KEYSTONE

Plug & Play implementation and interconnectivity study

Deliverable 2.2

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

KEYSTONE

Plug & Play implementation and interconnectivity study

Deliverable 2.2

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or CINEA. Neither the European Union nor the granting authority can be held responsible for them.

Deliverable details

Horizon Europe GA no.	Project acronym	Project title
101103740	KEYSTONE	Knowledgeable comprehensive and fully integrated smart solution for resilient, sustainable and optimized transport operations

Deliverable	Title	Work package
D2.2	Plug & Play implementation and interconnectivity study	WP2

Contractual delivery date	Project month	Actual delivery date	Delivery type	Dissemination level
31/07/2024	PM 14	01/08/2024	R	PU

Author(s)	Organisation
Andrea Mutti	T Bridge
Camille Leotta	T Bridge
Davide Maestroni	T Bridge
Cino Repetto	T Bridge
Salvatore Pappalardo	T Bridge

Internal reviewers
AETHON

Acronyms

Acronym	Meaning
EC	European Commission
WP	Work Package
ETA	Estimated Time of Arrival
SMART	Specific, Measurable, Archivable, Realistic, Time-bound
PCS	Port Community System
TMS	Transport Management System
API	Application Programming Interface
eID	electronic Identification
eIDAS	electronic IDentification, Authentication and trust Services
IdP	Identity Provider
ASP	Application Service Provider
CCAM	Connected, Cooperative, and Automated Mobility
C-ITS	Cooperative Intelligent Transport Systems
TOS	Terminal Operating System
UML	Unified Modelling Language
SRIA	strategic research and innovation agenda
T2T	truck-to-truck
T2I	truck-to-infrastructure T2I
ITU	Intermodal Transport Unit

Document history

Version	Date	Author	Affiliation	Summary
V0.1	16/04/2024	Andrea Mutti, Cino Repetto, Davide Maestroni, Camille Leotta, Salvatore Pappalardo	T Bridge	ToC & Executive Summary
V0.2	31/06/2024	Andrea Mutti, Cino Repetto, Davide Maestroni, Camille Leotta, Salvatore Pappalardo	T Bridge	Draft
V0.3	31/06/2024	Davide Maestroni	T Bridge	Added CCAM Chapter

V0.4	02/07/2024	Andrea Mutti, Cino Repetto, Davide Maestroni, Camille Leotta, Salvatore Pappalardo	T Bridge	Final draft
V0.5	04/07/2024	Zoe Petrakou, Charis Koutsis	AETHON	Review of D2.2
V1.0	01/08/2024	Andrea Mutti, Cino Repetto, Davide Maestroni, Camille Leotta, Salvatore Pappalardo	T Bridge	Final review & conversion to PDF format

Table of Contents

1. Executive Summary 10
2. Introduction 11
2.1. Background and preconditions 11
2.2. Objectives of the Deliverable 2.2 11
2.2.1. Introduction 11
2.2.2. Interconnection between different platforms 12
2.2.3. Cross-data space authentication mechanism for the API 12
2.2.4. High automation level vehicles (CCAM) 12
2.3. Overview of the connections with the other WPs 13
3. API reference model overview 14
3.1. Overview of T2.1 – Objectives and Definition of the API Reference Model 14
3.2. Objective of API Reference Model and connection with T2.2 15
4. Connection to other platforms 16
4.1. Overview 16
4.2. Platforms stemming from the use cases study 16
4.2.1. Police controls over transport 17
4.2.2. Data integration between TMS and PCS 22
4.3. Legal implications in the retrieval and use of the information involved in the use cases 24
5. A custom example of interconnectivity 27
5.1. Introduction 27
5.2. EDIGES 27
5.3. GRUBER BEYOND 30
5.3.1. ORDERS 30
5.3.2. EVENTS 36
5.3.3. A look up on the future 38
6. Cross data space authentication mechanisms for the API 39
6.1. EID / EIDAS founding concepts 39
6.1.1. EID principles 39
6.1.2. A typical example of use case involving the eID 40
6.1.3. Use of the eID to implement the “Plug and play” policies 41
6.1.4. EIDAS principles 42
6.1.5. How the concept of interoperability is implemented in eIDAS 43
6.2. EIDAS authentication guidelines 44

6.2.1. Overview 44
6.2.2. A typical example of use case involving the eIDAS 44
6.2.3. Operative side 46
6.2.4. Where to find what: online documentation 49
7. Consideration about the vehicles of high automation levels 51
7.1. CCAM / C-ITS overview 51
7.2. EU CCAM Projects 52
7.2.1. CCAM Partnership 52
7.2.2. ROADART 53
7.2.3. 5G Blueprint 53
7.2.4. MODI project 54
7.3. CCAM in KEYSTONE 55
8. Conclusions 57
8.1. Summary of findings 57
8.1.1. About API reference model 57
8.1.2. Interfacing different platforms and legals implications 57
8.1.3. eID/eIDAS: principles and guidelines 59
8.1.4. CCAM: state of art and integration in KEYSTONE 59
References 61
Annex 1 62

List of Figures

Figure 1 - Police controls over transport use case diagram 17
Figure 2 - Police controls over transport sequence diagram 19
Figure 3 - Police controls over transport alternative use case diagram 20
Figure 4 - Police controls over transport alternative sequence diagram 21
Figure 5 - Data integration between TMS and PCS use case diagram 22
Figure 6 - Data integration between TMS and PCS sequence diagram 24
Figure 7 - A typical example of use case involving the eID sequence diagram 41
Figure 8 - A typical example of use case involving the eIDAS sequence diagram 46

List of Tables

Table 1 - Data helping enforcers controls 25
Table 2 - Data and datatypes from EDIGES TOS platform 28
Table 3 - Examples of calls and responses to the GRUBER BEYOND TMC platform REST services (endpoint orders/all) 30

Table 4 - Examples of calls and responses to the GRUBER BEYOND TMC platform REST services (endpoint orders/{id_order}) 32
Table 5 - Examples of calls and response to the GRUBER BEYOND TMC platform REST services (endpoint events/trip/{id_trip}) 37
Table 6 - eIDAS nodes status 48
Table 7 - Online documentation 49
Table 8 - Single points of contact 62

1. Executive Summary

The heterogenic purposes of the document can be summarised with the following points:

- **Theoretical Purpose:** To encompass aspects such as user authentication and potential developments in the field of highly automated vehicles.
- **Pragmatic Purpose:** To serve as a bridge between the study of existing platforms (referred to the “as is” state) and the development of use cases derived from requirements.
- **API Design Purpose:** To assist in the design of APIs by defining which data to retrieve and from which platforms it should or can be obtained, and to determine the most profitable technology to use on a case-by-case basis.

These purposes, from a side outline the document’s scope, from theoretical considerations to practical applications and technical design, but, from the other side, represented the main and biggest problem addressed during the compilation of the document itself

Nevertheless, some important solution has been given for the more pragmatic purposes:

- **Interfacing external platforms:** The document details the complexities and challenges of data extraction and management across different platforms, emphasizing the need for seamless communication and data flow among diverse systems. Diagrams and textual explanations help clarify these complex data integration processes.
  The document discusses two platforms, EDIGES and GRUBER BEYOND, which are being considered for two pilot projects in intermodal transport and data communication between TMS and PCS. EDIGES, the TOS platform for the Novara intermodal center, manages train arrivals, truck loading, and ITU pickup data transmission to KEYSTONE via APIs. It details the data structure for ITU pickup from EDIGES. GRUBER BEYOND, GRUBER’s TMS platform, provides REST services as microservices for accessing order-related data and ETA. It describes the Orders and Events management systems, including API call examples and response data for order and trip event retrieval.
- **Use of eID/eIDAS:** The document provides guidelines on how public sector service providers can connect to existing eIDAS nodes and implement eIDAS authentication. It also includes information on key resources and documentation available online for further reference and implementation.
- **Overview of the high automation level vehicles:** The focus was on the state of the art. Nevertheless, important words have been spent both about a plausible level of integration and about benefits that the use of the CCAM could take in Keystone project.

2. Introduction

2.1. Background and preconditions

The fast digitalisation of the world in the last decade has brought significant advancement, impacting also the realm of transportation and logistics.

This upgrading has brought numerous benefits but also it has introduced complex challenges for the different stakeholders.

For example, the need for adapting to this fast-paced change has led to the proliferation of a multitude of platforms designed to manage different logistic processes.

However, these platforms often operate as isolated silos, presenting a lack of integration and interoperability within the whole system, due to a so large number of different technologies and standards.

This results in an inefficient flow of data shared within actors aggravated by the number of actors and complexity of the existing processes themselves, leading to communication problems, unnecessary overlaps and delays in the decision-making processes, with the consequently rise of operational costs and increased avoidable risks.

It is in this context that KEYSTONE aims to boost digitalisation and data exchange between the different actors of the logistics chain by proposing intelligent solutions under a standardised API platform format and a web-app solution proposed for two real-world pilots.

This standardised API configuration leads to the implementation of Plug & Play principles from the already implemented framework defined during Task 2.1 and the respective report Deliverable 2.1 “Plug and Play implementation framework: the API reference model”. These standards allow the connection between the different stakeholders that make up the ecosystem, enabling a fluid and agile exchange of information under strict security parameters, making visible information that is often complex to obtain due to the different channels on the table and the different objectives and interests of the actors.

2.2. Objectives of the Deliverable 2.2

2.2.1. Introduction

Task 2.2 aims on the one hand at an accurate analysis of certain aspects of the process, while on the other hand at dissecting the more theoretical aspects of some aspects that will not necessarily be part of this project but could represent a possible future evolution.

The Deliverable 2.2, using a presentation, schematic for most of the parts, clarifies and puts order among topics that are apparently so heterogeneous.

This document is based on two levels: a more theoretical one that encompasses aspects such as user authentication and potential developments in the field of highly automated vehicles, and a decidedly more pragmatic one that serves as a bridge between the study of existing platforms (referred to the “as is” state) and the development of use cases derived from requirements.

Moreover, this document will be able to help in the design of APIs since it will define which data to retrieve and from which platforms it should or can be obtained, as well as trying, in this context, to understand which technology will be most profitable to use on a case-by-case basis.

2.2.2. Interconnection between different platforms

The interconnection between the involving systems includes seamless integration and interaction across different platforms, facilitating data exchange driven by the intermodal shipping and transportation process.

The focus of KEYSTONE lies precisely in the integration of heterogeneous platforms and the establishment of a standard for harmonizing diverse data formats. Task2.2 represents one of the initial steps in this direction, transitioning from analysis to design.

In fact, Task2.2 takes the first step toward this integration by addressing how to retrieve necessary data, where to obtain it, and which technology to use. This process will naturally draw from use cases directly derived from the Deliverable 1.4, while also leveraging insights gained from the study of platforms conducted in Task1.3 and described in the corresponding deliverable.

A more technical approach will be centred on the technology used to extract data from identified platforms, serving as the crucial link between analysis and design.

Given the critical importance of data security, it is evident that robust security measures are central to integration efforts. Safeguarding sensitive data and ensuring privacy will be paramount.

The retrieval of sensitive data from the involved platforms is closely tied to the legal framework, which sets boundaries for accessing and utilizing information from various sources.

For instance, data privacy laws restrict the types of information that can be retrieved, emphasizing the legal considerations that must inform the process definition and data management, including potential processing.

2.2.3. Cross-data space authentication mechanism for the API

KEYSTONE, in its primary intent, serves as a bridge between different platforms and heterogeneous data. This can also be summarized by considering KEYSTONE as a data space crossing system.

In this context, data —namely, information— becomes the cornerstone upon which the process relies and, moreover, the share of data, that underpins the concept of data space, becomes the primary fundament of the process itself.

From this perspective, cross-data space authentication mechanisms are crucial to ensuring their security and enabling reliable and compliant access and sharing. Specifically, this document will address the use of eID (electronic identification) as a canonical authentication mechanism through a national IdP. Additionally, it will provide guidelines for utilizing the eIDAS network of nodes as a mechanism for sharing eID with users of different nationalities within the European Union itself.

2.2.4. High automation level vehicles (CCAM)

The fast evolution affecting every aspect of transportation is evident to all, especially when we consider the technological advancements that transport vehicles are undergoing. Let’s take, for example, the seamless integration occurring among vehicles, infrastructure, and digital platforms within the concept of Cooperative, Connected, and Automated Mobility (CCAM).

This swift evolution cannot be overlooked, especially as we approach the study of information exchange between different platforms and the integration of data originating from databases that may exhibit significant technological disparities. From this perspective, we can envision the immense potential impact that CCAM technology could have within the KEYSTONE project.

2.3. Overview of the connections with the other WPs

The KEYSTONE project aims to take a significant evolutionary step in the intermodal transport sector by creating an advanced digital ecosystem.

In this context, the assigned task is crucial: to define, initially, the data that will need to be extracted from the platforms with which KEYSTONE will interact. This data will form the foundation for accurate monitoring of goods throughout the transportation process.

The definition of use cases, as derived from the requirements and described in Deliverable 1.4, serves as the starting point. These use cases outline notable examples of situations in which the KEYSTONE system will come into play.

Deliverable 1.3 conducted an in-depth study of existing platforms. This study provides an overview of the technologies, protocols, and interfaces used in the intermodal transport sector. KEYSTONE must efficiently and securely interface with these platforms. It is precisely with these platforms and through the functionalities that are exposed by these platforms that KEYSTONE will have to try to interface.

A crucial aspect concerns the continuous transmission of data across heterogeneous platforms. The data extracted by KEYSTONE from external platforms will have to be submitted to other external platforms, ensuring an uninterrupted flow of information.

So, attention inevitably shifts to legal and regulatory requirements. Legislative acts related to data privacy and security impose strict constraints, which KEYSTONE aims to address adequately, ensuring compliance and protection of sensitive data.

Accurate data definition, platform interfacing, and privacy management are fundamental elements that, through a bottom-up approach, will be utilized in developing the API standard, scheduled for Task 2.3.

3. API reference model overview

3.1. Overview of T2.1 – Objectives and Definition of the API Reference Model

In the contemporary logistics sector, seamless communication and interoperability among diverse systems are crucial. The absence of standardization leads to fragmented environments, increasing costs, delays, and operational inefficiencies. The complexity of integrating various logistics modes—such as rail, road, and maritime—further exacerbates these challenges due to differing protocols and data formats. Addressing these issues necessitates a robust framework for standardized communication.

To resolve these interoperability challenges, an API Standard has been proposed as a foundational solution, and the creation of an API Reference Model is a critical step toward its implementation. This model serves as the blueprint for the API's architecture, ensuring compatibility across systems and facilitating efficient data exchange between logistics organizations and enforcement authorities.

Task 2.1 aims to create a comprehensive API Reference Model intended to standardize methodologies for API development and usage within the logistic sector. The API Reference model's main goal is to ensure smooth communication between the various systems employed by transport operators and authorities, solving current issues with efficiency and coordination.

As the Deliverable D2.1 "API Reference Model" outlines:

"The API Reference Model is a pivotal component within the broader context of the KEYSTONE project's objectives. The endeavor to unify transport data across Europe requires standardized and interoperable digital solutions. D2.1 serves as a foundational element in this pursuit, providing a structured framework for API standardization that facilitates seamless data exchange among diverse stakeholders.

[..]

