markets, called the *MaaS Stack*, where: the first tier is that of *eMobility Operators*, i.e. entities that own, administrate, and expose software functionalities regarding mobility, provided in a machine-readable form; the second tier that still focuses on single eMobility operators but enriches the taxonomy of services with the category of *Business Intelligence*, which includes services that provide insights on the performances of eMobility operators; for instance, an eTicketing Analysis Service suggesting new pricing policies or listing rarely used routes that could be discarded; the third tier concerns *MaaS Operators*, which are eMobility operators that federate and integrate their services with those of other eMobility operators.

From the risks analysed and assessed in the abovementioned work, the ones that fall in the context and scope of the MyCorridor project include: (i) data leakage/theft (also known as packet sniffing), (ii) service behaviour manipulation, (iii) service workflow manipulation, and (iv) pattern extraction (also known as data crossing). These risks are further elaborated below.

10.3.1 Data leakage/theft (packet sniffing)

Web data (web pages, images, emails etc.) are not transferred through the Internet as a whole entity, but as small pieces (packets) of information. These small packets are transmitted via the network, by passing through multiple control devices such as routers and switches; this packet transferring approach makes the information vulnerable to be captured and easy to be exploited by malicious web applications and users. The act of catching information bundles over the network is called *packet sniffing*. It is heavily used by hackers and malicious internet users in order to collect or alter data illegally.

In the context of MyCorridor, a malicious entity could collect information concerning an actor. This information could concern the actor's identity (personal information), as well as business and travel/destination information. Stolen information may include the travel preferences of an actor, the social media and types of services used by him/her, the content that s/he has downloaded, his/her hobbies and interests, his/her preferred payment method, and his/her current location. By collecting (and assembling) such pieces of data/information, a malicious entity gains knowledge about the MyCorridor actor, which can be exploited, for instance, in order to identify the position of an actor, advertise a bunch of products, or associate a user with a trip or a destination.

- A broadly used architectural solution to avoid packet sniffing and protect actors' data is to always use the **HTTPS communication protocol** in order to establish connections between the client and the server of the system; thus, the utilization of the HTTP protocol should be prohibited. In the context of MyCorridor project, the adoption of the HTTPS communication protocol will be implemented before the beginning of the second pilot phase.

10.3.2 Service behaviour manipulation

This type of threats concerns access and modification of services' raw data, as well as manipulation of their logic in order to change their outcomes. In principle, a verification of the correctness of a service should be performed through a service deployment (registration) interface. In practice, its complete verification is a very difficult task. Indicators of correctness include its compliance to a set of acceptable interfaces, communication protocols and data schemas.

Another way to verify the correctness of a service (specifically, the behaviour of a service), which is common in anti-malware checks, is to look at its actual behaviour through static or dynamic analysis [85], aiming to discover possible malicious behaviors. These techniques, which are mainly based on machine learning, graph theory and anomaly detection approaches, are far from infallible and require a considerable amount of data to be credible.

- For the needs of the project, the recommended solution to handle service behavior manipulation risks is through a secure mechanism that can verify the provider of a service (handling typical registration and authentication issues), while also offering the necessary functionalities for service management (registration, editing, viewing etc.). This mechanism should be a dedicated system component. Attention should be given to the design of interfaces offered for service registration, which should "guide" a service provider to easily register a service and strictly define its attributes, business rules, communication means, and formats of data exchanged. The solution proposed in the MyCorridor architecture, namely the **Service Registration Tool (SRT)** in the

presentation layer together with the **Service Provider Business Rules Editor** component in the application layer, satisfies fully the above requirements. The invocation and implementation of more sophisticated mechanisms [83] go out of the scope of the project.

10.3.3 Service workflow manipulation

This type of threats concerns manipulation of the expected workflow among services for various malicious purposes. This is mainly caused by altering the routing of information among services. Such alterations may completely disable a service in a specific workflow (thus making the associated data sources unreachable) or modify the outcome of the whole workflow due to missing data.

The most common approach to deal with this type of threats is through a proper definition of the related access and business rules. All valid workflow compositions are thus logged, and unexpected workflows can be detected and banned (if needed). More sophisticated approaches invoke machine learning mechanisms (similar to the ones used in dynamic malware analysis) to detect malicious workflows [85]. An effective preventive approach comes from the field of choreographic programming, permitting actors to agree on a formal definition of their workflows, which can be later compiled into their respective, compliant services [86].

- ➔ For the needs of the project, the recommended solution to handle service workflow manipulation risks is through a secure mechanism that manages the editing and composition of overall services' business rules. This mechanism should be a dedicated system component. Alike to the recommendations given above, aiming to handle the previous type of threats, attention should be also given here to the design of interfaces offered for overall business rules editing and composition, which should "guide" an authorized actor (i.e. MaaS aggregator) to easily modify the business rules that govern the platform (overall business strategy, tariffs/discount policies, loyalty schemes), and generate new services by composing existing registered services. The solution proposed in the MyCorridor architecture, namely the **MaaS Aggregator Dashboard** in the presentation layer, the **Service Orchestrator** component of the foreseen MaaS API in the communication layer, and the **Overall Business Rules Editor** component in the application layer, satisfies fully the above requirements. The invocation and implementation of more sophisticated mechanisms go out of the scope of the project.

10.3.4 Pattern extraction

This last type of threats concerns malicious activities that search for patterns in the diverse data sources of a MaaS platform. Pattern extraction may have important applications in the MaaS domain, and may facilitate rule extraction or classification. For instance, such a threat can perform data analysis and pattern discovery on tickets related datasets (stored in the associated providers' service data repositories) in order to retrieve sensitive information about business strategies and perform unfair competition; or interrelate data concerning travellers' locations with their identity data to extract patterns about their usual destinations and overall travelling behaviour (i.e. destination tagging).

To respond to this type of threats, an approach recommended for the MaaS context is to deploy data sanitization/masking techniques. These techniques aim at disguising sensitive information in databases by overwriting it with realistic looking but false data of a similar type [87]. This approach is able to appropriately mask the sensitive data and thus deny from malicious actors the possibility to perform pattern analysis. In other approaches, such sanitization/masking techniques are combined with anonymization algorithms that introduce a certain amount of noise and prevent data crossing from external entities [84].

→ The **MongoDB NoSQL** database has been utilized for the needs of the data layer of the MyCorridor project. It has been broadly admitted that MongoDB creates a flexible and consistent environment, which allows the developer to easily store a variety of structured and unstructured documents. At the same time, MongoDB either provides default mechanisms or is compatible with external (easy to be integrated) frameworks to support a list of security measures (for a detailed account, see [44]). We argue that the functionalities offered by the MongoDB solution (including role-based access control, authentication, encrypted communication, data encryption and protection, limitation of network exposure, and auditing facility) are adequate to respond to this type of threats.

10.4 DoS attacks

A DoS attack is an attack meant to shut down a service by making it inaccessible to its users. The method followed by a malicious actor performing a DoS attack is that it tries to overload the targeted service by sending requests that cause a crash. Usually, malicious requests contain huge amounts of data needed to be processed by the service. Hence, while the system tries to respond to the malicious client, it uses all the available resources (e.g. CPU and memory); this is the reason why the service shuts down. In general, DoS attacks occur in high-profile organizations, including banks, commerce and media companies, and government.

There are two main categories of methods of DoS attacks, namely flooding and crashing. A flooding-type attack targets to slow down and stop the server by overloading it. This category includes the following methods:

- Buffer overflow attacks. This is the most common DoS attack. Using this technique, the malicious user sends more traffic to the service than it is able to handle;
- ICMP (Internet Control Message Protocol) flood (also known as Ping flood). This is a common DoS attack in which the attacker shuts down the targeted service by overloading it with ICMP echo requests (also known as pings);
- SYN (short for "synchronize") flood. A SYN flood attack sends a request for connection to the targeted server and never completes the handshake; it continues until all the available ports for connection have been reserved, thus there are no ports available for a real user.

A crashing-type attack identifies and exploits available system's vulnerabilities that cause the system to crash. In this type of attacks, the malicious user sends input data that triggers the weaknesses of the system.

→ For the needs of the MyCorridor project, the recommended solution for making the system resistant to DoS attacks is to: (i) heavily utilize the HTTP Basic authentication; (ii) use only the HTTPS protocol for securing the connections; (iii) allow connections only from trusted/verified users.

10.5 Web services communication

As far as communication between web services is concerned, the two prominent approaches today are Simple Object Access Protocol (SOAP) and Representational State Transfer (REST). MyCorridor has adopted the second solution. Below, we justify why this solution is more reliable and sustainable for the needs of the project.

REST is a software architectural style which defines a set of practices, constraints and techniques to develop web services. In order for a REST web service to be considered RESTful, it has to support all the

HTTP methods (namely GET, HEAD, POST, PUT, PATCH, DELETE, CONNECT, OPTIONS and TRACE). Aiming for fast performance, reliability and reusability, a REST Web service does not utilize any kind of cookies. Also, a REST system needs to fulfil the following constraints:

- Client-server architecture (the separation of the user interface application from the server-side application);
- Statelessness (meaning that no client context is being stored on the server between requests);
- Cacheability (caching frequently used responses for future use);
- Code on demand (e.g. moving business logic from the server to the client side);
- Layered system (e.g. including load balancers and proxy servers that enhance the security of the system).

In contrast to other techniques and protocols, REST architectural style is not restricted to only one specific data format. RESTful web services can send data in plain text, JSON, XML or any preferred other format (as opposed to SOAP which demands XML as data exchange format). This makes the RESTful web services highly adaptable and easily expandable. Moreover, REST uses less bandwidth, making it more suitable for internet usage. Finally, as far as interoperability is concerned, the REST architectural style is the preferred solution since RESTful services are loosely coupled and do not need to follow rigid standards.

➔ For the needs of MyCorridor, the REST software architectural style is the correct choice, due to the project's requirements for high performance, security, reliability, robustness and fast response time. Furthermore, the REST software architectural style is broadly tested and very well documented; the existing available frameworks and libraries that support it outperform those of SOAP technology.

11 Conclusions

The Deliverable D2.2: "MyCorridor interoperable, open and seamless architecture and MyCorridor subsystems and modules specifications" has described in detail the system architecture of the MyCorridor platform. In particular, initially, the concept of TM2.0 was presented along with the benefits it can deliver to a MaaS platform, and the way in which this concept is integrated into the system architecture of the MyCorridor platform was described. Then, the methodology used for designing the system architecture was introduced. The selected UML-based methodology starts from the definition of the system non-functional requirements, proceeds with the definition of the system architecture components and their organization into a layered structure, moves on with the description of the structural submodules and the characteristics of each of the defined system architecture components (i.e. functional architecture) as well as the description of the interactions between them that facilitate the implementation of the defined use cases, and ends up with the definition of the overall system specifications that meet the system non-functional requirements. Finally, the last two sections describe the several interoperability and cross-border security issues that may arise during the operation of a MaaS platform, and present the way in which these issues are handled by design in the MyCorridor platform.

The work presented in this deliverable forms the basis for the actual development of all system architecture components, whose thorough description is provided in the deliverables D3.1: "MyCorridor cloud service delivery platform, service gateway, big data management module and business rules implementer module", D3.2: "MyCorridor traveler feedback integration module" and D3.3: "Mobility

tokens and e-payment services – the “EURO Mobility Ticket” “. Furthermore, the overall services integration process that is the core objective of the WP4: “MyCorridor MaaS” and which will be described in the deliverables D4.1: “Individual services integration into MyCorridor platform” and D4.2: “Aggregated service delivery across MyCorridor MaaS”, heavily depends on the system architecture design presented in this deliverable. Finally, it should be noted that the presented system architecture is subject to future, small-scale changes based on the results of the pilot realizations and the actual system deployment.

References

- [1] “UML.” [Online]. Available: <https://www.uml.org/>. [Accessed: 14-May-2019].
- [2] “VolereRequirementsSpecificationTemplate.” [Online]. Available: <https://www.volere.org/templates/volere-requirements-specification-template/>. [Accessed: 14-May-2019].
- [3] A. Vreeswijk, J., Van den Dries, R. and Gajadien, “Social community approach for traffic management in a MaaS context,” in *International Conference on Intelligent Transport Systems in Theory and Practice, mobil.TUM*, 2017.
- [4] “SWARCO.” [Online]. Available: <https://www.swarco.com/>. [Accessed: 24-May-2019].
- [5] “TomTom.” [Online]. Available: <https://www.tomtom.com>. [Accessed: 24-May-2019].
- [6] “ERTICO – ITS Europe.” [Online]. Available: <https://ertico.com/>. [Accessed: 24-May-2019].
- [7] “TM2.0 Membership.” [Online]. Available: <http://tm20.org/members>. [Accessed: 24-May-2019].
- [8] “TM2.0.” [Online]. Available: <https://tm20.org/>. [Accessed: 24-May-2019].
- [9] “TM2.0 Process.” [Online]. Available: <http://tm20.org/members>. [Accessed: 24-May-2019].
- [10] “DATEX II.” [Online]. Available: <https://datex2.eu/>. [Accessed: 10-Jun-2019].
- [11] “Interreg.” [Online]. Available: <http://interreg-maritime.eu/fr/web/pc-marittimo/home>. [Accessed: 05-Jun-2019].
- [12] “datiToscana.” [Online]. Available: <http://dati.toscana.it/>. [Accessed: 06-Jun-2019].
- [13] “Regional transport observatory.” [Online]. Available: <http://www501.regione.toscana.it/osservatoriotrasporti/>. [Accessed: 10-Jun-2019].
- [14] “SWOT analysis.” [Online]. Available: https://en.wikipedia.org/wiki/SWOT_analysis. [Accessed: 11-Jun-2019].
- [15] “Mobility as a Service (MaaS) Alliance.” [Online]. Available: <https://maas-alliance.eu/>. [Accessed: 27-May-2019].
- [16] “RegioMOVE.” [Online]. Available: <https://www.regiomove.de/>. [Accessed: 06-Jun-2019].
- [17] T. S. Cocone, L., Tsanidaki J., Flament M., Franco G., “Enabling Next Generation Transport Infrastructure: TM 2.0 Paradigm,” in *ITS World Congress*.

