iKoPA Integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge

Deliverable D1v2
Requirements Analysis and System Architecture

Version number	2.0
Dissemination level	Public
Project Coordination	htw saar
Due date	2018-11-30
Date of preparation	2018-12-15

Funded by the

Federal Ministry
of Education
and Research

Project Coordination
Prof. Dr. Horst Wieker
Head of ITS Research Group (FGVT) at the
htw saar – Hochschule für Technik und Wirtschaft des Saarlandes,
University of Applied Sciences
Department of Telecommunications
Campus Alt-Saarbrücken
Goebenstr. 40
D-66117 Saarbrücken
Germany

Phone +49 681 5867 195
Fax +49 681 5867 122
E-mail wieker@htwsaar.de

Legal Disclaimer:

The information in this document is provided 'as is', and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Authors:

Daniel Becker – DCAITI

Bud Bruegger – ULD

Manuel Fünfrocken – htw saar

Gundula Gagzow – ULD

Dimitrij Gashimov – htw saar

Mathias Küfner – bmt

Richard Petri – SIT

Delian Rachinski – SWARCO

Rasmus Robrahn – ULD

Andreas Schmid – SWARCO

Matthias Schmidt – FOKUS

Björn Schünemann – DCAITI

Mats Sturm – NXP

Jonas Vogt – htw saar

Eckhard Walters - NXP

Niclas Wolniak – htw saar

Harald Zwingelberg – ULD

Revision and History chart

Version	Date	Description
0.1	2016-08-10	**Initial version**
0.2	2016-10-31	**Studies included**
0.3	2016-12-16	**Requirements included**
0.4	2017-01-06	**Use Cases included**
0.5	2017-01-31	**Architecture included**
0.6	2017-02-13	**Review version**
0.7	2017-02-24	**Review included**
1.0	2017-02-28	**Final version v1**
1.1	2018-03-28	**System requirements structure added**
1.2	2018-10-23	**Data protection clarifications in system description, system architecture extended, visionary scenario extended, identity provider integrated, conclusion added, DAB GeoCast added**
1.3	2018-11-27	**Second review included**
2.0	2018-12-14	**Final version v2**

Table of Content

Figures

Tables

Executive Summary

Automated driving functions are a necessity for efficient electric driving. Missing and non-transparent communication structures and inconsistent information quality exacerbate a vehicle-manufacturer independent integration of automated driving. The integrated communication platform for automated electric vehicles (iKoPA) combines technologies in an innovative way. This includes the integration of multiple communication technologies (e.g. V2X, cellular, DAB, RFID) and of driver-assistant system architectures for high and full-automated driving functions. The electronic systems of the electric vehicles, traffic lights, charging stations and many other traffic related systems can communicate via the extended Car2X Systems Network. This connection is the foundation for new and optimized (fully) automated driving, parking and charging services.

iKoPA develops the basic design for a system, which serves as an open integrated platform for future intelligent transportation services. These services for automated driving will be connected in an innovative, future-proof and comprehensive way. The introduction of electric mobility services will be accelerated through this additional benefits. The system is basis for the vision of automated and electric powered future mobility concepts.

The deliverable D1 presents the architecture for that system and the way in which this architecture was derived from the visionary scenario, requirements and external factors that enframe the system.

1 MOTIVATION

The iKoPA project aims at designing and verifying a system architecture for flexible interaction between different Service Providers and communications network operators and remote nodes in a decentralized, scalable structure.

The network will extend the exiting architecture developed in the research project CONVERGE. It includes an open architecture for communication-, services-, and organization. Through services access points, Service Providers like electric mobility providers or vehicle manufacturers can be integrated into the open and secure network. The goal is a decentralized and dynamic coupling of all systems and stakeholders in a secure, distributed, privacy-friendly, scalable, flexible, and hybrid-communicating network.

The architecture of iKoPA will be specified in two steps. Each of which is resulting in an own deliverable referred to as D1v1 and D1v2. This document is the second and final one of this series. In the second version, the results and experiences form the demonstration implementation and real world verification are also included.

In a first step, an overall architecture is drafted and documented. The specification level is divided in two layers a high-level and a low-level architecture. The high-level architecture describes the overall architecture and the connection between the different planes and components. The low-level architecture focuses on the details. It describes components and interfaces more precise, and presents important communication concepts.

These major functional components are on one side take from the CONVERGE architecture and on the other side derived from an analysis of all functions necessary to support the use cases and requirements defined. Implementation details like hardware separation, interface bit level specifications and internal interfaces will not be specified.

The reason and motivation for this deliverable D1 are to achieve the following:

- To take the architecture proposal of [1] and generate a more detailed and elaborated view on the overall architecture
- To split the overall architecture in reasonable structural blocks
- To identify interfaces which are necessary between the different components and to specify those interfaces
- To further detail and elaborate the major architectural challenges

The document is structured as follows:

- **Chapter 2** describes the methodology and way how the architecture was created and which factors were considered.
- **Chapter 3** provides an overview about the goals that iKoPA tries to archive, the visionary scenario of iKoPA and the use cases derived from the goals and scenarios.
- **Chapter 4** gives an overview about state-of-the-art technologies important for the architecture and describes other technological determining factors.

- **Chapter 5** summarizes the requirements that were derived from the work in the chapters 2, 3 and 4.
- **Chapter 6** specified the architecture itself. A high-level architecture, a description of the functional blocks and interfaces, and a low-level description of important blocks and concepts are given.
- **Chapter 7** concludes the document. A short description about the legal aspects of data protection deliberations are presented and a résumé about the process and the architecture is drawn.

2 DESCRIPTION OF THE ARCHITECTURE PROCESS

How did the architecture develop? What steps were taken? In addition, which were the goals to be fulfilled? These are the questions chapter two answers. First, the process goals are described and in the second step, the process itself is explained.

2.1 Goals of the process

The Deliverable D1 is the result of the work package 1 (WP1) in iKoPA. It presents the requirements, the technical environment and the system architecture. Whereby, the work package 1 channels the requirements on the system and the technical status quo in a formal process and describes the use cases. Together with work package 5, WP1 defines means of verification for those requirements. With the requirements, the technical system is specified and described formally.

2.2 Description

In WP1, a formal way for the development of the architecture was specified. This way is described in Figure 1.

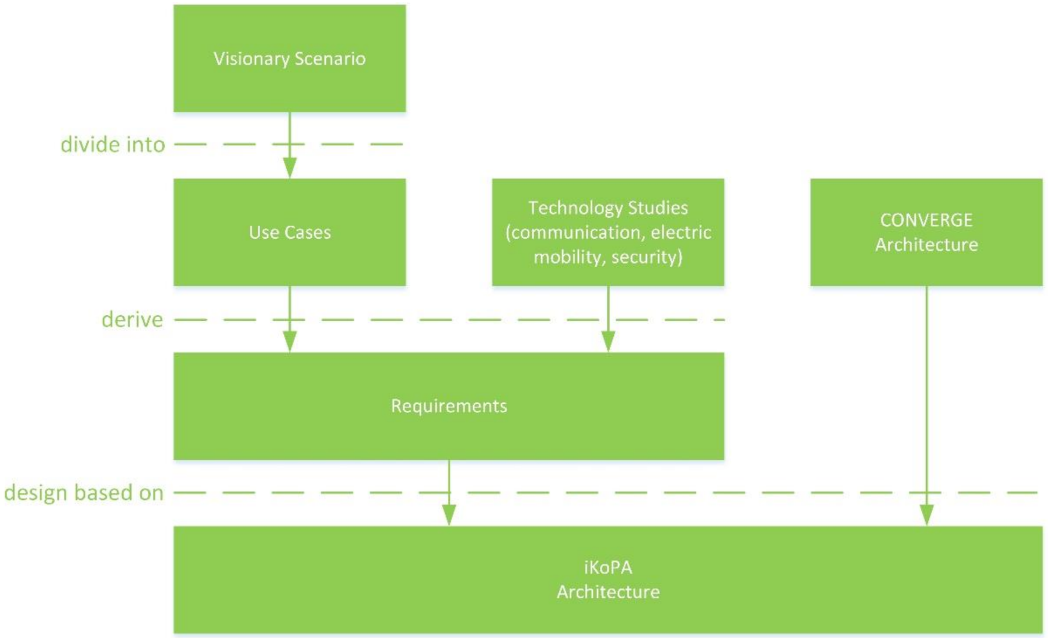


Figure 1: Architecture design process

During the application phase of the project a scenario about the usage of the technologies and the proposed innovations was developed. As one of the first tasks in the project, based on this initial description a visionary scenario was created. It describes the day of a young woman in Berlin and her interaction with automated vehicles, traffic infrastructure and traffic related communication technologies – with all communication secured and privacy friendly solutions.

The visionary scenario was then divided into segments. Those segments again were formally described as uses cases. At the same time, an overview about state of the art technologies was created. The studies comprised communication technologies, security technologies and the status of electric mobility. The last one especially regarding the interconnection of electric vehicles and the charging infrastructure. In addition, the baseline architecture planned to be used in iKoPA from the CONVERGE project was analyzed and the relevant parts described.

From the studies and use cases, the requirements were derived. The requirements are divided in different categories. The categories are privacy, security and system. Requirements were also classified as technical or organizational and as relevant for the architecture or the implementation.

In the final step, based on the requirements and the CONVERGE architecture, the iKoPA architecture was specified. The specification was divided into two layers. The high-level architecture presents an overview about the architecture the components and the interfaces. In the low-level architecture a more depth description of important components and overall concepts are described.

3 RESULTS OF THE ARCHITECTURE PROCESS

Following the architectural process, first the project goals and the visionary scenario are described. The scenario is then divided into individual use cases. The uses cases are the foundation for the following steps.

3.1 iKoPA Goals

To specify the project outcomes, iKoPA defines five project goals. They represent the technical and organizational guidelines during the project.

Linkage of automated driving functions with infrastructure-based data to improve electric mobility

> Until now, up to a few exceptions, automated navigation functions have been self-sufficient. The vehicles use only integrated data sources, in particular sensors and map data, for the driving function. The integration of external information into the sequence of an automated function, especially in the context of electric mobility, represents a significant research task since the possible increased driving efficiency has a direct effect on achievable rang of the car. By integrating the data received via communication into the timetable, a more efficient "intelligent" approach can be achieved in all automation stages. In particular, the external data must be linked to vehicle-driven perception by means of an intelligent fusion. This fusion differs from existing approaches to sensor fusion due to the unique properties of communication as a sensor.

Secure communication on a hardware basis, considering data protection aspects

> A hardware-based, uniform, scalable IT security platform is developed, which can be integrated into all relevant iKoPA components and offers both measures to ensure system integrity (i.e. protection against tampering of the systems themselves) as well as to secure communication. On this platform, all communication paths, e.g. cellular radio, DAB+ (Digital Audio Broadcast) and V2X (Vehicle-2-X communication). An integral part of all paths is hardware-based encryption, authentication and pseudonymization to ensure security and privacy. The project aims to provide a data protection-enhancing solution that not only complies with the legal requirements of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)[1] and the European General data protection Regulation (GDPR)[2], but also maintains the privacy interests of the vehicle drivers well beyond the minimum requirements. Data-minimization procedures and techniques will be implemented. It is to be determined which data is necessary in

[1] German version https://www.gesetze-im-internet.de/bdsg_1990/ and English translation https://www.gesetze-im-internet.de/englisch_bdsg/index.html

[2] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

order to operate the developed technology, so that only the latter have to be collected in compliance with the principle of necessity.

Converged unified communication across multiple communication systems

Uniform communication on very divergent communication technologies, a uniform architecture and data management will allow to decouple applications from the transmission path and to combine the individual advantages of the divergent technologies of cellular radio, DAB and V2X Until now, applications have to be adapted to the communication system. Therefore, in the future, developers of applications can concentrate on their actual task and only have to stipulate the requirements regarding communication. The communication system takes care of the transfer. This allows the specific advantages of the different systems to be combined and the correspondingly scarce resource radio bandwidth to be used more efficiently.

Multimodal interaction of the mobile nodes cellphone and vehicle

Both, equipped vehicles and commercial smartphones are supported as end nodes. This makes access to traffic-relevant information available to a large amount of user. Previous solutions that connect vehicles to back-end services in the cloud or offer local access to smartphones are generally based on proprietary interfaces with limited functionality. The main objectives is the linking of the vehicles with remote back-end systems via standardized interfaces and protocols, taking into account established (cellular radio, Wi-Fi) and novel (DAB TPEG (Transport Protocol Experts Group), ETSI ITS-G5) wireless communication technologies.

Integration of traffic and charging infrastructure

The aim of the integration is to provide a network of charging infrastructure, electric vehicles and infrastructure for traffic control in a manner appropriate to the needs of the market, in order to achieve appropriate support for automatic driving functions for electric driving. The integration provides the basis for applications such as optimized range planning, optimization of energy consumption, timely and locally precise automatic reservation of charging stations and charging management. The identification of gaps in the area of the communication protocols of the charging infrastructure and the chip-based V2X communication is to be achieved from the comparison of the demand with the current state of the art. The necessary interlocking of the communication techniques for the implementation of the application cases is developed both in general and defined specifically on the basis of the state of the art as well as a realistic economic implementation.

3.2 Visionary Scenario

The visionary scenario describes the ideas and possibilities that can be achieved with the architecture and technologies developed in iKoPA.

Berlin, the communicative city

In the beautiful city of Berlin, young Helena H. is working and living. She is a technical enthusiast and just bought her first semi-automated electric Vehicle. This vehicle is also equipped with state-of-the-art communication technologies.

On a sunny Tuesday morning during her holiday, Helena H. drives from her home in Grunewald to the nearby nursery of her confidence in Grunewald. Unfortunately, not all plants are available. Due to a recommendation, she wants to try a new nursery in Berlin Mitte. To find a parking lot where she also will be able to charge her vehicle Helena H. uses the app "Berlin smart parking – Your place to park". As a new feature, the app now allows the search for an automated parking lot. She wants to try this service today. As a benefit, the usage of the service is free of charge for people living in Berlin and the app can be used pseudonymously. The information about the car park is transmitted via DAB/TPEG to her vehicle. Now she books a suitable parking lot in the car park "ePark" next to the nursery via her mobile phones cellular connection. Following the booking the destination information will be automatically transferred (BYOD - Bring your own device) to the navigation system in her vehicle and used by the BerlinEnergyWay app. She uses the energy optimized routing function of the app "Berlin Energy Way – Good roads, good flow" on her way to Berlin Mitte. This app also utilizes the speed advisories transmitted via V2X for an energy and emission optimized trip. The local traffic lights also consider this information. This leads to smooth traffic flow and Helena H. arriving relaxed at the destination.

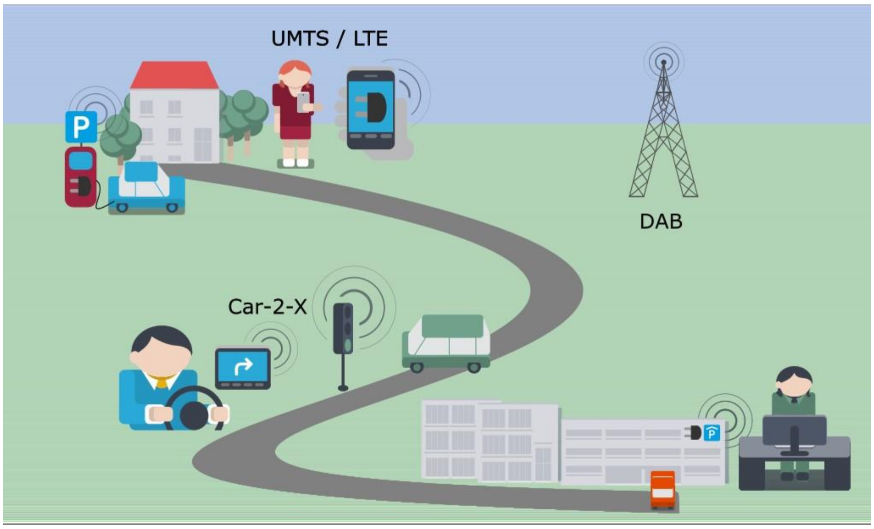


Figure 2: iKoPA scenario (part)

At the automated car park, Helena H. can lean back. After the gateway, the vehicle takes control. At first, it gets the necessary information via V2X communication about the location of the parking lot. With that information, the vehicle safely drives to the booked parking lot with charging capacity. During the drive, the vehicle is tracked through latest in camera technology. This position information is transmitted back to the vehicle for the automated drive. Arriving at the parking lot, the vehicle is authorized through its pseudonymous RFID tag and the parking lot barrier is lifted, so that the vehicle can drive on the spot. Helena H. can leave the car and go to the nursery. During her stay, the vehicle is charged at the charging station.

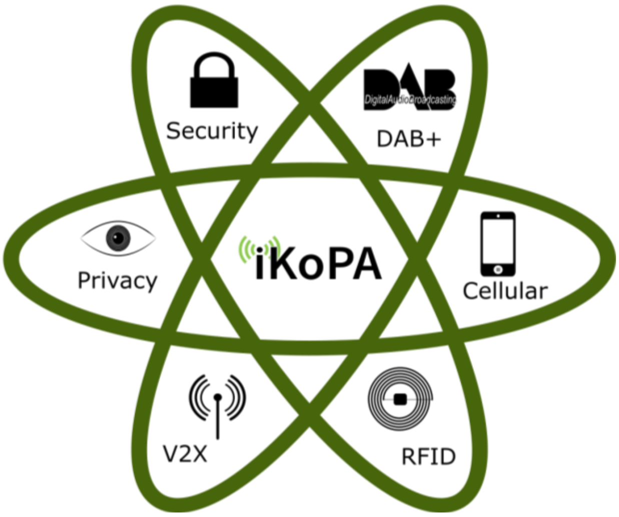


Figure 3: iKoPA communication technologies

With the help of modern communication technology (V2X, RFID, DAB+, …) the charging station can optimize the charging and additionally provide further information (e.g. updates) to the vehicle. When the vehicle is fully charged, it drives autonomously to an empty parking lot clearing the charging spot for other customers. After Helena H. has finished her shopping trip, she orders the vehicle via a smartphone app to come and pick her up in front of the car park. She puts her purchases into the vehicle and drives home.

Figure 4: Helena H. Driving

On the next day, Helena H. wants to go a hiking trip in the near Brandenburg. The first stage of the Oderlandweg from Wriezen to Falkenberg/Mark is her goal today. The way starts in one of the beautiful rural areas of Brandenburg. Because of the landscape and the low population density of the area the connection to information and warning services is limited, but Helena H. booked the full communication service and so her system always utilizes the communication system available (cellular or DAB). In this way, Helena has a high likelihood to stay informed and safe with up-to-date information and does not need to worry about unpleasant surprises on the road. The hiking path is another story …

3.3 Use Cases

The visionary scenario was the starting point for the development of the iKoPA use cases. First, it was split in individual technical parts. Afterwards, these parts were then formalized into use cases. Each use case has a description, the necessary steps and the related actors for the use case. In this chapter, first the identified actors are described followed by the use cases themselves.

3.3.1 The primary actors

In iKoPA, human and technical actors were identified in the visionary scenario and in the use cases. The following figure shows those identified actors. Thereby a stick man represents human actors and a rectangular represents a technical actors.

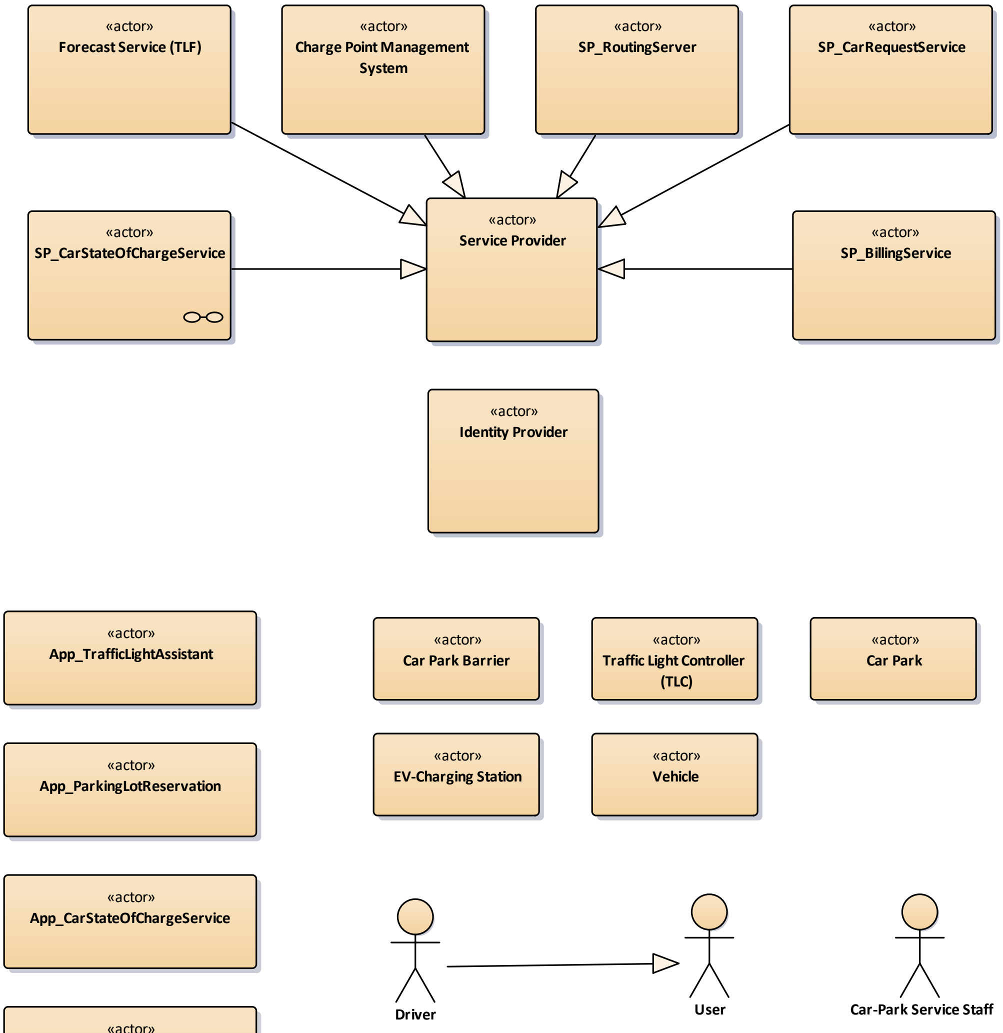

«actor» Forecast Service (TLF)
«actor» Charge Point Management System
«actor» SP_RoutingServer
«actor» SP_CarRequestService
«actor» SP_CarStateOfChargeService
«actor» Service Provider
«actor» SP_BillingService
«actor» Identity Provider
«actor» App_TrafficLightAssistant
«actor» Car Park Barrier
«actor» Traffic Light Controller (TLC)
«actor» Car Park
«actor» App_ParkingLotReservation
«actor» EV-Charging Station
«actor» Vehicle
«actor» App_CarStateOfChargeService
«actor» App_CarRequestService
Driver
User
Car-Park Service Staff

Figure 5: Actors overview

For every actor the associated use cases and, if applicable, the inheritance structure are listed. The "associations" tables list on the left side the use cases (source), which use the actor (target). The "outgoing structural relationship" tables describe inheritance relationship of the actor. Meaning that this actor is a specialization of on more abstract actor. For example, the "Driver" is a special case of the more general "User". The "ingoing structural relationship" tables describe the opposite direction. Actors with this table are a generalization of the actors mentioned in the table.

3.3.1.1 App_CarRequestService

This is a smartphone app to request a vehicle. The Vehicle should drive automatically to the position specified by the Driver.

ASSOCIATIONS	
Source: UC-11.3: Drive automated to the requested position	Target: App_CarRequestService
Source: UC-11.1: Register for Car Reqest Service	Target: App_CarRequestService
Source: UC-11.2: Request Vehicle	Target: App_CarRequestService

3.3.1.2 App_CarStateOfChargeService

This is a smartphone app to remotely request the charging status of the own Vehicle and to inform the User, when the Vehicle is fully charged.

ASSOCIATIONS	
Source: UC-10: Receive state of charge of Vehicle	Target: App_CarStateOfChargeService
Source: UC-10.1: Receive state of charge of Vehicle to registered App	Target: App_CarStateOfChargeService
Source: UC-10.0: Registration for state of charge of Vehicle via App	Target: App_CarStateOfChargeService
Source: UC-10.2: Send state of charge of Vehicle to registered App	Target: App_CarStateOfChargeService

3.3.1.3 App_ParkingLotReservation

This is a smartphone app, which allows lookup and reservation of a parking lot.

ASSOCIATIONS	
Source: UC-01.4: Designate destination location	Target: App_ParkingLotReservation
Source: UC-01.1: Seek and select charging park	Target: App_ParkingLotReservation
Source: UC-01.2: Reserve charging point	Target: App_ParkingLotReservation
Source: UC-02.0: Follow navigation guides	Target: App_ParkingLotReservation

3.3.1.4 App_TrafficLightAssistant

This is an app that could either exist/run on a smartphone or on an on-board vehicle multimedia platform. The app uses Traffic Light Forecast (TLF) data to produce useful information to the driver like Green Light Optimal Speed Advisory (GLOSA) or Time to Green (TTG).

ASSOCIATIONS	
Source: UC-03.0: Use speed advisory on traffic lights	Target: App_TrafficLightAssistant
Source: UC-03.2: Provide forecast centrally	Target: App_TrafficLightAssistant
Source: UC-03.1: Provide forecast locally	Target: App_TrafficLightAssistant

3.3.1.5 Car Park

This is an actor, which represents the IT-Systems of the car park.

ASSOCIATIONS	
Source: UC-07.1: Initial assignment of Vehicle to the infrastructure of the Car Park	Target: Car Park
Source: UC-07.2: Track Vehicles using cameras	Target: Car Park
Source: UC-09: Communicate with charger & charge	Target: Car Park
Source: UC-04.1: Authenticates at the Car Park via V2X	Target: Car Park
Source: UC-06.2: Register arrival and departure from Car Park	Target: Car Park
Source: UC-06.1: Report reservation to SP_BillingService	Target: Car Park
Source: UC-06.3: Register arrival and departure from charging space	Target: Car Park

ASSOCIATIONS	
Source: UC-07.0: Camera-based in-Car Park positioning	Target: Car Park
Source: UC-04.2: Get entrance permission	Target: Car Park
Source: UC-08.1: Makes use of a charging / parking service	Target: Car Park
Source: UC-05.0: Park (partly)automated at charger	Target: Car Park

3.3.1.6 Car Park Barrier

The barrier is the access control of the Car Park. Only Vehicles with a valid reservation or if parking space is available are allowed to enter the Car Park.

ASSOCIATIONS	
Source: UC-08.0: Get access to Car Park	Target: Car Park barrier
Source: UC-04.2: Get entrance permission	Target: Car Park barrier

3.3.1.7 Car-Park Service Staff

Persons within a Car Park who can take care of premium car services such as cleaning, inspection, 'manual' valet parking, etc. In our scenario, this actor plugs in electric Vehicles to the EV-Charging Station after they arrive autonomously at the charging space, if they cannot charge inductively.

ASSOCIATIONS	
Source: UC-09: Communicate with charger & charge	Target: Car-Park Service Staff

3.3.1.8 Charge Point Management System

An EV-Charging Station operator runs such a technical system to 'manage' his EV-Charging Station. This can be a system in the cloud or a part of a Car Park management system.

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from Charge Point Management System to Service Provider

ASSOCIATIONS	
Source: UC-09: Communicate with charger & charge	Target: Charge Point Management System

3.3.1.9 Driver

The Driver is a human person, which operates a Vehicle or is going to operate a Vehicle in the near future, e.g. because he is entering the vehicle.

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from Driver to User

ASSOCIATIONS	
Source: UC-02.0: Follow navigation guides	Target: Driver
Source: UC-12.1.0: Drive safe	Target: Driver
Source: UC-10.1: Receive state of charge of Vehicle to registered app	Target: Driver
Source: UC-12.3.0: Acquire information supply	Target: Driver
Source: UC-10.0: Registration for state of charge of Vehicle via app	Target: Driver
Source: UC-12.2.0: Drive informed	Target: Driver
Source: UC-06: Pay parking and charging	Target: Driver
Source: UC-11.1: Register for SP_CarRequestService	Target: Driver
Source: UC-11.2: Request Vehicle	Target: Driver
Source: UC-02: Follow navigation guides	Target: Driver
Target: UC-11: Request Vehicle	Target: Driver
Target: UC-11.0: Request Vehicle	Target: Driver
Target: UC-01.0: Ensure parking and charging facility	Target: Driver
Target: UC-03: Use Traffic Light Forecast for energy efficient behavior	Target: Driver
Target: UC-12.1.1: Get TPEG hazard warning	Target: Driver
Target: UC-10: Receive state of charge of Vehicle	Target: Driver
Target: UC-01: Ensure parking and charging facility	Target: Driver

ASSOCIATIONS	
Target: UC-12.0: Drive informed and safe	Target: Driver
Source: UC-12.2.2: Initiate a rerouting task	Target: Driver
Source: UC-12.2.5: Alert about significant ETA change	Target: Driver
Source: UC-02.4: Update routing information	Target: Driver
Source: UC-12.2.3: Alert Driver about a range problem	Target: Driver
Source: UC-03.2: Provide forecast centrally	Target: Driver
Source: UC-03.0: Use speed advisory on traffic lights	Target: Driver
Source: UC-06.0: Pay parking and charging	Target: Driver
Source: UC-12.2.1: Show information status quality	Target: Driver
Source: UC-03.1: Provide forecast locally	Target: Driver
Source: UC-12.0: Drive informed and safe	Target: Driver
Source: UC-01.2: Reserve charging point	Target: Driver
Source: UC-12.1.4: Driver is sure to be informed	Target: Driver
Source: UC-11.3: Drive automated to the requested position	Target: Driver
Source: UC-12.1.3: Warning about information supply stall	Target: Driver

3.3.1.10 EV-Charging Station

An EV-Charging Station is a device that is used for external charging of an electric Vehicle's battery. The electrical current is delivered to the Vehicle's onboard battery system through standard cable connector (plug). The EV-Charging Station can be connected to and managed by a remote system. The interface to the remote system is implemented by standard communication protocols (like OCPP or something similar).

ASSOCIATIONS	
Source: UC-06.3: Register arrival and departure from charging spot	Target: EV-Charging Station
Source: UC-09: Communicate with charger & charge	Target: EV-Charging Station

3.3.1.11 Forecast Service (TLF)

The traffic light Forecast Service creates a forecast for each intersection. An intersection is represented by its Traffic Light Controller.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from Forecast Service (TLF) to Service Provider

ASSOCIATIONS	
Target: UC-03: Use Traffic Light Forecast for energy efficient behavior	Target: Forecast Service (TLF)
Target: UC-03.1: Provide forecast locally	Target: Forecast Service (TLF)
Source: UC-03.2: Provide forecast centrally	Target: Forecast Service (TLF)
Source: UC-03.0: Use speed advisory on traffic lights	Target: Forecast Service (TLF)

3.3.1.12 Identity Provider

The Identity Provider manages the active Users of the iKoPA System and serves as a trusted third party to authenticate Users.

ASSOCIATIONS	
Source: UC-08.2: Register initially as potential customer and User	Target: Identity Provider

3.3.1.13 SP_BillingService

A service, which handles the billing processes e.g. for a Driver/Vehicle reserving an EV-Charging Station.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from SP_BillingService to Service Provider

ASSOCIATIONS	
Source: UC-06.2: Register arrival and departure from Car Park	Target: SP_BillingService
Source: UC-06.3: Register arrival and departure from charging spot	Target: SP_BillingService

ASSOCIATIONS	
Source: UC-06.1 Report reservation to SP_BillingService	Target: SP_BillingService

3.3.1.14 SP_CarRequestService

This is a Service Provider for the Car Request Service. The SP_CarRequestService allows Users to request a connected Vehicle. The Vehicle will drive autonomously to the User.

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from SP_CarRequestService to Service Provider

ASSOCIATIONS	
Source: UC-11.1: Register for SP_CarReqestService	Target: SP_CarRequestService
Source: UC-11.3: Drive automated to the requested position	Target: SP_CarRequestService
Source: UC-11.2: Request Vehicle	Target: SP_CarRequestService

3.3.1.15 SP_CarStateOfChargeService

The Service Provider SP_CarStateOfChargeServiceis the broker between the Vehicle and the User to provide the User with the information about the charging status of the Vehicle.

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from SP_CarStateOfChargeService to Service Provider

ASSOCIATIONS	
Source: UC-10.0: Registration for state of charge of Vehicle via app	Target: SP_CarStateOfChargeService

3.3.1.16 SP_RoutingServer

The SP_RoutingServer is a server, which provides routing advice to clients by performing a strategic routing for the whole traffic network of its region. (e.g., a city)

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from SP_RoutingServer to Service Provider

ASSOCIATIONS	
Source: UC-02.2: Calculate routes on central server	Target: SP_RoutingServer

3.3.1.17 Service Provider

The Service Provider is an instance managing the availability of information to consumers.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Generalization from Forecast Service (TLF) to Service Provider
⇨ Generalization from SP_CarRequestService to Service Provider
⇨ Generalization from SP_CarStateOfChargeService to Service Provider
⇨ Generalization from SP_BillingService to Service Provider
⇨ Generalization from SP_RoutingServer to Service Provider
⇨ Generalization from Charge Point Management System to Service Provider

ASSOCIATIONS	
Source: UC-03.2: Provide forecast centrally	Target: Service Provider

3.3.1.18 Traffic Light Controller

The Traffic Light Controller can be described as the "computer in the grey cabinet" somewhere at an intersection, which executes all traffic light programs. It can also communicate with the Traffic Management Centre (TMC) - if there is one.

ASSOCIATIONS	
Target: UC-03: Use Traffic Light Forecast for energy efficient behavior	Target: Traffic Light Controller (TLC)

ASSOCIATIONS	
Target: UC-03.1: Provide forecast locally	Target: Traffic Light Controller (TLC)
Source: UC-03.0: Use speed advisory on traffic lights	Target: Traffic Light Controller (TLC)
Source: UC-03.2 Provide forecast centrally	Target: Traffic Light Controller (TLC)

3.3.1.19 User

The User is a person that interacts with the system. The User is a generalization of the Driver.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Generalization from Driver to User

ASSOCIATIONS	
Source: UC-09: Communicate with charger & charge	Target: User

3.3.1.20 Vehicle

The actor Vehicle represents all mechanical and IT parts of the Vehicle including (partly-) automated driving facilities.

ASSOCIATIONS	
Target: UC-09: Communicate with charger & charge	Target: Vehicle
Target: UC-03: Use Traffic Light Forecast for energy efficient behavior	Target: Vehicle
Target: UC-08: Get access to Car Park	Target: Vehicle
Target: UC-03.0: Use speed advisory on traffic lights	Target: Vehicle
Target: UC-08.0: Get access to Car Park	Target: Vehicle
Target: UC-05.0: Park (partly)automated at charger	Target: Vehicle
Target: UC-04.0: Receive entrance clearance for Car Park	Target: Vehicle

ASSOCIATIONS	
Source: UC-06.3 Register arrival and departure from charging spot	Target: Vehicle
Source: UC-07.2: Track Vehicles using cameras	Target: Vehicle
Source: UC-03.1: Provide forecast locally	Target: Vehicle
Source: UC-04: Receive entrance clearance for Car Park	Target: Vehicle
Source: UC-08.1: makes use of a charging / parking service	Target: Vehicle
Source: UC-12.1.2: Vehicle takes preventive safety measurements	Target: Vehicle
Source: UC-03.2: Provide forecast centrally	Target: Vehicle
Source: UC-10.2: Send state of charge of Vehicle to registered app	Target: Vehicle
Source: UC-10.0: Registration for state of charge of Vehicle via app	Target: Vehicle
Source: UC-07.0: Camera-based in-Car Park positioning	Target: Vehicle
Source: UC-12.1.2: Vehicle takes preventive safety measurements	Target: Vehicle
Source: UC-11.1: Register for SP_CarRequestService	Target: Vehicle
Source: UC-04.2: Get entrance permission	Target: Vehicle
Source: UC-08.2: Register initially as potential customer and User	Target: Vehicle
Source: UC-06.2: Register arrival and departure from Car Park	Target: Vehicle
Source: UC-11.2: Request Vehicle	Target: Vehicle
Source: UC-11.3: Drive automated to the requested position	Target: Vehicle
Source: UC-07.1: Initial assignment of Vehicle to the infrastructure of the Car Park	Target: Vehicle
Source: UC-04.1: Authenticates at the Car Park via V2X	Target: Vehicle

3.3.2 Overview of primary system use cases

In iKoPA 12 main use cases were derived from the visionary scenario. These are:

- UC-01: Ensure parking and charging facility
- UC-02: Follow navigation guides
- UC-03: Use Traffic Light Forecast for energy efficient behavior
- UC-04: Receive entrance clearance for Car Park
- UC-05: Park (partly)automated at charger
- UC-06: Pay parking and charging
- UC-07: Camera-based in-Car Park positioning
- UC-08: Get access to Car Park
- UC-09: Communicate with charger & charge
- UC-10: Receive state of charge of Vehicle
- UC-11: Request Vehicle
- UC-12: Drive informed and safe

The relation between the use cases and the most important actors are described in Figure 6. All use cases and sub use cases are described in the following sections.

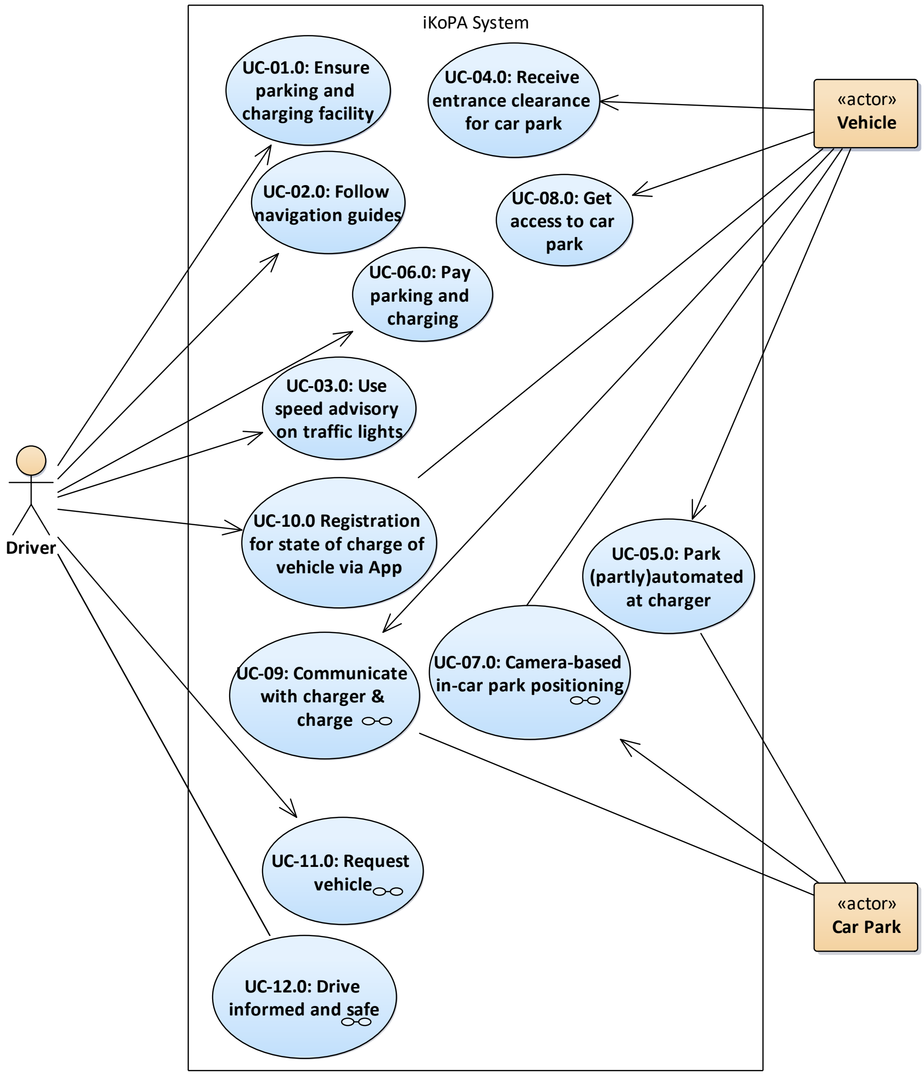

iKoPA System
UC-01.0: Ensure parking and charging facility
UC-04.0: Receive entrance clearance for car park
«actor» Vehicle
UC-02.0: Follow navigation guides
UC-08.0: Get access to car park
UC-06.0: Pay parking and charging
UC-03.0: Use speed advisory on traffic lights
Driver
UC-10.0 Registration for state of charge of vehicle via App
UC-05.0: Park (partly)automated at charger
UC-09: Communicate with charger & charge
UC-07.0: Camera-based in-car park positioning
UC-11.0: Request vehicle
«actor» Car Park
UC-12.0: Drive informed and safe

Figure 6: Use case overview

3.3.3 Detailed view of primary & secondary system use cases

Every use case and the sub use cases are described in detail. For every use case a diagram is given. It describes the relation of the sub uses cases and the interaction with the actors. The uses case is described in relation to the visionary scenario and, if necessary, prerequisites are given. Additionally, every (sub) use case is described with a prose text and a formal step-by-step description including alternatives and exceptions.

3.3.3.1 UC-01: Ensure parking and charging facility

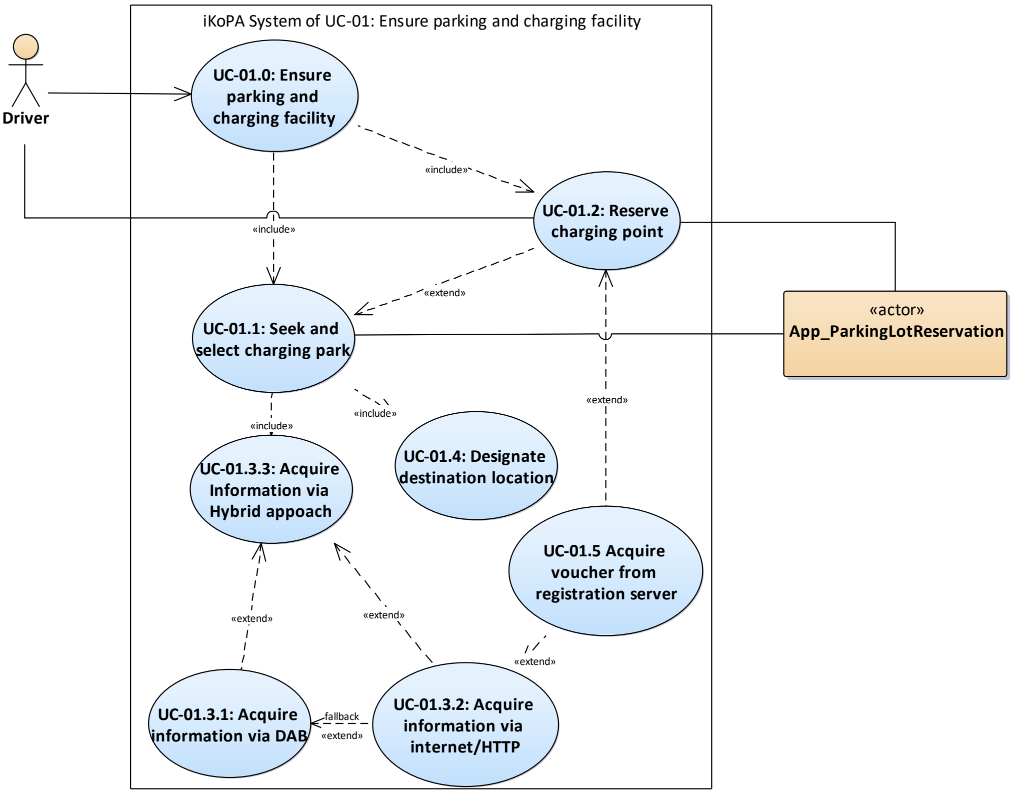

iKoPA System of UC-01: Ensure parking and charging facility
Driver
UC-01.0: Ensure parking and charging facility
«include»
UC-01.2: Reserve charging point
«include»
«extend»
UC-01.1: Seek and select charging park
«actor»
App_ParkingLotReservation
«extend»
«include»
«include»
UC-01.3.3: Acquire Information via Hybrid appoach
UC-01.4: Designate destination location
UC-01.5 Acquire voucher from registration server
«extend»
«extend»
«extend»
UC-01.3.1: Acquire information via DAB
fallback
«extend»
UC-01.3.2: Acquire information via internet/HTTP

Figure 7: UC-01: Ensure parking and charging facility

3.3.3.1.1 UC-01.0: Ensure parking and charging facility

The User selects and reserves a facility at the destination, that allows parking and charging (called charging point, in a charging park).

SCENARIOS

Basic Path.

Helena H. looks up and selects a parking location as her target. This includes information about charging options and the reservation process for a suitable parking and charging point. Information about existing

SCENARIOS

and available parking and charging sites is transmitted to her car by different communication technologies, like DAB and LTE. –

1. The user seeks and selects the charging park.
    Uses: UC-01.1: Seek and select charging park
2. A TPEG EMI Charging Point in the TPEG EMI Charging Park is selected.
    Uses: UC-01.2: Reserve charging point
3. Use case ends.
    Uses: –

3.3.3.1.2 UC-01.1: Seek and select charging park

A charging park is searched and from a collection of suitable options. The User reserves a suitable parking lot.

EXTERNAL REQUIREMENTS

Requirement. REQ-F-001: TPEG traffic information is broadcasted via DAB

SCENARIOS

Basic Path.

A charging park near the destination location is searched and from a collection of suitable options, the user selects one. As a result, the system has a usable precise location where the Vehicle needs to go. (Note: this location may differ from the location, where the User is willing to get, as no charging park might be exactly at the desired User location).

1. User designates destination location.
    Uses: UC-01.4: Designate destination location
2. Information is acquired via hybrid approach.
    Uses: UC-01.3.3: Acquire Information via Hybrid approach
3. App_ParkingLotReservation shows compatible TPEG EMI Charging Park s in the relevant destination area.
    Uses: –
4. Driver selects TPEG EMI Charging Park to access additional information.
    Uses: –

Alternate: 4a. Reservation not possible

5. Driver decides to try a reservation and triggers a reservation request.
    Uses: –

Alternate: 5a. No reservation

6. TPEG EMI Charging Point is reserved.
    Uses: UC-01.2: Reserve charging point
7. Use case ends.
    Uses: –

SCENARIOS

Alternate. No reservation

1. Driver decides not to try a reservation.
   Uses: –
2. Use case ends.
   Uses: –

Alternate. Reservation not possible

1. Reservation is not supported by the TPEG EMI Charging Park
   Uses: –
2. Use case ends.
   Uses: –

CONSTRAINTS

Invariant. Transmitted and available information through DAB and HTTP/Internet must be consistent and compatible.

There shall not be a significant difference between the information available through DAB reception and HTTP/Internet. The receiver does not try to check for inconsistencies and conflicts but is satisfied if it can acquire a sufficient information set through one method.

3.3.3.1.3 UC-01.2 Reserve charging point

The user reserves a parking lot, with an EV-Charging Station (called a "charging point" in a "charging park"). The charging park (in e.g. Car Park) must be near the desired destination of the user, and is selected by the User.

PRE-CONDITION CONSTRAINT

Specific charging park was selected by the user

The user has selected a charging park where he likes to make a reservation for a charging point (including parking space). The charging park is described by a specific location and a reference to the parkID_key is provided. The charging park may contain multiple charging points.

User has decided to try a reservation in the specified charging park.

The User is registered with the E-Mobility Provider

The User has received an e-Mobility Account Identifier (EMAID) that it can use to make reservation requests.

SCENARIOS
Basic Path. The app App_ParkingLotReservation sends a reservation request to the server. The server responds and acknowledges the reservation, including a reservation voucher that may be used to proof that a reservation was requested and acknowledged. 1. Request and receive signed voucher from identity provider. Uses: – 2. App_ParkingLotReservation sends the voucher (previously received from identity provider) and a reservation request to the reservation server. Uses: – Exception: 2a. Impossible to send reservation request 3. The reservation server answers with a reservation response, confirming the reservation. Uses: – Alternate: 3a. No confirmation Exception: 3b. No response; Timeout 4. Use case ends. Uses: –
Alternate. No confirmation 1. Reservation server answers with a reservation response, but without confirming the reservation. Uses: – 2. Use case ends. Uses: –
Exception. No response; Timeout 1. No Reservation Response is received from the reservation server within a given amount of time, causing a timeout. Uses: – 2. Use case ends. Uses: –
Exception. Impossible to send Reservation Request 1. The underlying transport layer tells the App_ParkingLotReservation that no Reservation Request could be send (either due to a timeout or because of a lack of a bidirectional connection). Uses: – 2. Use case ends. Uses: –

3.3.3.1.4 UC-01.3.1: Acquire information via DAB

To acquire DAB information the DAB receiver has to be tunes accordingly, so that the DAB TPEG service can receive the information about the relevant destination area.

SCENARIOS
Basic Path. The appropriate service is tuned, using the DAB receiver. The data takes some time for reception, depending on the reception quality and the amount of data. If reception quality is bad or the amount of data exceeds certain limits a timeout may occur or the User may decide to wait no longer to receive data via DAB, but to use other means of communication. 1. TPEG-Traffic-Information-Storage loads and decodes data from DAB receiver. Uses: – Exception: 1a. Timeout while trying to load all data Alternate: 1b. User becomes impatient 2. TPEG-Traffic-Information-Storage estimates (guesses) that all data is loaded and is up-to-date. Uses: – 3. Use case ends. Uses: –
Alternate. User becomes impatient 1. The User decides that loading data via DAB reception takes too long and it prefers to use Internet Connectivity instead. Uses: – 2. Information is acquired via Internet connectivity. Uses: UC-01.3.2: Acquire information via internet/HTTP 3. Use case ends. Uses: –
Exception. Timeout while trying to load all data 1. Loading all data using DAB reception takes too long, causing an abort and failback to Internet connectivity. Uses: – 2. Information is acquired via Internet connectivity. Uses: UC-01.3.2: Acquire information via internet/HTTP 3. Use case ends. Uses: –

3.3.3.1.5 UC-01.3.2: Acquire information via internet/HTTP

Load the required information about the relevant destination area, directly via Internet Connectivity from a known internet address.

SCENARIOS

Basic Path.

First, a voucher is requested and received from the Identity Provider, to assure anonymity against other servers. The voucher is used to authenticate against the server that provides the information about parking and charging availabilities.

1. Request and receive voucher from Identity Provider.
   Uses: –
2. Establish a connection via Internet connectivity, handover voucher (previously received from Identity Provider) and request the desired information.
   Uses: –

Exception: 2a. Unable to make internet/HTTP connection

3. Receive the desired information via the same Internet connectivity.
   Uses: –

Exception: 3a. No reception of the desired data or not decodable

4. Use case ends.
   Uses: –

Exception. Unable to make internet/HTTP connection

1. No connection via internet/HTTP can be established, thus no Internet connectivity.
   Uses: –
2. An error message is shown to the User.
   Uses: –
3. Acquiring information has failed.
   Uses: –
4. Use case ends.
   Uses: –

Exception. No reception of the desired data or not decodable

1. No response is received, it is not the desired information or the response is not decodable.
   Uses: –
2. The user is informed about the error.
   Uses: –
3. Acquiring the desired information has failed.
   Uses: –
4. Use case ends.
   Uses: –

3.3.3.1.6 UC-01.3.3: Acquire Information via Hybrid approach

Use an appropriate TPEG service and load the desired information, about available charging parks in the relevant destination area.

PRE-CONDITION CONSTRAINT

E-Mobility Provider must have provided a basic configuration

This includes static information about

- access information where updates for this base information can be loaded directly from the E-Mobility Provider via internet/HTTP
- which DAB TPEG EMI services provide current information about EV-Charging Stations, that are provided by or have roaming contracts with the E-Mobility Provider
- where to load on-demand TPEG EMI data directly via internet/HTTP about EV-Charging Stations that are provided by or have roaming contracts with the E-Mobility Provider
- where to make a reservation request via internet/HTTP using the TPEG EMI protocol/application

This might overlap or match hybrid orientation information.

SCENARIOS

Basic Path.

Preferably a DAB based transmission is used to receive information about charging and Car Parks, including free and reservable capacities. The reception is monitored and different communications are used in case the preferred options are unavailable or fail to deliver sufficient information in time.

1. TPEG-Traffic-Information-Storage tunes the DAB receiver to appropriate TPEG EMI service (by using predefined information which DAB TPEG EMI service to use).

Uses: –

Exception: 1a. Unable to tune DAB receiver to TPEG service

2. TPEG-Traffic-Information-Storage checks minimum reception quality (signal strength, error rate) on the DAB reception.

Uses: –

Exception: 2a. DAB reception quality insufficient

3. Information is acquire via DAB reception.

Uses: UC-01.3.1: Acquire information via DAB

4. Use case ends.

Uses: –

Exception. Unable to tune DAB receiver to TPEG service

In case the information may not be available through DAB, other means of communication are used, such as cellular based transmission. The same TPEG based information shall be available through different carriers, while not all of them might be available at a certain point in time.

1. TPEG-Traffic-Information-Storage fails to tune DAB receiver to appropriate service.

Uses: –

2. Information is acquired via Internet connectivity.

Uses: UC-01.3.2: Acquire information via internet/HTTP

3. Use case ends.

Uses: –

SCENARIOS
Exception. DAB reception quality insufficient In case the retrieval of information through the preferred communication path fails, other means of communication are used, such as cellular based transmission. The same TPEG based information shall be available through different carriers, that might have different quality and performance in different situations and the system selects the best option. 1. Quality of the DAB reception is estimated as insufficient. Uses: – 2. Information is acquired via Internet Connectivity. Uses: UC-01.3.2: Acquire information via internet/HTTP 3. Use case ends. Uses: –

3.3.3.1.7 UC-01.4: Designate destination location

The user types in an address and the navigation system finds the location and matches it to its map. As a result, the system has a sufficiently precise location that describes the destination desired by the User.

SCENARIOS
Basic Path. The user enters information, describing the intended target of the voyage. The navigation system uses its internal logical map to match this information and to pin it down to a specific precise reference in this internal logical map that can be used to plan the route and guide the travel. 1. The user types in the desired location address. Uses: – Alternate: 1a. Incomplete address 2. The Navigation system (local autarkic) finds a perfect match in its logic location database. Uses: – Alternate: 2a. Imperfect match 3. Use case ends. Uses: –
Alternate. Incomplete address In case the entered information is not complete, thus does not allow to match to one specific location in the logical map, the user tries to make a best-effort guess, offer some possible completions to the user and ask him to select a specific option. 1. The user gives an incomplete address. Uses: – 2. The Navigation System searches for possible completions and shows them to the user. Uses: – 3. The user selects one of the given options. Uses: –

SCENARIOS

Alternate. Imperfect match

In case the entered information do not make a match with the internal logical map, the system makes a best effort guess about the "nearest match", using internal metrics. A limited number of options are presented to the user that is ask to pick one of them.

1. The Navigation System does not find a perfect match.
   Uses: –
2. The Navigation System searches for similar options and presents them to the user.
   Uses: –
3. The user selects one of the given options.
   Uses: –

3.3.3.1.8 UC-01.5 Acquire voucher from identity provider

A voucher is requested and received from the Identity Provider.

SCENARIOS

Basic Path.

A voucher is requested and received from the Identity Provider, which is the only server who knows the true identity of the User. The voucher from the Identity Provider is then used to make authenticate to other servers, while keeping anonymity or pseudonymity.

1. Contact Identity Provider via Internet/HTTP.
   Uses: –
2. Authenticate with the Identity Provider
   Uses: –
3. Receive a voucher, signed by the Identity Provider
   Uses: –

3.3.3.2 UC-02: Follow navigation guides

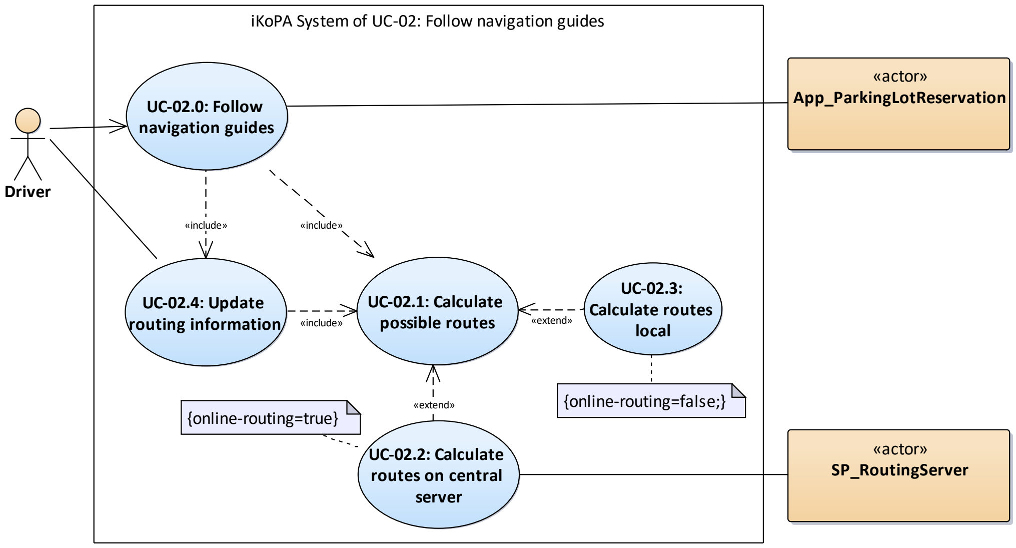

iKoPA System of UC-02: Follow navigation guides
Driver
UC-02.0: Follow navigation guides
«actor» App_ParkingLotReservation
«include»
«include»
UC-02.4: Update routing information
«include»
UC-02.1: Calculate possible routes
«extend»
UC-02.3: Calculate routes local
{online-routing=true}
«extend»
{online-routing=false;}
UC-02.2: Calculate routes on central server
«actor» SP_RoutingServer

Figure 8: UC-02: Follow navigation guides

3.3.3.2.1 UC-02.0: Follow navigation guides

This use case describes how a system in the vehicle calculates possible routes to a given destination and how it guides the driver to this destination. In the visionary scenario, Helena H. uses this use case to navigate to the new nursery.

PRE-CONDITION CONSTRAINT

Network connection for navigation system is present.

Destination has been obtained from other system.

SCENARIOS

Basic Path.

In this use case, the navigation system calculates possible routes to a destination given by the parking reservation app. This can be done either ‘offline’/in-vehicle or 'online' with the help of a SP_Routing Server. The navigation system then prompts the routes to the Driver for selection. Afterwards, it provides the Driver with driving commands to assist him in driving to the destination.