By creating the API Reference Model, D2.1 contributes directly to KEYSTONE's mission of bridging existing gaps in data-driven operations. It lays the groundwork for standardized communication protocols, enabling Plug-and-Play solutions that transcend the limitations of legacy systems. Moreover, D2.1 aligns with the project's aim to integrate existing data-driven platforms and services, fostering collaboration and interoperability across the European transport ecosystem.

[..]

By establishing standardized protocols and frameworks for data exchange, D2.1 [and the API reference model that it produced] contributes to enhanced safety, collaboration, cost efficiency, and scalability within the transport and logistics sector, ultimately advancing the overarching goals of the KEYSTONE project."

To achieve this goal, the development of the API Reference Model begins with an extensive literature review. This review examines existing methodologies, protocols, and best practices for API standardization. By understanding the current landscape, the gaps and areas for improvements are identified that the API Reference Model must address. This step ensures that the model is built on a thorough understanding of existing standards and practices.

A key part of developing the API Reference Model is exploring how APIs can be clearly defined and represented. This aligns with the KEYSTONE paradigm, which emphasizes that end-users should be able to

define their own APIs. Simultaneously, it should be straightforward for other end-users to map these services without requiring extensive programming or documentation. This approach ensures that the APIs are flexible and user-friendly, making them more accessible and easier to integrate across different systems.

The result of Task2.1 is the development of detailed documentation for the API Reference Model. This documentation is meant to be thorough and easy to understand, acting as a basic guide for the API Standard, which will be implemented in Task2.3, and the interactions across different systems.

3.2. Objective of API Reference Model and connection with T2.2

The development of the API Reference Model followed a structured and comprehensive methodology designed to ensure clarity, consistency, and effectiveness. This methodology began with a thorough analysis of requirements and the definition of use cases deriving from T1.4, which were essential for understanding both the functional and non-functional needs of the system. By identifying the key use cases that the API Reference Model must support, the development team was able to pinpoint the core functionalities and interactions required for seamless data exchange between organizations and authorities. This initial phase also involved determining the standardized approach to document sharing and compliance verification, which is crucial for the efficient transmission of essential information such as driver and vehicle details and transport operation types. This ensures that all stakeholders have access to accurate and up-to-date data.

Once the requirements were established, the focus shifted to designing the architecture and structure of the API Reference Model. This phase involved creating detailed Unified Modelling Language (UML) diagrams, including class diagrams and sequence diagrams, to visualize the components, relationships, and interactions within the system. The design adhered to best practices and design principles to achieve scalability, modularity, and adaptability for future enhancements. Comprehensive documentation was produced to secure the usability and maintainability of the API, ensuring that it could be easily integrated and understood by all users.

Finally, the methodology encompassed deploying the API Reference Model into use cases. Deployment strategies were carefully planned to facilitate a seamless transition to the operational phase, ensuring that the model could be effectively implemented in real-world scenarios, which will be further defined and thoroughly planned in the context of WP4, a work package dedicated to planning and executing pilots. This structured approach, encompassing thorough requirement analysis, detailed architectural design, and strategic deployment planning, was crucial for the successful realization of the API Reference Model's objectives.

The API Reference Model in its turn sets the stage for Task2.2, which aims to elaborate on specific components of the model to enhance interconnectivity and data exchange within the logistic sector. The primary goal of Task2.2 is to ensure seamless integration and communication between various platforms utilized within the logistic sector, including RESPER, ERRU, TACHONET, eFTI, etc. These platforms are essential for managing and regulating transportation activities, and Task2.2 seeks to define precise requirements for their interconnectivity. Importantly, the API Reference Model provides the necessary guidelines and standards for achieving this interoperability effectively.

Additionally, Task2.2 addresses the critical aspect of establishing robust authentication mechanisms for the APIs. This involves leveraging eID systems and cross-data space authentication mechanisms to ensure secure and reliable data exchange. The API Reference Model provides the foundation for implementing these authentication mechanisms consistently across different platforms and systems, thereby enhancing data integrity and trust among stakeholders.

In general, the API Reference Model aims to offer a consistent and adaptable framework that greatly improves compatibility throughout the logistic sector. By improving operational efficiency, reducing errors, and facilitating better coordination among stakeholders (enforcement authorities and logistic operators), the API Reference Model contributes to the creation of a more integrated and efficient logistic ecosystem.

4. Connection to other platforms

4.1. Overview

The interfacing of different systems is a crucial theme in the field of computer science and software engineering, particularly when defining a communication channel between systems that interact with one another through heterogeneous technologies.

The potential challenges that need to be addressed are evident, especially from a purely technical perspective. However, it is by no means guaranteed that solving technical problems will automatically resolve all possible issues.

In fact, many of these challenges may be related to the type of data we need to extract and handle. Therefore, we must consider the manipulation and management of data we encounter, from a legal and regulatory standpoint, too.

In our specific case, KEYSTONE necessarily has to interface with existing systems, and this requires embracing the technology through which these systems provide access to their data.

Regarding the data we require, we can divide what is obtainable from one of the systems we can interact with from what is unattainable and represents an information gap. Consider data that may be subject to privacy restrictions, where we might not have authorization to obtain it even if it is technically accessible. Alternatively, there may be data not yet available on the platforms we interface with.

Especially in the latter case, it could be plausible to bridge the information gap by implementing a proprietary database located on a server within KEYSTONE's control. This could include a cloud-based structure, which would potentially reduce the operational effort required for management and maintenance.

Naturally, the possibility of filling the information gap through the implementation of a local database at KEYSTONE, while entirely plausible, falls outside the scope of Task2.2. Such a scenario will be explored and carefully considered in the context of WP3, which has the objective to design and develop the KEYSTONE web app interface and backend, while this specific section focuses exclusively and in detail on the data that can be obtained from existing platforms.

4.2. Platforms stemming from the use cases study

As previously mentioned in last paragraph, Deliverable 2.2 focuses on defining the data to be extracted from the platforms with which KEYSTONE interfaces. Naturally and canonically, identifying and defining the data we need to extract from these platforms involves pinpointing the technologies that provide access to this data.

All of this is analysed here exemplarily for the use cases that emerged during the study conducted in Task 1.4 and for the platforms involved in these use cases, as studied within the scope of Task 1.3.

For this reason, the study that characterizes Task 2.2 must necessarily begin where the study carried out within Task 1.4 ends, namely from the formalization of use cases extracted from the two scenarios that will compose the basis of the pilots that will be designed and implemented in the context of the dedicated WP4.

As we can see, next paragraphs will provide two types of diagrams for describing the use cases we have to consider, the use case diagrams and the sequence diagrams. In fact, use case diagrams provide a high-level view of system functionalities, while sequence diagrams delve into object interactions during execution.

Moreover, a textual description of the sequence of interactions will follow. Actually, the so said “use case stories” provide a detailed step-by-step descriptions of system behaviour and interactions, including alternative and optional flows, and help to define how a system should function in various situations.

The next sections delve into the use cases in more detail.

4.2.1. Police controls over transport

4.2.1.1. From Deliverable 1.4

For instance, we have identified an intermodal rail shipment originating from an origin port, such as Rotterdam, and forwarded by rail to an inland terminal, potentially Novara's terminal. Subsequently, the last-mile transportation operation, typically conducted via road, involves enforcement authorities, such as police, which can check for compliance with regulations by carrying out necessary controls.

What is described in the Deliverable 1.4 in relation to this use case, can be obviously schematized by using a use case diagram and completed describing its interactions among the various system components using a sequence diagram.

The next sections delve into the use cases in more detail.

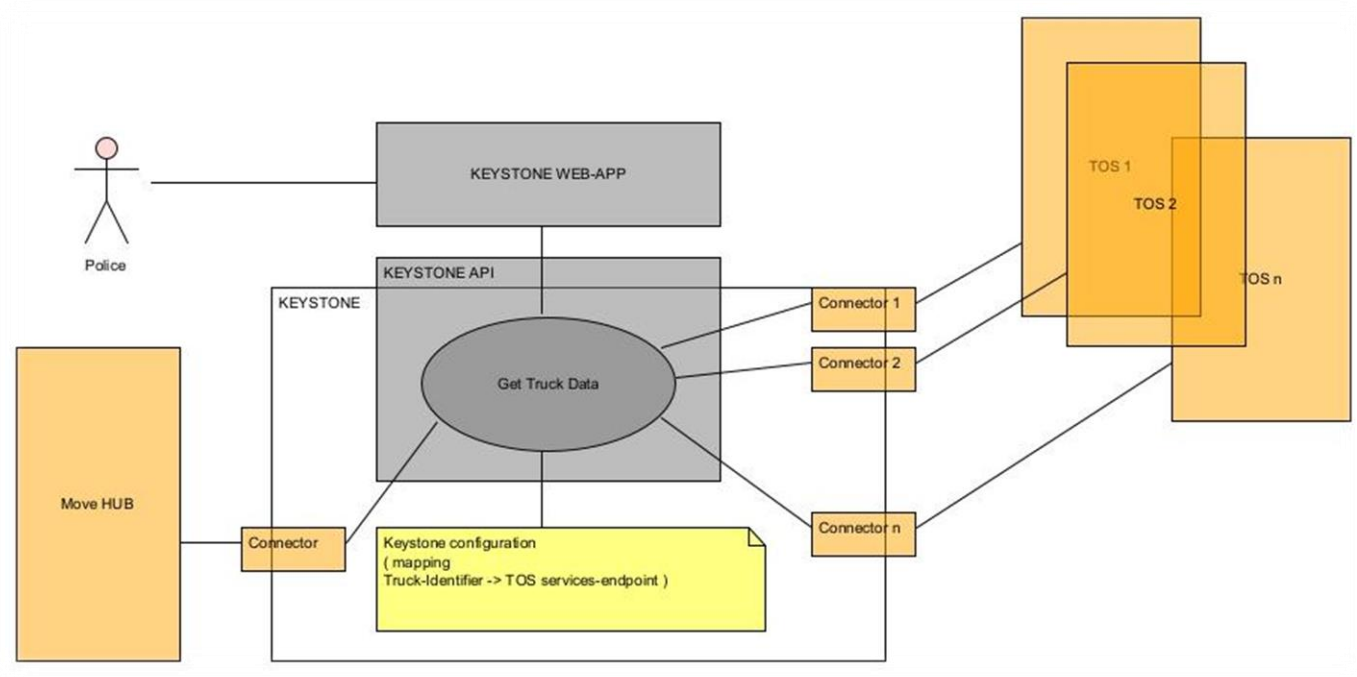

Figure 1 - Police controls over transport use case diagram

In the diagram shown here, it is hypothesized that it is possible to extract data also from the MoveHub platform, which in turn shares data from other platforms present in the European Union member states and addresses the same data to all the federated platforms.

The data involved in the sharing process onto the MoveHub net:

- Tachograph Cards (data from TACHOnet)
- Infringements committed by transport undertakings and evaluation system (data from ERRU)
- Driving licenses (data from RESPER)
- Information about professional drivers' qualification between MS (data from ProDriveNet)
- Information about roadside inspections done in a MS different than the MS of registration of the vehicle (data from RSI)

Naturally, this is a hypothesis of possible use, as at present it would be necessary to request access to at least mock-up data, which is technically possible but not actually provided except by using the HTML portal and therefore through a user interface and not through access with a web services connector.

Nevertheless, the following interactions are observed:

- The Police access the KEYSTONE web-app.
- The KEYSTONE web-app interfaces with KEYSTONE through the APIs.
- KEYSTONE retrieves the requested data using appropriate connectors that adapt the requests to the different TOS with which it necessarily interfaces.
- In case of connection with MoveHub, KEYSTONE retrieves the requested data using an appropriate connector.
- The data extracted from the TOS (and eventually from MoveHub) has not persisted in KEYSTONE because extraction of data and their visualization happen in a synchronous way.

This last point has a positive impact on operational aspects, as it relieves KEYSTONE from security, privacy, and data consistency issues, as well as the need for table maintenance and periodic backups.

4.2.1.2. Sequence diagram and use case story

The sequence diagram precisely depicts the interactions among the KEYSTONE webapp, its backend and the TOS. The interaction between the KEYSTONE APIs and MoveHub is defined as "optional", to do in case it is effectively possible.

The execution timeline, from top to bottom, represents the chronological order in which interactions occur when this specific use case is executed.

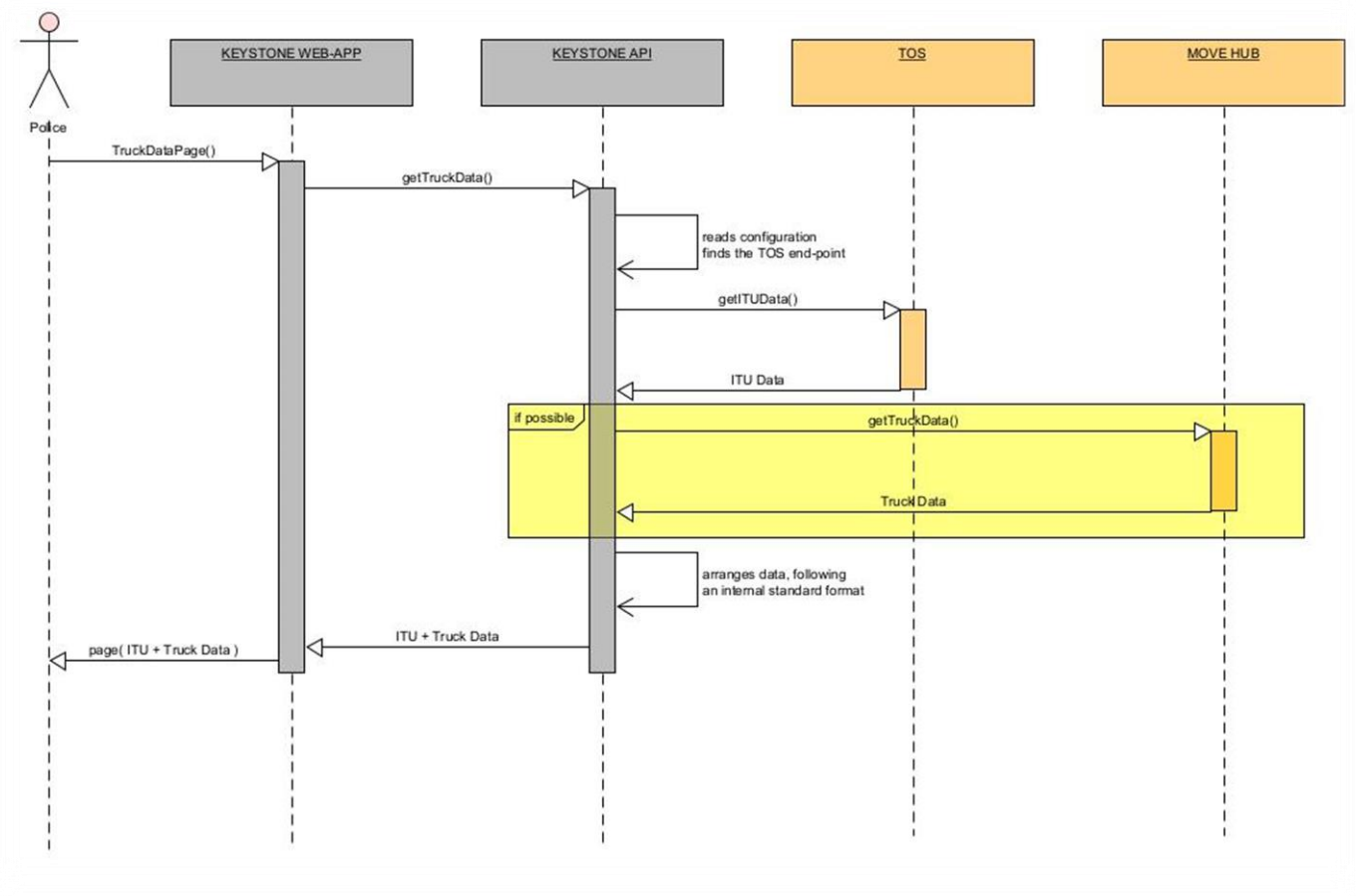

Figure 2 - Police controls over transport sequence diagram

From the sequence diagram, it is possible to provide the use case story, a textual description.