- [18] "Unified Modeling Language (UML)." .
- [19] "Volere." [Online]. Available: <https://www.volere.org/>. [Accessed: 14-May-2019].
- [20] "SocialCar." [Online]. Available: <http://socialcar-project.eu/>. [Accessed: 14-May-2019].
- [21] "GDPR." [Online]. Available: <https://eugdpr.org/>. [Accessed: 26-May-2019].
- [22] "Android." [Online]. Available: <https://www.android.com/>. [Accessed: 14-May-2019].
- [23] "iOS." [Online]. Available: <https://www.apple.com/ios/ios-12/>. [Accessed: 14-May-2019].
- [24] "OpenTripPlanner (OTP)." [Online]. Available: <http://www.opentripplanner.org/>. [Accessed: 14-May-2019].
- [25] "LGPL." [Online]. Available: <https://www.gnu.org/copyleft/lesser.html>. [Accessed: 14-May-2019].
- [26] "OpenStreetMap." [Online]. Available: <https://www.openstreetmap.org/>. [Accessed: 14-May-2019].
- [27] "GTFS Static Overview." [Online]. Available: <https://developers.google.com/transit/gtfs/>. [Accessed: 14-May-2019].
- [28] "JSON." [Online]. Available: <https://www.json.org/>. [Accessed: 14-May-2019].
- [29] "XML." [Online]. Available: <https://www.w3.org/TR/REC-xml/>. [Accessed: 14-May-2019].
- [30] "cURL." [Online]. Available: <https://curl.haxx.se/>. [Accessed: 14-May-2019].
- [31] "RapidJSON." [Online]. Available: <http://rapidjson.org/>. [Accessed: 14-May-2019].
- [32] "Angular." [Online]. Available: <https://angular.io/>. [Accessed: 14-May-2019].
- [33] "TypeScript." [Online]. Available: <https://www.typescriptlang.org/>. [Accessed: 10-Jun-2019].
- [34] "JavaScript." [Online]. Available: <https://www.javascript.com/>. [Accessed: 12-Jun-2019].
- [35] "Bootstrap." [Online]. Available: <https://getbootstrap.com/>. [Accessed: 10-Jun-2019].
- [36] "jQuery." [Online]. Available: <https://jquery.com/>. [Accessed: 10-Jun-2019].
- [37] "Place Autocomplete." [Online]. Available: <https://developers.google.com/maps/documentation/javascript/examples/places-autocomplete>. [Accessed: 10-Jun-2019].
- [38] "NoSQL." [Online]. Available: <https://en.wikipedia.org/wiki/NoSQL>. [Accessed: 15-Jun-2019].
- [39] "Whim." [Online]. Available: <https://whimapp.com/>. [Accessed: 24-May-2019].
- [40] "Eve." [Online]. Available: <https://docs.python-eve.org/en/stable/>. [Accessed: 14-May-2019].
- [41] "PythonEve_Authentication_Authorization." [Online]. Available: <https://docs.python-eve.org/en/stable/authentication.html>. [Accessed: 24-May-2019].
- [42] "bcrypt." [Online]. Available: <https://pypi.org/project/bcrypt/>. [Accessed: 24-May-2019].

- [43] "hashlib." [Online]. Available: <https://docs.python.org/3/library/hashlib.html>. [Accessed: 24-May-2019].
- [44] "MongoDB - Security Checklist." [Online]. Available: <https://docs.mongodb.com/manual/administration/security-checklist/>. [Accessed: 24-May-2019].
- [45] "String resources." [Online]. Available: <https://developer.android.com/guide/topics/resources/string-resource>. [Accessed: 24-May-2019].
- [46] "Launch Screen." [Online]. Available: <https://developer.apple.com/design/human-interface-guidelines/ios/icons-and-images/launch-screen/>. [Accessed: 24-May-2019].
- [47] "iOS - Managing strings yourself." [Online]. Available: <https://developer.apple.com/library/archive/documentation/MacOSX/Conceptual/BPInternational/MaintainingYourOwnStringsFiles/MaintainingYourOwnStringsFiles.html>. [Accessed: 24-May-2019].
- [48] "CurrencyConverter." [Online]. Available: <https://pypi.org/project/CurrencyConverter/>. [Accessed: 24-May-2019].
- [49] "DPIA." [Online]. Available: <https://gdpr.eu/data-protection-impact-assessment-template/>. [Accessed: 24-May-2019].
- [50] "MaaS Guidebook." [Online]. Available: <https://maas.guide/>. [Accessed: 27-May-2019].
- [51] "maas-api." [Online]. Available: <http://docs.maas-api.org/>. [Accessed: 27-May-2019].
- [52] "taxi.eu." [Online]. Available: <https://www.taxi.eu/en/>. [Accessed: 22-Jun-2019].
- [53] "Uber." [Online]. Available: <https://www.uber.com>. [Accessed: 20-Jun-2019].
- [54] "CheckMyBus." [Online]. Available: <https://www.checkmybus.com/>. [Accessed: 22-Jun-2019].
- [55] "OpenMP." [Online]. Available: <https://www.openmp.org/>. [Accessed: 21-Jun-2019].
- [56] "POSIX Threads." [Online]. Available: https://en.wikipedia.org/wiki/POSIX_Threads. [Accessed: 21-Jun-2019].
- [57] "GTFS Realtime Overview." [Online]. Available: <https://developers.google.com/transit/gtfs-realtime/>. [Accessed: 20-Jun-2019].
- [58] "Uber API." [Online]. Available: <https://developer.uber.com/>. [Accessed: 21-Jun-2019].
- [59] "ZipCar." [Online]. Available: <https://www.zipcar.com/>. [Accessed: 12-Jun-2019].
- [60] "General Bikeshare Feed Specification - GBFS." [Online]. Available: <https://github.com/NABSA/gbfs>. [Accessed: 22-Jun-2019].
- [61] "Carma API." [Online]. Available: <https://api.car.ma/apidoc/>. [Accessed: 13-Jun-2016].
- [62] "CarpoolWorld API." [Online]. Available: <http://www.carpoolworld.com/developers.html>. [Accessed: 13-Jun-2019].

- [63] “Return on Investment - ROI.” [Online]. Available: https://en.wikipedia.org/wiki/Return_on_investment. [Accessed: 12-Jun-2019].
- [64] “PDF.” [Online]. Available: <https://en.wikipedia.org/wiki/PDF>. [Accessed: 10-Jun-2019].
- [65] “BSON.” [Online]. Available: <http://bsonspec.org/>. [Accessed: 16-Jun-2019].
- [66] “MongoDB.” [Online]. Available: <https://www.mongodb.com/>. [Accessed: 14-May-2019].
- [67] “RDF.” [Online]. Available: <https://www.w3.org/2001/sw/wiki/RDF>. [Accessed: 15-Jun-2019].
- [68] “OWL.” [Online]. Available: <https://www.w3.org/OWL/>. [Accessed: 12-Jun-2019].
- [69] L. Bass, P. Clements, and R. Kazman, *Software Architecture in Practice*. 2013.
- [70] “hashlib.” [Online]. Available: <https://docs.python.org/2/library/hashlib.html>. [Accessed: 14-May-2019].
- [71] “cryptography.” [Online]. Available: <https://github.com/pyca/cryptography>. [Accessed: 24-May-2019].
- [72] “PyPy.” [Online]. Available: <https://pypy.org/>. [Accessed: 10-Jun-2019].
- [73] “PyCrypto.” [Online]. Available: <https://www.dlitz.net/software/pycrypto/>. [Accessed: 24-May-2019].
- [74] “bcrypt.” [Online]. Available: <https://pypi.org/project/bcrypt/>. [Accessed: 14-May-2019].
- [75] “enisa.”
- [76] G. Pangalos, N. Nader, and I. Pagkalos, “Using the NETC@RDS approach as a basis for cross-border electronic authentication,” in *IFIP Advances in Information and Communication Technology*, 2013.
- [77] “The STORK project.” [Online]. Available: ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu. [Accessed: 24-May-2019].
- [78] “STORK 2.0 Interconnection Supporting Service.” [Online]. Available: <https://joinup.ec.europa.eu/solution/stork-20-interconnection-supporting-service/about>. [Accessed: 24-May-2019].
- [79] B. Zwattendorfer, I. Sumelong, and H. Leitold, “Middleware Architecture for Cross-Border Identification and Authentication,” *J. Inf. Assur. Secur.*, vol. 8, no. 2, pp. 107–118, 2013.
- [80] “CAVAL Web Services Specifications for Travel Agents Interoperation.” [Online]. Available: <http://caval.travel/index.html>. [Accessed: 24-May-2019].
- [81] Y. L. Simmhan, B. Plale, and D. Gannon, “A survey of data provenance in e-science,” *ACM SIGMOD Rec.*, 2005.
- [82] C. Dai, D. Lin, E. Bertino, and M. Kantarcioglu, “An approach to evaluate data trustworthiness based on data provenance,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008.
- [83] F. Callegati, S. Giallorenzo, A. Melis, and M. Prandini, “Data security issues in MaaS-enabling

platforms," in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow, RTSI 2016*, 2016.

- [84] F. Callegati, S. Giallorenzo, A. Melis, and M. Prandini, "Insider Threats in Emerging Mobility-as-a-Service Scenarios," *CoRR*, vol. abs/1609.0, 2016.
- [85] M. D. Ernst, "Static and dynamic analysis: synergy and duality," *ICSE Work. Dyn. Anal.*, 2003.
- [86] M. Dalla Preda, S. Giallorenzo, I. Lanese, J. Mauro, and M. Gabbrielli, "AIOCJ: A Choreographic Framework for Safe Adaptive Distributed Applications," 2014.
- [87] N. 2000 Ltd., "Data Sanitization Techniques," *Techniques*, 2000.
- [88] B. Fairbairn, "POPD – Requirement No.1, Deliverable 10.1 MyCorridor (Mobility as a Service in a multimodal European cross-border Corridor) project (G.A.: 723384), <http://mycorridor.eu/>," 2017.
- [89] G. Dovinola, "MyCorridor Ethics Manual, Deliverable 9.2, MyCorridor (Mobility as a Service in a multimodal European cross-border Corridor) project (G.A.: 723384), <http://mycorridor.eu/>," 2017.

Annex 1: Data Management Plan Update

1 Introduction

The current Annex presents the current update of the Data Management Plan (DMP) of MyCorridor as of its first version as being presented in D2.1 (submitted and approved by the EC). It will be referred in the project from now on as DMP v2. Note that some of the provided information in this version (DMP v2) is subject to revision for legal approval and will be updated in the next version of DMP to be released in D6.1 "Pilot plans framework and tools" (DMP 3rd version). In particular, the technical partners of the MyCorridor Consortium have helpfully put together an updated version of the Data Management Plan ("DMP") and a first draft of the Data Protection Impact Assessment ("DPIA"), based on their in-depth technical knowledge. The DMP and DPIA are now being finalised from a legal perspective by the MyCorridor Consortium legal partner, Osborne Clarke. Osborne Clarke is working through this review and will be able to provide an updated version of the DMP and DPIA to be included in the update of D6.1: "Pilot plans framework and tools".

In order to create an effective Mobility as a Service ("MaaS") solution, such as MyCorridor, data is key. As a result, to finalise the DMP and DPIA, Osborne Clarke will need to work closely with its technical Consortium partners over the next few weeks

It details, as it is expected by its nature, how MyCorridor Consortium will manage the data to be collected, processed and used in various ways and for various purposes throughout the project, the Consortium decisions with respect to making the data Findable, Accessible, Interoperable and Re-usable (FAIR) and the respective mechanisms to enable data management decisions. It also details the roles of the different Consortium Partners related to data management.

Next versions of the DMP are expected as follows:

- DMP 3rd version (DMP v3) will be annexed in the update of the D6.1: "Pilot plans framework and tools", that will further elaborate on the data collected and processed in the context of the real-life pilot trials of the project (2nd round) in order to accommodate the purposes of MyCorridor solution and MaaS paradigm evaluation and impact assessment upon the framework defined therein. Refinements to ensure legal approval are also expected in this version.
- DMP 4th version (DMP final) will be annexed in the D6.2: Pilot results consolidation. This will include among other the authorizations whenever required from the ethical committees (of several levels) as well as the DPO (and other) approvals whenever applicable, according to the roles, obligations and mechanisms defined in this document.

Due to the fact that the project will collect user-related data, the Consortium will fully comply with any laws and regulations in any relevant jurisdiction relating to privacy or the use or processing of data relating to natural persons, including: (a) EU Directives 95/46/EC and 2002/58/EC (as amended by 2009/139/EC) and any legislation implementing or made pursuant to such directives and the Privacy and Electronic Communications (EC Directive) Regulations 2003; (b) from 25 May 2018, the EU General Data Protection Regulation 2016/679 ("GDPR"); and (c) any laws or regulations ratifying, implementing, adopting, supplementing or replacing GDPR; in each case, to the extent in force, and as such are updated, amended or replaced from time to time.

The relevant data management aspects are being analysed in this document and are related to a) the data collected and processed in any way in order to allow the operation of the one-stop-shop as well as the validation and impact assessment activities of MyCorridor, b) consortium decisions with respect to



making the data FAIR and the respective mechanisms to support these decisions, c) the security processes to be applied, including data recovery as well as secure storage and transfer of sensitive data and d) the related ethical aspects with respect to e.g., (sensitive) personal data, informed consent, restrictions and constraints of contacting and testing MyCorridor services with real life users, etc., as defined in the ethical framework and policy of MyCorridor [88][89] taking into account European and national/local ethical guidelines and legislation.

2 Data in MyCorridor

2.1 Mission related to Data Management

MyCorridor mission is to facilitate sustainable travel in urban and interurban areas and across borders by replacing private vehicle ownership by private vehicle use, as just one element in an integrated/multimodal MaaS chain. To this end, MyCorridor will provide an innovative platform, based on mature ITS technology that will combine connected traffic management and multi modal services so as to facilitate modal shift. MyCorridor will prove this paradigm change through a number of European sites, which are performing long distance and cross border Pilots in a corridor of 6 European countries; from the South (Greece, Italy) up to Central (Austria, Germany, the Netherlands) and Eastern Europe (Czech Republic). Those sites will develop Mobility Package tokens, purchased through a one-stop-shop and will incorporate several types of transport and added value services.

This mission is split into the following 3 objectives as included in MyCorridor Grant Agreement:

- **Objective 1:** Integration of MaaS vehicles into a multimodal service chains platform;
- **Objective 2:** Provision of a new business paradigm, actor and model for pan-European cross-border adoption; and
- **Objective 3:** Proof of concept of the new business model and integrated platform by selected UC's and performance of full operational analysis and impact assessment through interconnected Pilots across a European corridor.