SCENARIOS

1. Driver opens Navigation System (local autarkic).
    Uses: –

2. Navigation System (local autarkic) displays destination point, received from App_ParkingLotReservation, on map.
    Uses: –

Exception: *2a*. Destination not received

3. UC-02.1: Calculate possible routes.
    Uses: –

Exception: *3a*. No possible route found

4. Navigation System (local autarkic) shows possible routes to Driver and waits for route selection.
    Uses: –

5. Driver selects desired route.
    Uses: –

Exception: *5a*. No route selected

6. Navigation System (local autarkic) starts navigation to destination via selected route.
    Uses: –

7. Use case ends.
    Uses: –

Exception. Destination not received

1. Destination point not received from App_ParkingLotReservation.
    Uses: –

2. Use case ends.
    Uses: –

Exception. No possible route found

1. No possible route returned by UC-02.1: Calculate possible routes.
    Uses: –

2. Inform Driver.
    Uses: –

3. Use case ends.
    Uses: –

Exception. No route selected

1. Driver does not select a route until the system is shut down.
    Uses: –

2. Use case ends.
    Uses: –

POST CONDITION CONSTRAINT

Route guidance in the navigation system is active.

3.3.3.2.2 UC-02.1: Calculate possible routes

The navigation system calculates possible routes.

SCENARIOS

Basic Path.

The navigation system calculates possible routes, depending on the traffic input, User preferences and Vehicle properties.

1. Navigation System (local autarkic) calculates preliminary routes based on map data, preferences and currently known data.
   Uses: –

Exception: *1a*. No route possible

2. UC-02.3: Calculate routes locally (this is the default).
   Uses: –

Alternate: *2a*. Online route calculation

3. Navigation System (local autarkic) returns route.
   Uses: –
4. Use case ends.
   Uses: –

Alternate. Online route calculation

In this sub-use case, the route to the destination is calculated, either purely locally or by communicating with a backend routing server.

1. UC-02.2: Calculate routes on central server (if online calculation is chosen.)
   Uses: –

Alternate. Offline route calculation

1. UC-02.3: Calculate routes locally
   Uses: –

Exception. No route possible

1. Notify Navigation System (local autarkic).
   Uses: –
2. Use case ends.
   Uses: –

3.3.3.2.3 UC-02.2: Calculate routes on central server

Calculate routes remotely on a central server with all information available there.

PRE-CONDITION CONSTRAINT

Connection to Sp_RoutingServer is available.

Destination is known.

SCENARIOS

Basic Path.

Calculate routes remotely on a central server with all information available there, e.g. a traffic forecast based on historical data.

1. Forward destination and vehicle information to SP_RoutingServer.
   Uses: –
2. SP_RoutingServer responds with route.
   Uses: –

Exception: *2a*. No route received

3. Traffic information from TPEG-Traffic-Information-Storage is added to route for clarification.
   Uses: –
4. Return received route.
   Uses: –
5. Use case ends.
   Uses: –

Exception. No route received

1. Inform Navigation System (local autarkic).
   Uses: –
2. Use case ends.
   Uses: –

POST CONDITION CONSTRAINT

Route is known.

3.3.3.2.4 UC-02.3: Calculate routes locally

Calculate the routes locally with information available to the navigation system.

SCENARIOS

Basic Path.
Calculate the routes locally with information available to the navigation system.

1. Destination is sent to the Navigation System (local autarkic).
   Uses: –
2. Navigation System (local autarkic) obtains traffic data from TPEG-Traffic-Information-Storage.
   Uses: –

Exception: *2a*. Destination not sent
Exception: *2b*. No TPEG Information available

3. Navigation System (local autarkic) calculates possible routes based on available data.
   Uses: –
4. Navigation System (local autarkic) returns optimal route.
   Uses: –

Exception: *4a*. No route possible

5. Use case ends.
   Uses: –

Exception. Destination not sent

1. Return error indication.
   Uses: –
2. Use case ends.
   Uses: –

Exception. No TPEG Information available

1. No traffic information is obtained from TPEG-Traffic-Information-Storage.
   Uses: –

Exception. No route possible

1. No possible route is found.
   Uses: –
2. Inform User about routing problem.
   Uses: –
3. Use case ends.
   Uses: –

3.3.3.2.5 UC-02.4: Update routing information

The navigation system updates the routing information, either because it has been triggered to do so (e.g. as new traffic information is available) or because the driver has left the route.

PRE-CONDITION CONSTRAINT

A route has been selected and the navigation was running.

An event occurred, which triggered a re-calculation of the route.

SCENARIOS

Basic Path.
In this sub-use case, the possible routes calculated by the navigation system are shown to the driver. He then selects one of the routes. The selected route is used by the navigation system to navigate to the destination.

1. UC-02.1: Calculate possible routes.
    Uses: –
Exception: *1a*. No possible route found
2. Navigation System (local autarkic) shows new route to Driver and waits for confirmation.
    Uses: –
3. Driver confirms new route.
    Uses: –
Alternate: *3a*. Driver does not confirm new route
4. Navigation System (local autarkic) starts navigation to destination via selected route.
    Uses: –
5. Use case ends.
    Uses: –

Exception. No possible route found

1. UC-02.1: Calculate possible routes does not return any usable route.
    Uses: –
2. Inform Driver that navigation is not possible.
    Uses: –
3. Use case ends.
    Uses: –

Alternate. Driver does not confirm new route

1. Driver does not confirm new route.
    Uses: –
2. Navigation System (local autarkic) continuous navigating on previously selected route.
    Uses: –
3. Use case ends.
    Uses: –

3.3.3.3 UC-03: Use Traffic Light Forecast for energy efficient behavior

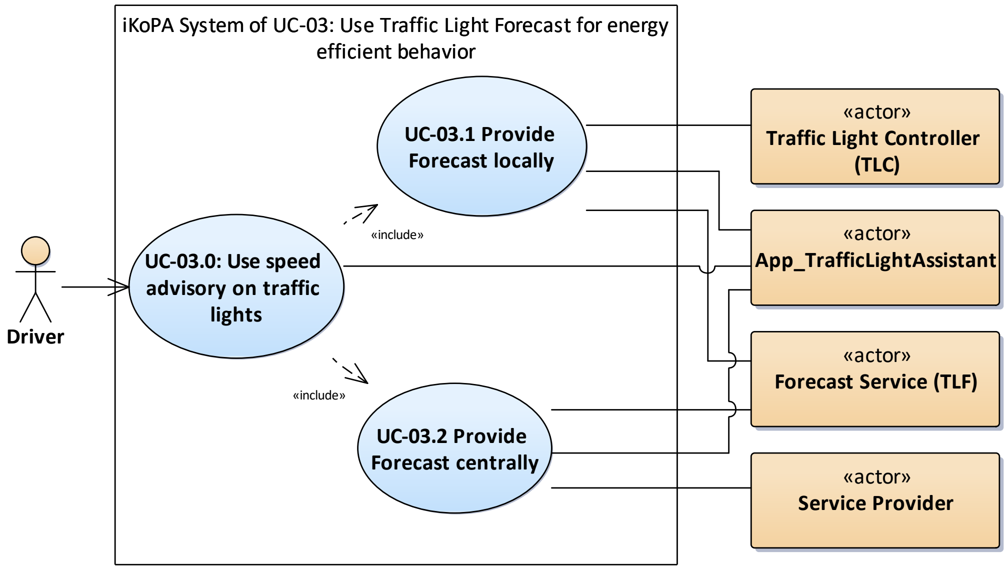

iKoPA System of UC-03: Use Traffic Light Forecast for energy efficient behavior
UC-03.1 Provide Forecast locally
UC-03.0: Use speed advisory on traffic lights
UC-03.2 Provide Forecast centrally
«include»
«include»
Driver
«actor» Traffic Light Controller (TLC)
«actor» App_TrafficLightAssistant
«actor» Forecast Service (TLF)
«actor» Service Provider

Figure 9: UC-03: Use Traffic Light Forecast for energy efficient behavior

3.3.3.3.1 UC-03.0: Use speed advisory on traffic lights

The smartphone/e-vehicle app receives a Traffic Light Forecast (TLF) and uses it to display information that could be used by the driver in order to optimize driving behavior in the most energy efficient way. The displayed information can be in the form of a Green Light Optimal Speed Advisory (GLOSA) or Time to Green (TTG). The TLF data could be further used by onboard-automated cruise control functionality in order to enable adaptive speed adjustments, which could increase efficiency and comfort of driving.

SCENARIOS

Basic Path.
The Traffic Light Forecast (TLF) data is generated by the Forecast Service based on parameters continuously provided by the local Traffic Light Controller. The forecast data is received by the smartphone/e-vehicle app and is used to produce information for Green Light Optimal Speed Advisory (GLOSA) and/or Time to Green (TTG).

1. Traffic Light Controller (TLC) provides current detection and signal group data to Forecast service.
    Uses: –

Alternate: *1a*. 11p local path

2. Forecast Service (TLF) generates a forecast based und current [and historic] data.
    Uses: –

3. The forecast is linked to the corresponding MAP representation and both are issued as a SPAT/MAP message on a service interface.
    Uses: –

4. Dissemination & reception - Sub-Use cases
    Uses: –

SCENARIOS

Alternate: *4a*. Central path

5. Return from sub-use cases.
    Uses: –
6. App_TrafficLightAssistant shows GLOSA or TTG.
    Uses: –
7. Vehicle adapts its longitudinal movement automatically or manually.
    Uses: –
8. Use case ends
    Uses: –

Alternate. 11p local path

1. <include> UC-03.1 Provide Forecast locally
    Uses: –

Alternate. Central path

1. <include> UC-03.2 Provide Forecast centrally
    Uses: –

3.3.3.3.2 UC-03.1_local: Provide forecast locally

The TLF data is broadcasted locally within the area of the serviced intersection.

SCENARIOS

Basic Path.

In this use case the TLF data is delivered to the Traffic Light Controller and broadcasted locally over a standard V2X dedicated wireless interface.

1. Traffic Light Controller (TLC) uses the generated SPAT/MAP of the Forecast Service (TLF) to disseminate it via 802.11p (locally).
    Uses: –
2. The Vehicle reaches the area of the intersection (recognized by 802.11p reception) and receives Traffic Light Forecast via 11p.
    Uses: –
3. Sub-use case ends: return to basic path.
    Uses: –

3.3.3.3.3 UC-03.2_central: Provide forecast centrally

The TLF data is disseminated and consumed by others through a central service.

PRE-CONDITION CONSTRAINT

As the case may be the User must have registered to get access to the central service depending on if the service can be used free of charge or not.

SCENARIOS

Basic Path.

The TLF data is disseminated globally to users by a Service Provider over a wireless network (DAB+, cellular or other).

1. Service Provider receives a generated SPAT/MAP from the Forecast Service (TLF).
   Uses: –
2. Vehicle reaches area of intersection recognized by app functionality through GPS geo-fencing mechanism.
   Uses: –
3. App_TrafficLightAssistance acquires/filters out the TLF data for the recognized intersection.
   Uses: –
4. Sub-Use case ends: return to basic path.
   Uses: –

3.3.3.4 UC-04: Receive entrance clearance for car park via V2X authentication

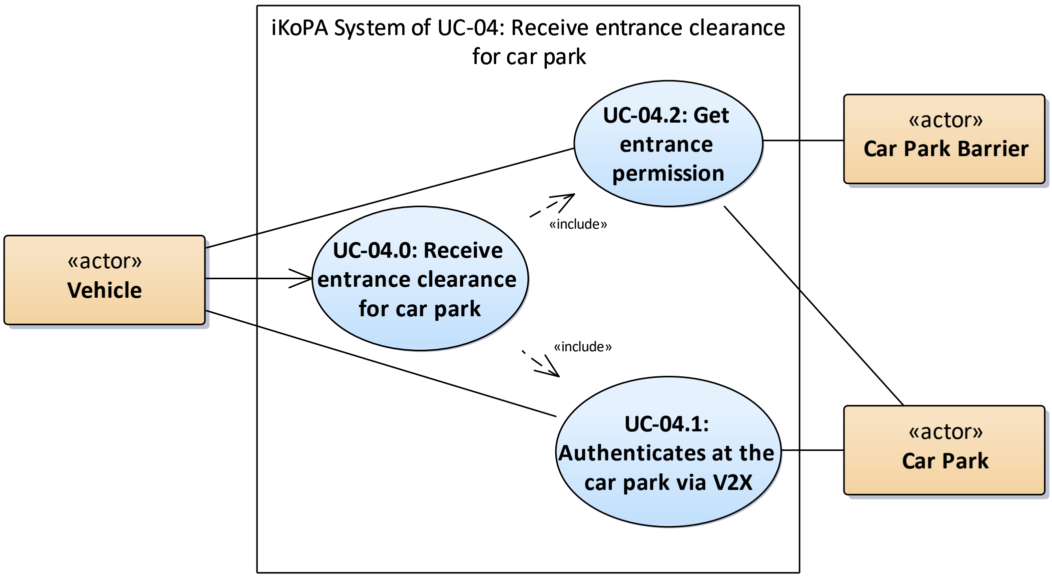

iKoPA System of UC-04: Receive entrance clearance for car park
UC-04.2: Get entrance permission
«actor» Car Park Barrier
«include»
«actor» Vehicle
UC-04.0: Receive entrance clearance for car park
«include»
UC-04.1: Authenticates at the car park via V2X
«actor» Car Park

Figure 10: UC-04: Receive entrance clearance for car park

3.3.3.4.1 UC-04.0: Receive entrance clearance for Car Park

Vehicle authenticates itself at the car park via V2X and gets entrance permission via opening a barrier or giving green light.

SCENARIOS
Basic Path. The sequence of V2X authentication follows: The Vehicle approaches the Car Park. When in reach of the Car Park RSU, i.e. 300 - 1500 m distance, the V2X RSU regularly identifies itself as a barrier. The V2X Vehicle's OBU sends the V2X registration message requesting entrance. The Car Park RSU sends a challenge to the V2X OBU in the form of a set of random numbers. The Vehicle reacts by sending a signed response encrypted with its private key received during registration. The Car Park RSU confirms the V2X response message as valid using the public key. As a final action, the Car Park barrier opens up the way for the vehicle and the vehicle enters the car park. 1. UC-04.1: Authenticate at the Car Park via V2X Uses: – 2. UC-04.2: Get entrance permission Uses: – 3. Use case ends. Uses: –

3.3.3.4.2 UC-04.1: Authenticate at the Car Park via V2X

The Vehicle arrives at the Car Park. It sends its authentication request via V2X to the barrier's V2X station. The barrier RSU checks the request by sending a challenge to the Vehicle. The Vehicle signs with the private key received during reservation. The barrier checks authentication with the public key. If confirmed, the barrier opens. Traffic light colors signal the authentication result option.

PRE-CONDITION CONSTRAINT
The Vehicle identification is registered at the Identity Provider.
The Vehicle identification via V2X is implemented.
The Vehicle has a valid reservation for the Car Park.
The Vehicle is located near the Car Park.

The Car Park RSU has access to the reservation data.

SCENARIOS

Basic Path.

The authentication procedure is based on the following concept: A Vehicle approaches the Car Park with the V2X OBU getting into the reach of Car Park RSU. The Car Park RSU sends regular messages: "I am a barrier, Vehicles, please authenticate!". The Vehicle's V2X OBU sends the V2X authentication request; the Car Park Barrier challenges the vehicle and gets a signed response back. As next step, the Car Park RSU checks whether the signature from the V2X OBU is valid without involving the reservation backend server, and without knowledge of the Vehicle's identity.

1. Vehicle approaches Car Park with the Vehicle V2X OBU getting into the reach of Car Park RSU.
   Uses: –
2. Vehicle V2X OBU sending the V2X registration message carrying the identification information.
   Uses: –
3. Car park RSU checks whether the registration message of Vehicle V2X OBU is valid involving the reservation service backend service.
   Uses: –
4. Use case ends.
   Uses: –

POST CONDITION CONSTRAINT

The reservation status is updated in the reservation backend server.

3.3.3.4.3 UC-04.2: Get entrance permission

The Car Park barrier gets the authorization result from the local V2X station after the authentication procedure. If the Vehicle is allowed to access, the Car Park the barrier is opened and the Vehicle may pass.

PRE-CONDITION CONSTRAINT

The Vehicle identification is registered in the Identity Provider.

The Vehicle identification via V2X is implemented.

The Vehicle has a valid reservation for Car Park.

Car Park RSU of Car Park has access to the reservation data.

SCENARIOS

Basic Path.
Access to the Car Park is granted with the following set of actions: First, the Car Park RSU confirms the V2X reservation message as valid. Then the Car Park barrier opens up the way for the Vehicle. The Vehicle then enters the Car Park, which ends the use case.

1. Car Park RSU confirms the V2X RegistrationMessage as valid to the Vehicle V2X OBU.
   Uses: –
Exception: *1a*. Technical issue
Exception: *1b*. Authentication invalid
Exception: *1c*. Capacity not sufficient
2. Car Park barrier opens up the way for Vehicle.
   Uses: –
3. Vehicle enters the Car Park.
   Uses: –
4. Use case ends.
   Uses: –

Exception. Authentication invalid

1. Car park RSU denies the V2X reservation message since authentication is invalid.
   Uses: –
2. Car park barrier stays in the blocking position.
   Uses: –
3. Car park RSU sends V2X denial message to Vehicle V2X OBU that the authentication is invalid.
   Uses: –
4. Use case ends.
   Uses: –

Exception. Capacity not sufficient

1. Car park RSU denies the V2X reservation message since the system has technical issues.
   Uses: –
2. Car park barrier stays in the blocking position.
   Uses: –
3. Car park RSU sends V2X denial message to Vehicle V2X OBU that the system does not work properly.
   Uses: –
4. Use case ends.
   Uses: –

SCENARIOS
Exception. Technical issue 1. Car park RSU denies the V2X reservation message since the system has technical issues. Uses: – 2. Car park barrier stays in the blocking position. Uses: – 3. Car park RSU sends V2X denial message to Vehicle V2X OBU that the system does not work properly. Uses: – 4. Use case ends. Uses: –

POST CONDITION CONSTRAINT
Car park barrier closes after vehicle entered.
The reservation status is updated in the reservation backend server.

3.3.3.5 UC-05: Park (partly) automated at charger

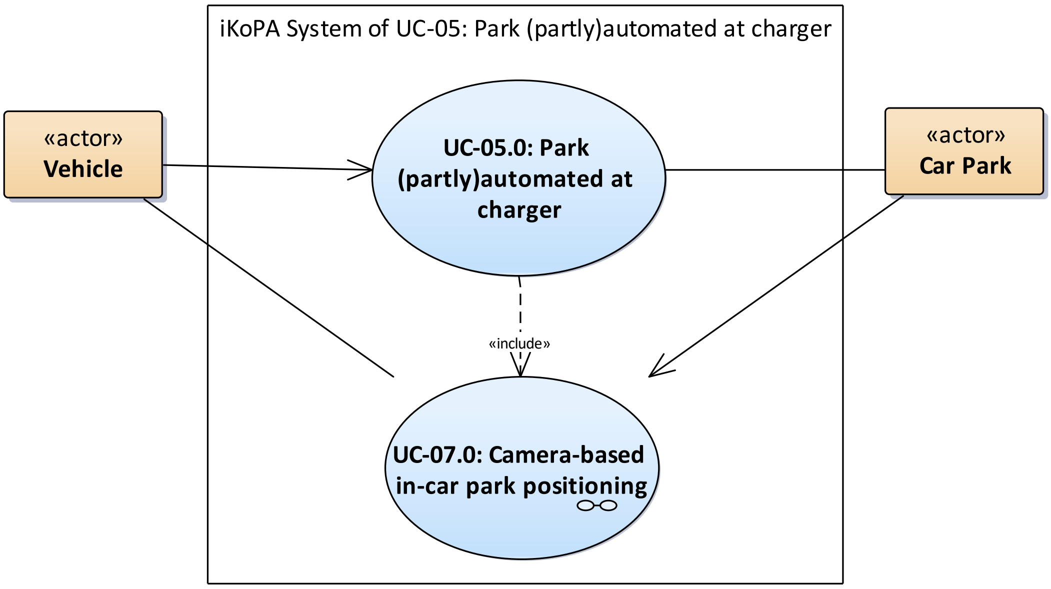

iKoPA System of UC-05: Park (partly)automated at charger
«actor»
Vehicle
UC-05.0: Park (partly)automated at charger
«actor»
Car Park
«include»
UC-07.0: Camera-based in-car park positioning

Figure 11: UC-05: Park (partly) automated at charger

3.3.3.5.1 UC-05.0: Park (partly) automated at charger

The Vehicle drives (partly) automated to the EV-Charging Station and parks there.

RESPONSIBILITIES (INTERNAL REQUIREMENTS)

☑ . Use case 04 has to be finished successfully.

In order not to check the authentication and the reservation of the Vehicle twice, use case 05 can only start when use case 04 has finished successfully.

SCENARIOS

Basic Path.

Helena H. reaches the Car Park Barrier at the Car Park of the shopping mall with her Vehicle. She leaves the Vehicle and goes shopping. Meanwhile the Vehicle drives (partly) automated from the entrance of the Car Park to the reserved charging spot. After finishing her shopping tour, Helena returns to the barrier of the Car Park and calls her Vehicle via the App_CarRequestService. When the Vehicle arrives, Helena takes it over and continues her travel. This use case will be triggered by use case 4.2 after the authentication procedure and the reservation check are completed.

Afterwards the Car Park checks the V2X connection between the Vehicle and Car Pank the occupancy status of charging spot. If the pre-reserved charging spot is empty, the Car Park calculates the indoor route to the EV-Charging Station and transmits it to the Vehicle. The Vehicle calculates the real driving trajectory from the received routing information. If these steps are preformed successfully, the vehicle starts driving and the car park invokes use case 07.

1. Car Park checks V2X Connection between Vehicle and Car Park.
   Uses: –
2. Car Park checks occupancy of parking lot.
   Uses: –
3. Car Park calculates indoor route to the parking lot.
   Uses: –
4. Car Park transmits route to Vehicle.
   Uses: –
5. The Vehicle calculates a trajectory from the routing information.
   Uses: –
6. Vehicle starts driving.
   Uses: –
7. The UC-07.0: Camera-based in-car park positioning will be invoked.
   Uses: –
8. Use case ends.
   Uses: –

3.3.3.6 UC-06: Pay parking and charging

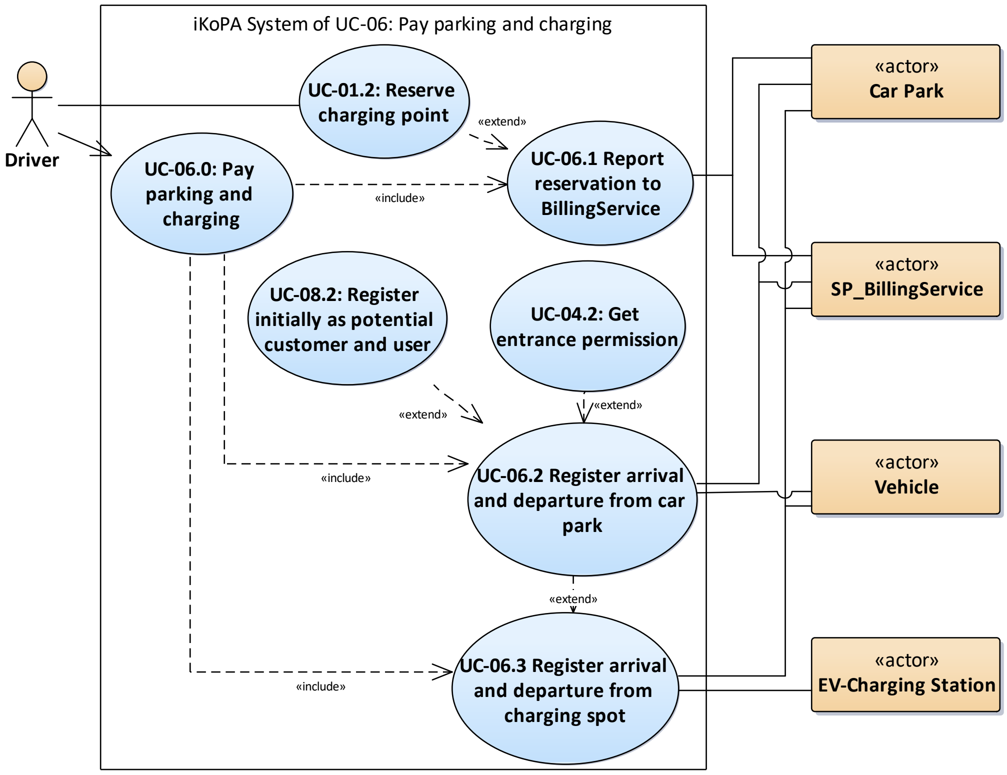

iKoPA System of UC-06: Pay parking and charging
Driver
UC-01.2: Reserve charging point
«extend»
UC-06.1 Report reservation to BillingService
UC-06.0: Pay parking and charging
«include»
UC-08.2: Register initially as potential customer and user
UC-04.2: Get entrance permission
«extend»
«extend»
UC-06.2 Register arrival and departure from car park
«include»
«extend»
UC-06.3 Register arrival and departure from charging spot
«include»
«actor» Car Park
«actor» SP_BillingService
«actor» Vehicle
«actor» EV-Charging Station

Figure 12: UC-06: Pay parking and charging

3.3.3.6.1 UC-06.0: Pay parking and charging

The Driver automatically pays the parking and charging bill.

SCENARIOS

Basic Path.

The payment model is based on the time spent in a Car Park and charging spot (as opposed to a model based on the power-consumption). The time spent in the Car Park and charging spot is determined and recorded separately to account for different costs and prices.

‘

1. <include> UC-06.1 Report reservation to SP_BillingService
   Uses: –
2. <include> UC-06.2 Register arrival and departure from Car Park
   Uses: –
3. <include> UC-06.3 Register arrival and departure from charging spot
   Uses: –
4. Use case ends.
   Uses: –

3.3.3.6.2 UC-06.1: Report reservation to SP_BillingService

The necessary information to bill the Driver for a reservation is reported to a SP_BillingService.

PRE-CONDITION CONSTRAINT
The User reserved a charging park E-Mobility Provider.
The reservation was confirmed.
The user is registered at the SP_BillingService.

SCENARIOS

Basic Path.
Information about a reservation is passed on to the SP_BillingService. The intent is to extend the UC-1.2 to enable automatic billing of a reservation, for example, by charging a reservation fee.

1. <extend> UC-01.2.
   Uses: –
2. The Car Park reports the information necessary for billing to the SP_BillingService.
   Uses: –
3. Use case ends.
   Uses: –

3.3.3.6.3 UC-06.2: Register arrival and departure from Car Park

The time spent in the Car Park is automatically determined by registering the arrival and departure time.

PRE-CONDITION CONSTRAINT
The Vehicle received entrance permission

SCENARIOS

Basic Path.
As the pricing model is based on the time spent in the Car Park, the actual time spent of the Vehicle in the Car Park must be determined. To determine the duration, the Car Park registers the time of entry and exit of the Vehicle. After the time is determined, the Car Park reports the time spent to the SP_BillingService.

SCENARIOS
1. <extend> UC-04.02 and UC-08.02. Uses: – 2. The Vehicle enters the Car Park. Uses: – 3. The (IT systems of the) Car Park registers the time of entry. Uses: – 4. The Vehicle parks in the Car Park. Uses: – 5. The Vehicle leaves the Car Park. Uses: – 6. The (IT systems of the) Car Park registers the time of departure. Uses: – 7. The Car Park determines the time spent and reports to the SP_BillingService. Uses: – 8. Use case ends. Uses: –

POST CONDITION CONSTRAINT
The time spent in the car park is known.

3.3.3.6.4 UC-06.3*:* Register arrival and departure from charging spot

The time spent in the charging spot is automatically determined by registering the arrival and departure time.

PRE-CONDITION CONSTRAINT
The vehicle entered the Car Park.
The Vehicle received entrance permission.

SCENARIOS
Basic Path. Similar to UC-6.2, the time spent of the Vehicle at an EV-Charging Station must be determined. To determine the duration, the EV-Charging Station registers the time of arrival and departure of the Vehicle. The arrival and departure times are reported to the Car Park, which in turn determines the time spent at an EV-Charging Station. The duration is then reported to the billing service.

SCENARIOS

1. <extend> UC-06.2
   Uses: –
2. The Vehicle enters the EV-Charging Station.
   Uses: –
3. The EV-Charging Station reports the time of arrival to the Car Park.
   Uses: –
4. The Vehicle charges.
   Uses: –
5. The Vehicle departs from the EV-Charging Station.
   Uses: –
6. The EV-Charging Station reports time of departure to the Car Park.
   Uses: –
7. The Car Park determines the time spent and reports to the SP_BillingService.
   Uses: –
8. The Vehicle leaves the CarPark.
   Uses: –

Alternate: *8a*. Continued parking (w/o charging)

9. Use case ends.
   Uses: –

Alternate. Continued parking (w/o charging)

1. The Vehicle moves to another parking lot.
   Uses: –
2. Use case ends.
   Uses: –

POST CONDITION CONSTRAINT

The time spent at the EV-Charging Station is known

3.3.3.7 UC-07: Camera-based in-Car Park positioning

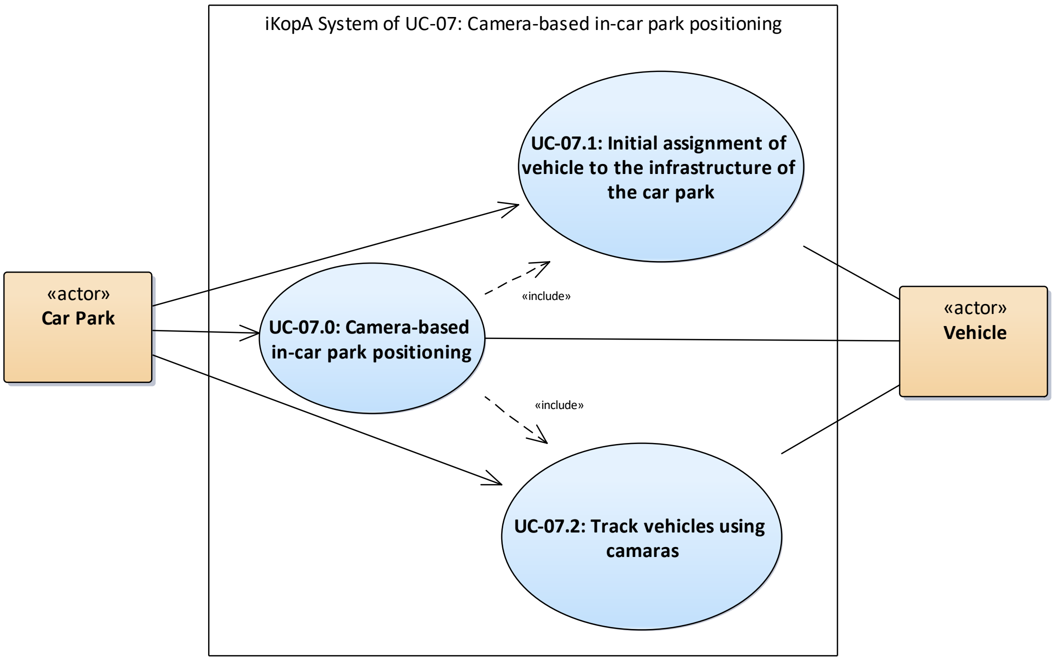

iKopA System of UC-07: Camera-based in-car park positioning
UC-07.1: Initial assignment of vehicle to the infrastructure of the car park
«actor»
Car Park
UC-07.0: Camera-based in-car park positioning
«include»
«include»
«actor»
Vehicle
UC-07.2: Track vehicles using camaras

Figure 13: UC-07: Camera-based in-car park positioning

3.3.3.7.1 UC-07.0: Camera-based in-Car Park positioning

The position data of the Vehicle in enhanced by combining it with position information created by the Car Parks camera system.

SCENARIOS

Basic Path.

This use case tracks the autonomous Vehicle in the Car Park and provides it with precise position information as a GPS supplement/replacement. This information is necessary to improve the internal sensor information of the vehicle with additional information received by the camera system of the Car Park.

This use case will be invoked by use case 05 "Park (partly) automated at charger". At the beginning, the lane cameras capture the vehicle, which is waiting in front of the Car Park Barrier. In the following step, the captured image of the vehicle will be assigned to the authenticated vehicle, which got the entrance permission. The camera system pursues the moving vehicle in a running loop and send the position data back to the car. This process continues about every 100 ms until the car reaches its final charging or parking position.

1. Use case 07.1 “Initial assignment of vehicle to the infrastructure of the car park" will be invoked.
   Uses:
2. Use case 07.2 "Track vehicles using cameras" will be invoked.
   Uses:
3. Use case ends.
   Uses:

3.3.3.7.2 UC-07.1: Initial assignment of vehicle to the infrastructure of the Car Park

The optically captured vehicle at the entrance of the Car Park is assigned to the authenticated Vehicle connected via V2X communication.

SCENARIOS

Basic Path.

In this initial step, the Car Park sets up an assignment between the Vehicles, which is waiting at the barrier of the Car Park (captured by the lane cameras) and the Vehicle, which is successfully registered via the V2X communication to the Car Park. The assignment procedure is based on the following concept. First, the Car Park classifies the object at the entrance barrier as a Vehicle. In the following step, the Car Park determines the current position of the Vehicle in front of the Car Park. Finally, the Car Park assigns the vehicle captured by the camera system in front of the Car Park to the Vehicle-ID of the vehicle, which got the entrance permission via V2X connection.

1. Car Park classifies the object at the Car Park Barrier as a Vehicle.
   Uses: –
2. Car Park determines the current position of the Vehicle in front of the Car Park.
   Uses: Tracking Camera System
3. Car Park assigns the Vehicle in front of the Car Park to the Vehicle-ID of the Vehicle, which got entrance permission via V2X connection.
   Uses: –
4. Use case ends.
   Uses: –

3.3.3.7.3 UC-07.2: Track vehicles using cameras

The moving vehicle is tracked by the camera system.

SCENARIOS

Basic Path.

The aim of this sub-use case is to provide the autonomously driving Vehicle with highly accurate and up-to-date position data captured by the camera system. This process will run in a loop so that about every 100 ms a new position will be sent to the vehicle. The loop will stop when the vehicle reaches its charging spot or, in the return case, the Car Park Barrier.

1. Car Park tracks the position of the considered Vehicle every 100ms.
   Uses: Tracking Camera System
2. Car Park transmits the position to the assigned Vehicle.
   Uses: Car Park RSU, Vehicle V2X OBU
3. Use case ends.
   Uses: –

3.3.3.8 UC-08: Get access to parking lot via RFID Identification

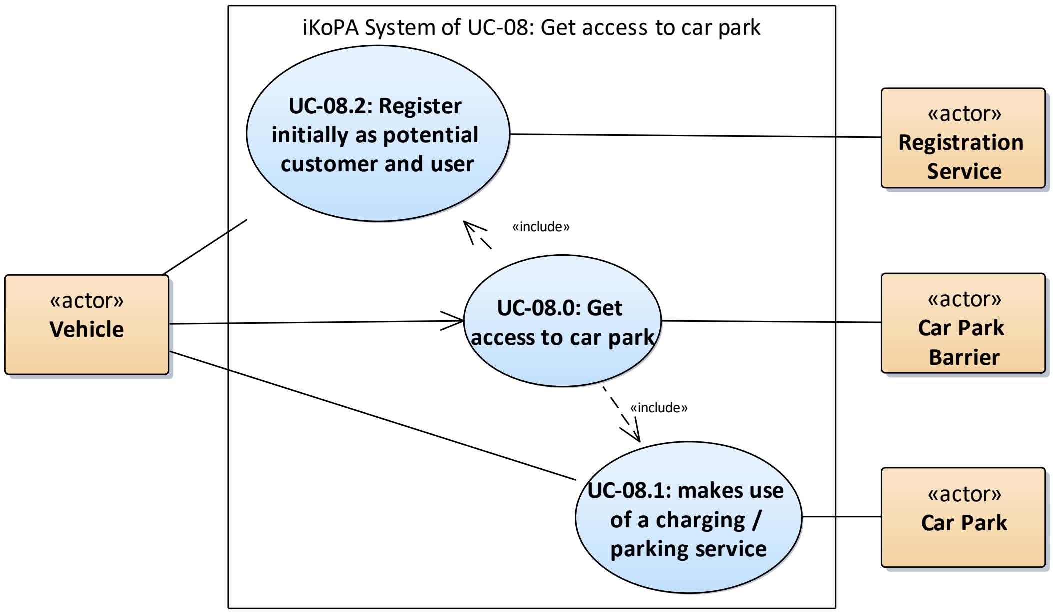

iKoPA System of UC-08: Get access to car park
UC-08.2: Register initially as potential customer and user
«include»
«actor» Vehicle
UC-08.0: Get access to car park
«include»
UC-08.1: makes use of a charging / parking service
«actor» Registration Service
«actor» Car Park Barrier
«actor» Car Park

Figure 14: UC-08: Get access to parking lot

3.3.3.8.1 UC-08.0: Get access to Car Park

The Car Park Barrier checks a Vehicle's identification and granting access to the Car Park only if the identity of the Vehicle's RFID tag matches an entry of a dynamic white list of accepted vehicles.

SCENARIOS
Basic Path. The access to the Car Park is granted based on the following RFID treatment: A Vehicle approaches a Car Park with its dynamic RFID license plate registered in a local white list. The RFID reader at the car park checks the RFID license plate of vehicle. The reader confirms the RFID tag as valid by checking against a white list received from the cloud, stored locally, or communicated during the reservation. The Car Park barrier opens up the way for Vehicle whereupon the Vehicle enters the Car park. Thereafter, the Vehicle can drive to the assigned parking lot. 1. UC-08.1: Usage of a charging / parking service Uses: – 2. UC-08.2: Register initially as potential customer and User Uses: – 3. Use case ends. Uses: –

3.3.3.8.2 UC-08.1: Usage of charging / parking service

The Vehicle has access to Car Park. This is signaled by a barrier opening and/or a traffic light showing green. The vehicle charges at an EV-Charging Station and/or parks on an assigned or available parking lot by means of automatic parking

PRE-CONDITION CONSTRAINT
The vehicle has a valid reservation for the parking lot.
The RFID reader of the Car Park has access to the reservation data.

SCENARIOS

Basic Path.
After identification, the Vehicle can access the Car Park with the following sequence of actions: the vehicle approaches the parking lot with the RFID license. The RFID reader at the Car Park checks the RFID license plate of the Vehicle against its white list or a list communicated during a reservation procedure. The Vehicle charges and/or parks, which ends the use case.

1. Vehicle approaches parking lot RFID reader with the Vehicle RFID license.
   Uses: –
2. Parking lot RFID reader at the Car Park checks the vehicle RFID license plate of the Vehicle.
   Uses: –
3. Use case ends.
   Uses: –

POST CONDITION CONSTRAINT
The reservation status is updated in the reservation backend server.

3.3.3.8.3 UC-08.2: Register initially as potential customer and User

Before a customer can reserve a parking lot, it has to register as a potential customer. After that, it can identify and is allowed to enter.

PRE-CONDITION CONSTRAINT
The Vehicle has a valid reservation for car parking lot.
RFID reader of the Car Park has access to the registration data.

SCENARIOS

Basic Path.

The vehicle needs to be registered as follows: The user registers for the service and receives a programmable RFID tag as well as a NFC Tag. The RFID tag is for the vehicle, the NFC Tag is for pairing the User/smartphone to the Vehicle. This RFID tag is used for the reservation using the smartphone in proximity to NFC. It is then used for get access using the RFID reader at the barrier in distance to the RFID tag.

1. Parking lot RFID reader confirms the vehicle RFID license plate tag as valid.
   Uses: –

Exception: *1a*. Authentication invalid

Exception: *1b*. Technical issues

2. Reservation Service opens up the way for vehicle.
   Uses: –
3. Vehicle drives onto assigned parking lot.
   Uses: –
4. Use case ends.
   Uses: –

Exception. Authentication invalid

1. Parking lot RFID reader denies entry, because the authentication is invalid.
   Uses: –
2. Parking lot barrier stays in the blocking position.
   Uses: –
3. Parking lot RFID reader indicates that the authentication is invalid by showing e.g. a red light.
   Uses: –
4. Use case ends.
   Uses: –

Exception. Technical issues

1. Parking lot RFID reader denies the RFID tag, because the system has technical issues.
   Uses: –
2. Parking lot barrier stays in the blocking position.
   Uses: –
3. Parking lot RFID reader does not show any response to the RFID tag.
   Uses: –
4. Use case ends.
   Uses: –

POST CONDITION CONSTRAINT

The reservation status is updated in the reservation backend server.

3.3.3.9 UC-09: Communicate with charger & charge

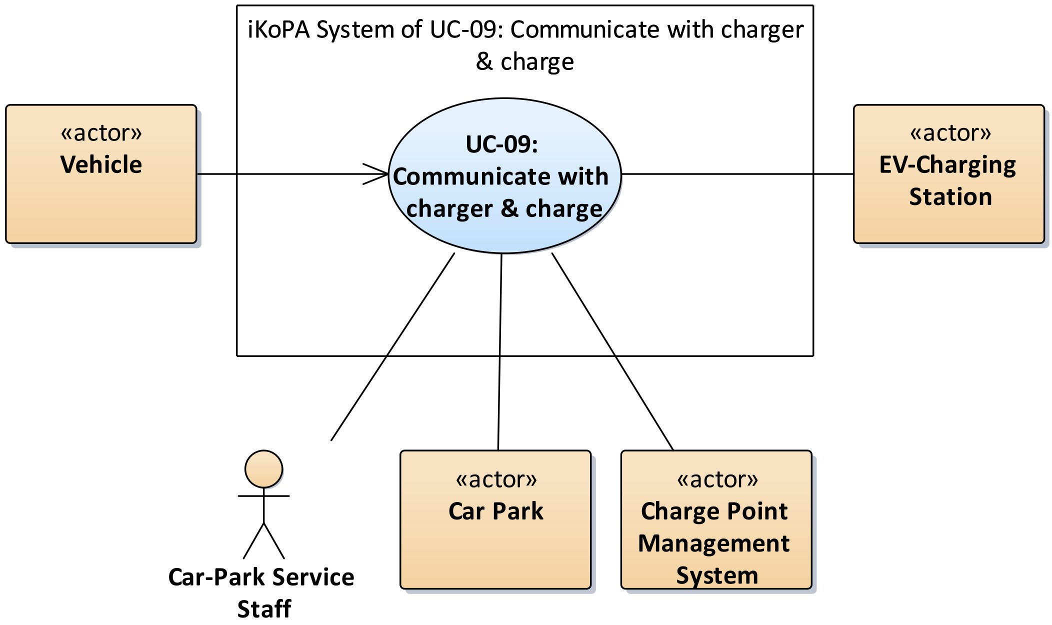

iKoPA System of UC-09: Communicate with charger & charge
«actor» Vehicle
UC-09: Communicate with charger & charge
«actor» EV-Charging Station
Car-Park Service Staff
«actor» Car Park
«actor» Charge Point Management System

Figure 15: UC-09: Communicate with charger & charge

3.3.3.9.1 UC-09: Communicate with charger & charge

The Vehicle is connected to the EV-Charging Station and the charging process is taking place.

PRE-CONDITION CONSTRAINT
For Service Provider path: User has (registered) relation to Service Provider. The User has a contract with a Service Provider. The User has a valid reservation for an appointed time slot of the charging spot.
For Service Provider path with Car Park: Service Provider and Car Park operator have business relation. Car Park operator and Service Provider must have a relation to allow reservations or billing information to be exchanged and to allow the User to access the parking lot with the reserved EV-Charging Station.

SCENARIOS
Basic Path. Vehicle has arrived at the destination, which has a dedicated charging spot for electric vehicles. 1. Vehicle is parking in the reserved spot with EV-Charging Station. Uses: – Alternate: *1a*. Involve Service Provider (and Car Park) - Part 1

SCENARIOS

2. Vehicle authenticates to the EV-Charging Station.

Uses: –

3. Charging Point Management System asks Car-Park Service Staff to connect Vehicle.

Uses: –

4. Car-Park Service Staff connects Vehicle and the charging process is starting.

Uses: –

5. Charging is in process (EV-Charging Station reports status to Charge Point Management System).

Uses: –

6. Car-Park Service Staff disconnects Vehicle after charging is finished / on request that User wants to collect the Vehicle.

Uses: –

7. EV-Charging Station reports service consumption information to Charge Point Management System.

Uses: –

Alternate: *7a*. Involve Service Provider (and car park) - Part 2

8. Payment process (direct on site or via Service provider) is treated through the Charge Point Management System and its connection to the Car Park control.

Uses: –

9. Vehicle is returned to User

Uses: –

10. Use Cases ends

Uses: –

Alternate. Involve Service Provider (and car park) - Part 1

1. User is checking for free spaces and books a charging space with his provider for a certain charging point (in a certain Car Park).

Uses: –

2. Electric mobility preservation systems execute reservation locally (and prepare to give User access to the Car Park).

Uses: –

3. User arrives with his Vehicle (at the Car Park and gets entry permission) and starts (autonomous) parking the Vehicle at the reserved charging point.

Uses: –

Alternate. Involve Service Provider (and car park) - Part 2

1. Charge Point Management System takes care of billing.

Uses: –

2. Car park supports leave of user Vehicle by allowing to leave at the exit barrier.

Uses: –

3. Charge Point Management System use the B2B service contracting relation for clearing / billing.

Uses: –

4. End of use case path / back to Basic Path.

Uses: –

3.3.3.10 UC-10: Receive state of charge of Vehicle

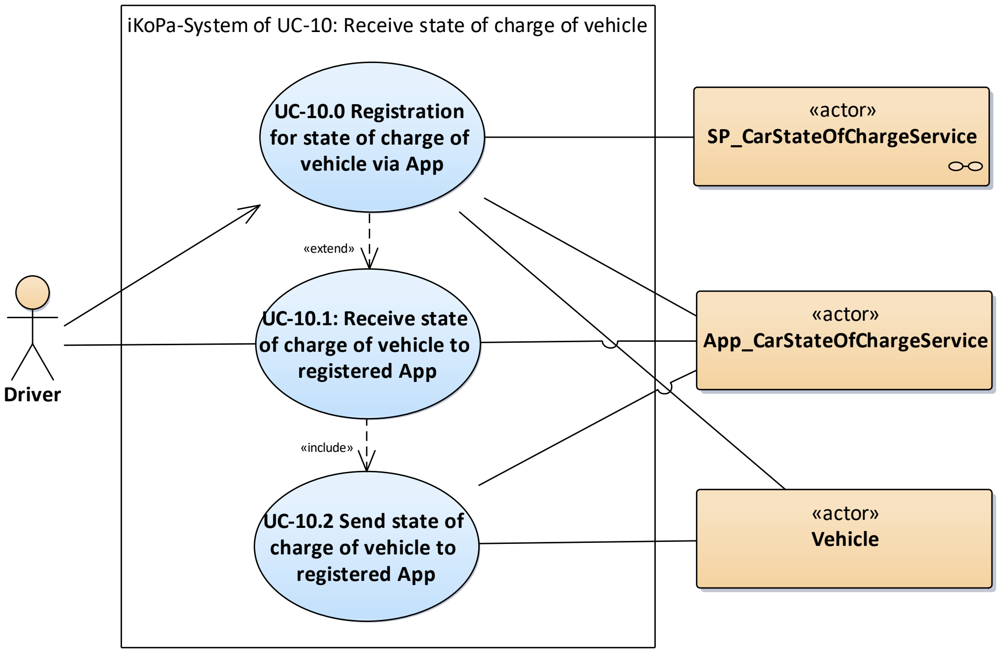

iKoPa-System of UC-10: Receive state of charge of vehicle
UC-10.0 Registration for state of charge of vehicle via App
«extend»
UC-10.1: Receive state of charge of vehicle to registered App
«include»
UC-10.2 Send state of charge of vehicle to registered App
Driver
«actor»
SP_CarStateOfChargeService
«actor»
App_CarStateOfChargeService
«actor»
Vehicle

Figure 16: UC-10: Receive state of charge of vehicle

3.3.3.10.1 UC-10.0*:* Registration for state of charge of vehicle via App

The Driver sends (via App_CarStateOFChargeService) registration to receive state of charge (SOC) of the vehicle.

SCENARIOS

Basic Path.

In this path, the Driver tries to register for the service via smartphone. The Service Provider confirms or rejects the registration.

1. Driver sends registration for service of SP_CarStateofChargeService via App_CarStateOfChargeService.
   Uses: –
2. SP_CarStateOfChargeService receives and checks registration.
   Uses: –
3. SP_CarStateOfChargeService send confirmation to App_CarStateOfChargeService and Vehicle.
   Uses: –

Alternate: *3a*. Rejection

4. App_CarStateOfChargeService receives confirmation.
   Uses: –
5. App_CarStateOfChargeService informs Driver.
   Uses: –
6. Use case ends
   Uses: –

SCENARIOS

Alternate. Rejection

1. SP_CarStateOfChargeService send rejection to App_CarStateOfChargeService.
   Uses: –
2. App_CarStateOfChargeService receive rejection.
   Uses: –
3. App_CarStateOfChargeService informs Driver.
   Uses: –
4. Use case ends.
   Uses: –

3.3.3.10.2 UC-10.1: Receive state of charge of vehicle to registered App

The driver receives state of charge (SOC) of the vehicle on his cell phone.

SCENARIOS

Basic Path. Basic Path

Driver receives the state of charge via smartphone.

1. App_CarStateOfChargeService receives "state of charge".
   Uses: –
2. App_CarStateOfChargeService notifies the Driver.
   Uses: –
3. Use case ends.
   Uses: –

3.3.3.10.3 UC-10.2: Send state of charge of vehicle to registered App

The vehicle sends the state of charge (SOC) to the APP_CarStateOfChargeService.

SCENARIOS

Basic Path. Basic Path

Vehicle sends the state of charge to the smartphone.

1. Vehicle sends "state of charge of vehicle" to registered App_CarStateOfChargeService.
   Uses: –
2. Use case ends.
   Uses: –

3.3.3.11 UC-11: Request vehicle

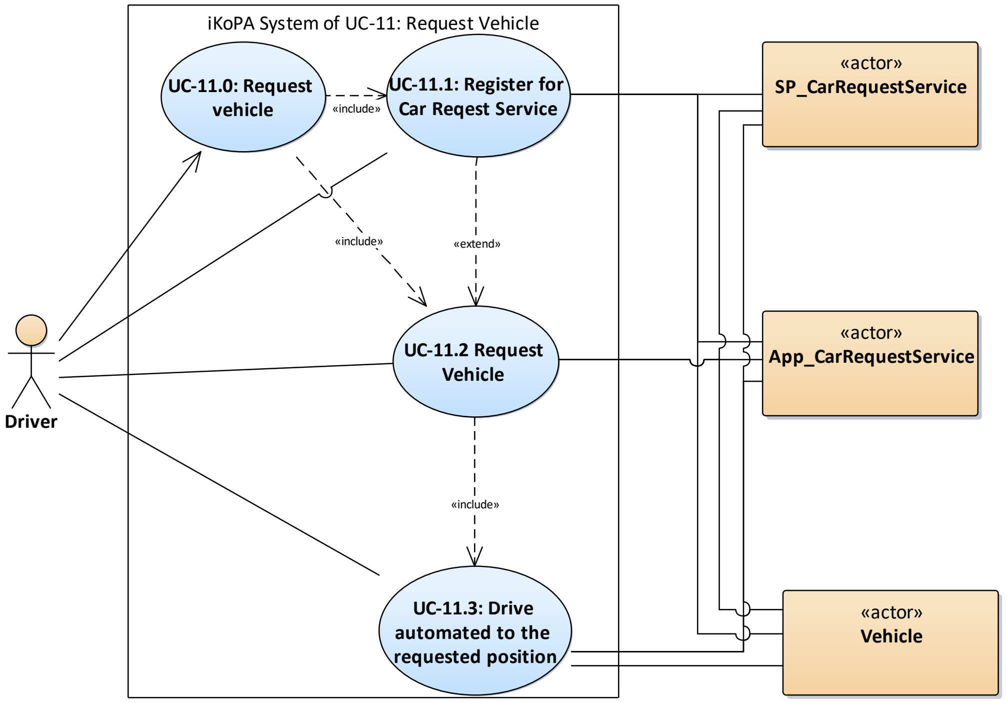


Figure 17: UC-11: Request vehicle

3.3.3.11.1 UC-11.0: Request vehicle

The Driver wants to be picked up at a specific position in the Car Park. Therefore, a request needs to be initiated to the Vehicle.

SCENARIOS

Basic Path. Basic Path

To be picked up by the Vehicle, the Driver requests the Vehicle to a specific position in or in front of the Car Park. This request is initiated via a personal device; most likely a smartphone. After an authorization check, the Vehicle will automatically drive from its current position (in most cases a parking lot) to the request position of the Driver. This could be either a defined area, parking space or a specific position in the Car Park.

1. <include> UC-11.1: Register for Car Request Service
   Uses: –
2. <include> UC-11.2 Request Vehicle
   Uses: –
3. Use case ends.
   Uses: –

3.3.3.11.2 UC-11.1: Register for car request service

The Driver and its Vehicle register to be able to use the service.

SCENARIOS

Basic Path. Basic Path

To request the Vehicle, the Driver registers the Cehicle and his personal device to the SP_CarRequestService, which handles authorization of the service usage and the request authorization.

1. Driver and Vehicle register at SP_CarRequestService.
   Uses: –
2. SP_CarRequestService receives registration.
   Uses: –
3. SP_CarRequestService checks authorization for service usage.
   Uses: –
4. SP_CarRequestService sends registration confirmation to App_CarRequestService and Vehicle.
   Uses: –

Alternate: *4a*. Not authorized

5. App_CarRequestService informs Driver about registration confirmation.
   Uses: –
6. Use case ends.
   Uses: –

Alternate. Not authorized

1. SP_CarRequestService sends registration rejection to App_CarRequestService and Vehicle.
   Uses: –
2. App_CarRequestService informs Driver about registration rejection.
   Uses: –
3. Use case ends.
   Uses: –

3.3.3.11.3 UC-11.2: Request Vehicle

This is the process of requesting the Vehicle to a specific position.

SCENARIOS

Basic Path.

The Driver requests the vehicle via the App_CarRequestService on his smartphone. The request authorization will be done by the SP_CarRequestService.

1. Driver initiates request via App_CarRequestService.
   Uses: –
2. App_CarRequestService sends request to the SP_CarRequestService.
   Uses: –

SCENARIOS

3. SP_CarRequestService checks for authorization for service usage.
Uses: –
4. SP_CarRequestService forwards message to Vehicle to drive to requested position.
Uses: –
Alternate: *4a*. Not authorized to use service
5. Vehicle checks request for authorization.
Uses: –
6. Vehicle checks for possible route.
Uses: –
Alternate: *6a*. Not authorized to request Vehicle
7. Vehicle send confirmation to Driver via SP_CarRequestService.
Uses: –
Alternate: *7a*. No possible route found
8. UC-UC-11.2: Drive automated to the requested position.
Uses: –
9. Use case ends.
Uses: –

Alternate. Not authorized to use service

1. SP_CarRequestService sends service authorization rejection to App_CarRequestService.
Uses: –
2. App_CarRequestService informs Driver about service authorization rejection.
Uses: –
3. Use case ends.
Uses: –

Alternate. Not authorized to request Vehicle

1. Vehicle sends Vehicle authorization rejection to SP_CarRequestService.
Uses: –
2. SP_CarRequestService sends Vehicle authorization rejection to App_CarRequestService.
Uses: –
3. App_CarRequestService informs Driver about Vehicle authorization rejection.
Uses: –
4. Use case ends.
Uses: –

Alternate. No possible route found

1. Vehicle sends information that no possible route was found to SP_CarRequestService.
Uses: –
2. SP_CarRequestService sends information that no possible route was found to App_CarRequestService.
Uses: –
3. App_CarRequestService informs Driver about that no possible route was found by the vehicle.
Uses: –
4. Use case ends.
Uses: –

3.3.3.11.4 UC-11.3: Drive automated to the requested position

If the request of the Vehicle was authorized, the vehicle starts driving to the requested position automatically.

SCENARIOS

Basic Path.
The Vehicle drives automatically to the requested position to pick up the Driver.

1. Vehicle drives automatically to requested position.
   Uses: –
Alternate: *1a*. Not possible to drive automated to position
2. Vehicle parks/holds at requested position.
   Uses: –
Alternate: *2a*. Not possible to park/hold at requested position
3. Use case ends.
   Uses: –

Exception. Not authorized

1. Inform Driver about rejection.
   Uses: –
2. Post misbehavior.
   Uses: –

Alternate. Not possible to drive automated to position

1. Vehicle sends information to SP_CarRequestService about problems driving automatically.
   Uses: –
2. SP_CarRequestService send information to App_CarRequestService about problems Vehicle driving automated.
   Uses: –
3. App_CarRequestService informs Driver about problems Vehicle driving automatically.
   Uses: –
4. Use case ends.
   Uses: –

Alternate. Not possible to park/hold at requested position

1. Vehicle sends information to SP_CarRequestService about problems parking/holding at requested position.
   Uses: –
2. SP_CarRequestService send information to App_CarRequestService about the Vehicle not being able to park/hold at the requested position.
   Uses: –
3. App_CarRequestService informs Driver that the Vehicle is not able to park/hold at the requested position.
   Uses: –
4. Use case ends.
   Uses: –

3.3.3.12 UC-12: Drive informed and safe

This use case combines the users need to be informed and to stay safe during the voyage. Both require a steady stream of information, to reach the vehicle. Multiple carriers are used to accomplish this need for information supply, but if all means fail, this situation is still part of the management within the use case. The user shall be aware of his information status at all time, to allow him trusting the information service to warn him if there are known issues, relevant to his voyage.