1. Police use the KEYSTONE webapp to interact with the system, asking for a page with the data of the truck and the data of transport.
2. KEYSTONE obtains the references to the services from of the TOS platform exposing the data of the truck (by example KEYSTONE could call the TOSs' services and matching data coming from there with the truck plate number).
3. KEYSTONE can connect services from other platforms (by example MoveHub, if will be possible) and can extract data needed from that site.
4. KEYSTONE connects to the correct TOS and downloads the data of the truck and transport (ITU)
5. Data is standardized and prepared for the response.
6. Data is sent to the webapp, to be viewed in a user-friendly format and thus checked by the Police.

4.2.1.3. A plausible alternative

In the aforementioned use case, it seems sensible to retrieve transportation data based on the license plate of the vehicle under police control. This would allow stopping the vehicle already possessing transportation data, thus minimizing both inspection times and limiting stops to cases deemed of greater interest by the inspection personnel.

It is reasonable to consider maintaining transportation data in a local KEYSTONE database and retrieving this data upon request, ensuring it is associated with the vehicle's license plate and the timestamp interval defined by the loading time and estimated arrival time at the destination.

The necessity of having data readily available suggests implementing a mechanism where KEYSTONE acts as a server and listens for communications from the TOS.

The TOS would make calls whenever there is a need to transfer new data to KEYSTONE or modify previously sent data.

However, since this approach would require the TOS to implement the client and map its internal data structure to KEYSTONE's standard, an alternative mixed client-server architecture could be considered.

Such an architecture would be more flexible and adaptable to diverse requirements.

A comprehensive use case diagram is provided below.

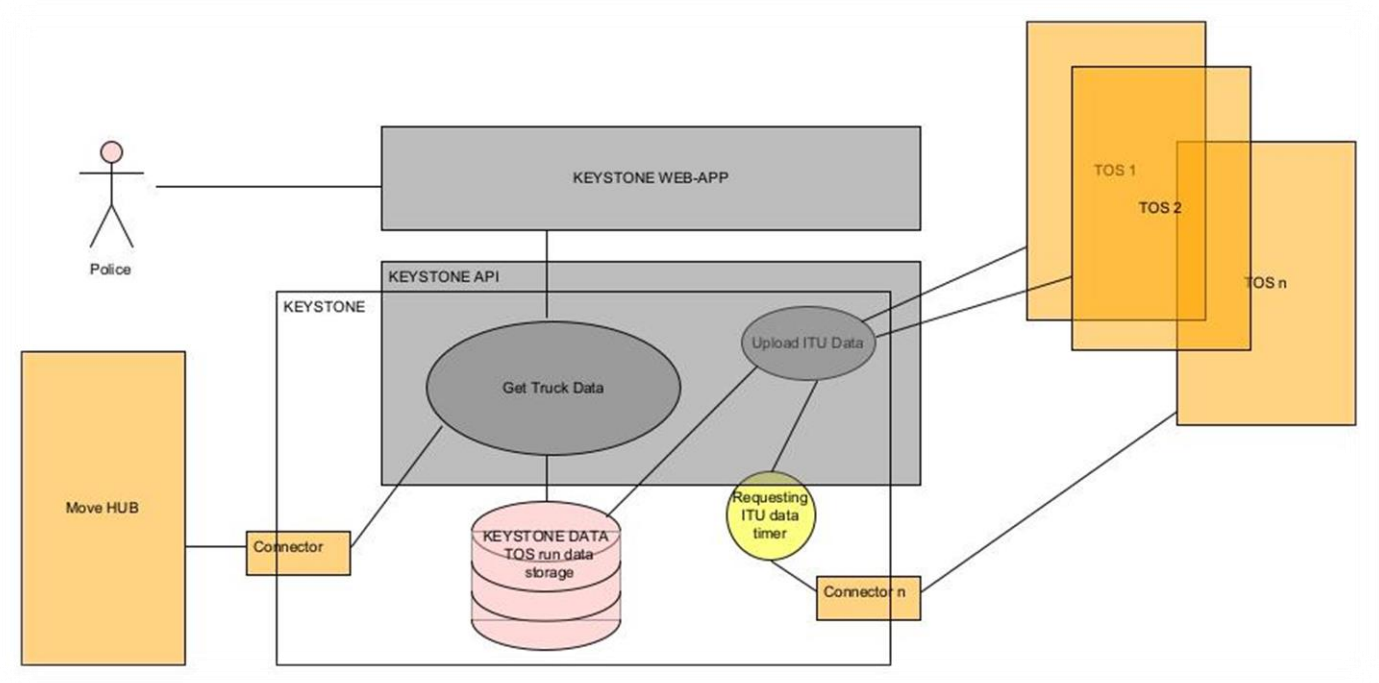

Figure 3 - Police controls over transport alternative use case diagram

In this alternative use case, the main differences are:

- The presence of a local database on which data comes from platforms which KEYSTONE interfaces with.
- The presence of APIs implemented specifically for receiving data comes from platforms which KEYSTONE interfaces with (in our case, from TOSs)
- The presence of a "timer" for requesting the data from TOSs connecting by a connector and being used as lato server of the web services
- The incremented flexibility, due to the fact with this architecture we can interface KEYSTONE platform both with TOSs working in push and with TOSs exposing their data via web services.

4.2.1.4. Alternative sequence diagram and related use case story

The following sequence diagram shows both the possibilities to have a connection with the various TOSs

- Calling the KEYSTONE's API and uploading the data, every time there are new data and every time the submitted data changed
- Waiting the temporized call from a KEYSTONE timer, that downloads or upgrades the needed data with a certain frequency

For all the rest is exactly as the previous one. Let' see it.

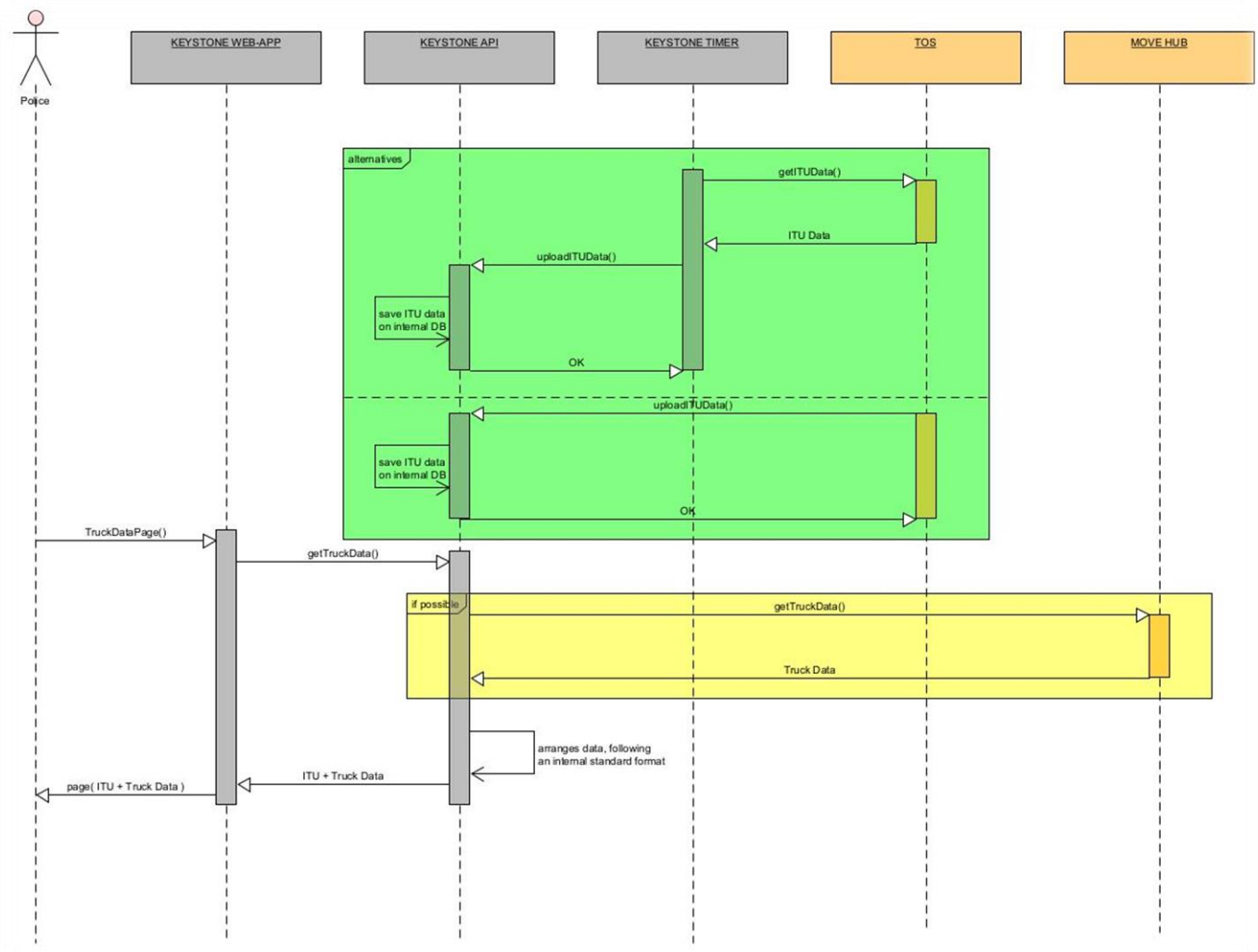

Figure 4 - Police controls over transport alternative sequence diagram

From the sequence diagram, it is possible to provide the use case story, a textual description, as just done in the previous paragraphs.

1. Data from TOS comes to KEYSTONE APIs:
   a. TOS, every time it needs (in case of a new transport leaving the intermodal center or in case of changes to a transport that previously leaved the intermodal center), uploads its data (ITU data) to the KEYSTONE APIs.
   b. A timer, with a certain frequence, uses a connector to ask for data from TOS (ITU data) and uploads this data to the KEYSTONE APIs.
2. Police use the KEYSTONE webapp to interact with the system, asking for a page with the data of the truck and the data of transport.
3. KEYSTONE can connect services from other platforms (by example MoveHub, if will be possible)

and can extract data needed from that site.
4. ITU data are taken from the database.
5. Data is standardized and prepared for the response.
6. Data is sent to the webapp, for being viewed.

4.2.2. Data integration between TMS and PCS

4.2.2.1. From Deliverable 1.4

“In the example provided, road transport via truck is utilized, envisioning the collection of a container from a manufacturing company and its transportation to the loading port.

[..]

“.. administrative authorities, like port authorities, are involved in this scenario”

[..]

“The interactions with port authority will be realized in advance by a prenotice of arrival to the PCS, possible just thanks to KEYSTONE.”

As said for the previous use case, what is described in the Deliverable 1.4 can be schematized by using a use case diagram and completed describing its interactions among the various system components using a sequence diagram.

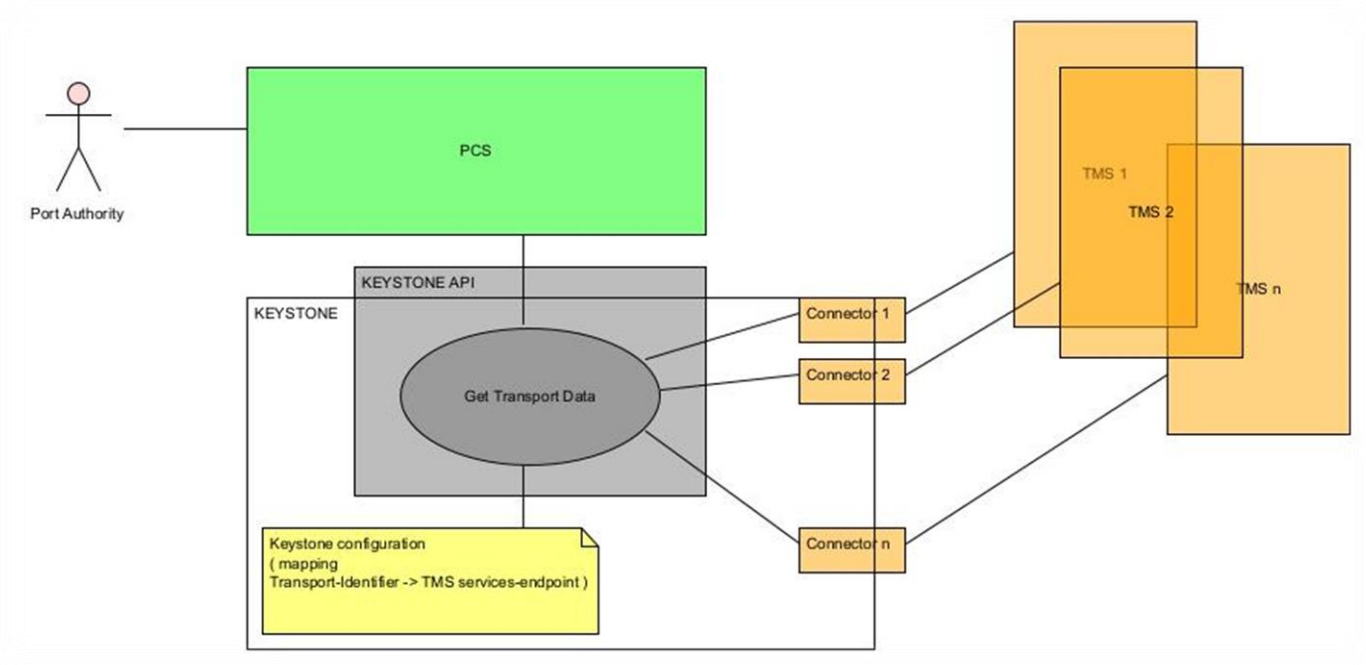

Figure 5 - Data integration between TMS and PCS use case diagram

Also in this case, what has been conceived in Task 1.4, is somewhat surpassed by a diagram that highlights the components of the KEYSTONE system with which the use case itself can and must interact.

Specifically, the following interactions are observed:

- The port authority interacts with the PCS.
- The PCS, just like all external systems, typically interface with KEYSTONE through the APIs provided by KEYSTONE itself.
- KEYSTONE retrieves the requested data using appropriate connectors that adapt the requests to the different TMS (Transportation Management Systems) with which it necessarily interfaces.
- The data extracted from the TMS has not persisted in KEYSTONE because communication with the PCS is synchronous and on-demand.

As the previous use case, this last point has a positive impact on operational aspects, as it relieves KEYSTONE from security, privacy, and data consistency issues, as well as the need for table maintenance and periodic backups.