In order for MyCorridor to achieve its mission and to meet its objectives, a series of data is required to be collected, processed, used and managed, some of which are personal data. Therefore, an analytic Data Privacy Impact Assessment is conducted and provided in section 9. Data collection and processing in MyCorridor adheres to the respective European regulations, encompassing GDPR regulation.

2.2 Clusters of data in MyCorridor

The types of data to be collected and processed, the various ways of collection and processing as well as the rationale in each case are discussed in the Data Privacy Impact Assessment (DPIA) of section 9. The key data clusters are as follows:

1. ***Data collected and processed in order to accommodate the operational functions of MyCorridor one-stop-shop***
 - 1a. *Personalisation data*
 - 1b. *Data logged during usage*
 - 1c. *Traveller feedback data*
 - 1d. *Data related to payment transactions*
 - 1e. *Data related to back-office negotiation*
2. ***Data that will be logged in the mobile devices during Pilots***
3. ***Metadata from the services that will be created by the system to support the system functionalities***
4. ***Data that will be collected during focus groups, surveys and during Pilots***

2.3 Dataset Description

This chapter provides a preliminary template (see Table 30) to be used for describing the datasets to be produced or collected in MyCorridor project. As the nature and extent of the datasets can evolve during the project, changes in the template may occur. The most fields of this template have been completed for the key data clusters of the project in the context of the DPIA in section 9. Still, those will be revised and the missing fields will be added until the end of the project and before the sharing of the data in the context

of the Open Research Data Pilot (ORDP). In specific, the fields that are currently missing are namely the Standards and metadata, the Data Sharing, the Re-used existing data and the Data Utility fields.

Table 30. Dataset Description template.

Dataset Reference	MyCorridor_WPX_AX.X_XX: Each dataset will have a reference that will be generated by the combination of the name of the project, the Work Package and Activity in which it is generated and its version (for example: MyCorridor_WP5_A5.1_01)
Dataset Name	Name of the dataset
Dataset Description	Each dataset will have a full data description explaining the data provenance, origin and usefulness. Reference may be made to existing data that could be reused.
Standards and metadata	<ul style="list-style-type: none"> • The metadata attributes list • The used methodologies
File format	All the format that defines data
Data Origin	Specify the origin of the data.
Data Size	State the expected size of the data
Data Sharing	<p>Explanation of the sharing policies related to the dataset between the next options:</p> <ul style="list-style-type: none"> • Open: Open for public disposal • Embargo: It will become public when the embargo period applied by the publisher is over. In case it is categorized as embargo the end date of the embargo period must be written in DD/MM/YYYY format. • Restricted: Only for project internal use. <p>Each dataset must have its distribution license. Provide information about personal data and mention if the data is anonymized or not. Tell if the dataset entails personal data and how this issue is taken into account.</p>
Archiving and Preservation	The preservation guarantee and the data storage during and after the project (for example: databases, institutional repositories, public repositories, etc.)
Re-used existing data	Y/N. If Yes, state the re-used data and how/from where they were retrieved.
Data Utility	Outline to whom the dataset could be useful – potential secondary users.
Link to Dataset	Url link to actual dataset with the same filename (if Open)

3 FAIR data

MyCorridor project will in principle participate in the Open Research Data Pilot (ORDP) but data marked as “restricted” or under an “embargo” period (see the dataset description above) will be excluded. To this end, the data that will be generated during the project and will be included in ORDP should be ‘FAIR’, that is findable, accessible, interoperable and reusable. These requirements do not affect implementation choices and don’t necessarily suggest any specific technology, standard, or implementation solution.

The FAIR principles were generated to improve the practices for data management and data-curation, and FAIR aims to describe the principles in order to be applied to a wide range of data management purposes, whether it is data collection or data management of larger research projects regardless of scientific disciplines.

With the endorsement of the FAIR principles by H2020 and their implementation in the guidelines for H2020, the FAIR principles serve as a template for lifecycle data management and ensure that the most

important components for lifecycle are covered. This is intended as an implementation of the FAIR concept rather than a strict technical implementation of the FAIR principles.

Making data findable, including provisions for metadata

- The datasets will have very rich metadata to facilitate the findability.
- All the datasets will have a Digital Object Identifiers provided by the MyCorridor public repository (ZENODO; please see below).
- The reference used for the dataset will follow this format: MyCorridor_WPX_AX.X_XX, including clear indication of the related WP, activity and version of the dataset.
- The standards for metadata will be defined in the “Standards and metadata” section of the dataset description table (see the current version of the template in the previous section).

Making data openly accessible

- Datasets openly available are marked as “Open” in the “Data Sharing” section of the dataset description table (see Table 30).
- The repository that each dataset is stored, including Open access datasets, is mentioned in the “Archiving and Preservation” section of the dataset description table (see Table 30). ZENODO will be one of the considered options.
- “Data sharing” section of the dataset description table (see Table 30) will also include information with respect to the methods or software used to access the data of each dataset.
- Data and their associated metadata will be deposited either in a public repository or in an institutional repository.
- “Data sharing” section of the dataset description table (see Table 30) will outline the rules to access the data if restrictions exist.

Making data interoperable

- Metadata vocabularies, standards and methodologies will depend on the repository to be hosted (incl. public, institutional, etc.) and will be provided in the “Standards and metadata” section of the dataset description table (see Table 30).

Increase data re-use (through clarifying licenses)

- All the data producers will license their data to allow the widest reuse possible. More details about license types and rules will be provided in the final version of the DMP.
- “Data Sharing” section of the dataset description table (see Table 30) is the field where the data sharing policy of each dataset is defined. By default, the data that will be made available will be available for reuse. If any constraints exist, an “embargo period” or “restricted flag” will be explicitly raised in this section of Table 30.
- The data producers will make their data available for third-parties within public repositories only for scientific publications validation purposes.

4 Open Access approach

MyCorridor Consortium has agreed to follow an “open access” approach (as much as possible depending on the specific data type) following the respective Horizon 2020 guidelines to ensure that the results of the project provide the greatest impact possible. MyCorridor will ensure the open access¹ to all peer-reviewed scientific publications and Deliverables relating to its results and will provide access to the research data needed to validate the results presented in deposited scientific publications. Publications and research data made available to third parties will not contain any personal information.

¹ http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/open-access_en.htm

The following lists the minimum fields of metadata that should come with a MyCorridor project-generated scientific publication in a repository:

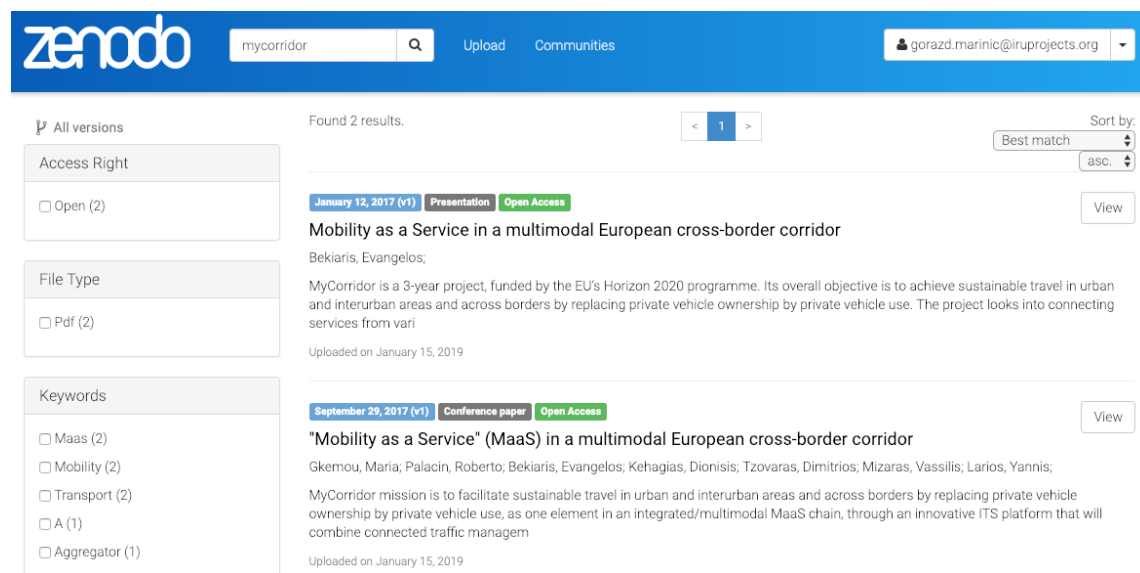
- The terms: “European Union (EU)”, “Horizon 2020”
- Name of the action (Research and Innovation Action)
- Acronym and grant number (MyCorridor, 723384)
- Publication date
- Length of embargo period if applicable
- Persistent identifier

When referencing Open access data, MyCorridor will include as a minimum the following statement demonstrating EU support (with relevant information included into the repository metadata):

“MyCorridor is funded by the European Union within Horizon 2020 research and innovation programme under grant agreement No 723384”.

The MyCorridor Consortium will strive to make many of the collected datasets open access. When this is not the case, the data sharing field for that particular dataset will describe why access has been restricted (see dataset description in section 2.3).

MyCorridor has started making its public Deliverables and publications available with Open Access in ZENODO², which is a free service developed by CERN under the EU FP7 project OpenAIREplus (grant agreement no.283595), under a dedicated account for MyCorridor. Under the same account, all the research derived datasets that will emerge in the project and will be decided to be **Open** for sharing by the Consortium will be shared. By the end of the project, this process will have been completed.



With regard to the specific repositories where MyCorridor datasets will be held during and after the project, they will be noted in the “Archiving and Preservation” field of the dataset. In cases where the project partners maintain additional institutional repositories, these will be also listed in the final DMP version.

² <https://zenodo.org/>

In summary, as a baseline MyCorridor partners shall deposit:

- Scientific publications – in ZENODO dedicated repository of the project, on their respective institute repositories (when relevant) as well as in the Library of the project web site.
- Research data – in ZENODO dedicated repository of the project.
- Other public project output files (i.e. Deliverables) – in ZENODO dedicated repository of the project and the project web site.

This version of the DMP does not include the actual metadata about the Research Data being produced in MyCorridor project. Details about technical means and services for building repositories and accessing to this metadata will be provided in the next version of the DMP. The initial template document is provided in Chapter 2.3 and will be used by project partners to provide all requested information.

5 Key Data Management roles and assignment in MyCorridor

5.1 Key GDPR roles and assignment in MyCorridor

According to GDPR principles, the following roles, and then assignments, are identified.

1. **Data manager** is the natural or legal person that coordinates the actions related to data management, is responsible for the actual implementation of the DMP successive versions and for the compliance to Open Research Data Pilot guidelines. In MyCorridor, this role is undertaken by **Aimilia Bantouna (WINGS)** who is the leader of DMP Deliverables in the project (D2.1 and its updates).
2. **Data controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In MyCorridor this role is undertaken primarily by **Gennaro Ciccarelli (TTS)**, as TTS is responsible for the evaluation WP (WP6) and the impact assessment task (A6.4) of the project and, secondarily, by **Katerina Toulou (CERTH/HIT)** being the leader of *A6.1: Pilot plans and impact framework*; thus meaning they both determine which type of data will be logged/collected/stored and processed and for which purpose.
3. **Data processor** is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller and under its guidance. In MyCorridor, data processors are all entities participating in user trials as well entities holding modules of the one-stop-shop. In specific, in MyCorridor, those are as follows:
 - **CERTH/ITI**: Implementer and holder of the back-end platform of the one-stop-shop.
 - **CERTH/HIT**: Implementer and holder of the front-end part of the application.
 - **AMCO**: Implementer and holder of the back-office module (external module to the back-end of the one-stop-shop).
 - **VivaWallet**: Implementer and holder of the payment module (external module to the back-end of the one-stop-shop).
 - **Operational (meaning recruiting local users) test sites**: SRFG, MAPTm, SWARCO MIZAR, RSM, CERTH/HIT, Chaps, AMCO

Notes/clarifications:

1. *In the context of the first pilot round that was a lab test and in the context of the focus groups of the second round as well as in the context of the focus groups of WP1, pseudonymized data of the participants are collected on local level. Still, the performance/usage data of the travellers related to mobility – to be logged in the context of the 2nd real life pilot round – will be all automatically logged in the back-end platform of the one-stop-shop or, in addition and if needed, through another*

GDPR compliant centrally operated mobile analytics platform.

2. *The front-end modules (Android and iPhone devices that will be running the mobile applications that have been developed), even if they store any personal or other data locally belong to the travellers themselves; as such, it is not an objective of MyCorridor data management.*
3. *Data processing” encompasses also any type of “data storage”, temporary or not.*
4. **Data Protection Officer (DPO)** is an enterprise security leadership role to oversee data protection strategy and implementation to ensure compliance with GDPR requirements. The DPO assists the controller or the processor in all issues relating to the protection of personal data. As of 25 May 2018, Regulation (EU) 2016/679 has made mandatory for every public authority and corporation that handles personal data in the EU to have a data protection officer. **In the case of MyCorridor, all entities as mentioned in point 3 above have checked if they are obliged to have a DPO appointed on entity level and proceed with the necessary actions. This is denoted in section 5.2 of this document.**
5. **Supervisory Authority (or Data Protection Authority; <https://gdpr-info.eu/art-51-gdpr/>)** is a public authority in an EU country responsible for monitoring compliance with GDPR. An EU country within the European Union is also referred to as a *member state*. The key role of the Supervisory Authority is:
 - to advise companies about GDPR
 - conduct audits on compliance with GDPR
 - address complaints from data subjects
 - issue fines when companies are deliberately not complying with GDPR.

In the case of MyCorridor, this means that even if the entity is not obliged to have a DPO, each data processor has checked if they are obliged to obtain approval by the respective authority of their country.

6. A **data subject** ‘is a natural person whose personal data is processed by a controller or processor’. In MyCorridor, those subjects are all those participating in focus groups, user surveys and pilot activities. However, we use the term user/participant, as it is more appropriate to both their involvement and role in the MyCorridor pilots.

Another type of body, not relevant to the GDPR but relevant to the data management of the project is the Ethics Committees on institutional or country level. Those are Committees that may exist on your entity/institutional AND/OR on national level and from which all entities participating in user trials may need to get approval before proceeding with user trials. As mentioned, they are not relevant to GDPR bodies (though they might address data privacy issues as well), but actually they pre-existed and they tackle with issues related to safety, risk assessment and security of the trials that will be conducted. Ethical issues are addressed in the context of the relevant activities of the project.