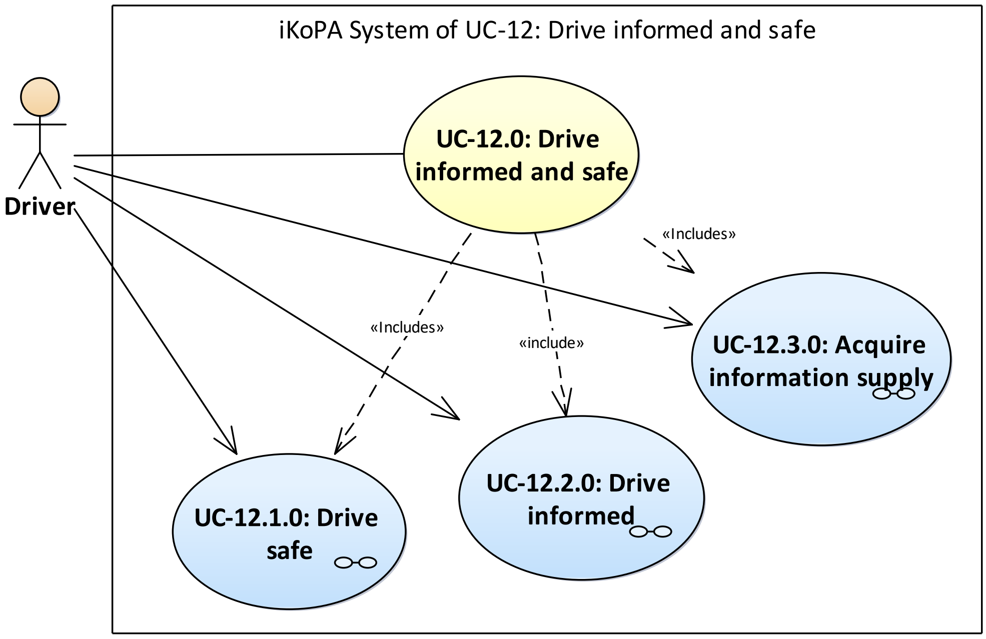

iKoPA System of UC-12: Drive informed and safe
Driver
UC-12.0: Drive informed and safe
«Includes»
«include»
«Includes»
UC-12.3.0: Acquire information supply
UC-12.2.0: Drive informed
UC-12.1.0: Drive safe

Figure 18: UC-12: Drive informed and safe

3.3.3.12.1 UC-12.1.0: Drive safe

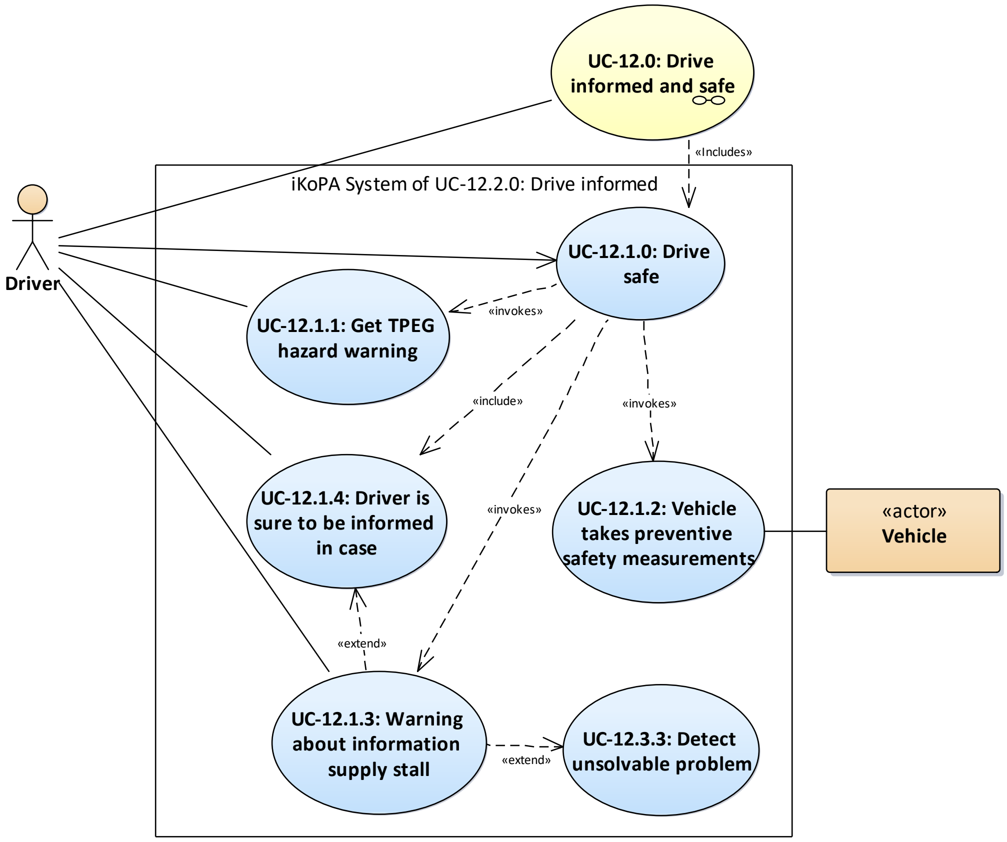

UC-12.0: Drive informed and safe
«Includes»
iKoPA System of UC-12.2.0: Drive informed
Driver
UC-12.1.0: Drive safe
«invokes»
UC-12.1.1: Get TPEG hazard warning
«include»
«invokes»
UC-12.1.4: Driver is sure to be informed in case
«invokes»
UC-12.1.2: Vehicle takes preventive safety measurements
«actor»
Vehicle
«extend»
UC-12.1.3: Warning about information supply stall
«extend»
UC-12.3.3: Detect unsolvable problem

Figure 19: UC-12.1.0: Drive safe

The Driver is provided with any available safety relevant information quickly. In case this is not guaranteed, he gets a warning. If a relevant hazard is detected, the Driver and the Vehicle subsystems are alerted to take preventive measures in time.

SCENARIOS

Basic Path.

Both the Vehicle systems and the Driver are assured and informed, that critical information, such as hazard warnings, are provided in time. This is the recommended condition, while mostly no such critical information is received. If both, the constant information supply and the lack of critical information are given, nothing is triggered and no action is required.

1. Driver is sure to be informed in case of a relevant hazard.
   Uses: UC-12.1.4: Driver is sure to be informed in case of a relevant hazard

Exception: *1a*. Information supply stalls

2. If nothing happens and all is well, the driver is not bothered with any details.
   Uses: –

Alternate: *2a*. Relevant information becomes available

3. Driver reaches his destination.
   Uses: –

SCENARIOS

4. Use case ends.
    Uses: –

Alternate. Relevant information becomes available

As soon as new information, that is safety relevant, becomes available, both the Driver and the Vehicle systems are informed, to allow them to take action accordingly. Both updates of previous information and new events are regarded as "new information" in this case. Additionally, even the cancellation of previously issued warnings will be such new information. All the information is forwarded as events that will work standalone and can be related to each other. A typical example is the information about an obstacle or icy patches on the road. This critical information is given to the Driver and the Vehicle systems. The intention is that they will react in a manner that is suitable for the specific event and danger. For the given example, this may be the reduction of speed. While the critical information is delivered it is not enforced that Drivers or other Vehicle systems react upon them in a certain way. This will be the responsibility of the receiver of such safety triggers.

1. Relevant information about hazards ahead becomes available.
    Uses: –
2. The Vehicle takes preventive safety measures.
    Uses: UC-12.1.2: Vehicle takes preventive safety measure
3. The driver is informed about a TPEG TEC Message with hazard warning.
    Uses: UC-12.1.1: Get TPEG TEC Message with hazard warning
4. Use case ends.
    Uses: –

Exception. Information supply stalls

In the case of a stall in the information supply, the system detects it and will information both the Driver and the other vehicle systems. This is done by triggering an event, very similar to when a hazard warning is received. However, the semantics of it will be different, as it represents no direct danger, but an uncertainty whether there might be such dangers that cannot be communicated to the Vehicle, at the moment. A typical example would be a Driver on the wrong side of the road that is well known to the police and the information supplier. A vehicle that is in a dead spot and may not receive any message about this danger. As the lack of information does not necessarily mean, that there is a danger, but also does not mean, that there is no danger, the reaction to this lack may be more generic and could include improved attention.

1. Constant information supply stalls. New information about hazards will not become available in time.
    Uses: –
2. The Driver is informed about an information supply stall.
    Uses: UC-12.1.3: Warning about information supply stall
3. Use case ends.
    Uses: –

CONSTRAINTS

Invariant. The driver has the desire to "drive safe".

3.3.3.12.1.1 UC-12.1.1: Get TPEG hazard warning

If an information about dangers ahead becomes relevant or available, the Driver is informed and shall react accordingly

RESPONSIBILITIES (INTERNAL REQUIREMENTS)

Functional. Possibility to display information to the User.

SCENARIOS

Basic Path.

As soon as new information classified as a warning of a hazard is received, it is forwarded to other systems and to the Driver, to assure awareness of the hazard. The driver then decides by itself which action to take.

1. The Driver gets an alert to inform him about dangers ahead that might be relevant for him.
   Uses: –
2. The Driver decides which action to take, and takes this action.
   Uses: –
3. Use case ends.
   Uses: –

CONSTRAINTS

Invariant. Information about a possibly relevant hazard ahead is present-

3.3.3.12.1.2 UC-12.1.2: Vehicle takes preventive safety measures

According to information about dangers ahead, the system of the Vehicle take preventive measures to counteract.

RESPONSIBILITIES (INTERNAL REQUIREMENTS)

Functional. There needs to be an interface to the Vehicle subsystems to allow them to listen to hazard warnings.

SCENARIOS

Basic Path.

If a hazard warning becomes relevant or available, a general event for specific subsystems in the Vehicle is triggered, to allow appropriate automatic preventive measurements. E.g. traction control adaption to icy patches ahead, reduction of vehicle speed by throttling the engine power in advance, activating sidelights if visibility is reduced, inform brake assistant system, that a sudden stop is more likely, etc... This depends strongly on the integrated automatic subsystems of the Vehicle and the degree of driving autonomously.

SCENARIOS

1. The Vehicle subsystems are informed about dangers ahead that might be relevant.
   Uses: Basic Path
2. The Vehicle subsystems decide and take the action they find suitable.
   Uses: Basic Path
3. Use case ends.
   Uses: Basic Path

CONSTRAINTS

Invariant. Information about a possibly relevant hazard ahead is present

3.3.3.12.1.3 UC-12.1.3: Warning about information supply stall

If the supply with information updates stalls, both the Driver and other systems need to be informed of this, as this is reduces the service quality.

RESPONSIBILITIES (INTERNAL REQUIREMENTS)

Functional. Possibility to display information to the User.

SCENARIOS

Basic Path.

If no constant stream of safety relevant information can be guaranteed, this is detected and the Driver is informed that safety might be reduced because of this lack of knowledge about hazards ahead. This condition is avoided by the system, by using all available sources of information. All DAB, ITS G5 and Internet (via mobile networks) are used, usually without consulting the Driver. Only if all these approaches fail, this use case comes into action. The driver is NOT meant to fix this condition (like an RDS-TP-loss warning beep), but is asked to consider driving more carefully.

1. Driver gets a warning, that he might not be informed in case relevant information about dangers ahead becomes available.
   Uses: –
2. As soon as information supply is reestablished, he gets an optional information that the safe driving is restored.
   Uses: –
3. Use case ends.
   Uses: –

CONSTRAINTS

Invariant. A situation with an insufficient information supply is present.

3.3.3.12.1.4 UC-12.1.4: Driver is sure to be informed of a relevant hazard

The Driver knows that he will be informed about dangers ahead, and his Vehicle will automatically take preventive measurements, if relevant information becomes available. Part his trust in the information service is the knowledge, that the system will inform him about any change in the information status.

RESPONSIBILITIES (INTERNAL REQUIREMENTS)
☑ Functional. Method to acquire constantly updated traffic information must be available.

SCENARIOS

Basic Path.

The Driver has trust in the information service to warn him, in case relevant information becomes available. As soon as the information status does change he is informed.

1. Driver knows that he will be informed about possible hazards, and his Vehicle will automatically take preventive measurements, if relevant information becomes available.

    Uses: –

2. If this status changes, the driver is informed.

    Uses: –

3. Driver is informed about an information supply stall.

    Uses: UC-12.1.3: Warning about information supply stall

4. Use case ends.

    Uses: –

CONSTRAINTS
Invariant. A stable information supply is established.

3.3.3.12.2 UC-12.2.0: Drive informed

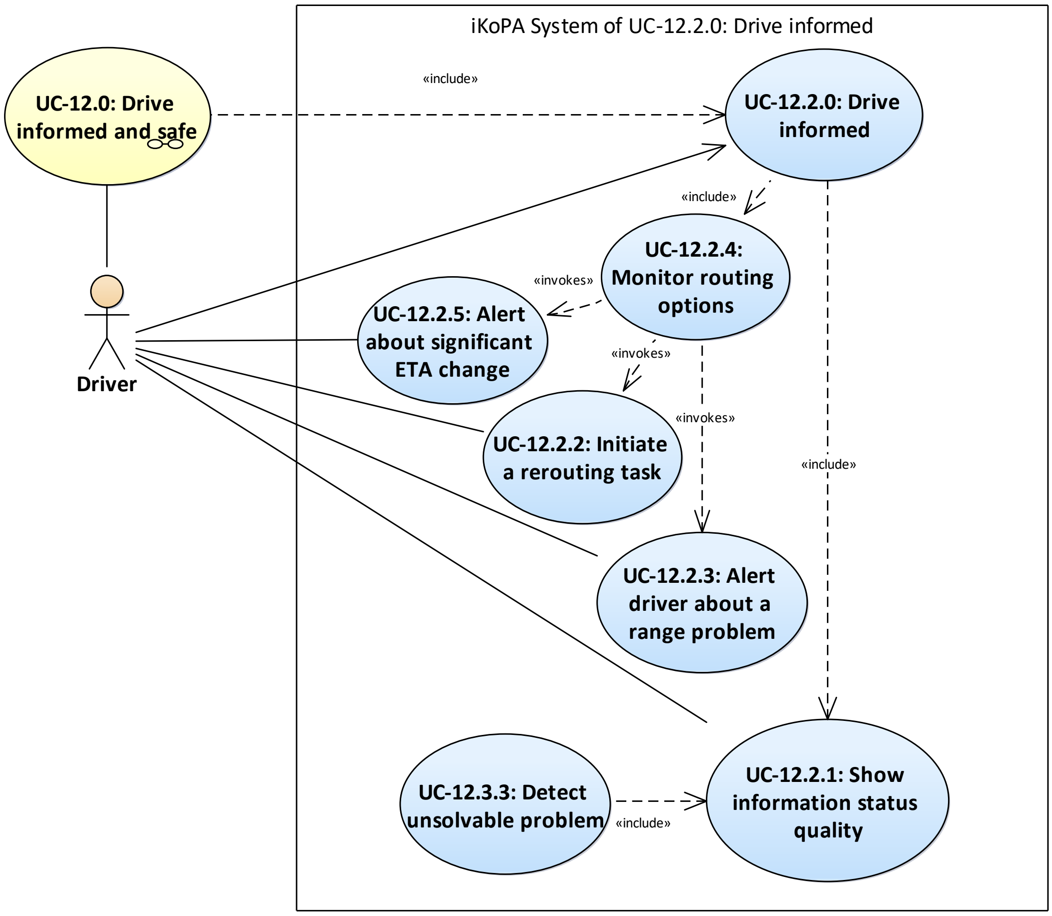

iKoPA System of UC-12.2.0: Drive informed
UC-12.0: Drive informed and safe
«include»
UC-12.2.0: Drive informed
«include»
UC-12.2.4: Monitor routing options
«invokes»
UC-12.2.5: Alert about significant ETA change
«invokes»
Driver
UC-12.2.2: Initiate a rerouting task
«invokes»
«include»
UC-12.2.3: Alert driver about a range problem
UC-12.3.3: Detect unsolvable problem
«include»
UC-12.2.1: Show information status quality

Figure 20: UC-12.2: Drive informed

The Driver gets optional information about the estimated arrival time. He is informed about drastic changes, a potential need to change the route or any problem with the available driving range (dependent from the battery charging state).

SCENARIOS
Basic Path. The Driver has the constant option to get information of the estimated arrival time and any obstacles on its way. He is aware whether the currently followed route is still the best option or if there is new information available, that recommends a different route. For example, this may be the case if there is huge traffic jam detected on its way, while alternative routes seem to stay clear. In most cases, a roadblock will be a non-optional reason for a re-routing, except for a situation where the remaining battery power will not be sufficient to drive the detour and it is possible to re-charge the batteries on this way. These calculations use the available information received through different communication technologies and by reading the onboard car sensors. In effect, the driver shall be presented the best available information, to decide the next steps while trying to reach the desired target.

SCENARIOS

1. The Driver stays informed about the current situation.
   Uses: –
2. Monitor routing options (different route alternatives).
   Uses: UC-12.2.4: Monitor routing options
3. Show information status quality.
   Uses: UC-12.2.1: Show information status quality
4. Driver reaches his destination.
   Uses: –
5. Use case ends.
   Uses: –

CONSTRAINTS

Invariant. The user has the desire to "drive informed".

3.3.3.12.2.1 UC-12.2.1: Show information status quality

No alert is triggered, but the information status quality is shown to the User, without bothering him with technical details.

RESPONSIBILITIES (INTERNAL REQUIREMENTS)

Functional. Possibility to display information to the User

PRE-CONDITION CONSTRAINT

An updated information status quality has become available

SCENARIOS

Basic Path.

The information status quality is offered to the User, without bothering him with details and without catching the awareness. The User just may look it up, if he feels the need to do so. Technical details are avoided and just a general “ok” information is provided.

1. The information status quality is shown to the User, without urging him to look at it
   Uses: –
2. An unimposing symbol shows a good or sufficient status.
   Uses: –

Alternate: *2a*. Bad quality

3. Driver reaches his destination.
   Uses: –
4. Use case ends.
   Uses: –

SCENARIOS

Alternate. Bad quality

1. Bad information status quality is shown with a more obvious symbol (e.g. red) to given an optional hint that information supply has stalled or is below the required minimum.
   Uses: –
2. If the quality increases, the original symbol for good or sufficient information status quality is restored.
   Uses: –
3. The Driver reaches his destination.
   Uses: –
4. Use case ends.
   Uses: –

3.3.3.12.2.2 UC-12.2.2: Initiate a rerouting task

If information becomes available that shows that the previously followed route is no longer the best option a decision and rerouting is triggered.

PRE-CONDITION CONSTRAINT

A primary route has been set (as a base to calculate a delta against).

A route, which is better than the primary route, has been identified.

SCENARIOS

Basic Path.

If information becomes available that shows, that the currently planned route is considerably slower than another route, a rerouting task is initiated. This activity is tightly entangled with the routing-system. According to the configuration and calculated situation, an automatic change of the routing may occur where the driver may or may not be explicitly informed. Alternatively, the driver is informed in advanced of the change and must conform it first.

1. According to current calculation, a new route is found, that has significant advantages over the original route.
   Uses: –
2. The User is informed about the new route and the advantages.
   Uses: –
3. The User accepts the new route.
   Uses: –

Alternate: *3a*. The User sticks to old route

Exception: *3b*. The User aborts routing

4. The new route is set as the designated route and the navigation hints are generated according to this new route.
   Uses: –

SCENARIOS

5. Use case ends.
   Uses: –

Alternate. The User sticks to old route

1. The User rejects the advice to follow a new route and keeps with the old route.
   Uses: –
2. Navigation hints are given according to old route.
   Uses: –
3. Use case ends.
   Uses: –

Exception. The User aborts routing

1. The User aborts routing and navigation (for the moment) completely.
   Uses: –
2. No further navigation hints are given and from now on, no route is designated, so no delta calculations are possible.
   Uses: –
3. Use case ends.
   Uses: –

3.3.3.12.2.3 UC-12.2.3: Alert driver about a range problem

If new information is received, that shows that the destination may not be reached by following the current route, due to a lack of energy, the driver is informed.

PRE-CONDITION CONSTRAINT

A range problem has been detected

SCENARIOS

Basic Path.

If information becomes available, that shows a potential problem with the available driving range of the Vehicles battery power, the Driver is alerted. He may get additional information to help him, with the crucial decision on how to proceed. A typical situation could be a roadblock ahead, when the destination is almost reached. If the battery power is already very low, a rerouting could consume too much energy to offer a certain arrival. However, waiting in a long lasting traffic jam, while lights and air-condition are on, could drain the battery too soon as well. Therefore, the Driver may decide to reduce power, search for a parking shop, navigate to a charging park or just take the risk.

1. The current calculation that takes the current traffic situation into account comes to the conclusion, that the remaining power in the batteries of the Vehicle might not be sufficient to reach the destination.
   Uses: –
2. The user is alerted about this situation.
   Uses: –

SCENARIOS

3. Different possible solutions might be offered, if available.
   Uses: –
4. The User decides which actions he likes to take.
   Uses: –
5. Use case ends.
   Uses: –

3.3.3.12.2.4 UC-12.2.4: Monitor routing options

Continuously recalculate routing options, by taking the current traffic situation into account, and compare with the currently designated and followed route to find significantly better routes and to detect upcoming range problems.

RESPONSIBILITIES (INTERNAL REQUIREMENTS)

☑ Functional. Method to (re-)calculate routing options must be available.

☑ Functional. Method to acquire constantly updated traffic information must be available.

SCENARIOS

Basic Path.

Repeated recalculations, using the most up to date information, scrutinize the current route and compare alternatives. Significant findings are reported to trigger actions, as soon as possible.

1. The current situation is constantly monitored, by repeatedly calculating the current and alternative routes.
   Uses: –
2. No significant changes or problems are found. The Driver is not informed or bothered.
   Uses: –

Alternate: *2a*. ETA changes significantly

Alternate: *2b*. Arrival has become uncertain because of a lack of range

Alternate: *2c*. A better route is found

3. The Driver reaches his destination.
   Uses: –
4. Use cases ends.
   Uses: –

Alternate. ETA changes significantly

1. A significant change in estimated arrival time (ETA) has been found, because recalculation with information about the current traffic situation shows new figures.
   Uses: –
2. The Driver is informed about this significant change.
   Uses: UC-12.2.5: Alert about significant ETA change
3. Use case ends.
   Uses: –

SCENARIOS

Alternate. A better route is found

1. A significantly better route has been found by recalculation that takes current information about the traffic situation into account.
   Uses: –
2. A rerouting is triggered.
   Uses: UC-12.2.2: Initiate a rerouting task
3. Use case ends.
   Uses: –

Alternate. Arrival has become uncertain because of a lack of range

1. The latest recalculation with current traffic information shows that it might take more energy to reach the destination than energy is still available in the batteries. The available driving range is not sufficient.
   Uses: –
2. The user is informed about this problem.
   Uses: UC-12.2.3: Alert driver about a range problem
3. Use case ends.
   Uses: –

CONSTRAINTS

Invariant. Updated information about the traffic situation is needed before a new calculation can be done.

Invariant. A primary route has been designated, to allow delta comparison against it.

3.3.3.12.2.5 UC-12.2.5: Alert about significant ETA change

The User (or vehicle subsystems) is alerted about a significant change of the estimated arrival time, which is a result of current routing calculation that takes into account the current traffic situation. This might be used to inform peers about the ETA change, change appointments or reservations or reconsider the whole travel plan.

PRE-CONDITION CONSTRAINT

A primary route is set (to allow delta calculations against).

A previously (or originally) calculated ETA is known.

A current calculation shows a significant difference to the previously calculated ETA.

SCENARIOS

Basic Path. Basic Path

As new information becomes available and the system learns that the estimated arrival time has changed, the user is informed to allow him to take according action

1. Current calculation shows a significant difference to the original estimated arrival time calculation.
   Uses: –
2. The Driver is informed about the significant change and the new estimated arrival time-
   Uses: –
3. The Driver takes action, as desired by him.
   Uses: –
4. Use case ends.
   Uses: –

3.3.3.12.3 UC-12.3.0*:* Acquire information

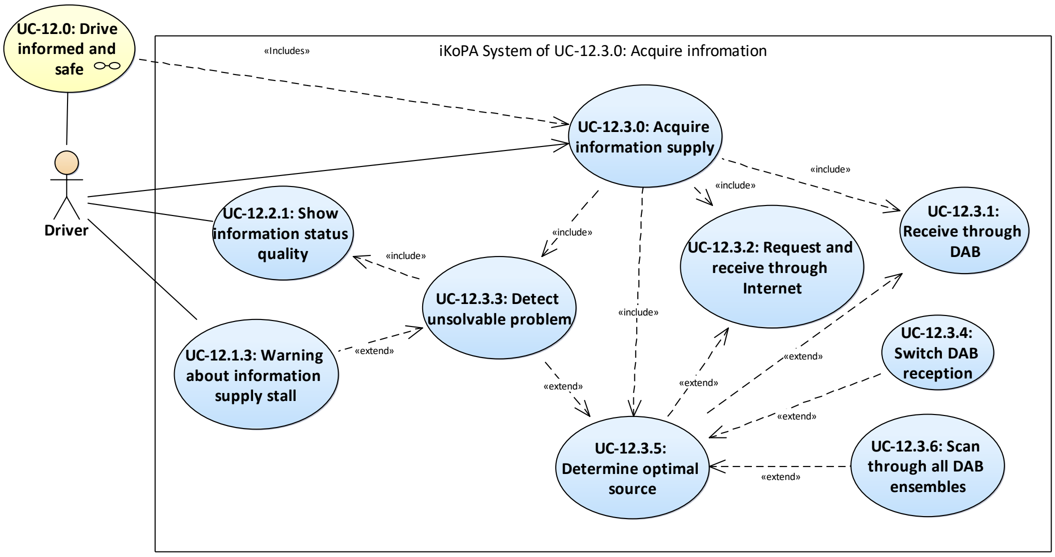

UC-12.0: Drive informed and safe
«Includes»
iKoPA System of UC-12.3.0: Acquire infromation
UC-12.3.0: Acquire information supply
«include»
«include»
UC-12.3.1: Receive through DAB
Driver
UC-12.2.1: Show information status quality
«include»
«include»
UC-12.3.2: Request and receive through Internet
UC-12.3.3: Detect unsolvable problem
«include»
UC-12.1.3: Warning about information supply stall
«extend»
«extend»
«extend»
«extend»
UC-12.3.4: Switch DAB reception
«extend»
UC-12.3.5: Determine optimal source
«extend»
UC-12.3.6: Scan through all DAB ensembles

Figure 21: UC-12.3 Acquire information

The task "Perpetually receiving a constant stream of information through any options available and needed to fill the TPEG-Traffic-Information-Storage" is performed by an entity that monitors and controls the received data streams and connections in a smart way, using meta-information about services and access options.

SCENARIOS

Basic Path.

Where sufficiently available the streamed information from DAB reception are preferred, as it is available with no extra costs and has no limitation in the concurrent usage by many receivers. Cellular communication is used as an addition to fill any gaps and to maintain a constant flow of information. This

SCENARIOS

may only fail, where DAB, cellular and other additional means of transportation are not sufficiently supporting the need for constant information updates. This is the case in places, where no mobile wireless connectivity is available. This may be the case, especially at locations far away from cities and in difficult topological landscapes. The system monitors and detects, whether the data supply is effectively working within given parameters or if the supply is stalling, in which case an alert is issued to inform both the Driver and relating systems to be aware of the missing information. This should trigger a system status change, as it is no longer assured that critical information, such as hazard warnings, will be received in time.

1. Acquire the needed information.
   Uses: –
2. Use DAB reception if possible and in a suitable manner.
   Uses: –
3. Use Internet connectivity (e.g. cellular networks) where needed and in a suitable manner.
   Uses: –
4. Detect unsolvable problems and inform the user.
   Uses: UC-12.3.3: Detect unsolvable problem
5. Use case ends.
   Uses: –

3.3.3.12.3.1 UC-12.3.1: Receive information through DAB

An information stream is received through a DAB TPEG service, using DAB reception by utilizing a DAB receiver that monitors the reception.

RESPONSIBILITIES (INTERNAL REQUIREMENTS)

☑ Functional. DAB reception quality information must be available.

A DAB receiver (reception chip) is able to measure the BER (bit error rate) and signal strength. Especially the BER gives a good idea of how well all the content from the DAB ensemble may be decoded. The receiver is not able to calculate or measure the precise BER but it can deliver a quite reliable estimation, which is commonly used to determine reception quality. This BER (and other information, like the signal strength) must be available for the decision logic to figure out which DAB ensemble to use and if DAB reception is sufficient at all. A suitable API is needed that allows to request or read the BER. The BER estimation is based on the EEP (even error protection) of the DAB standard and covers the lower levels of the transport stack, below/before the byte stream becomes available.

☑ Functional. Decoding meta information must be available.

The receiver itself delivers a byte stream, which contains multiple protocol layers that bring their own error detection (CRC) and error correction (FEC) mechanisms. It must be possible to get information about how well the decoding is working and if CRC fails or FEC had to correct errors. This allows the decision logic to determine if there are any remaining reception problems and if the currently used DAB TPEG service is sufficiently suitable.

PRE-CONDITION CONSTRAINT

Tuning information, which DAB ensemble and which TPEG service to be used, must be present.

SCENARIOS

Basic Path.
TPEG information delivered by using a DAB receiver is preferred and used as a primary source of information.

1. DAB reception through a DAB receiver using a suitable DAB TPEG service.
   Uses: –
   Exception: *1a*. Reception problems
2. Use case ends.
   Uses: –

Exception. Reception problems

1. In case of problems with the DAB reception, an immediate new determination of the optimal source is forced.
   Uses: –
2. Determine optimal source.
   Uses: UC-12.3.5: Determine optimal source
3. Use case ends.
   Uses: –

CONSTRAINTS

Invariant. Reception quality must be sufficient.

3.3.3.12.3.2 UC-12.3.2: Request and receive information through Internet

Uses Internet connectivity to request information and receive it. This is meant to act more as a fallback but not as the primary source of information.

PRE-CONDITION CONSTRAINT

Information about the Internet address where the request shall be sent to must be present.

SCENARIOS

Basic Path.
A connection using cellular networks (e.g. LTE) or other means of communication is established and assured, to receive needed TPEG encoded information.

1. Establish Internet connectivity (e.g. by using cellular networks).
   Uses: –
   Exception: *1a*. On error
2. Send a TPEG specific request.
   Uses: –

SCENARIOS

Exception: *2a*. On error

3. Receive a TPEG specific response.

   Uses: –

Exception: *3a*. On error

4. Decode and use the TPEG traffic information.

   Uses: –

Exception: *4a*. On error

5. Use case ends.

   Uses: –

Exception. On error

1. No connection could be established, no response was received, a timeout occurred or the received information could not be decoded or understood.

   Uses: –

2. The determination logic is informed about a problem.

   Uses: –

3. Use case ends.

   Uses: –

3.3.3.12.3.3 UC-12.3.3: Detect unsolvable problem

A problem is detected that could (temporarily) not be solved. No reception through available methods was available for some time.

SCENARIOS

Basic Path.

If information supply fails or exceeds valid limitations, this problem is reported to both the User and other systems, while still trying to reestablish the supply.

1. Information supply is impossible or does not meet the configured requirements.

   Uses: –

2. Show the bad information status quality to the User.

   Uses: UC-12.2.1: Show information status quality

3. Alert the Driver about the missing information supply and the missing ability to inform him about potential hazards ahead.

   Uses: UC-12.1.3: Warning about information supply stall

4. Retry to acquire information supply by seeking a solution, over and over again, until information could be supplied again.

   Uses: UC-12.3.5: Determine optimal source

5. Show information about the improved information status quality.

   Uses: UC-12.2.1: Show information status quality

6. Use case ends.

   Uses: –

3.3.3.12.3.4 UC-12.3.4: Switch DAB reception

The DAB ensemble must be switched to receive a different DAB TPEG Service more suitable and/or with better reception quality.

PRE-CONDITION CONSTRAINT
Tuning information, to which DAB ensemble to switch to, must be present.

SCENARIOS

Basic Path.

Seeking a valid information supply, provided by DAB, the DAB receiver is retuned to an appropriate service, which is containing the required information and may be received in sufficient quality.

1. Retune DAB receiver to another DAB ensemble
   Uses: –

Exception: *1a*. On error

2. Seek the desired DAB TPEG service.
   Uses: –

Exception: *2a*. On error

3. Decoding and using the DAB TPEG service.
   Uses: –

Exception: *3a*. On error

4. Use case ends.
   Uses: –

Exception. On error

1. Actions fails.
   Uses: –
2. Force an immediate redetermination of the optimal source.
   Uses: –
3. Use case ends.
   Uses: –

3.3.3.12.3.5 UC-12.3.5: Determine optimal source

Once in a while, but repeatedly, the optimal source for reception is determined by using meta-information (hybrid orientation data) and information from the receivers. Maybe a scan through available DAB ensembles and DAB services is needed to figure out which DAB TPEG services are usable at that moment. (This needs a receiver module to be switched through different DAB ensembles.)

SCENARIOS
Basic Path. A scan through all receivable DAB ensembles collects information about services that may be used, including their content and reception quality. After information was collected, a decision is made, which DAB service to tune to, or to switch to other means of communication. 1. Scan through all DAB ensemble. Uses: UC-12.3.6: Scan through all DAB ensembles 2. Determine, that reception through DAB is suitable. Uses: – Alternate: *2a*. Use internet instead Alternate: *2b*. No suitable solution found 3. Switch DAB reception to the most suitable DAB TPEG service. Uses: UC-12.3.4: Switch DAB reception 4. Receive (continuously) through DAB reception. Uses: UC-12.3.1: Receive through DAB 5. Use case ends. Uses: –
Alternate. Use internet instead 1. Decide, that it is more suitable to use internet connectivity (e.g. via mobile networks). Uses: – 2. Receive information (repeatedly) using Internet connectivity. Uses: – 3. Use case ends. Uses: –
Alternate. No suitable solution found 1. No suitable reception through DAB is possible, nor is a suitable solution through internet possible. Uses: – 2. Detect unsolvable problem. Uses: UC-12.3.3: Detect unsolvable problem 3. Use case ends. Uses: –

CONSTRAINTS
Invariant. Hybrid orientation data must be present to support an optimal decision.

3.3.3.12.3.6 UC-12.3.6: Scan through all DAB ensembles

A scan through all DAB ensembles collects information about usable services and tuning information.

SCENARIOS

Basic Path.

The DAB receiver makes a complete scan through all DAB frequencies, seeks for DAB ensembles, decodes them, looks out for DAB TPEG services, decodes them, and looks into their IDs, applications and content. This will typically take quite a while (up to several minutes), and needs to be done on a regular basis, to adapt to changing environmental conditions. This is critical, because a DAB receiver that does such a scan may not simultaneously decode and use content from a specific DAB ensemble. This means that listening to a DAB audio program while doing a DAB scan is not possible. Similarly, the decoding of a DAB TPEG service is not possible while doing a scan. The technical solution for this is to have multiple DAB receivers on board that work cooperatively together, e.g., first receiver does scanning, the second receiver delivers audio program, and the third receiver decodes the DAB TPEG service.

There is a naming issue: What is a "receiver"? Is it the technical core unit that can only decode one DAB ensemble at a time, or shall it be the overall device that holds multiple functional units and therefore could decode multiple DAB ensembles at a time? Either way this has to be described, including the multiplicity of the required and available possibilities of simultaneous DAB ensemble decoding.

1. Start a full scan through all DAB frequencies.

Uses: –

Exception: *1a*. Receiver unavailable

2. Seek for DAB ensemble.

Uses: –

3. Look for DAB TPEG service.

Uses: –

4. Try to decode the DAB TPEG service.

Uses: –

5. Deliver the collected information to the decision logic.

Uses: –

6. Use case ends.

Uses: –

Exception. Receiver unavailable

1. No DAB receiver is found, not functional or may not be used exclusively for a full scan.

Uses: –

2. An error is reported back to the decision logic with the information that DAB might not be available at all.

Uses: –

3. Use case ends.

Uses: –

4 TECHNOLOGIES

4.1 Analysis of technologies

In this section, the communication technologies will be analyzed. First, the privacy and security requirements are considered. Then, the communication relationships of the use cases are presented in tabular form. This is followed by a short presentation of communications technologies. In conclusion, for each communication relationship a communication technology will be proposed.

Requirements

In the iKoPA project, the different systems exchange data with each other. This data may be personal or non-personal. Personal data (e.g. name, address, account number, etc.) is information that can be assigned to a person and non-personal data can be information e.g. about a car park. All this data must be transmitted in compliance with security and privacy requirements.

Security requirements

In order to prevent information manipulation during data exchange, the messages should be signed and checked for valid signatures. The communication must be secured to prevent unauthorized access to the information.

Privacy requirements

Privacy is concerned about the protection of the informational self-determination of the persons whose data is processed. Personal data may not be stored without reason and without consent. For example, the anonymity of the user shall be maintained throughout the flow of information. Tracking of users should be prevented. This means that when communication does not require identification of the parties, the identities shall be completely hidden or pseudonymized.

iKoPA Use cases

This section presents the communication relationships for the use cases. The communication relation are presented in tabular form. The rows represent the sender station and the columns represent the receiver station. The cells with “x” show that there is no communication between the stations. The cells with content are separated in four parts. The first line represents the communication type, the second line represents the identifiability of the actors, the third line represents communication security and the fourth line represents communication integrity.

<u>Communication types</u>

- **Unicast** – sending of messages to a destination identified by a unique address.
- **Broadcast** – sending of messages to all recipients simultaneously.
- **Geobroadcast** – sending of messages to all recipients simultaneously in a geographical area.
- **Multicast** – sending of messages to a group of recipients simultaneously.

Identifiability

- **Identifiable** – the actor is recognizable using his real identity.
- **Pseudonymized** – the actor is using a pseudonym, obfuscating its real identity. It is recognizable only as long as it is using the same pseudonym or if different pseudonyms can be linked together.
- **Anonym** – the actor cannot be recognized at all.

Communication security

- **Encrypted** – encoding messages in such a way that only authorized parties can read it.
- **Unencrypted** – encryption is not necessary, because the content of the message is public information.

Communication integrity

- **Signed** – signed message gives a recipient reason to believe that it was created by a known sender.

4.1.1 Use case communication characteristics

- UC1: ensure parking and charging facility

  The user selects and reserves a facility at the destination, which allows parking and charging.

Table 1: UC1 communication characteristics

receiver sender	smartphone	IVS	E-Mobility Provider	DAB Service Provider
smartphone	x	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x
IVS	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x	x	x
E-Mobility Provider	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x	x	x
DAB Service Provider	x	broadcast pseudonymized (sender), anonym (receiver) unencrypted signed	x	x

- UC2: Follow Navigation guides

  The driver receives navigation guidelines, which are enhanced by information of the traffic network.

Table 2: UC2 communication characteristics

receiver sender	smartphone	IVS	routing server
smartphone	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x
IVS	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed
routing server	x	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x

- UC3: Use speed advisory on traffic lights

  The driver / (e-)vehicle receives a Traffic Light Forecast (TLF) and uses it to optimize its behavior most energy efficient.

Table 3: UC3 communication characteristics

receiver sender	smartphone	IVS	IRS	forecast Service Provider	DAB Service Provider
smartphone	x	x	x	x	x
IVS	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x	x	x	x
IRS	x	geobroadcast pseudonymized (sender), anonym (receiver) unencrypted signed	x	unicast identifiable (sender), identifiable (receiver) encrypted signed	x
forecast Service Provider	x	x	x	x	unicast identifiable (sender), identifiable (receiver) encrypted signed
DAB service provider	x	broadcast pseudonymized (sender), anonym (receiver) unencrypted signed	x	x	x

- UC4: Receive entrance clearance for car park

  The vehicle receives a clearance to enter into the car park based on an identification.

Table 4: UC4 communication characteristics

receiver sender	**IVS**	**IRS (car park)**	**Identity provider**
IVS	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x
IRS (car park)	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed
identity provider	x	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x

- UC5: Park (partly) automated at charger

  The vehicle drives (partly) automated to the charger and parks there.

Table 5: UC5 communication characteristics

receiver sender	**IVS**	**IRS (car park)**
IVS	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed
IRS (car park)	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x

- UC6: Pay parking and charging

The driver automatically pays the parking and charging bill.

Table 6: UC6 communication characteristics

receiver sender	IVS	IRS (car park)	barrier (parking lot)	billing service	IRS (charging station)
IVS	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed
IRS (car park)	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x
barrier (parking lot)	x	x	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x
billing service	x	x	x	x	x
IRS (charging station)	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x

- UC7: Camera-based in-car park positioning

  The position data of the vehicle is enhanced by combining it with position information created by the car parks camera system.

Table 7: UC7 communication characteristics

receiver sender	IVS	IRS (car park)	cam-based positioning system
IVS	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x
IRS (car park)	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed
cam-based positioning system	x	unicast identifiable (sender), identifiable (receiver) encrypted signed	x

- UC8: Get access to parking lot

  The Vehicle authenticates itself at the car park and gets entrance permission.

Table 8: UC8 communication characteristics

receiver sender	IVS	barrier (parking lot)	identity provider
IVS	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x
barrier (parking lot)	x	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed
identity provider	x	unicast identifiable (sender), identifiable (receiver) encrypted signed	x

- UC9: Communicate with charger & charge

The vehicle communicates with the charger and is charging.

Table 9: UC9 communication characteristics

receiver sender	IVS	IRS (charging station)	car park
IVS	x	unicast pseudonymized (sender), pseudonymized (receiver) encrypted signed	x
IRS (charging station)	broadcast pseudonymized (sender), anonym (receiver) unencrypted signed	x	unicast identifiable (sender), identifiable (receiver) encrypted signed
car park	x	unicast identifiable (sender), identifiable (receiver) encrypted signed	x

- UC10: Receive state of charge of vehicle

The driver receives state of charge (SOC) of the vehicle on his cell phone.

Table 10: UC10 communication characteristics

receiver sender	smartphone	Service Provider	IVS
smartphone	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x
Service Provider	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x	unicast identifiable (sender), pseudonymized (receiver) encrypted signed
IVS	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x

- UC11: Request Vehicle

The driver requests the vehicle, so he is automatically picked up.

Table 11: UC11 communication characteristics

receiver / sender	smartphone	Service Provider	IVS
smartphone	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x
Service Provider	unicast identifiable (sender), pseudonymized (receiver) encrypted signed	x	unicast identifiable (sender), pseudonymized (receiver) encrypted signed
IVS	x	unicast pseudonymized (sender), identifiable (receiver) encrypted signed	x

- UC12: Drive informed and safe

The driver will be informed about information affecting its route, arrival and safety while driving. He is assured that critical news will reach him, while he is driving, even if on the road through rural areas, with low connectivity (DAB and/or mobile networks). If there is a situation where information supply cannot be guaranteed, he is informed about this.

Table 12: UC12 communication characteristics

receiver / sender	DAB Service Provider	IVS	smartphone
DAB Service Provider	x	broadcast pseudonymized (sender), anonym (receiver) unencrypted signed	x
IVS	x	x	unicast identifiable (sender), pseudonymized (receiver) encrypted signed
smartphone	x	x	x

4.1.2 Communication technologies

Communication technologies allow for the exchange of data or information between electronic systems. In this chapter, the relevant communication technologies such as DAB, cellular, RFID and ETSI ITS G5 are described.

ITS-G5

For the communication between vehicles (up to 1500m distances) the standard ETSI ITS G5 is an option. This uses the 5.9 GHz frequency band and is based on the Wi-Fi standard IEEE 802.11p. This is a special version of the Wi-Fi standard IEEE 802.11a, which has been optimized for the data exchange between vehicles. In the US the technology is called WAVE (**W**ireless **A**ccess in **V**ehicular **E**nvironments).

The vehicles form ad-hoc networks: If a communication partner isn't within the transmission range, other vehicles transmit the information (multi-hopping) or they save the data and forward it later.

Cellular

Mobile networks have evolved from talk and SMS networks, driven by the demands of modern smartphones, to mobile broadband data networks. Today, LTE is a standard for the mobile wireless communication. LTE specification (Release 8-9) allows download speed up to 300 Mbit/s and upload speed up to 80 Mbit/s.

DAB (Digital Audio Broadcasting)

The popular VHF (**V**ery **H**igh **F**requency) radio system will be progressively replaced in Europe by the DAB (Digital Audio Broadcast) radio, which is already used in some EU countries. By 2022, the VHF radio system will be switched off in some countries (for example, the UK, Sweden and Norway) and completely replaced by the DAB radio. The more powerful DAB network may also transmit TMC (**T**raffic **M**essage **C**hannel) messages. However, more and more frequently the TPEG (**T**ransport **P**rotocol **E**xperts **G**roup) standard is used for traffic messages. TPEG messages contain much more details than TMC to improve the route planning. TPEG application can address features like car park, petrol price information, charging facilities for electric vehicles or weather information.

RFID (Radio-Frequency Identification)

RFID is a method for the automatic and contactless identification of objects. RFID system consists of a reader and a transponder. The retrieval of information from a RFID transponder is possible from a distance up to several hundred meters. Depending on the distance from the reader to the transponder, the connection is established based on LF, HF or UHF. The magnetic fields generated by the reader are used at short distances to supply the transponder with power. Active tags with their own power supply can be used to achieve greater distances. Transponder may either be read-only, having a factory-assigned number, or may be read/write, where specific data can be written into the transponder.

LAN

LAN (Local Area Network) is a computer network. Ethernet is the most common standard for LAN.

WLAN

WLAN (Wireless Local Area Network) is a wireless computer network. Most modern WLAN are based on IEEE 802.11 standard.

Evaluation

Because of the study, an evaluation of the communication relationships between the entities identified in the use cases is made. The analysis is structured according to use cases and takes the form of a matrix. For each communication relationship, an appropriate communication technology is selected and listed in the matrix. Possible values are "possible", "limited" and "not possible".

4.1.2.1 Use case communication matrices

In the following section for every use case a communication matrix and a description of the communication necessary for the use case is presented.

4.1.2.1.1 UC1: Ensure parking and charging facilities

There are four communication paths in this use case (Table 13: UC1 communication technology matrix). In the communication path from the smartphone to the E-Mobility Provider two technologies are possible: the direct cellular connection or the connection via the onboard wireless network in the vehicle. For the communication of the IVS to the smartphone, the wireless network in the vehicle should be preferred. Cellular connection is possible, but should be considered secondary because of higher effort[3]. In addition, the DAB Service Provider obviously uses the DAB technology.

Table 13: UC1 communication technology matrix

	ITS G5	**Cellular**	**DAB**	**RFID**	**LAN**	**WLAN**
smartphone → E-Mobility Provider	not possible	**possible**	not possible	not possible	not possible	**possible**
IVS → smartphone	not possible	**possible**	not possible	not possible	not possible	**possible**
E-Mobility Provider → smartphone	not possible	**possible**	not possible	not possible	not possible	**possible**
DAB Service Provider → IVS	not possible	not possible	**possible**	not possible	not possible	not possible

4.1.2.1.2 UC2: Follow navigation guides

There are four communication paths in this use case (Table 14). In the communication path, from the smartphone to the IVS and back two technologies are possible. These are the direct mobile connection or the connection via the onboard network in the vehicle. The preferred technology should be onboard WLAN. Cellular connection is possible, but

[3] The cellular communication to the smartphone is basically only possible via an additional service.

should be considered secondary because it requires higher effort. In addition, cellular technology should be used for the communication with the routing server.

Table 14: UC2 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN	WLAN
smartphone → IVS	not possible	**possible**	not possible	not possible	not possible	**possible**
IVS → smartphone	not possible	**possible**	not possible	not possible	not possible	**possible**
IVS → routing server	not possible	**possible**	not possible	not possible	not possible	not possible
routing server → IVS	not possible	**possible**	not possible	not possible	not possible	not possible

4.1.2.1.3 UC3 Use Traffic Light Forecast for energy efficient behavior

There are five communication paths in this use case (Table 15). In the communication path from the IVS to the smartphone two technologies are possible. These are the direct cellular connection or the connection via the onboard wireless network in the vehicle. The onboard WLAN should be preferred. Mobile connection is possible, but should be considered secondary because it requires a higher effort. The connection from the IRS to the IVS may be established over ITS G5 or cellular. For the connection of the IRS to the forecast Service Provider and forecast Service Provider to the DAB Service Provider, it depends on the situation. Both, cellular or wired connections are possible. In addition, the DAB Service Provider obviously uses the DAB technology.

Table 15: UC3 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN	WLAN
IVS → smartphone	not possible	**possible**	not possible	not possible	not possible	**possible**
IRS → IVS	**possible**	**possible**	not possible	not possible	not possible	not possible
IRS → forecast Service Provider	not possible	**possible**	not possible	not possible	**possible**	not possible
forecast Service Provider → DAB Service Provider	not possible	**possible**	not possible	not possible	**possible**	not possible
DAB Service Provider → IVS	not possible	not possible	**possible**	not possible	not possible	not possible

4.1.2.1.4 UC4: Receive entrance clearance for car park via V2X authentication

There are four communication paths in this use case (Table 16). For the identification of the IVS at the car park IRS three technologies are possible: ITS G5, cellular or RFID. RFID or G5 should be preferred. Mobile connection is possible, but should be considered secondary because it requires a higher effort. The connection from the IRS to the IVS may be done over ITS G5 or cellular. For the connection of the IRS to the identity provider and back, it depends on the situation. Both, cellular or wired connection are possible, but wired communication is preferred.

Table 16: UC4 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN
IVS → IRS (Car Park)	**possible**	**possible**	not possible	**possible**	not possible
IRS (Car Park) → IVS	**possible**	**possible**	not possible	not possible	not possible
IRS (Car Park) → identity provider	not possible	**possible**	not possible	not possible	**possible**
identity provider → IRS (Car Park)	not possible	**possible**	not possible	not possible	**possible**

4.1.2.1.5 UC5: Park (partly) automated at charger

There are two communication paths in this use case (Table 17). For the identification of the IVS at the car park IRS, three technologies are possible: ITS G5, cellular or RFID. The connection from the IRS to the IVS may be established over ITS G5 or cellular.

Table 17: UC5 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN
IVS → IRS (Car Park)	**possible**	**possible**	not possible	**possible**	not possible
IRS (Car Park) → IVS	**possible**	**possible**	not possible	not possible	not possible

4.1.2.1.6 UC6: Pay parking and charging

There are eight communication paths in this use case (Table 18). For the identification of the IVS at the barrier, three technologies are possible: ITS G5, cellular or RFID. The connection from the IRS (car park, barrier, and charging system) to the IVS and back may be established over ITS G5 or cellular. For the connection of the IRS (car park, parking lot, and charging station) to the billing service, it depends on the situation. Both, cellular and wired connection are possible.

Table 18: UC6 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN
IVS → IRS (Car Park)	**possible**	**possible**	not possible	not possible	not possible
IVS → barrier (parking lot)	**possible**	**possible**	not possible	**possible**	not possible
IVS → IRS (charging system)	**possible**	**possible**	not possible	not possible	not possible
IRS (Car Park) → IVS	**possible**	**possible**	not possible	not possible	not possible
IRS (Car Park) → billing service	not possible	**possible**	not possible	not possible	**possible**
barrier (parking lot) → billing service	not possible	**possible**	not possible	not possible	**possible**
IRS (charging station) → IVS	**possible**	**possible**	not possible	not possible	not possible
IRS (charging station) → billing service	not possible	**possible**	not possible	not possible	**possible**

4.1.2.1.7 UC7: Camera-based in-Car Park positioning

There are four communication paths in this use case (Table 19). The connection from the IVS to the IRS and back may be established over ITS G5 or cellular. For the connection of the IRS to the cam-based positioning system and back, it depends on the situation. Cellular or wired connections are possible.

Table 19: UC7 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN
IVS → IRS (car park)	**possible**	**possible**	not possible	not possible	not possible
IRS (car park) → IVS	**possible**	**possible**	not possible	not possible	not possible
IRS (Car Park) → Camera-based positioning system	not possible	**possible**	not possible	not possible	**possible**
Camera-based positioning system → IRS (Car Park)	not possible	**possible**	not possible	not possible	**possible**

4.1.2.1.8 UC8: Get access to parking lot via RFID Identification

There are three communication paths in this use case (Table 20). For the identification of the IVS at the barrier, three technologies are possible: ITS G5, cellular or RFID. For the connection of the barrier to identity provider and back, it depends on the situation. Cellular or wired connections are possible.

Table 20: UC8 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN
IVS -→barrier (parking lot)	**possible**	**possible**	not possible	**possible**	not possible
barrier (parking lot) → identity provider	not possible	**possible**	not possible	not possible	**possible**
identity provider → barrier (parking lot)	not possible	**possible**	not possible	not possible	**possible**

4.1.2.1.9 UC9: Communicate with charger & charge

There are four communication paths in this use case (Table 21). The connection from the IVS to the IRS and back may be established over ITS G5 or cellular. For the connection of the IRS to the car park and back, it depends on the situation. Cellular or wired connections are possible.

Table 21: UC9 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN
IVS → IRS (charging station)	**possible**	**possible**	not possible	not possible	not possible
IRS (charging station) → IVS	**possible**	**possible**	not possible	not possible	not possible
IRS (charging station) → Car Park	not possible	**possible**	not possible	not possible	**possible**
car park → IRS (Car Park)	not possible	**possible**	not possible	not possible	**possible**

4.1.2.1.10 UC10: Receive state of charge of Vehicle

There are five communication paths in this use case (Table 22). The communication from the smartphone to the Service Provider and back should be realized via cellular, but it can also be established via public WLAN. The communication from the IVS to the Service Provider and back should be realized via cellular.

Table 22: UC10 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN	WLAN
smartphone → Service Provider	not possible	**possible**	not possible	not possible	not possible	**possible**
Service Provider → smartphone	not possible	**possible**	not possible	not possible	not possible	**possible**
Service Provider → IVS	not possible	**possible**	not possible	not possible	not possible	not possible
IVS → smartphone	not possible	**possible**	not possible	not possible	not possible	not possible
IVS → Service Provider	not possible	**possible**	not possible	not possible	not possible	not possible

4.1.2.1.11 UC11: Request vehicle

There are four communication paths in this use case (Table 23). The communication from the smartphone to the Service Provider and back should be realized via cellular. Can also be done via (public) WLAN. It depends on the situation (existing WLAN or cellular). Both solutions are equally feasible. The communication from the IVS to the Service Provider and back should be realized via cellular.

Table 23: UC11 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN	WLAN
Smartphone → Service Provider	not possible	**possible**	not possible	not possible	not possible	**possible**
Service Provider → smartphone	not possible	**possible**	not possible	not possible	not possible	**possible**
Service Provider → IVS	not possible	**possible**	not possible	not possible	not possible	not possible
IVS → Service Provider	not possible	**possible**	not possible	not possible	not possible	not possible

4.1.2.1.12 UC12: Drive informed and safe

There are two communication paths in this use case (Table 24). DAB Service Provider communicates to the IVS via DAB. As a fallback, a cellular connection could be established. In the communication path from the IVS to the smartphone two technologies are possible, which are the direct cellular connection or the connection via the onboard wireless network in the vehicle.

Table 24: UC12 communication technology matrix

	ITS G5	Cellular	DAB	RFID	LAN	WLAN
DAB Service Provider → IVS	not possible	***limited***	**possible**	not possible	not possible	not possible
IVS → smartphone	not possible	***limited***	not possible	not possible	not possible	**possible**

4.2 CONVERGE

With Intelligent Transport Systems (ITS) at the edge of deployment, pioneering approaches to traffic management and vehicle safety issues are increasingly growing together. However, a holistic system architecture for flexible interaction between different Service Providers and communications network operators that supports a decentralized and saleable structure is still missing. The aim of the German research project CONVERGE was to close this gap.

The developed Car2X Systems Network (see Figure 22) is a dynamical extendable association for cooperative systems in ITS, comparable to the internet with open standards and interoperability, which picks up current innovations in the field of information and communication technology (ICT) and thus provides novel approaches for system- and software-design.

The stated goal of CONVERGE was the definition of an architecture and interface for a Car2X Systems Network. This network is supposed to be open, providing its integration interfaces to the international standardization process as well as being scalable and flexible, to ensure a successful rollout. The entities of the network are distributed and provider-independent, allowing for a flexible role model in which several participants can fulfill a role, lowering financial barriers to participate. The system shall not be limited by national borders, enabling a trans-regional and international deployment. To account for high requirements and standards in the field of IT security, this is considered and actively included in the developments for each component as well as the overall system design. The innovative approach of a hybrid-communicating network encompasses the communication between backend components and mobile ITS stations like vehicles via various access technologies. Currently this includes ETSI ITS G5, a wireless standard specialized for ITS, and cellular communication. [1]

4.2.1 CONVERGE as a basis for iKoPA

The introduction of C-ITS is on the horizon. The automotive industry and the public sector are currently working on the last open topics in standardization and harmonization. In addition, the first preparations for a large-scale deployment of V2X technology are already on their way. For the deployment and the actual operational phase, a solid, reliable, extendable and secure communication architecture is imperative. iKoPA in this matter does not want to create a new architecture but use an existing one and extend that, if necessary, for the special needs towards automatic driving and electric mobility. To reuse an existing architecture also has the advantage that the solutions developed are compatible with a variety of other applications already developed for this architecture. An open architecture ensures that many new stakeholders can easily join the community and extend the number of Service Providers and services available. The architecture should also provide an economically feasible solution, so that it is financially interesting to use the architecture for participants. It should be possible for users of the architecture to generate a cost benefit.

For this purpose, the architecture devolved in the research project CONVERGE was chosen. It combines the features needed for the architecture baseline and the applications to be developed in iKoPA. It has a distributed structure based on a newly developed role model approach, combining technical and economical roles. So it does not relay on one stakeholder, but any role can be fulfilled by many institutions. The communication in CONVERGE is secured at any point of time and the privacy of the users is ensured. In addition, the economical approach fulfills the requirements of an easy and risk reduced introduction of new services. The following chapter describes the CONVERGE concepts in more detail.

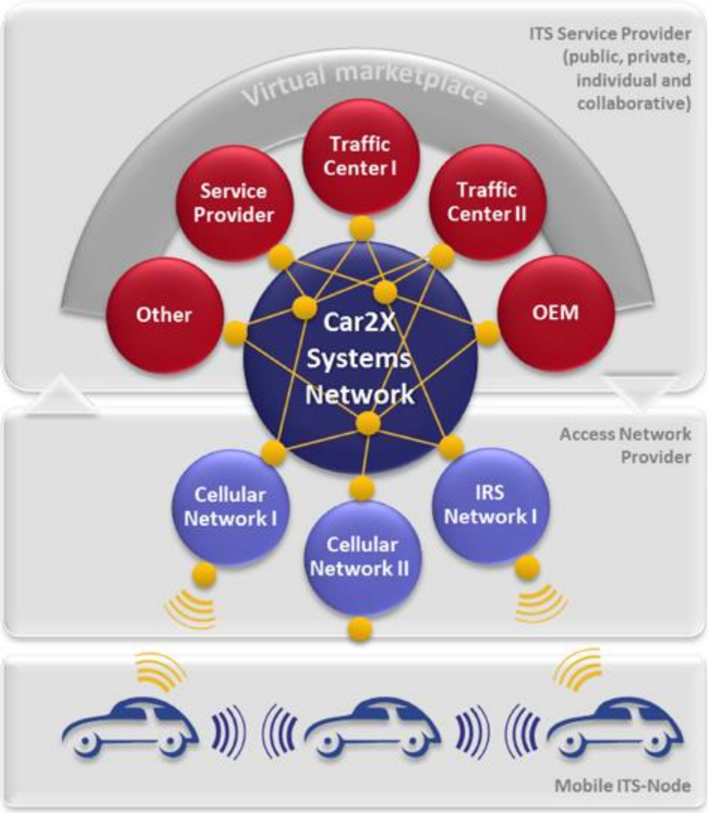


Figure 22: CONVERGE Car2X Systems Network [1]

4.2.2 Architecture Overview

The following picture gives an overview of the architecture of the Car2X Systems Network. It shows the major components on the first level of detail and the separation of the system in functional blocks. The arrows do not indicate data flow but indicate which block is exposing or using an interface respectively. For better readability, only logical interfaces are shown in this diagram. Typically, those logical interfaces (logical connections from one block in Figure 23) are consisting of a chain of physical interfaces, which are not shown here. Some interfaces like e.g. the interface B3 are used by many other blocks and including all those connections would introduce additional complexity into the diagram.