4.2.2.2. Sequence diagram and use case story

The sequence diagram precisely depicts the interactions between the PCS, KEYSTONE, and the TMS from which data is extracted for display by the Port Authority to schedule port access.

The execution timeline, from top to bottom, represents the chronological order in which interactions occur when this specific use case is executed.

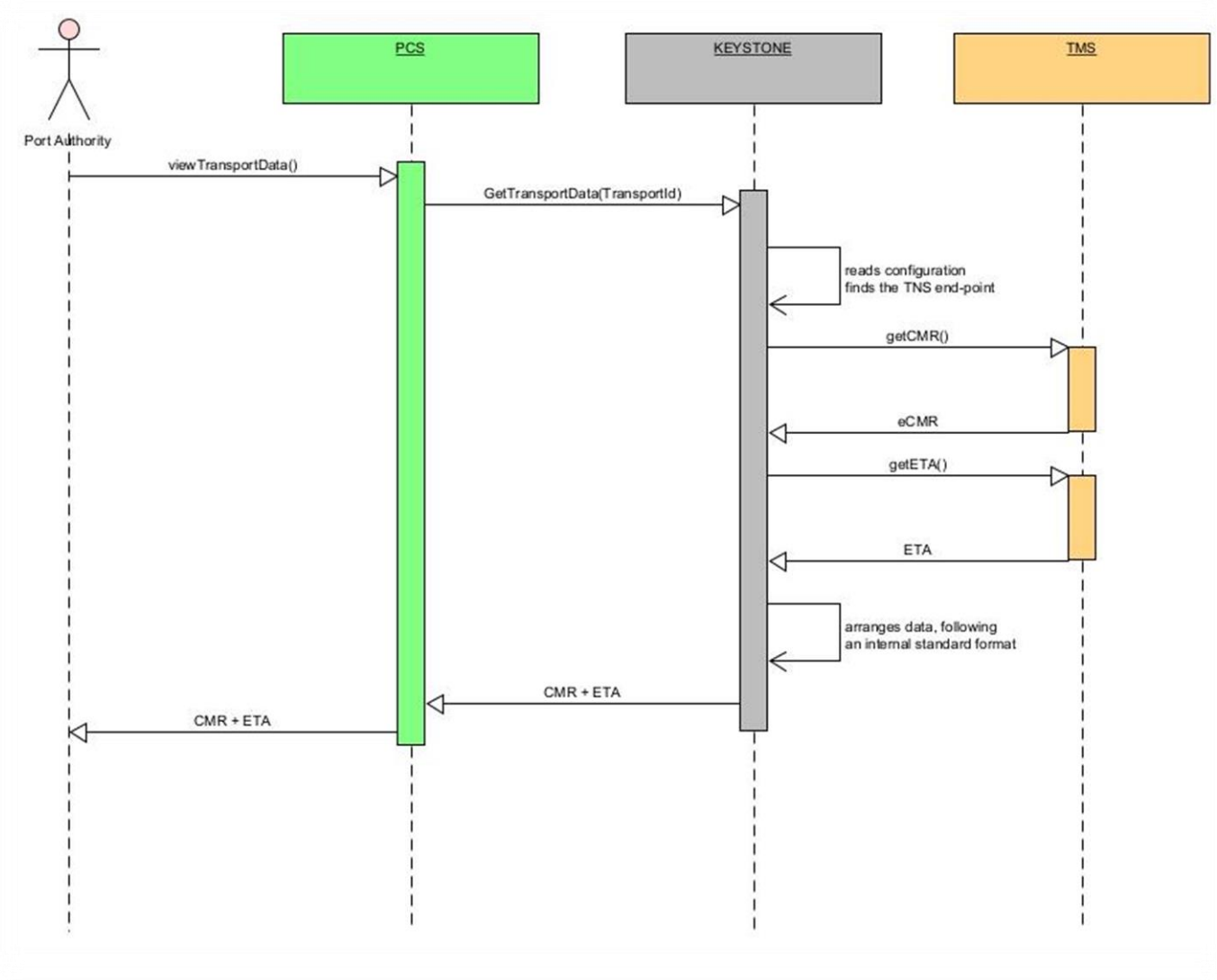

Figure 6 - Data integration between TMS and PCS sequence diagram

From the sequence diagram, it is possible to provide the use case story, a textual description.

1. The Port Authority interacts with its PCS for have a plan of the next arrivals at the port
2. PCS asks for transport data to KEYSTONE system, passing an identifier of the transport company of which want to have data from
3. KEYSTONE obtains the references to the services of the TMS platform exposing the data the transport (by example the KEYSTONE could be configured with a map between transport company and its TMS services endpoint)
4. KEYSTONE connects to the correct TMS and downloads the data of the transport (e-CMR)
5. KEYSTONE connects to the correct TMS and downloads the estimated time of arrival (ETA)
6. Data is standardized and prepared for the response
7. Data is sent to the PCS
8. Data is viewed from the Post Authority

4.3. Legal implications in the retrieval and use of the information involved in the use cases

It is likely that a transport operator is checked for compliance with the following EU regulations (among others) during roadside check or during a check at the premises of the company:

1. Rules on Driving and Rest times contained in Regulation (EC) No 561/2006 of the European Parliament and of the Council.
2. Rules on installation and use of tachographs, driver cards and record sheets as well as malfunctions of tachograph contained in Regulation (EU) No 165/2014 of the European Parliament and of the Council.
3. Working time rules contained in Directive 2002/15/EC of the European Parliament and of the Council.
4. Weight and dimension rules as per Council Directive 96/53/EC.
5. Rules on roadworthiness of a vehicle i.e. keeping the vehicle in a safe and roadworthy condition and proof of periodic roadworthiness tests as per Directive 2014/45/EU and Directive 2014/47/EU of the European Parliament and of the Council.
6. Rules on fitting and correct use of speed limitation device as per Council Directive 92/6/EEC.
7. Rules on initial qualification and periodic training of drivers as per Directive 2003/59/EC.
8. Driving licences requirements as per Directive 2006/126/EC.
9. Rules on Transport of dangerous goods by road in Directive 2008/68/EC.
10. Rules on access to the international road haulage market as per Regulation (EC) No 1072/2009.
11. Rules on access to the market for coach and bus services as contained in Regulation (EC) No 1073/2009.
12. Rules on Animal transport as per Council Regulation (EC) No 1/2005.
13. Rules on contractual obligations contained in Regulation (EC) No 593/2008.
14. Rules on posting of workers in road transport as per Directive (EU) No 2020/1057.

To conduct checks for compliance with above regulations the enforcers may check the following types of data:

Table 1 - Data helping enforcers controls

Information that can help enforcers	Data about
Identification Document (ID) + visa or residence permit for some third country drivers	Driver
Driving Licence	Driver
Certificate of Professional Competence for Drivers (CPC or Code 95)/driver qualification card as per Directive (EU) 2022/2561 as proof of initial and periodic training	Driver
Authority to drive (if driver non-EU)/Third Country Driver Attestation	Driver
Driver Tachograph Card	Driver
ADR driver training certificate	Driver
Posting Declaration	Driver
Social Security A1 form	Driver
Tachograph records/data/printouts	Driver/Vehicle
Additional trip related documents such as ferry tickets, fuel receipts etc.	Driver/Vehicle
Vehicle Registration	Vehicle
Proof of recent technical inspections	Vehicle

Certificate of Conformity	Vehicle
Vehicle Technical Papers	Vehicle
Insurance Documents	Vehicle
Roadworthiness Certificate	Vehicle
ADR approval certificate of the vehicle	Vehicle
Consignment note or equivalent (CMR document)	Load
Passenger Waybill	Load
All paperwork associated with a hazardous load	Load
Journey Form (Occasional passenger transport)	Load
Certificate of Professional Competence for Transport Managers as per REGULATION (EC) No 1071/2009	Transport Undertaking/Manager
ADR authorisations	Transport Undertaking
European Conference of Ministers of Transport (ECMT) permit	Transport Undertaking
Bilateral agreement permit (biliteral international, transit or cross-trade)	Transport Undertaking
Authorization for regular lines in passenger transport	Transport Undertaking
Community License (certified true copy) or equivalent document for third country operator (e.g., UK)	Transport Undertaking
Risk Rating	Transport Undertaking
Proof of Disposal of any Historic Infringement	Transport Undertaking/Driver

It must be noted that information needed by enforcers may be of different types

- Some information may be available to enforcers upfront from a primary source and maybe usable as such (e.g., tachograph data).
- Some information may need further validation from authorities in the foreign country where the transport company is registered (e.g., validity of licenses and cards).
- Lastly, some information may still need to be collected from authorities in the foreign country where the transport company is registered (e.g., information on past infringements) or from the transport company itself (e.g., documents on posting of drivers and other regulatory compliance documents).

5. A custom example of interconnectivity

5.1. Introduction

As emerged from the many meetings held with our partners, our focus will be on implementing two pilot projects as outlined in the dedicated WP4 and its objectives.

From these demonstration scenarios, which will be formally defined later within the WP4, we have extracted the use cases recently presented in this document.

This has allowed us to concentrate on the interaction with a specific TOS, which will be the subject of the pilot related to intermodal transport, and with a well-defined TMS, which will, in turn, be the subject of the pilot project related to transport and communication of transport data between TMS and PCS.

Let's now analyse in a more depth way the interaction with the two platforms that currently appear to be the main candidates for implementing the two pilot projects within WP4.

5.2. EDIGES

"EDIGES" is the TOS platform for the intermodal centre in Novara.

The scenario under consideration involves the arrival of a train at the Novara intermodal centre, announced by the train's ETA, the loading of the truck, and the transmission of ITU pickup data to the KEYSTONE platform via APIs.

In this specific case, where KEYSTONE acts as the server, it isn't necessary to implement a connector to the TOS. Additionally, a specific part of the API must be instead designed to receive data from the TOS.

It makes sense to use the same technology for implementing the APIs through which KEYSTONE will expose its data to the web app and third-party systems.

Implementing push services with the same technology as pull services is the norm as the proliferation of different technologies certainly goes against the principles of symmetry and uniformity and naturally favors maintenance and update processes.

Nevertheless, it could facilitate the integration of push connections, the fact of proposing interfaces of different technologies for the same service. For example, you could have both the SOAP interface and the REST interface, which then flow to the same business layer. This would of course increase maintenance costs but would help the integration of third-party systems.

At this stage, we propose using REST services, although this document won't provide APIs writing guidelines; those will be addressed and formalized in subsequent deliverables, namely D2.3 API standard and D2.5 API standard V2, which will provide an elaborate overview of the development of the API standard and the implementation of a specific Python library, using the reference model outlined in D2.1. As for the data obtained from EDIGES, let's analyse what EDIGES offers regarding transport and truck data, specifically grouped under the name "ITU Pickup."

Below is an extract related to the ITU details from the EDIGES documentation that describes the data contained in the XML structure.

Segment description:

- **PickupGateout:** identifies the message of picking-up the ITU by road.
- **Supplier:** includes the univocal identification of the EDI partner of the Goal operator.
- **Orderer:** name of the receiver of the XML EDI message.
- **ItuDetails:** identifies the picking-up of the ITU.
- **DeliveryDistribution:** this segment contains information regarding delivery process, before Terminal arrival or distribution information after ITU pickup.

The table of the elements follows, seeming to be of a certain importance in the KEYSTONE context and related to the use case described at the Paragraph “A plausible alternative”

Table 2 - Data and datatypes from EDIGES TOS platform

Segment	Element	Type	Description
PickupGateout	pickupGateOutMsgDate[1]	String, length 8	Pickup Gate Out date of message.
	pickupGateOutMsgTime[2]	String, length 8	Pickup Gate Out time of message.
Supplier	supplierCompanyName	String, length 0..20	Supplier Name.
Orderer	ordererCompanyName	String, length 0..20	Orderer Name.
ItuDetails	trainNumber	String, length 0..6	Train Number.

[1] The data format was originally saved in the attribute of the XML element, since the EDIGES services are implemented with SOAP technology. If we want to maintain the same datatype (String) we have surely to add a field with the format of the date. By example pickupGateOutMsgDateFormat (e.g. “yyyyMMdd”)

[2] The data format was originally saved in the attribute of the XML element, since the EDIGES services are implemented with SOAP technology. If we want to maintain the same datatype (String) we have surely to add a field with the format of the date. By example pickupGateOutMsgTimeFormat (e.g. “HH:mm:ss”)

	departureDate[3]	String, length 8	Date of departure (Date of closure of unit acceptance in terminal, not the real train departure from terminal)
	realTrainDepartureDate[4]	String, length 8	Real train departure date from terminal.
	wagonNumber	String, length 0..13	Wagon Number.
	ituCode	String, length 0..20	ITU Code.
	driverName	String, length 0..20	Driver name.
	driverIdNumber	String, length 0..20	Driver Identification document number.
	driverIdDocument	String, length 0..10	Driver Identification document type.
	driverCompany	String, length 0..20	Driver company.
	DriverCompanyUIRRCode	Integer, 5	Driver company UIRR code.
	vehicleLicencePlate	String, length 0..20	Vehicle licence plate.

[3] The data format was originally saved in the attribute of the XML element, since the EDIGES services are implemented with SOAP technology. If we want to maintain the same datatype (String) we have surely to add a field with the format of the date. By example departureDateFormat (e.g. “yyyyMMdd”)

[4] The data format was originally saved in the attribute of the XML element, since the EDIGES services are implemented with SOAP technology. If we want to maintain the same datatype (String) we have surely to add a field with the format of the date. By example realTrainDepartureDateFormat (e.g. “yyyyMMdd”)

5.3. GRUBER BEYOND

“GRUBER BEYOND” is the GRUBER’s Transportation Management System (TMS), entirely developed by GRUBER Logistic company.

The platform exposes REST services organized as microservices and callable by using an API Key that needs to be specified in the Api Key Header.

Most APIs require a X-ZUMO-AUTH header, that can be requested in the User Managment API /user_authentication endpoint, using credentials created in the Mydesk Platform[5].

There are two main services from which one can retrieve data related to a transport (data that typically contribute to the composition of the CMR/eCMR) and the estimated time of arrival (ETA) at the destination. Let’s see what they are and which data they involve[6].

5.3.1. ORDERS

The GRUBER LOGISTIC’s orders management system (gl-ms-orders) allows access to all data related to orders processed by Gruber Logistic.

Among the GET methods, there is one to retrieve all orders, with the possibility to filter based on fields of interest. For example, considering the specific use case at the paragraph "Data integration between TMS and PCS" and applying it to the context in which the PCS related to the ports of the Ligurian Sea integrates with GRUBER BEYOND services, one could imagine making a call to download all orders (to be optimized when possible, using an appropriate filter).