5.2 Data processed per entity & GDPR obligations

In the table below, each data processor is associated to the type(s) of data that will administer (or has administered in the past) in the context of the project.

Data Collector/Processor (entity - country)	Role in the project	Type of data processed
CERTH/ITI – Greece	Implementer and holder of the back-end platform of the one-stop-shop.	<ul style="list-style-type: none"> • Data collected and processed in order to accommodate the

Data Collector/Processor (entity - country)	Role in the project	Type of data processed
		operational functions of MyCorridor one-stop-shop <ul style="list-style-type: none"> • Metadata from the services that will be created by the system to support the system functionalities
CERTH/HIT - Greece	Implementer and holder of the front-end part of the application & test sites.	<ul style="list-style-type: none"> • Data that will be logged in the mobile devices during Pilots • Data that will be collected during focus groups, surveys and during Pilots
AMCO – Greece	Implementer and holder of the back-office module (external module to the back-end of the one-stop-shop) & Test site.	<ul style="list-style-type: none"> • Data collected and processed in order to accommodate the operational functions of MyCorridor one-stop-shop (Back-office)
VivaWallet – Greece	Implementer and holder of the payment module (external module to the back-end of the one-stop-shop).	<ul style="list-style-type: none"> • Data collected and processed in order to accommodate the operational functions of MyCorridor one-stop-shop (Payment)
SRFG (Austria), MAPTm (the Netherlands), SWARCO MIZAR (Italy), RSM (Italy), Chaps (Czech Republic)	Test sites.	<ul style="list-style-type: none"> • Data that will be collected during focus groups, surveys and during Pilots.

Upon the above classification as well as the legal status of each entity/country towards GDPR, the following table presents the relevant information for each data processor in MyCorridor. For each entity that is obliged to a DPO approval, all the mechanisms that are described in DPIA of section 9 will be applied.

Data Processor (entity - country)	DPO position in the entity [Yes/No]	If Yes, provide DPO contact [Name; E-mail]	Availability of Supervisory Authority (Data Protection Authority) that need to get approval from [Yes & Name/No and which one by name]	If the entity is not obliged for any reason (i.e. for the concrete test conditions of MyCorridor) to get any or some of the approvals requested, please explain in short here why.
CERTH/ITI - Greece	Yes, at CERTH organization level.	Ioannis Chalinidis; ivchal@certh.gr	No	After the GDPR implementation, no DPA approval is required. The process is handled internally (decision only available in Greek).
CERTH/HIT - Greece	Yes, at CERTH organization level.	Ioannis Chalinidis; ivchal@certh.gr	No	After the GDPR implementation, no DPA approval is required. The process is handled internally (decision only available in Greek).
AMCO - Greece	No	Not applicable	No	After the GDPR implementation, no DPA approval is required. The process is handled internally (decision only available in Greek).
VivaWallet - Greece	No	Not applicable	No	After the GDPR implementation, no DPA approval is required. The process is handled internally (decision only

Data Processor (entity - country)	DPO position in the entity [Yes/No]	If Yes, provide DPO contact [Name; E-mail]	Availability of Supervisory Authority (Data Protection Authority) that need to get approval from [Yes & Name/No and which one by name]	If the entity is not obliged for any reason (i.e. for the concrete test conditions of MyCorridor) to get any or some of the approvals requested, please explain in short here why.
				available in Greek)
SRFG (Austria)	No	Not applicable	There is a Data Protection Authority in Austria but SRFG does not need to get approval for the conduction of the pilots.	SRFG is required to register activities only at the data processing register (which it did). It is not required to get consent for the processing of personalized data from the Data Protection Authority in Austria, especially since we are pseudonymising or anonymising the data that we collect during the pilots, focus groups, etc.
MAPTm (the Netherlands)	YES	Giovanni Huiskens, Giovanni.huiskens@maptm.nl	The Dutch authority is Autoriteit Persoonsgegevens but no special approval is needed as long as the GDPR is respected.	N/A
SWARCO MIZAR (Italy)	YES	Peter Suhren FIRST PRIVACY GmbH; office@first-privacy.com	YES The Italian Data Protection Authority (legislative decree	N/A

Data Processor (entity - country)	DPO position in the entity [Yes/No]	If Yes, provide DPO contact [Name; E-mail]	Availability of Supervisory Authority (Data Protection Authority) that need to get approval from [Yes & Name/No and which one by name]	If the entity is not obliged for any reason (i.e. for the concrete test conditions of MyCorridor) to get any or some of the approvals requested, please explain in short here why.
			No. 196/2003); Giuseppe Busia is currently Secretary General to the DPA, garante@gpdp.it	
RSM (Italy)	<i>Yes (external to the entity; details to be confirmed in the next version)</i>	<i>Details to be provided in the next version.</i>	<i>No need for approval; to be confirmed in the next version.</i>	
Chaps (Czech Republic)	NO	N/A	NO	Not required for such type of research.

All research entities participating in the MyCorridor project shall ensure that they have entered into an appropriate data sharing agreement prior to any personal data being shared.

6 Data Security

MyCorridor open cloud system will provide out-of-the-box security mechanisms and management procedures so as to a) ensure personal (sensitive) data protection through a strict process of data collection, anonymization, harmonization and integration and b) guarantee data integrity and reliability, ensuring system's high performance operation through the exchange of the necessary information.

The consortium research partners will fully comply at all times with all applicable data protection legislation and regulation during this project, to ensure the security and protection of individuals' personal information in relation to this project. This includes compliance with the General Data Protection Regulation (GDPR), as of 25 May 2018. The consortium and research partners acknowledge the various new obligations and the new rights granted to data subjects under the GDPR and are aware of the significant fines that may be imposed should a data breach occur.

In terms of **personal data protection**, personal data will be anonymised and strictly used for project's purposes. Before collecting any personal data, the Local Ethics Representative (see Chapter 3 of D9.2 "MyCorridor Ethics Manual" [89]) will be responsible for informing the involved pilot users/participants and collecting their informed consents (see Chapter 7.2) that will be maintained and stored based on the Grant Agreement rules and European/local laws. No personal data will be centrally stored, without

anonymization or pseudonymisation. No personal information will be made available by the Local Ethics Representative to the pilot sites, i.e., MyCorridor partners participating in the pilots. Only one person per site (the Local Ethics Representative) will have access to the informed consent form containing the personal information and only that person will be aware of the relation between the participant's unique identifier code and their personal identity, in order to administer the tests. In practice, the Local Ethics Representative will collect those data required for contacting the participants and arranging with them the sequence of the current or future tests. The Local Ethics Representative will then issue a single Test ID (unique identifier code) for each of them. This person (Local Ethics Representative) will not participate in the evaluation and will not know how each user behaved. One month before the end of the project, this reference, i.e., the reference between the Test ID and the real-life contact details of the participant, together with any other personal information held on the participant will be deleted, thus safeguarding full anonymization of the results.

The stored data will refer to a user's age, gender, nationality and preferences for travelling and commuting (see the exhaustive list in DPIA of section 9) but this information will be safeguarded, stored and processed only in accordance with all applicable data protection laws and regulations. The stored data will not contain any other identifier apart from the Test ID. In no circumstances will a participant be asked for information relating to their beliefs, political or sexual preferences. User-related data will be securely and safely stored. Also, data will be scrambled where possible and abstracted to permit its use to achieve project outcomes while ensuring data integrity and security.

Any party which provides any data or information (the "Providing Party") to another party (the "Receiving Party") in connection with the project will not include any personal information relating to an identified or identifiable natural person or data subject. To this end, the Providing Party will anonymise or pseudonymise all data delivered to other parties to an extent sufficient to ensure that a person without prior knowledge of the original data and its collection cannot, from the anonymised or pseudonymised data and any other available information, deduce the personal identity of participants.

Each party shall be solely responsible for the selection of specific database vendors/data collectors/data providers, and for the performance (including any breach) of its contracts between it and such database vendors/data collectors, (to which no other project partner shall be a party, and under which no other partner assumes any obligation or liability) and shall further warrant that it has the authority to disclose the information, if any, which it provides to the other parties, and that where legally required and relevant, it has obtained appropriate informed consents from all the individuals involved.

Partners supplying special data analysis tooling, shall have the right on written notice and without liability to terminate the license that it has granted for such tooling to be used in connection with the project, if the supplying partner knows or has reasonable cause to believe that the processing of particular data through such tooling infringes the rights (including without limitation privacy, publicity, reputation and intellectual property rights) of any third party, including of any individual.

Each pilot site will have its own Ethics Committee and one person will be nominated per site as responsible for following the project's Ethics Management Panel (EMP) recommendations and data protection (see D9.2 "MyCorridor Ethics Manual" [89] for more).

In terms of **privacy of MyCorridor system**, the following rules apply:

- All required user data will be stored at their profile and be securely protected by the relevant WP2 mechanism. Relevant preferences relate to their transportation modes and everyday mobility and transfer preferences. The user will have the option to set or delete their profile. No identification data will be stored, they will all be anonymised and aggregated and will only serve analysis purposes;

- The user's location and route will be only temporarily stored (i.e., during a trip), in order to assist the user and the system to provide the appropriate mobility product; they will be automatically deleted afterwards, unless the user wishes to store them;
- The user will have the capacity to view, change or delete- as he/she wishes- all stored data by the system (including their profile data, if chosen to be stored).

7 Ethical aspects

7.1 Ethical and legal issues related to data sharing

The project involves data collection in the context of user testing and demonstration activities. For this reason, human participants will be involved in certain aspects of the project and data concerning their profile, their preferences and driving/riding behaviour, their usage history of searching and selecting services will be collected. Given that these data are considered personal (even sensitive in cases such as the health status), the core ethical/legal issues within MyCorridor related to data collection and sharing are:

- Privacy protection and confidentiality;
- Informed consent;
- Incidental findings;
- Transparency of the collected data management by the final system and during its pilots;
- IT-Security and identity management;
- Risk assessment (Insurance);
- Delegation of control; and
- Incentives (Financial inducements, etc.).

The proper management of these issues is carefully investigated and monitored within WP10 and A9.3 led by the Ethics Manager and supported by Ethics Board. All relevant principles and the main procedures regarding privacy, data protection, security, legal issues and ethical challenges are defined in the Project's Ethics Manual [89] and will be updated in their upcoming versions. The described procedures have been drafted and will be updated in consultation with the project's Ethics Management Panel (composed of one external member, the Coordinator, the Technical & Innovation Manager and the Quality Manager) that will act as supervisors of the ethical activities of the project and the local ethics committees at each pilot site, in order to take into account both European and national ethical and legal requirements.

7.2 Informed Consent

MyCorridor scenarios will target participants with competence to understand the informed consent information. Pilot sites, i.e., MyCorridor partners participating in the pilots, will receive only anonymised and coded or pseudonymised information. Any recorded data will be available to pilot sites only in anonymised format.

The informed consent form, which each participant will be asked to complete prior to their participation in the pilots, aims at ensuring that the user accepts participation and is informed about all relevant aspects of the research project; it will be collected in written form after the users have been provided with clear and understandable information about their role (including rights and duties), the objectives of the research, the methodology used, the duration of the research, the possibility to withdraw at any time, confidentiality and safety issues, risks and benefits.

The basic elements of the MyCorridor informed consent include:

1. The objective of the study, its duration and procedure

2. Possible risks, discomforts and side-effects
3. Privacy and data protection procedures
4. The possibility to decline the offer and to withdraw at any point of the process (and without consequences)
5. Contact person

All test volunteers will receive detailed oral information. In addition, they will receive in the language of the country conducting the test pilot:

- a commonly understandable written description of the project;
- the project goals;
- the planned project progress;
- the related testing and examination procedures;
- advice on unrestricted disclaimer rights on their agreement.

The latest version of the GDPR compliant informed consent form for MyCorridor is provided in Annex 2.

8 GDPR & Ethics related implications/obligations for MyCorridor

The GDPR aims to secure the privacy rights of EU citizens but it is also designed to bolster innovation. This duality has resulted in some key differences between the GDPR and the Data Protection Directive that are relevant to MyCorridor personal data processing activities.

8.1 Research privilege and consent

As a research and innovation action, MyCorridor processes personal data only for research and evaluation purposes of pilot tests. GDPR has done away with many restrictions on data processing for research purposes. This has resulted in the easing of a number of conditions on secondary data processing (Article 6(4); Recital 50) and, to some extent, on the requirement for data subjects' consent (Article 6(1)(f); Recitals 47, 157), as long as adequate safeguards are put in place for data processing. Just like the broad definition of privacy in the GDPR, 'research' is also interpreted broadly.

Despite the relaxing of conditions on data processing for research, MyCorridor will continue eliciting unambiguous consent from subjects after giving them the appropriate information in clear and simple terms using the GDPR compliant informed consent forms. All test sites will use standard protocols for the use of these consent forms to inform users on what we do with the data, and get their approval for this.

8.1.1 Privacy by design

The GDPR states that "the controller shall...implement appropriate technical and organisational measures...in order to meet the requirements of this Regulation and protect the rights of data subjects". MyCorridor DMP's detail the procedures that will be followed to ensure compliance with the GDPR requirement for data processors and controllers to hold and process only the data necessary for its activities (data minimisation), as well as the limitation of access to personal data to those needing it for processing (Article 23).

8.1.2 Data protection officer and GDPR roles and back-up mechanisms applied

Under the GDPR regulation, approval by a Data Protection Officer (DPO) or notification of the Data Protection Authority (DPA), “whichever applies according to the Data Protection Directive (EC Directive 95/46, currently under revision, and the national law” apply to **controllers and processors whose core activities consists of operations requiring regular and systematic monitoring of data subjects on a large scale and who processes special categories of data** (Article 35).

As MyCorridor **does not fall into these categories**, it is not mandatory to appoint a DPO or get authorisation from DPAs. Still, and despite the fact that MyCorridor is not obliged to appoint a DPO or get authorisation from DPAs, and on top of establishing all the defined roles in the project MyCorridor has already applied the following mechanisms to be on the safe side, all data processors of MyCorridor have been asked to investigate if:

1. Their entity is obliged to establish a DPO on institutional level and who is that.
2. If obliged to DPO, to get written approval that they are authorised to proceed with the planned research tasks and approval on the DPIA risk measures; all relevant mechanisms defined in the context of section 9 DPIA.
3. If, regardless of the existence of an Institutional DPO, they are obliged to take and submit approval by the National Data Agency.