The architecture defines four structural blocks, which describe a set of components and/or a sub-block (which again can consist out of components and/or sub blocks, and so on).

- Governance: All legal, financial, contractual components necessary to start the Car2X Systems network and to keep it running from a management point of view. Additionally, the Root Certification Authority and the Enrolment Authorities are included in this block. [1]

- Backend: Consists of the Service Providers and the technical components for the communication between the Service Providers themselves and between the Service Providers and the service users using the communication networks. Furthermore, several security components are included in this block. [1]
- Communication Networks: Providing the connectivity between services providers and service users. This includes for example geographical based information distribution. [1]
- Intelligent Transportation System Stations: Traditionally the user of services provided by the Service Providers. However, in CONVERGE the role of an intelligent distribution platform and an information provider can be fulfilled by a vehicle or a smartphone (ITS Personal Station). [1]

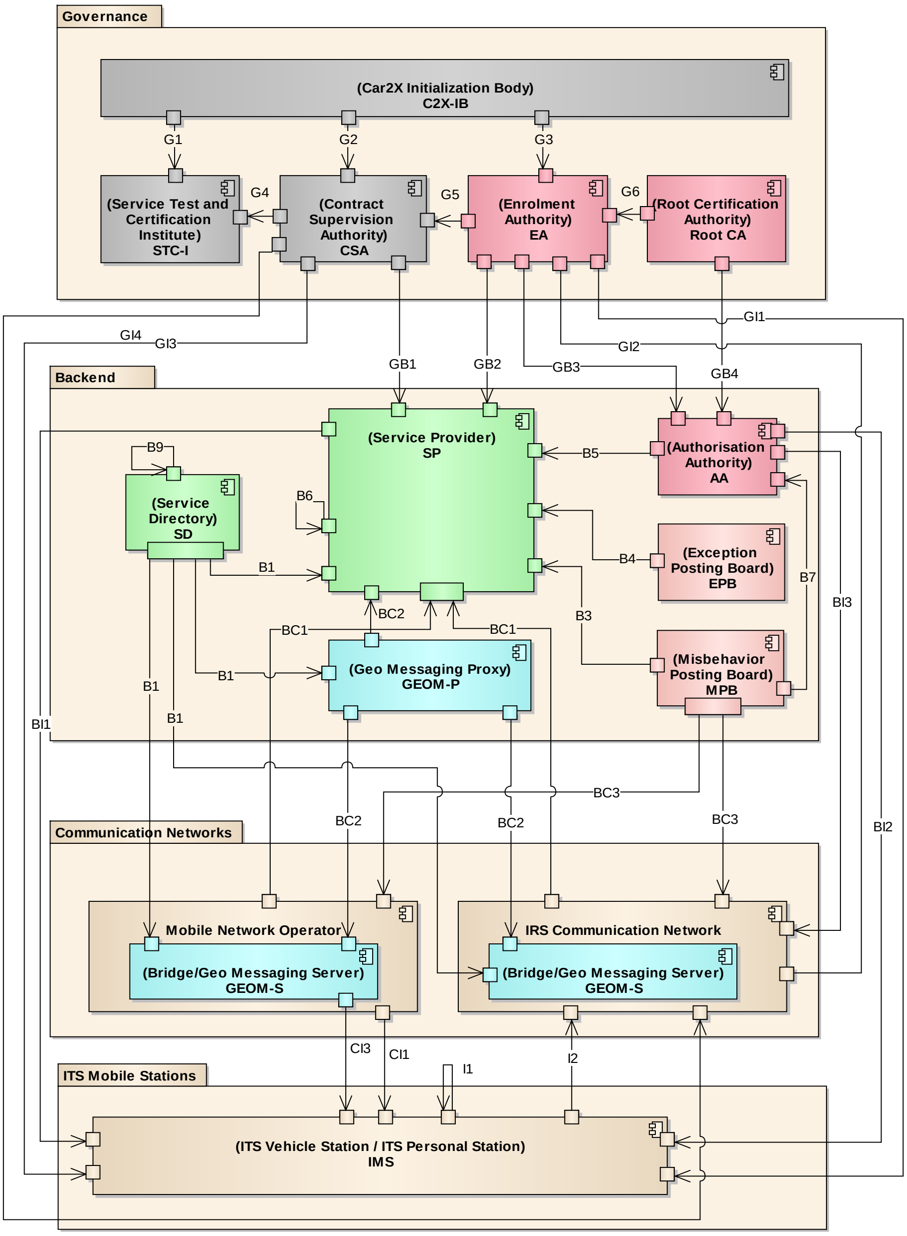

Governance
(Car2X Initialization Body)
C2X-IB
G1
G2
G3
(Service Test and Certification Institute)
STC-I
G4
(Contract Supervision Authority)
CSA
G5
(Enrolment Authority)
EA
G6
(Root Certification Authority)
Root CA
GI1
GI2
GI3
GI4
GB1
GB2
GB3
GB4
Backend
(Service Provider)
SP
(Authorisation Authority)
AA
B5
B9
(Service Directory)
SD
B6
B1
B4
(Exception Posting Board)
EPB
B7
BI3
BC2
BC1
B3
(Geo Messaging Proxy)
GEOM-P
(Misbehavior Posting Board)
MPB
B1
B1
BI1
BC3
BC2
BC2
BC3
BI2
Communication Networks
Mobile Network Operator
(Bridge/Geo Messaging Server)
GEOM-S
IRS Communication Network
(Bridge/Geo Messaging Server)
GEOM-S
CI3
CI1
I1
I2
ITS Mobile Stations
(ITS Vehicle Station / ITS Personal Station)
IMS

Figure 23: Overview on Car2X Systems Network Architecture [1]

4.2.3 Components

The following paragraphs list the components as described by the CONVERGE architecture. The description was taken from the CONVERGE Deliverable D4.3 [1]. It is a one-to-one copy of the description, so the information is compact. To get a more detailed view on the CONVERGE architecture the Deliverable D4.3 has to be consulted.

4.2.3.1 Car2X Initialization Body (C2X-IB)

Extract of document [1].

Summary

In order to instantiate the general rules for the Car2X Systems Network, the so-called “Car2X Initialization Body” is introduced which is a kind of participants’ agreement on a legal framework. The participants can be all kinds of persons, parties a stakeholders playing a certain role in the set-up, operation or usage of the C2X-SN. The Initialization Body is responsible for the set-up of contractual frameworks and dedicated contracts for services inside and access to of the C2X Systems Network. It specifies a set of rules and conditions that are to be applied by all participants of the C2X Systems Network. A “Contract Supervision Authority” (CSA) is taking stewardship of this legal framework. If a new participant (e.g. Service Provider or a Communication Network Provider) joins the Car2X Systems Network, ground rules have to be acknowledged and committed to.

Input

Inputs for the C2X-IB are the requirements and constraints that exist for a sensible functioning of such a cooperation. The inputs include organizational, legal, technical and commercial constraints and requirements.

Output

The output of the C2X-IB is a set of rules and agreements that have to be obeyed by all participants that want to be part of the C2X-SN. The rules are used by other parts of the governance subsystem of the C2X-SN such as Service Test and Certification Institute (STC-I), Contract Supervision Authority (CSA), Enrolment Authority (EA) and Root Certification Authority (Root-CA).

Interfaces

The C2X-IB provides interfaces to several functional components of the governance subsystem (STCI, CSA). Those interfaces are not realized as software or hardware interfaces but are a set of descriptions of rules and contractual conditions.

Functional description

The C2X-IB shall take into account all existing organizational, legal, technical and commercial constraints and requirements that are needed to define a proper cooperative work in the C2X-SN. It shall provide a set of rules and contractual conditions that should be obeyed by all participants of the C2X-SN and is the base for the operation and set up of the C2X-SN

Nonfunctional description

Not applicable.

4.2.3.2 Service Test and Certification Institute (STC-I)

Extract of document [1].

Summary

The quality of a service provided within the Car2X Systems Network has to meet some minimum standards. This will be checked by the “Service Test and Certification Institute” which will have to give input to the CSA in order to complete the admission of a new service to the Car2X Systems Network.

Input

The input for the STC-I are rules and agreements defined by the C2X-IB (Interface G1) as well as information about services that Service Providers (SP) want to provide to Service Users (SU) (Interface G4).

Output

Acknowledgements in order to allow services to be provided to SUs (Interface G4)

Interfaces

G1, G4

Functional description

The STC-I checks a new service for its compliance with the rules and constraints defined by the C2X-IB and provides an acknowledgement or refusal of the service to the CSA.

Nonfunctional description

Not applicable.

4.2.3.3 Contract Supervision Authority (CSA)

Extract of document [1].

Summary

The CSA is a body that is taking care and controls the compliance of all participants (ITS-S and C-ITS services) of the Car2X Systems Network and the involvement of those participants to the overall agreements made by the C2X initialization body during their participation in the C2X-SN.

Input

Rules and agreements defined by the C2X-IB (Interface G2).

Information about services that Service Providers (SP) want to provide to Service Users (SU) and registration information (Interface GB1).

Registration requests from ITS Stations (ITS-S) in order to get part of the C2X-SN. (Interfaces GI3 and GI4).

Acknowledgements in order to allow services to be provided to SUs (Interface G4)

Output

The output is an acceptance or denial of the registration requests of ITS-S via the interface G5 to the Enrolment Authority (EA).

It could also be an acceptance of new services to the C2X-SN via GB1 directly to the SPs or indirectly via the EA and the interface GB2.

Interfaces

G1, G4, G5, GB1, GI3, GI4

Functional description

The CSA controls the compliance of new services that are requested at the C2X-SN to the rules and constraints given by the C2X-IB. It also controls requests for ITS-S for registration when they want to enter the C2X-IB for the first time.

Nonfunctional description

Not applicable.

4.2.3.4 Root CA

Extract of document [1].

Summary

Enabling the trustful exchange of information between participants within the Car2X Systems Network is of very high importance. To achieve this trustful exchange a Public-Key-Infrastructure (PKI) will be implemented. The PKI consists of different Certification Authorities (CA) such as Root CA, Enrolment Authority and Authorization Authority.

The Root CA is the root of trust for all digital certificates in the communication system. It will issue certificates to the subsequent CAs if they follow the agreed security policies. To ensure that the policies are fulfilled, the Root CA is able and authorized to audit the subsequent CAs.

There shall be a low, limited number of Root CAs, because of the work needed for mutual trust and possibly cross-certification.

Input

The Root CA gets certificate request from clients (subsequent CAs) as input.

Interfaces

G6 and GB4 are instances of only one logical interface between the Root CA and its clients. Via this interface certificate request are gathered and responded by certificates.

Output

The Root CA issues certificates to clients.

Functional Description

The Root CA shall receive certificate requests and respond to them with certificates. The process is not automated, since an audit by experts is required before the certificate is issued.

Nonfunctional Description

The Root CA evaluates the certificate request, audits the client according to the security policy and issue the corresponding certificate.

4.2.3.5 Long Term CA (LTCA)

Extract of document [1].

See Enrolment Authority below.

4.2.3.6 Pseudonym CA (PCA)

Extract of document [1].

See Authorization Authority below.

4.2.3.7 Enrolment Authority (EA [C2C-CC: Long Term Certification Authority (LTCA)])

Extract of document [1].

Summary

An Enrolment Authority (EA) is in charge of providing Enrolment Credentials (EC) to ITS Stations (ITS-S).

There are different kinds of EAs involved.

- The Enrolment Authority, which issues Enrolment Credentials to ITS vehicle stations, will be operated by the respective vehicle or vehicle-equipment manufacturers. The Car-2-Car Communication Consortium (C2C-CC) term for this kind of EA is Long Term CA (LTCA). The ECs issued by this LTCA are called Long Term Certificates (LTC) by the C2C-CC.
- The EA, which issues ECs to ITS Roadside Stations (IRS), will be operated by the IRS manufacturer. There is no C2C-CC synonym for this kind of EA.
- The EA which provides ECs to Service Providers.

The EA has to ensure that all of its clients operate within the specified security policy.

Input

The EA receives an enrolment request from the corresponding client (IVS, IRS or SP) via interfaces GB2, GI1 or GI3. This process is most likely being done at some point during manufacturing in case of IVS, IPS and IRS and at set up of servers or services in case of SP.

Other inputs are requests from the CSA for the setup of new participants of the C2X-SN via the interface G5.

Interfaces

The interface for enrolment request and response is vendor specific.

Output

The EA issues an enrolment credential (i.e. a kind of certificate) to the client via the interfaces GB2, GI2 or GI3.

Functional Description

The EA receives an enrolment request and responds to it with an enrolment credential.

Nonfunctional Description

Due to the vendor specific interface, we will not specify nonfunctional requirements for that process.

4.2.3.8 Authorization Authority (AA [C2C-CC: Pseudonym Certification Authority (PCA)])

Extract of document [1].

Summary

An Authorization Authority (AA) is in charge of issuing Authorization Tickets (AT) to ITS-S.

There are different kinds of AAs involved:

- The AA, which issues ATs to IVS. This one is operated by the respective IVS manufacturer. The C2C-CC term for that kind of AA is Pseudonym CA (PCA). The C2C-CC term for AT is Pseudonym Certificate (PC), because of the pseudonymous nature of this certificate.
- The AA, which issues ATs to IRS. This one is probably operated by the Roadside Network operator. These do not have to be pseudonymous and frequently changed like the PCs above.
- The AA, which issues ATs to ITS-Central Station for service specific use. CONVERGE project introduces a Service Provider CA (SP CA) that will offer service specific AT.

Input

The AA receives authorization requests, which are signed by the EC of the client. The authenticity and integrity of the request can be validated with this signature.

Interfaces

The protocols B5, GB4, BI2, BI3 and B7 for the interfaces between AA and the corresponding ITS- Stations are specified by the C2C-CC Pilot PKI documentation or in [1] chapter 3.3. They can be used over various communication links.

Output

The AA issues or denies ATs as a response for authorization requests. These ATs are short-lived, pseudonymous certificates for the use in communication between ITS-S (IVS, IRS, and ICS).

Functional Description

The AA shall receive an authorization request and respond with an AT if the digital signature of the request is valid and originated from a valid ITS-S (i.e. EC is valid).

Nonfunctional Description

The process is automated and is processed within in a reasonable time (e.g. 30 seconds).

4.2.3.9 Service Provider (SP)

Extract of document [1].

Summary

One major functional block within the Car2X Systems Network is the Service Provider. This is a generic functional block, which represents all possible participants within the Backend/Backbone level of the Car2X Systems Network. Examples would be OEMs, Road Authorities, and Data Providers of any kind like e.g. MDM.

Input

The following Input is needed for the SP:

- Acceptance of new services to be provided to SUs in the C2X-SN via the interface GB1.
- Acceptance of registration requests from the EA via interface GB2.
- Information exchange with other service Providers for cooperative services via the interface B6
- Information about existing services registered in the Service Directory via the interface B1.
- Information and data from mobile nodes via the interface BI1.
- Feedback from the Geo Messaging Proxy (GEOM-P) component via the interface BC2.
- Response from the Authorization Authority for ticket requests via the interface B5.
- Control Information about possibilities of the Communication Networks (CN) via the interface BC1.

Interfaces

GB1, GB2, BC1, B1, B3, B4, B5, B6, BI1.

Output

The SP produces the following output:

- Requests for new services to the CSA via the interface GB1.
- Requests for registration to the EA via the interface GB2.
- Signaling information given to the CNs via the interface BC1.
- Requests for information about existing services or information about new services in given to the SD via the interface B1.
- Data and control information given to the GEOM-P via the interface BC2.
- Information about misbehavior of entities of the C2X-SN to the Misbehavior Posting Board (MPB) via the interface B3.
- Information about exceptions in the operation of services given to the Exception Posting Board (EPB) via the interface B4.
- Requests for authorization tickets to the AA via the interface B5
- Information about services and data given to other SPs via the interface B6
- Information and data given to the mobile nodes in the C2X-SN via the interface BI1.

Functional Description

There are some generic operations such as authorization, service discovery, service announcement, misbehavior and exception information that will be functionally provided by all SPs in a similar way. The core functionality of SPs however is subject to the special services that a SP provides and cannot be explained in detail here.

Nonfunctional Description

Nonfunctional behavior is subject to the respective services provided by a certain SP and cannot be explained in detail here.

4.2.3.10 Service Directory (SD)

Extract of document [1].

Summary

The general service management concept is described in [1]. The Service Directory is a substantial part of this concept. In order to provide a mechanism for discovering and connecting to services offered by different Service Providers, a Service Directory (SD) will be used, providing the necessary information.

Input

An Announcement of the start of a new services or the stop of an existing services offered by SPs via the interface B1 as well as information about services existing in other instances of the SD via the interface B9.

Interfaces

B1, B9

Output

Information about services existing at the SD as information as well as requests for services to other instances of the SD function via the interface B9

Information about existing services within the SD function via the interface B1.

Functional Description

The SD function, which in turn might be formed by different instances of SD components, is responsible for providing a repository for services that exist in the C2X-SN. For details about the SD function, refer to [1] chapter 4.1.5

Nonfunctional Description

For details, see [1] chapter 4.1.5.

4.2.3.11 Exception Posting Board (EPB)

Extract of document [1].

Summary

For a service, it is necessary to become aware of temporary disruption or complete discontinuation of another service it relies on.

The “Exception Posting Board” is a entity to which exceptions such as service interruptions can be reported. In case a Service Provider has discontinued its service without notice, there has to be a way to notify the Service Providers depending on the vanished Service Provider’s services and to remove the remaining entries if the service is unavailable permanently in different entities within the C2X-SN.

If a SP notices a disruption in another SP’s service, it will send a notification to the EPB including its own identity, details about the service it tried to access, time of day, repetitions etc.

The EPB provider will contact the provider of the discontinued service and check whether the service outage is intermittent or permanent. The affected Service Provider and, in case of permanent or longer unavailability, the SD will be notified accordingly.

Input

The input is information about exceptions in services from the SPs via the interface B4.

Interfaces

B4.

Output

The output is information about exceptions in services to the SPs via the interface B4.

Functional Description

The EPB gets information about temporary or permanent disruption of existing services from the Service Providers, checks that information and, if necessary, provides the information back to SUs that use those services

Nonfunctional Description

Information about service availability has to be provided in a reasonable time. Which absolute time is reasonable depends on the requirements of a certain service.

4.2.3.12 Misbehavior Posting Board (MPB)

Extract of document [1].

Summary

The MPB is an entity to which suspected misbehavior of any kind within the Car2X Systems Network can be reported. Reports of suspected misbehavior are aggregated according to the pseudonyms of reporting and suspected misbehaving ITS-S, location and possibly other factors.

In a next step, this information can be used to trigger an appropriate countermeasure in order to mitigate or stop the misbehavior. This could include reversing the pseudonymity of a station by combining information of the Authorization Authority and Enrolment Authority in order to identify a misbehaving station.

Input

The input is information about misbehavior of any kind from all participants of the C2X-SN via the interface B3 and BC3 or a query about misbehavior from the AA via the interface B7.

Interfaces

B3, BC3, B7.

Output

The output is information about reported misbehavior to the AA via the interface B7.

Functional Description

The MPB is keeping track of the reported misbehavior from all entities of the C2X-SN and provides that information to the AA (see [1] section 4.1.6).

Nonfunctional Description

Not applicable.

4.2.3.13 Geo Messaging Proxy (GEOM-P)

Extract of document [1].

Summary

The GEOM-P is the part of the geomessaging concept that is located in the backend. This is the major entry point for delivery of geomessaging data from the perspective of a C-ITS service.

Through the SD, the GEOM-P will obtain a list of Geo Messaging Servers (GEOM-S) offering services for a specific geographic area.

In turn, the GEOM-P will offer its services to interested SPs through the SD including the aggregated area of coverage of the GEOM-Ss it is connected with.

The GEOM-P will connect to one or many Geo Messaging Servers (GEOM-S) which take over the task to finally distribute the geo messages via different communication networks to the respective geographical areas.

Input

The inputs are data packets that are to be geographically distributed from application side via the interface BC2 and information about existing GEOM-Ss and their capabilities from the SD via the interface B1.

Interfaces

BC2, B1

Output

The outputs are data packets with a geographical destination sent to GEOM-Ss via the interface BC2 and information about the GEOM-P service to be entered in the SD via the interface B1.

Functional Description

See [1] section 4.1.2.

Nonfunctional Description

See [1] section 4.1.2.

4.2.3.14 Geo Messaging Server (GEOM-S)

Extract of document [1].

Summary

“Geomessaging” is necessary to enable distribution of messages within a certain geographical area. This entity or hierarchy of entities can be placed at various locations within the Car2X Systems Network.

All GEOM-Ss will register at the SD with their area of coverage.

Input

The inputs are data packets that should be distributed in geographical areas via the interface BC2 and information about mobile nodes and their status from the interface CI3.

Interfaces

B1, BC2, CI3

Output

The output are data packets that have geographical destination areas to be sent to mobile nodes via the interface CI3.

Functional Description

See [1] section 4.1.2.

Nonfunctional Description

See [1] section 4.1.2.

4.2.3.15 Bridge

Extract of document [1].

Summary

The Bridge enables three different addressing schemes for Service Providers to send messages to mobile nodes (IVS and IPS). First, messages can refer a certain geographical area and therefore the relevant recipients are those who have indicated interest for that area. This way of addressing, we refer to as geomessaging. Geomessaging is handled by the Geo Messaging Server GEOM-S, which is therefore a part of the Bridge. Second, a message can refer to a special attribute of the recipients. This way of addressing, we refer to as "Attribute-based-addressing". Third, a message can refer to a special topic, which the recipients have indicated to be interested in. This way of addressing, we refer to as "Topic based addressing".

Input

The inputs are data packets that should be distributed to mobile nodes according to certain attributes (e.g. geographical position, vehicle type) via the interface BC2 and information about mobile nodes and their status from the interface CI3.

Interfaces

B1, BC2, CI3

Output

The Bridge outputs data packets that have geographical destination areas or that are related to other attributes of mobile nodes to be sent to mobile nodes via the interface CI3.

Functional Description

See [1] section 4.1.7.

Nonfunctional Description

See [1] section 4.1.7.

4.2.3.15.1 Communication Network (CN)

Extract of document [1].

Summary

Two Communication Networks are examined in the scope of the CONVERGE project: ITS Roadside Station (IRS) networks and cellular mobile networks. These networks can take on several roles within the Car2X Systems Network. One role is of course to provide transport of information between a Service Provider and an ITS-Station. Communication Networks themselves can have certain attributes and can act as Service Provider themselves.

Input

Data packets transferred from the mobile nodes via the interface CI1 and I2.

Interfaces

BC1, BC3, CI1, GI3, GI4, I2.

Output

Data packets to be transferred to the mobile nodes via the interface CI1 and I2.

Data packets from Service Providers to be transferred to the mobile nodes via the interface BC1.

Information about misbehavior detected in the communication network to be sent to the MPB via the interface BC3.

Functional Description

See [1] chapter 5.

Nonfunctional Description

See [1] chapter 5.

4.2.3.16 Mobile ITS Stations

Extract of document [1].

Summary

There are three types of ITS-Stations distinguished the UML diagrams in Figure 23: IVS, IRS (implicitly in the IRS Network) and IPS. As the inputs and outputs as well as the interfaces are similar for all three types of ITS stations mentioned below, the description of them is only given once. ITS Central Stations (ICS) are included in their role as Service Providers and users, see [1] chapter 4.2.3.9.

Input

- Information from Service Providers in order to use services via the interface BI1.
- Control information from the GEOM-S e.g. information about the geographical area via the interface CI3.
- Information coming from other entities in the C2X-SN through the cellular radio interface via the interface CI1.
- Information exchange from other IVSs via the interface I1 (e.g. ETSI ITS-G5 type messages from other vehicles).
- Information exchange from ITS Roadside Stations (IRS) via the interface I2 (e.g. ETSI ITS-G5 type messages from an ITS Backend service or from the IRS itself).

Interfaces

GI1, GI3, BI1, BI2, CI1, CI3, I2. GI2, GI4

Output

- Registration requests sent to the EA via the interface GI1 and GI2.
- Registration information sent to the CSA via the interface GI3 or GI4.
- Information in the course of using services that are provided from a SP in the backend using the interface BI1.
- Request for authorization tickets sent to the AA via the interface BI2.
- Information sent to other entities in the C2X-SN through the cellular radio interface via the interface CI1.
- Update information used in the geomessaging process about leaving or entering tiles to the GEOM-S using the interface CI3.
- Information exchange to other IVSs via the interface I1 (e.g. ETSI ITS-G5 type messages from other vehicles).
- Information exchange to ITS Roadside Stations (IRS) via the interface I2 (e.g. ETSI ITS-G5 type messages from an ITS Backend service or from the IRS itself).

4.2.3.17 ITS Vehicle Station (IVS)

Extract of document [1].

Summary

The IVS is a mobile ITS-Station that is integrated into a car.

Functional Description

The IVS is one representation of the mobile node in the vehicle-mounted variant in the C2X-SN architecture. Mobile nodes might be in vehicles or other mobile devices (e.g. Smartphones). The functionalities that are provided by an IVS might differ depending on the type and functionality of the IVS. Some of the functionality like a Geo Messaging Client functionality or different kinds of security functions however exists in all IVS. For more detailed information refer to [1] chapter 6.

Nonfunctional Description

See [1] chapter 6.

4.2.3.18 ITS Roadside Station (IRS)

Extract of document [1].

Summary

The IRS is a unit, which is permanently or semi-permanently installed on the roadside. An example is a permanently installed IRS in traffic light or a semi-permanently installed IRS in a blocking trailer present at a road works site. In CONVERGE, an IRS is not a component on its own, but is part of the IRS Communication Network.

Functional Description

The IRS is one representation of the ITS Station in the roadside mounted variant in the C2X-SN architecture. An IRS is similar in its basic functionality to the IVS, however it is not or very limited moving. The functionalities that are provided by an IRS might differ depending on the type and functionality of the IRS. Some of the functionality like Geo Messaging Client functionality or different kinds of security functions however exists in all IVSs. For more detailed information refer to [1] chapter 6.2. An IRS might provide additional functionality with respect to its stationary or quasi-stationary nature. Those functionalities could be aggregation of information or provision of special kind of data like crossroads topologies.

Nonfunctional Description

See [1] chapter 6.

ITS Personal Stations (IPS)

The IPS is similar to the IVS. The difference is that this kind of end user equipment is not integrated into a vehicle but used as personal utility (e.g. Smartphone).

Functional Description

The IPS is one representation of the mobile node in the non-vehicle mounted variant in the C2X-SN architecture. The functionalities that are provided by an IPS might differ depending on the type and functionality of the IPS. Some of the functionality like Geo Messaging Client functionality or different kinds of security functions however exists in all IVSs.

4.2.4 Architecture concepts

Geomessaging & Bridge

To transmit information about events or value-added services to service users in a specific, geographical area a geomessaging system is needed. To increase the probability of message delivery in zones with difficult communication conditions, a so-called hybrid communication approach is used. This approach simultaneously uses multiple communication networks to transmit information.

However, not every information is relevant for every participant in an area. To separate recipients in the same area also by message content, the so called GeoMessaging-Bridge-Server (GBS) has been introduced in CONVERGE. This server distributes information in geographical areas and filters recipients by topic and target group. The principle can be illustrated with an example: Imagine an old bridge for which a structural analysis showed that the bridge could not handle the weight of vehicles and trucks anymore. To reduce the stress on the building without cutting the traffic route, the bridge is closed for truck traffic. Smaller vehicles may still use the bridge, but a speed limit is installed to decrease their velocity. This information can now be distribution via GBS. In the zone around the affected bride, trucks get the information that the bridge is closed. Vehicles get the information about the speed limit. Therefore, each party just gets the information needed by them. Depending on the communication network, this reduces the number of messages send and therefore reduces utilization of the communication channel. In addition, the number of messages, which need to be processed by the receivers, is minimized, because only relevant information is received. In this example the geomassaging part is responsible for the geographical dissemination while the bridge part is responsible for the topic (here: traffic information) and the type of service user (here: vehicle or trucks).

Security

In ITS architectures, different stakeholders exist with different privacy needs. To respect those needs, three different levels of identifiability have been introduced in the past years: anonymous, pseudonymous and identifiable. When communicating with an anonymous participant, it is impossible for each party to determine, which participant one is communicating to. When using a pseudonymous communication, the pseudonym in use by the participants can be determined. However, the pseudonym shall not be traceable to a specific, identifiable participant. Therefore, a pseudonym is somewhat similar to an alias, but way stronger disconnected from the real identity. In the last case, identifiable, the communication partners can be clearly identified and linked to a real world entity.

The security of an architecture needs to possess an end-to-end security mechanism. This provides protection from malicious nodes in the architecture itself and prevents man-in-the-middle attacks from outsiders. Those end-to-end mechanisms need to provide means to provide non-reputable, authorized and verifiable, communication, as those are essential to establish trust between partakers. For certain communications, it is also necessary to be able to perform confidential communication, which is protected against eavesdropping.

Such a security environment can be created by merging Transport Layer Security (TLS) for TCP/IP-based backend connection and ETSI TS 103 097 secured messaging for wireless communications.

In both architectures, one or more central cross-certified Public-Key-Infrastructure (PKI) issues certificates used to secure the communication. To support pseudonymity, this infrastructure separates Enrolment Authority (EA) and Authorization Authority (AA). By separating those two, it gets possible to create pseudonym certificates that cannot be linked to a user, while maintaining the possibility to only allow certain users into the network. When joining, a user requests a long-term certificate after he has been verified. With this certificate, which already does not hold any elements, which could be used by a third party to identify the user, the user requests pseudonymous authorization tickets from the PCA. With these tickets, the user secures all future communication. It is obvious, that the privacy of the user can only be endangered, if EA and AA collaborate to link long-term certificates to used authorization tickets.

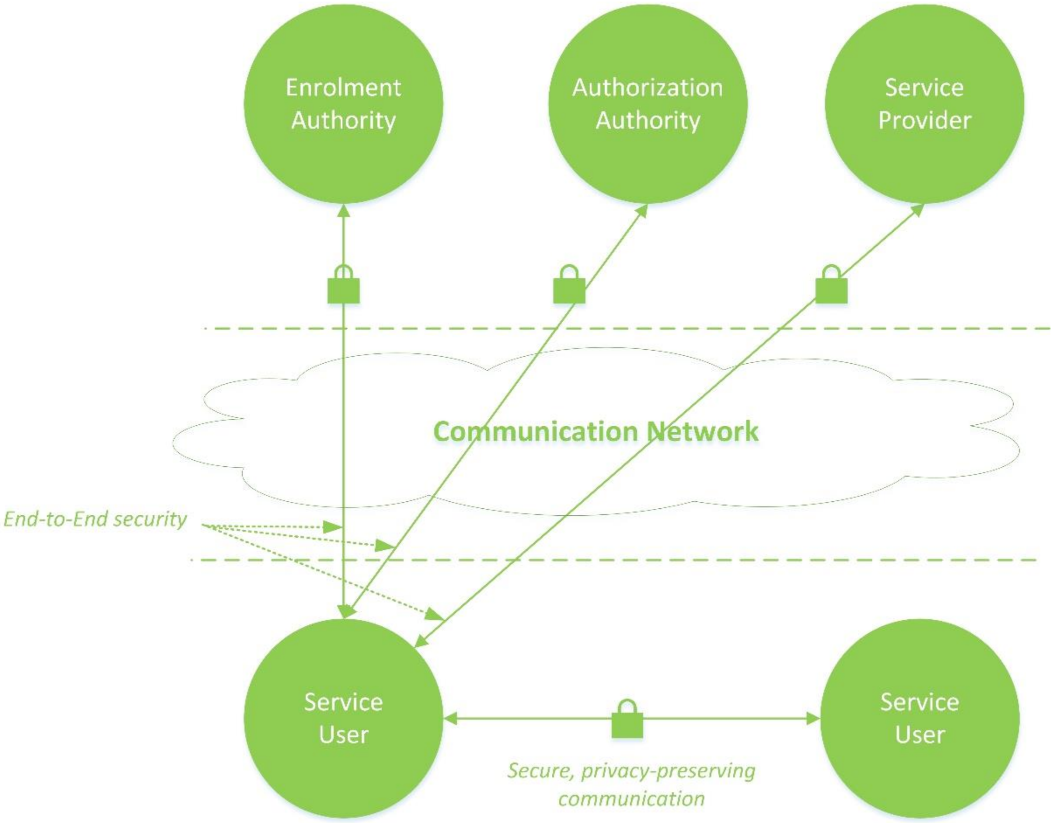


Figure 24: CONVERGE security principle

Service Directory & service concept

A Service is a form of information exchange; mostly in the context of some kind of application, whereas communication has to take place between two parties. These parties are known as Service Provider (SP), the party offering the service, and a Service User (SU), the party using the service. Usually, a single SP will have multiple SU consuming its services. To be able to interact with each other they first need to find each other. The so-called Service Directory (SD) therefore contains a listing of all services available. Service Providers publish their services in the service directory so that Service User can look up services.

Before a Service Provider can publish its services in the Service Directory, the services must be tested. This tests are performed by the service test and authorization institution (STA-I). All services must be compliant to the rules set by the system, like service interaction possibilities, service quality, service availability, security mechanisms, etc. Only after a service has passed the evaluation, the service provider is eligible to request a certificate for the service.

With the certificate, a Service Provider can place its service in the Service Directory and make it possible for Service User to use the service.

To use a service, the Service User also needs a valid certificate. With that, the authorization process can take place. The usage itself is done via a direct communication between the SP and the SU. Since all communication links in the systems network are encrypted, this communication is secured against eavesdropping. As Service Provider and

Service User use different certificates, a malicious Service User cannot provide a service to other users, as they would not recognize its certificate as a Service Provider certificate.

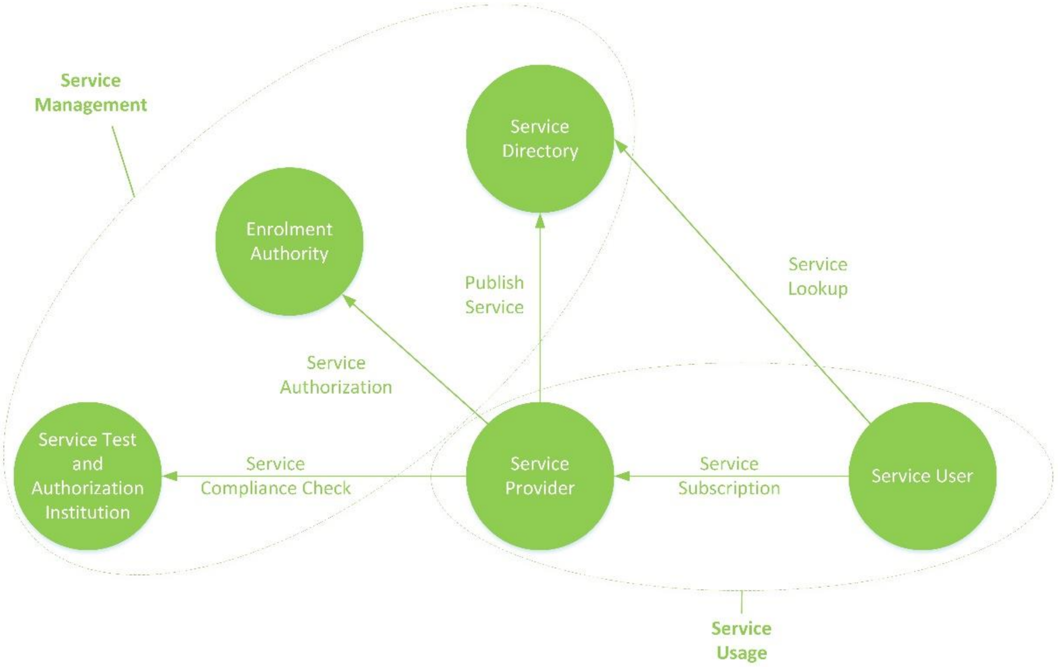


Figure 25: Service concept.

To ensure pseudonymity while consuming services, a concept of pseudonym service usage is necessary. This concept even supports decentralized billing. It is scalable and most importantly ensures that the service consumer cannot be track by third parties regarding the services they use or their usage patterns.

This concept utilizes the whole spectrum of PKI infrastructure and reuses the security concepts of pseudonyms and the infrastructure created for vehicle-to-x ETSI ITS G5 communication. Every service gets a dedicated identifier for the service: the so-called application ID (AID). For the service usage, a dedicated pool of pseudonyms is created and linked to the AID of the service. Additionally, those pseudonyms can be extended with service specific permissions (SSP). These permissions define exactly what type of message are allowed to be signed with a pseudonym. The Service Users use the pseudonym and his associated private key to authenticate itself against the Service Provider.

The following figure illustrates the concept. The Root CA (RA; one or more can exist) is the source of the certificate trust chain and acts therefore as a so-called security anchor. It certifies the underlying EA, AA and SPA. The Enrolment Authority (EA) is responsible for the identity of the service user. It ties his cryptographic identity to the user. The Authorization Authority (AA) issues a set of pseudonyms for the user. These pseudonyms are used by the user to secure the communication and protect its privacy. The services provider authority (SPA) issues certificates for the Service Providers.

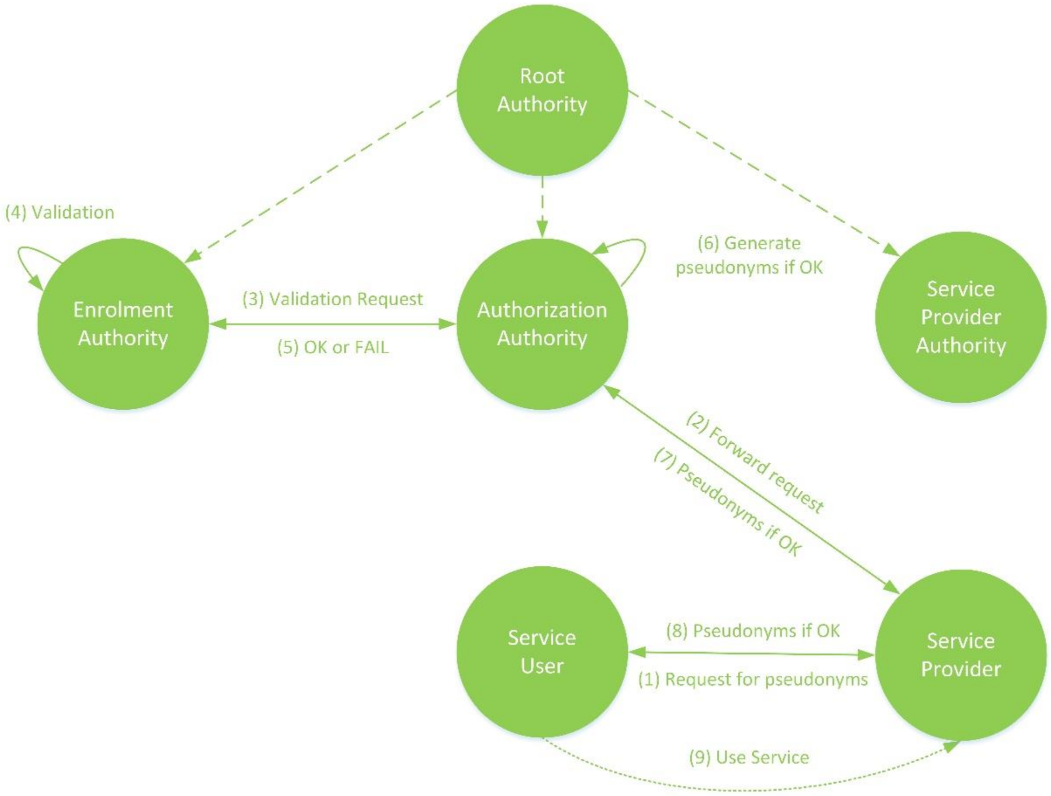


Figure 26: Pseudonymous service usage.

4.2.5 Role model

When creating software architectures, it is already best practice to create roles to specify behavior of logical elements. These roles describe which set of functionalities an actor who is fulfilling this role must provide to the architecture.

Roles therefore specify the responsibilities of each actor, without being tied to a specific entity. By abstracting the behavior, it is easier to identify, which set of functionality of an entity is necessary for the architecture. In addition, it is easy to replace the actor or introduce a second actor to also fulfill this role.

The behavior described by roles is called ’action’. Characteristics of actions are:

- Actions are complementary and/or neutral. This means, if an action is assigned to a role, further assigned actions may not contradict actions already in place.
- The contribution of actions for goal fulfillment of a role can be measured.
- The summarized actions can be implemented by an actor. If a role is oversized, so that an actor is not able to implement all actions, this role must be redefined.

As ubiquitous and straightforward as this approach is in the technical world, it is relatively rare and seldom used in economic fields. However, its various advantages could be used, if a role model, then called ’institutional role model’ is also used to describe the responsibilities of economic institutions. Economic institutions are firms, public authorities, federations, courts, and fixed institutions. They possess full action rights, property rights, and obligations to act as a social subsystem.

In traditional economics, technical roles are fulfilled by an institution. If e.g. a firm alone cannot take on the responsibility of fulfilling the role, two or more institutions might join and create a new organization. The foundation of a new organization takes time and is not cheap. Furthermore, this approach is not very flexible and fails, if one of the partners decides to leave. It is understandable, that institutions from different fields and with different interested will be differently strong invested in the various market phases.

To have the flexibility to cope with changing interest of institutions, it is wise to use the role model approach two-fold: First to identify and specify technical roles and second to specify roles for economic activities. The possible economic activities are grouped in so-called meta-roles:

- Business management takes place via a corporate management,
- Sales which contains the actions of sales and service offer,
- Procurement which contains the actions of procurement and data acquisition,
- Production which summarizes research & development, manufacturing, storekeeping and administration,
- Human resources which contains the actions of human resource management,
- Financial Management covers external and internal financing, and interior investment,
- Controlling does not contain the monitoring system, but all activities to make accounting and controlling possible.

With those meta-roles in mind, one can specify, how those roles should be taken by the different actors in the various market phases.

4.3 Analysis of Communication Protocols and Security

4.3.1 Communication Protocols

This chapter discusses the results of an initial communication protocol analysis. The goal is to introduce the technology from communication perspective and outline the challenges and working assumptions. Focus lies on the interexchange between machines and machines as well as protocol related essential human interactions. In addition, tool support is addressed specifically for RFID.

It is not the intention to cover all definitions of all protocol elements, as the elaboration of the protocol details is part of the actual project study scope.

4.3.1.1 The DAB standard

The Digital Audio Broadcasting (DAB) is a completely new technology for the broadcast and reception of radio stations. This new system within its digital format enables signals to be broadcasted in a quality that is comparable to CD quality [2] (p.421). Thus, listeners who have heard DAB digital radio have noted a significantly better sound quality and "presence" of the new radio standard [3]. Furthermore, the DAB avoids and mitigates multipath effects that often occur on FM transmissions [2] (p.421). Additionally, the system implements a single frequency network (SFN), which does not require returning when moving from one coverage area to the next [2] (p.421). As displayed below DAB (Figure 27) digital radio is now well established in many countries around the world from the UK and Europe to Canada, Australia and many other countries. It will replace the existing FM and AM broadcast station [4]. However, those are not the only advantages using the DAB standard.

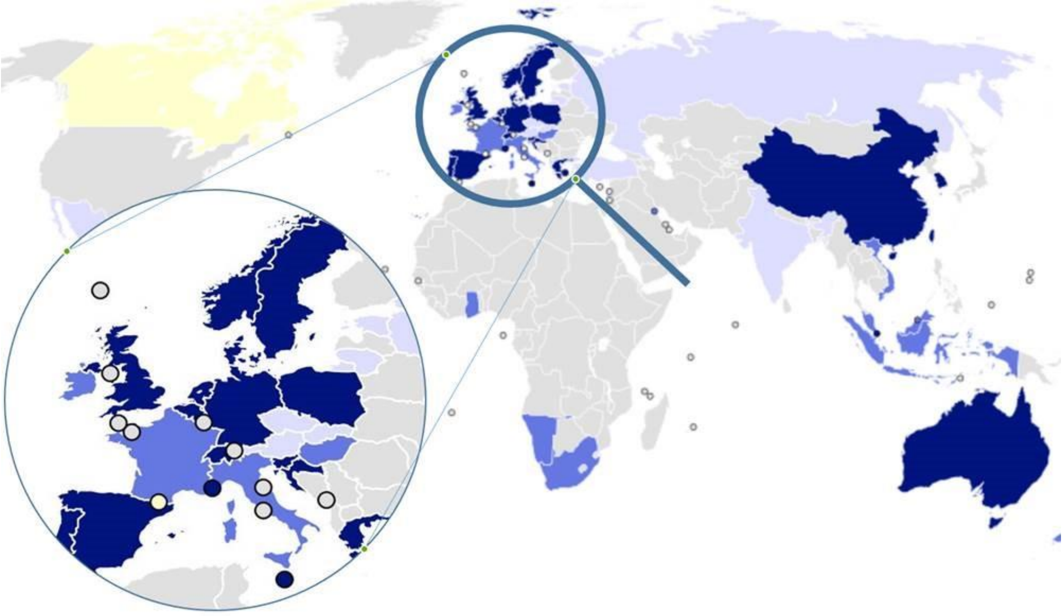


Figure 27: Distribution of DAB/DAB+[4]

■ Countries with regular services
▨ Countries with trials / tests
□ Countries with interest
🟨 DAB no longer used

New data service like Program Associated Data (PAD), Program Associated Data Slideshow (SLS), Electronic Program Guide (EPG) and most importantly Traffic and Traveler Service Information using Transport Protocol Expert Group (TPEG) technology can be transmitted via the DAB standard [4] (p.155ff).

For instance, the Program Associated Data is scrolling text, which is displayed on a small screen via the Digital radio sets, which carry the information about the program one is listening to [4] (p.43). This could be for example: a plot summary to a play, the details of the currently played track, websites, e-mail addresses, up to the minute sports news and even the upcoming program. Another option that comes with the data services is Electronic Program Guide (EPG), which enables the selection of programs by genre and pre-selection of the listeners preferences [4] (p.176ff). However, the most important standard in the context of the iKoPA project is the Transport Protocol Expert Group (TPEG) protocol, which will be discussed in more detail in the following.

[4] Source: https://en.wikipedia.org/wiki/Countries_using_DAB/DMB, CC BY-SA 3.0

4.3.1.2 TPEG Communication Protocol

TPEG stands for the format standardized by the Transport Protocol Experts Group and is a new mode of delivering traffic information via digital broadcast formats such as DAB, DMB, DVB or the Internet [4] (p.141).

The major use case for TPEG messages is the machine readability allowing the navigation system to semantically understand what is happening on the road and to take action upon this information. Therefore, TPEG may not have to absorb the driver's attention at all.

Data are coded prior to transmission and can be converted in a number of ways by the receiver. Motorists can either let a synthetic voice read information aloud or view information as text or in graphic form on a car's navigational system.

TPEG Messages are built with the following structure [5]:

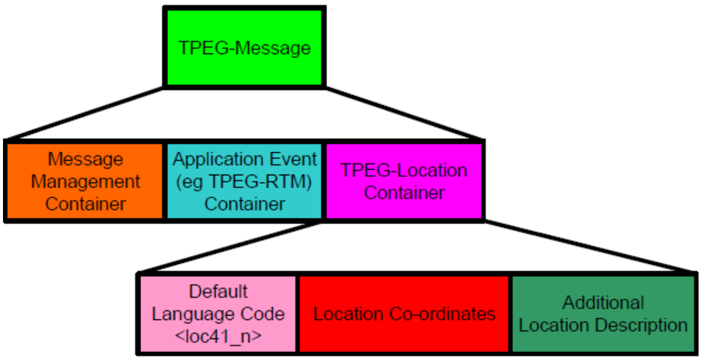

TPEG-Message
Message Management Container
Application Event (eg TPEG-RTM) Container
TPEG-Location Container
Default Language Code <loc41_n>
Location Co-ordinates
Additional Location Description

Figure 28: Principle structure of a TPEG message [5] (p.15)

- MMC - Message Management Container (when)
- APP - Application Container (what)
- LRC – Location Reference Container (where)

A short History review

One major motivation when defining TPEG was to overcome limitations and be ready for future challenges which clearly could not be addressed by the successfully established RDS-TMC service DAB offers outstanding capacity and speed, outstripping GSM and RDS-TMC; it has space available for a much more detailed and accurate coding method [6]. In the UK, the British Broadcasting Corporation (BBC) has allocated up to 8000bps of traffic and travel data on its DAB multiplexer. In September 1995, the BBC Digital Radio service went on air [6]. Then many organizations and companies decided to make the principle of RDS-TMC non-proprietary, not restricted to preassigned locations, and compatible with the DATEX data dictionary [6]. The Traffic Protocols Experts Group (TPEG) protocol was born. It has many advantages including the precise localization option on digital maps, the supplementary services for weather reports as well as large events [7] (p.1). To sum it up it is possible to bundle several services in the TPEG, which offer a large opportunity. Meanwhile the second generation TPEG-2 is in specification (ISO TS 21219-series). The following applications can be supported within the TPEG service (ISO TS 21219-series):

Traffic Event Compact application	TEC
Traffic Flow and Prediction	TFP
Fuel Price Information	FPI

Weather Information	WEA
Parking Information application	PKI
Electric-mobility charging infrastructure	EMI
Vigilance Location Information	VLI
Road and Multimodal Routes	RMR

The most important application in the context of iKoPA is the Parking Information application (PKI) and e-mobility charging infrastructure (EMI). These applications enable the transmission and reception of parking information as well as charging stations. The latter is used in the project to show the availability of charging stations for electrical vehicles. In conjunction with this data, the reservation via LTE can be done so that the user of the iKoPA Network System is able to get a use of the whole functionality of the integrated communication platform.

Please note: In the context of TPEG, you may come across “LTE”, which may be an abbreviation of “Light Encryption” and could likely be a source of confusion.

TPEG can be transferred via two carriers: 1.) Broadcast DAB, 2.) Point-to-Point via Cellular. In iKoPA, we are going to support both carrier methods, as they are complementary and choices can be made depending on the according needs.

Table 25: TPEG via Digital Radio and Cellular

Digital Radio	Cellular http
Fast update, pushed over the air, no need for data request	Large coverage possible
Only 1 system to operate, fixed cost for service providers only, none for users	IP connection shared with other vehicle functions
Allows cost free data transfer Lifetime license model, no data carrier fees to pay	Allows other customer specific location based services to be delivered
Not flexible for different customers	Map, location table and vehicle and OEM specific differences can be supported
Large data set for receivers – memory/message handling (solved with high scale integration)	Bandwidth concern
Inconsistent rollout	Subscription required → Cost

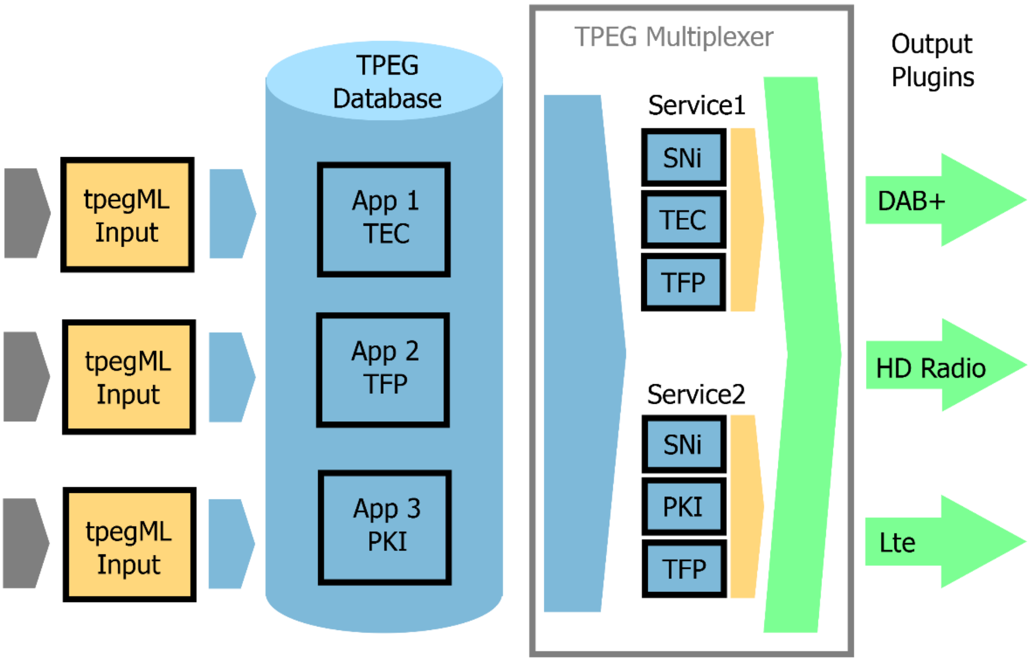


Figure 29: TPEG propagation technologies (own figure)

4.3.1.3 V2X protocols in general

The V2X communication protocol has to follow the standard:

> IEEE Standard 802.11p-2010 IEEE Standard for Information Technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. [16]

"At some point, IEEE 802.11p was considered for dedicated short-range communications (DSRC), a U.S. Department of Transportation project based on the Communications, Air-interface, Long and Medium range (CALM) architecture of the International Organization for Standardization for vehicle-based communication networks, particularly for applications such as toll collection, vehicle safety services, and commerce transactions via cars. The ultimate vision was a nationwide network that enables communications between vehicles and roadside access points or other vehicles. This work built on its predecessor ASTM E2213-03 from ASTM International. In Europe, IEEE 802.11p was used as a basis for the ITS-G5 standard, supporting the GeoNetworking protocol for vehicle to vehicle and vehicle to infrastructure communication. ITS G5 and GeoNetworking is being standardized by the European Telecommunications Standards Institute for Intelligent Transport Systems." [8]

Typical Use Cases for **V2V (vehicle to vehicle)** in this respect are:

1. Hazardous location warning
2. Slow vehicle warning
3. Traffic Jam ahead warning

4. Stationary vehicle warning
5. Emergency Brake light
6. Emergency vehicle warning
7. Motorcycle approaching indication

Typical Use Cases for **V2I (vehicle to infrastructure)** in this respect are:

1. Road works warning
2. In-vehicle signage
3. Signal phase and time
4. Probe Vehicle Data

The standard foresees a number of key communication elements, among which the following are considered the most relevant ones:

- Cooperative Awareness Message (CAM)
  - Type of Vehicle, Position, Speed, Heading
  - Broadcasted by all vehicles with 1 up to 10 Hz
  - Data elements for prioritization
- Decentralized Environment Notification Message (DENM)
  - Type of Event, Region of Event
  - Broadcasted by roadside infrastructure or vehicle
- Signal Phase and Timing (SPAT)
  - Status of traffic controller,
  - Prediction of duration and phases
  - Data elements for prioritization response
  - Abstract permissions instead of ambiguous colors
  - Permissions linked to maneuvers possible on specific lanes, represented in MAP
- MAP
  - Topological definition of lanes within an Intersection approach
  - Topological definition of connections between lanes
  - Type of lanes
  - Restrictions at lanes

The protocol stack comprises elements from Layer 1 (Physical) to Application layer. Below the structure with reference to the IEEE standards.

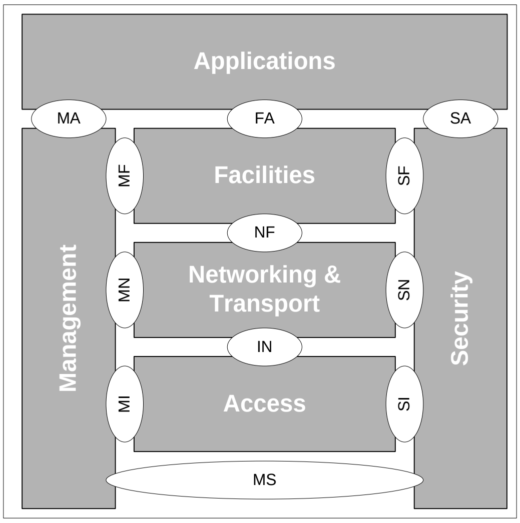


Figure 30: ITS Station architecture [9]

In iKoPA, we will for sure utilize the SPAT / MAP protocol.

Details of the data frames and elements in SPAT and MAP are specified in the following document on over 400 pages:

SURFACE VEHICLE STANDARD
J2735TM SEP2015
Issued 2006-12
Revised 2015-09
Superseding J2735 NOV2009
(R) Dedicated Short Range Communications (DSRC) Message Set Dictionary.

As the document is complex, we recommend you focus on:

page 32:	Definition von MAP Message
page 40:	Definition von SPAT Message
page 67:	Data Frame Intersection State (with links to other objects)
page 312:	Comments on 2014 Revision (Europe extension)
page 385-391:	MAP and SPAT use and operation

The European usage of these elements shall be standardized in ISO/PRF TS 19091 ”Intelligent transport systems -- Cooperative ITS -- Using V2I and I2V communications for applications related to signalized intersections”

V2X protocols in iKoPA

In iKoPA, from communication of the vehicle side, we are going to use

- CarPark Communication V2X – Trigger for automated driving
  - Position periodically
  - Route and route update
- V2X Traffic Light Forecast
  - SPAT
  - MAP
- V2X Authentication (CarPark)
  - Probably a proprietary protocol for Identification and registration of vehicles to complement RFID identification. The latter needs to be

    worked out in close re-use similarity to the concept applied in RFID, i.e. using Tag ID TID and authentication and pseudonymization methods.

- DAB and cellular communication
- Coupling with BYOD for Service Usage (and for displaying information)
- Vehicle Data Access (CAN), TimeSyncServer
- Possibly traffic situation info exchange via TPEG messages: Intelligent Transport Systems (ITS) — Traffic and Travel Information (TTI) via Transport Protocol Experts Group, Generation 2 (TPEG2) - Part 25: Electromoblity Information (TPEG2-EMI_1.0/001); TISA Reference: SP14003

SPAT/MAP for Traffic Light management

MAP will be produced manually for the test intersection(s) and will be added as integral part of the message. SPAT will be produced by the Traffic Light Forecast (TLF) service.

In case of IEEE 802.11p, one partner will take care that the data is available on the air-interface by implementing the RSU extension at the Merzig and possibly Berlin test side intersections and linking it to the TLF (Traffic Light Forecast) service.