Table 3 - Examples of calls and responses to the GRUBER BEYOND TMC platform REST services (endpoint orders/all)

Web Service	Endpoint	Example call	Example of response data
gl-ms-orders	https://gw.gruber-logistics.com/orders/v1/orders/all	https://gw.gruber-logistics.com/orders/v1/orders/all?getAll=true	{ "message": "", "success": false, "data": { "currentPage": 1, "pageSize": 10, "rowCount": 76, "pageCount": 8, "results": [{ "id_order": "5-C-BZ-2021-276", "administrative_status": "OPEN", "currency_type": "EUR", "gruber_company": "5", "gruber_branch": "BZ", "gruber_type": "T", "customer": {

[5] Reachable at the address https://mydesk.gruber-logistics.com/login
[6] Access to the GRUBER BEYOND’s APIs’ developer site by https://developer.gruber-logistics.dev/

```
        "id_customer": "5-C-139162",
        "company_code": "5/C/139162",
        "company_name": "PELLINI CAFFE'  SPA",
        "language": "IT",
        "isGruber": false
      },
      "first_loading_address": {
        "name": "Test loading point from WCF",
        "street": "Via Venezia, 49",
        "city": "Trento",
        "zip": "38122",
        "province": "TN",
        "zone": "I38",
        "country": "IT",
        "address_reference": "",
        "email": "",
        "phone": ""
      },
      "first_loading_datetime": "2021-09-06T12:00:00.000Z",
      "last_unloading_address": {
        "name": "Unloading point",
        "street": "Marburger Str. 390",
        "city": "Kreuztal",
        "zip": "57223",
        "province": "",
        "zone": "D57",
        "country": "DE",
        "address_reference": "",
        "email": "",
        "phone": ""
      },
      "last_unloading_datetime": "2021-09-08T08:30:00.000Z",
      "order_date": "2021-09-06T11:46:00.000Z",
      "order_number": "276/BZ/2021",
      "order_reference": [
        {
          "_id": "61360b6b588253002224a422",
          "type": "ORDER",
          "value": "202106091415"
        }
      ],
      "status": "NOEVENTS",
      "total_charge": 0,
      "transport_document": [],
      "insert_user": "bonetta@gmail.com",
      "update_user": "bonetta@gmail.com",
```

			"syncToSGAStatus": "NO", "created_at": "2021-09-06T11:46:00.000Z" }] } }

From the list of all orders (eventually filtered) and extracting the orders' identifiers, it will be possible to access the data of each individual order. This is the service doing it.

Table 4 - Examples of calls and responses to the GRUBER BEYOND TMC platform REST services (endpoint orders/{id_order})

Web Service	Endpoint	Example call	Example of response data

gl-ms-orders	https://gw.gruber-logistics.com/orders/v1/orders/	https://gw.gruber-logistics.com/orders/v1/orders/5-C-BZ-2021-276	{
			"message": "",
			"success": false,
			"data": {
			"id_order": "5-C-BZ-2021-276",
			"administrative_status": "OPEN",
			"created_at": "2021-09-06T11:46:00.000Z",
			"cancelled": false,
			"currency_type": "EUR",
			"gruber_company": "5",
			"gruber_branch": "BZ",
			"gruber_type": "T",
			"customer": {
			"id_customer": "5-C-139162",
			"company_code": "5/C/139162",
			"company_name": "PELLINI CAFFE' SPA",
			"language": "IT",
			"isGruber": false
			},
			"detailed_charge": [
			{
			"charge_amount": 200,
			"charge_description": "Freight"
			}
			],
			"dispatcher": {
			"id_dispatcher": "5-04",
			"name": "Karl Viehweider",
			"email": "abc@gruber-logistics.com",
			"phone": "+39 0471 825 603"
			},
			"first_loading_address": {
			"position": {

```
        "coordinates": [
          0
        ]
      },
      "name": "Test loading point from WCF",
      "street": "Via Venezia, 49",
      "city": "Trento",
      "zip": "38122",
      "province": "TN",
      "zone": "I38",
      "country": "IT",
      "address_reference": "",
      "email": "",
      "phone": ""
    },
    "first_loading_datetime": "2021-09-06T12:00:00.000Z",
    "last_unloading_address": {
      "position": {
        "coordinates": [
          0
        ]
      },
      "name": "Unloading point",
      "street": "Marburger Str. 390",
      "city": "Kreuztal",
      "zip": "57223",
      "province": "",
      "zone": "D57",
      "country": "DE",
      "address_reference": "",
      "email": "",
      "phone": ""
    },
    "last_unloading_datetime": "2021-09-08T08:30:00.000Z",
    "mode": "Road",
    "order_date": "2021-09-06T11:46:00.000Z",
    "order_number": "276/BZ/2021",
    "order_reference": [
      {
        "_id": "61360b6b588253002224a422",
        "type": "ORDER",
        "value": "202106091415"
      }
    ],
    "specifications": [
      {
```

```
    "code": "CODE",
    "qty": 13,
    "note": "Note for the specifications"
  }
],
"status": "NOEVENTS",
"stops": [
  {
    "address": {
      "position": {
        "coordinates": [
          0
        ]
      },
      "name": "Test loading point from WCF",
      "street": "Via Venezia, 49",
      "city": "Trento",
      "zip": "38122",
      "province": "TN",
      "zone": "I38",
      "country": "IT",
      "address_reference": "",
      "email": "",
      "phone": ""
    },
    "requested_datetime": {
      "from": "2021-08-24T07:00:00.000Z",
      "to": "2021-08-24T08:00:00.000Z",
      "range": "Between",
      "compulsory": false
    },
    "external_key": [
      "5-C-BZ-2021-256_1"
    ],
    "stop_type": "COLLECTION",
    "goods": {
      "goods_type": "AS",
      "goods_description": "Accessori",
      "weight": 5,
      "reference": "",
      "size": [
        {
          "type": "Type of Size",
          "description": "Size Description",
          "width": 2,
          "height": 12,
          "depth": 5,
          "unitary": true,
```

```
            "um": "mm"
          }
        ],
        "ums": [
          {
            "um": "QTY",
            "um_description": "Quantità",
            "qty": 1
          }
        ],
        "source_destination": "GRUBER LOGISTICS - INTERPORTO REGIONALE DELLA PUGL VIALE GIUSEPPE DE GENNARO, 1 70123 BARI BA IT",
        "returnable_packaging": [
          {
            "type": "string",
            "qty": 1
          }
        ]
      },
      "note": "Notes",
      "stop_reference": "string",
      "stop_remarks": "Remarks",
      "goods_value": {
        "currency": "EUR",
        "amount": 120.2
      },
      "pallet_exchange": [
        {
          "type": "pallet type",
          "qty": 10
        }
      ],
      "adr": [
        {
          "code": "xxx",
          "package_type": "type of package",
          "package_description": "package description goes here",
          "qty": 10,
          "um": "Weight",
          "amount": 120,
          "limited_qty": true
        }
      ]
    }
  ],
  "total_charge": 0,
```

			"transport_document": [],
			"trips": [
			{
			"id_trip": "string"
			}
			],
			"updated_at": "2022-01-12T11:45:45.737Z",
			"cash_on_delivery": {
			"currency": "EUR",
			"amount": 101.3,
			"type": "BANK_CHECK"
			},
			"information_complete": true,
			"rules_applied": [
			{
			"datetime": "2021-09-06T12:00:00.000Z",
			"rule_Id": "Id for Rules Collections"
			}
			],
			"incoterms": "EXW",
			"insert_user": "bonetta@gmail.com",
			"update_user": "bonetta@gmail.com",
			"syncToSGAStatus": "SYNCED",
			"sgaError": [
			{
			"datetime": "2021-09-06T12:00:00.000Z",
			"error": "Error at Sync to SGA Detail Goes here"
			}
			]
			}
			}

5.3.2. EVENTS

The GRUBER LOGISTIC's events management system (gl-ms-events) allows access to all data related to events processed by Gruber Logistic.

Events are a fundamental entity in GRUBER BEYOND platform, since they can regard both the orders and the trips, can be descriptive about what just happened or predictive about what should happen and can be continuously updated, so to have the data up to date.

The call to the service events/v1/events/trip, passing the trip identifier as input data, provides as output the list of all events that occurred during that trip.

Among these events, once submitted by the TMS, there will be an estimate of the arrival time at the destination, and this data, which naturally represents the ETA, will be constantly updated until the actual arrival time, to provide a particularly accurate estimate.

Table 5 - Examples of calls and response to the GRUBER BEYOND TMC platform REST services (endpoint events/trip/{id_trip})

Web Service	Endpoint	Example call	Example of response data

gl-ms-events	https://gw.gruber-logistics.com/events/v1/events/trip/	https://gw.gruber-logistics.com/events/v1/events/trip/5f7186529a2932001c888804	{
			"message": "",
			"success": false,
			"data": {
			"{id_trip}": [
			{
			"_id": "5f7186529a2932001c888804",
			"unique_key": "TVV_5-C-BZ-2020-138_LOA_2",
			"additional_info": {
			"terminal": "N",
			"tipo_scarico": ""
			},
			"address": {
			"position": {
			"type": "Point",
			"coordinates": [
			8.85484,
			45.61188
			]
			},
			"ragione_sociale": "HUPAC SPA",
			"indirizzo": "VIA DOGANA 8/10",
			"zona": "I21",
			"cap": "21052",
			"localita": "BUSTO ARSIZIO",
			"provincia": "VA",
			"nazione": "IT"
			},
			"asset": {
			"asset_id": "",
			"asset_type": ""
			},
			"cliente_numero_carico_scarico": "1",
			"event_type": {
			"name": "LOA",
			"description": "Arrived at loading place",
			"order": 1,
			"category": "timeline",
			"status": "LOADING",
			"trip_show": true,
			"order_show": true,
			"time_show": true,
			"update_isExpected": true,
			"canBeDone": false

```
        },
        "expected_datetime": "2019-12-31T08:00:00+0100",
        "fixed": false,
        "id_order": [
          "5-C-BZ-2019-63809"
        ],
        "id_trip": "5-C-BZ-2020-138",
        "id_trip_previous": "",
        "isExpected": true,
        "limit_confirm_datetime": "2019-12-31T10:00:00.000Z",
        "limit_expected_datetime": "2019-12-31T06:00:00.000Z",
        "origine": "T2_VIAGGI_VETTORI",
        "progressivo": 2,
        "provisional": false,
        "timezone": "Europe/Rome",
        "update_time": "2021-06-22T15:09:48.629Z",
        "vehicle": {
          "id": "",
          "id_trailer": "",
          "plate_number": "",
          "trailer_plate_number": ""
        },
        "progressivo_alias": [],
        "isDeletable": false
      }
    ]
  }
}
```


5.3.3. A look up on the future

What has been described so far regarding GRUBER BEYOND represents the state of the art, namely, how to obtain the necessary data for KEYSTONE based on the current production setup. Naturally, all of this has little more than theoretical value, as a brute-force approach could result in significantly long data reception times or even data processing times.

For this reason, and to facilitate integration with KEYSTONE, the implementation of a specific endpoint has been planned by GRUBER BEYOND.

This endpoint will allow optimized retrieval of all events related to a geographical location with a single request, filtering by date and using an approximation relative to the geographical point expressed in meters of radius.

The service that will be enriched with an endpoint is that of events, these are the specifications:

https://gw.gruber-logistics.com/events/v1/events/address/coordinate/[coordinates, in the format degrees decimal, by example for the Port of La Spezia could be 44.10277669891818,9.828622485156103]

Query Parameter: radius (in Meters, default 5000)
Query Parameter: fromDate (format as ISO8601[7])
Query Parameter: toDate (format as ISO8601)
Query Parameter: eventType (default undefined)

Both fromDate and toDate values, will filter on Planned or Effective Date.

The endpoint will return all events where the Address.Coordinates are in circle with centre in coordinate and radius the value of the "radius" field.

6. Cross data space authentication mechanisms for the API

6.1. EID / EIDAS founding concepts

6.1.1. EID principles

The electronic identification is a digital solution used to prove the identity of citizens or organizations. It is a method for verifying the identity of a person or entity through electronic means.

- eIDs allow access to services initially provided by government entities as well as private companies.
- eIDs serve as digital proofs of identity. They are issued by government authorities or agencies authorized by the government and contain specific information about the holder, such as name, date of birth, photo, tax code, etc.
- eIDs enable online authentication. When a user connects to a digital service, they can use their eID to securely demonstrate their identity.

During registration with an identity provider, the user provides a range of sensitive data, which is authenticated and verified by the identity provider. In return, the user gains the ability to authenticate with all service providers that have agreements with the identity provider, or vice versa, based on the conventions established by the identity provider.

In the context of electronic identification (eID), authentication occurs through the following steps:

1. **Identification:** The user presents their authentication data (such as username and password) to the system.
2. **Verification:** The system verifies the user's identity by comparing the provided data with registered information.
3. **Access:** If the identity is confirmed, the user gains access to the desired services or resources and the service provider obtains the access to the user's data it needs.

[7] Year, YYYY, four-digit, abbreviated to two-digit
Month, MM, 01 to 12
Day, D, day of the week, 1 to 7

EID ensures a higher level of trust compared to traditional credentials, allowing secure and reliable access to online services. This is why European Union member states have adopted eIDs as a tool to ensure secure access to digital services.

Moreover, it contributes to privacy protection and fraud prevention.

6.1.2. A typical example of use case involving the eID

The typical scenario is when a user wants to access a service offered by a service provider.

To access these services, the user must authenticate his/herself.

The precondition is that the service provider has partnered with an identity provider to enable authentication via eID.

Use case:

1. **User Visits Service Provider's Site:** The user visits the website through which the service provider has decided to expose its services and selects the desired service.
2. **Redirected to Login Page:** The user is redirected to the login page.
3. **Choosing eID Authentication:** The user chooses to access the service via eID, using one of the affiliated identity providers.
4. **Entering Credentials:** The user enters their credentials (e.g., username and password, or other authentication levels).
5. **Identity Verification by IdP:** The IdP verifies the user's identity and redirects them back to the originating platform with a positive authentication response.
6. **Authenticated Access:** The user is now authenticated and can access the chosen service.