As being evident through section 5, it seems (to be reconfirmed in the next version) that the vast majority of them are not obliged to any type of GDPR related approval for MyCorridor.

8.1.3 Internal record keeping

To comply with GDPR requirements on record keeping (Article 30), MyCorridor asks all data controllers and processors acting on behalf of the data controller (all acting under the auspices of the project Data Manager) to record their processing activities in standard forms (Annex 3); basically those referring to personal data. These forms include information regarding the contact information of the data controller(s) and processor(s), purpose and categories of processing, a general description of the technical and organisational security measures, etc. These are submitted to the project Data Manager and, in turn, Project Coordinator for presentation when needed.

9 Data Privacy Impact Assessment

The first version of the Data Privacy Impact Assessment (DPIA) has been essentially prepared in view of the first and second pilots of the project. The herein provided version stands as the current version of DPIA. Still, DPIA is an evolving process in the project. As such, continuous updates fed by respective developments in the project as well as the currently undergoing revisions for legal approval will emerge. Nevertheless, the next and close to final revision of the DPIA will be held and close before the start of the 2nd pilot round and will be included in the 3rd version of DMP that will be annexed in the update of D6.1. In particular, the technical partners of the MyCorridor Consortium have helpfully put together an updated version of the Data Management Plan ("DMP") and a first draft of the Data Protection Impact Assessment ("DPIA"), based on their in-depth technical knowledge. The DMP and DPIA are now being finalised from a legal perspective by the MyCorridor Consortium legal partner, Osborne Clarke. Osborne Clarke is working through this review and will be able to provide an updated version of the DMP and DPIA to be included in the next version of D6.1. In order to create an effective Mobility as a Service ("MaaS") solution, such as MyCorridor, data is key. As a result, to finalise the DMP and DPIA, Osborne Clarke will need to work closely with its technical Consortium partners over the next few weeks. The final one will be part of the last DMP of the project; annexed in D6.2.

In addition to the DPIA, the data privacy policy of the project is continuously being updated adhering to the evolving outcome of the DPIA running in the project. The current data privacy policy of the project can be reached through the project web site ([MyCorridor data privacy policy](#)), will be found in the service registration tool (intended for the service providers) and the mobile apps (intended for the travellers), whereas, the final version of it will be also attached at D7.3: B2B master contract, B2C terms of use, privacy and cookie policy.

9.1 Intro

The Privacy Impact Assessment is required under Article 35 of the General Data Protection Regulation (EU) 2016/679. A PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions. For the DPIA in MyCorridor, we have followed a respective GDPR compliant template, customised for the needs of the project, which follows decomposed and accordingly answered in the sections below. MyCorridor responses are *in Blue Font and Italics*.

Why should I do a PIA?	When should I start a PIA?
<ul style="list-style-type: none"> <i>To identify privacy risks to individuals.</i> <i>To identify privacy and data protection compliance liabilities for your organisation.</i> <i>To protect your reputation.</i> <i>To instil public trust and confidence in your project/product.</i> <i>To avoid expensive, inadequate “bolt-on” solutions.</i> <i>To inform your communications strategy.</i> 	<p><i>PIAs are most effective when they are started at an early stage of a project, when:</i></p> <ul style="list-style-type: none"> <i>the project is being designed;</i> <i>you know what you want to do and how you're going to do it;</i> <i>you know who else is involved.</i> <p><i>But ideally it should be started before:</i></p> <ul style="list-style-type: none"> <i>decisions are set in stone;</i> <i>you have procured systems; and</i> <i>you have signed contracts/MOUs/agreements.</i>

9.2 Do I have to do a PIA?

Determining if you need to do a PIA - screening questions

Answering **yes** to **any** of these questions indicates that a PIA is necessary.

- Will the project involve the collection of new information about individuals? *Yes*
- Will the project compel individuals to provide information about themselves? *In the context of focus groups, user surveys and interviews, the project has and will ask information about participants. Apart from that, through the personalisation mechanism that is put in force – in the context of the one-stop-shop – the travellers are asked optionally and only if they wish to get personalised services to provide information about themselves. Finally, the service providers who wish to register their service through the project service registration tool are asked to provide information about their service.*
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? *The information about individuals, meaning travellers, will be disclosed only to the project Consortium for research purposes. The service providers that are not part*

of the Consortium will not have access to any information for travellers; other than the one they already (possible) have from the operation of their service.

- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? *Yes. Traveller preferences and intention data as well as traveller behaviour data will be indeed collected either to allow the operation of the one-stop-shop or to accommodate research purposes; meaning validation of the MyCorridor solutions and MaaS paradigm and its impact assessment against several layers (mobility patterns, impact on traffic efficiency, environment, etc.). Still, data minimisation principle will be applied as much as possible and applicable.*
- Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. *Non-intrusive technologies will be used. Non direct privacy intrusiveness is anticipated. For example, positioning data of the travellers will be logged to allow smooth operation of MaaS provided (i.e. with regard to traffic management support). As another example, the tracking of travel choices – along several aspects – will be held; either because it is a requirement for a function of the system or because it is of MyCorridor research interest. We additionally recorded data without identifying the users. The mobile phone screen was recorded with a screen cast application and a camera recorder the user's interactions with the mobile application (hands and screen). In all cases, informed consent for all of them will be an absolute prerequisite by the travellers, whilst the data privacy policy of the project will be prompt to the participants prior to signature.*
- Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? *No*
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private. *We collect accessibility information. However, these pieces of information are important for creating the user profile. There is a necessity in order to provide to the user adequate and appropriate travelling experience. User information and travel preferences are anonymised and coded and as such cannot be identified. Will the project require you to contact individuals in ways which they may find intrusive? No*

9.3 Step 1: Identify the need for a DPIA

Explain broadly what aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as relevant deliverables and other supportive documents that reside in SharePoint. Summarize why you identified the need for a DPIA.

1. Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

MyCorridor is a 3-year project, funded by the EU's Horizon 2020 programme. Its overall objective is to achieve sustainable travel in urban and interurban areas and across borders by replacing private vehicle ownership with private vehicle use. The project looks into connecting services from various service providers and providing the travelers with alternatives to replace their own vehicle trip with combined shared vehicles and multimodal transport solutions. The project is part of the Mobility as a Service (MaaS) concept that puts users at the core of transport services, offering them tailor-made mobility solutions based on their individual needs and preferences. Throughout the project activities, a MaaS one-stop-shop will be developed that will be accessed via mobile applications in Android and iPhone by the travelers. The 2 phases Pilots of the project will evaluate the performance and added value of the one-

stop-shop developed in the project but also of the MaaS paradigm overall through it across several aspects (i.e. shift of mobility patterns, traffic efficiency, user acceptance and experience, etc.).

2. You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Relevant documents are namely the Grant Agreement of the project, all project documentation released so far, but especially D1.1: “MyCorridor Use Cases”, D2.1: “Data management plan”, D2.2: “MyCorridor interoperable, open and seamless architecture and MyCorridor subsystems and modules specifications”, D3.1: “MyCorridor cloud service delivery platform, service gateway, big data management module and business rules implementer module”, D5.1: “Profiling mechanism and personalization algorithms”, D5.2: “Mobile applications and interfaces” and D6.1: “Pilot plans framework and tools”.

3. Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

A PIA is performed in MyCorridor as among the data that will be collected and processed during system operation in the project pilots, personal information will be also collected for creating the user profile and preferences. Apart from that traveller behavior data, some of which being personal, will be collected for the research tasks of the project (i.e. evaluation of one-stop-shop, impact assessment studies). Pilots will involve user testing with users, where data will be anonymously collected but, especially for the 1st phase, data will be pseudonymised in most pilot sites.

9.4 Step 2: Describe the processing

Describe the nature of the processing:

1. How are you collecting, using, storing and deleting data?

It is necessary to distinguish the major categories of data sources, as follows:

2. Data collected and processed in order to accommodate the operational functions of MyCorridor one-stop-shop

This cluster of data consists of the following categories:

1a. Personalisation data: *MyCorridor one-stop-shop will offer personalised, context-aware and inclusive MaaS services. In order to do so, it encompasses the following processes:*

- a) user profiling for matchmaking algorithms (running in the back-end) operation resulting in personalised services (context and user specific). In specific, matchmaking takes place in the back-end of the system, receiving as input the travellers’ profiles and personalisation indices and providing as output the mobility package that considers as the most appropriate for them. This matchmaking input-output – which is associated to personalisation– is perhaps one of the most interesting types of data that will be available in MyCorridor, as they will associate traveller’s preferences and profiles to mobility recommendations/outputs/products, the acceptance of which will be later objectively validated through actual usage;*
- b) device-oriented adaptation (e.g., to specific types of devices, Hardware model, Operating system and versions, on different screen sizes and screen resolutions, Preferred language, Time zone settings to address individual preferences, adhering also to key accessibility principles)*

The above processes require the collection, the processing and the management of different types of data, the main categories of which are as follows:

- a) User’s profile;*

Describe the nature of the processing:

- b) User's preferences
- c) Traveller behaviour history of searching and selecting/using services
- d) Traveller position

1b. Data logged during usage: A series of data will be logged during performance – meaning **during travellers' interaction with the one-stop-shop** through the mobile application. In specific, the following data is logged during use of the MyOSS app by the travellers:

1. Number of MaaS&Go trips
2. Average number of legs per MaaS&Go trip
3. Average number of different services per MaaS&Go trips
4. Average number of mobility/infomobility/TM services/added value services selection per MaaS&Go trip
5. Average number of different transportation mode ("CAR", "METRO", "BUS", etc.) services selection per MaaS&Go trip
6. Average weight of different services per MaaS&Go trip
7. Average rating of different services per MaaS&Go trip
8. Number of MaaS packages
9. Average number of different services per MaaSPacks purchase
10. Average number of mobility/infomobility/TM services/added value services selection per MaaSPacks purchase
11. Average number of different transportation mode ("CAR", "METRO", "BUS", ..) services selection per MaaSPacks purchase
12. Average weight of different services per MaaSPacks purchase
13. Average rating of different services per MaaSPacks purchase
14. For each service of the one stop shop:
 - a. Number of times the service has been selected
 - b. Number of times the service was selected by travellers per different age range ["21 and Under"; "22 to 34"; "35 to 44"; "45 to 54"; "55 to 64"; "65 and Over"]
 - c. Number of times the service was selected per type (as internally clustered) of travellers ["DAILY_COMMUTER"; "BUSINESS_TRAVELLER"; "SPONTANEOUS_USER"; "BLEISURE"; "MEDIUM_IT_LITERACY_USER"; "MOBILITY_RESTRICTED_USER"]
 - d. Number of times the service was selected by travellers per type of routing preference ["SHORTEST"; "NEAREST"; "CHEAPEST"; "FEWER_INTERCHANGES_TRANSFERS"; "FASTEST"]
 - e. Number of times the service was selected by travellers with payment method preference ["BY_CARD"; "BY_PAYPAL"; "PREPAID_CARD"; "MASTERPASS"; "BANK_TRANSFER"; "CASH_AT_PAYMENT"]
 - f. Number of times the service was selected by travellers per transportation mode preference ["CAR"; "METRO"; "BUS"; "RAIL"; "TRAM"; "FERRY"; "TAXI"; "BIKE"; "WALK"]
 - g. Number of times the service was selected by male and female travellers
 - h. Number of times the service was selected by travellers who want to travel with their pets
 - i. Number of times the service was selected by travellers who want to have a meal when travelling
 - j. Number of times the service was selected by travellers who travel with luggage
 - k. Number of wheelies of the travellers that selected the service
 - l. Number of times the service was selected by travellers per cost preference ["ECONOMY"; "STANDARD"; "PREMIUM"]

Describe the nature of the processing:

- m. Number of times the service was selected by travellers per type of accessibility preference ["WHEELCHAIR_MOBILITY_RESTRICTIONS"; "HEARING_IMPAIRMENTS"; "COGNITIVE_DISABILITIES"; "OLDER_USERS"; "BLIND_VISION_IMPAIRMENTS"; "CHRONIC_CONDITIONS"]
- 15. In the context of MyCorridor project, we define the traveller MaaS session. A traveller MaaS session is the time period during which the traveller interacts with the platform in order to purchase MaaS offerings. A traveller MaaS session starts as soon as the traveller submit a trip request to the platform (i.e. select origin, destination, departure data of the trip, etc.), and ends when the traveller receives the mobility tokens that correspond to the purchased services. For each traveller MaaS session, the following data is recorded:
 - a. Session interaction time
 - b. Time for completion of a user request
 - c. Visit times and frequency
 - d. No. of registrations
 - e. Issues and errors reported

Correspondingly, the following is logged **during service providers' interaction with the one-stop-shop** (in registration phase):

- 16. In the context of MyCorridor project, we define the service MaaS session. A service MaaS session is the time period during which the service provider interacts with the platform in order to either register a new service or to modify the attributes of an already registered service. A service MaaS session begins as soon as the service provider hits the "Add new service" button or selects a service and hits the "Edit service" button in the SRT, and ends when the service provider hits the "Submit" button in the service registration/editing form in the SRT. For each service provider session, the following data is recorded:
 - a. Session duration
 - b. Visit times and frequency
 - c. No. of registrations
 - d. Issues and errors reported
 - e. Service registration/integration success
 - f. Number of tries

Traveller data will be anonymised, meaning that the identity data (i.e. email and username) will be encrypted before stored in the data repositories. Also, no device identifier data (i.e. IMEI³) is stored in the data repositories. Moreover the service provider data in the respective MaaS sessions will be anonymised. Still, in their aggregated form, after being processed, will feed the impact assessment of A6.4.

1c. Traveller feedback data: Through the Traveller Feedback Module of A3.4 and as reported in D3.2, an upper level (subjective) evaluation of the one-stop-shop as a whole and its products on individual basis will be enabled. This feedback will help the development team to assess how travellers generally perceive the mobile application and if it was well-received. Besides this, the traveller can provide feedback about his/her user experience through closed-ended questions after having a MaaS product/service experience.