Concerning Cloud-Interface to Traffic light forecast: it will provide an interface (HTTP; JSON or XML) – examples can be added on request) which delivers all forecasts on regular interval.

A **Service Provider** (App or TPEG service) has

- to select the SPAT forecasts needed,
- process further towards dissemination (usually a geo-based selection plus adding the MAP provided in a separate process).
    - Idea1 behind this concept: MAPs are static and do not need an update. Thus, they are only transferred when needed.
    - Idea2 behind this concept: a Service Provider always will have a mechanism for the right geo-selection for its client devices

A **service** (App/receiver) has

- to interpret the data and create a service (e.g. speed advice, time to green count down, start-stop engine, vehicle energy management, ACC, gearshift…)

4.3.1.4 RFID

4.3.1.4.1 Basic Concept

By using UHF (Ultra-High Frequency) RFID technology, items can be tracked in real time and traced through the entire supply chain, while providing full end-to-end transparency at the same time. UHF RFID systems offer a range of up to 20 m and the technology works up to speeds of 250km/h. It can be used for continuous tracking and real-time locating tools, products, trains, cars, reusable containers, and other assets over long distances within any monitored perimeter. Such perimeters can be hospitals, factories, cruise ships or more extensive environments like luggage systems of international airports or public transport systems. Since individual perimeters can be linked, RFID based real-time locating systems, can cover complete supply chains: From production over transport, storage and retail to the consumer – including product authentication, brand protection as well as consumer interaction.

Some selected iKoPA related key features could be named:

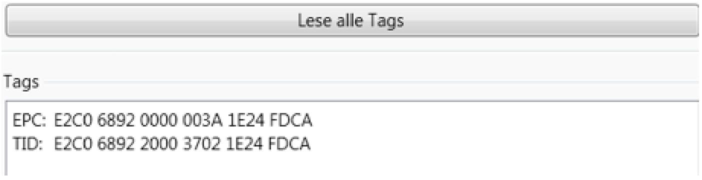
- Designed in accordance with GS1™ UHF RFID Gen2 v2.0 [Annex N, Tag Alteration (Authenticate)]
- AES (Advanced Encryption Standard) cryptographic authentication according to ISO/IEC 29167-10
- 96-bit unique tag identifier (TID), factory-locked with 48-bit unique serial number
- Tag authentication via 128-bit AES unique crypto key
- Privacy protection via Untraceable command and 128-bit
- AES group crypto key
- Trust Provisioning for Secure Secrets
- Tag authentication and privacy protection based on cryptographic security
- Long read/write ranges due to excellent chip sensitivity
- Hassle-free deployment even without significant security know-how or secure backend infrastructure

There are number of applications where combination of high read range with high security brings value:

- automatic vehicle identification (e.g. electronic toll collection)
- visitor / staff access control and location service (e.g. at theme parks)
- visitor classification and pre-processing (e.g. at border crossings)
- retail SCM / brand protection (e.g. expensive wines or fashion items)
- asset tracking (e.g. for high value assets)

In iKoPA the focus is on the first item: automated vehicle identification.

When programming RFID chips one distinguishes two parameters: EPC (Electronic Product Code) and TID (Tag ID). The TID is different for every RFID worldwide. It is composed out of a manufacturer code and a serial number. A live example of hexadecimal coded TID and EPC for an example RFID vignette is shown below. *Note*: The length of the TID can vary by tag and manufacturer. A live example for EPC and TID is given below. In this case, this is the Tag prepared as “iKoPA 5” before programming.



```
EPC:  E2C0 6892 0000 003A 1E24 FDCA
TID:  E2C0 6892 2000 3702 1E24 FDCA
```

Figure 31: Example of an RFID Identification pair – TAG number #5 iKoPA[5]

The TID is the Tag Identifier, and it is unique worldwide.

The EPC was developed on behalf of the US American industry by the MIT and is maintained today in collaboration between the Auto-ID Labs and EPCglobal, now GS1. GS1 International is an international industry collaboration entity seated in Brussels, working

[5] Source: Kathrein-RFID Reader RRU4 ReaderStart SW screen shot

on standardization of ISO. In case the EPC length is set to be 96-bit, the EPC is by default self-pre-serialized following a 96-bit EPC serialization scheme according to the multi-vendor chip-based serialization guideline meaning the lower 38-bit will always contain 3 bits for the manufacturer code (e.g. 111 for NXP) and 35-bit serial number taken from the lower 35-bits of the TID serial number.

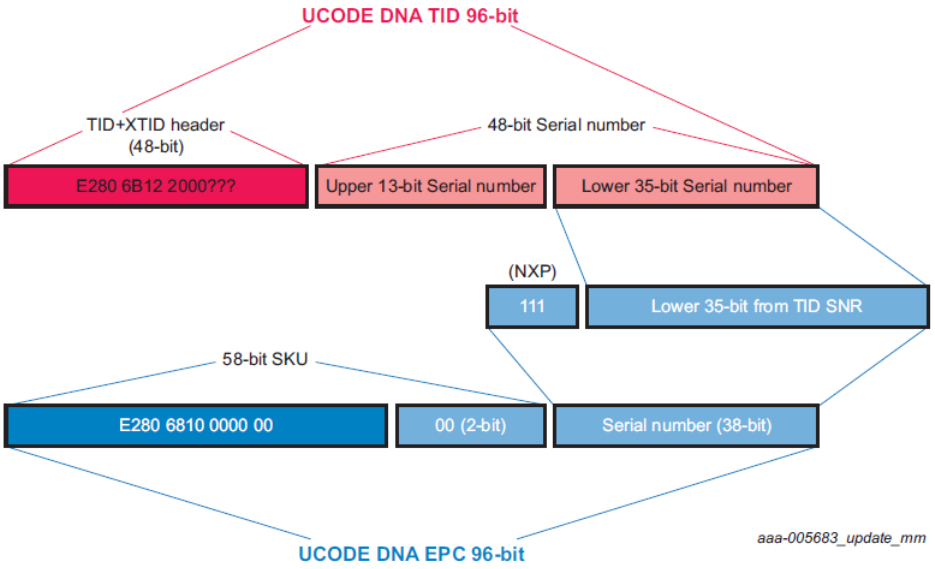


Figure 32: TID structure based on NXP Semiconductors SL3S50xxx UCODE DNA[6]

The industrial standardization organization GS1 (former Uniform Code Council (UCC)) and EAN International has been built for the definition of essential standards as well as marking and public relations for the EPC code, so a consortium EPCglobal Inc. was founded. GS1 International as newly arranged these activities in Brussels on international grounds. In Germany this task is organized by GS1 Germany, former CCG, located in Cologne (Köln).

Compatibility with other international standardization has been secured. Accordingly, the RF transmission for the electronic product code has been configured according to the rules for the various ISO standards ISO/IEC 18000-6C etc. Further standards define and regulate the compatibility with other code and key handling systems, e.g. the numbering system follows the international standard ISO/IEC 15418.

Short elaboration of the RFID reading technology [10][7]

[6] Source: NXP Semiconductors SL3S50xxx UCODE DNA fig.5

[7] For further information, please refer to NXP Semiconductors Germany GmbH UCODE DNA application note AN11778: “How to use the UCODE DNA”, to be requested from NXP marketing under NDA.

- Interrogator (=reader) to tag Link: An interrogator transmits information to the UCODE DNA by modulating a UHF RF signal. The UCODE DNA receives both information and operating energy from this RF signal. Tags are passive, meaning that they have no battery and receive all of their operating energy from the interrogators RF waveform. An interrogator is using a fixed modulation and data rate for the duration of at least one inventory round. It communicates to the UCODE DNA by modulating an RF carrier
- Tag to interrogator (reader) Link: Upon transmitting a valid command, an interrogator receives information from a UCODE DNA tag by transmitting an unmodulated RF carrier and listening for a backscattered reply. The UCODE DNA backscatters by switching the reflection coefficient of its antenna between two states in accordance with the data being sent.

In iKoPA, it is planned to utilize so-called passive RFID chips. These are based on purely passive, non-battery supported RFID ICs. These chips are power supplied via energy harvesting out of the received RF signal. The received energy is then used to supply the chip with power.

Depending on the transmitted power, the gain of the antenna and the physical implementation, matching and size of the RFID tags the reading distance can vary. In Europe the maximum transmit power is constrained by +33dBm. In return, the RFID transmits a response signal in half-duplex mode. The transmission is performed as a reflection of the received signal. This is also known as backscattering. Accordingly, the RFID chip transmits data by alternating between short circuit and matching impedance of the RF-input. The reflection is received by the transmitting device. For secured reception of the reflected signal at the RF input of the transmitter a signal level of -60 - -80dBm is expected. Taking into account the transmit signal of +33dBm the bridging across the overall signal path is at a level of 90-100dB.

Based on these signal constraints and the given hardware solution of available Interrogator and RFID tag we are typically reaching a read-out distance of up to 15 meters, i.e. a two-way signal distance of 30 m from and back to the interrogator device.

4.3.1.4.2 Communication protocol RFID interrogator – Car Park electronics

The chosen RFID interrogator Kathrein RRU4 comes with a separate RFID interrogator antenna, control interface (up to 4 GPIOs) and an Ethernet interface. Via Ethernet, two control interfaces are supported:

- Interactive protocol from a PC Software "Reader-Start" as well as a
- Low level communication protocol.

The latter is described in a document "Communication protocol Kathrein RFID UHF interrogator for RRU4, ARU4, M-ARU, ERU, RDR." This document is valid for all Kathrein RFID interrogator and describes the communication protocols, the commands and configuration parameters required for software development, the interrogator sends. Although reference is made in, the text to RRU4 respect, with the same commands can be controlled any other interrogator. The document can be ordered from Kathrein or downloaded from the home page but needs company registration.

The protocol is command and response transmission based and supports op-codes like: GPIOSetOutput, GetAntennaMod etc.

The interactive protocol from a PC Software “Reader-Start in contrast is meant to interact between humans and interrogator for test, configuration setting and scenario programming. E.g., definition of accepted EPC and TID pairs and intended actions is possible with the Reader-Start based control. Possibly for the iKoPA demonstrator we can live with the reader-start and do not need a sophisticated communication protocol. The advantage of Reader-Start is that the interrogator can also operate stand-alone without being controlled or serviced through Ethernet.

4.3.1.4.3 Key handling using RFID UCODE DNA

Bringing security to passive UHF, the UCODE DNA tag IC combines exceptional long-range contactless performance with a cutting-edge cryptographic security implementation for tag. The applied UCODE DNA with AES encryption feature comes with the following key security features.

- **AES Authentication and Privacy:** “UCODE DNA supports up to two 128-bit AES authentication keys. They are stored in the tag IC’s securely guarded internal memory, and can be pre-programmed and locked or inserted by the user. These cryptographic keys can be used for tag authentication or for privacy protection.” [11]
- **Trust Provisioning:** “To simplify development while strengthening the security of end applications, a Trust Provisioning service is offered which results in a UCODE DNA product that is ready to use as shipped. NXP’s unique service includes generating master passwords for Kill and Access, deriving individual Kill and Access passwords for each tag, and inserting these passwords into the tag. NXP also generates AES master keys, deriving all unique and tag-specific keys and then inserting them into the tag.” [11]
- **Key handling with Key 0 and Key 1:** UCODE DNA supports up to two 128-bit AES authentication keys: Key0 and Key1. They are stored in the internal memory of the tag IC and can either be pre-programmed or locked by NXP or can be inserted by the user. When not pre-programmed by NXP, the keys can be temporarily accessed (up until they are locked/confirmed) by addressing virtual user memory addresses.

Besides supporting all mandatory parts of ISO/IEC 29167-10, UCODE DNA also supports the following:

- TAM1 for Tag Authentication
- TAM2 for Tag Authentication with additional enciphered custom data
- security timeout
- three memory profiles (EPC, TID, User Memory)
- two operating modes:
  - No additional data (authentication only)
  - CBC-encryption of additional custom data, max. 128 bits
- two 128-bit encryption keys:
  - Key0 for Tag Authentication
  - Key1 for Group and Tag Authentication

For further information please refer to the NXP Semiconductors Germany GmbH UCODE DNA component description, which requires personalized NDA due to its confidentiality nature: “SL3S50xx Rev. 3.0 Jun 2015”

4.3.1.4.4 Authentication and Privacy using RFID UCODE DNA features

Today, urban applications are being developed in isolation, with dedicated teams addressing individual use cases in logistics, traffic management, parking, public transport, waste management, and so on. A higher layer of technology used to unify and aggregate these various use cases, creates the thread needed to connect everything and create genuinely smart and secure applications. A layer of trust, used to issue, derive, and authenticate identities, provides the security that is necessary to authenticate and determine any kind of assets.

The applied UCODE DNA with AES encryption feature comes with the following key security features.

- Tag authentication via 128-bit AES unique crypto key
- Privacy protection via Untraceable command and 128-bit
- AES group crypto key
- Trust Provisioning for Secure Secrets
- Tag authentication and privacy protection based on cryptographic security

UCODE DNA ensures privacy by allowing a tag to be securely identified and authenticated without unveiling its identity to its environment (e.g. avoid eavesdropping).

Following a scenario how **authentication** can be realized:

- During tag initialization, all parts of the memory which can be used for individual tracking (series number part of EPC, TID or the user memory) can be hidden with the **untraceable** command. Enough information still needs to be traceable to assign a single AES key (group key) to the tag.
    - **Key1** needs to be program as the group key (i.e. must be same for the whole product group) whereas **key0** should be programmed with an individual key diversified with a master key and the full EPC/TID as diversification input.
    - **AccessPW** needs to be set and locked (ideally unique for each tag) to prevent reading the hidden information directly. In the application (identification), parts of the EPC/TID which are not hidden should be identified by a standard tag inventory. This information is then used to select the group key applicable to this tag.
- As the next step, send the Authenticate (TAM2) command with **Key1** and request full encrypted EPC/TID. The responded data is used to determine the full EPC/TID.
- Then send the Authenticate (TAM1) command with **key0**. The responded data is used to fully confirm the authenticity of the tag.
- **AccessPW** should not be sent in the application at all, as this can easily be sniffed by attackers.

Data Processing after the communication (in secure environment):

- **Find the assigned group key** from the unhidden EPC/TID part (e.g. database) → group-key determined (key1).
- **Decrypt the full encrypted** EPC/TID response with the group key → full EPC/TID determined.

- **Derive the individual key** (key0) from the full EPC/TID and the master key → determine individual key (key0).
- Verify the TAM1 response of the tag by performing the same calculation with the individual key → **determine the authenticity of the tag** with the individual key.

4.3.2 Existing Security Mechanisms

4.3.2.1 Trusted Platform Modules

A TPM [12] is a Hardware Security Module (HSM) with a range of features beyond the traditional key management functionality present in most HSMs. One of the first scenarios for TPMs was a secure method for device identification. Smartcards were already widely deployed to enable secure identification, but only in the context of personal identification. A TPM is embedded directly on the motherboard and thus permanently bound to the computer (or embedded device). Thus, it could for example be used to identify a machine to a VPN, which enables an organization to restrict a VPN to only known machines. Moreover, in contrast to smartcards, as the TPM is present during boot time, enabling even more use cases. The Platform Configuration Registers (PCRs) can be used to store measurements of the platforms, i.e. a unique fingerprint of the software (BIOS, OS Kernel, etc.) running on the platform. Encryption or authorization keys can be bound to specific measurements, which in turn can give an organization assurance, that machines are running unmodified software, even if it is a remote system. The TPM also supports privacy sensitive applications with its capability to create attestation identity keys (AIKs), which are keys that cannot be liked to a specific TPM but it can still be proven that they were generated by a trusted TPM.

The TPM 2.0 standard is a complete overhaul of the TPM standard, which brings a range of powerful features. The most prominent are its algorithm agility, the enhanced authorization features and its implementation flexibility. In the previous standard, only the RSA encryption and signing standard were available to TPMs. The designated hash algorithm was the SHA-1 standard. The RSA algorithm is still considered secure, albeit requiring larger key sizes nowadays. The SHA-1 algorithm however can be considered broken and is being phased out. Instead of "hard coding" newer stronger algorithms, the standard opts for an agile approach, which supports a wide range of algorithms. The algorithms are identified by a regularly updated list of algorithm identifiers, of which a TPM must implement at least a specific mandatory subset.

The Enhanced Authorization features offer new possibilities for the setup of authorization conditions for TPM functionalities such as the restriction of keys. From simple password authentication, over signed policies, time based restrictions or counters; to even arbitrary logical combinations of these are possible. If secret keys where previously bound to specific PCR values, they can now for example be bound to values signed by the manufacturer together with a counter to enable downgrade protections (i.e. a key is only usable with a signed software with a version number that is equal or higher).

Lastly, the TPM standard became much more flexible in terms of its implementation. Previously the standard only intended a TPM to be implemented as a discrete physical chip. The TPM 2.0 standard offers a new wide range of possibilities, such as the integration of a TPM into a System on a Chip (SoC) or even as a "Firmware TPM" in form of a software.

Firmware TPMs require some form of hardware enhanced protection mechanism supported by the CPU of the system, such as a Hypervisor or Microkernel, or Memory Separation techniques like the ARM TrustZone and Intel SGX. While only a hardware implementation of a TPM, such as a physical chip or SoC, can offer the highest protection levels, Firmware based implementation may still offer enough protection for many applications while drastically reducing the cost.

In the context of iKoPA, the TPM 2.0 technology can serve as powerful building block to enable secure services. It can create, store and use secrets perform cryptographic algorithms. Furthermore, it can enforce protection policies, preventing unauthorized use of secret keys by third parties or malicious code.

4.3.2.2 Transport Layer Security

The "Transport Layer Security" (TLS) protocol (formerly "Secure Sockets Layer", SSL) provides communication security for two parties on a computer network. The most widespread use case of this protocol is securing "HTTP" web-traffic. The aim of the protocol is to establish an authenticated and (usually) privacy protected channel in a client-server setting. The protocol is designed to be "Crypto-Agile", i.e. designed to be extendable with arbitrary encryption or authentication schemes. The supported schemes are declared in so called "cipher suites", which define the schemes to be used for key-generation, authentication and encryption.

The protocol is started by the client with a handshake procedure. During this handshake, the client authenticates the server (mutual authentication is also possible) using a certificate based scheme[8] and negotiates the encryption parameters. A notable feature of this handshake is that it can support ciphers which guarantee "perfect forward secrecy" (PFS). In this case, the handshake is used with a key-agreement scheme -- for example the Diffie-Hellman protocol -- to generate new encryption keys for each connection. The PFS property in this case guarantees that even if the private keys associated with the servers' certificate are compromised, previous connections cannot be compromised as well. After the handshake is concluded, client and server have agreed on a cipher suite and encryption keys to be used for further communication.

In the context of the iKoPA project, we suggest the use of the TLS protocol in its most recent version (currently 1.2) to secure all communication routed over unsecured networks (i.e. the internet or networks not physically secured against third parties). In all cases a cipher suite featuring the PFS property should be used. Only unilateral authentication should be used in case of communication with users to preserve the privacy. In the case of communication between iKoPA services, mutual authentication is recommended unless an application specific authentication method is present. Authentication should be established with a PKI infrastructure.

Acceptable cipher suites are:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

[8] A signature scheme using certificates is the most common use case, but other schemes are also possible.

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

4.3.2.3 Security in V2X communication

Since V2X plays a vital role in the connected car, the trustworthiness of these V2X messages must be ensured. Therefore, messages are authenticated using digital signatures, proving their origin and integrity to the receiver.

Due to the ad-hoc nature of the application – others are not known upfront – keys for verification need to be exchanged dynamically. The use of public-key crypto simplifies that, because only the non-secret public key is exchanged. Certificate authorities, as part of a larger Public Key Infrastructure (PKI), authorize vehicles and roadside units to send messages by issuing certificates describing their digital identity and their permissions.

In addition, the privacy of the driver must be protected. Each vehicle can regularly change its identifier (“pseudonym”) to make it harder to identify or follow a specific vehicle. All these identities need to be managed by the PKI and once operational; it will likely be the largest of its kind.

The vehicle implementation also has to deal with some challenging requirements. The sender must ensure that the secret (private) keys that it uses to create the digital signatures cannot leak. Otherwise, they could be misused to send fake messages that go undetected. Such attacks could easily be scaled: a single compromised key could be cloned and be misused to affect smart traffic systems across a large geographic region, such as a complete state or country. A tamper-resistant Secure Element therefore provides the right level of protection for such keys.

On the receiver side, the main challenge is performance. Each individual vehicle sends messages at a low rate – in typical situations, no more than ten per second – but due to the broadcast nature of V2X, a receiver can receive hundreds of messages per second in crowded traffic situations with many nearby vehicles and RSUs. The signature verification for these messages imposes a big computational load and requires high-speed crypto accelerators to be integrated into the receiver.

4.3.2.4 Authentication Mechanisms

Authentication schemes aim to guarantee one of the following properties: the identity of a communication party (identification), or the origin of a message (data origin authentication). This divides the schemes in two major classes. On the one side are "offline" schemes, which bind an identity to a message, allowing the verification of the origin (and integrity) of a message. The prominent example are signature schemes, which can be used to "digitally sign" messages and documents. On the flip side are "online" schemes, which aim to prove the identity of an active communication party. Prominent examples are smartcards and tokens used to identify users of a web-service, or even something like a car key, which identifies itself to the car. An extensive guide to authentication mechanisms can be consulted in [13].

4.3.2.5 Signature Schemes

A signature scheme enables a user A to bind a message to her identity. This binding should be verifiable by any third party. As such, there are the following requirements to such a scheme:

- A signing method $S_{\mathcal{A}}(m) = s$ must exist, which maps a message m to a signature s.
- A signature verification method $V_{\mathcal{A}}(m, s)$, which any third party can use to verify a message-signature pair, i.e. by mapping it to a Boolean value.
- Modifying a message-signature pair (without affecting its verification outcome) must be impossible
- A signature should ideally be "non-reputable", i.e. the author of the signature should not be able to challenge the authorship.
- No third party should be able to forge a signature, even after obtaining a lot of valid message-signature pairs.

The common pattern of signature schemes starts with the generation of a key-pair (e, d), with e kept secret and d publicly distributed. The secret key e can then be used to generate a signature for a message, while the public key d is used by third parties to verify the signature. The security of these schemes depends on the difficulty of determining e from (possibly multiple) valid signatures (or from the public key d). Note that only public-key (or "asymmetric") schemes are suitable signature schemes. Schemes based on symmetric encryption cannot fulfill these requirements. These schemes are however very useful for verification of session-bound communication, and are called "Message Authentication Codes" (MAC).

Prominent example for signature schemes are the RSA signature scheme, and the DSA or its Elliptic Curve (EC) variant ECDSA. All of these schemes are suitable for the iKoPA project; on the condition of adequate key sizes (at least 2048 bit for RSA and DSA, and at least 256-bit for EC based methods).

4.3.2.6 Identification Schemes

An identification scheme is used actively by two participants, and aims to prove the identity of one participant to the other.

- Two users A and B participate in an exchange, after which user B (the verifier) is convinced of the identity of user A (the claimant).
- User A should be (provably) active during such an exchange.
- A listening third party should not be able to impersonate user A, even if such an exchange is intercepted often.
- In some cases, it is desirable that even user B is not be able to impersonate A after such an exchange, i.e. the identity is not transferable.

Any identification scheme uses one or more attribute of A as identification. These attributes are usually classified in three categories: knowledge, possession and inherent properties. Knowledge could be represented by simple passwords, PINs or cryptographic keys. Knowledge is usually combined with a something possessed, such as a secure smartcard or password generator. Inherent properties of a human user could be biometric attributes (e.g. a fingerprint). Computer chips can also offer inherent properties such as "physically uncloneable functions" (PUF), which are special circuits with properties subject to subtle manufacturing variations, and thus unique to every chip.

Password based Authentication

A weak but simple form of authentication are passwords. In its simplest incarnation, as shown in Figure 33, the claimant (A) authenticates itself to the verifier (B) by sending its identity (usually something unique like an E-Mail address or username is used) together with a password p. The verifier can then corroborate the correctness of the password by performing a lookup in a table of previously agreed upon passwords. This simple approach exhibits two problematic aspects:

- An attacker could impersonate the verifier to coerce the claimant to send the password, or the transmission could be intercepted
- The password table stored at the verifier must be read and write-protected against unauthorized third parties

$$\mathcal{A} \xrightarrow{\mathcal{A}, p} \mathcal{B}$$

$$H(p|s) \overset{?}{=} H(p_{\mathcal{A}}|s)$$

Figure 33: Authentication with passwords

To avoid eavesdropping or impersonation, the exchange must be performed in a private and authenticated manner, i.e. A must first authenticate B and establish an encrypted connection. To reduce the strong storage requirements for the password table, a one-way function – such as a hash function H – may be used to protect the password. Instead of storing the password itself, the verifier stores the hashed password, i.e. $H(p)$. During the password identification, the verifier now hashes the received password and compares to the stored hash. To further protect against dictionary attacks, in which an attacker uses a dictionary of password and hash pairs to resolve a stored hash to a password, the verifier uses a "salt" value s during hashing. A salt value in this context is a random t-bit string, which is concatenated to the password prior hashing. This way, an attacker would require a dictionary with 2^t variations of each stored password. Further measures to increase the required workload of a dictionary attack could also include a fixed iteration count of H, i.e. by repeatedly using the hash function. Common key-derivation functions like "PBKDF2" or "scrypt" may be used to facilitate this.

Password based authentication cannot fulfill all properties listed in Section 4.3.2.6. The verifier could for example impersonate the claimant after an exchange, as the verifier receives and stores the password. This is in most cases not problematic -- for example if the verifier is a centralized service such as a website -- and a well-accepted method of authentication. The security of this mechanism however relies[9] on the privacy of the connection and prior authentication of B by A.

[9] Apart from the strength of the password, which could be enforced by one or both parties.

Challenge response authentication

A much stronger method of authentication is offered by "Challenge-Response" identification. During challenge-response protocols, the claimant proves knowledge of a secret without revealing by introducing a time-variant challenge. The challenge is typically chosen by the verifier and sent to the claimant, who in turn constructs a response which depends on the secret and challenge. One way to construct such a protocol is to use an encryption function[10] E_K with a previously shared key K, as shown in Figure 34. The claimant then encrypts the challenge and sends the result to the verifier, which decrypts and checks if the result matches the expected challenge. The encrypted challenge serves as a proof knowledge of K and also proves that the claimant actively participated during the protocol. A stronger alternative to an encryption function with a shared key is the use of a signature scheme. In this case, the claimant signs the challenge with a signature scheme and the verifier simply checks the signature.

$$\begin{tikzcd} \mathcal{A} \arrow[r, bend right, "2.\ \mathcal{A}, E_k(c)"'] & \mathcal{B} \arrow[l, bend right, "1.\ c"'] & c \stackrel{?}{=} D_k(E_K(c)) \end{tikzcd}$$

Figure 34: Basic challenge response authentication with a symmetric cipher

The security of this protocol relies on the security of the encryption function, and the freshness of the challenge. The challenge must have an origin subsequent to the beginning of the protocol. The challenge could for example be a random number or string chosen by the verifier during the protocol. In this case, the chance of guessing the challenge prior the protocol must be negligible; otherwise, an attacker might guess the challenge and construct a valid response by interacting with the claimant. Another possible challenge could be a sequence number – which the verifier must check to be strictly monotonic – or a timestamp.

Distance Bounding

Some applications, such as access control (e.g. door locks or car keys), have a further requirement. In these cases, the location claimant must be verified as well -- i.e. the distance between the claimant and verifier. If this distance is not bounded, relay attacks (also called mafia attacks) are possible. The attacker could simply establish a relay between the claimant and verifier by forwarding challenge and response (see Figure 35), and gain access. A prominent example is a radio attack on wireless electronic car keys [14]. The attackers simply amplified and relayed the radio signals between car and keys,

$$\begin{tikzcd} \mathcal{A} \arrow[r, bend right, "3.\ \mathcal{A}, S_{\mathcal{A}}(c)"'] & \overline{\mathcal{B}} \arrow[l, bend right, "1.\ c"'] \arrow[r, leftrightarrow, "\mathcal{E}"] & \overline{\mathcal{A}} \arrow[r, bend right, "4.\ \mathcal{A}, S_{\mathcal{A}}(c)"'] & \mathcal{B} \arrow[l, bend right, "2.\ c"'] & V_{\mathcal{A}}(c)? \end{tikzcd}$$

Figure 35: A relay attack on a challenge response authentication

[10] Another possibility is a keyed hash function or a MAC.

and succeeded to unlock and start vehicles in the driveway, with the keys located further away (e.g. in the house).

Relay attacks can be mitigated, however with very limited effectiveness. A physical protection could be employed to hamper relay signals, for example a shielded card input in automated teller machines. A physical detection of a relay may be employed, e.g. by detecting amplified signals. Both of these measures depend on the application, but are likely to be circumventable or error prone. A last measure is a "presence detection" of the user, for example if the car key requires a button press to perform the protocol instead of performing it automatically.

Another method are distance-bounding protocols. These protocols usually consist of a repeated exchange of random bits, as shown in Figure 36. Both the verifier and claimant rapidly exchange random bits, while the verifier measures the round trip time of each message. All random bits are then concatenated and serve as a challenge for a challenge response method. The round trip time then serves as a measure of distance for the verifier. As relay methods introduce a latency by nature, the verifier simply sets an upper bound for acceptable time, as the round trip together with the speed of light determines the maximum physical distance.

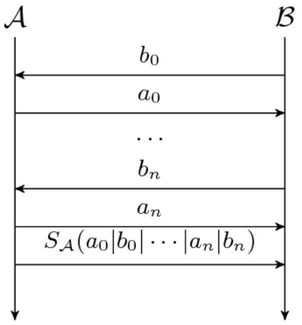


Figure 36: A basic distance bounding protocol

4.3.3 Challenges and Problem statements in iKoPA

In this chapter, we will discuss the challenges and problems of the communication protocols with regards to the iKoPA project.

4.3.3.1 TPEG Electric mobility charging Infrastructure (TPEG2-EMI)

The TPEG2-EMI plays a significant role for the success of the project. It will enable the whole functionality of broadcasting and reception of the parking and charging functions, namely the availability of charge points in the supported target car parks or single charging stations in the field. The challenges of the creation of such service will be the appropriate integration of TPEG2-EMI in the universal architecture, i.e. the syntax as well as the semantics. After this, one can deal with the technical specification, implementation such as the installation of a backend server transmitting the required information of the availability of the charging and parking facilities as well as the appropriate reception. On the transmission side, it is planned to use EMI over the DAB channel and on the reception side, DAB will be integrated in a special hardware for communication. Also on the transmission side, the following challenges are most eminent for the iKoPA project:

Challenge/Problem integration of EMI in a general architecture, supporting hybrid (broadcast and connected) information dissemination framed by a data collection and data usage block

On the reception side, the key challenge will be the integration of the TPEG decoder, which will decode the TPEG PKI and extract the most important information for the user. For both, IP and DAB based TPEG messages; the TPEG decoder has to be merged into the middleware in order to develop a functional software application. However, this is more part of the integration and system application level and not so much an issue on the level of communication protocols. Therefore, it will not be discussed further.

TPEG EMI is specifically designed to deliver information about charging infrastructure and includes structures and concepts from current e-mobility products and regulations used in the market. Even TPEG EMI in its version 1.0 might need some adaptions and tweaking, according to the research and findings in iKoPA it provides a good base how e-mobility information and entities are structured.

TPEG EMI allows the description of so-called “charging parks”, in a detailed structure, including standardized and regulated identifiers for charging equipment. The amount and availability of different charging adapters can be described, in combination with the precise location, entry and exit of a charging park.

The TPEG EMI concept follows the broadly accepted market paradigm of e-mobility providers and charging park operators that work together by establishing a framework of eRoaming agreements. The consumer (driver) has its contractual relationship with the e-mobility provider but is able to use various charging parks from different charging park operators, due to these roaming agreements. TPEG EMI allows the description of all relevant information about the available roaming agreements and thus allows a user to understand, based on the TPEG EMI information, which charging park he might use, according to its personal e-mobility contract.

In addition, TPEG EMI allows showing the availability of charging points, by explaining how many of them are currently occupied, respectively are free. This is, in contrast to most other data, dynamic information that shall constantly be updated, where a TPEG EMI DAB broadcast service comes in handy.

Both, the static and the dynamic information are relevant for iKoPA, as the intention is to support a driver by planning a trip and a parking stop with an available charging point. To know where relevant and compatible charging parks are located, and to have knowledge about their current free capacity is vital to fulfill the iKoPA use cases.

As a third field of functions, TPEG EMI comes with an included reservation concept and protocol. Without leaving the domain of TPEG EMI it is therefore possible to handle reservation requests and responses. As iKoPA intends to establish a reservation functionality for a charging spot, the TPEG EMI reservation concept might be quite helpful. Even if the project decides not to use it directly, it might still give essential hints, how reservation shall be designed within the existing market situation of e-mobility. Furthermore, TPEG EMI tries to support the given market situation and found e-mobility concepts, without enforcing them. At various elements in its data structure TPEG EMI allows to stay partially independent from e-mobility identifiers like EMAID and EVSE by making them optional [15].

iKoPA intends to discuss various aspects of the TPEG EMI protocol, anent its privacy issues, that have not been thought of, when TPEG EMI was created, e.g. whether anonymous or pseudonymous usage is feasible or if an opt-in to special privacy agreement will be needed. These questions arise when changes in the free capacities are published, especially in small charging parks, and in charging parks (almost) full or (almost) empty. This includes reservation management, as it implicitly needs to publish information whether there are free capacities left and thus if a reservation is possible at all.

On the other hand, questions arise about possible denial of service attacks, by using vast amounts of reservations. In case of anonymous reservation options, it would be easy to undertake such an assault, causing a significant economic damage, by blocking out any real customers. Thus, mechanisms are needed to limit such an attack vector. A deposit could be a possible solution, if it is possible to make it compatible with privacy and concepts about the customer relations.

Such a deposit could as well help with another problem: a driver might fail to give way and remove its car from a charging point, after charging is complete and reservation period ends, effectively blocking out other customers again. This might even compromise following reservations, if it is allowed to reserve a charging point in advanced. iKoPA needs to decide whether it will allow reservations only if a charging point is currently free, or if it shall be possible to make reservation for the future in assumption that other vehicles will leave the point when their reservation window has ended. If only free charging points can be reserved, they might immediately be physically blocked to ensure that it will stay free until the reserving customer has arrived. On the other hand, this will block out intermediate customers, leading to the consequence that the window for reservation prior to arrival must be limited to a reasonable short period, e.g. 30 minutes, to avoid long periods of blocking.

Despite these thoughts and the e-mobility provider contracts that are often used to handle payment, it would be possible to allow anonymous booking, by just requesting a charging point for a given time and receiving an acknowledgment in combination with a secret token, that allows access and identification at the charging park. By using such a secret reservation token, it might not even be necessary to scan the number plate of the vehicle or to use any unique user-ids, if the problems (denial of service, blocked charging point, deposit, payment) are solved or accepted otherwise.

In general, it is important to avoid premature binding of the driver and/or vehicle to a specific e-mobility provider and to allow flexible switching between e-mobility providers and contracts. A flexible concept could work like this:

> First, the driver must acquire an “electric fuel card” (similar to conventional fuel cards). Each driver may have its own electric fuel card and each driver even might have multiple of these electric fuel cards that it might freely choose from and switch between them, to reduce linkability. This would work best if a specific fuel card supports a prepaid concept, is payable by cash and avoids any bank account data or other personal information.

Potentially this electric fuel card nevertheless enforces a judicial opt-in to handle privacy issues. In addition, the electric fuel card shall allow deposit functionality, to handle denial of service threat and failure to remove car from charging point. The deposit would be locked at the moment a reservation is granted, and will be freed up again, the moment the vehicle leaves the charging point.

Included in the electric fuel card would be some kind of account id. The e-mobility provider shall include initial information where and how relevant information services could be accessed. In theory, the electric fuel card could be designed to fit into a slot in the vehicle and support automatic transfer of configuration and initialization of the systems. By just swapping cards drivers could easily reconfigure all systems and use different pseudonyms, payment methods and information services. The vehicle systems read this information from the electric fuel card and use it, e.g. for reservation, deposit handling, charging and payment, without the need for the driver to enter any data manually.

The initial configuration from the electric fuel card shall be used to tell the system where it could access DAB TPEG EMI services or where it could access a similar internet based HTTP TPEG EMI service that delivers information about charging parks compatible with the e-mobility contract, stored on the electric fuel card. This would allow the development of a flexible, unbound, but easy to use and complete service package.

A relevant protocol for executing eRoaming is called OICP. It can be retrieved after registration from the web under the link: https://www.hubject.com/downloads/oicp/.

Further information concerning the communication protocol TPEG EMI can be retrieved from the TISA organization.

4.3.3.2 TPEG Parking Information Application (TPEG2-PKI)

One application in the context of the iKoPA project can be the Parking Information Application (TPEG2-PKI). This application enables the transmission and reception of parking information, which is used in the project to show the availability of charging stations for electrical vehicles. Since the electrical charging station will be installed at a dedicated parking lot, the charging station could be seen in a simplified way as an attribute of that parking lot. Therefore, no far-reaching modifications of the original application are needed. It would still serve the same purpose and would only be extended to the charging station status. In conjunction with this data, the reservation via cellular communication can be done so that the user of the iKoPA Network System is able to get a use of the whole functionality of the integrated communication platform.

Please note: In the context of TPEG2-PKI there is also a possibility to distinguish “fuel type” combustion vehicles from “electricity” vehicles, but details on plugs, providers, IDs etc. are missing. Therefore, it may be clumsy to distinguish parking lots from charging lots. In addition, there seems to be no support for reservation. Accordingly, TPEG2-PKI may be suited for pure car cark signaling, but for electrical vehicles and reservation services EMI seems to be more suited.

4.3.3.3 Considerations for Reservation service and automated Car-Park entry

Use cases 1, 4, and 8 describe scenarios, in which a user reserves a parking lot in a car park. The user drives the vehicle to the car park, which detects the presence of the user and grants access (i.e. by raising a barrier or unlocking a charger). These use cases require an access control system, with the following capabilities:

- A user must be able to be registered in the system.
- A user must be able to request a reservation for a parking lot at a desired car park.
- A confirmed reservation authorizes a user to enter a car park, and consequently
- A car park must be able to identify and verify users and vehicles with a valid reservation.

- These capabilities must be implemented while using only a minimal amount of identifying information about the user, following the principle of data minimization.

Use case 4 describes an identification of the vehicle via the V2X protocol, while Use cases provides an identification using an RFID chip embedded in the license plate (or windshield) of the vehicle.

4.3.3.3.1 Access control via V2X

As V2X enabled devices usually feature powerful processors, sophisticated authentication schemes can be used. In this context, we propose the use of a public-key protocol, such as the Schnorr identification scheme[11] or a signature scheme. The main challenge for the access control via the V2X protocol is distance bounding. The protocol cannot guarantee a low enough latency between messages to perform distance bounding. An attacker could drive up to the car park and relay the V2X authentication to a vehicle driving miles away[12]. To thwart a relay attack, a user presence detection should be performed, for example in the following way:

- An authentication protocol between car and car park is started
- A confirmation request is displayed to the user in the vehicle
- The user confirms with a physical interaction (e.g. button press in the vehicle or on the personal device)
- The car only completes the authentication upon confirmation

The V2X authentication use case has not been part of the standard of the IEEE 802.11p standard message types, which were discussed in the previous section. However, the authentication plays a vital role in the connected car. Therefore, it could also be very relevant for the IEEE 802.11p standard to adopt a message type, which could be used for authentication. The aim of the iKoPA project will be to come up with a message type for authentication fitting the purpose and security and privacy needs of the connected car. Considering that RFID will also be implemented for authentication in the project, the AES 128 standard could be a feasible communication protocol to implement also into the IEEE 802.11p for the authentication. The development and testing of the new message type will be part of the project work and has to be analyzed throughout the project. Consequently, it cannot be addressed in this analysis. Due to its novelty, V2X Authentication has the potential to become standardized.

4.3.3.3.2 Access Control with RFID Tags

The main challenge in this scenario is the limited functionality of the RFID tags. By nature, these devices can only perform authentication protocols based on a symmetric encryption function. Any party in possession of the secret stored within these tags can:

- Perform the authentication, i.e. impersonate the RFID tag.

[11] https://worldwide.espacenet.com/publicationDetails/biblio?locale=de_EP&CC=EP&NR=0384475#

[12] Note that light travels about 300km in one thousandth of a second.

- Uniquely identify the RFID tag itself, and thus track the vehicle.

Hence, the requirements for the secure storage and usage of the key are raised immensely. It must be ensured, that only the necessary parties --- i.e. the identity provider, the barrier and the tag itself --- are able to store and use the secret.

To prevent the corruption of the secret key it should be ensured to only communicate those data, which are required in the specific case in hand, or which it has consciously been decided to disclose to others (need-to-know principle). These requirements can be enforced by a TPM. For example, if a TPM is embedded into the RFID interrogator of the barrier, it would be possible for the identity provider to encrypt the secrets in a way that only the target TPM is capable of decrypting it. Furthermore, the key can be coupled with conditions, which must be met for its use, which will be enforced by the Enhanced Authorization features of the TPM 2.0 standard. The key could for example be restricted for use during a certain time (i.e. only during the reserved time slot), and only if the software loaded within the reader is not manipulated. The RFID interrogator could also use the TPM directly as a coprocessor[13], in which case the secrets would never even have to leave the TPM, completely unreachable for any third party. To further protect the privacy of RFID users, future RFID-TAG solutions should be able to change their ID and use a (shared) secret per authentication triggered and set by an external application. With that RFID-TAGs cannot be used to track or identify users.

4.3.3.4 Conclusion

The Connected Car is a complex IT system on wheels, consisting of many ECUs (forming the vehicle’s “brains”) that are linked together via the in-vehicle network (its “spine”). To secure all of this, an integral approach is needed where countermeasures are applied at all levels. Most prominently, the Connected Car needs:

- Secure authentication at its external interfaces, to prevent unauthorized access.
- Secure communication on its in-vehicle network, as well via its external interfaces, to prevent data theft and manipulation.
- Firmware protection and update, in the form of secure boot and secure OTA updates

The exact security requirements for a specific vehicle shall be determined using a thorough risk analysis that must be part of its design process. Furthermore, the security architecture and its implementation needs to be managed during its entire lifecycle, which means that it requires for example active key management and secure firmware updates.

[13] Depending on the technical feasibility on the side of the RFID interrogator.

4.3.4 Security

4.3.4.1 Authentication mechanism for Reservation Functionality

In this section, we give an outlook on a possible system architecture for the reservation functionality described in section 4.3.3.3. The architecture offers a secure method of authentication between a vehicle and the car park access control facilities (e.g. a barrier), while preserving a user's privacy by providing a pseudonymization mechanism. The components and their communication sequences are shown in Figure 37. The backend components, an identity provider, a reservation service, and the car pack backend are shown on the top. The front-end components are the User, either represented by the smartphone or the vehicle, and the access control at the parking lot, for example the barrier.

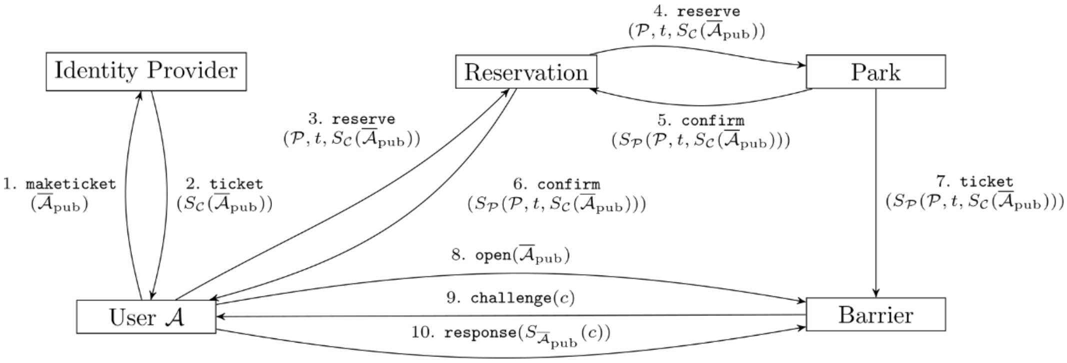

4. reserve $(\mathcal{P}, t, S_{\mathcal{C}}(\overline{\mathcal{A}}_{\text{pub}}))$
Identity Provider
Reservation
Park
3. reserve $(\mathcal{P}, t, S_{\mathcal{C}}(\overline{\mathcal{A}}_{\text{pub}}))$
5. confirm $(S_{\mathcal{P}}(\mathcal{P}, t, S_{\mathcal{C}}(\overline{\mathcal{A}}_{\text{pub}})))$
1. maketicket $(\overline{\mathcal{A}}_{\text{pub}})$
2. ticket $(S_{\mathcal{C}}(\overline{\mathcal{A}}_{\text{pub}}))$
6. confirm $(S_{\mathcal{P}}(\mathcal{P}, t, S_{\mathcal{C}}(\overline{\mathcal{A}}_{\text{pub}})))$
7. ticket $(S_{\mathcal{P}}(\mathcal{P}, t, S_{\mathcal{C}}(\overline{\mathcal{A}}_{\text{pub}})))$
8. open$(\overline{\mathcal{A}}_{\text{pub}})$
9. challenge(c)
User $\mathcal{A}$
Barrier
10. response$(S_{\overline{\mathcal{A}}_{\text{pub}}}(c))$

Figure 37: Message sequence reservation process

The backend services of the registration and the reservation are split systems to enhance the privacy protection of the user. The identity provider fulfills the role of a trusted party for all systems components. It contains all the registration information of the users (e.g. identity), and serves to create and attest to pseudonyms (a key pair for an identification scheme) which participants can use to identify themselves to other services. Other services in turn use the trust in the identity provider to verify the validity of the pseudonyms, while not being able to resolve the identity behind the pseudonym. Hence, the first step of a registered user in a reservation process is to create a fresh pseudonym, which the identity provider will certify, as shown in messages 1 and 2 in Figure 37. A user will then contact the reservation service under this pseudonym and transmit the desired reservation data (e.g. the car park, time, etc.), shown in message 3. The reservation service will forward this request to the car park, which will confirm the reservation (if resources are available) by signing the request and returning the information to the user as shown in messages 5 and 6. This signature should be non-reputable and serves as proof of the reservation for the user. This is called a ticket in this context. This ticket now contains all the reservation data (car park, time, and the users' pseudonym) and is signed by the car park. The user can now approach the car park barrier and transmit this ticket to the barrier. The barrier is able to verify the ticket with the public key of the car park, and could potentially work "offline" (making message 7 obsolete). The barrier should however still perform a challenge response authentication (message 9 and 10) with the vehicle to obtain a proof of identity.

4.3.4.2 Key handling principles and considerations for RFID Authentication

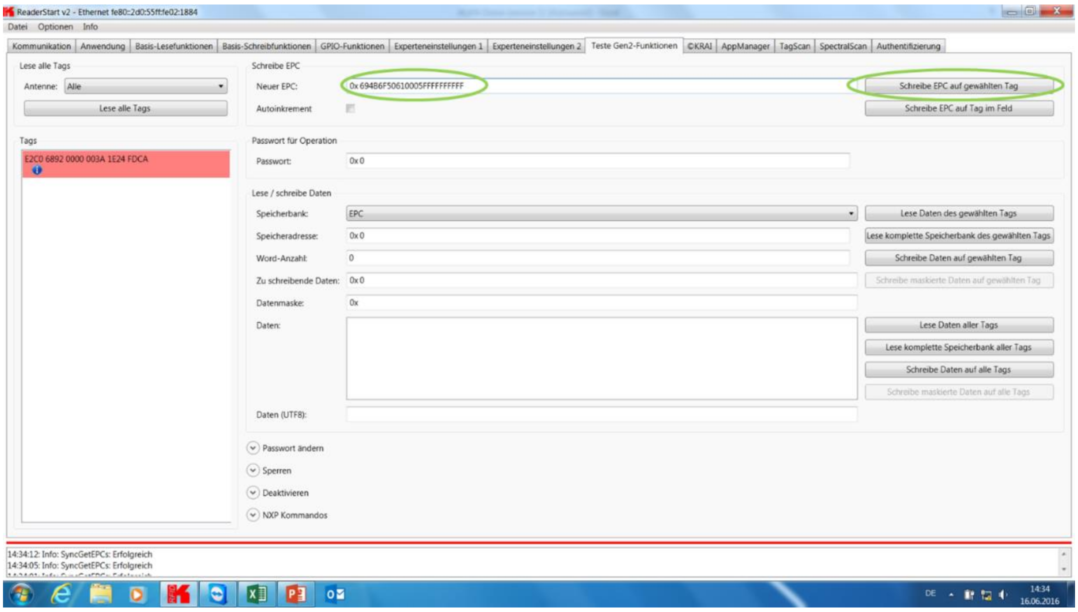
Section 4.3.4.1 described a general architecture, which may be used as an authentication mechanism at the car par barrier. In the case of a V2X based authentication, this architecture could likely be implemented without major modifications. In the case of RFID, however, many modifications must be made due to the nature of the tags. This section describes possible design options to solve the challenges and requirements mentioned in section 4.3.3.3.2.

4.3.4.2.1 iKoPA RFID tags, Examples and Test environment

In iKoPA it is proposed to use a group of RFID Tags with EPC/TID containing the text "iKoPA", i.e. the hex sequence **0x 69 6B 4F 50 61** followed by a serial number of the demonstrator series.

Details, numbering and prototyping will have to be determined in the course of the project. The following figure shows the user interface of the development environment. For testing a Kathrein RFID interrogator with ReaderStart Firmware version v2 2.55.00 is used.

A new ID can be programmed as shown in the example of a screenshot below.



ReaderStart v2 - Ethernet fe80::2d0:55ff:fe02:1884

Antenne: Alle

Tags: E2C0 6892 0000 003A 1E24 FDCA

Neuer EPC: 0x 69486F50610005FFFFFFFFFF

Passwort: 0x 0

Speicherbank: EPC

Speicheradresse: 0x 0

Word-Anzahl: 0

Zu schreibende Daten: 0x 0

Datenmaske: 0x

14:34:12: Info: SyncGetEPCs: Erfolgreich
14:34:05: Info: SyncGetEPCs: Erfolgreich

Figure 38: RFID EPC re-programing iKoPA format[14]

4.3.4.2.2 Secure Key distribution between the systems components

As described in section 4.3.1.4.3 to 4.3.1.4.4, the UCODE DNA RFID tags can be employed to mask any identifying information to an UHF RFID reader, unless an authentication with a group-key (key1) is performed. This feature can be used to protect against tracking by

[14] Source: Kathrein-RFID PC-SW "ReaderStart v2.55", screen shot.

third parties. For example, the tags used in the iKoPA group could be protected with this feature, only revealing information to iKoPA RFID interrogators, which possess a secret group key. Hence, the requirements for storage and usage of such a group key are considerably high. TPM technology can in turn be employed to protect such a key. The secret key can, for example, be transmitted in a manner that only a TPM could use it. In this case, a TPM could be integrated into the RFID interrogator and receive this key in such a format. Due to the enhanced authorization features of TPM 2.0, the key can not only be restricted for the use in the interrogator, but also be restricted to a specific software-state, preventing the use of the group key by manipulated RFID interrogators.

A similar method can be used to distribute the tag authentication key (key0). As mentioned in section 4.3.3.3.2, this key will not only uniquely identify a tag, but also allow impersonation. As such, this key should only be distributed in a “need-to-know” manner, restricting it to components, which require it to implement (parts of) use cases. The most obvious components, which will require the key are the tag itself and the RFID interrogator, but other components to be identified may require knowledge of the key in order to enable the distribution of the key to the RFID interrogator. In the following, two possible key distribution mechanisms are described.

Centralized Key Distribution

During initialization of the tags, keys are generated by a service and programmed into the tags. The service then also stores the keys and maps them to an identifier. The identifier then serves as a handle, which the owner of the tag (the user) can use during a reservation to indicate which RFID tag will be used to authenticate in front of the barrier. The central key service would then need to securely distribute the keys behind the identifying handles to the barriers or the respective RFID interrogators.

Decentralized Key Distribution

Instead of using a centralized service, each user could be responsible for the storage and distribution of the keys their respective RFID tags. During a reservation, a user would need to transmit the key of the tag securely to the RFID interrogator of the destination. This method has the clear advantage, that no central service has the knowledge of all keys, or the capability of mapping keys (and in turn RFID tags) to users. The tag initialization, however, is slightly more complicated. Either a user must initialize a tag him or herself, which may be impossible for some users due to technical constraints, or tags are initialized by a service and paired with a copy of the key, which is then distributed to users. For example, the tags are produced and programed with the key, which is also printed onto some documentation in machine-readable form (e.g. a “QR-Code”). A user could then purchase anonymously in a store. The machine-readable document could then be scanned by the user’s smartphone, which in turn distributes the key to the RFID interrogators during reservation.

Protecting keys during distribution and use

In order to improve the security and privacy, TPMs could be used. For example, if the RFID interrogators were to be fitted with a TPM. During reservation, the RFID tags key is encrypted with the data-binding feature of TPMs. This way, only the TPM of the RFID interrogator is able to decrypt and use the key. In addition to that, the decryption and use of the key can be bound to additional restrictions defined by the enhanced authorization features of TPMs.

Usage of TPMs in iKoPA

Incorporating a TPM into existing hardware components, which are planned to be used within the iKoPA project may not always be technically feasible or too costly. The concepts can, however, still be demonstrated with a simulated TPM. A TPM simulation software is employed in this case which allows the operation of TPM compatible software for demonstration. Future hardware revisions could then incorporate a TPM and run the same software without modifications.

4.3.5 Outlook DAB Geocast

The iKoPA architecture is derived from the CONVERGE project, while adding additional technologies and concepts, with the idea to merge them somehow and make them work together in an overall architecture.

The specific question here is, if all technologies need to be merged to one combined hub or if there could be different solutions to make them each work somehow in the other domain.

4.3.5.1 Current situation

In the following section, the relevant features and attributes of the involved technologies and protocols are listed. Those are the foundation for the discussion of different solution possibilities in the following section.

TPEG:

- Based on raw binary stream; includes own methods for synchronizing and framing.
- TPEG can be transported through any carrier featuring binary streams, both unidirectional and bidirectional, thus, the transport layer of TPEG is unidirectional and stream based.
- Due to the usage of (infinite) binary streams, TPEG requires connection-oriented communication (in contrast to packet-oriented transmission).
- TPEG receivers use a subscription-based model by tuning and receiving a specific TPEG service by polling/streaming a specific URL with a specific TPEG service.
- There may be multiple concurrent TPEG services with different content and use cases in mind, with different purpose from different originators or for different service quality levels. Those services could be present in the exactly same area on the same carrier or on overlapping or different areas and carriers.
- The TPEG specification covers all layers from the binary stream, data structures, general message management layer, up to the business logic (aka TPEG applications, expressing the semantics).
- TPEG includes a structured service concept, including originator, carrier, services as entities and IDs that are globally designated.
- Management for messages, including sequences/progress (allowing to manage updates), cancel and expiration information (allowing to clean out obsolete messages) and message IDs (allowing discrimination, management and cross-reference between messages).

- Multiple business logics for different kind of data, designed for different use cases described as “TPEG applications” (extendable with additional “applications”), e.g. TEC, EMI, PKI, TFP …
- Data types are fully modelled with a TPEG specific meta-description method, using mostly UML, which can be used to compile XML and binary formats, parsers, generators and converters.
- Data models are versioned (to express updates to the data model) and can be partially independent for each TPEG application or share some common “tool sets”.
- TPEG includes a location-referencing container in the messages (with some rare exceptions) that allows using multiple and different location referencing methods.
- TPEG location referencing is focused on logical structures used by automobiles to recognized specific logical items in maps (e.g. a specific ramp of a specific highway), but not only physical parameters (e.g. WGS84).
- TPEG is derived from TMC and traffic announcements and features many commonly known information from those domains.
- TPEG is (other than TMC) not focused on human readable text, but on machine-usable information, e.g. information for route guidance systems, to learn about the state of roads and incidents affecting the route.

Geocast:

- Mostly a paradigm and logic concept.
- Core idea: Deliver a message over various carriers and systems into a specific area.
- Payload container to transport different application specific data.
- Header including targeted geographical area.
- Technical architecture to accomplish the delivery of messages to targeted geo areas by using servers handling the necessary stuff specific for different technologies and carriers.
- Message based, not stream based.
- Message management (e.g. versions, expiration) and service structures are currently not standardized.
- For the domain of traffic is often combined with DENM but not limited to it, thus may carry different payload as well.
- Uses non-connection-orientated communication and works well together with other non-connection-orientated communication.

Internet / cellular connection:

- Data transmission can be both message based and connection-orientated.
- Messages can be sent and/or connections can be formed on an on-demand base.
- Focuses on bidirectional communication. Unlike DAB, cellular provides an uplink.
- Mostly only unicast (while broadcast is possible it is rarely implemented in cellular; technological successors (e.g. 5G) of the current LTE might be better suited for broadcast).
- No direct inherit geo-cast functionality; but cell based broadcast is possible.

DAB/DAB+:

- DAB broadcast covers a certain designated broadcast area, that is planned coordinated and built on a long-term base, using multiple (e.g. 2 to 100) broadcasting antennas (each on e.g. 100m high towers) all broadcasting on the same frequency.
- The smallest unit of DAB broadcast is a “DAB-ensemble” with an exact amount of transmission capacity sufficient for e.g. about 16 typical audio programs.
- Different DAB-ensembles may exist in different parts of the country with partly or fully overlapping broadcast areas.
- Services and transmission capacities must be requested, approved, preconfigured and maintained on a long term basis, but a once established service does not necessarily need to be active all the time and does not necessarily need to transmit data at a constant data rate.
- Services and transmission capacities must be paid by the sender (mostly on a constant level) and managed, even if not used all the time or only for varying data rates.
- Services must be accounted by a person or company.
- Ensembles and services are structured and identified by ServiceIDs and Ensemble IDs globally approved and designated (which are independent from e.g. TPEG).
- DAB features different kind of protocols that can be configured for different bitrates (but bitrates cannot be dynamic, and can be reconfigured not too often due to technical and organizational reasons).
- The basic transport layer features both “stream mode” and “packet mode”, where “stream mode” is e.g. used for audio programs.
- Protocols on top of this provide both radio specific features (e.g. Labels, Slideshows) and general-purpose protocols, e.g. TDC: Transparent Data Channel, supporting raw byte streams to be broadcasted.
- DAB has error protection and error detection on different layers, with the option to use re-transmission as an additional tool to correct transmission errors; however, DAB cannot guarantee delivery and has no ability check if data was received at all. When using re-transmission functionality this includes a variability on the reception time.
- DAB features a high-level protocol called “MOT” = “Mobile Object Transfer Protocol”, being able to transmit, manage, repeat / re-transmit version / update and cancel /expire messages carrying different kind of media payload (as data BLOBs).
- MOT works partially similar to TPEG on the transport layer, but is specified and implemented completely independent from TPEG.
- MOT covers synchronizing, framing, error protection, re-transmission, message IDs, object “names”, versions etc. and thus is a broadcast specific protocol similar to file-transfer protocols on the internet but modified to work on a unidirectional base.