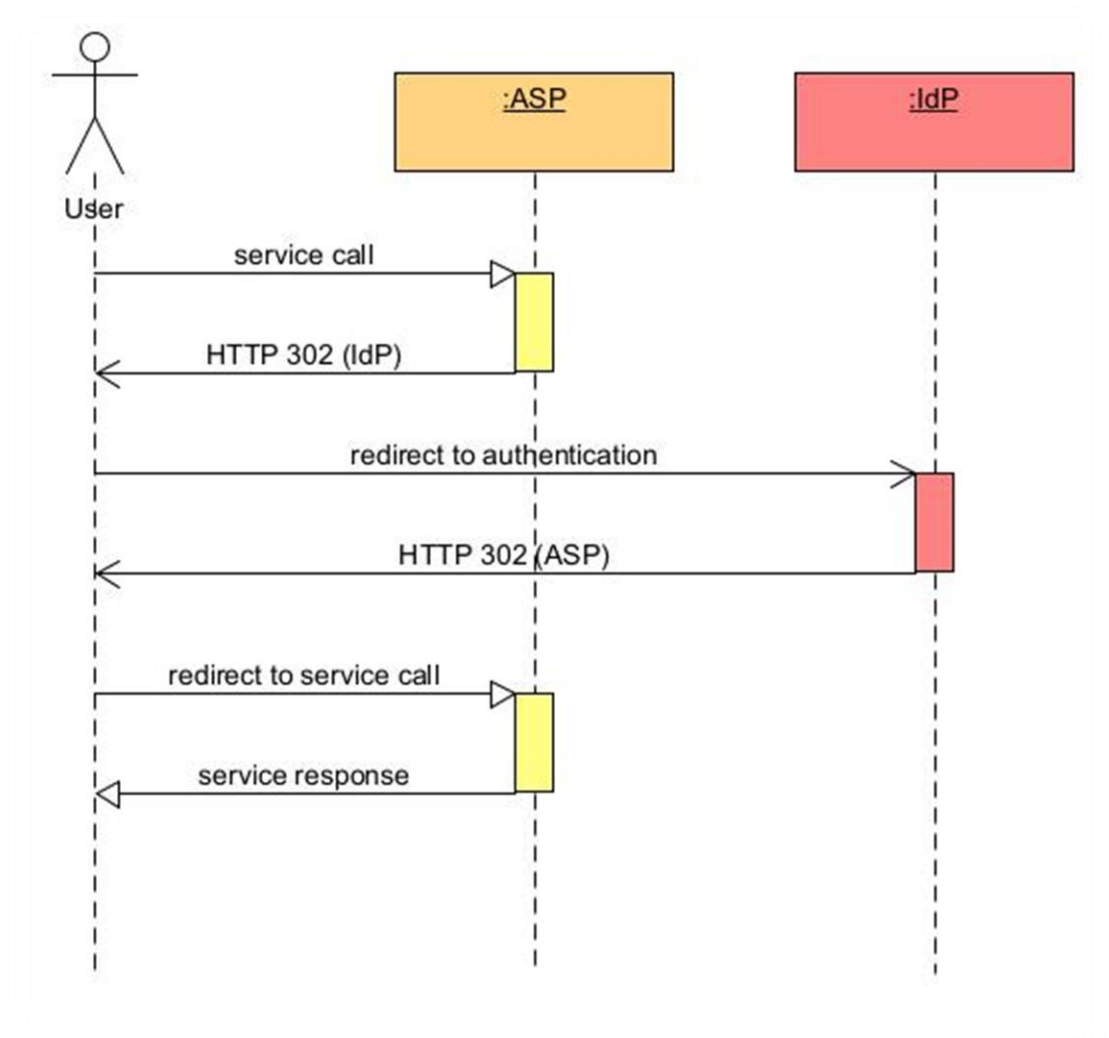

Figure 7 - A typical example of use case involving the eID sequence diagram

There are many benefits in the use of the eID. Among these, the main ones are that:

- The user does not need to create a new account on the service provider's platform, but he/she can use the same credentials to access multiple services from various service providers.
- The service providers can rely on a secure and reliable authentication system.

6.1.3. Use of the eID to implement the "Plug and play" policies

Directly from the example of the previous paragraph, it emerges how the use of an IdP can simplify "plug and play" design in various ways:

- **Centralized Authentication:** An IdP manages authentication and authorization for multiple services or applications. When a new service is added, it can simply connect to the existing IdP without having to implement authentication logic from scratch.
- **Credential Reuse:** Users can use the same credentials (username and password) to access multiple services. There's no need to create separate accounts for each application.
- **Centralized User Management:** The IdP allows centralized user management. Changes to permissions or user data automatically reflect across all connected services.

- **Scalability:** Adding new services is simpler because the IdP handles authentication. There's no need to modify each service separately.

6.1.4. EIDAS principles

The eIDAS Regulation (acronym for electronic IDentification, Authentication, and trust Services) is a legislative act of the European Union that plays a fundamental role in the field of electronic identification and trust services for electronic transactions.

Approved by EU Regulation No. 910/2014 on July 23, 2014, eIDAS has been in full effect since July 1, 2016, providing a common regulatory framework for secure electronic interactions among citizens, companies and public administrations within the European Union8.

Its primary objective is to enhance the security and effectiveness of electronic services and e-business transactions. It is based on key principles such as electronic identification and data privacy as well as trust services (such as electronic signatures, electronic time stamps, and certified delivery services).

6.1.4.1. All these key principles are implemented and have their natural outcome into the interoperability between the electronic identification systems of European Union member states. Digital identity

eIDAS establishes rules for electronic identification, allowing citizens and businesses to use recognized digital identification methods across all EU member states.

These methods include electronic identity cards, mobile apps, and other tools that enable secure online authentication.

Thanks to these rules, citizens can access public and private services without having to create new credentials for each country, significantly simplifying the user experience.

6.1.4.2. Data privacy protection

eIDAS places a strong emphasis on protecting personal data privacy. When citizens and businesses use electronic identification methods, their sensitive information are handled securely.

The regulation ensures that personal data are processed lawfully, transparently, and with respect for individuals' rights. It establishes guidelines for data controllers and processors to handle data responsibly.

6.1.4.3. Trust services

eIDAS introduces the concept of "trust services", which encompasses electronic signatures, electronic seals, time stamps, and other authentication tools.

These services contribute to ensuring the integrity and security of digital transactions. Specifically, regarding electronic signatures, eIDAS establishes norms and defines a standard for them.

[8] We can find the complete text of this regulation at the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.

These digital signatures are legally valid and recognized throughout the European Union. They allow authentication of digital documents, contracts, and other online transactions, playing a crucial role in ensuring the security and integrity of electronic communications.

6.1.4.4. Interoperability

eIDAS Regulation promotes interoperability among the electronic identification systems of EU member states. This means that citizens and businesses can use the same digital identity to access services in different EU countries.

This aspect of eIDAS is arguably the most crucial from a practical standpoint, given its potential impact on cross-border usage of digital identities across all EU member states.

It plays a vital role in ensuring smooth and secure management of digital identities and trust services within the European Union.

6.1.5. How the concept of interoperability is implemented in eIDAS

The implementation of the eIDAS node network is crucial to ensure the effectiveness of the principles described in the preceding paragraph. In fact, eIDAS nodes are technological infrastructures that enable the verification and validation of digital identities and electronic signatures across borders, using the identity providers from the individual's country of origin who is validating their identity.

6.1.5.1. EIDAS node net

Each member state that desires to use the eIDAS services, must confederate itself with the eIDAS node net and activate its own "eIDAS node". This node serves as a connection point among all the national electronic identification systems of the member states.

The goal is to enable full cross-border interoperability of digital identity systems and the circular use of eIDs among European Union member states.

6.1.5.2. Mutual recognition

eIDAS Regulation establishes mutual recognition for eIDs issued by the European Union countries, provided they meet the specified regulatory criteria and have been duly notified to the Commission.

It means that an eID issued in one Member State is valid and recognized in all others. For example, an Italian citizen, having of course an Italian eID, can use it to access online services in other European Union countries without having to create new credentials.

6.1.5.3. Technologically neutral framework

The interoperability requires the development of a technologically neutral framework. This means that no specific technical solution is favored for the implementation of eID.

Procedural and technical standards facilitate cooperation among the European Union member states, ensuring seamless exchange of electronic identification data and promoting a consistent digital ecosystem across the European Union.

In summary, interoperability in eIDAS creates an environment where digital identities can be used securely and reliably for cross-border transactions, simplifying user experiences and enhancing trust in online services.

6.2. EIDAS authentication guidelines

6.2.1. Overview

The eIDAS allows European citizens to use their national eIDs when accessing online services in another European country. For example, a citizen of a European Union member state can authenticate themselves using the eID issued by their home country even when accessing online services of any other European Union member state.

The implementation of eIDAS requires interoperability in multiple ways, meaning that each European Union member state's eID must be recognized and accepted uniformly across the entire European Union, ensuring a seamless user experience.

At the heart of the eIDAS solution lies the eIDAS protocol. This protocol acts as a bridge between national eID systems, allowing them to exchange information securely.

When a citizen from one member state accesses an online service in another member state, the eIDAS protocol translates the authentication request into a common format that all member states understand. This common format ensures that the authentication process remains consistent and reliable across borders.

The interoperability of the eIDs coming from Member States allows them to be accepted and recognized in other Member States. This breakthrough opens new possibilities and opportunities for citizens to seamlessly use services across borders.

6.2.2. A typical example of use case involving the eIDAS

The typical scenario is when a user wants to access an online service offered by a service provider of a state member in a European country different from the one of his/her origin.

To access to such a service, the user must authenticate his/herself.

The precondition is that the service provider has partnered with an identity provider to enable authentication via eID and its member state is federated with the eIDAS node net.

Use case:

1. **User Visits Service Provider's Site:** The user visits the website through which the service provider has decided to expose its services and selects the desired service.
2. **Redirected to Login Page:** The user is redirected to the login page.
3. **Choosing eIDAS Authentication:** The user chooses to access the service via eIDAS, due to the fact it has origin from a state different from the one of the ASP and the ASP has published the eIDAS login button on its site.
4. **Redirect to the IdP:** The user is redirected through the eIDAS node net to the eIDAS of the country of his/her origin. From this latter node, the user is yet redirected to the IdP of the same country with a request about a minimal set of attributes suitable in the eIDAS node net (e.g. date of birth, family name, name, eID code)

5. **Entering Credentials:** The user enters their credentials (e.g., username and password, or other authentication levels).
6. **Identity Verification by IdP:** The IdP of his/her country verifies the user's identity and redirects them back to the originating platform with a positive authentication response. Note that the user will have a further interaction with the eIDAS of his/her country for approving the attributes set that the Service Provider will use.
7. **Authenticated Access:** The user is now authenticated and can access the chosen service.

The connection between the service provider and the related eIDAS node could be implemented using an IdP of the same country as proxy to the related eIDAS node itself.

Instead, this use case presents a simplified version in which the ASP of a member state communicates directly with the related eIDAS node. This choice has been mainly made because the use of the IdP as proxy doesn't affect with a big change the interactions between the user and the eIDAS net of a different country.

The following sequence diagram schematizes a typical example in which a user from Spain interacts with the eIDAS node net when he/she tries to use a service exposed by an Italian application service provider.

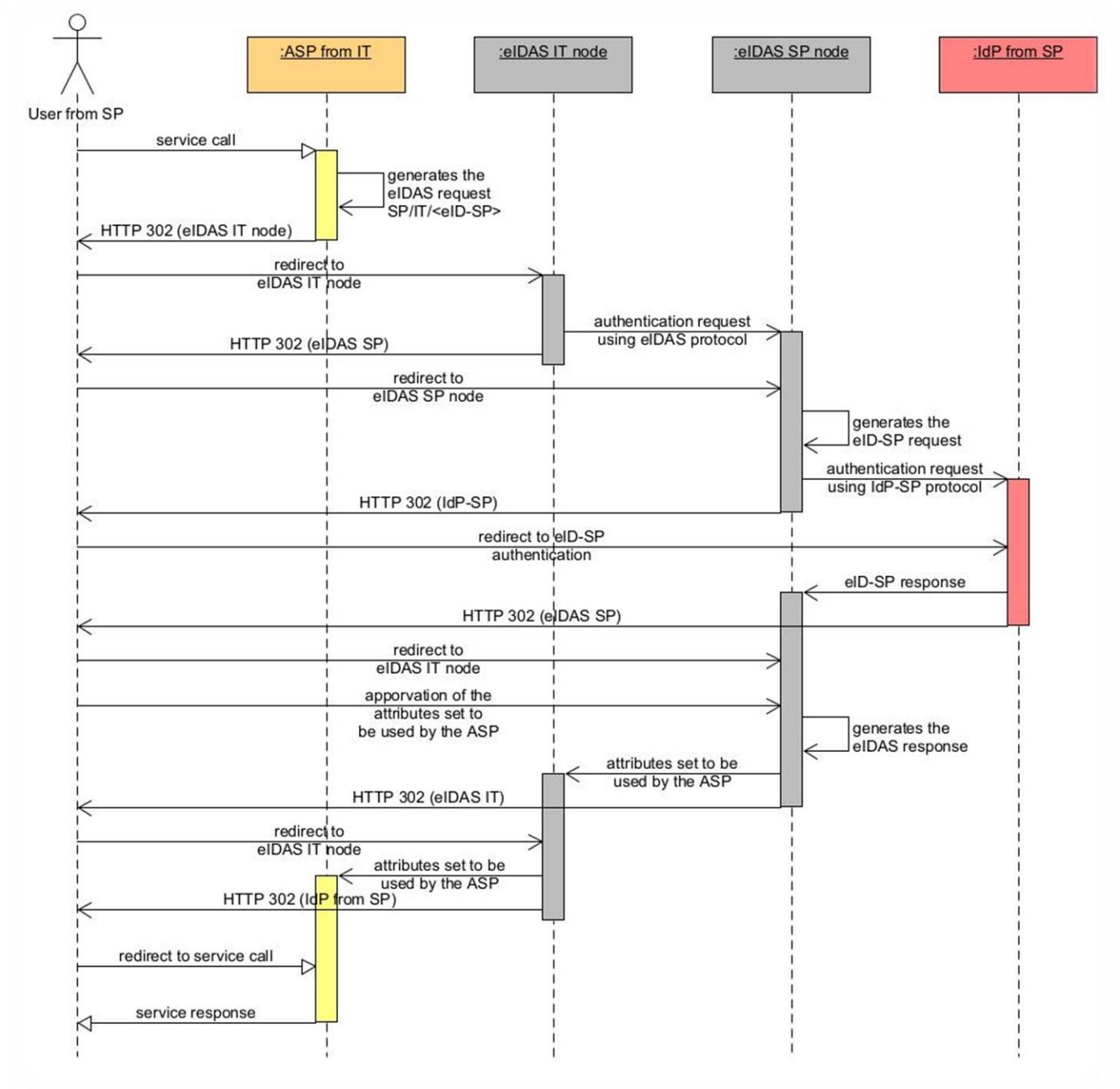

Figure 8 - A typical example of use case involving the eIDAS sequence diagram

6.2.3. Operative side

This paragraph illustrates the process through which public sector service providers can establish connections with existing eIDAS nodes.

These connections allow the provision of online services capable of identifying citizens and businesses from other European Union member states through a single authentication point.

This occurs without having to address all the issues inevitably related to user profiling and by adhering to plug-and-play principles.

Specifically, these services are designed for eGovernment portals, which serve as essential platforms for citizens in performing various administrative tasks. It is within this same context that KEYSTONE, as a project benefiting from public funding, fits.

The eIDAS Regulation (910/2014) and its implementing decisions establish the legal framework for the supervision of electronic identification.

According to the current regulations, all public entities that offer online services and authenticate users based on a national eID scheme must also recognize notified eID schemes from other EU member states.

This obligation to recognize a foreign eID scheme applies to all online services that require a 'substantial' or 'high' level of identity assurance, provided that the foreign eID scheme offers the same or higher level of identity assurance as the national one.

Compliance is optional for services with a 'low' level of assurance.

In this context, given the prototypical nature of what will be developed in this initial phase of KEYSTONE, it can be imagined that there may be no need for a substantial or high level of assurance.

However, with a view to avoiding the longstanding issue of user profiling, preparing for a higher level of assurance that may become advisable (if not necessary) in a subsequent step toward production, and especially aligning with a European standard for cross-border authentication, it would be plausible to integrate with the eIDAS node network from the outset (unless critical issues have emerged to date).

The mutual recognition of different national eIDs is made possible through the implementation of an eIDAS node by each member state. These nodes are configured to recognize all notified eID schemes in Europe.

Public sector service providers must connect to an eIDAS node to authenticate users from various member states and offer them services.

In our specific case, it is conceivable to connect to the Italian eIDAS node and use it to grant access to users from other member states. Access for Italian users would be guaranteed in this scenario by an Italian IdP, which would be invoked directly during authentication once SPID-based access is chosen.

KEYSTONE could provide services and leverage authentication through the eIDAS node network by directly integrating with the Italian node using the native eIDAS language. It would prepare the eIDAS request immediately upon receiving an authentication request from a user coming from another member state.