As such, the data that will be collected are as follows:

³ Franchi, L., Tarle M. (2017). Dissemination strategy and actions (1), Deliverable 8.2, MyCorridor (Mobility as a Service in a multimodal European cross-border Corridor) project (G.A.: 723384), <http://mycorridor.eu/>

Describe the nature of the processing:

1. **Subjective feedback** of the travellers on the one-stop-shop and on the mobility products they have selected/used. In specific, feedback is required and may be optionally provided by the traveller on the following:
 - a. The integrated application (MyCorridor one-stop-shop platform);
 - i. Level of satisfaction (ranking on a 5-point scale)
 - ii. Ease of use (ranking on a 5-point scale)
 - iii. Net Promoter Score – “recommendation of the App to a friend”
 - b. The MaaS package and the corresponding mobility products/services used;
 - i. Ranking on a 5-point scale rating.
 - ii. Free comments
 - iii. Image (only for the service)
 - c. The overall pre-customised MaaS packaged offered by the MaaS aggregator (called “MaaS offers”);
 - d. Open suggestions for improvements and new features.

Regarding the closed-ended questions, answers to the following will be recorded, whenever provided (optionally) by the travellers.

2. **Operational data logged during usage** and associated with the traveller feedback module. In specific:
 - a. Frequency of a MaaS product/service use;
 - b. Combinations of mobility services by travellers (and frequency/ popularity of combinations).

1d. Data related to payment transactions:

No payment transaction data are processed by the system. All the payments are being done using VivaWallet's payment facilities (which have a banking institute license), without the need for local storage or processing of any type of payment data.

1e. Data related to back-office negotiation:

- Data regarding the mobility product selection by the traveller (e.g. start and end point of the trip, date, time, etc.)
- Data regarding the selected mobility products, by the service provider (e.g. timetables with routes, availability of service for specific date, etc.)
- Data regarding the cost of the selected mobility product, by the service provider.

2. Data that will be logged in the mobile devices during Pilots

The data that will be logged locally in the mobile devices, running the mobile apps, will be as follows:

1. Traveller e-mail and password
2. Traveller mobile device token
3. History of usage of the mobile app

The first two data items are transferred to the back-end of the system, whereas all of them are saved as system variables with no other mobile app having access to them and are being deleted with the mobile app uninstallation from the device.

Describe the nature of the processing:

3. Metadata from the services that will be created by the system to support the system functionalities

This metadata is provided by the service providers that integrate their services in the MyCorridor one-stop-shop platform. They refer to those data that will be provided so as to describe the services, as follows:

- 1. Name of the service*
- 2. Cluster (as defined in the deliverable D1.1) of the service*
- 3. Subcluster (as defined in the deliverable D1.1) of the service*
- 4. Mobility product (as defined in the deliverable D1.1) of the service*
- 5. A set of operation locations of the service*
- 6. A set of operation time periods of the service*
- 7. The URL of the official website of the service*
- 8. A flag denoting the existence of an operation API of the service*
- 9. The base URL of the API of the service*
- 10. The response type (i.e. JSON, XML or both) of the API of the service*
- 11. A flag denoting the existence of an operation booking API of the service*
- 12. The base URL of the booking API of the service*
- 13. The response type (i.e. JSON, XML or both) of the booking API of the service*
- 14. A set of business rules that apply to the service (e.g. tariffs)*
- 15. The transportation model of the service (applies only to mobility services)*
- 16. A flag denoting is the service is provided free of charge or not (i.e. paid service)*
- 17. The cost of the service (if it is a paid service)*
- 18. The currency accepted for the payment of the service (if it is a paid service)*
- 19. General comments for the service*
- 20. Issues regarding the description or the operation of the service detected by the MaaS aggregator*
- 21. The registration status of the service*
- 22. The weight of the service, i.e. a number (from 0 to 1) denoting the importance of the service within the MyCorridor MaaS ecosystem*
- 23. The average rating of the service based on travellers' feedback*
- 24. A document (in PDF format) describing in detail both the operation API and the booking API of the service*

Moreover, MyCorridor will deliver Value-Added Services (VAS), i.e., services giving added value to the user and enhancing user experience. They may be closely associated to mobility or not. In this direction, the platform integrates data from open sources (e.g. weather forecasts, points of interest – POIs, and concerts and festivals in the area of destination) and provides the respective information to the user depending on his/her preferences denoted in his/her profile (see personalization data). The specific data that are used and processed (but not stored) regarding the above are as follows:

- a) Category of interests/activities (e.g., museums, concerts, etc.),*
- b) the time and*
- c) the place (in terms of coordinates).*

Note that a user can explicitly declare if s/he wants to receive VAS, and if s/he wants, what types of VAS information to receive (e.g. weather forecasts and/or information for upcoming festivals). This choices can be made by the user through this profile.

4. Data that will be collected during focus groups, workshops, surveys and during Pilots

Describe the nature of the processing:

Data collected during **focus groups** and **workshops** (WP1/WP6) -with travellers and service providers, respectively- were anonymous. Audio recordings and notes were collected. As soon as audio recordings were transcribed, they were deleted. Data were reported only aggregated under topics and themes (so far reported in D6.1). No verbatim information was shared or used. Further, data collection focus group data collection will be conducted after the end of the second Pilot with stakeholders and travellers alike. The same data types will be collected under the following topics:

Travellers	Stakeholders & service providers
<ul style="list-style-type: none"> Personalised travelling preferences Packages Behavioural change Learning curve (drawing) Best and worse experiences 	<ul style="list-style-type: none"> Benefits to the city (pilot site region) Market penetration Sustainability and Growth Next steps in business wrapping Other urban areas

Surveys were carried out and served WP1 needs and were completely anonymous. Data collected were mainly close-ended questions with no personal information. The survey items can be found in D1.1, Annex 2: Online MaaS survey. Respondents consented before participation.

A survey will be conducted during the second evaluation phase to address the baseline impact assessment requirements (A6.4). Data collection will be pseudonymized and will include demographics, mobility patterns) both open and close-ended question items). Consent will be obtained prior participation. All consent documents link out to the MyCorridor Data Privacy Policy which can be accessed through the MyCorridor mobile application.

These types of data are collected during all types of qualitative surveys, focus groups (WP1 & WP6), workshops (WP7) and, of course, pilots (WP6) that will take place in the project. These data are **collected, managed and processed by MyCorridor partners**. Those may be collected from travellers (all types of them), service providers/developers as well as other types of stakeholders. In all cases, they will be anonymised/pseudonymised, whereas all types of participants sign an informed consent prior to participate in any survey/trial, after having read the data privacy policy of the project.

The data that will be collected will be aggregated, processed and used in order to accommodate the research goals of the project, which is the evaluation of the project solutions, the MaaS paradigm and their impact assessment across several layers.

There are two key sub-clusters of data, namely **subjective** and **usage/performance** data.

The **subjective data that have been /will be collected from the travellers** are as follows:

1st evaluation phase (detailed account can be found in Annex III 'Testing procedures and Protocols' of D6.1).

Baseline interview/questionnaire (11 open and 13 close-ended items):

1. Background information (including age and gender);
2. Computer/mobile literacy

Describe the nature of the processing:

3. *Mobility needs & wants (i.e. Current travel preferences, habits and needs);*
4. *Online consumer attitude, behaviour & experience;*
5. *MaaS awareness;*
6. *MyCorridor platform pre-acceptance.*

Post-questionnaires

7. *Scenario-specific easiness and usefulness (5 Likert scale; usability);*
8. *Mobile app evaluation (c; open ended items; usability);*
9. *Standardized questionnaire called the SUPR-Q. It stands for the Standardized Universal Percentile Rank-Questionnaire, with four essential elements (Usability, Credibility (Trust, Value & Comfort), Loyalty, Appearance) (5 Likert scale)*
10. *Standardised Acceptance scale (TAM3) (Likert-7 scale) – Post acceptance*

2nd evaluation phase

During the second evaluation phase, the subjective data will be collected through a GDPR compliant online tool and they will be mostly in the form of close-ended questions.

11. *Basic demographic (3 Qs)*
12. *Travelling mobile app literacy (2 Qs)*
13. *Preferred incentives and mobility patterns (3 Qs)*
14. *MaaS knowledge and expectations (3 Qs)*
15. *MyOSS pre-acceptance (3 Qs)*

In addition to the above, the following data types will also be collected during the second evaluation phase through means of dedicated face-to-face questionnaires and an online survey to users, both aimed at establishing the baseline information that is required to perform the impact assessment:

16. *Subjective data including age range, mental physical impairments, education levels, occupation, income levels, number of driving licenses in the household, number of vehicles owned in the household, etc.*
17. *Data on current users' mobility patterns including journey purpose, frequency, time of journey departure/arrival, modal choices, public transport accessibility, parking availability, average journey distance, average journey time to travel to most visited destinations; ad-hoc questions will also be addressed to rate users' perception to transport accessibility, comfort, wellbeing, trustworthiness in transport, transport security and personal safety when travelling*

Random/pop up close-ended question items:

18. *Customer Satisfaction rating (5-point Likert scale)*
19. *Easiness (5-point Likert scale)*
20. *Net Promoter Score- future success of mobile app (NPS)*
21. *Happiness/Comfort/Trust (Empathy)*
22. *Change in travel experience (change in adoption; 5-point Likert scale)*

Describe the nature of the processing:

Post-participation questionnaire

- 23. SUPRQm (Sauro, 2017) (16-items UX and benchmarking; 5-Likert scale);
- 24. MaaS acceptance, value, prospect (5-point Likert and open-ended question items),
- 25. Favourite MyOSS pack and incentive. (open ended question items)

A specific set of questions will be asked to users to ascertain the change, as resulting from the introduction of MyCorridor, in perceived accessibility to transport services, transport comfort & wellbeing, trustworthiness in transport, transport security and personal safety when travelling.

Completion of digital diaries (qualitative) by a small percentage of users at each plot site on the following:

- 26. Nature, description, quality of journeys
- 27. Decision making process on using the app
- 28. Location of decision
- 29. Evaluation of travelling experience
- 30. Direct comparison with other travelling apps currently or generally used
- 31. General improvement
- 32. Satisfaction/perceived
- 33. Comments

The **subjective data that have been /will be collected from the service providers** are as follows:

1st and 2nd evaluation phase with service providers. Completion of online form and a spreadsheet completed by the responsible researcher.

Service providers' interview (before use of Service Registration Tool)

- 34. . Background information (3 open-ended question items)
- 35. Previous Experience/Current Behaviour (3 open-ended question items)
- 36. Constraints/Cost/Value (2 open-ended items)
- 37. . Risk/Impact (3 open ended items)

As far as the impact assessment is concerned, before the 2nd evaluation phase starts data will be requested to service providers, through means of a dedicated questionnaire, as regards the composition of their own vehicle fleet, type of vehicles and fuel types used across all transport modes in order to ultimately perform CO2 emissions reduction calculations. Additional questions will also be asked regarding the operating model, revenue levels, organizational structure and data sharing policies of different service providers involved in the trials.

Service provider registration tool and integration process evaluation (post-questionnaire)

- 38. Background information (mostly close-ended question items, includes only age and gender from potentially sensitive data)
- 39. Service Registration Tool use and performance (mixture of open-ended =, 5-Likert and nominal question items)
- 40. Use of supporting documentation (mixture of open-ended =, 5-Likert and nominal question items)

Describe the nature of the processing:

41. Learnability (close-ended; 4-Likert scale)
42. Sustainability and maintainability
43. Changeability (close-ended; yes/no)
44. Effort (open and close-ended items)
45. System Usability Scale (close-ended; Likert scale)

For the purpose of the Impact Assessment (A6.4), the following set of information will need to be gathered from service providers:

- a. No. of service providers that collaborate/work together as a result of MyCorridor
 - b. Revenue increase levels achieved by service providers as a result of MyCorridor platform.
 - c. Questions to evaluate implemented mechanisms to cooperate regarding the type, frequency and volume of data shared as part of MyCorridor, as well as what organisational changes operators may have put in place and how this has impacted their business operations
 - d. Legal & policy modifications questions
46. Performance rating
 47. Complexity rating
 48. Accuracy rating

The subjective data that have been /will be collected from other stakeholders are as follows:

Collected through focus groups and the data types, collection method and clusters/themes are presented in the table in page 20.

The usage/performance data that have been/will be collected from the travellers are as follows:

During the first evaluation phase, the following performance data were collected through mobile phone screen casting and recordings:

49. Clicks
50. Errors/slips
51. Task/scenario completion rate
52. Completion rate and success/partial success/failure

During the 2nd evaluation phase, apart from the logged data reported in Section B-1b, the following will be recorded:

53. Preferred redeemed coupons (if implemented)
54. Most popular incentive (if implemented)
55. Ratio of registered/vs. unregistered users (if implemented)
56. Preferred entry point(s) (potentially via external analytics platform)

The usage/performance data that have been /will be collected from the service providers are as follows:

Through the completion of the facilitator diary the following data are collected in both 1st and 2nd evaluation phase:

Describe the nature of the processing:

57. Completion rates

58. Errors/mistakes (including severity)

For each of the following data items, the **way** of using/storing/processing/deleting, the data format and the **specific location** are being denoted.