4.3.5.2 Merging approaches

The general idea of merging "all somehow" together, can be done quite differently and could consist of multiple individual parts working together to be fully interoperable. However, it is not clear, how this should be done or if it can be fully accomplished.

4.3.5.2.1 GeoCast transported in TPEG

GeoCasts could be transported in TPEG as BLOBs or could use the transport or message management layer of TPEG. However, this would need some new specifications as TPEG does not include the transport of generic data. Beyond that, the TISA[15] (specification authority of TPEG and TMC) has proclaimed that it is not intending to approve specifications that "abuse" TPEG as a transport layer for different applications, by defining BLOBs. Therefore, to use TPEG as a base, the most promising approach is to model the business logic completely in terms of the TPEG description concept as TPEG specific UML, which will give it the ability to compile both the TPEG ML (XML) and TPEG binary format.

This opinion is mostly used because of compatibility questions as TPEG services signal, which data model in which version is required to use for a specific service. This however, would not be possible with unstructured BLOBs that merely could contain anything that is fully unknown to TPEG and cannot be managed or signalize. Up to now, TPEG specifications do not cover generic BLOBs but each parser and converter is able to verify if TPEG data is well formed in all its parts.

As GeoCast itself is more a concept and some headers, without a specific business logic, this would mean that any specific business logic would need their specific corresponding data model in means of TPEG. This is a heavy duty and even if this work is done, it must be maintained for any changes or updates.

However, if this were solved for some or all parts of GeoCast, this would specify and allow the best possible merge of GeoCast into TPEG.

Additionally, the GeoCasts need a message management (aka Lifetime-Management) being generated for them, when injected into the TPEG domain, as TPEG is based on managed messaged, that are not just fired and forgotten, but that are repeated on broadcast channels, can be updated, canceled and expired. The concepts of TPEG and pure simple GeoCast do differ here. At least a simple solution is required, e.g. to give GeoCasts a generic lifespan of 2 Minutes and manage them accordingly, by creating message management identifier and attributes, remembering them and sending cancel messages before they actually expire.

A better solution would be to give the GeoCast data a concept of lifetime (which only some implementation currently have), thus how long are they active and valid, and when do they actually become obsolete according to the information and event they are based

[15] https://tisa.org/

on. However, this would create another TPEG application just loosely inspired by GeoCasts.

Unfortunately, GeoCast itself is open to include not just DENM but other data models. To model this properly into TPEG while avoiding BLOBs, the set of possible payload needs to be defined and limited. Just sticking to DENM however does not make much sense, as it fulfills some needs that are mostly already addressed in the own data models of TPEG. An alternative application data model to do merely the same is not very helpful.

Despite the generic payload and ability to utilize DENM, GeoCast is a concept to address a certain area. This could be merged into existing or new TPEG application data models. Here again TPEG brings its own mechanism by using a Location Referencing Container, that can be filled with a geographic and logic description, that is attached to each TPEG message.

The most interesting question that arises here is the semantic of these locations and a potential redesign and expansion to distinguish between a geographic description of the position where a certain event happens, the geographic description where the information might be relevant and the geographic description of the area that is directly affected.

All this is no solution for just letting unmodified GeoCasts ride piggyback on TPEG. Nevertheless, the real question is in fact different. TPEG is in no means for transport only but provides an own data model and concept in itself. However, DAB is in fact a possibility to transport both GeoCast and TPEG. If TPEG itself could be of any help here by carrying BLOBs of GeoCasts is more a political question, than a technical. For GeoCast, it would be sufficient if it can be transported and distributed via DAB in any way.

4.3.5.2.2 Virtual Multi-Regional Broadcast Network

Virtual Multi-Regional Broadcast Networks are conceptual idea that would be needed for any kind of on-demand message delivery over a larger area and would cover not only GeoCasts but as well any other kind of messages to be delivered on a larger on-demand area not directly bound to the broadcast coverage areas of DAB.

For DAB, the broadcast area, thus the area where a specific single frequency network can be received, is the defining geo area for any contained service. This is an implicit and fixed “GeoCast” to one specific predefined area. TPEG services use this, as they are designed specifically for specific broadcast areas to match the contained information to the area of the transmission. The “area” of the content thus follows the area of the technical broadcast, but not the other way round.

GeoCasts on the other hand focus on the free selection and definition of on-demand customizable areas independent from the coverage of single carriers or single broadcasts.

DAB and TPEG have a similar concept, but solve this with different concepts:

- For sub-areas, meta-information (location) can be provided and the receiver filters the data for relevant (or desired) information. This is strongly used in TPEG and theoretically possible for DAB audio programs (but rarely used). This filtering is mostly done on the message-level and rarely used for the whole service.

- For super-areas, covering more than one broadcast network, multiple broadcast networks are utilized and the identical or similar service uses the same ServiceIDs or information is provided how different services shall be linked together. Such concepts exist similar but somehow different on both DAB and TPEG level.
- Combining both, information/service can be transmitted in multiple broadcast networks, forming a big overall meta-broadcast area covering the intended area, but with the ability to provide additional meta-information that allow the receiver to filter services or single messages for specific areas.

Forming larger virtual broadcast-areas is done on a service-based level, not on a message-based level. Thus, there must be suitable services on all the required DAB ensembles and broadcast networks that would allow sending messages everywhere.

There is in an important fundamental paradigm for both DAB services and TPEG services: each service with a specific ID must contain the exact same kind of “service”, thus the same content or information. A receiver that detects multiple transmissions of different broadcast networks containing the same ServiceID can assume that it does not matter which of them it uses as either should contain the exact same elements. Therefore, the receiver can make its decision based on signal strength, carrier-to-noise-ratio, etc. ServiceID shall guarantee identity and equality of the behavior and content.

In general, it is not allowed to transmit services with the same ServiceID in different carriers with different content. However, this rule is sometimes broken, which leads to much discussion, controversy, technical issues and irritation. To be formally correct, multiple broadcast networks with different coverage that each contain only those data relevant for the specific area and therefore have divergent content, shall use different ServiceIDs. While this is the correct way, it requires a feature that allows binding different services with different ServiceIDs together on a higher layer to form some kind of super-service or syndication. DAB allows this with “hardlinking” and “softlinking”, especially designed for audio services. However, this is not perfect but sufficient for radio applications.

TPEG on the other hand is missing such a concept and has only the ability to identify originator and carrier independent from each other.

A fully formal logical approach to form “super-services”, in a flexible and powerful way, is missing. It could however be solved “out-of-band” or be included as additional meta-information provided in the broadcasts described in a new kind of protocol.

If multiple services with different ServiceIDs are setup in various broadcasting networks a virtual large scale broadcasting meta-network can be archived. A logical instance must be present that has knowledge about the different coverage areas and services and is able to route the incoming data to different services in different broadcasting networks. The receiver on the other hand is able to use these different services and has knowledge about which service to use for a specific position. Potentially, data will be sent in more than one broadcast, especially if they overlap. The goal is that a data for a specific position shall occur in every broadcast network that could potentially be received at a certain position.

There is a basic layer, in each of the broadcast networks with a ServiceID that identifies the single service in one broadcast network. In addition, there is another layer with a logical meta-network and meta-service and a MetaServiceID that binds all together to form the Virtual Multi-Regional Network that could be the base for GeoCast messages. While the different lower layer broadcast networks and the logical meta-network need to be planned, approved, configured long beforehand and need to be operated 24x7, the single GeoCast messages can be transmitted whenever needed without further preparation or approval. The meta-network and the different broadcast networks form a permanent connection that is populated with message-based information, whenever there is the need to send them.

This might sound trivial, but for typical digital broadcast networks derived from radio and television domains and concepts, this is an important issue that must be implemented.

4.3.5.2.3 GeoCast transported in DAB

By avoiding TPEG when making GeoCast DAB-"conform", some specification overhead is avoided, while still GeoCast is integrated into existing broadcasting systems. In general, DAB is able to transport various kind of data with different protocols and protocol combination that are specific for DAB. TPEG itself uses some rather low-level protocol of DAB, called "TDC", that provides a binary stream. However, this stream is transported in a so-called packet mode sub-channel that allows mixing it with other streams and using dynamic bitrates, avoiding strict real-time requirements and avoiding potential padding bytes.

GeoCast could be somehow transported in a similar manner.

For any kind of transport, meta-information is required that indicate that GeoCast is contained, allowing a receiver to detect and use the GeoCast messages within a DAB-ensemble.

DAB is not prepared for the data/application type "GeoCast", as this is not yet widely known or used. It would be required to expand DAB by adding some GeoCast type to the appropriate table[16] (e.g. "user application type") in the specification. This needs to be arranged and approved through "WorldDAB"[17] who is managing the DAB specifications. This could be accomplished for a practical approach but some work would be needed.

4.3.5.2.3.1 GeoCast transported in TDC

The TDC[18] (Transparent Data Channel) has some variability and options that could be used for different purpose. Some of them are predefined for specific higher protocols or applications. Other could be freely used or defined for new purposes or new protocols.

[16] „registered tables“ for DAB at ETSI TS 101 756

[17] https://www.worlddab.org/

[18] TDC specification at ETSI TS 101 759

A featured called “MSC data groups” span across multiple packets of a packet mode sub-channel. This could be used as a base for GeoCast messages, if properly defined. These data groups form a unit that is split up for transport, by the lower layer. At the receiver, a data group is collected and merged. For higher reliability, some or all parts of the data group can be retransmitted. CRC checksum for each part are used to detect transmission errors.

By putting one GeoCast message into MSC data groups, they could be transported in DAB rather easily. Depending on the kind of repetition strategy, the GeoCasts could arrive in different order at the receiver unless a very restricted strategy is used.

This approach is the best and simplest “fire-and-forget” concept that is provided by basic functionality of DAB that is likely to be supported in various receivers.

Despite any streaming methods, the MSC data groups make it easy to find the beginning of a GeoCast message, solving a potential syncing problem that could arise if GeoCast are just concatenated into an infinite stream with padding.

4.3.5.2.3.2 GeoCast transported in MOT

A high-level protocol of DAB is MOT[19] (Multimedia Object Transfer Protocol). It works on top of simpler mechanisms like TDC, data groups and packets. The idea is similar to a file transfer protocol that replicates a certain state of “objects” (that could represent files) that have unique identifiers and carry a version, expiration time and provide an ability to be “canceled” (thus deleted). DAB is used to broadcast any updates (thus changes) and to repeat any current object to allow new receivers to catch up.

MOT was designed mainly to transport so called “Broadcast Websites” with HTML files and image files, but can be used for any other kind of payload that works in the given concept. Even TPEG could have been designed to be transported by MOT, but was intentionally specified independent from MOT to support multiple carriers, including simpler lower protocol layers. MOT has a generic concept, but is a very specific implementation, only found in DAB and DRM (Digital Radio Mondial).

To make GeoCasts work in DAB, it would be a valid approach. However, MOT requires to support message management (aka lifecycle management) by providing a unique ID for each message that is maintained through different updates and finally canceled when the message becomes no longer valid. MOT is based on the paradigm of repeated transmission of still valid messages, to give new receivers and receivers with short interrupted receptions the ability to catch up. This makes it necessary to define a period of validity for that the message is repeated in the broadcast and is recognized as valid by the receiver. If the reception is lost before the cancel information is received, the expiration time makes the receiver drop the message after a predefined time. This

[19] MOT specification at ETSI EN 301 234

management and information must be available for MOT. It could be “forged” by a DAB/MOT specific adapter.

Still there will be the need to extend the registered specification tables to offer an entry for the object type “GeoCast” in MOT and there is a virtual multi-regional broadcast network needed.

4.3.5.2.3.3 GeoCast transported with a new protocol

DAB provides different protocols on different layers that could be used to define a new protocol specific for GeoCast adaption in DAB, on top of them. The simplest layer would be a stream mode sub-channel that has a fixed bitrate, no framing but must be filled with a very precise amount of data per second, no matter what. This would allow to define a perfect and most efficient new protocol, providing an adaptation for GeoCast over DAB. However, this would mean much work and requires various software on transmission and reception side to be established, while using few pre-implemented standard solutions.

Intermediate approaches using TDC, packets mode, data groups or MOT, or any mixture of these, to add additional new protocol layers is valid as well. There is even a predefined “IP tunneling” protocol, but its usage is not recommended here as IP (even it was once popular as “generic approach”) offers low advantages when stuffed into a unidirectional broadcasting approach.

4.3.5.2.4 TPEG transported as GeoCast

TPEG itself does cover all layers from a binary stream upwards until the application layer. It does not really need any other protocol to be transported but is in general itself able to be transported in almost any carrier that provides a raw byte stream.

To make it worse, GeoCast does not offer an (infinite) raw byte stream, but relies on messages with a limited size. TPEG as it is does not support this.

However, TPEG is lacking the ability to manage the concept of GeoCasts by itself. It is based on specific services on certain carriers (bearers) that are itself identified in TPEG as carrier services, defined by carrier ServiceIDs.

GeoCast is not defining a proper transport layer or service structure that is required for TPEG to work. The concept of “GeoCast” being a transport mechanism for TPEG is not suitable. TPEG itself is defined as a “ready to be consumed” interface directly to the consumer’s device, without any intermediate dissection and repackaging. Trying this will lead to various complications and is not supported by TPEG specifications.

There might be a chance to redefine a specific flavor of TPEG and rip away some layers, to make it fit into the GeoCast concept. The lower layers of TPEG could be erased, just keeping the message management and everything upward. GeoCast would then replace the transport mechanism, while TPEG does the message management and defines the application logic. Limited message length of GeoCast could be a problem. Despite that, the approach might work pretty well, if a proper feed of TPEG messages is inserted into GeoCast, including updates, repetitions and canceling messages.

The major obstacle would be that TPEG specification just does not include the option to use such a transport mechanism. An implementation would need modification to the TPEG specification or the resulting technology would not be specification conform TPEG but just a derived variation, maybe lacking support in receivers and from providers.

4.3.5.2.5 GeoCast as routing mechanism in TPEG

TPEG yet does not support the idea of virtual multi-regional broadcast networks, meta-broadcasts or meta-services properly. However, there is some need to do so, that might be addressed in future updates of the TPEG specifications.

In fact, the ARD TPEG service in Germany is actually implemented as some kind of virtual multi-regional broadcast network, but uses the identical identifiers to do so, creating some problems in receivers that stick to the TPEG specifications.

A receiver that is located in the center of a broadcast X might have good reception from another more distant broadcast Y. As the ServiceIDs are identical, it assumes that it does not matter which service it uses, as long as it has good reception. While he tunes to broadcast Y, he will not receive any information for his position, but only for distant positions covered in Y. If it would switch to broadcast X it would receive with relevant information. However, the receiver is unable to tell which broadcast does cover which area and which he should prefer or choose. When switching between X and Y and vice versa some message updates could get lost, leaving the local message management in an inconsistent state that is only cleaned up by the failback of “expiration” after a while, which is not very nifty.

Currently, the different ARD institutions each control and edit information for their specific area. However, there is some overlap at the borders. They all merge their edited information together in a central server, which then splits them up again into different regions. In theory, this central server should do some smart management, but this is not yet fully implemented. The split up data is then returned to the different institutions that do the broadcast for their specific area. One of the main purposes of this central server, merging and splitting is, to allow broadcast areas to overlap and messages to occur identically in different DAB-ensembles with consistent message management.

In fact, the functionality of this central server is similar to what GeoCasting tries to describe. In a similar way the GeoCast concept could be used as an intermediate exchange mechanism and a middle layer for TPEG related information and data.

However, this would not be an open system, merged, combined and used by many parties, but will be integrated into a closed service concept. Each provider or consortium of providers will need its own GeoCast routing server and its own set of TPEG broadcasts and services.

It is not possible and not intended to allow many different message originators or a dynamic number of message originators to be broadcasted in a common TPEG service. Each originator spans its own namespace of MessageIDs and is logically represented as a separated service component in the TPEG service. All service components must be declared and described in the so-called “SNI” of the TPEG service. Allowing hundreds of potential contributors to be represented as different originators would blow up the SNI and will leave the receiver puzzled what all these different, yet mostly empty, service components might be.

However, there are some discussions if TPEG SNI and other TPEG aspects could be improved in the future, as the current service concept lacks some flexibility and lacks some crucial information about the quality, semantic, bond and intention of a service. Improvements here could lead to other and better options how GeoCasts could be merged with TPEG.

Important to recognize is that the idea of this chapter is restricted to TPEG messages (e.g. as TPEG ML) on the input and output of the GeoCast mechanism. The solution does not allow any other kind of data. The same mechanism could be setup for different kind of data, e.g. Datex2, which is typically used for communication and exchange between traffic centers, but a mixture of inhomogeneous data or an open interface for unknown or generic data is not applicable, as the targeted services are not able to work on a generic level. Thus, GeoCast can be used here, but GeoCast shall not be understood as a generic solution alone.

4.3.5.2.6 Geographical areas

A typical problem is that services, especially broadcasts, have their own specific coverage area or availability area. In the domain of television and radio broadcasts, this effective broadcast area is the primary and defining parameter that reflects in the area of availability for any service transported through that broadcast.

However, this concept is not always true and valid, especially if the transported information itself has certain relevance for specific locations or area. In most cases, these specified areas do not match the effectively covered areas of the broadcast. DAB broadcasts, DVB-T2 broadcasts and similar are somehow itself complicated, as they are not static and simple to map to the areas. Through seasons, daytime and weather the coverage area may change. In most parts, there will not be a 100% certain reception, but only some 90-99.99% sure reception over area and/or over time. There might be some very fine grain gaps and some small spots quite far away with good receptions on the other hand. Reception is dependent on the equipment used and the location, e.g. outside or inside. Therefore, there is a theoretical coverage area described by some assumptions and statistics and there is a real coverage area for individual equipment and situation, which cannot be fully described. That means that the broadcaster can never be sure, where a broadcast can be received and where not. Broadcast networks designed for proper reception in cities and inside of houses in the city, might be received 300 km away on a mountaintop as well. On the other hand, the same service might be unusable at small spot where reception is blocked or interrupted by electromagnetic noise.

The following different kind of areas could be distinguished:

- Theoretical calculated broadcast area, according to statistics and assumptions.
- Theoretical simplified broadcast area (as used in maps for consumers).
- Maximum expected possible broadcast area (quite huge).
- Intended broadcast area (thus this is the job to be solved by the transmitters).

For broadcasts, especially those of single frequency networks with dozens of transmitters and vast areas of hundreds of kilometers of scattered coverage, the divergence between those kinds are extremely important.

For a message or information, a location could be attached, allowing to enhance the described information or to define its geographic reference. There could be point-locations, lines, polygons, areas, and complex areas with gaps, holes and islands or logical locations that are not precisely predefined by coordinates, but reference certain roads, crossings, segments or road classes.

Independent of the syntax and shape there are different semantics possible, which should be defined when making use of locations:

- Location where the described information happens, e.g. where is the accident, where did the avalanche blast, what part of the road is flooded, which building is on fire.
- Location that is affected by the described information, e.g. area covered in smoke, road segment to be avoided as it only would lead you to a blocked road, etc.
- Location that is affecting the described information, e.g. cause of a traffic jam that is located outside or at the edge of the traffic jam itself.
- Location where the described information could somehow be relevant, e.g. routing decision hundreds of kilometers away to avoid a blocked road and vast traffic jam.
- Location that describes a route (e.g. redirection for a blocked road), thus a location that does not focus on the event itself, but works around and outside the immediate location of the event.

Not only the match of location (area, point, line …) is relevant, but the intention of the user of the information is relevant as well. Is he moving towards the other location or away from it? Is the location beyond his target or in between? Will the route be affected by something? Will route alternatives be affected by something? Will he reach the relevant location when the information is still valid or will the information be obsolete until he could be there? Etc.

The following different kind of areas could be distinguished for services and content:

- Area that is superset to all possible locations that may be contained in the service. When using the service, all locations will be inside this area. No location (whatever it describes) outside of this area is intended or should be expected when using this service.
- Area for which all relevant information (of a specific kind) will be provided for sure. This is some kind of guarantee that the critical information will be delivered, for this area, e.g. ice on the road or a reckless driver. The service can be trusted to include that information for this area.
- Area where something must be located to be mentioned in the service. Only events with a location inside this area are part of this service. E.g. an accident located outside this area will not be part of the service.
- Area for which something must be relevant to be mentioned in the service. Typically, this is the implemented reality for radio traffic announcements and the assumed coverage area of the broadcast. Only the information that might be relevant for the receivers inside the coverage is broadcasted.

- Area for updates of a once in the service included message, will be reported (even if the location has moved “outside”) – this area could be defined as “global”. E.g. a traffic jam reaching inside your relevance area but then shrinking and vanishing from it, should nevertheless still be mentioned and updated. Receivers should not be left in uncertainty as they might ask, “What happened to this jam. Is it still there?”

Those areas could be defined differently for different kind of information. Information that is more critical could have larger areas defined, while trivial information could have smaller areas. The receiver just needs to know what he could expect.

This might seem too complicate at first, but in fact, this complexity is immanently happening already, while not explicitly declared and described, leading to wrong assumptions and expectations. On the other hand this complexity it mostly relevant for the conventional design work, without the need to expose this to the consumers.

All these aspects need to be managed, declared and reported in a manner the receiver can use them to make decisions. Especially for broadcast, typical receivers are not able to tune and receive all potentially available transmissions simultaneously. Most DAB receiver chips today are only capable of receiving one or two DAB-ensembles. Even there is trend to be able to receive more than two, the potential maximum amount of more than 30 DAB-ensembles transmitted on different frequencies in parallel, will not be usable by any receiver soon. Therefore, there can always be situations where the receiver needs to make decisions which DAB-ensemble to use. A control channel or information repository including all meta information about all available services nearby, that holds properties, would allow to determine the best and worst services to be used, much faster and more reliable. The above explained areas and location concepts could be the base for such meta-information, that might be available as repository on an online server, which could be cached before or that could be published and broadcasted actively.

However, perfect knowledge about each service and its properties nearby, might not be enough, when competing recommendations occur. While the routing and navigation system e.g. requires the most suitable TPEG service, the consumer might desire to listen to a certain specific audio program. A GeoCast application might require a different DAB-ensemble that contains a specific service and the traffic announcement functionality recommends tuning to a DAB-ensemble with an audio program that provides proper traffic announcements.

The receiver itself might see different broadcasts that might contain services with identical IDs but that have different reception reliability. Without further information, he should always prefer the one with the most reliable reception. But driving in a certain direction, the weaker broadcast could be the better one, because it is transmitted in and for the area he is heading to, while the still stronger broadcast only contains services and information that cover the area he is about to leave behind.

These complicate decisions and necessary information are neither fully covered by TPEG nor GeoCast yet. Especially the intended route and the prospect of information needed in the future when reaching a distant area yet out of scope, needs more than just addressing a certain area flat. There must be additional information to make best use possible. TPEG at least has the idea that a service shall somehow be tailored according to the broadcast he is transmitted in, but does not specify in detail nor describe in what manner this is done or intended.

4.3.5.3 Résumé

There needs to be a virtual multi-regional broadcast to be established to provide the possibility of on-demand message transmission. Details must be defined, arranged, service IDs must be requested and approved and bills must be paid, even if no messages are sent.

To let generic GeoCast messages use DAB broadcast as a carrier, the best options are either to use some kind of TDC transmission or to utilize MOT, while adding message lifecycle management to the GeoCast messages. To use TPEG here is not necessary and could lead to some additional complications as TPEG is not designed to act as a standalone transport mechanism.

TPEG itself could not be merged with generic other data, as it defines all layers from byte stream up to application layer by itself. To transport TPEG with GeoCast does not really make sense and GeoCasts lacks functionality required by TPEG. However, GeoCast mechanisms could be used in a closed approach for TPEG to route and merge information for broadcast in different regions. A similar thing is already done by the ARD TPEG service. This however would not allow other generic data using GeoCast to be integrated into TPEG services.

TPEG itself on the other hand does not require any mechanics to be broadcasted on other carriers. It is based on a raw binary stream that can be a unicast. Any carrier able to provide this is usable by TPEG easily. All other things are self-contained within the TPEG transport stream, defined in the specification.

Of course there are, in the long run, other possible technical solutions, how the different technologies could be merged and combined in various ways, if enough innovative planning is spend on it. Yet this is not covered by today’s specifications but by expanding and modifying them, new derived protocols can be established. Both GeoCast and TPEG itself will be developed to provide more and better functionality on relevant aspects, which could automatically lead to a better compatibility.

4.4 Electric Mobility

Registered electric vehicles on the road have reached a significant increase during the last years with over 550 000 cars sold worldwide in 2015. Thus, the global threshold of over 1 million electric vehicles on the road has been exceeded [16]. Approximately 1.3 million electric vehicles (EVs) on the road today are the result of significant efforts in technology development and policy support during the last decade. Increase in EV numbers is also achieved through dedication of public and private investments in electric vehicle charging infrastructure, necessary to support electric transportation. Adoption of available ICT technology and initiatives in R&D and standardization have made possible the emerging of a number of electric mobility services.

Currently there is a large variety of charging hardware and standards related to exchange of information among vehicle and infrastructure side. So far, that has been one of the big challenges towards a faster adoption of the electric cars.

In the context of iKoPA project, an analysis of the existing charging infrastructure for electric vehicles and their connectivity is the main subject of the study. The provided information will support the project implementation.

4.4.1 Electric vehicles

An electric car is a vehicle that is propelled by one or more electric motors, using electrical energy stored in rechargeable batteries or another energy storage device. Currently on the market, there are two major types of electric vehicles depending on their drive:

- **Hybrid vehicles** that use a combination of internal combustion engine and electric motor in order to propel the car. Usually the electrical storage capacity is very limited and electrical drive is used only for a slight improvement of the overall fuel consumption of the car. Charging of the battery can be performed either on-board through brake energy recuperation and a generator tied to the combustion engine or it can be supplied by an external electrical supply (called Plug-in hybrid vehicles).
- **Pure electric vehicles** that rely only on battery power in order to drive the motors. Batteries are with high storage capacity and are charged mainly by external electricity supply. Most electric vehicles are equipped with brake energy recuperation system. In some cases, the car can be equipped with a small internal combustion engine used as a "range extender", driving only the electrical generator that powers the batteries.

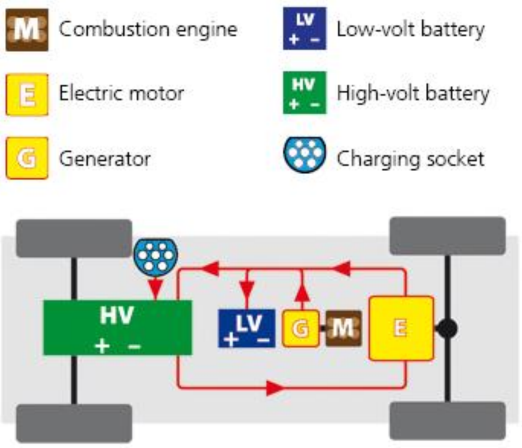


Figure 39: Common EV drive technology[20]

[20] Source: http://www.mennekes.de/index.php?id=antriebsarten&L=1

Constant improvements in battery technology in terms of capacity per volume have provided newer models of pure electric vehicles with a better range before a recharge is needed. This allows electric vehicle users to overcome range anxiety considerations and expand their journeys. Currently, there is a good variety of commercially available electric vehicles. Most of the car manufacturers have developed and introduced a number of models that are with either hybrid or pure electric drive. Since the early days of electric cars development, there has not been a common approach for how the charging of the batteries should be performed in terms of physical connection with the electrical power grid and the communication between components onboard and on infrastructure's side. That has led to an emerging of a number of proprietary electrical connectors, interfaces and communication protocols used by car manufacturers and technology vendors. So far, these shortcomings have been one of the limiting factors for the faster adoption of electric vehicles. Currently many efforts are being made in order to introduce and deploy common industry standards that will have a positive effect for the future of electric vehicles.

4.4.2 Overview of electric mobility related standards

The following diagram gives a summary of all relevant international standards that can be applied and are adopted by the electric mobility industry.

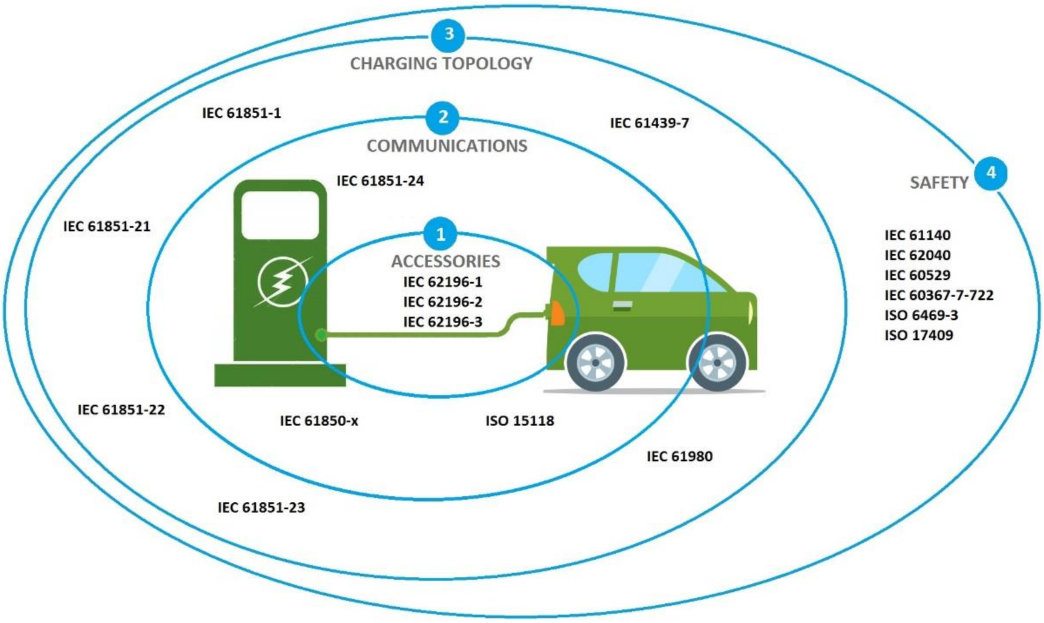


Figure 40: Overview of electric mobility related standards

The following areas of electric vehicle equipment and usage are covered by the relevant standards [17]

- **1) Accessories:** The relevant standards cover the charging process and electrical connections between the vehicle and the power supply infrastructure:
  - **IEC 62196:** Plugs, socket-outlets, vehicle connectors and vehicle inlets - Conductive charging of electric vehicles

        - Part 1: General requirements;
        - Part 2: Dimensional compatibility and interchangeability requirements for a.c. pin and contact-tube accessories;
        - Part 3: Dimensional compatibility and interchangeability requirements for d.c. and a.c./d.c. pin and contact-tube vehicle couplers;
- **2) Communications:** The relevant standards cover the signaling and data exchange between the electric vehicle and the charging infrastructure:
    - **ISO 15118-1,2,3**: Road vehicles – Vehicle to grid communication interface:
        - Part 1: General information and use case definition;
        - Part 2: Network and application protocol requirements;
        - Part 3: Physical and data link layer requirements;
    - **IEC 61850**-x: Communication networks and systems for power utility automation. Introduction and overview;
    - **IEC 61851-24**: Electric vehicle conductive charging system:
        - Part 24: Digital communication between a DC EV charging station and an electric vehicle for control of DC charging;
- **3) Charging hardware:** The relevant standards cover the specifics of the charging infrastructure hardware:
    - **IEC 61439-7:** Low-voltage switchgear and control gear assemblies:
        - Part 7: Assemblies for specific applications such as marinas, camping sites, market squares, electric vehicles charging stations;
    - **IEC 61980:** Electric vehicle wireless power transfer systems:
        - Part 1: General requirements;
    - **IEC 61851-1, 21, 22, 23**: Electric vehicle conductive charging system:
        - Part 1: General requirements;
        - Part 21: Electric vehicle requirements for conductive connection to an AC/DC supply;
        - Part 22: AC electric vehicle charging station;
        - Part 23: DC electric vehicle charging station;
- **4) Safety security:** The relevant standards cover safety aspects on the electric vehicle's side:
    - **IEC 61140:** Protection against electric shock. Common aspects for installation and equipment;
    - **IEC 62040:** Uninterruptible power systems (UPS);
    - **IEC 60364-7-722:** Low-voltage electrical installations:
        - Part 7-722: Requirements for special installations or locations - Supplies for electric vehicles;
    - **ISO 6469-3:** Electrically propelled road vehicles - Safety specifications:
        - Part 3: Protection of persons against electric shock;
    - **ISO/FDIS 17409**: Electrically propelled road vehicles - Connection to an external electric power supply – Safety requirements

4.4.3 Charging of electric vehicles

Electric vehicles typically use high-density batteries for storing energy. The following methods for external supply of electrical energy are being used:

- AC Charging:

Alternating current has been used as a standard charging method for all electric vehicles. It is available through private and public outlets connected to the electrical supply grid. Some sockets are dedicated for EV charging and are available in the form of specialized equipment (usually referred to as AC charging stations). AC is transformed into DC by an onboard rectifier that charges the batteries.

- DC Charging:
  An external rectifier (typically part of a charging station) transforms AC from the electrical supply grid and delivers it directly to the EV batteries, bypassing the onboard charger. The external DC rectifier can be significantly more powerful than the onboard, so batteries are able to charge a lot faster.
- Inductive charging:
  With this method, charge is delivered wirelessly to the vehicle through electromagnetic induction. The charging station can be integrated into the road surface, so when a vehicle is positioned above, it is charged without the need to connect wires. This is a relatively new method for the EV industry with promising uses particularly for public transport applications (electrical buses).
- Battery replacement:
  The concept for quick battery swapping has been implemented on a limited scale by some EV manufacturers. So far this" charging" method is not widely adopted due to shortcomings, related to battery ownership considerations and the mechanics of the swapping procedure.

4.4.3.1 Charging modes

Charging modes for electric vehicles and electrical connectors are specified in the international standard **IEC 62196-1:2014.** According to the standard four modes of charging an electric vehicle are specified [18]:

- **Mode 1:** Uncontrolled AC charging by the electric grid through a cable connecting a general-purpose socket outlet (Schuko, CEE) and a specific connector on the electric vehicle's side. Batteries are charged by the vehicle's onboard charger (rectifier). Usually this type of charging is not recommended due to the lack of protective or charge control devices, which might lead to socket and cable overheating and malfunction after several hours of near maximum power drain.

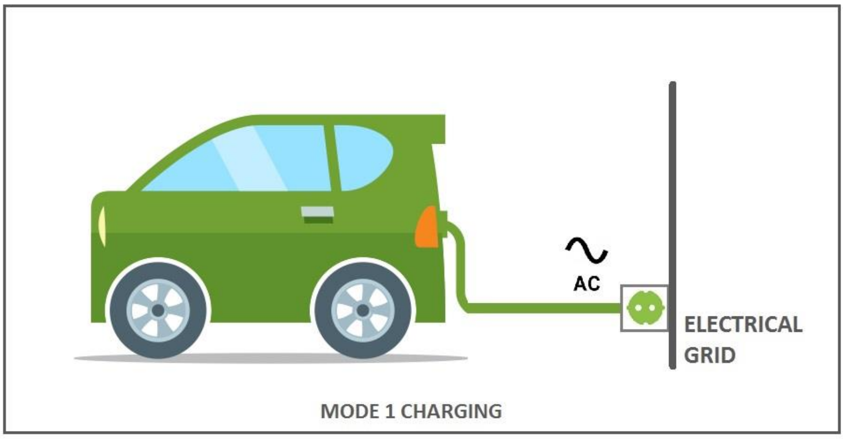


Figure 41: Mode 1 charging

- **Mode 2:** AC charging by the electric grid through a cable with integrated protection and control device connecting a general-purpose socket outlet (Schuko, CEE) and a specific plug on the EV's side. The control/protection device monitors and secures the charging process through exchange of data (PCF) with the electric vehicle through a standardized communication interface. AC supply and connection to the grid are the same as in Mode 1.

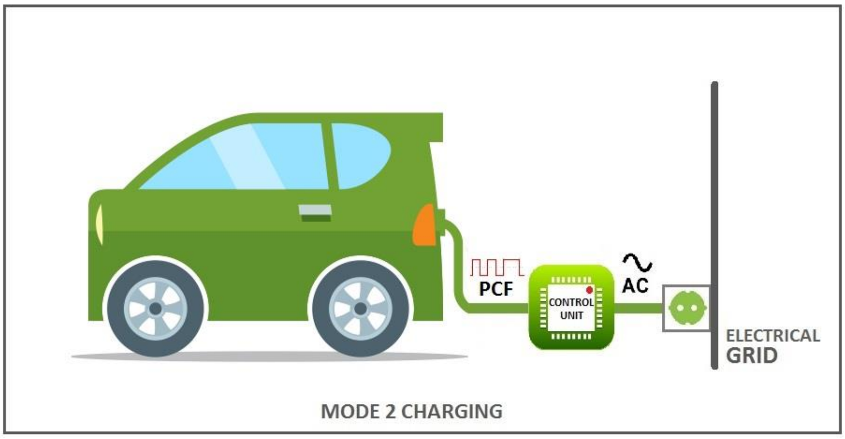


Figure 42: Mode 2 charging

- **Mode 3:** AC charging by an outlet dedicated for electric vehicles socket, containing an integrated protection and control device (typically called charge points or stations). The cable is connected on both sides through specific connectors. On some charging stations, the cable is permanently fixed as part of the installation. Mode 3 charging stations typically are engineered to supply higher charging currents and voltage of up to 63A (400V). However, the charging time is limited by the electric vehicles on board charger that still has to rectify the AC to DC current. The control/protection device is an integrated part of the charging station and secures the charging process through exchange of data (PCF) through a standardized communication interface.

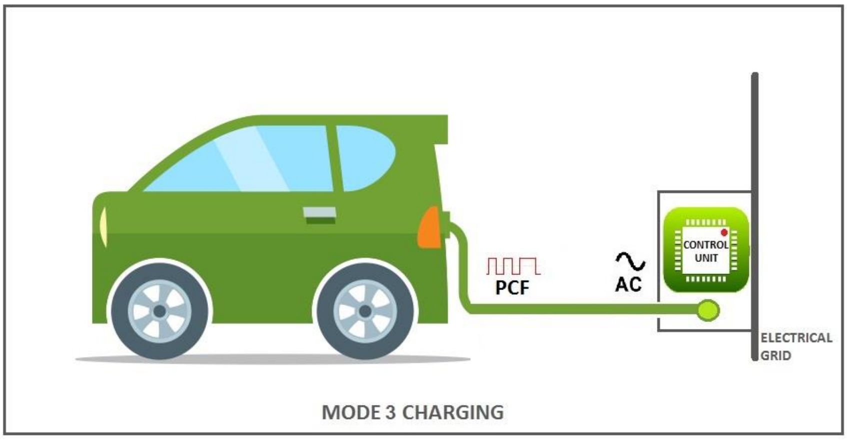


Figure 43: Mode 3 charging

- **Mode 4:** DC charging by a dedicated external charger with integrated protection and control device. The external charger supplies high DC current directly to the on board batteries, bypassing the on board rectifier. The EV is connected to the DC charger by specific connectors. The control/protection device is an integrated part of the charging station and secures the charging process through additional exchange of data (PCF and COM) through a standardized communication interface.

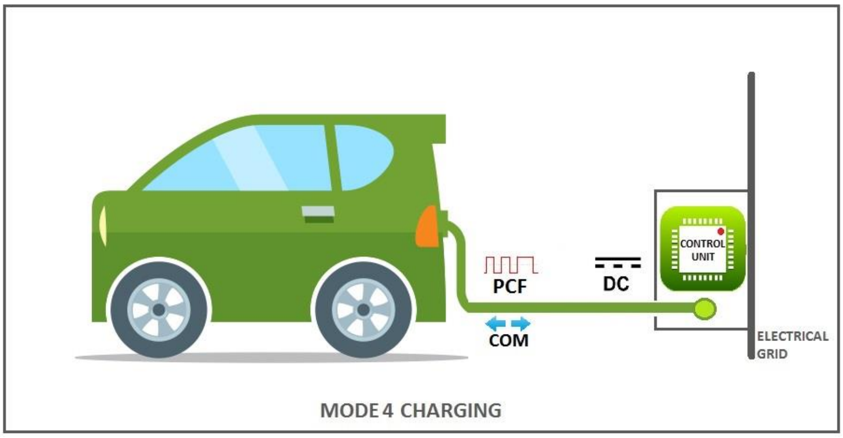


Figure 44: Mode 4 charging

Typically, Mode 1 and Mode 2 are common for home/overnight or office/workday charging from a widely available general purpose electrical sockets. Mode 3 and Mode 4 are common for purpose built charging sockets or “stations”. This type of charging is mostly intended for public use in the form of designated stations or points.

4.4.3.2 Connection to the electrical power supply grid

In Europe the most common plugs for connection to the AC power supply grid are:

- The **Schucko plug**, typically available at household sockets or public charging spots. Single-phase current can deliver charging power levels of up to 3.6kW (230V, 16A).

- The **CEE plugs:** standard plugs that are available in two variants:
  - As a single phase, "blue" socket, commonly available at camping sites. It can deliver charging power of up to 3.6kW (230V, 16A);

  - As a triple phase "red" socket for industrial applications, available in 2 variants:
    - CEE 16 delivering charging power levels of up to 11kW (400V, 16A);
    - CEE 32 delivering charging power levels of up to 22kW (400V, 32A);

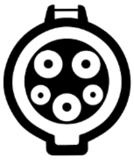
Typically, users are equipping their electric vehicles with sets of charging cables that gives them the opportunity to charge in most scenarios from the available common power supply infrastructure.

4.4.3.3 Connection to the electric vehicle for AC charging

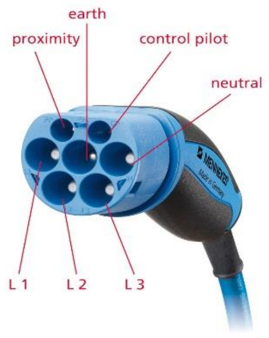
In order for electric vehicles to be charged everywhere with no problems it is necessary to have a standardized electrical connections and charging methods. During years of electric vehicles development and introduction of newer models, a number of different connectors adopted by individual manufacturers were introduced. Efforts are made in order to introduce standards that could be widely adopted, so users can benefit from the mutual compatibility of charging infrastructure and electric vehicles. At the moment there are a number of existing types of connectors that are preferred by individual EV manufacturers or are common for a particular market or geographical location.

The international standard **IEC 62196-2:2016** has specified the most widely adopted **connector types and signaling** for **AC** charging of electric vehicles. There are three main types of connectors:

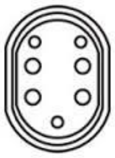
- **Type 1**: This connector was developed in Japan by a manufacturer called Yazaki (also known as the "Yazaki plug"). It is also specified as a standard connector in SAE J1772-2009 and is mostly found on charging equipment in North America and Japan. It is used for single phase AC charging with power up to 7.4kW. The connector has five pins for two AC wires, protective earth and 2 signal pins for control function. The Type 1 plug can be used for Mode 2 and 3 charging. This type of connector is not widely adopted in the European market.



- **Type 2**: This connector was developed in Germany by a connector manufacturer called Mennekes and it has been widely adopted by the European market. It supports single and triple phase AC charging giving the possibility to supply power levels from 3.6kW up to 43.5kW. Type 2 connectors are used both on vehicles and on infrastructure's side. It has seven pins: 4 electrical (3 phases and 1 neutral), protective earth and 2 pins for the control function. Since April 2014, the Type 2 connector has been approved by the EU parliament as the standard plug for AC charging of EVs in Europe.



- **Type 3:** This connector was developed by the *"EV Plug Alliance"* back in 2010. The connector is equipped with an additional shutter that protects the electrical contacts. This feature made the plug compliant with Italian electrical safety standards, so it was widely adopted for that market. Optional shutters available for Type 2 plugs and the policy to approve a single standard for Europe limited the overall adoption of the Type 3 connector. Currently the Type 3 connector could be considered as abandoned by the EV industry.



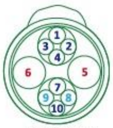
4.4.3.4 Connection to the electric vehicle for DC charging

When fast DC charging technology was introduced by individual electric vehicle manufacturers there was no common standard for the connectors. There are several designs of connectors dedicated for DC charging only that in time were widely adopted by particular markets like North America, Europe, Japan and China. At the moment three different existing systems for DC mode 4 charging are specified in the IEC 61851-23 standard. Each system has a communication protocol, specified in IEC 61851-24 and a connector configuration, specified in IEC 62196-3. The three specified systems are:

- **System A** (Annex AA of IEC 61851-23)

  This system is also known under the trade name **CHAdeMO** or **JEVS G105** (according to Japan's standard)**.** It was initially developed and introduced by Japanese industry, including Nissan, Mitsubishi, Toyota, Fuji HI and TEPCO. The connector is specified as Configuration AA of IEC 62196-3 and it is able to deliver power levels of up to 62.5kW. The communication between the external charging equipment and the on board electronics uses CAN protocol over dedicated wires/pins. Communication is specified in Annex A of IEC61851-24.

  Up to date more then 11 000 charging stations worldwide (3000+ for Europe) are equipped with CHAdeMO connectors [19]. Electric vehicles by Japanese car manufacturers are standardly equipped with CHAdeMO outlets.



Pin layout

- **System B** (Annex BB of IEC 61851-23):

  This system is also known as **GB/T** (according to Chinese standard) and it is developed and used by the Chinese electric vehicle industry. The connector is specified as Configuration BB of IEC 62196-3. The communication between the external charging equipment and the on board electronics uses CAN protocol over dedicated wires/pins. Communication is specified in Annex B of IEC61851-24. So far, this type of plug is only used in the Chinese market.

- **System C** (Annex CC of IEC 61851-23)

  This system is also known as **COMBO** and its concept is based on adding dedicated DC pins to existing connectors for AC charging, so electric vehicles can be charged through a single socket outlet. Communication between the charging infrastructure and on board electronics is based on power line communication (PLC) protocol that is also becoming the standard for future smart grid applications. The communication is specified in Annex C of IEC 61851-24. There are two types of COMBO connectors:

  - Configuration EE (IEC 62196-3): This connector is also known as the **COMBO1** and it is based on the IEC Type 1 connector with added pins for DC charging. This type of connector is currently adopted by the North American market.

  - Configuration FF (IEC 62196-3): This connector is also known as the **COMBO2** and is based on the IEC Type 2 connector with added pins for DC charging. This type of connector is proposed by the German industry in the face of CharIn [20] as a standard solution for Europe. The connector is engineered to support currents up to 125A and voltages up to 850V.

Another popular, but not standardized DC connector can be found on Tesla's supercharger stations. Its design is proprietary and the plug is only intended for charging of Tesla's electric vehicles. Having a propriety connector has been the business model of this particular manufacturer, giving Tesla's owners the exclusivity to use Tesla's own charging infrastructure. Tesla's connector and supercharging stations are able to deliver up to 120kW of DC power to the on board batteries.

4.4.4 Communication of electric vehicles with the charging infrastructure

4.4.4.1 Basic signaling during electric vehicle charging

When an electric vehicle is charged in Mode 2 and 3 basic communications is established between the vehicle and the control unit on the infrastructure's side. All connector types of IEC 62196-2 are equipped with 2 dedicated pins: the *control pilot* (CP) pin and the *proximity pilot* (PP) pin additional to the normal electrical connection pins. The proximity pilot signal is used by the electric vehicle to detect when it is plugged in. This signal is used by the electric vehicle on-board management system to inhibit movement while the charging cable is attached and to stop charging as the plug is about to be disconnected, so no arcing occurs. The PP also allows charging stations to detect when a cable is plugged in and recognize its current rating, used to determine the safe charging power rate. The charging station communicates this data to the on-board system via the control pilot pin in the form of a pulse width modulated (PWM) signal. This way the electric vehicle can set the on-board charger to match the input current. During the charging process, the on-board management system constantly communicates its state to the control unit on the charging station side. This basic communication is specified in “Annex A” of IEC 61851-1 and is commonly called “Pilot Control Function” (PCF). The functionality is safety relevant, so nearly all electric vehicles around the world support it. The communication uses PWM.

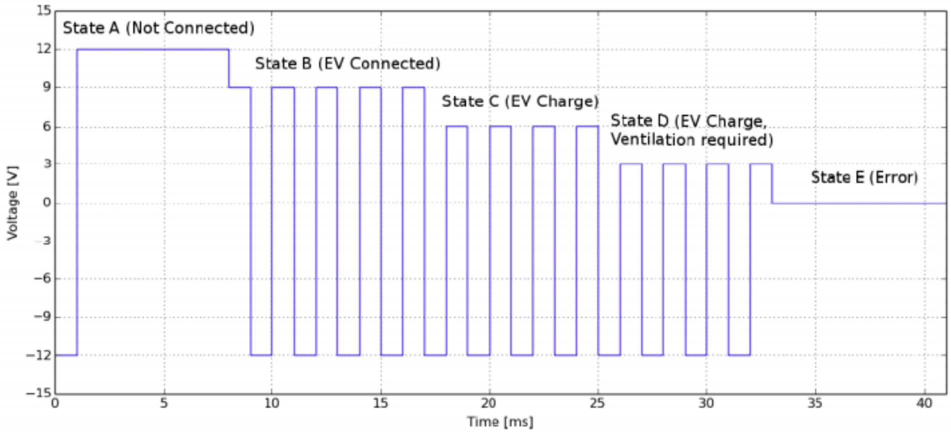


Figure 45: PWM signaling for Pilot control function [21]

The Pilot control function is also referred to as “Low level” communication between vehicle and charging infrastructure.

High power DC charging requires the synchronization and control of additional parameters and a so-called “high level” communication with the vehicle has to be established. For the different charging systems communication, interfaces are specified in IEC 61851-24. The data transfer is based on CAN bus (Controller Area Network) communication for Systems A and B and PLC (Power Line Communication) for System C connectors. The following common parameters are transmitted and synchronized between the on board management system and the charging station control unit:

- Battery parameters: Target charge voltage, battery capacity, maximum charging time, etc.;
- Charger parameters: Available output voltage/current, error thresholds, etc.;
- Initiation/termination signals;
- Charging current control parameters: calculated optimal current based on battery condition (called also State of Charge - SoC);

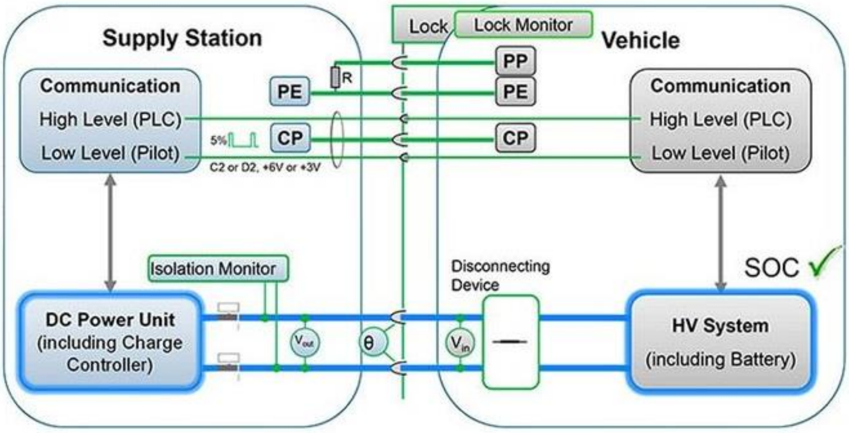


Figure 46: Typical communication architecture for mode 4 charging [8]

Currently most of the current generation of electric vehicles are equipped with standardized connectors for fast DC charging that support the specified communication interfaces. However, the amount of exchanged information is limited to managing the safety of the charging process itself. For additional services, electric vehicle users have to rely on interaction with third party applications or terminals, integrated into the charging stations. Newly developed and adopted communication protocols are able to support and extend the functionalities of the charging process.

4.4.4.2 Connecting electric vehicle to infrastructure (V2G)

In order to have efficient networks of charging stations that are able to handle large numbers of electric vehicles with the available power and electrical grid resources, it is necessary to have remote management of the charging process. This means that infrastructure, including electrical grid backend, charging equipment and electric vehicles have been able to exchange information in a uniform way. So far, there are existing standards or solutions that are widely adopted by the e-mobility industry for interfacing electric vehicles to charging stations and network operator backend systems. However, the concept of smart charging involves a number of additional stakeholders and systems, particularly on the electrical grid backend that are already interconnected through standardized communication. Including electric vehicles as the endpoint and charging stations as integration point for the information exchange requires a common communication standard to be adopted by all the parties in the link chain.

As a result of such initiative, a new standard **ISO 15118** is recently introduced. So far, it is considered to become the common interface for connecting electric vehicles to power supply infrastructure (the so-called vehicle to grid – V2G communication).

The new standard is based on Power Line Communication (PLC) specified also as the Home Plug Green PHY standard, widely adopted by the electrical industry for Smart Energy and Smart Grid application. The concept utilizes existing power line cables as the physical layer for transmitting the communication signals. The ISO 15118 incorporates also the older IEC 61851-1 standard for operational safety during mode 2 and 3 charging, assuring backward compatibility for older generation electric vehicles. According to the standard, secure data transmission is provided with TLS encryption. Communication to the electric vehicle is carried via the control pilot wire in the charging cable, coexistent with the PWM signal of IEC61851-1.

Currently the Type 2, Type 3 and COMBO connectors are compatible with ISO 15118 providing AC and DC charging. The new standard supports communication of extensive data between charging station and vehicle before, during and after charging, enabling functionalities for [9]:

- Start of charging with “high” level communication;
- Certificate installation and update;
- Identification, authentication and authorization;
- Optimized and scheduled charging;
- Level control (load management) for AC/DC charging;
- Charge metering information exchange;
- Charging with interruptions by grid side;

Such functionalities give the opportunity not only for smart charging, but for implementation of additional added value services that could increase the efficiency and the overall experience for electric vehicle users.

Currently the European Automobile Manufacturer’s Association (ACEA) and the Union of Electricity Industry in Europe (EURELECTRIC) recommend ISO 15118 as the standard for electric mobility. [22] Although ISO 15118 is a relatively new standard and there already is an older generation of installed charging infrastructure and electric vehicle stock, it might take time until its wider adoption is achieved.

4.4.5 Key actors and market models for the public charging infrastructure

Electricity is increasingly assumed as the transport fuel of the future that should contribute to achieve the internationally agreed climate goals. With advancement of battery technology and policy support electric vehicles are entering large scale deployment. That implies that a large number of private and public charging stations are to be integrated into the existing electricity networks and services to end users of electric vehicles provided.

Public charging infrastructure is intended to be freely accessible so it could provide the electric vehicle users with experience and confidence similar to the conventional petrol powered vehicles. In order to charge the battery of its vehicle from a public station a user must pay an amount of money for the consumed electrical power. Normally this process is covered by contractual relations with e-mobility Service Providers, giving the freedom to charge on any compatible station, without having to consider network operators. Individual e-mobility Service Providers might have agreements for interoperability, so users can charge outside their “home” networks that are originally covered by their contract. This process is typically called “roaming” or “e-roaming” and is in a way similar to the concept used by mobile phone networks. The e-mobility services have become common for the European market and are provided through interaction of a number of individual stakeholders (actors) from both the charging infrastructure and the electrical supply domains. The following actors have active roles for the typical e-mobility service [23]:

- **Electricity Supply Retailer**:
  Companies that hold licenses (or are active on the electricity market) to sell electricity that they produce or purchase on the electricity market to end users that have a contract with fixed location for the supply.
- **Distribution System Operator (DSO)**:

An entity that holds and manages the assets for electricity distribution networks. Responsibilities include connecting all loads to the electrical system and maintaining of safe, stable and reliable power supply network to the customers.

- **Charging station owner**:
  An entity that owns the charging station equipment. It could be a charging station operator or other private or public entity. In some case it could be a public entity that has invested in infrastructure (for instance through a sustainability program), but the actual operation is given to a 3rd party network operator;
- **Charging station operator:**
  An entity that manages the charging station infrastructure from an operational and technical point of view (i.e. access control, management, data collection, maintenance). There can be operators that provide only technical service and operators that also offer commercial services to electric vehicle users.
- **E-mobility Service Provider:**
  An entity that sells e-mobility services to end customers. Such services include seamless and payment free access to charging stations from different charging station operators. Additional services like parking, electricity supply and others might also be included in the contract.
- **E-mobility customer:**
  A client of the e-mobility Service Providers. Typically, electric vehicle owners/drivers, but could also be a legal entity (like private companies).
- **E-mobility clearinghouse:**
  A platform among charging station operators and e-mobility Service Providers. Its role is to organize and process the exchange of data, authorize individual service requests and identify the involved parties. It also distributes service data summaries, so contractual clearing and invoicing among the parties is performed.

In practice several roles can be performed by a single actor. For instance, an e-mobility Service Provider can also be a charging stations operator or a DSO could be in charge of deploying the charging infrastructure and thus act also as network operator. Another possibility is an electricity supply retailer also acting as an e-mobility Service Provider. Other combinations are also possible. Currently there are two market models that are widely adopted in Europe.

4.4.5.1 The independent e-mobility market model

This model is currently implemented in **Germany**, France, Spain and Denmark. The public charging stations are deployed independently from DSO/grid business. The implementation of a charging station, including building, owning and operation is a competitive activity that can be performed by any market representative. This means that more than one interested party can install charging stations in a city or even a street. From DSO's point of view connections to charging stations are treated as any other to the grid. The DSO can provide metering for the charging station or in liberalized metering market (like in Germany), a 3rd party provides the relevant metering data to the DSO for the calculation of fees.