The steps to follow can be summarized as follows:

1. **Get in touch with the single point of contact:** see the table in Annex 1, with the e-mail addresses of the points of contact, one for each country federated with the eIDAS services. The information presented is the result of a collaborative effort between the European Commission and Member States to provide information that will be useful for organizations helping to set up or connect to the eIDAS Network.

2. **Prepare and give to the single point of contact a draft of the integration plan:** Involve the single point of contact will make sure to have a support when it will be needed.

3. **Develop a local test eIDAS node:** this permits to do all the integration tests between the ASP and the node before affecting the integration environment with tests at development time
4. **Ask the integration with the Italian eIDAS node:** In the specific case of the integration with the Italian eIDAS node, a test environment will be in the disposability of the development teams, before switching in production so to permit the end-to-end tests for all use cases.

Table 6 - eIDAS nodes status

Country	Status	Reuse of eID sample Implementation software
Austria	In production	Yes - partly
Belgium	In production	Yes
Bulgaria	In production	Yes
Croatia	In production	Yes
Cyprus	Under development	Yes
Czech Republic	In production	Yes
Denmark	In production	Own implementation
Estonia	In production	Yes
Finland	In production	Yes
France	N/A	Yes
Germany	In production	Own implementation
Greece	Under development	Yes
Hungary	Under development	Own implementation
Iceland	In production	Yes
Ireland	Under development	Yes
Italy	In production	Yes
Latvia	In production	Yes
Liechtenstein	Under development	Yes
Lithuania	In production	Yes

Luxembourg	In production	Yes
Malta	In production	Yes
Netherlands	In production	Yes
Norway	In production	Yes
Poland	In production	Yes
Portugal	In production	Yes
Romania	Planned	Yes
Slovakia	In production	Yes
Slovenia	In production	Yes
Spain	In production	Yes
Sweden	In production	Own implementation
United Kingdom	In production	Own implementation

6.2.4. Where to find what: online documentation

What is discussed in this document regarding eID and the eIDAS node network essentially constitutes a description of the principles on which these systems are based, as well as a reworking of fundamental concepts. In the end, some guidelines for addressing cross-border authentication in European Union member countries have been briefly outlined.

However, it should be emphasized that all of this primarily has a descriptive value. From an operational standpoint, it is necessary to refer to the official documentation available online and constantly updated.

Therefore, when transitioning from understanding the tools to the practical implementation of both the prototype of an eIDAS node for testing purposes and the actual integration of KEYSTONE with one of the eIDAS network nodes, consulting the documentation table online and drawing from the documentation itself is essential.

Similarly, there are examples and templates that cannot be overlooked when writing the code.

Table 7 - Online documentation

Document	Link	Description
Get Started with an ASP	https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/Get+Started+eID	Where to find an help to offer online (private and/or

		public) services capable of identifying citizens and businesses from other Member States.
Last stable version	https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eIDAS-Node+version+2.7.1	A collection of resources for the eIDAS-Node 2.7.1, released on 13 November 2023.
Regulation (EU) No 910/2014 n - 910/2	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
User Community for eID	https://ec.europa.eu/digital-building-blocks/sites/display/EIDCOMMUNITY/eID+User+Community	The eID User Community space enables stakeholders to exchange information on cross-border eID-related topics.
Git hub for the eIDAS Italian node	https://github.com/AgID/eidas-italian-node	The eIDAS Italian node's technical support uses GitHub issues as a tool for managing, sharing and resolving technical issues.

7. Consideration about the vehicles of high automation levels

7.1. CCAM / C-ITS overview

The progress in the mobility field can open new possibilities for future development and innovation in traffic management. In the future, vehicles and infrastructure, which are already digitalized, will become more connected and interactive. For this reason, the concept of Cooperative, Connected, and Automated Mobility (CCAM) will increase in importance in mobility projects (European Commission, Cooperative, connected and automated mobility (CCAM), 2021)

CCAM serves as an umbrella term for intelligent mobility. Cars of the future will be more connected to each other and to infrastructure and traffic signals, ultimately leading to autonomous driving. CCAM aims to achieve several important objectives in smart mobility (SWARCO, 2024):

- Enhance road safety
- Facilitate universal mobility access
- Minimize the environmental impact of vehicles
- Eliminate unnecessary trips (logistics)
- Decrease traffic congestion
- Encourage the use of micro-mobility solutions
- Expand urban green areas and bike lanes
- Support autonomous vehicles in public transport, logistics, and personal travel

Within the European context, CCAM implementation relies on four interconnected tools:

1. Large-scale deployment projects (C-Roads)
2. Common Vision (C-ITS Platform)
3. Legal certainty (ITS Directive Delegated Act)
4. Deployment Framework (EU C-ITS Strategy)

The C-ITS (Cooperative Intelligent Transport Systems) platform is designed as a cooperative framework that includes national authorities, C-ITS stakeholders, and the European Commission. Its purpose is to develop a shared vision for the interoperable deployment of C-ITS across the EU.

The platform provides policy recommendations, creates roadmaps, and establishes deployment strategies for C-ITS, addressing critical cross-cutting issues (European Commission, Cooperative, connected and automated mobility (CCAM), 2021).

The primary goal of C-ITS is to achieve a shared vision for the interoperable deployment of Cooperative Intelligent Transport Systems, contributing to cooperative, connected, and automated mobility (CCAM) within the European Union.

The EU's efforts focus on security, data protection, compliance assessment, and hybrid communication, all of which are crucial for the interoperability and development of C-ITS (European Commission, Cooperative, connected and automated mobility (CCAM), 2021).

C-Roads platforms are tools provided to authorities and road operators to harmonize the deployment activities of cooperative intelligent transport systems (C-ITS) across Europe. These platforms enhance transport efficiency, safety, and cleanliness.

The Directive 2010/40/EU accelerates ITS deployment across Europe, promoting interoperable services while allowing Member States flexibility in choosing systems. Priorities include traffic information, the eCall[9] emergency system, intelligent truck parking, and real-time data.

The new Directive (EU) 2023/2661 adapts to emerging mobility options, promoting the digital availability of crucial road and traffic data for safer driving on the TEN-T network (European Commission, ITS Directive and Action Plan, 2023).

The European strategy for Cooperative Intelligent Transport Systems (C-ITS) is welcomed for its collaborative effort between public and private sectors, aiming to rapidly develop interoperable C-ITS services across Europe. The strategy emphasizes the need for a clear legal framework under the ITS Directive to ensure service continuity, interoperability, and backward compatibility.

C-ITS strategy enhances fuel efficiency, reduces transport costs, and minimizes traffic's environmental impact. Recognizing the importance of digital technologies in road transport, the strategy advocates for infrastructure development to support C-ITS deployment.

Additionally, it highlights the EU's competitive advantage in C-ITS technology and calls for a coordinated and ambitious strategy to prevent fragmentation and expedite implementation. (European Parliament, 2018)

7.2. EU CCAM Projects

To develop its CCAM projects EU has founded several research projects in this section will be showed only the most related to KEYSTONE.

7.2.1. CCAM Partnership[10]

The goal of CCAM is increase road safety, reducing congestion, creating a more user-centred and inclusive mobility system with less environmental footprint.

The project will accelerate the innovation pace through collaborative research, testing and demonstration with the final goal to implement automated mobility (CCAM Partnership, 2021).

The elimination of barriers between European countries is another goal of CCAM Partnership to guarantee the acceptance and efficient rollout of automation technologies and services.

The project will be developed in 3 phases, parts of a roadmap called SRIA (strategic research and innovation agenda) (CCAM Partnership, 2021).

- The first step (2021-2024) is concerned on development of building blocks, this phase is dedicated to developing tools useful for CCAM implementation, some of technologies developed will help to

[9] eCall is a system used in vehicles across the EU which automatically makes a free 112 emergency call if your vehicle is involved in a serious road accident. You can also activate eCall manually by pushing a button.
Source: eCall 112-based emergency assistance from your vehicle - Your Europe (europa.eu)
[10] https://www.ccam.eu/what-is-ccam/ccam-partnership/

engage citizen and users, increase safety standards and improve vehicles and infrastructure technology levels.

- The second phase (2025-2027) will be focused on testing the readiness of technologies developed validating operational environments and, in certain cases, implementing these tools in large scale
- The third phase (2028-2030) will be focused on the implementation of large-scale demonstration projects all over Europe of technologies developed.

7.2.2. ROADART

The ROADART project[11] focuses on developing a dependable, automated system for truck-to-truck (T2T) and truck-to-infrastructure (T2I) communication. This safety-oriented T2TI/T2I communication platform can promptly alert professional drivers to immediate hazards and deliver essential information about upcoming road conditions (Roadart consortium, 2018).

The project has been focused on cutting greenhouse gas emission in transports and reduce transports cost trough fuel savings.

The aim of ROADART has been the platform, used in the pilots to demonstrate the reaching of the ROADART objectives.

The ROADART platform aims to enhance corporate Intelligent Transportation Systems (ITS) by investigating diversity and beam forming techniques.

Key objectives include:

1. **Channel Measurements:** Assessing mobile radio channel conditions for Truck-to-Truck (T2T) and Truck-to-Infrastructure (T2I) links.
2. **Radio Channel Characterization:** Developing statistical models for ROADART-specific multi-antenna channels.
3. **Antenna Techniques:** Investigating multiple antenna diversity, beamforming, and spatial modulation.
4. **Safety Enhancement:** Implementing Cooperative Adaptive Cruise Control on trucks to improve robustness in wireless communication.

Ultimately, ROADART seeks to optimize radio channels for safer, more efficient T2T/T2I services, considering practical challenges like installation on heavy-duty vehicles and special scenarios such as tunnels and platooning (Roadart consortium, 2018).

7.2.3. 5G Blueprint

5G Blueprint[12] objective is design and validate an IT architecture, new business models and innovative procedure in governance that can be supportive for uninterrupted cross-border teleoperated transport based on 5G connectivity (5G blueprint consortium, 5G Blueprint about, 2023).

The project will help teleoperated transport with 5g technology, bringing some improvement in logistic as example: reduction in waiting time, safer driving, reduction of labor shortage, automated mobility facilitator, increase liability, make safer data sharing.

[11] http://www.roadart.eu/
[12] https://www.5gblueprint.eu/about/#1647350734972-c8a70012-7120

The Project's objectives are linked to technology, business and governance. (5G blueprint consortium, 5G blueprint next generation connectivity for enhanced, safe, and effcient transport and logistics, 2023)

Technological Goals:

- **Design and implement a 5G Network for Connected and Automated Mobility Services** → Develop a 5G infrastructure to support seamless communication between vehicles.
- **Prototype Teleoperated System** → Create and deploy a functional prototype for remote-controlled operation of vehicles using 5G technology.
- **Enhance Safety and Value** → Implement features that improve safety and add value to the teleoperated transport system.
- **Validate End-to-End Teleoperated Transport Solution** → Test and validate the entire teleoperated transport solution in real-world scenarios, especially for cross-border operations using 5G technologies.

Business Goals:

- **Market Analysis for 5G Teleoperated Transport** → Conduct a thorough market analysis to understand the demand, potential customers, and competitive landscape for teleoperated transport services powered by 5G.
- **Discover Commercial Advantages** → Identify unique selling points and commercial benefits of teleoperated transport, emphasizing the advantages of 5G connectivity.
- **Promote Teleoperated Transport Adoption** → Develop strategies to promote the adoption of teleoperated transport solutions.
- **Highlight Importance in Connected and Automated Mobility** → Showcase how teleoperated transport, enabled by 5G, contributes to the broader field of connected and automated mobility.

Governance Goals:

- **Regulatory and Governance Understanding** → Investigate legal, regulatory, and governance aspects related to teleoperated transport systems.
- **Action Identification** → Identify actionable steps to address regulatory challenges and ensure compliance.

The projects final output will be a blueprint for a common European deployment of connected and Automated transport through teleoperation solutions in logistics sector (5G blueprint consortium, 2023).

7.2.4. MODI project

MODI[13] is a leading European cross-border initiative aimed at accelerating the deployment of Connected, Cooperative, and Automated Mobility (CCAM) solutions to significantly enhance logistics chains. MODI encompasses five use cases and involves a public-private partnership of 34 organizations from eight countries.

This initiative focuses on testing and validating CCAM solutions in real-world logistics operations.

The objectives of MODI are:

[13] https://modiproject.eu/modi-makes-progress-data-collection-and-first-trip-completed-on-rotterdam-oslo-ccam-corridor/

1. **Implement Innovative Technologies for Automated Mobility in Logistics:**
    - Explore cutting-edge technologies and solutions for connected cooperative, and automated mobility (CCAM) within logistics.
    - Focus on SAE L4 CCAM vehicles, which operate autonomously without human intervention.
    - Consider business-oriented integration to address logistical challenges effectively.
2. **Recommendations for Supporting Infrastructure and Regulations:**
    - Define specific adaptations needed for infrastructure (both physical and digital) to facilitate CCAM deployment.
    - Address vehicle regulations and standards to enable broader adoption of CCAM.
    - Streamline the introduction of CCAM vehicles by overcoming regulatory barriers.
3. **Business Models Involving CCAM Vehicles in Logistics:**
    - Showcase viable business models that incorporate CCAM vehicles.
    - Highlight how coordinated CCAM driving can lead to greater profits for logistics companies.
    - Emphasize the economic benefits of CCAM adoption.
4. **Technical and Socio-Economic Impact Assessments:**
    - Evaluate the technical feasibility and socio-economic impact of MODI L4 CCAM solutions.
    - Communicate findings in the context of best practices.
    - Consider real-world conditions and practical implications.

The project is ongoing, but the first pilot has shown some improvement and important insight about transports conditions: different motorway entrance procedures, speed limits, shoulder usage, and road marking vary across countries and about mobile network connectivity loss on borders (MODI Consortium, 2024).

7.3. CCAM in KEYSTONE

The preceding paragraphs have explained how CCAM can be developed within the European goods logistics market. Among the many projects funded at the European level, several are related to freight transport. Within the context of KEYSTONE, some of the innovations presented by this research can be applied to the cases of study.

The KEYSTONE app in can be improved with possibility to interface with CCAM Technologies giving the possibility to users to exchange data without any type of physical interaction. Information like drive licenses, ETA, tachograph data could be sent in automatic way with CCAM in future thanks technological development.

On first case study about a road police check in transport CCAM ca be used to check drive licenses, tachograph data, and documents regarding vehicles and goods with an interface that can be useful for the KEYSTONE purposes.

The examples brought by some EU Project like 5G blueprint and MODI project can improve and simplify the communications between vehicles and enforcement authorities. Thanks to 5G technologies information can be shared faster to road police without need to stop vehicles and loose times and resources for inspections to operators compliant with rules.

For the second KEYSTONE use case, the ideas bring by ROADART project can be helpful because a radio communication between vehicles and infrastructure (in KEYSTONE case the Port Gates) can be helpful for an exchange of information about port operations between road transports actors and port authorities.

KEYSTONE app can be an useful interface where PCS messages to operators can be sent. Some information like congestion in terminals, or request for more documentations can be sent directly to users through the KEYSTONE webapp.