Data cluster	Data item	Way of collecting / storing/ processing/ using/ deleting	Data origin	Data size	Data format	Location
1a. Personalisation data	They include travellers' profile information, travellers' trip requests, selected services and history of trips, and travellers' positions during trips	The data will be collected by the mobile app and will be stored in the Travellers Data Repository.	CERTH	It cannot be accurately estimated beforehand, as it depends on the use of the mobile app by the traveller (e.g. frequency of trip requests, frequency of performed trips, etc.)	JSON	The data will be collected by the mobile app and will be stored in the Travellers Data Repository.
1bi. Data logged during usage	MaaS use statistics	Collection through travellers' interaction with the MyCorridor mobile app	CERTH	Cannot be accurately estimated beforehand. It depends on the number of travellers that will use the app, the time period during which	JSON	Data are collected by the mobile application and are stored in the Travellers Data Repository

Describe the nature of the processing:

				they will using it, the number of sessions they will perform, etc.		
1bii. Data logged during usage	MaaS use patterns	They will be generated based on processing that will take place in the Big Data	CERTH	Cannot be accurately estimated beforehand. It depends of the size of the MaaS use statistics that will be recorded.	JSON	Data are processed by the Big Data Management Module and stored in both the Services Data Repository and the Travellers Data Repository
1biii. Data logged during usage	Performance data collected through facilitator diaries for travelers (1 st phase) and service providers (1 st /2 nd phase)	Collection through spreadsheet	CERTH	No more than 100kb	.xlsx	Offline storage at each pilot site pc and share with SRFG (no identification is possible)
1c. Traveller feedback data	Travellers' feedback regarding the overall MyCorridor app, and each of the provided services as well	They will be collected by the Traveller Feedback Module	CERTH	Cannot be accurately estimated beforehand. It depends on the number of travellers that will use the app, the frequency of the submitted feedback reports, etc.	JSON	The data will be received and processed by the Traveller Feedback Module, and they will be stored in the Services Data Repository
1d. Data related to	No data collected	Not-applicable	Not-applicable	Not-applicable	Not-applicable	Not-applicable

Describe the nature of the processing:

<i>payment transactions</i>						
1e. Data related to back-office negotiation	Data regarding the mobility product selection by the traveller (e.g. start and end point of the trip, date, time, etc.) Data regarding the selected mobility products, by the service provider (e.g. timetables with routes, availability of service for specific date, etc.) Data regarding the cost of the selected mobility product, by the service provider.	They will be collected by the Payment Module	Travelers and service providers	Cannot be accurately estimated beforehand. It depends on the number of travellers that will use the app, the time period during which they will use it, the number of sessions they will perform, etc.	JSON	Service providers' database and MyCorridor database
2.Data that will be logged (in the cloud server and the mobile devices) during Pilots	They include the e-mails and passwords of the travellers, the mobile device tokens and the history of usage of the mobile app (e.g. number of performed trip requests, selected services, etc.).	They will be collected by the mobile app and stored in the backend data repositories (i.e. the Travellers Data Repository and the Services Data Repository)	CERTH	Cannot be accurately estimated beforehand. It depends on the number of travellers that will participate in the pilots.	JSON	Data are collected by the mobile app and stored in the backend data repositories (i.e. the Travellers Data Repository and the Services Data Repository)
3.Metadata from the services that will be created by the system to support the	They include basic information of the services that are required for initializing the service registration process	They will be collected by the Service Registration	CERTH	The average size of such data object is estimated to 1.7KB.	JSON	The data will be collected by the Service Registration Tool (SRT) and they will

Describe the nature of the processing:

system functionalities		n Tool (SRT)				be stored in the Services Data Repository
4a. Data that will be collected during Pilots	Surveys (WP1 and WP6 real-life assessment)	Online through GDPR compliant platforms	CERTH/TTS	TBE	.csv/.sav	CERTH platform account/offline secure storage (pc)
	1 st evaluation phase – Travellers/service providers (incl. 2 nd)	Offline spreadsheets	Pilot sites	TBE	.xls	Offline secure storage (pc)
	2 nd evaluation phase Online questionnaire/survey	Online through GDPR compliant platforms	CERTH/TTS/S RFG	TBE	.csv (at least)	Online secure account space and offline secure storage (pc)
	2 nd evaluation phase questionnaires/surveys to travelers and service providers (for collecting baseline information before 2 nd phase pilots start)	Offline spreadsheets	Pilot sites/TTS	-	.xls	Offline secure storage
	2 nd evaluation phase questionnaires/surveys to travelers and service providers (during trials and/or after 2 nd phase pilots end)	Offline spreadsheets	Pilot sites/TTS	-	.xls	Offline secure storage
4b. Data that will be collected during workshops and focus groups	Audio recordings Notes	Offline recorder (only transcripts will be stored; audio recording will be deleted as soon as	Pilot sites, UoN (WP1 focus group)	TBE	.doc	Offline secure storage (pc)

Describe the nature of the processing:

		they are transcribed)				
--	--	-----------------------	--	--	--	--

3. What is the source of the data?

*The primary data sources are the actual users/travelers/participants. Another primary source of data is coming from the service providers that have registered and provide their service through the MyC one-stop-shop. The source includes all different types of services, i.e. mobility, infomobility, traffic management, and added value services. It should be clarified that the data received from calls on the actual APIs of the service providers are processed in the MyCorridor back-end and presented to the travelers, **but they are not stored in the MyCorridor data repositories.***

4. Will you be sharing data with anyone?

Sharing of data will be as follows per type of data.

1. Data collected and processed in order to accommodate the operational functions of MyCorridor one-stop-shop

1a. Personalisation data – These data are used for providing personalized MaaS offerings to the travelers, and they are not shared with any entity.

1b. Data logged during usage – In the context of A3.2 “Big Data Management Module”, a set of statistics regarding the MaaS usage will be recorded (as described above). These data will be processed by designed and implemented data analytics techniques in order to identify MaaS usage patterns. These patterns/insights can be shared with the service providers, whose services are registered in the MyCorridor platform. The traveler that uses the MyCorridor platform will know, by the time he registers in the platform, that the defined MaaS usage data will be recorded and processed by the platform, and the processing results will be provided to the service providers only upon his acceptance. If the traveler does not give his permission, no MaaS usage data regarding his activity within MyCorridor platform will be recorded, and therefore no processing will take place.

1c. Traveller feedback data – Subjective views of travellers on the one-stop-shop and its mobility products will be shared with other travellers in anonymised manner. In addition, the traveller will be given the opportunity to share through social media (Facebook, Twitter and Google+) their subjective views. Finally, the module provides functionality to the service providers that want to receive the feedbacks about their services. It is important to stress that traveller feedback collection on service level is asked and collected only upon consent of the service provider. The MyCorridor MaaS aggregator (in this case and for the context of the research project, CERTH/ITI) can use the same functionality to retrieve the list of services and post processing the data. The information provided to the traveller for each service includes the **average rating**, the **number of usages**, the **services combined with a specific service** and the **comments and the images provided by other travellers**. The same information can also be retrieved by the service providers for their services.

1d. Data related to payment transactions – Non-applicable.

1e. Data related to back-office negotiation – Will not be shared at all and with anyone.

2. Data that will be logged in the mobile devices will not be shared other than with the back-end for operational reasons.

3. Metadata from the services that will be created by the system to support the system functionalities – Will not be shared at all and with anyone.

4. Data that will be collected during focus groups, surveys and during Pilots –will be decided to which level will be shared in ZENODO at the end of the project in the context of the Open Research Pilot.

Describe the nature of the processing:

5. Flow diagrams or other way of describing data flows such as the one depicted below (Figure 43).

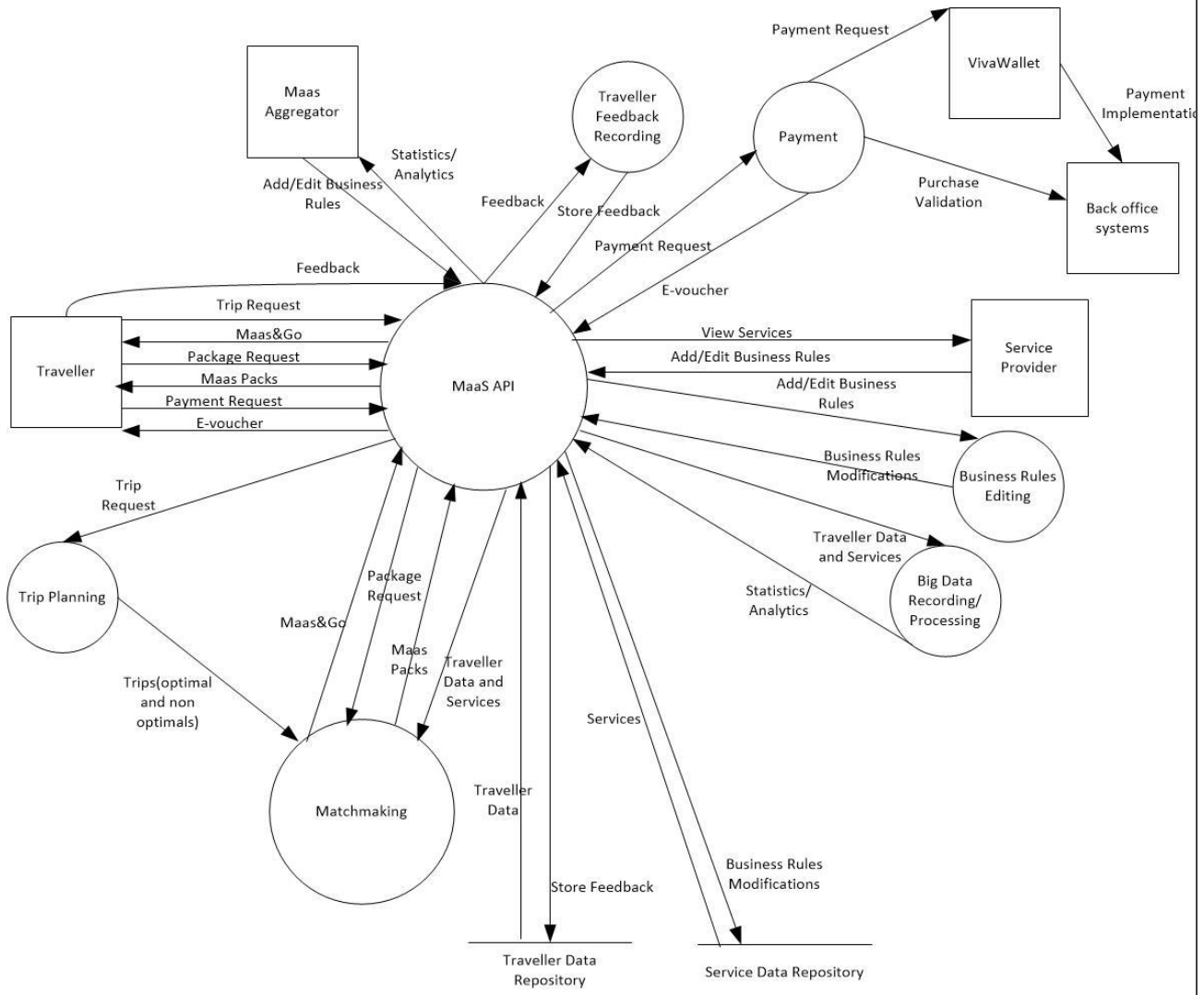


Figure 43. MyCorridor data flow diagram

The service delivery platform comprises the following parts (those highlighted in yellow require user data collection and processing). Implementation of modules:

1. Service Registration Tool
2. Matchmaking Module
3. Big Data Management Module
4. Business Rules Implementer Module
5. Traveler Feedback Integration Module
6. Payment Module

Secure RESTful API ensure data security and privacy:

1. MyCorridor MaaS API

Describe the nature of the processing:

2. Data repositories

5. What types of processing identified as likely high risk are involved?

No high-risk data processing is involved. The only high risk are the face and audio data collected by pilot site partners during the first Pilot round. However, this type of data collection, apart from the fact that it is optional and collected upon informed consent of the travelers addressing this part in specific, is only stored at pilot sites (administered by only one person locally defined) and never shared outside the organization. If collected, will be used to complete the facilitator diaries and will be destroyed immediately afterwards.

Describe the scope of the processing:

1. What is the nature of the data, and does it include special category or criminal offence data?

Please see analytic clustering of data in previous section.

2. How much data will you be collecting and using?

*Only necessary data is collected. During the lifetime of the project, data from around 700 users are collected (UC surveys and focus groups, focus groups, 2 phases of Pilot user testing, stakeholders focus groups). **How often?** UC related data collection (survey and focus groups) were held the first nine months of the project's lifetime, the user and service providers' focus groups as well as the 1st pilot phase were held in the second year of the project and beginning of third year of the project. The 2nd pilot phase and the focus groups with stakeholders will be held the third and last year of the project. The specific number of journeys that will be achieved in each pilot site of MyCorridor during the 2nd real-life pilots will be reported in detail in D6.2: Pilot results consolidation and D6.3: MyCorridor impact assessment.*

3. How long will you keep it?

The name, contact details (telephone, e-mail) will be kept in the database only for the duration of the project. This is required in MyCorridor in order to strengthen the iterative nature of the project that there will be an attempt to involve the same users that will be recruited by the project to the greatest possible extent, starting from the field trials of WP1 the first year of the project until the last evaluation round towards the end of the project; therefore, it is necessary that contact details are kept as long as the project is running. Contact details are kept by only one allocated person within the evaluation team that safeguards their details and stores them separately from their results.

Data collected (anonymized/pseudonymized format) will be kept for 5 years.

4. How many individuals are affected?

See answer in Q2.

5. What geographical area does it cover?

Participants from the pilot site countries are involved: Austria, Czech Republic, Germany, Greece, Italy, the Netherlands and geographical corridors in between them.

Describe the context of the processing:

1. What is the nature of your relationship with the individuals?

Participants are volunteers and are recruited solely for evaluating the MyOSS mobile application and the Service Registration Tool; both developments of the project. The same is valid for all the user surveys, focus groups and workshops of the project.

2. How much control will they have?

As GDPR has already been implemented, participants can request access to their data even after their participation has been completed. They can also ask to delete them even after participation as well. User profile data can be changed whenever they want, by altering the existing settings or not given at all or given to the degree they wish (which is perfectly allowed via the personalisation mechanism of the project). The existing [MyCorridor data privacy policy](#) clearly states what type of control participants/users can exert over their data.

3. Would they expect you to use their data in this way?

User are informed about how data are collected, stored, processed, analysed and disseminated. These pieces of information are provided in both the consent form (template annexed in the end of this document) and online (<http://www.mycorridor.eu/privacy-policy/>). Data will not be used in any other way that the one given to users through these two aforementioned channels.

4. Do they include children or other vulnerable groups?

Children will not be recruited but older individuals and users with disabilities will be included.

5. Are there prior concerns over this type of processing or security flaws?

There are no concerns or security flaws that need further consideration.

6. Is it novel in any way?

Data collection is not novel. It is systematic and clear.

7. What is the current state of technology in this area?

MaaS is a new paradigm-shifting concept and technologies (web services, portals, mobile applications) have been developed and existing in the mobility market, the last five years. In other words, commercial technological endeavours have already penetrated the relevant mobility market.

8. Are there any current issues of public concern that you should factor in?

No public concern related issues exist or are anticipated.

Describe the context of the processing:

9. Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Data processors are experienced data scientists and engineers. Partners taking up these roles are all trained and hold postgraduate degrees.

Describe the purposes of the processing:

1. What do you want to achieve?

Goals are different per data cluster and purpose, as they are defined in Step 2 section of this PIA.