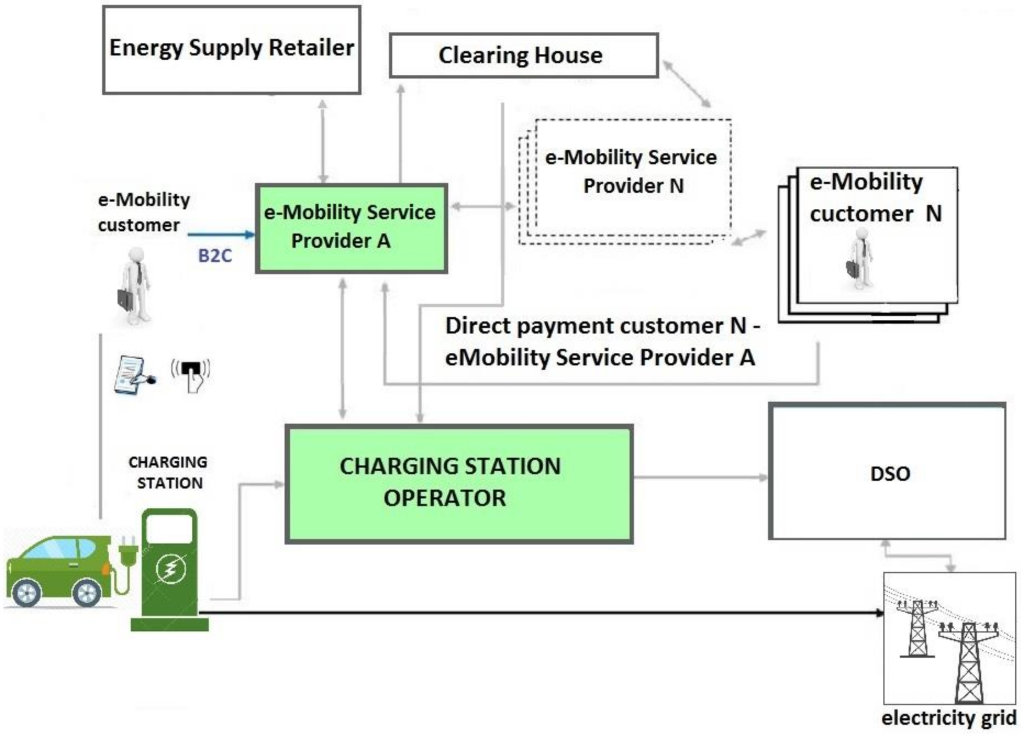

Energy Supply Retailer
Clearing House
e-Mobility Service Provider N
e-Mobility cuctomer N
e-Mobility customer
B2C
e-Mobility Service Provider A
Direct payment customer N - eMobility Service Provider A
CHARGING STATION
CHARGING STATION OPERATOR
DSO
electricity grid

Figure 47: The independent e-mobility market model [11]

Hint: Grey arrows: B2B contractual relations; Blue arrow: B2C contractual relations;
Black arrow: Physical connection;

In this market model, it is common that a single party at the same time owns the charging stations infrastructure, operates it and serves customers as an e-mobility Service Provider (green area boxes in the graphic above). The e-mobility Service Provider normally buys electricity from an energy supply retailer. It is also possible that Energy supply retailers act themselves as e-mobility Service Providers and charging station operators. The final price that an end customer is paying for charging normally includes the sum of the following fees:

energy fee + service fee + grid fee + charging infrastructure fee;

Customers of an e-mobility service can gain access to the charging infrastructure in different ways:

- As a customer that wants to use a station that is operated by an e-mobility Service Provider with whom he has a (long-term) contract on a subscription basis.
- When a customer wants to use a station operated by a different e-mobility Service Provider access can be granted via a roaming agreement. (*In the graphic above if an e-mobility Service Provider "N" has a roaming agreement with e-mobility Service Provider "A", then customer "N" could use a particular charging station operated by e-mobility provider "A"*).
  - Roaming agreements are generally private contracts between e-mobility providers that could be administered either through a clearinghouse (providing authentication services) or through a bilateral agreement, or a combination of both.

    - The clearinghouse also performs the financial clearing.
    - In some cases, depending on the relations a direct communication between charging station operator and clearinghouse might be needed (for customer authentication, etc.). Cases are defined in contractual relationships among the involved parties.
- Functionality of direct payment systems or “Pay-as-you-go” (with credit cards, cash terminals, SMS, etc.). This model is available for both types of customers – those with or without a contract with an e-mobility Service Provider.

4.4.5.2 The integrated infrastructure market model

The integrated infrastructure model [11] is currently implemented in Italy, Ireland and Luxembourg and it is characterized by a charging infrastructure market operated as part of the DSO business. That means the public charging infrastructure is part of a regulated business of operating and managing the electricity grid. Its deployment is part of the activities performed by the DSO. In some markets, it is possible that more than one DSO could exist (depending on individual country’s regulation). The budget for investments in charging infrastructure is provided through the general network fees. In this model, the DSO acts as the charging station operator that installs and manages charging stations and allows different e-mobility Service Providers to compete in providing service to the end customer.

The customer normally has a service contract with one or more e-mobility providers and is able to charge at each public station deployed by the DSO. For that reason, the DSO is also able to execute clearinghouse functionalities resolving B2B relationships among e-mobility Service Providers. In markets with more than one DSO a “higher level”, clearinghouse is necessary in order to deal with multiple integrated infrastructures managed by individual DSOs. This type of clearinghouse is also necessary for managing “international” e-mobility customers that have contacts with “foreign” Service Providers and want to use a charging station deployed by the DSO.

From the customer point of view access to services and transactions are similar to the independent e-mobility market model. The only differences arise in the final price calculations. In this market model, since the DSO is the one investing in new infrastructure, there are no individual “infrastructure fees” claimed by a charging station operator. Instead, the costs are included in the general grid fee charged to all electric grid end customers. This way the significant funds necessary for the deployment of new charging infrastructure could be efficiently gathered and allocated.

4.4.6 Connectivity for the charging infrastructure

The large number of actors that have to act in an interoperable environment defines the necessity for open communication protocols that have to interface large number of different systems. The most common and widely adopted communication protocols by the e-mobility business area are reviewed in the following chapters. The following figure provides an overview of the various actors and their communication links:

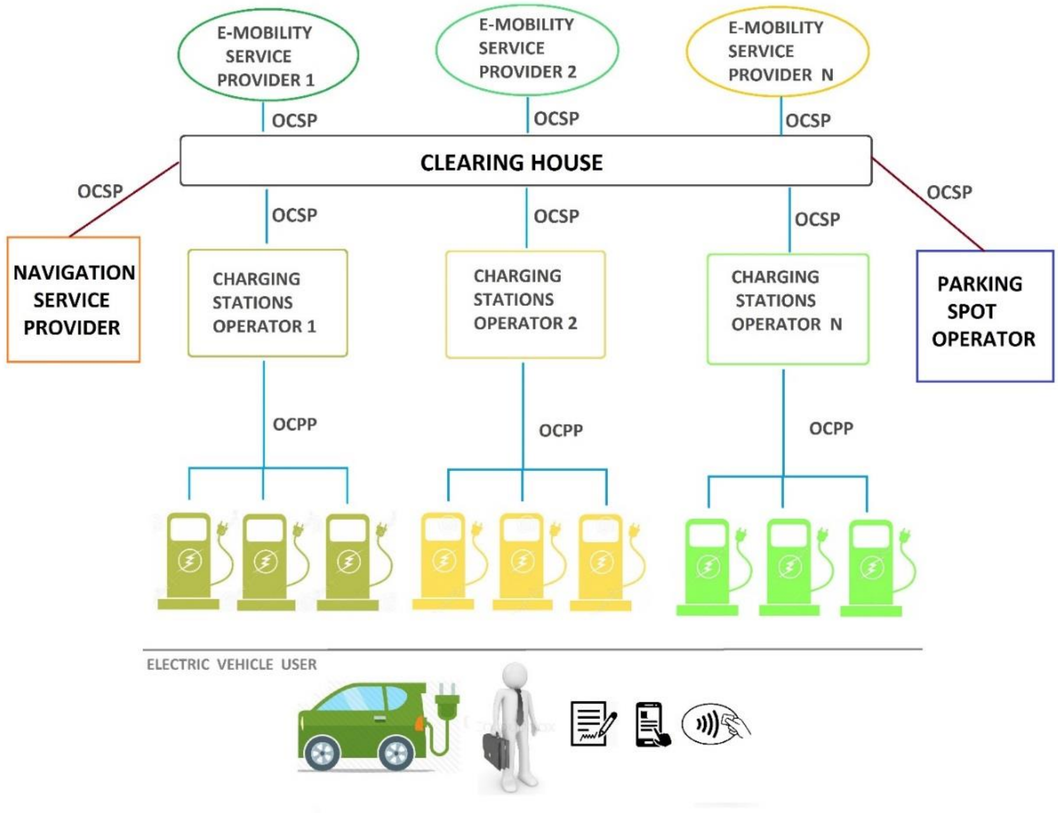

E-MOBILITY SERVICE PROVIDER 1
E-MOBILITY SERVICE PROVIDER 2
E-MOBILITY SERVICE PROVIDER N
OCSP
OCSP
OCSP
CLEARING HOUSE
OCSP
OCSP
NAVIGATION SERVICE PROVIDER
PARKING SPOT OPERATOR
OCSP
OCSP
OCSP
CHARGING STATIONS OPERATOR 1
CHARGING STATIONS OPERATOR 2
CHARGING STATIONS OPERATOR N
OCPP
OCPP
OCPP
ELECTRIC VEHICLE USER

Figure 48: Charging actors

The diagram demonstrates a model that has become popular in the e-mobility business area. With the development of newer versions of the open protocols, additional actors can be involved enhancing or providing new services and functionalities.

4.4.6.1 The Open Charge Point Protocol (OCPP)

The older generation of charging stations infrastructure has been relying mostly on proprietary interfaces in order to connect to a network management system. Such solutions have proven to be ineffective, particularly for business models that rely on interoperability of the charging infrastructure and the backend systems. With the aim for interconnection and integration of multiple charging network operators, industry members have taken initiatives for defining common open interfaces that could overcome the shortcomings of the proprietary-licensing model. Such an initiative was undertaken by the Open Charge Alliance (OCA) and has led to the development of the **Open Charge Point Protocol (OCPP).** The essence of the OCPP is to provide a uniform and open solution for the communication between charging stations and network operators, regardless of the field equipment vendor.

The OCPP protocol is based on SOAP (Simple Object Access Protocol) and JSON (Java Script Object Notation) technology. The SOAP messages are based on XML (Extensible Mark-up Language) standard, giving the benefit of legible text content. The following functionalities are embedded into the OCPP v1.5 protocol [12]:

- Starting up a charging station: A process of charging station initiation with the central system after it is switched on.
- Heartbeat: Regular signaling of availability of the charging station to the central system;
- Starting of transaction: A process of authorization with ID or charge pass (credentials are typically supplied by the user through a charging card);
- Stopping of transaction: A process of charging termination by the user (with charge pass);
- Firmware updates: A process for managing the remote updates of the charging station's firmware.
- Dealing with errors: In the event of failure at the charging station, the associated error message is transmitted to the central system;
- Diagnostics: Response of the charging station to diagnostic inquiries by the central system;
- Reservation: Since version 1.5, the functionality for remote charging station reservation is supported. The central system sends a message to the charging station containing reservation time, authorized ID card and a specific reservation ID. Reservation is refused by the charging station in case it is occupied or is out of order. Reservation could be cancelled by the central system.
- Manufacturer specific tasks: Since v.1.5 it is possible to implement manufacturer specific messages.
- Change configuration: A process for modifying of charge station's settings by the central system;
- Other options: It is also possible from a remote central system to start and stop a transaction (charge action), to unlock the connector, to restart the charge point and to modify its status.

The latest version 1.6 of OCPP supports functionalities for smart or managed charging, giving the possibility to schedule a charge action and to select a desired load level.

However, these new functionalities have to be supported by the charging station equipment.

So far, **OCPP** has been widely adopted and supported by an increasing number of charging equipment manufacturers. Currently, it is reported to have more than 20,000 installations worldwide. [24].

4.4.6.2 The Open Clearing House Protocol (OCHP)

The purpose of the OCHP protocol is to provide connectivity among the various e-mobility actors that offer services to the end user. The concept of the protocol is based on the assumption that a clearinghouse entity connects the various Service Providers in order for a user to easily charge its vehicle on every charging station regardless of the operator. By providing roaming support the complexity of relationships are significantly reduced from many-to-many bilateral partner contracts towards a one to many connections between the Clearinghouse and the Service Providers. The clearinghouse facilitates the mutual exchange of roaming authorizations, charge data and charge point information among its partners [25]. The formal act of clearing in essence is the assignment of charge detail records to the corresponding e-mobility Service Provider. The financial clearing is executed in a subsequent step which is not within the scope of the provided by OCHP interface. However, the transmitted data is used as a base to calculate payment requests. Normally the following sequence is followed:

- A Service Provider *A* uploads authorization data of its users to the clearinghouse;
- The Charging station operators that have a roaming contract with *A* download this authorization data from the clearinghouse;
- The Charging station operators enable the authorizations for use on their charging stations;
- A user of Service Provider *A* can now charge its vehicle at all charging stations of the Charging station operators defined in the previous steps;
- The Charging station operator uploads the charge data (records) to the clearinghouse;
- The charge data (record) is routed by the clearinghouse to the Service Provider *A*;
- Service provider *A* pays the roaming partner for the charging performed by its customer;
- Service provider *A* bills its customer;

The interface between the system of the clearinghouse and systems of the various partners includes the following components (data types):

- Exchange of Authorization Data (Roaming Authorizations);
- Exchange of Charge Data (Raw Billing Data);
- Exchange of Charge Point Information (Static and Live POI data);
- Exchange of Tariff information;
- Single Authorization Requests (Single Token Requests);
- Exchange of Parking lot Information (Static and live POI data);

The data flows for the interface are summarized on the diagram below:

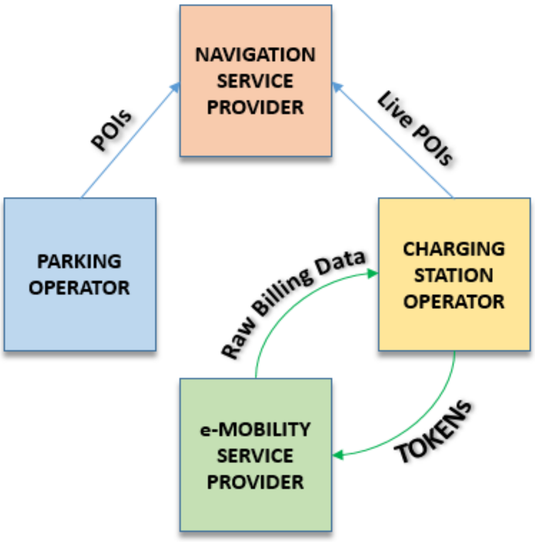

NAVIGATION SERVICE PROVIDER
POIs
Live POIs
PARKING OPERATOR
Raw Billing Data
CHARGING STATION OPERATOR
e-MOBILITY SERVICE PROVIDER
TOKENS

Figure 49: OCHP interfaces [13]

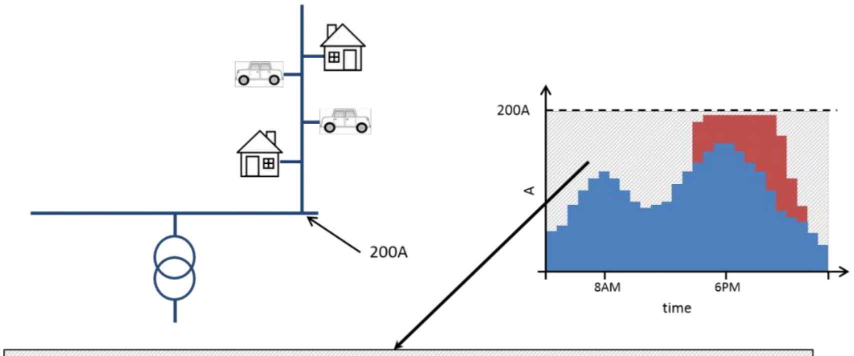
For a more detailed description of the data types and the message contents of the OCHP protocol, please refer to the official technical documentation [25].

Latest versions of OCHP also supports direct communication between roaming partners, which allows services like remote charging session control to be available to end users. Such a service can be in the form of a single mobile app (by a provider) that accesses all charging stations regardless of the operator and provides charging session control. The use cases that are supported by the *OCHPdirect* interface includes [25]:

- Remote Start: A user starts a charging process at an operator‘s charge station by using a provider‘s app. They are starting the process from a – of the operator's point of view – remote service.
- Remote Stop: A user stops a charging process at an operator‘s charge pole by using a provider‘s app (that was remotely started).
- Live Info: A user requests information about a charging process at an operator's charge station by using a provider's app (from which the process was started).
- Charge Event: A user gets informed by a provider's app about status changes of a charging process at an operator's charge station, even if it wasn't started remotely.
- Remote Control: A user controls a charging process at an operator‘s charge pole that was not remotely started by using a provider‘s app.
- Remote Action: A user triggers advanced and not charging process related actions at a charge point or charging station of an operator.

4.4.6.3 The Open Smart Charging Protocol

The OSCP protocol was adopted by the Open Charge Alliance since May 2015. Its purpose is to communicate a 24-hour prediction of the local available energy capacity to the Charge station operators. This input will allow the Service Provider to adjust its charging profiles for the electric vehicles within the limits of the available capacity. The protocol provides an interface between the charge station backend management system and energy management system on the site of the DSO (Distribution System Operator). [26]



The Open Smart Charging Protocol (OSCP) communicates a 24-hour forecast of the availably capacity of the electricity grid. Based on this forecast (blue), service providers can generate charging profiles (red) for electrical vehicles that make optimal use of available capacity without overburdening the net.

Figure 50: OSCP principle [14]

The DSO produces a forecast for the available capacity over time and transmits it to the back office management system of the local charging station network. There are two important messages within OSCP:

- Information about the available capacity for flexible loads;
- The possibility to return capacity or ask for extra;

So far, the benefits of the OSCP protocol have been demonstrated only in pilot projects and whether it will be widely adopted is too early to say. Another similar standardized communication interface is defined by ISO 15118. Since it is based on PLC communication, which is widely adopted by the electrical grid domain, it is more likely that it will be adopted also by the e-mobility industry in the future. It also provides a direct communication with the electric vehicles itself, which makes it more suitable for flexible load control (better known as the "smart grid").

4.4.7 Charging stations equipment

Publicly available charging stations are a key factor for increasing the number of electric vehicle users. According to statistics, the total number of public charging stations in 2015 reached approximately 190,000 outlets worldwide (*source: Global EV Outlook 2016 by IEA*). Of them approximately 28,000 support mode 3 and 4 charging and roughly 20% of these or around 5600 are situated throughout European countries. The growth rate for the last 5 years shows that the number of fast charging stations doubles on an annual basis, which is in line with the increase of electric vehicles on the road. The quickly increasing numbers of charging stations also implies that latest generation equipment that complies with newer standards and communication protocols can support added value services for electric vehicle users that are at the center of new business models. The following chapter gives an overview of currently existing charging infrastructure.

In general, four categories of charging infrastructure can be distinguished:

- Public charging stations on public domains (on-street);
- Public charging stations on private domains (car parks at commercial areas, shopping centers, etc.);
- Semi-public charging stations on public or private domains (car sharing services, hotels, business car parks, etc.)
- Private charging stations (home or workplace locations);

The term "public" in this case means that charging stations are open for usage by an indefinite number of users.

Private charging infrastructure is normally not associated with e-mobility services and its usage is more or less restricted and defined on an individual case-by-case basis

4.4.7.1 AC charging stations

Typically, mode 1 and 2 charging is with power levels of 3.6kW available at the general-purpose electrical sockets. It is most common for private domestic use or in some cases at designated public spots, where users can plug in their vehicles. There is number of manufacturers that supply charging cables with integrated control device and matching connectors for the vehicle. The typical installation is shown below. [27]

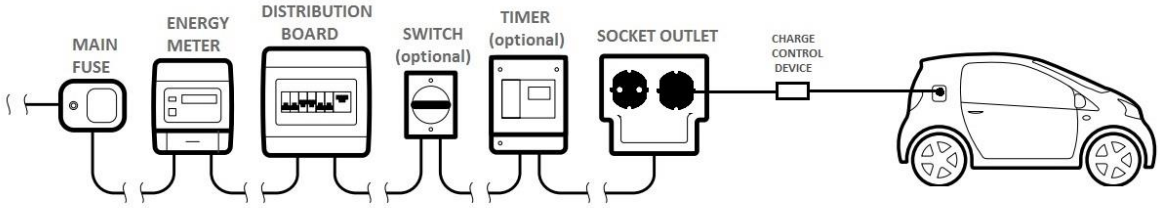


Figure 51: Typical Mode 2 charging connection [15]

Mode 3 charging stations are more common for public use and can deliver power levels of 3.6kW to 43 kW. The control device is an integrated part of the charging equipment. Mode 3 charging stations normally have compact physical dimensions, as there is no need for massive AC/DC rectifiers used for mode 4 charging. Usually they are mounted on walls (the so called “wall mount”) and some configurations are in the form of pillars or self-standing units. Normally there are two options for connecting the electric vehicle:

- With a cable that is permanently attached to the charging station on one end (usually referred to as “tethered” connection) and with standard IEC62196-2 connector for the electric vehicle’s side;
- With a standard IEC62196-2 Type 2 socket to which the user connects his own cable;

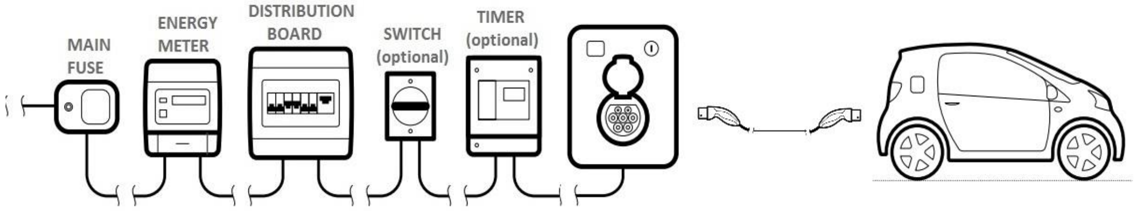


Figure 52: Typical Mode 3 charging connection [15]

Some configurations of the charging stations are equipped with energy meters, terminals and RFID readers, so users can authenticate and control the charging process.

4.4.7.2 DC charging stations

Typically, mode 4 DC stations are able to supply power levels ranging from 20 – 50kW. Some newer models can deliver up to 70-120kW and are called “superchargers” (currently only Tesla models). Due to the larger external AC/DC rectifier, this type of charging station has bigger physical dimensions, similar to that of a standard petrol station. Normally, the connection to the electric vehicle is done with a tethered cable and IEC61926-3 connector.

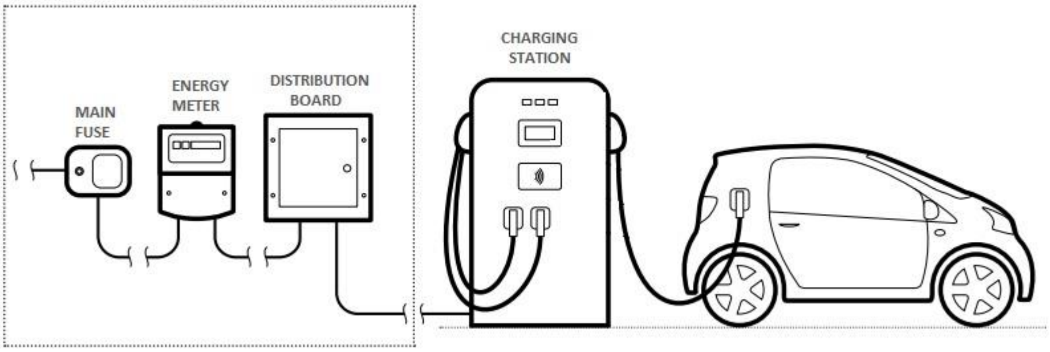


Figure 53: Typical Mode 4 charging connection [15]

4.4.7.3 Typical charging station configurations

The most common commercially available charging station configurations for the European market are summarized in the table below:

Charge point power rating	Power supply output	Typical charging time (0-100%)*	Charging mode (IEC61851)	Charge point side connector	Vehicle side connector (IEC62196)	Suitable locations
AC: 3.6 kW	230V AC, 16A, single phase	6-8 hours	2	Schuko ===== Schuko ===== Schuko =====	Type 1 Type 2 Type 3	Domestic, Workplace
AC: 3.6kW	230V AC, 16A, single phase	6-8 hours	3	Type 2 =====	Type 1	Workplace, On-street, Public car parks
AC: 7.2kW	230V AC, 32A, single phase	3-4 hours	3	Type 2 =====	Type 2	
AC: 11kW	400V AC, 16A, triple phase	2-3 hours	3	Tethered cable =====	Type 1	
AC: 22kW	400V AC, 32A, triple phase	1-2 hours	3	Tethered cable =====	Type 2	
AC: 43kW	400V AC, 63A, triple phase	20-30 minutes	3	Tethered cable =====	Type 3	
DC: 20kW - 50kW	400-500V DC, 100-125A	20-30 minutes	4	Tethered cable ===== Tethered cable =====	CHaDEMO COMBO 2	On-street, Public car parks

* estimation is for a 24kWh battery capacity

Figure 54: Charging station configurations

Normally charging stations are referred to by users as "**slow**" or "**fast**", depending on their power rating and necessary time to fully charge a battery. So far there is no clear agreement for these labels, but it is commonly assumed that if charging' duration is longer than 1-2 hours, it is "slow".

4.4.8 User interaction and authentication with public charging stations

Most of the public charging stations are part of networks that are operated as a commercial service by an e-mobility Service Provider. Users can have a contract with one or multiple providers that offer e-mobility services in a given region. In order to use a particular charging station a user has to authenticate to the Service Provider that operates that network. Most of the charging stations are commonly equipped with terminals that include a screen and input devices, including wireless card readers based on RFID technology. Normally a user that has a contract with a Service Provider has been issued an RFID card that contains credentials uniquely associated with his account. In order to initiate the charging process, the driver uses its RFID card with the integrated reader device on the charging station. The read credentials are transmitted to the backend system, where a service request is generated and verification of user's status (active plans, available credit etc.) is performed. If the transaction is cleared, a confirmation of service is set and a charge initiation action is performed. Once a charge is complete or interrupted by the user, a similar procedure is used. The driver uses the RFID card to terminate the charging process and the backend system generates a service report used to debit the user account.

So far, there is a large variety of online websites and smartphone applications dedicated for electric vehicle users. In some cases, an e-mobility Service Provider can also deliver his own smartphone applications. The common functionalities normally available in such a smartphone application may include:

- Real time availability: The user can check if a particular charging station is occupied or out of order prior to taking the trip to the spot.
- Navigation: Guidance to the charging station's location;
- Start/Stop a charge: Control the charging process through the mobile application user interface;
- Get notifications: Real time updates of the charging status that can include kilometers per charge, session cost amount, energy consumed, etc.

With the functionalities available in the newer open communication protocols for the charging infrastructure it becomes possible for smartphone apps by Service Providers to have remote reservation and flexible charge control implemented in their feature sets. As part of the iKoPA project such an application will be developed and demonstrated.

5 REQUIREMENTS

The use cases (section 3.3) and the state-of-the-art overviews (section 4) in the relevant technical areas are the base from which the requirements were derived. The requirements themselves are the foundation for the architecture as defined in chapter 6. First, general information about the requirements are given than the more than 150 requirements itself are listed and described. The requirements will later in the project from the basis for the evaluation of the pilots developed within iKoPA.

5.1 Requirement structure

Each requirement is described in detail in the following section. The description for each of the requirements consists of the following properties:

- **Code**: Bijective identification.
- **Name**: Name of the requirement.
- **Scope**: Architecture or Implementation.
- **Class**: Technical or Organizational.
- **Source**: The use cases the requirement is derived from.
- **Description**: Elaboration of the requirement.
- **Means of Verification**: Description how the fulfillment of the requirement should be verified.

The requirements are divided in three parts, which are sorted in dedicated subsections below:

- Privacy (Pxx)
- Security (SEC)
- System (SYS)

Whereby the privacy requirements are further categorized:

- PAV – Privacy Availability
- PCF – Privacy Confidentiality
- PIN – Privacy Integrity
- PIV – Privacy Intervenability
- PTR – Privacy Transparency
- PUL – Privacy Unlinkability

The structure of the privacy requirements is based on the standard data protection model – a methodology proposed by the conference of the German data protection authorities on state national level [28] and also described by [29].

The words MUST, SHALL and MAY are used as described in RFC 2119 [30].

5.2 Detailed description of each requirement

The process of preparing the requirements was made in several iterations in the interdisciplinary project team. In a first stage, a set of high level requirements was derived and later defined more precisely. During this process, identical and related requirements were merged and new requirements were derived from existing ones where necessary. Du to that fact, not all requirements numbers are assigned in the final version.

5.2.1 Privacy Requirements

The sorting and the description of the privacy requirements is based on the standard data protection model as proposed by the data protection authorities of the German federal states. The purpose of the requirements is to protect fundamental rights, particularly the right to protection of personal data as it is also set forth in the charter of fundamental rights of the European Union. All data protection goals are also reflected in the GDPR. For tables linking each of the data protection requirements to relevant norms of the GDPR (but also to the Federal German Data Protection Act and the data protection acts of the German federal states) see chapter 6.2.1 of the Standard Data Protection Model [28].

The first three protection goals are the classic protection goals of data security: Availability, Integrity and Confidentiality. The protection goals of Unlinkability, Transparency and Intervenability are the data protection specific goals. Availability as a protection goal means that personal data shall “be available and can be used properly in the intended process.” Integrity is defined as the continuous compliance of systems and processes with the specifications. The protection goal of Confidentiality protects personal data from unauthorized access. Unauthorized access can not only happen from third parties but also from service provider employees who do not need access to the personal data. Unlinkability is defined as purpose limitation. The protection goal of Transparency demands that data subjects, system operators and supervisory authorities are able to understand the collection and processing of personal data as well as the circumstances, e.g. the used systems and the data flows. Intervenability protects the data subject’s rights to notification, information, rectification, blocking and erasure. Data minimization is in the current version of the Standard Data Protection Model considered to be a fundamental protection goal that influences all other protection goals. It is the operationalization of the necessity principle. Only the data that is necessary for a certain purpose shall be processed. [29].

From these protection goals measures are derived that can be taken to protect data subjects when their personal data is processed.

REQ-PAV-001 Data portability

Req Code	Scope	Class
REQ-PAV-001	Architecture	Technical
Source		
Description		
The system shall be able to provide the data subject upon request with a copy of its personal data in a structured, machine-readable and commonly used format to comply with Art. 20 GDPR. If requested by the data subject, the personal data has to be transmitted from one data controller to another one, where technically feasible. This shall only be the case, if the data processing is based on consent or on a contract and the processing is carried out by automated means. This requirement is supposed to prevent situations where a data subject wants to change to a different service provider but decides against it, because he cannot easily take his personal data to a different service provider. In consequence it may also be suggested to deploy standardized data formats or where not existing yet, to contribute to relevant standardization efforts in the industry branch.		
Means of Verification		
The data subject can obtain a copy of his personal data in a structured, machine-readable and commonly used format.		

REQ-PAV-002 Availability

Req Code	Scope	Class
REQ-PAV-002	Architecture	Technical
Source		
Description		
The system shall ensure that personal data is available to the data subjects.		
Means of Verification		
The architecture description contains a section, which explains, how it is ensured that personal data is available to the data subjects.		

REQ-PAV-003 Backups

Req Code	Scope	Class
REQ-PAV-003	Implementation	Technical
Source		
Description		
The system shall be able to create backups of personal data to ensure their availability.		
Means of Verification		
There are interfaces that can be used to export personal data.		

REQ-PCF-001 Encryption of stored personal data

Req Code	Scope	Class
REQ-PCF-001	Implementation	Technical
Source		
Description		
The system shall encrypt stored personal data. This applies to data stored in the car as well as data stored in backend services.		
Means of Verification		
Stored personal data is encrypted.		

REQ-PCF-002 Encrypting personal data during transfer

Req Code	Scope	Class
REQ-PCF-002	Implementation	Technical
Source		
Description		
The system shall encrypt personal data during transfer. Encryption methods should be chosen to provide the necessary security against decryption by third parties, however the needs for appropriately fast communication may be kept in mind, e.g. where communication with cars or infrastructure elements require a delay-free communication.		
Means of Verification		
Personal data is encrypted during transfer.		

REQ-PCF-003 Encrypting personal data during transfer - End to end encryption

Req Code	Scope	Class
REQ-PCF-003	Implementation	Technical
Source		
Description		
The system shall provide for an end-to-end encryption during the transfer of personal data.		
Means of Verification		
It is explained or demonstrated how end-to-end encryption protects personal data during transfer. If end-to-end encryption is not possible, the reasons are explained.		

REQ-PCF-004 Information request

Req Code	Scope	Class
REQ-PCF-004	Architecture	Organizational
Source		
Description		
The data controllers and data processors in iKoPA shall check whether an information request by another entity, e.g. a public authority, is justified or has to be denied.		
Means of Verification		
Organizational processes describe how controllers and processors can check whether an information request is justified.		

REQ-PIN-001 Protection against modification - stored data

Req Code	Scope	Class
REQ-PIN-001	Implementation	Technical
Source		
Description		
The system shall protect stored personal data against unintended or unauthorized modifications. The necessary of level of the protection requirement category applicable (normal, high, or very high) may vary. E.g., the total count of the odometer constitutes a central aspect for the remaining value and thus must be stored tamperproof. This is not necessary for all data and thus needs to be decided based on the data values at hand.		
Means of Verification		
Demonstrate or explain how stored personal data is protected against unintended or unauthorized modifications.		

REQ-PIN-002 Protection against modification - transfer of data

Req Code	Scope	Class
REQ-PIN-002	Implementation	Technical
Source		
Description		
The system shall protect personal data against unintended or unauthorized modifications during transfer.		
Means of Verification		
Demonstrate or explain how personal data is protected against unintended or unauthorized modifications during transfer.		

REQ-PIN-003 Detection of modification

Req Code	Scope	Class
REQ-PIN-003	Architecture	Technical
Source		
Description		
Where unintended or unauthorized modifications of personal data cannot be prevented, the system shall be able to detect these modifications.		
Means of Verification		
Demonstrate or explain how unauthorized or unintended modifications of personal data can be detected.		

REQ-PIV-001 Deletion of personal data

Req Code	Scope	Class
REQ-PIV-001	Implementation	abstract
Source		
Description		
Personal data shall be deleted after purpose the data was collected for has been reached unless legal obligations demand the storage of the personal data.		
Means of Verification		
There is no personal data in the system that no longer serves a purpose or is required by law.		

REQ-PIV-002 Choosing between online and offline routing

Req Code	Scope	Class
REQ-PIV-002	Architecture	Technical
Source		
UC-02.02		
Description		
For navigation the data subject shall be able to choose an option where the current location and route are not transferred to a routing server, e.g. with offline navigation or only downloading map tiles.		
Means of Verification		
There is a method to switch between local routing and online routing.		

REQ-PIV-003 Control transmission of personal data

Req Code	Scope	Class
REQ-PIV-003	Implementation	Technical
Source		
Description		
The system shall allow the data subject to switch off the transmission of personal data and the collection of personal data inside his car.		
Means of Verification		
A User can switch off transmission of personal data and the collection of personal data in his car. If this is not possible due to security or safety reasons, these reasons are explained.		

REQ-PIV-004 Configure data processing

Req Code	Scope	Class
REQ-PIV-004	Implementation	Technical
Source		
Description		
The system shall allow the data subject to configure which personal data he wants to be processed.		
Means of Verification		
A User can configure the system in a way that allows him to choose what personal data is processed.		

REQ-PIV-005 Correction of personal data

Req Code	Scope	Class
REQ-PIV-005	Implementation	Technical
Source		
Description		
The system shall provide a process to correct personal data.		
Means of Verification		
Incorrect personal data that is stored in the system can be corrected.		

REQ-PIV-006 Block personal data from processing

Req Code	Scope	Class
REQ-PIV-006	Implementation	Technical
Source		
Description		
Systems shall block personal data from further processing if it cannot be deleted for legal reasons. The data may only be further processed for the purpose that demands the retention of the data.		
Means of Verification		
It is described or demonstrated how personal data can be blocked from further processing.		

REQ-PIV-007 Consent revocation

Req Code	Scope	Class
REQ-PIV-007	Implementation	Technical
Source		
Description		
Where the data processing is based on consent as legal ground, the system shall have appropriate means to react to a revocation of the consent.		
Means of Verification		
It is described or demonstrated how the data subject can revoke his consent and how a revocation is handled by the system.		

REQ-PIV-008 Data processing after consent revocation

Req Code	Scope	Class
REQ-PIV-008	Implementation	Technical
Source		
Description		
After consent has been revoked, the system shall terminate the processing of personal data if that data processing was based on the revoked consent.		
Means of Verification		
It is described or demonstrated how the processing of personal data can be stopped after a consent revocation.		

REQ-PIV-009 Configure data processing - presets

Req Code	Scope	Class
REQ-PIV-009	Implementation	Technical
Source		
Description		
The system shall support the User when he configures his privacy settings by providing him with predefined settings for different privacy preferences. The default setting should be set to privacy-preserving options (privacy by default).		
Means of Verification		
It is described or demonstrated how the User can switch between different predefined privacy settings. This can be achieved by a User accessible menu that offers privacy settings and the menu offers a range of predefined privacy settings.		

REQ-PIV-010 Deletion of personal data - User request

Req Code	Scope	Class
REQ-PIV-010	Implementation	Technical
Source		
Description		
The system shall provide a process to delete personal data upon a request by a User.		
Means of Verification		
It shall be described or demonstrated how the system can react to a deletion request by a User.		

REQ-PIV-011 Deletion of personal data - Data stored in the car

Req Code	Scope	Class
REQ-PIV-011	Implementation	Technical
Source		
Description		
The system shall allow the data subject to delete personal data stored in his car. This shall not include the mileage and other data determining the market value of a car.		
Means of Verification		
It is explained how a data subject can delete personal data that is stored in his car.		

REQ-PIV-012 Deletion of personal data - Backups

Req Code	Scope	Class
REQ-PIV-012	Implementation	Technical
Source		
Description		
If personal data is deleted, it shall be ensured that it is also deleted on backups.		
Means of Verification		
A mechanism is in place and working that ensures that personal data is deleted from backups too.		

REQ-PTR-001 Documentation

Req Code	Scope	Class
REQ-PTR-001	Architecture	abstract
Source		
Description		
The system and especially the flow and storage of personal data shall be explained and the documentation shall be available to data subjects. Where third parties have to get or process the personal data this circumstance is made transparent to the data subject.		
Means of Verification		
Expert review: An expert on data protection reviews the documentation.		

REQ-PTR-002 Privacy Impact Assessment

Req Code	Scope	Class
REQ-PTR-002	Architecture	abstract
Source		
Description		
A data protection impact assessment shall be created and published. The impact assessment shall analyze risks concerning the data subjects’ rights and the countermeasures that were taken.		
Means of Verification		
As for the pilot developed in the iKoPA project a data protection impact assessment will be part of the final data protection deliverable by the end of the project.		

REQ-PTR-003 Display data processing to the User

Req Code	Scope	Class
REQ-PTR-003	Implementation	Technical
Source		
Description		
The system shall be able to inform the data subject about the following: - the kind of personal data being processed - the purpose or purposes the data is processed for - the recipients of personal data		
Means of Verification		
The app or another part of the system has a method to display to the User what kind of personal data is being processed for what purposes.		

REQ-PTR-004 Determine Purpose

Req Code	Scope	Class
REQ-PTR-004	Implementation	Organizational
Source		
Description		
Before personal data is processed, the purpose for the processing shall be documented.		
Means of Verification		
A document is available where the purposes of the processing of personal data are defined.		

REQ-PTR-005 Definition of legitimate purposes

Req Code	Scope	Class
REQ-PTR-005	Architecture	Organizational
Source		
Description		
It shall be documented, what the legitimate purposes are, that personal data can be processed for. According to Art. 5 (1) (b) GDPR states that personal data shall only be collected for legitimate purposes. It follows from this wording, that not all purposes are legitimate.		
Means of Verification		
There is a document with a definition of legitimate purposes.		

REQ-PTR-006 Determination of data controller

Req Code	Scope	Class
REQ-PTR-006	Architecture	Organizational
Source		
Description		
It shall be clearly defined who the data controller is or would be which determines who is responsible for the legality of the data processing.		
Means of Verification		
It is described which entity would be a data controller under which circumstances.		

REQ-PTR-007 Documentation - Highlights

Req Code	Scope	Class
REQ-PTR-007	Implementation	Organizational
Source		
Description		
The documentation shall contain the following information in comprehendible language: ● which personal data is processed for which purpose ● data flows on the level of machines as well as on the level of entities ● access possibilities ● risks of undesired access ● countermeasures taken with regards to these risks ● defined procedures for creating, changing and deleting data ● defined procedures for User requests or requests from other parties		
Means of Verification		
There exists documentation that includes the topics mentioned in the description.		

REQ-PTR-008 Provide information on involved parties

Req Code	Scope	Class
REQ-PTR-008	Implementation	Technical
Source		
Description		
The system shall provide the User with information on which parties are involved in communication e.g. as data processors.		
Means of Verification		
It is explained or demonstrated how data subjects are informed about the parties involved in a communication.		

REQ-PTR-009 Information request by data subject

Req Code	Scope	Class
REQ-PTR-009	Implementation	Technical
Source		
Description		
A data subject asking for information about his personal data shall be provided with the requested information in due time. The process shall take no longer than one month to comply with Art. 12 of the General Data Protection Regulation.		
Means of Verification		
It is explained or demonstrated how a data subject can get information about his personal data. This could be achieved through the app, where the User can be informed about the way he can contact the controller or by directly contacting the controller through the app.		

REQ-PTR-010 Information request by data subject - authentication

Req Code	Scope	Class
REQ-PTR-010	Implementation	Technical
Source		
Description		
If a data subject asks for information about his personal data, he shall be authenticated to prevent that someone can request the information that belongs to a different data subject. The means of authentication must not hinder data subjects from enacting their right of access.		
Means of Verification		
It is explained or demonstrated how a data subject has to authenticate himself when requesting his personal data.		

REQ-PTR-011 Information request by data subject - pseudonyms

Req Code	Scope	Class
REQ-PTR-011	Implementation	Technical
Source		
Description		
The data subject shall be able to request pseudonymous personal data. To achieve that he shall be able to authenticate under the used pseudonym.		
Means of Verification		
It is explained or demonstrated how a User can request pseudonymous personal data.		

REQ-PTR-012 Information in case of data breach

Req Code	Scope	Class
REQ-PTR-012	Architecture	Technical
Source		
Description		
The system shall be able to provide the data subjects with information in case of a data breach if the breach is likely to result in a high risk for the rights and freedoms of the data subject. The data subject shall be informed about the nature of the breach, the categories and approximate number of personal data as well as the approximate number of data subjects concerned. The information shall also describe the likely consequences of the breach for the data subject and the measures that were taken.		
Means of Verification		
A process and responsibilities are defined, describing how Users can be provided with the information detailed in the requirement. This can be achieved by using an existing interface or a data-protection interface.		

REQ-PUL-001 Avoiding central entities

Req Code	Scope	Class
REQ-PUL-001	Architecture	abstract
Source		
Description		
The system shall not have central entities that bear the risk that personal data is linked unless necessary for provision of a requested service.		
Means of Verification		
An architecture review shows that no central entities in the architecture that can link personal data.		

REQ-PUL-002 Data minimization

Req Code	Scope	Class
REQ-PUL-002	Architecture	abstract
Source		
Description		
The system shall process only the personal data that is necessary for a certain legitimate purpose.		
Means of Verification		
Expert review: A data protection expert reviews the processing of personal data.		

REQ-PUL-003 Anonymization

Req Code	Scope	Class
REQ-PUL-003	Architecture	abstract
Source		
Description		
Personal data shall be anonymized as early as possible. If the data subject has to be identifiable for specific previously defined purposes the data may stay personal. If used for other purposes the data must be copied and anonymized for all other purposes.		
Means of Verification		
If the data subject does not need to be identifiable, the data is processed in a way that the data subject is no longer identifiable.		

REQ-PUL-004 Pseudonymization

Req Code	Scope	Class
REQ-PUL-004	Architecture	abstract
Source		
Description		
If anonymization is not possible, personal data shall be pseudonymized. This means that personal data is processed in such a way that it can no longer be linked to a data subjected without additional information.		
Means of Verification		
For an assessor it is clearly visible where in the architecture personal data is processed. An assessor can see that the architecture provides means or even triggers Users to avoid usage of personal data or at least uses pseudonyms when processes cannot work without personal data.		

REQ-PUL-005 Purpose limitation

Req Code	Scope	Class
REQ-PUL-005	Architecture	abstract
Source		
Description		
Personal data shall not be processed for purposes that are incompatible with the purposes the data was collected for.		
Means of Verification		
Expert review: A data protection expert reviews the data processing concerning the principle of purpose limitation.		

REQ-PUL-006 Multiple accounts

Req Code	Scope	Class
REQ-PUL-006	Implementation	Technical
Source		
Description		
The system shall allow data subjects to create multiple accounts.		
Means of Verification		
There is a possibility for a single User to create multiple accounts.		

REQ-PUL-007 Acquiring personal data for testing purposes

Req Code	Scope	Class
REQ-PUL-007	Implementation	abstract
Source		
Description		
During the development, it might be necessary to gather personal data for testing purposes that would be unnecessary in a deployment scenario. Where this happens, it needs to be documented so these parts of the system/software can be removed before a deployment of the system.		
Means of Verification		
It is documented, where the system gathers personal data for testing purposes.		

REQ-PUL-008 Privacy by Default

Req Code	Scope	Class
REQ-PUL-008	Implementation	Technical
Source		
Description		
The default settings of the system shall be preconfigured in the most privacy-friendly way. This means that it should be preconfigured to process none or as few personal data as possible. Opt-in shall be preferred over opt-out.		
Means of Verification		
Expert review: A data protection expert reviews the pre-configuration.		

REQ-PUL-009 Unlinkability of multiple reservations

Req Code	Scope	Class
REQ-PUL-009	Architecture	Abstract
Source		
Description		
The backend systems shall be unable to link together multiple reservation events.		
Means of Verification		
It is not possible to determine if two reservations come from the same data subject or not.		

REQ-PUL-010 Unlinkability of car park entrances

Req Code	Scope	Class
REQ-PUL-010	Architecture	Technical
Source		
Description		
The backend systems shall be unable to link together multiple car park entrances by the same data subject.		
Means of Verification		
It is not possible to link together multiple car park entrances.		

REQ-PUL-011 Unlinkability of multiple charging sessions

Req Code	Scope	Class
REQ-PUL-011	Architecture	Technical
Source		
Description		
The backend systems shall be unable to link together multiple charging events by the same data subject unless necessary for billing purposes.		
Means of Verification		
It is explained or demonstrated how the data subject is protected against the linkage of his charging sessions.		

REQ-PUL-012 Access restriction to personal data

Req Code	Scope	Class
REQ-PUL-012	Implementation	Organizational
Source		
Description		
Access to personal data shall be restricted to the extent necessary for a specific purpose.		
Means of Verification		
Personal data that is stored in the car or in the backend is protected against unauthorized access.		

REQ-PUL-013 Privacy by Default - Advertisement

Req Code	Scope	Class
REQ-PUL-013	Implementation	Technical
Source		
Description		
The system shall allow services that are not part of the basic functionality only to be available after an opt-in. Examples for such services could include personalized advertisements or market research services.		
Means of Verification		
It is described, how data subjects are protected from advertisement and market research if they do not opt-in to these services.		

REQ-PUL-014 ABCs - Issuer

Req Code	Scope	Class
REQ-PUL-014	Architecture	Organizational
Source		
Description		
The architecture shall provide an entity that can issue credentials to Users.		
Means of Verification		
The architecture describes an entity that can issue credentials to Users.		

REQ-PUL-015 ABCs - Revocation Authority

Req Code	Scope	Class
REQ-PUL-015	Architecture	Organizational
Source		
Description		
The architecture shall provide an entity that can revoke issued credentials.		
Means of Verification		
The architecture describes an entity that can revoke issued credentials.		

REQ-PUL-016 ABCs - Inspector

Req Code	Scope	Class
REQ-PUL-016	Architecture	Organizational
Source		
Description		
The architecture may provide an entity that can de-anonymize presentation tokens under specific pre-defined circumstances.		
Means of Verification		
The architecture describes an entity that can de-anonymize presentation tokens under specific circumstances.		

REQ-PUL-017 ABCs - Verifier

Req Code	Scope	Class
REQ-PUL-017	Architecture	Organizational
Source		
Description		
The architecture shall define which entities need to be able to authenticate a User through ABCs. This may be a requirement that entities of the governance level of the architecture impose on Service Providers.		
Means of Verification		
It is described which entities shall be able to authenticate a User through ABCs		

REQ-PUL-018 Privacy friendly payment

Req Code	Scope	Class
REQ-PUL-018	Implementation	Organizational
Source		
Description		
The system shall allow Users to use privacy friendly payment methods, where no detailed billing is necessary. E.g.: flat rates or prepaid.		
Means of Verification		
It is described how the system allows data subjects to use privacy friendly payment methods.		

REQ-PUL-019 Limitation of read and write permissions

Req Code	Scope	Class
REQ-PUL-019	Implementation	Technical
Source		
Description		
Read and write permissions concerning personal data shall be limited to the extent necessary.		
Means of Verification		
It is described how read and write permissions are limited.		

REQ-PUL-020 Knowledge of service directory about subscribed services

Req Code	Scope	Class
REQ-PUL-020	Architecture	Technical
Source		
Description		
The service directory shall not know which services a User is subscribed to as this may reveal a lot of information about a data subjects interests.		
Means of Verification		
It is explained how it is ensured, that the service directory does not gain knowledge about the services that a certain User is subscribed to.		

REQ-PUL-021 ABCs - Inspector - Definition of cases in which the pseudonymization can be lifted

Req Code	Scope	Class
REQ-PUL-021	Architecture	Organizational
Source		
Description		
It shall be defined, in which cases it is necessary to reveal the identity of a User. This could be necessary for criminal investigations or civil lawsuits.		
Means of Verification		
It is explained under which circumstances an inspector can reveal the identity of a User.		

REQ-PUL-022 Interfaces

Req Code	Scope	Class
REQ-PUL-022	Architecture	Technical
Source		
Description		
The system shall only have necessary interfaces for exchange of personal data. For each interface in the system there needs to be a certain purpose as unnecessary interfaces increase the danger of unwanted access to personal data.		
Means of Verification		
It is documented what purpose each interface serves.		

5.2.2 Security Requirements

REQ-SEC-001 A connection security mechanism is used

Req Code	Scope	Class
REQ-SEC-001	Implementation	Technical
Source		
Description		
All active external communication channels (e.g. between services and Users) use a form of connection security, providing authenticity and privacy (where applicable). Authenticity is ensured via a Public Key Infrastructure where applicable.		
Means of Verification		
Identify connections and check if a connection security mechanism is used. For connections over IP-based infrastructure (i.e. internet, networks) may use TLS 1.2. V2X based communication may use V2X security mechanisms (e.g. ETSI TS 103 097). Check if a PKI is in place and properly configured at the end-points.		

REQ-SEC-002 No safety relevant decisions based on unverified data are performed autonomously

Req Code	Scope	Class
REQ-SEC-002	Implementation	abstract
Source		
Description		
Decisions with implications to safety must not be performed, if the origin of the data, which the decisions are based on, cannot be verified. Safety relevant decisions are, for example, the speed or steering of an autonomous vehicle. The data origin can be verified with either cryptographically strong signature schemes, or physical protections (e.g. an internal physically protected network or storage). If an encrypted connection is used, the delay for the crypto operation has to be under a certain limit.		
Means of Verification		
Identify safety critical actions, which are performed autonomously by the systems components (i.e. actions that may lead to loss of property or life), and answer the following question: Are these actions triggered by verifiable data and is the data actually verified?		

5.2.3 System Requirements

Below is a table with categories which should help to get an overview over the system requirements. One can use the categories to identify relevant requirements for a certain task. Every category is further divided into different stations with corresponding requirements. The stations are:

APP: Requirements for the application the User can use to interact with the system

RS-V: Requirements for the remote station vehicle system

RS-I: Requirements for the remote station infrastructure systems (i.e. charging station)

BACKEND: Requirements for back-end functionality

SYSTEM: Requirements for the overall system

Category	Station	REQ-SYS-Numbers
Hardware	RS-I	128, 129
Configuration	APP	086
	RS-V	005, 086
Infrastructure	RS-V	011
	RS-I	011, 012, 020
	SYSTEM	113, 114, 123, 124, 126
Communication	APP	046, 078, 100
	RS-V	010, 019, **032**, 047, 078, 095, 100, 101, 103, 111, 112, 125, 134
	RS-I	100, 111, 112, 125, 134
	BACKEND	022, 027, 028, 029, 046, 047, 095, 100
	SYSTEM	117, 118, 119, 120, 126, 136
User interaction	APP	001, 080, 086
	RS-V	001, 080, 086
Organization	SYSTEM	007, 109
Basic information	APP	079
	RS-V	000, 002, 006, 030, 079
	SYSTEM	087
Connectivity	RS-V	003, 004, 010, 011, 019, 111, 112
	RS-I	011
	SYSTEM	114, 136
Verification	RS-I	021
	BACKEND	022
Location	RS-V	023, 024
Basic functionality	APP	036, 037, 133, 143

	RS-V	025, 026, 031, 036, 093, 097, 098, 099, 133, 135
	RS-I	093
	BACKEND	034, 035, 130, 131, 132, 141
	SYSTEM	088, 115, 122, 123, 124, 127, 140
Service	BACKEND	141
Implementation	BACKEND	033, 081, 082, 083, 084, 085, 138
Security	APP	048, 102
	RS-V	045, 048, 092, 105
	SYSTEM	043, 044, 089, 091, 094, 121, 137, 139
Specification	RS-V	095, 096, 114, 116
	BACKEND	095
	SYSTEM	110, 113, 126, 138

REQ-SYS-000 Internet connectivity available

Req Code	Scope	Class
REQ-SYS-000	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard systems in the vehicle offer information about the availability of internet connectivity. This shall include information if such a connection is available at all, an indication of the quality of the connection. E.g. if it is a connection via WLAN, or cellular network, which protocol is used (GSM, UMTS, LTE), if the signal to noise ratio is bad and which connection speed can be established.		
Means of Verification		
The architecture describes an interface that allows vehicle components to obtain network connectivity information.		

REQ-SYS-001 Navigation system exists in vehicle

Req Code	Scope	Class
REQ-SYS-001	Implementation	Technical
Source		
UC-02.1		
Description		
The iKoPA system shall provide access for the Driver to a navigation system while sitting inside the vehicle.		
Means of Verification		
A Driver sits in the vehicle and can input a route and follow the routing.		

REQ-SYS-002 TPEG-Service internet address must be known

Req Code	Scope	Class
REQ-SYS-002	Architecture	Technical
Source		
UC-01.3.2		
Description		
The system needs to know where (internet address) to access a TPEG service, that delivers the needed information, prior to connecting to it. This shall be independent from any DAB reception (that might exist, but might as well not be available).		
Means of Verification		
The architecture includes a local method for the vehicle systems to acquire the needed internet address.		

REQ-SYS-003 HTTP connection can be used

Req Code	Scope	Class
REQ-SYS-003	Architecture	Technical
Source		
UC-01.3.2		
Description		
The system needs a method to initiate a HTTP connection to access a TPEG service internet address. The HTTP connection method shall deliver the HTTP headers and HTTP content of the response. The HTTP connection method shall be able to work in a streaming mode, where data is already returned locally, while the HTTP connection prevails.		
Means of Verification		
The architecture includes a local method for the vehicle systems that accepts an internet address (URL) and delivers HTTP content and HTTP headers. The results are locally already returned, while the HTTP connection is still active and potentially receives more data. (So called "stream processing").		

REQ-SYS-004 TPEG-Service accessible via internet HTTP

Req Code	Scope	Class
REQ-SYS-004	Architecture	Technical
Source		
UC-01.3.2		
Description		
The system needs a TPEG service that delivers required data, and offers it at a specific internet address, using HTTP.		
Means of Verification		
The architecture includes a local method for the vehicle systems to access the TPEG service via internet HTTP.		

REQ-SYS-005 DAB TDC is tunable

Req Code	Scope	Class
REQ-SYS-005	Architecture	Technical
Source		
UC-01.3.1		
Description		
The system shall be able to use a local method to tune to a specific DAB TDC (transparent data channel) by providing DAB tuning information, and receiving the data stream in that channel.		
Means of Verification		
The architecture includes a local method for the vehicle systems to tune and receive an existing DAB Ensemble. A specific TDC in it can be tuned a received and the stream data, transmitted in it, is locally delivered as a constant (and potentially infinite) stream.		

REQ-SYS-006 DAB Ensemble service information from FIC is provided

Req Code	Scope	Class
REQ-SYS-006	Architecture	Technical
Source		
UC-01.3.1		
Description		
The system has a local method that gives access to the service information extracted from the FIC (Fast information channel), of a specified DAB Ensemble. This method shall allow searching for DAB TPEG services and acquiring the necessary access information. A "DAB Ensemble" is the smallest unit that can be broadcasted via transmitters. It is a multiplex of different channels, containing structural information in exactly one so-called "FIC" and content data in multiple so called "sub channels". This typically allows broadcasting multiple audio programs and/or data services. The DAB Ensemble has a fixed total gross bandwidth. Each DAB Ensemble can be transmitted by one or more transmitter stations, forming a so called "single frequency network" that might span small areas (e.g. city center), up to very large areas (e.g. whole Germany or beyond). FIC (fast information channel) is the essential first source of information that must be read by typical receivers. It describes the content and structure of the DAB Ensembles, and allows to search for specific services and their IDs. According to the information received and decoded from the FIC, it is possible to use the content of the DAB ensemble and to access the relevant sub channels and the contained services and data. The FIC therefore helps to lookup the sub channel and to figure out which sub channel contains what kind of data. In the next step, the specific sub channel is then read and decoded. For reception, it is typical that low level API delivers the FIC as is or a medium level API may deliver decoded information (similar to a local database, describing structure and services of the DAB ensemble). Such an API would as well deliver one specific sub channel as an infinite stream of bytes. Depending on its content, it needs to be decoded by higher levels of the software. A TPEG decoder would take such a sub channel stream (as a generic byte stream) and decode it, according to the TPEG protocol. Further information see: [31].		
Means of Verification		
The architecture includes a local method for the vehicle systems that delivers service information for a specific DAB Ensemble. By using the returned information, it is possible to identify DAB TPEG services and to start reception (see REQ-SYS-005).		

REQ-SYS-007 Necessity of a legal ground for data processing

Req Code	Scope	Class
REQ-SYS-007	Architecture	Organizational
Source		
Description		
If personal data is processed valid legal ground for the processing is required alternatively an informed consent of the data subjects concerned.		
Means of Verification		
Expert review: A legal expert on data protection law reviews the possible legal grounds or the consent forms.		

REQ-SYS-009 Identity provider for vehicles is provided by the cloud

Req Code	Scope	Class
REQ-SYS-009	Architecture	Technical
Source		
UC-04.1; UC-08.1		
Description		
The System shall have a method that recognizes vehicles by their identification registered in the cloud (i.e. the backend server) and services the authentication of the vehicle in the overall system. This is for the initial process only. For services usage pseudonym or anonym identifications derived from the identification should be used.		
Means of Verification		
A method shall exist that allows registration of vehicles with unique vehicle identification. The identity provider can be used within the systems network.		