Operators can answer to PCS request connecting their TMS to KEYSTONE and send directly all information via CCAM. Also, ETA can be sent to PCS using CCAM technologies and reducing difficulties for ports authorities to find information and improving ports efficiency. The implication of CCAM in KEYSTONE can be useful for the future development of the project. The European Union has prioritized Cooperated Connected Automated Mobility (CCAM) in its mobility strategy. Several projects developed in recent years have demonstrated that CCAM can increase efficiency and expedite operations in transportation. The most interesting projects mentioned earlier can inspire Keystone app developers to integrate some CCAM features, enhancing the competitiveness of the app. The results of projects such as 5G Blueprint, CCAM Partnership, ROADART, and MODI should be studied in subsequent phases to learn from their experiences, results, lessons, and developments and imagine future cooperation between projects.

8. Conclusions

8.1. Summary of findings

The digitalisation of transportation and logistics has brought both benefits and challenges, including the proliferation of various platforms that lack integration and interoperability. This leads to inefficiencies in data flow, communication problems, and increased operational costs.

KEYSTONE aims to address these issues by proposing intelligent solutions for data exchange among logistics stakeholders through a standardised API platform format.

This document provides an analysis of the Plug & Play principles implementation within the API reference model, focusing on theoretical aspects like user authentication and practical aspects like defining APIs for data retrieval.

Task 2.2 aims to analyse these aspects to bridge existing platforms with future developments in the logistics industry.

8.1.1. About API reference model

The API Reference Model is a critical component in the logistics sector, aiming to standardize methodologies for API development and usage. It serves as a blueprint for architecture, ensuring compatibility and efficient data exchange between logistics organizations and enforcement authorities. The model contributes to the KEYSTONE project's goal of unifying transport data across Europe by providing a structured framework for API standardization.

The development of the API Reference Model involves an extensive literature review to identify gaps in existing standards and practices and emphasizes clear definition and representation of APIs. The documentation produced acts as a guide for the API Standard implementation and interactions across systems.

The methodology for developing the API Reference Model includes requirements analysis, use case definition, architectural design, and deployment planning. It focuses on scalability, modularity, and adaptability, ensuring usability and maintainability.

The API Reference Model is linked to Task 2.2, which aims to enhance interconnectivity and data exchange in the logistics sector. It focuses on integrating various platforms and establishing robust authentication mechanisms, following the guidelines and standards set by the API Reference Model.

Overall, the model aims to improve operational efficiency, reduce errors, and facilitate better coordination among stakeholders, leading to a more integrated and efficient logistics ecosystem.

8.1.2. Interfacing different platforms and legals implications

The importance of interfacing different systems in computer science and software engineering is highlighted, with a focus on the challenges, particularly related to data manipulation and management.

In the case of KEYSTONE, interfacing with existing systems requires embracing the technology through which data is accessed.

The use cases studied in Deliverable 1.4 are analysed to define the data to be extracted from the platforms interfacing with KEYSTONE.

Use case and sequence diagrams are used to describe the interactions and scenarios. In one use case involving police controls over transport, the data shared via MoveHub is highlighted, along with the interactions with the KEYSTONE webapp. A textual use case story is provided to detail the step-by-step interactions when extracting and viewing data.

An alternative use case is also considered, involving a local database at KEYSTONE to maintain transportation data, with APIs implemented for data retrieval from TOSs. This alternative mixed client-server architecture provides flexibility in interfacing with different TOS requirements. A sequence diagram and use case story are presented to illustrate the interactions and data flow in this alternative scenario.

A second use case involving data integration between TMS and PCS is explored, focusing on interactions between the Port Authority, PCS, KEYSTONE, and TMS. The sequence diagram and use case story outline the interactions for retrieving and displaying transport data for port access scheduling. The importance of synchronous communication and on-demand data retrieval to reduce operational challenges is emphasized in both use cases.

Overall, the analysis of data extraction and management from various platforms in the context of KEYSTONE’s interfacing highlights the technical intricacies and challenges involved in ensuring seamless communication and data flow between heterogeneous systems. The use of diagrams and textual descriptions aids in understanding the interactions and scenarios in these complex data integration processes.

The legal implications surrounding the retrieval and use of information in transport operator compliance with EU regulations are crucial during roadside checks or company premise inspections.

Various regulations, such as those concerning driving and rest times, tachograph installation and use, working time rules, and roadworthiness, must be adhered to.

Enforcers can access a range of data types to verify compliance, including driver identification documents, vehicle registration, insurance documents, and journey forms.

Some information may be readily available, while other data may require validation or collection from authorities in the transport company's home country. Ensuring proper documentation and adherence to regulations is vital to avoid legal consequences and ensure safe and compliant transport operations.

The document provides details on two platforms, EDIGES and GRUBER BEYOND, which are candidates for implementing two pilot projects related to intermodal transport and transport data communication between TMS and PCS.

EDIGES is the TOS platform for the Novara intermodal centre, focusing on train arrival, truck loading, and transmission of ITU pickup data to the KEYSTONE platform via APIs. The document outlines the data structure and elements related to ITU pickup from EDIGES, such as PickupGateout, Supplier, Orderer, ItuDetails, and DeliveryDistribution.

On the other hand, GRUBER BEYOND is GRUBER's TMS platform, offering REST services organized as microservices for accessing data related to orders and estimated time of arrival (ETA). The document describes the Orders management system and Events management system in GRUBER BEYOND, providing examples of API calls and response data for retrieving order details and trip events.

8.1.3. eID/eIDAS: principles and guidelines

The content discusses the principles and implementation of electronic identification (eID) and the eIDAS node network. It explains how eIDs work, the benefits of using them, and their role in authentication for online services.

The eIDAS Regulation is highlighted as a key legislative act of the EU governing electronic identification and trust services.

The concept of interoperability among EU member states' electronic identification systems is emphasized, with the eIDAS node network serving as the infrastructure for cross-border authentication.

The document provides guidelines on how public sector service providers can connect to existing eIDAS nodes and implement eIDAS authentication. It also includes information on key resources and documentation available online for further reference and implementation.

8.1.4. CCAM: state of art and integration in KEYSTONE

CCAM, which stands for Cooperative, Connected, and Automated Mobility, is a key concept in the future of intelligent mobility.

This umbrella term encompasses various objectives aimed at enhancing road safety, increasing mobility access, reducing environmental impact, minimizing traffic congestion, and promoting the use of micro-mobility solutions.

Within the European context, CCAM implementation relies on tools such as large-scale deployment projects (C-Roads), the Common Vision (C-ITS Platform), legal certainty (ITS Directive Delegated Act), and the Deployment Framework (EU C-ITS Strategy).

The C-ITS platform is designed to promote the interoperable deployment of Cooperative Intelligent Transport Systems across the EU, bringing together national authorities, stakeholders, and the European Commission. It focuses on policy recommendations, roadmaps, and deployment strategies critical for the development of CCAM.

The primary goal of C-ITS is to achieve interoperable deployment of intelligent transport systems, contributing to cooperative, connected, and automated mobility within the EU.

The EU's efforts in CCAM also focus on security, data protection, compliance assessment, and hybrid communication to ensure interoperability and development.

Projects such as C-Roads platforms aim to harmonize the deployment activities of cooperative intelligent transport systems across Europe, enhancing transport efficiency and safety.

Directives such as 2010/40/EU and 2023/2661 promote ITS deployment and adapt to emerging mobility options, ensuring safer driving and efficient transport operations.

Additionally, EU-funded projects like CCAM Partnership, ROADART, 5G Blueprint, and MODI are at the forefront of developing and testing innovative CCAM solutions.

These projects focus on improving road safety, reducing congestion, cutting greenhouse gas emissions, and enhancing logistics operations through automation and connectivity.

They aim to develop technologies, business models, and governance procedures to support uninterrupted cross-border teleoperated transport using 5G technology.

Overall, CCAM is set to revolutionize the way we approach mobility and transportation, with a strong focus on safety, efficiency, sustainability, and innovation.

Projects like those in the KEYSTONE initiative are exploring how CCAM technologies can be integrated into various case studies, such as improving communication between vehicles and enforcement authorities and enhancing port operations through radio communication.

CCAM has the potential to transform the future of transportation and logistics, making it safer, more efficient, and more sustainable.

References

5G blueprint consortium. (2023). *5G Blueprint about*. Tratto da 5G Blueprint: https://www.5gblueprint.eu/about/#1647350734972-c8a70012-7120

5G blueprint consortium. (2023). *5G blueprint next generation connectivity for enhanced, safe, and effcient transport and logistics*. Tratto da 5G Blueprint: https://www.5gblueprint.eu/wp-content/uploads/sites/62/2023/11/5GBPoverview_4pA4_2023-update-v3-final-event_2_WEB.pdf

CCAM Partnership. (2021). *WHAT IS CCAM ?* Tratto da CCAM: https://www.ccam.eu/what-is-ccam/ccam-partnership/

Doe, J. (2003). *Lorem Ipsum.* TX: DC Books.

European Commission. (2021, November 17). *Cooperative, connected and automated mobility (CCAM)*. Tratto da transport.ec.europa: https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/cooperative-connected-and-automated-mobility-ccam_en

European Commission. (2023). *ITS Directive and Action Plan*. Tratto da transport.ec.europa.eu: https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/its-directive-and-action-plan_en

European Parliament. (2018, March 13). *europarl.europa.eu*. Tratto da European Parliament resolution of 13 March 2018 on a European strategy on Cooperative Intelligent Transport Systems: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0063_EN.html

MODI Consortium. (2024). *MODI Makes Progress*. Tratto da MODI: https://modiproject.eu/modi-makes-progress-data-collection-and-first-trip-completed-on-rotterdam-oslo-ccam-corridor/

Roadart consortium. (2018). *Roadart Project*. Tratto da Roadart: http://www.roadart.eu/

SWARCO. (2024). *CCAM: Cooperative, connected & automated mobility*. Tratto da SWARCO: https://www.swarco.com/mobility-future/connected-mobility/ccam

Annex 1

Table 8 - Single points of contact

Single point of contact	Single point of contact	e-mail
Austria	Austrian Federal Ministry of Finance Dept. V/A/2 (Digitalisation and eGovernment – International and Legal Affairs; eGovernment Strategy)	post.szrb@bmf.gv.at
Belgium	Federal Public Service Policy and Support (BOSA) Directorate General Digital Transformation Boulevard Simon Bolivar 30 WTC III 1000 Bruxelles Belgium	eidas@bosa.fgov.be
Bulgaria	Ministry of e-Government, Electronic Identification Directorate 6 "Gen. Yosif V. Gurko" Str. 1000 Sofia Bulgaria	Mail@egov.government.bg
Croatia	Ministry of Economy, Entrepreneurship and Crafts Ulica grada Vukovara 78 10 000 Zagreb Croatia	hrvoje.perinic@rdd.hr Maja.Radisic-Zuvanic@mingor.hr ured@rdd.hr e-poslovanje@mingor.hr
Cyprus	Department of Electronic Communications, Ministry of Transport, Communications and Works 286 Strovolos Avenue, Strovolos, Nicosia, Cyprus Postal Address: PO Box 24647, 1302 Nicosia, Cyprus	
Czech Republic	Ministry of the Interior Nad Štolou 3, 170 00, Prague 7 Czech Republic	eidas@mvcr.cz

Denmark	Agency for Digital Government, Ministry of Digital Government and Gender Equality Landgreven 4 Postboks 2193 1017 København K	digst@digst.dk eidas@digst.dk
Estonia	Information System Authority Pärnu maantee 139a, Tallinn 15169 Estonia	eidas@lists.ria.ee Phone: +372 663 0200 Fax: +372 663 0201
Finland	Finnish Transport and Communications Agency, Traficom TRAFICOM PO Box 313 FI00059 Helsinki Finland	eidas@traficom.fi eidas-support@dvv.fi
France	Direction interministérielle du numérique (DINUM) 20 avenue de Ségur 75007 Paris France	eidas@franceconnect.gouv.fr
Germany	Federal Ministry of the Interior, Building and Community Alt-Moabit 140 10557 Berlin Germany	eID@bmi.bund.de
Greece	Hellenic Ministry of Digital Governance Directorate General for Digital Governance Directorate for Electronic Governance Department of Security Services Fragoudi 11 & Alexandrou Pandou, 17671 Kallithea, Athens Greece	eIDAS-SPOC@mindigital.gr
Hungary	Ministry of Interior József Attila utca 2-4 1051 Budapest Hungary	

Ireland	Office for the Government Chief Information Officer, Department of Public Expenditure and Reform 3A Mayor Street Upper, Spencer Dock Dublin 1, D01 PF72 Ireland	eIDAS@per.gov.ie
Italy	Agenzia per l'Italia Digitale (AGID) Viale Liszt 21 0144 Rome Italy	eidas-spid@agid.gov.it
Latvia	Supervisory Committee of Digital Security K. Valdemāra iela 10/12 Rīga, LV-1473 Latvia	eiuk@mod.gov.lv
Lithuania	The Ministry of the Interior (Strategic Decisions Support Group; Information Technology & Communication Department) Šventaragio str. 2, LT-01510, Vilnius	eIDAS@eIDAS.gov.lt
Luxembourg	Centre des technologies de l'information de l'Etat 1, rue Mercier B.P. 1111 L - 2144 - Luxembourg Luxembourg	eidas@ctie.etat.lu
Malta	Malta Information Technology Agency (MITA) Gattard House National Road Blata l-Bajda HMR 9010 Malta	eidas.mita@gov.mt
Netherlands	Ministry of the Interior and Kingdom Relations (Directorate Information Society and Government) Turfmarkt 147	eidas@minbzk.nl

	2511 DP The Hague The Netherlands	
Poland	Ministry of Digital Affairs ul. Królewska 27 00-060 Warsaw Poland	
Portugal	Agency for the Administrative Modernization (AMA) Rua Abranches Ferrão n.º 10, 3º G 1600 - 001 Lisbon Portugal	info.cidadao@ama.pt
Romania	Ministry of Communications and Information Society (Agency for Digital Agenda in Romania) Bulevardul Libertăţii nr. 14, Sector 5 Cod 050706, Bucureşti România	
Slovakia	Government Office of the Slovak Republic - National Agency for Network and Electronic Services (NASES) Kollárova 8 917 02 Trnava Slovak Republic	eidas@nases.gov.sk
Slovenia	Ministry of Digital Transformation Davčna ulica 1 SI-1000 Ljubljana Republic of Slovenia	si-trust@gov.si
Spain	Ministry of Economy and Business c/Joan Maragall 41 28020 Madrid Spain	lfe@mineco.es sgssi@mineco.es eidas@correo.gob.es
Sweden	Agency for Digital Goverment Box 14 SE-851 02 Sundsvall Sweden	e-legitimation@digg.se +46 771 11 44 00 (+46 72 468 54 09 for acute security incidents at non-office time)

United Kingdom	Government Digital Service The White Chapel Building 10 Whitechapel High St London E1 8QS UNITED KINGDOM	eidas-support@digital.cabinet-office.gov.uk
Iceland	Post and Telecom Administration Sudurlandsbraut 4 108 Reykjavik Iceland	
Liechtenstein	Ministry of General Government Affairs Peter-Kaiser-Platz 1 P.O. Box 684 9490 Vaduz Liechtenstein	eidas@llv.li
Norway	EEA Norwegian Digitalisation Agency (Digdir) Postboks 1382 Vika N-0114 OSLO Norway	postmottak@digdir.no SPOC Contact: Tor Alvik Tor.Alvik@digdir.no +47 41586754

KEYSTONE

Let’s stay in touch

Follow us online & subscribe to our newsletter!

www.keystone-project.com

KEYSTONE EU

@KEYSTONE_EU