- *Offer MaaS in a seamless, interoperable, inclusive and cross-border fashion.*
- *Evaluate the usability, user experience and acceptance of MaaS concept, of MyOSS mobile application and Service Registration Tool.*
- *Estimate the impact (e.g. socioeconomic, ecological, in mobility, etc.) in future EU mobility and relevant market(s).*
- *Offer personalized mobility services and MaaS packs and, as such, achieve accurate user profiling.*
- *Create user-oriented business models and MaaS packages.*
- *Offer personalized incentives and loyalty schemes.*
- *Ensure payment is made and it is interoperable, secure and safe.*
- *Automatically collect feedback about the user experiences with the mobile app and services (i.e. traveller's feedback module).*
- *Collect usage analytics.*
- *Acquire all necessary information about the service(s) to be integrated to MyCorridor platform (i.e. Service Registration Tool).*

2. What is the intended effect on individuals?

No effect is intended on individuals. Still, some side effects would be the familiarisation with novel mobility solutions and MaaS, the latest trends/patterns in mobility, the critical revision of their current mobility habits and the potential for changing them aiming at a better Quality of Life.

3. What are the benefits of the processing – for you, and more broadly?

Data processing will ensure that goals mention in Point 1 are reached and decisions based on results are taken.

9.5 Step 3: Consultation process

Consider how to consult with relevant stakeholders:

1. Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.

Data from users have been/ will be collected during:

- Focus groups (audio transcripts – anonymized/pseudonymised during collection)
- On-line/Physical Surveys (questionnaire completion - anonymous during data collection)
- Pilots through mobile/web analytics and subjective forms (on-line or physically distributed). Audio and video data recordings (no face/only screen and hands' interaction) is also applicable only for the 1st round of Pilots.

2. Who else do you need to involve within your organisation?

Apart from Consortium Partners, where specific role allocation has been assigned, MyCorridor will involve external to the Consortium service providers to broaden the MaaS paradigm it wants to prove.

3. Do you need to ask your processors to assist?

Yes. In MyCorridor, test sites which act as data processors are at the same time service providers with the task to recruit more – external to the project – service providers.

4. Do you plan to consult information security experts, or any other experts?

OC is a legal entity and it is a Partner of MyCorridor project. They supported the development of the consent forms, the data privacy policy and release forms (for photographs and videos) to ensure they are GDPR compliant. They also oversee the conduct of DPIA and DMP in MyCorridor. In addition, CERTH/ITI and UPAT are IT experts responsible for the security protocols in the one-stop-shop.

9.6 Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular:

1. What is your lawful basis for processing?

- Data processing of data will be performed only to create the user profile and match users' preferences with transport modes, services and MaaS packs. Travellers are informed of the data privacy and are prompt to read it before signing-up the consent form.
- Data sharing with service providers is performed under an MoU agreement. Service providers are also prompt to read the data privacy and give consent before registering their service.
- A GDPR compliant informed consent for travellers is provided in Annex 2 of the current document. Please see also the principles defined in the Ethics Manual of the project.

2. Does the processing actually achieve your purpose?

The project follows the principle of data limitation. We collect and analyse only necessary data. Data processing ensures personalized mobile user experience and allows the app to offer to travellers the correct information and support.

3. Is there another way to achieve the same outcome?

Describe compliance and proportionality measures, in particular:

There is no other way to reach the same outcome.

4. How will you prevent function creep?

The technologies developed within the project are solely used for mobility and transportation. There will be no widening or change of use till the end of the project. Added value services related to health, leisure, etc. are also integrated only to support mobility.

5. How will you ensure data quality and data minimisation?

Service delivery platform: Real-time and continuous inspections are in place as well as technologies. Only necessary data are collected. Pilot tests: Data quality is ensured by thorough completeness and correctness of user data collected immediately after the end of each user testing session. Data quality is also ensured as it emerges from the evaluation and impact assessment framework defined in the project (D6.1). Finally, the project adopts the data minimization policy and will process only the necessary private data in order the mobile application can offer personalized travel experience and secure access to the user's profile as well as to carry out the consolidated analysis (D6.2) and impact assessment (D6.3).

6. What information will you give individuals?

***User testing:** Users are informed about data treatment, storage, types, deletion, etc. by relevant articles in the project's [data privacy policy](#). In addition, they are informed about their rights and the whole process in the informed sheet of the consent form and in case of audio or video recordings, they are informed through the release form. In addition, before any testing takes place, users are informed about the project, its objectives and the pilots (minimum information about the pilot's objectives is provided, to avoid users becoming biased).*

***Service delivery platform:** data collected and processed from separate parts of the platform are included in the data privacy policy and are available for service providers, users and visitors to know about them.*

7. How will you help to support their rights? What measures do you take to ensure processors comply?

The roles of collectors and processors are clearly discussed in section 2 of the current document. And derived obligations are discussed in section 8 of the current document.

8. How do you safeguard any international transfers?

No international transfers are taking place. Payment transactions are being held in the European context.

9.7 Step 5: Identify and assess risks

#	Privacy issue	Risk to individuals	Compliance risk	Associated organization / corporate risk	Likelihood of harm [remote, possible or probable]	Severity of harm [minimal, significant or severe]	Overall risk [low, medium or high]
1.	<i>Risk that the security of the data is compromised (i.e. data breach).</i>	<i>Risk that sensitive personal data is lost or stolen or destroyed causing distress or damage to the data.</i>	<i>Risk of breach of data protection legislation.</i>	<i>Risk of reputational damage to entity/entities involved and of enforcement action being brought. Risk to delivery of research objectives both current and in the future. Risk of complaints or litigation from affected individuals.</i>	<i>Remote</i>	<i>Significant</i>	<i>Low</i>
2.	<i>Risk that due to a data breach, the true identity of a user will be identified</i>	<i>Risk that the real identity of a user will be identified. This means that, for example, the stored locations will be matched with a user and thus the locations of the places he most frequently visits (i.e. home, work, etc.) will be identified.</i>	<i>Risk of breach of data privacy legislation.</i>	<i>As above.</i>	<i>Remote</i>	<i>Significant</i>	<i>Low</i>
3.	<i>Risk that personal data is retained for longer than is necessary.</i>	<i>Risk that individual's data is held for longer than is required and</i>	<i>Risk of breach of data protection legislation.</i>	<i>As above.</i>	<i>Remote</i>	<i>Minimal</i>	<i>Low</i>

#	Privacy issue	Risk to individuals	Compliance risk	Associated organization / corporate risk	Likelihood of harm [remote, possible or probable]	Severity of harm [minimal, significant or severe]	Overall risk [low, medium or high]
		<i>that security and other organisational methods applied to the personal data lapse.</i>					

9.8 Step 6: Identify measures to reduce risk

For each of the above risks identified, the following measures were defined:

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk [eliminated; reduced; accepted]	Residual risk [low; medium; high]	Measure approved [Yes/No]
1	<i>The access to a specific set of information is restricted only to the owner of this information (e.g. the travel preference of a traveller can be modified only by the traveller himself, due to the use of MongoDB, NoSQL data collections.</i>	<i>Reduced</i>	<i>Low</i>	<i>Yes</i>
2	<i>The whole MyCorridor back-end will be behind HTTPS (secure HTTP connections), thus reducing the platform's robustness against malicious attacks.</i>	<i>Reduced</i>	<i>Low</i>	<i>Yes</i>
3	<i>All identity data (i.e. emails and passwords) are encrypted (using highly reliable hashing algorithms, e.g. bcrypt) before stored in the MyCorridor data repositories. Therefore, even in the event of a data breach, an attacker will not be able to de-hash the encrypted information (at a reasonable time) and identify the user's true identity.</i>	<i>Reduced</i>	<i>Low</i>	<i>Yes</i>
4	<i>A process of completely deleting all stored data has been designed and developed, and it will be triggered by the system administrators at the end of the project.</i>	<i>Reduced</i>	<i>Low</i>	<i>Yes</i>

9.9 Step 7: Sign off and record outcomes

According to the obligations defined in section 8, whenever and for whichever controllers and basically processors applicable, the following table will be completed for the above listed measures (of Step 6) that will be annexed in *D6.2: Pilot results consolidation* along with the local approvals related to Ethics and GDPR, whenever applicable.

1. Who has approved the privacy risks involved in the project? What solutions need to be implemented?

<i>Risk</i>	<i>Approved solution</i>	<i>Approved by</i>
<i>E.g. Risk 1</i>	<i>Data will be deleted when it is no longer necessary to retain such data.</i>	<i>E.g. Data Protection Officer. Note, if there is no DPO or National Agency responsible for that, the data manager (WINGS) will be responsible for looking into the privacy risks (with support from MyCorridor legal partner, i.e., Osborne-Clark, and MyCorridor Technical manager, i.e., CERTH) and proposing the mitigation solution.</i>

2. Integrate the PIA outcomes back into the project plan. Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?

Overall: For integrating back into the plan, responsible is WINGS. For implementing the solutions, depends on who has developed the corresponding part. For contact in the future for the project, should again be WINGS, as Data Manager.

<i>Action to be taken</i>	<i>Date for completion of actions</i>	<i>Responsibility for action</i>
<i>Data to be deleted.</i>	<i>Insert date/description of when.</i>	<i>E.g. Data Protection Officer.</i>

Annex 2: MyCorridor GDPR compliant Informed Consent Form

Participant Briefing Sheet

What is this all about?

The MyCorridor project is a research project aiming to introduce new ways for individuals to organise travel. It is funded by the European Commission as part of its Horizon 2020 programme, and consists of 16 universities and companies across Europe (the "**MyCorridor Research Partners**", "**we**", "**us**") and one legal team. Further information about the MyCorridor project is available here <http://mycorridor.eu/>.

You have been asked to participate in a focus group/user survey/trial as part of MyCorridor to talk about your views on a new way of organising travel/evaluate the project solutions and MaaS.

Your views will be used to inform the development of 'Mobility as a Service' and the specific products of MyCorridor project. 'Mobility as a Service' has been described as follows:

'Mobility as a service means you access any travel (car, bus, train, underground metro, taxi, coach, tram, bike, planes etc.) through the use of a single card or app on your phone. It means increasingly less ownership for example of cars or bikes. Cars will be shared. You will pay a subscription to access any of these, and the card or app will be valid wherever you go in the country or across different countries. So no need for different travel cards or multiple tickets in different places. The app will store information about every journey you take, about where you go, at what time, how you travel and the cost.'

The MyCorridor Research Partners need to understand how different people, in different circumstances, feel about Mobility as a Service, and whether it would be something people would want to use in their own lives, perhaps when travelling to work, to study, or on holiday.

Taking part

Taking part in the focus group/user survey/pilot trial is voluntary. You do not have to take part. You can withdraw from participating at any time and without having to give a reason for withdrawing. We will maintain a record of what people say during the focus groups/user surveys/pilots, to benefit the research of the MyCorridor project and to publish these results in a publically available report. All information collected will be anonymised/pseudonymised, so no one will know who said what. The report will be publicly available and you will be able to request a copy using the contact details below.

We will also use the anonymised/pseudonymised information collected for research, publications, conferences, exhibitions, other MyCorridor-related dissemination activities and archiving for research purposes. Save for where you have consented to your photo being used (as further detailed below), all information collected will be anonymised prior to any such use and you will not be identifiable in any research, publications, conferences, exhibitions, other MyCorridor-related dissemination activities or in any archiving for research purposes.

Photos



We would like to take some photos to use in further research, publications, conferences, exhibitions, other MyCorridor related dissemination activities and archiving. For example, we will use social networks to publicise information relating to MyCorridor's research activities and we would like to include focus group photos to accompany related MyCorridor social media posts.

We require your consent to take and use your photos and therefore, we will only take your photo if you consent by ticking the corresponding box in the Participant Consent Form. If you do not consent, you can still take part in the focus group but we will not take your photo.

If you do consent to us using your photo, you may withdraw this consent at any time.

We will only store your photos for as long as required to assist in MyCorridor publications, conferences, exhibitions, other MyCorridor-related dissemination activities and archiving. We will not store any photos taken during focus groups for any longer than three (3) years after the relevant focus group was held.

MyCorridor's Privacy Policy

MyCorridor data privacy policy contains information about the personal information that we collect from you, and how we collect, store, use and share your personal information. It also sets out your rights to control personal information we hold about you. We will notify you if any changes are made to our Privacy Policy.

Who is responsible for this study?

The Lead Researcher is Roberto Palacin, who is based at Newcastle University (one of the MyCorridor Research Partners) in the United Kingdom. You can contact him at roberto.palacin@newcastle.ac.uk

Alternatively, you can talk to the person running your focus group/survey/trial at **<please insert email address to the focus group organization>**.



Participant Consent Form

I agree to participate in this focus group/user survey/pilot trial being carried out as part of MyCorridor project.

☐

I can confirm that (*please tick each box to indicate you agree*):

I have read and understood the information relating to this participation (contained in the Participant Briefing Sheet)

☐

I understand I can ask questions at any point before, during or after the participation using the contact details provided

☐

I understand that the data collected for this study will be stored securely

☐

I understand that all information collected during my participation will be recorded and stored anonymously

☐

I understand that all information collected during my participation will be used for research purposes only

☐

I understand that my name will not be used on any documents or in any presentations about the research

☐

I understand that I can leave the study at any time without needing to say why

☐

I agree to my photo being taken during my participation and for it to be used by MyCorridor in MyCorridor-related publications, conferences, exhibitions, other MyCorridor-related dissemination activities and archiving

☐

I consent to receiving emails from the MyCorridor Research Partners relating to MyCorridor events, products and services.

☐

Signature of participant.....

Name (in capitals)

Date.....

If you have any questions about this research please feel free to contact:

Name: <please insert the name of contact person>

Email: <please insert the email address of the contact person >

Telephone: <please insert the telephone number of the contact person>

Annex 3: Data processing - record keeping template

*NOTE: The information requested here is in line with the requirement to maintain data processing records under the GDPR and **is specific to personal data**. All data controllers and processors must also keep records of data set descriptions according to the latest Data Management Plan and DPIA. Where applicable, this information must be verified by the organizational Data Protection Officer.*

I. Data controller's record of processing activities

1	Contact details of Data Controller
Email	
Company address	
Telephone	
2	Purpose of processing
3	Description of categories of data subjects and of the categories of personal data
4	Categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations
5	Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation

5	Where possible, the envisaged time limits for erasure of the different categories of data
6	Where possible, a general description of the technical and organisational security measures for
a	the pseudonymisation and encryption of personal data;
b	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c	the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;

II. Data processor's record of processing activities

1	Contact details of Data Processor	
Email		
Company address		
Telephone		
2	Categories of processing carried out on behalf of the Controller	

3	Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation
4	Where possible, a general description of the technical and organisational security measures for
a	the pseudonymisation and encryption of personal data;
b	the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c	the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
d	a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;