REQ-SYS-010 The vehicle is equipped with V2X communication means

Req Code	Scope	Class
REQ-SYS-010	Architecture	Technical
Source		
UC-04.1		
Description		
The vehicle has means to communicate its unique vehicle ID to the infrastructure via V2X (=G5 / 802.11p) communication as functional alternative to RFID vehicle Identification Technology.		
Means of Verification		
The vehicle has a local method that allows to identify towards the infrastructure via V2X technology.		

REQ-SYS-011 The infrastructure is equipped with V2X communication

Req Code	Scope	Class
REQ-SYS-011	Architecture	Technical
Source		
UC-04.1		
Description		
The infrastructure has means to communicate via V2X in order to receive an identification from another (mobile) station via V2X technology infrastructure.		
Means of Verification		
The infrastructure has a local method that allows receipt of stations identification via V2X technology		

REQ-SYS-012 The infrastructure equipped with an access barrier

Req Code	Scope	Class
REQ-SYS-012	Architecture	Technical
Source		
UC-04.1; UC-08.1		
Description		
The combined car park and vehicle-charging infrastructure shall have means to grant or block access of vehicles.		
Means of Verification		
A method exists in the infrastructure to physically block or grant vehicle access to the combined car park and charging facilities		

REQ-SYS-019 The vehicle is equipped with a RFID Tag

Req Code	Scope	Class
REQ-SYS-019	Architecture	Technical
Source		
UC-08.1		
Description		
The vehicle shall be equipped with an RFID Tag that enables the reading from the infrastructure of the unique vehicle identification through RFID technology. In the future, this ID should by dynamically changeable to allow pseudonym service usage with no tracking.		
Means of Verification		
The vehicle has a RFID tag or is able to hold such an tag.		

REQ-SYS-020 The car park infrastructure equipped with a RFID reader

Req Code	Scope	Class
REQ-SYS-020	Architecture	Technical
Source		
UC-08.1		
Description		
The car park infrastructure is equipped with a RFID reader to read all accessible RFID Tags that are in the reach of the RFID reader.		
Means of Verification		
The infrastructure has a local method to read all accessible RFID Tags within the reach of the RFID reader.		

REQ-SYS-021 The infrastructure access to the reservation service backend server.

Req Code	Scope	Class
REQ-SYS-021	Architecture	Technical
Source		
UC-08.2, UC-04.2		
Description		
The combined car park and vehicle charging infrastructure has means to access reservation data of the reservation service backend server to check the validity of the reservation.		
Means of Verification		
A method exists in the infrastructure that can check the validity of a reservation data using the reservation service backend server.		

REQ-SYS-022 The reservation service backend server has access to the registration backend server.

Req Code	Scope	Class
REQ-SYS-022	Architecture	Technical
Source		
UC-04.1, UC-08.1		
Description		
The reservation service backend server has access to the registration backend server to verify the validity of the reservation data within the registration data.		
Means of Verification		
A method exists in the cloud that can prove the access from the reservation service backend server to registration backend server to check the validity of a reservation.		

REQ-SYS-023 Postal address can be translated to map location

Req Code	Scope	Class
REQ-SYS-023	Architecture	Technical
Source		
UC-01.4		
Description		
The onboard system (vehicle) shall be able to translate a postal address (destination) to a map location that is used internally.		
Means of Verification		
The architecture includes a local method for the vehicle systems that takes a postal address (e.g. city, street, house number) and returns a logical location within the map used internally (e.g. for filtering charging parks nearby, for calculating a route, etc.)		

REQ-SYS-024 TPEG locations can be translated to map locations

Req Code	Scope	Class
REQ-SYS-024	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard system (vehicle) has a local method to translate locations used by TPEG services, into map locations (used internally). To guarantee functionality for situations where TPEG service can be received via DAB, but no internet connection exists, the method must be operational without internet connection.		
Means of Verification		
The architecture includes a local method for the vehicle systems that takes locations in the format used by TPEG services, and returns a logical location matched in the map, that is used internally.		

REQ-SYS-025 DAB Ensembles can be sought

Req Code	Scope	Class
REQ-SYS-025	Architecture	Technical
Source		
UC-12, UC-01, UC-02		
Description		
The onboard system (vehicle) has a local method to scan through receivable DAB Ensembles. A DAB receiver scans through all possible frequencies, looks for DAB ensembles and returns information about DAB ensembles found, including their tuning information.		
Means of Verification		
The architecture includes a local method for the vehicle systems that delivers a collection of tuning information about DAB ensembles that can be currently received.		

REQ-SYS-026 DAB reception quality is reported

Req Code	Scope	Class
REQ-SYS-026	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard system (vehicle) has a local method to report DAB reception quality, to tell if reception works sufficiently and to compare the quality of different DAB ensembles and DAB services. For a currently tuned DAB ensemble, the quality report can be delivered without interruption of the reception of streams from this DAB ensemble. A report for a currently not tuned DAB ensemble shall be possible, but may need retuning of the receiver and thus would interrupt the reception. The quality report may include signal strength, signal to noise ration and bit error rates.		
Means of Verification		
The architecture includes a local method for the vehicle systems that delivers DAB quality information for a given DAB ensemble.		

REQ-SYS-027 TPEG service with charging park information transmitted in DAB

Req Code	Scope	Class
REQ-SYS-027	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The cloud/backend services broadcast as a DAB service a TPEG service that contains the needed information for booking and using a charging park. The transmission area of the DAB broadcast covers the relevant area, where an intended receiver may be located. Car park operator delivers the TPEG information to all service providers interested. The information is available for broadcasting (cellular, DAB) for all interested services.		
Means of Verification		
The architecture includes a suitable service, with a suitable transmission area and a suitable content is being broadcasted.		

REQ-SYS-028 TPEG service with safety information transmitted in DAB

Req Code	Scope	Class
REQ-SYS-028	Architecture	Technical
Source		
UC-12		
Description		
The cloud/backend services broadcast as a DAB service a TPEG service that contains the needed safety related information. The transmission area of the DAB broadcast covers the relevant area, where an intended receiver may be located. The content of the TPEG service should cover at least the transmission area.		
Means of Verification		
The architecture includes a suitable service, with a suitable transmission area and a suitable content is being broadcasted.		

REQ-SYS-029 TPEG service with traffic information transmitted in DAB

Req Code	Scope	Class
REQ-SYS-029	Architecture	Technical
Source		
UC-12		
Description		
The cloud/backend services broadcast as a DAB service a TPEG service that contains the needed information about the current traffic situation. The transmission area of the DAB broadcast covers the relevant area, where an intended receiver may be located. The content of the TPEG service should cover an area larger than the transmission area, including an outlook beyond the transmissions area.		
Means of Verification		
The architecture includes a suitable service, with a suitable transmission area and a suitable content is being broadcasted.		

REQ-SYS-030 Internet address for reservation request known

Req Code	Scope	Class
REQ-SYS-030	Architecture	Technical
Source		
UC-01		
Description		
The onboard systems (vehicle) shall hold an internet address (IP) that can be used to send a reservation request. This information must not be retrieved via IP communication.		
Means of Verification		
The architecture includes a local method for the vehicle systems to know where to send a reservation request. This information must be known as soon as the User selects the desired charging park.		

REQ-SYS-031 Charging parks can be filtered

Req Code	Scope	Class
REQ-SYS-031	Architecture	Technical
Source		
UC-01		
Description		
The onboard systems (vehicle) have a local method to filter the available charging parks by multiple criteria. As soon as information about charging parks is available in the onboard system (vehicle) the available charging parks are filtered by distance from the destination, by suitability to charge this vehicle and by suitability to handle reservation and payment. Additional criteria such as maximal possible vehicle height or others more might be used. The result of the filtering is used to present remaining charging parks to the User.		
Means of Verification		
A local method exists to filter charging parks by at least the following criteria: a) Distance to a given logical location (according to the internal map). b) Suitability to charge the given vehicle (thus our vehicle). c) Suitability to handle payment methods. d) Possibility to reserve a charging point.		

REQ-SYS-032 Reservation request can be sent

Req Code	Scope	Class
REQ-SYS-032	Architecture	Technical
Source		
UC-01		
Description		
The onboard systems (vehicle) are able to send a reservation request to an internet address.		
Means of Verification		
The architecture includes a local method for the vehicle systems to allow sending a reservation request via internet connection.		

REQ-SYS-033 Reservation information is forwarded

Req Code	Scope	Class
REQ-SYS-033	Architecture	Technical
Source		
UC-01		
Description		
The cloud/backend services shall forward reservation information to the parking garage. The forwarded information allows the parking garage to grant access to the charging park and charging point and to support the payment process. The parking garage acknowledges the transmission.		
Means of Verification		
The architecture includes a method to handle communication, about reservations, between the cloud/backend service and the parking garage.		

REQ-SYS-034 Charging park information available

Req Code	Scope	Class
REQ-SYS-034	Architecture	Technical
Source		
UC-01		
Description		
The cloud/backend services shall have access to information about relevant charging parks (static data) and their status and capacity (dynamic data). This includes general static information about the charging parks (e.g. location, size, kind of service) and dynamic (fast changing) information (e.g. free capacity). All information needed to support the broadcast of a TPEG service is available. Status and free capacity is frequently delivered to the cloud/backend services.		
Means of Verification		
The architecture includes a mechanism assuring that the cloud/backend services have all needed information for the TPEG services. This includes a) knowledge about all relevant charging parks, b) location of the charging parks, c) size and current capacity (free vs. occupied points), d) available services for charging, payment and reservation.		

REQ-SYS-035 Current safety relevant information is known

Req Code	Scope	Class
REQ-SYS-035	Architecture	Technical
Source		
UC-01		
Description		
The cloud/backend services have knowledge about safety relevant information that is used to support the TPEG service. This includes information about dangers such as obstacles, accidents, lost loads or debris, road conditions, sight conditions, other vehicles, traffic situations, etc.		
Means of Verification		
The architecture includes a mechanism that keeps the relevant information available and constantly updated in the cloud/backend services.		

REQ-SYS-036 The route can be calculated

Req Code	Scope	Class
REQ-SYS-036	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard system (vehicle) have a method to calculate a route from one location (e.g. current location) and another location (e.g. destination), by using a map the represents actual roads and take traffic rules (e.g. where you are allowed to turn) into account. For the calculation, the current traffic situation is taken into account. The calculation yields the route and the estimated duration.		
Means of Verification		
The architecture includes a component in the vehicle systems to do routing calculations based on a map. It has an interface for the reception of the current traffic situation. The received traffic situation is taken into account for the routing calculation.		

REQ-SYS-037 Information can be presented to the User

Req Code	Scope	Class
REQ-SYS-037	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard systems (vehicle) is able to give information about a) information supply quality b) danger is ahead c) problem with route (e.g. roadblock) d) insufficient range e) change of arrival time Note: This requirement covers the essential need that this information can somehow be delivered to the User.		
Means of Verification		
The architecture includes a local method to deliver the information to the User.		

REQ-SYS-043 All data relevant for billing is digitally signed

Req Code	Scope	Class
REQ-SYS-043	Architecture	Technical
Source		
UC-06		
Description		
All the data, which is relevant for billing the parking fees, shall be digitally signed by the entity that gathered it. The data and signature shall be sent to the billing service as a pair.		
Means of Verification		
Check which data is relevant for billing (e.g. parking duration). Check which entity gathers this data (e.g. car park). Check if that entity digitally signs that data and if the data as well as the signature is sent to the billing service.		

REQ-SYS-044 The tracking information is transmitted via an authenticated channel

Req Code	Scope	Class
REQ-SYS-044	Architecture	Technical
Source		
UC-07		
Description		
The position tracking information established by the car park shall be sent to the vehicle via an authenticated communication channel. All data shall be checked for integrity and authenticity.		
Means of Verification		
Check if the car park and vehicle establish an authenticated communication channel (e.g. secured by SSL). Check if tracking information is checked for authenticity and integrity (e.g., a MAC is used).		

REQ-SYS-045 Driver authentication at the vehicle request Service Provider

Req Code	Scope	Class
REQ-SYS-045	Architecture	Technical
Source		
UC-11		
Description		
For the usage of the vehicle request service, the Driver needs to be authenticated at the vehicle request Service Provider.		
Means of Verification		
An entity providing a secure authentication mechanism exists.		

REQ-SYS-046 App vehicle request service can communicate with vehicle request Service Provider

Req Code	Scope	Class
REQ-SYS-046	Architecture	Technical
Source		
UC-011		
Description		
For the service usage and registration, the Driver shall be able to communicate with vehicle request Service Provider via the vehicle request app.		
Means of Verification		
A communication channel between vehicle request app and the vehicle request Service Provider is specified by the architecture.		

REQ-SYS-047 Vehicle can communicate with vehicle request Service Provider

Req Code	Scope	Class
REQ-SYS-047	Architecture	Technical
Source		
UC-011		
Description		
For the service usage and registration, the vehicle shall be able to communicate with vehicle request Service Provider.		
Means of Verification		
A communication channel between the Vehicle and vehicle request Service Provider is specified by the architecture.		

REQ-SYS-048 Driver authentication at Vehicle

Req Code	Scope	Class
REQ-SYS-048	Architecture	Technical
Source		
UC-11		
Description		
The Driver needs to be authenticated by the Vehicle, to be allowed to request the vehicle.		
Means of Verification		
A secure authentication mechanism is given. The Driver should be authenticated via his personal device (smartphone) to the vehicle. This coupling needs to be done before the vehicle request service can be used.		

REQ-SYS-078 Transmission of destination address

Req Code	Scope	Class
REQ-SYS-078	Architecture	Technical
Source		
UC-02		
Description		
The system shall use navigable, map independent addresses. (e.g. for communication of destination car-park between parking lot reservation app and the navigation system)		
Means of Verification		
Expert Rating: The architectures defines an interface, describing the format, data type and protocol, over which the address can be communicated.		

REQ-SYS-079 Present routes to Driver

Req Code	Scope	Class
REQ-SYS-079	Implementation	Technical
Source		
UC-02		
Description		
The system shall be able to present a selection of possible routes to a Driver.		
Means of Verification		
The tester (as a Driver) inputs a destination point of which he knows that multiple routes exist. The navigation system then shall provide him a selection of possible routes.		

REQ-SYS-080 Driver selects route

Req Code	Scope	Class
REQ-SYS-080	Implementation	Technical
Source		
UC-02		
Description		
The system shall allow the Driver to select one route out of a set of possible routes.		
Means of Verification		
Out of a set of possible routes (see REQ-SYS-079) the tester (in the role as Driver) selects a desired route in the navigation system. The navigation system then starts navigating this route.		

REQ-SYS-081 TPEG in navigation system

Req Code	Scope	Class
REQ-SYS-081	Implementation	Technical
Source		
UC-02		
Description		
The navigation system shall be able to interpret TPEG messages, which for example are queried from a storage, so it can adapt its routing choices.		
Means of Verification		
Expert Rating: A defined interface, specifying the format, data type, and protocol, exists over which TPEG messages can be communicated to the navigation system.		

REQ-SYS-082 TPEG information storage

Req Code	Scope	Class
REQ-SYS-082	Architecture	Technical
Source		
UC-02		
Description		
The system shall provide a mechanism to store TPEG information temporary. (This shall buffer TPEG information, e.g. received in periodic transmissions, so they are still available when a system component needs them.)		
Means of Verification		
Expert Rating: A component to store the information is planned in the architecture. Its interfaces, including the format, data types and protocol, is specified.		

REQ-SYS-083 Query TPEG information storage

Req Code	Scope	Class
REQ-SYS-083	Architecture	Technical
Source		
UC-02		
Description		
The system shall provide a mechanism for components to obtain current TPEG information from a buffer (TPEG information storage).		
Means of Verification		
Expert Rating: The TPEG information storage component in the architecture defines an interface, including format, data types and protocol, to query information from it.		

REQ-SYS-084 Forward destination to server

Req Code	Scope	Class
REQ-SYS-084	Architecture	Technical
Source		
UC-02		
Description		
The system shall provide a mechanism over which a vehicle navigation system can forward its destination and vehicle information to a routing server.		
Means of Verification		
Expert rating: The architecture describes a communication link, which can be used by the navigation system to communicate the necessary information.		

REQ-SYS-085 Transmit routes to vehicle

Req Code	Scope	Class
REQ-SYS-085	Architecture	Technical
Source		
UC-02		
Description		
The system shall provide a mechanism, over which a routing server can transmit n routes to a vehicle which previously requested them.(See REQ-SYS-084).		
Means of Verification		
Expert rating: The architecture describes a communication link, which can be used by the routing server to communicate back the necessary information.		

REQ-SYS-086 Decide which routing to use

Req Code	Scope	Class
REQ-SYS-086	Implementation	Technical
Source		
UC-02		
Description		
The system shall provide a possibility for the Driver to either use local routing or server site routing.		
Means of Verification		
The tester (in the role of a Driver) can configure server site routing or local routing.		

REQ-SYS-087 DAB TPEG service found

Req Code	Scope	Class
REQ-SYS-087	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The DAB receiver offers information about DAB TPEG services found/received, including information needed to pick and tune the service, and information to discriminate different services.		
Means of Verification		
The architecture includes a method how the DAB receiver gives information about DAB TPEG services.		

REQ-SYS-088 Clocks are synchronized

Req Code	Scope	Class
REQ-SYS-088	Architecture	Technical
Source		
UC-06		
Description		
The clocks of all entities that gather billing relevant data shall be synchronized with a time service.		
Means of Verification		
Check if the IT components use a time synchronization protocol.		

REQ-SYS-089 All data transmissions to billing services are encrypted and authenticated

Req Code	Scope	Class
REQ-SYS-089	Architecture	Technical
Source		
UC-06		
Description		
All the data transmissions to billing services shall be end-to-end encrypted.		
Means of Verification		
Check if data transmissions to billing services are handled using contemporary transport security (e.g. TLS), with encryption and authentication enabled.		

REQ-SYS-091 Pseudonymization shall be applied in the identity provider

Req Code	Scope	Class
REQ-SYS-091	Architecture	Technical
Source		
UC-04, UC-08		
Description		
Pseudonymization shall be applied in the identity provider in order to avoid that personal data is retrieved during parking or charging.		
Means of Verification		
The reserved parking and charging can be executed without tracking back to the person or vehicle.		

REQ-SYS-092 The vehicle has one and only one unique ID

Req Code	Scope	Class
REQ-SYS-092	Architecture	Technical
Source		
UC-04, UC-08		
Description		
The vehicle/User shall be use one and only one unique vehicle identification for an authentication necessary for a service usage. This ID should not be used for another service or even the usage of the same service at a later opportunity.		
Means of Verification		
Every registered vehicle can be identified for one authentication service usage with one unique ID independent whether RFID or V2X technology is used. Accordingly, the vehicle ID can be determined on the infrastructure side either by reading out the EPC/TID pair of the RFID via RFID Reader device or by reading out the same EPC/TID pair of the OBU via a new, to be specified message exchanged between OBU and RSU, on request of the RSU.		

REQ-SYS-093 Conditional access depending on availability

Req Code	Scope	Class
REQ-SYS-093	Architecture	Technical
Source		
UC-04, UC-08		
Description		
Registered vehicle gets access to parking/charging facilities depending on availability of the space.		
Means of Verification		
A vehicle is either accepted or rejected depending on whether unreserved space is available. The AP1 and AP2 architecture descriptions will define in details, how vehicles get access to a car park, if space is available or how they are rejected, if no space is available.		

REQ-SYS-094 Secure connection in authentication process

Req Code	Scope	Class
REQ-SYS-094	Architecture	Technical
Source		
UC-04, UC-08		
Description		
The communication link from the identification element to the identity provider is secured.		
Means of Verification		
The communication link from identification element to the identity provider cannot be hacked or corrupted by any external means independent from the identification method (RFID/V2X)		

REQ-SYS-095 Reservation protocol defined

Req Code	Scope	Class
REQ-SYS-095	Implementation	Technical
Source		
UC-01		
Description		
The onboard system (vehicle) and the background services (reservation service) shall support the same protocol that allows reservation of a charging slot (parking slot, with charging option). A protocol must be defined that describes which kind of information is exchanged in which format and chronology. This includes the questions, • if and how the reservation uses IDs, authentication and identification • what kind of information is included in the reservation (e.g. payment information, e-mobility-Provider Contract identification, vehicle number plate, desired kind of charger, vehicle dimensions, ...) • how a reservation request is identified and referenced later Compare to the TPEG EMI reservation protocol that may be used (directly or in a modified way). Architecture needs to make general decisions to ensure that data is available, the workflow is possible and privacy issues may be clarified. If reservations shall be adapted later (during the trip) due to a change in the estimated arrival time, this affects not only UC-01, but as well UC-02: Existing reservation must be referenced for changes, authentication might be needed to permit changes. Indirectly this affects other use cases that are based on information exchanged during the reservation (e.g. entry control for the charging park / parking area).		
Means of Verification		
The architecture shall include a general definition of the concepts and protocols that will be used and which information shall be exchanged during the reservation.		

REQ-SYS-096 TPEG information access needs to be defined

Req Code	Scope	Class
REQ-SYS-096	Implementation	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard systems (vehicle) need to agree on methods to access TPEG Information. Preferably the following shall be defined: • only one homogenous method is used for the access (but not multiple methods and concepts) • the TPEG information storage offers all TPEG information to all other components • the TPEG information handles the management of the TPEG information (TPEG messages) At least a general concept must be defined for the Architecture on these topics: • access API, based on an object model • if and how, which kind of events shall be triggered (so to say: proactive information upon reception) • kind of locations to be used (raw locations, mapped locations; based on which reference map) are used (so to say: which component does map matching)		
Means of Verification		
The architecture shall define a general access concept answering the given questions, to allow checking if all needed functionality is included in the architecture somewhere.		

REQ-SYS-097 TPEG binary stream must be decoded

Req Code	Scope	Class
REQ-SYS-097	Implementation	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard system (vehicle) shall be able to decode a received TPEG binary stream that allows filling the TPEG information storage. See as well REQ-SYS-096, where the object model for the TPEG information storage must be defined. This requirement covers the gap between reception and filling of the TPEG information storage.		
Means of Verification		
The architecture shall define a component that is able to decode the TPEG binary stream and to cover the gap between reception and the TPEG information storage.		

REQ-SYS-098 Spatial filtering possible

Req Code	Scope	Class
REQ-SYS-098	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard systems (vehicle) shall be able to do a spatial filtering. A geographical radius around a given position can filter information with attached location information. This functionality is needed to implement a correct hybrid TPEG approach, where (carrier dependent) information is filtered in the client (DAB TPEG service) or in the server (Internet TPEG service). Both (local and server side) spatial filtering shall use the same algorithm to ensure identical behavior. This allows switching between DAB and internet, without changing the behavior of the TPEG service.		
Means of Verification		
The architecture contains local functionality in the onboard system (vehicle) that allows spatial filtering.		

REQ-SYS-099 Hybrid TPEG switching is controlled

Req Code	Scope	Class
REQ-SYS-099	Implementation	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard system (vehicle) shall be able to make decisions which carrier (DAB, internet) to use, in order to receive a TPEG service. The decision shall include a mechanism to control reception via DAB and internet, thus to trigger and control the switching. This typically includes DAB tuning control, triggering internet requests and checking if reception is effectively possible by using a certain carrier.		
Means of Verification		
The architecture includes a mechanism that controls the reception of a TPEG service, by both using and controlling DAB reception and internet connectivity.		

REQ-SYS-100 App CarStateOfChargeService can communicate with Service Provider CarStateOfChargeService

Req Code	Scope	Class
REQ-SYS-100	Architecture	Technical
Source		
UC-10		
Description		
For the service usage and registration, App_CarStateOfChargeService shall be able to communicate with SP_CarStateOfChargeService.		
Means of Verification		
Communication channel between App_CarStateOfChargeService and SP_CarStateOfChargeService is specified by the architecture.		

REQ-SYS-101 Vehicle can communicate with App_CarStateOfChargeService

Req Code	Scope	Class
REQ-SYS-101	Architecture	Technical
Source		
UC-10		
Description		
For the service usage and registration, the vehicle shall be able to communicate with App_CarStateOfChargeService.		
Means of Verification		
A communication channel between the Vehicle and App_CarStateOfChargeService is specified by the architecture.		

REQ-SYS-102 Driver authentication at SP_CarStateOfChargeService

Req Code	Scope	Class
REQ-SYS-102	Architecture	Technical
Source		
UC-10		
Description		
For the usage of the CarStateOfCharge-Service, the Driver needs to be authenticated at the SP_CarStateOfChargeService via App_CarStateOfChargeService.		
Means of Verification		
A secure authentication mechanism for entities is given that authenticate the User's device at the SP_CarStateOfChargeService.		

REQ-SYS-103 Vehicle can communicate with SP_CarStateOfChargeService

Req Code	Scope	Class
REQ-SYS-103	Implementation	Technical
Source		
UC-10		
Description		
For the service usage and registration, the vehicle shall be able to communicate with SP_CarStateOfChargeService. Vehicle send to SP_CarStateOfChargeService its charge state.		
Means of Verification		
The registration of the vehicle and the charge state is available at the SP_CarStateOfChargeService.		

REQ-SYS-105 Vehicle authentication at SP_CarStateOfChargeService

Req Code	Scope	Class
REQ-SYS-105	Architecture	Technical
Source		
UC-10		
Description		
For the usage of the CarStateOfCharge-Service, the Vehicle needs to be authenticated at the SP_CarStateOfChargeService.		
Means of Verification		
A secure authentication mechanism usable by the Service Provider is described in the architecture.		

REQ-SYS-109 International transfer of personal data

Req Code	Scope	Class
REQ-SYS-109	Architecture	Organizational
Source		
Description		
If personal data is transferred to third countries (countries outside of the European union), an adequate level of protection has to be ensured and the User must be informed prior to the transfer with the option to prevent the transfer.		
Means of Verification		
Due to the legal uncertainties in this field, it is currently not possible to determine a reliable means of verification. Personal data must not be transferred to third countries.		

REQ-SYS-110 Traffic Light Forecast quality schema exists

Req Code	Scope	Class
REQ-SYS-110	Architecture	Technical
Source		
UC-03		
Description		
The Traffic Light Forecast quality must be quantified (e.g. deviation from real transition in seconds measured along forecast horizon) to allow monitoring of the forecast quality. The system shall be able to produce such a quality analysis report		
Means of Verification		
a) definition of quality measurement exists and b) system can output the quality		

REQ-SYS-111 Traffic Light Forecast can be received by IEEE 802.11p

Req Code	Scope	Class
REQ-SYS-111	Implementation	Technical
Source		
UC-03.1		
Description		
SPAT/MAP messages are sent by the intersection and received by an in-vehicle device successfully.		
Means of Verification		
Survey in-vehicle device service: Can GLOSA/TTG be shown if no internet is available? Fallback & debug: can log-files show what has been sent/received?		

REQ-SYS-112 Traffic Light Forecast can be received by Internet

Req Code	Scope	Class
REQ-SYS-112	Implementation	Technical
Source		
UC-00		
Description		
SPAT/MAP messages are sent by the central service and received by an in-vehicle device successfully.		
Means of Verification		
Survey in-vehicle device service: Can GLOSA/TTG be shown if no internet is available? Fallback & debug: can log-files show what has been sent/received?		

REQ-SYS-113 The architecture shall be flexible to allow extensions for new messages and protocol elements

Req Code	Scope	Class
REQ-SYS-113	Architecture	Technical
Source		
general		
Description		
User of the architecture shall know the possibilities and constraints the architecture imposes on such extensions. Reasoning: connected mobility is extending in the next years. New elements and improvement of existing mechanisms will occur.		
Means of Verification		
Explain by showing I) how these examples work: a) use introduction of authentication method, b) introduction of a handle that helps to identify one and the same information through different channels to be recognized it is the same on receiver side c) extension of existing message with new additional content; describe II) where are difficulties and limitations for extensions		

REQ-SYS-114 The architecture shall allow "hybrid" communication i.e. same content being delivered through multiple channels simultaneously

Req Code	Scope	Class
REQ-SYS-114	Architecture	Technical
Source		
UC-02		
Description		
The architecture shall support such approaches. Both – local (11p, V-LTE/D2D LTE) and central (internet services) or in-between (e.g. mobile edge computing) approaches must be possible realizations of the architecture. Reasoning: Today such approaches do exist (e.g. TPEG messages via DAP and mobile internet) or are required (e.g. V2X messages via 11p and LTE).		
Means of Verification		
Explain how the same content can be delivered over several communication channels. Explain how the different technologies can be a realization of the architecture.		

REQ-SYS-115 Same information through different channels can be identified to be the same by a receiver

Req Code	Scope	Class
REQ-SYS-115	Architecture	Technical
Source		
all/ UC-02		
Description		
A receiver must be able to identify information received through different channels as the same to prevent multiple display of the same information as otherwise this may lead to misunderstandings, overloads or Driver distraction e.g. if a warning is presented multiple times though it is on the same subject		
Means of Verification		
Explain how a receiving entity can identify that a message received through several ways is the same message.		

REQ-SYS-116 V2X PKI as defined for Europe is supported by the architecture

Req Code	Scope	Class
REQ-SYS-116	Architecture	Technical
Source		
all/ UC-02		
Description		
The architecture shall support V2X communication (ETSI ITS G5 starting with 11p and being applied to cellular technology in future) using a PKI approach to identify valid “ITS” stations.		
Means of Verification		
Explain how the PKI system (at least the one defined for Europe) can be used with the architecture. Explain how future variants (e.g. using Attribute Based Credentials “ABCs” will also suit to the architecture		

REQ-SYS-117 Bi-directional communication support

Req Code	Scope	Class
REQ-SYS-117	Architecture	Technical
Source		
all/ UC-02		
Description		
For certain services, the architecture must be capable to support bi-directional communication. Thus, the architecture must support such communications as some communication elements in connected services are using deliberately the advantage of 'unidirectional / broadcast' based communication technologies.		
Means of Verification		
Explain how bi-directional service scenarios can be achieved. Ideally show how this can be achieved even when involving a unidirectional technology e.g. DAB within a bi-directional service.		

REQ-SYS-118 The architecture shall support using SPAT/MAP messages

Req Code	Scope	Class
REQ-SYS-118	Architecture	Technical
Source		
UC-02		
Description		
Sub-requirement to REQ-SYS-011: The message processing of these messages must be possible within the architecture.		
Means of Verification		
A method (or component) for processing of SPAT/MAP messages should exist in the Architecture		

REQ-SYS-119 The architecture shall support using DENM messages

Req Code	Scope	Class
REQ-SYS-119	Architecture	Technical
Source		
all/ UC-02		
Description		
Sub-requirement to REQ-SYS-011: The message processing of these messages must be possible within the architecture.		
Means of Verification		
The architecture contains interfaces, especially between vehicles and infrastructure, which allow the communication of standard compliant DENM messages. For both sides - vehicle and infrastructure - the interfaces can be identified by an expert.		

REQ-SYS-120 The architecture shall support using CAM messages

Req Code	Scope	Class
REQ-SYS-120	Architecture	Technical
Source		
UC-02		
Description		
Sub-requirement to #141 REQ-SYS-011: The message processing of CAM messages must be possible within the architecture.		
Means of Verification		
Show by explanation / demonstration: Is the message sending and receiving possible?		

REQ-SYS-121 The architecture shall support using authentication messages

Req Code	Scope	Class
REQ-SYS-121	Architecture	Technical
Source		
all		
Description		
Sub-requirement to REQ-SYS-011: Several services require that a service consumer (Driver / vehicle) authenticate itself as a valid User (e.g. one who has paid, who has reserved). Such a mechanisms has not been standardized in v2X so far. The project shall propose / show such a mechanism.		
Means of Verification		
Show by explanation / demonstration: is such a function specified within the system? Is there an explanation which elements and functions are needed at which locations of the architecture?		

REQ-SYS-122 There shall be in-vehicle services using SPAT/MAP for energy efficient driving

Req Code	Scope	Class
REQ-SYS-122	Implementation	Technical
Source		
UC-02		
Description		
To demonstrate the benefits of SPAT/MAP forecast a service in the vehicle shall use the data and apply it to a service (e.g. GLOSA, TTG, ACC)		
Means of Verification		
Show by demonstration: Is such a service implemented? Do receiving vehicles use SPAT/MAP?		

REQ-SYS-123 The system shall support a service for Traffic Light Forecast (TLF)

Req Code	Scope	Class
REQ-SYS-123	Architecture	Technical
Source		
UC-02		
Description		
Various connected/autonomous functions benefit from knowing not just the state but also the forecast of permissions given by traffic signal. Thus a service producing the forecast (e.g. centrally) must be part of the architecture		
Means of Verification		
Show by going through the architecture: Can a service like TLF be represented in the architecture?		

REQ-SYS-124 The system shall support an option to run prioritization of vehicles at intersections

Req Code	Scope	Class
REQ-SYS-124	Architecture	Technical
Source		
UC-02		
Description		
Autonomous connected driving can leverage further benefits when it is used to replace and extend existing prioritization. The architecture shall support this feature and allow specific distinctions of priority categories such as i) special priority for rescue and executive use; ii) classic prioritization of public transport iii) soft and intelligent prioritization e.g. for vehicle clusters, heavy vehicles, green/autonomous vehicles		
Means of Verification		
The architecture has a communication links to forward vehicle information from the vehicles to a traffic control/prioritization service and communications links to traffic influence systems (e.g. a traffic light).		

REQ-SYS-125 EV Charging Station and Charge Point Management System can communicate on authentication

Req Code	Scope	Class
REQ-SYS-125	Architecture	Technical
Source		
UC-09		
Description		
When a User wants to charge, the charging station needs to know if it can allow the User to do so. This requirement demands an interface function between the Charge Point Management System and the EV Charging Station through which authentication information can be exchanged (e.g. tokens, whitelists).		
Means of Verification		
The Architecture has an interface supporting the required function.		

REQ-SYS-126 The architecture describes a linkage of charging stations to the overall system

Req Code	Scope	Class
REQ-SYS-126	Architecture	Technical
Source		
UC-09		
Description		
Charging stations must communicate with the consumers (vehicles / Users) on one hand and with its operator and further the services, they belong to, on the other hand. The architecture shall describe how such communication links can/shall be achieved		
Means of Verification		
Explain / demonstrate: Which connections are foreseen in general (framework architecture) and how can such communications links be achieved with standards?		

REQ-SYS-127 Open / nondiscriminatory access for all e-vehicles to charging infrastructure is supported

Req Code	Scope	Class
REQ-SYS-127	Architecture	Technical
Source		
UC-09		
Description		
The charging infrastructure should allow Users to be able to charge their vehicles regardless of the Service Provider or charging station operator. The architecture should support "roaming" functionality.		
Means of Verification		
A component exists in the architecture that allows individual charging station operators and e-mobility Service Providers to deliver roaming functionality to end Users.		

REQ-SYS-128 Type of charging plugs

Req Code	Scope	Class
REQ-SYS-128	Implementation	Technical
Source		
UC-09		
Description		
The charging station should be equipped only with standard connectors according to the specifications of IEC62196-2 for AC and IEC62196-3 for DC charging.		
Means of Verification		
It should be verified in the charging station technical specifications documents if the supplied connectors are listed as compliant to the required standards.		

REQ-SYS-129 Power supply for EV Charging stations

Req Code	Scope	Class
REQ-SYS-129	Implementation	Technical
Source		
UC-09		
Description		
The following Power Supply shall be supported: AC power level up to 22 kW. DC power level up to 50 kW.		
Means of Verification		
The power supply infrastructure and capacity at the car park should be reviewed by an electrical engineer prior charging station installation. It is mandatory that the power supply infrastructure has sufficient capacity to support the charging station’s power levels.		

REQ-SYS-130 Vehicle tracking in car park

Req Code	Scope	Class
REQ-SYS-130	Implementation	Technical
Source		
UC-07		
Description		
The camera system shall track a slowly moving car within the car park by a sequence of precise positioning coordinates. Special focus of attention is the handshaking procedure when a car moves from the viewing range of one camera to the neighboring range.		
Means of Verification		
Demonstrate how a vehicle, which enters the car park, will be permanently tracked from the entrance to the parking/charging lot.		

REQ-SYS-131 Tracking of persons and other obstacles

Req Code	Scope	Class
REQ-SYS-131	Implementation	Technical
Source		
UC-07		
Description		
The camera system shall track a moving person within the car park by a sequence of precise positioning coordinates. Special focus of attention is the handshaking procedure when the person moves from the viewing range of one camera to the neighboring range. The tracking data is only stored as long as the User is in a possible conflict area with the vehicle. When the User is outside the tracking area, the data is deleted immediately.		
Means of Verification		
The camera system detects the current position of persons and other obstacles in the car park		

REQ-SYS-132 Occupancy of parking/charging lots

Req Code	Scope	Class
REQ-SYS-132	Architecture	Technical
Source		
UC-07		
Description		
If a vehicle arrives at the entrance of the car park, the car park shall check whether the designated parking/charging lot is not occupied.		
Means of Verification		
The car park demonstrates the detection of the two different states of occupancy of a parking/charging lot.		

REQ-SYS-133 Driving route calculation

Req Code	Scope	Class
REQ-SYS-133	Implementation	Technical
Source		
UC-06		
Description		
The car park shall calculate a route on the underlying routing graph from the current position of the vehicle to the destination within the car park. When entering the car park this route will usually guide from the entrance to the booked parking or charging lot, when leaving the other way round.		
Means of Verification		
Demonstrate how a route from an arbitrary starting point to a pre-booked charging lot will be provided by the car park.		

REQ-SYS-134 Transmission of the driving route

Req Code	Scope	Class
REQ-SYS-134	Implementation	Technical
Source		
UC-06		
Description		
Each vehicle shall receive its own individual driving route from the car park via 802.11p Wi-Fi connection based on the ITS-G5 standard.		
Means of Verification		
The vehicle needs for the autonomous driving process a pre-calculated route transmitted from the car park. The transmission process will be demonstrated.		

REQ-SYS-135 Calculation of the driving trajectory

Req Code	Scope	Class
REQ-SYS-135	Architecture	Technical
Source		
UC-06		
Description		
Based on a pre-calculated driving route the vehicle shall calculate the individual driving trajectory. This trajectory takes into account the specific driving parameters of the individual car. Since the car has only access to its own set of parameters this job has to be performed by each vehicle separately.		
Means of Verification		
For the autonomous driving process, the vehicle needs a precise driving trajectory the car will be navigated on.		

REQ-SYS-136 DAB TPEG service usage independent from internet connectivity

Req Code	Scope	Class
REQ-SYS-136	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The system shall not depend on internet connectivity, but shall be able to fulfill all functionality, that can be designed self-sufficient, without using internet connectivity. This explicitly includes reception, decoding and usage of TPEG services via DAB. This excludes the inevitable upload of information, while sending a reservation request. Despite this requirement, it is allowed to use internet connectivity for other purpose and as optional enhancements or temporary alternatives, especially if DAB reception is not available.		
Means of Verification		
The architecture shows no dependencies to internet connectivity, for functions that receive, decode and use TPEG services via DAB.		

REQ-SYS-137 Availability information shall not show individuals

Req Code	Scope	Class
REQ-SYS-137	Architecture	Technical
Source		
UC-01		
Description		
The system shall not disclosure any information that allows conclusion on individuals and their behavior. Availability information of car parks / charging parks, shall not deliver exact numbers for charging parks that are full or almost full, respectively are empty or almost empty. Instead, only a coarse filling degree shall be given, to cover individuals in the critical zones. In addition no occupation information for specific positions shall be given. E.g.; a charging park, with most positions empty, but only one vehicle using it, shall not be described as "1 position occupied, 29 positions empty", but with "many free positions", as this does not allow knowledge about the one individual vehicle. If the vehicle departs, the reading would still be "many free positions", instead of the more precise "0 positions occupied", that would reveal that the one specific vehicle has left the charging park. In fact, precise information about availability is not necessary. A coarse information is sufficient, and precise numbers may change fast anyway. iKoPA has its focus und larger charging parks. For very small charging parks, this requirement would be much harder to solve.		
Means of Verification		
The method to show availability does not provide knowledge about single vehicles or single charging points, but uses coarse levels to describe the availability.		

REQ-SYS-138 Multiple contracts are supported

Req Code	Scope	Class
REQ-SYS-138	Architecture	Technical
Source		
UC-01		
Description		
The system shall allow the User, to have and use multiple contracts, as alternatives to ensure some kind of pseudonymization. This only applies if the system (e.g. the identity provider) requires the User to create and use an "account" of some kind. By holding multiple accounts with their own specific identifier, the User is able to use multiple such identifier alternatively, allowing him to hide its identity between multiple pseudonyms. To ensure this to work, it is necessary that there is no other linking element. Therefore, this requirement goes hand in hand with the next requirement REQ-SYS-139 that calls for anonymous prepaid methods.		
Means of Verification		
The system allows the User to create and manage multiple accounts and switch between them, as he likes.		

REQ-SYS-139 Anonymous prepaying is allowed

<table>
<tr><th>Req Code</th><th>Scope</th><th>Class</th></tr>
<tr><td>REQ-SYS-139</td><td>Architecture</td><td>Technical</td></tr>
<tr><th colspan="3">Source</th></tr>
<tr><td colspan="3">UC-01</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">The system shall allow that the User creates an account without the need to give a bank account or credit card, but by just prepaying without revealing his identity.
This is important in combination with REQ-SYS-138 ("multiple accounts") to ensure that individual or multiple accounts cannot be tracked or linked to each other. Prepaid payment could work with cash money that is paid at a kiosk or super market to a specific account. The User could easily open such an account at these stations and use them, without the need to deliver any information that allow linking to its identity.</td></tr>
<tr><th colspan="3">Means of Verification</th></tr>
<tr><td colspan="3">The prepaid concept, without revealing personal information, is allowed and included into the system architecture.</td></tr>
</table>

REQ-SYS-140 Registration is protected against denial of service attacks

<table>
<tr><th>Req Code</th><th>Scope</th><th>Class</th></tr>
<tr><td>REQ-SYS-140</td><td>Architecture</td><td>Technical</td></tr>
<tr><th colspan="3">Source</th></tr>
<tr><td colspan="3">UC-01</td></tr>
<tr><th colspan="3">Description</th></tr>
<tr><td colspan="3">The system includes concepts and methods to prevent denial of service attacks by making vast amounts of reservations, without really using them.
The problem arises with a reservation system that does not know or track individuals. It is unaware who makes reservations and unable to block or avenge bogus reservations. Even if the reservation system finds out, that a lot of reservations where not used, it cannot track or link them, thus is vulnerable to repeated DoS attacks. Attackers could consume all available resources by making many reservations, making it impossible for normal Users to use the service anymore.
The system design must solve this, by including mechanisms that reduce or deny DoS attacks, or at least make punishment and blocking of further attacks possible.
Most likely this must be included in the identity provider, not only the reservation server.
E.g., a deposit could be taken from the account of the User that fetches a token from the identity provider, in order to make a reservation. The deposit is release only after the reservation was used and the vehicle has left the charging park again.</td></tr>
<tr><th colspan="3">Means of Verification</th></tr>
<tr><td colspan="3">The system is capable to defend itself sufficiently against DoS attacks through reservation by
a) punishing responsible actors (Users) that make reservations without using them
and
b) limiting the amount of open (yet unused) reservations from one responsible actor (User).
To clarify: (a) does not necessarily mean that on the very first occurrence of an unused reservation actions must be taken, but the systems at least needs to remember (internally) that a reservation was not used, and needs to (internally) count the number of unused reservations, to enforce punishment when reaching a threshold.
Both (a) and (b) require the system to be able (somehow) to enforce effective responsibility for reservations.</td></tr>
</table>

REQ-SYS-141 Reservation service exists

Req Code	Scope	Class
REQ-SYS-141	Architecture	Technical
Source		
UC-01		
Description		
The cloud/backend services offer a service, accessible via internet, to make reservations for charging points.		
Means of Verification		
The architecture includes a service that can be accessed via internet, which allows sending reservation requests and that returns information whether the reservation was successful or not.		

REQ-SYS-142 Current traffic situation is known

Req Code	Scope	Class
REQ-SYS-142	Architecture	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The cloud/backend services shall be able to access information about current traffic situation that is relevant for support the TPEG service. This includes information about traffic jams, accidents, work sites, detour, inhibits and other kind of information that is required to plan a route, optimize a route or figure out if a route is passable.		
Means of Verification		
The architecture includes a mechanism that allows updating the current traffic situation in the cloud/backend services.		

REQ-SYS-143 Concept how to inform the User

Req Code	Scope	Class
REQ-SYS-143	Implementation	Technical
Source		
UC-01, UC-02, UC-12		
Description		
The onboard systems (vehicle) shall be able to inform the User about urgent and dangerous events (hazards), and less urgent, less critical circumstances (weak connectivity to the service, changes in ETA, range problems due to traffic jam, rerouting due to changed traffic situation, etc.).		
Means of Verification		
The User receives urgent warnings and information from the system and is able to understand it. He can see (visual) and hear (audible) the warnings. The sensor impression and sequence matches the detailed usability concept. (Note: The detailed usability concept is beyond the definition of the requirement, but the requirement recommends defining such a usability concept.)		

6 THE ARCHITECTURE

The architecture is the main result of the process conducted in work package 1 in iKoPA. The following chapter describes the architecture in detail including the components, interfaces and communication concepts. Chapter 6.1 presents an overview about the high-level architecture. Chapter 6.2 describes in abstract detail of the planes, interfaces and systems included in the architecture. Finally, chapter 6.3 describes important components and concepts in more depth and is therefore important for the concrete realization of the components and interfaces in context of a real-world realization.

6.1 Overview “High level”

The following diagram represents the high-level view on the iKoPA architecture.

The basic structure and concepts for the iKoPA architecture are based on the CONVERGE architecture. In the high-level view, many components and interfaces are the same or based on CONVERGE. Therefore, some similarities exist and are intended.

The architecture consists of four planes:

- Government: All high-level security and administrative management functions are located in the government plane.
- Backend: The Service Providers and the service management function are the main parts of the backend plane. In addition, operational management and security components are present.
- Communication Network: The access technologies and the message distribution systems are part of the communication network plane. The plane also includes system parts for services integrated in the communication networks.
- Remote Stations: All mobile stations (e.g. smartphone, vehicle) and infrastructure stations (e.g. charging station, traffic light), which are endpoint for a communication.

The planes, the components and the interfaces are described in more detail in the following sections.

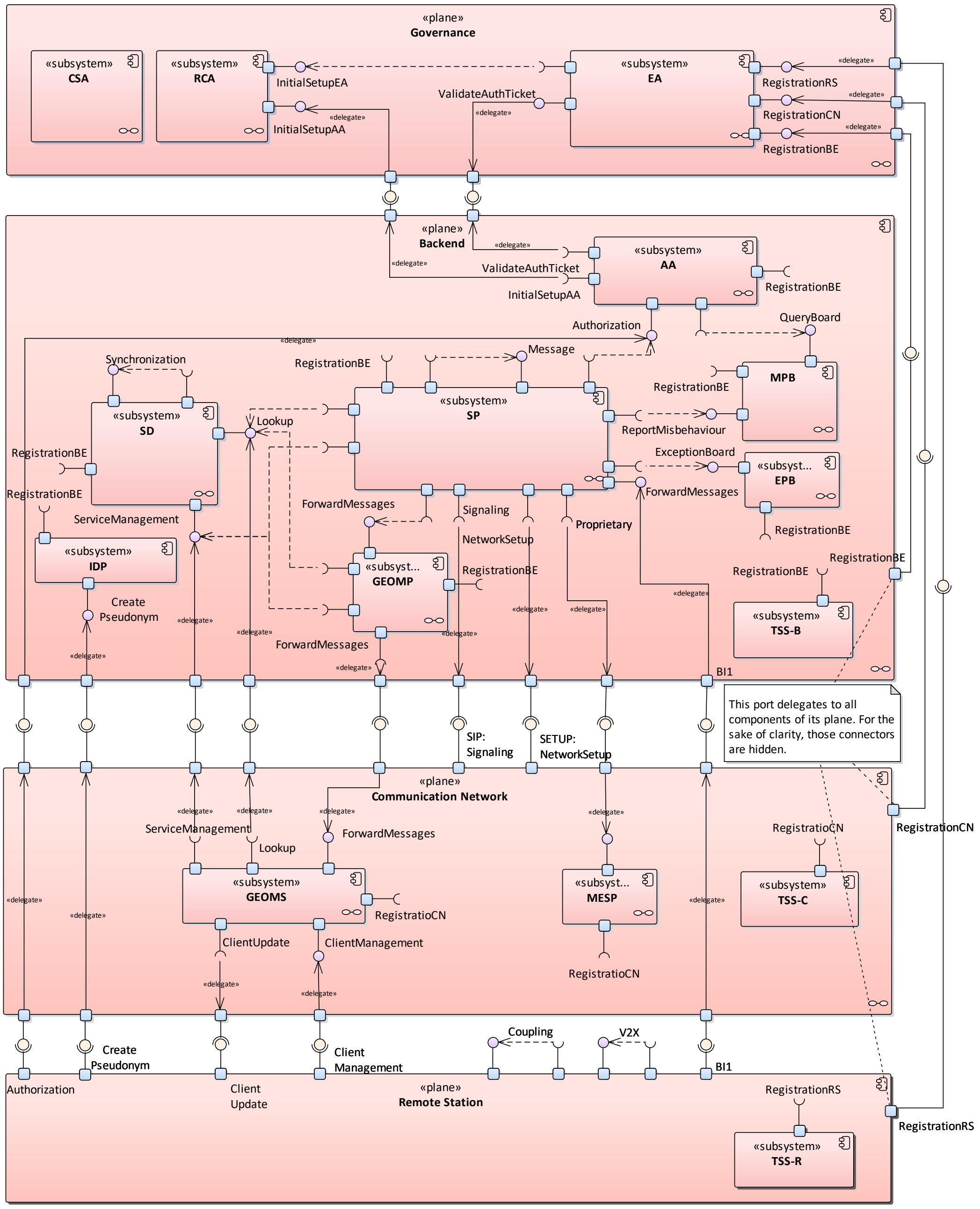


Figure 55: iKoPA high-level architecture

6.2 Components & Interfaces

In this chapter, all components of the high-level architecture will be described and grouped in planes. For every component a diagram, a description and the interfaces provided and used are described.

6.2.1 Governance plane

The governance plane consists of all legal, financial, and contractual components necessary to keep the system running from a management point of view. This also includes the Root Certification Authority and the Enrolment.

6.2.1.1 Contract Supervision Authority (CSA)

The CSA is a body that is taking care and controls the compliance of all participants (ITS-S and C-ITS services) of the network and the involvement of those participants to the overall agreements. Additionally, an entity can serve as a single point of contact for a data subject regarding data protection topics. This can be necessary, if different Service Providers have to be considered joint controllers because they jointly determine the purposes and means of data processing, Art. 26 of the General Data Protection Regulation. In such cases, the joint controllers have to find an arrangement to determine their respective data protection responsibilities. Joint controllership can be confusing for the data subject. To make it easier for a data subject to exercise his or her rights, the arrangement can designate a contact point. The CSA could serve as such a contact point. Another instrument of the General Data Protection Regulation might require a mediator between Service Providers, namely the right to data portability of Article 20 of the General Data Protection Regulation. The right to data portability allows the data subject under certain circumstances to request a Service Provider to transfer his personal data to a different Service Provider. To fulfil these requests, the Service Providers will have to agree on data formats that can be processed by all Service Providers to which the data subject might want his data to be transferred. This can lead to conflicts, where a mediating entity might be helpful.

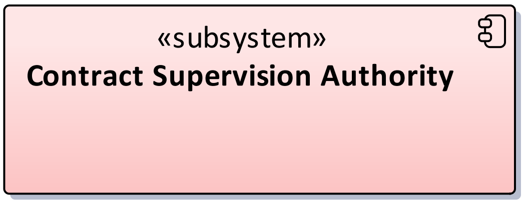


Figure 56: Contract Supervision Authority

6.2.1.2 Enrolment Authority (EA)

An EA is responsible for issuing Enrolment Credentials (EC) to ITS-S. There are different kinds of EA, which issues ECs:

- To remote stations, will be operated by the respective equipment manufacturers.
- To ITS Roadside Stations (IRS) that will be operated by the IRS manufacturer.
- To Service Providers.

The EA has to ensure that all of its clients operate within the specified security policy.

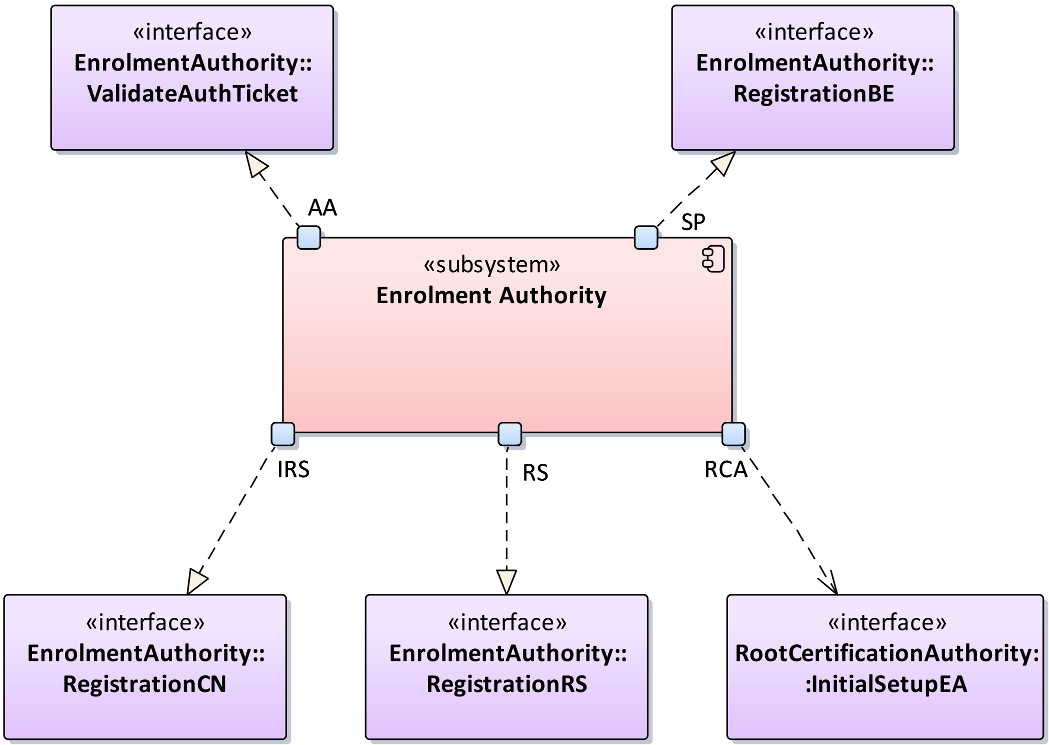


Figure 57: Enrolment Authority

6.2.1.2.1 Interfaces provided

RegistrationCN

This interface connects the communication network entities (ITS Roadside Station (IRS), MESP, etc.) to the Enrolment Authority (EA). It is used in the registration process of new network entities joining the network.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from IRS to RegistrationCN

[Direction is 'Source -> Destination'.]

RegistrationBE

This interface connects the backend systems (Service Provider (SP), Service Directory, etc.) to the Enrolment Authority (EA). It is used in the registration process of new backend entities joining the network.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from SP to RegistrationBE

[Direction is 'Source -> Destination'.]

RegistrationRS

This interface connects the remote stations (ITS Vehicle Station (IVS), smart phone, charging station, etc.) to the Enrolment Authority (EA). It is used in the registration process of new remote stations joining the network.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from RS to RegistrationRS

[Direction is 'Source -> Destination'.]

ValidateAuthTicket

This interface connects the Authorization Authority to the Enrolment Authority. It is required to validate Authorization Ticket request from ITS-S.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from AA to ValidateAuthTicket

[Direction is 'Source -> Destination'.]

6.2.1.2.2 Interfaces used

InitialSetupEA

This interface is used for the initial set-up of the Enrolment Authority (EA) credentials. Any valid EA will get an EA-Certificate from the Root Certification Authority (RCA).

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from EA to InitialSetupEA

[Direction is 'Source -> Destination'.]

6.2.1.3 Root CA (RCA)

A Public-Key-Infrastructure (PKI) will be implemented for the trustful exchange of information between participants within the network. Root CA, Enrolment Authority and Authorization Authority realize the PKI in the form of different Certification Authorities (CA). The RCA is the trust anchor for all digital certificates. The task of the RCA is to issue certificates to the subsequent CAs if they follow the agreed security policies. The RCA must be authorized and able to audit the subsequent CAs. There can and will be more than one RCA. The RCA will have to trust each other ("cross-certification").

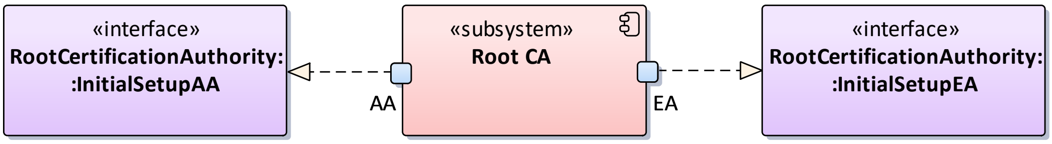

«interface»
RootCertificationAuthority::InitialSetupAA
«subsystem»
Root CA
AA
EA
«interface»
RootCertificationAuthority::InitialSetupEA

Figure 58: Root CA

6.2.1.3.1 Interfaces provided

InitialSetupAA

This interface is used for initial set up of the Authorization Authority (AA) credentials. Any AA that is acting according to the rules of the general network and that is trusted by the RCA will get an AA-Certificate from the Root Certification Authority (RCA).

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from AA to InitialSetupAA

[Direction is 'Source -> Destination'.]

InitialSetupEA

The interface is used for initial set-up of the Enrolment Authority (EA) credentials. Any valid EA will get an EA-Certificate from the Root Certification Authority (RCA).

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from EA to InitialSetupEA

[Direction is 'Source -> Destination'.]

6.2.1.3.2 Interfaces used

None

6.2.2 Backend Plane

The Backend Plane consists of the Service Providers and the technical components for the communication between the Service Providers themselves and between the Service Providers and the service users using the communication networks. Furthermore, several security components are included in this block.

6.2.2.1 Authorization Authority (AA)

An Authorization Authority (AA) is responsible of issuing Authorization Tickets (AT) to system participants. There are different kinds of AAs involved:

- Service Provider AA: For service specific usage.
- Network AA: The communication network operator probably operates this one. These do not have to be pseudonymous and frequently changed.
- Remote stations AA: For mobile user/equipment AT have to be issued by a Pseudonym CA (PCA). The term for AT is called Pseudonym Certificate (PC), because of the pseudonymous nature of this certificate. These AT should only be used a short time. For the traffic infrastructure equipment, the ATs do not have to be pseudonymous and do not have to be changed as often as PCs.

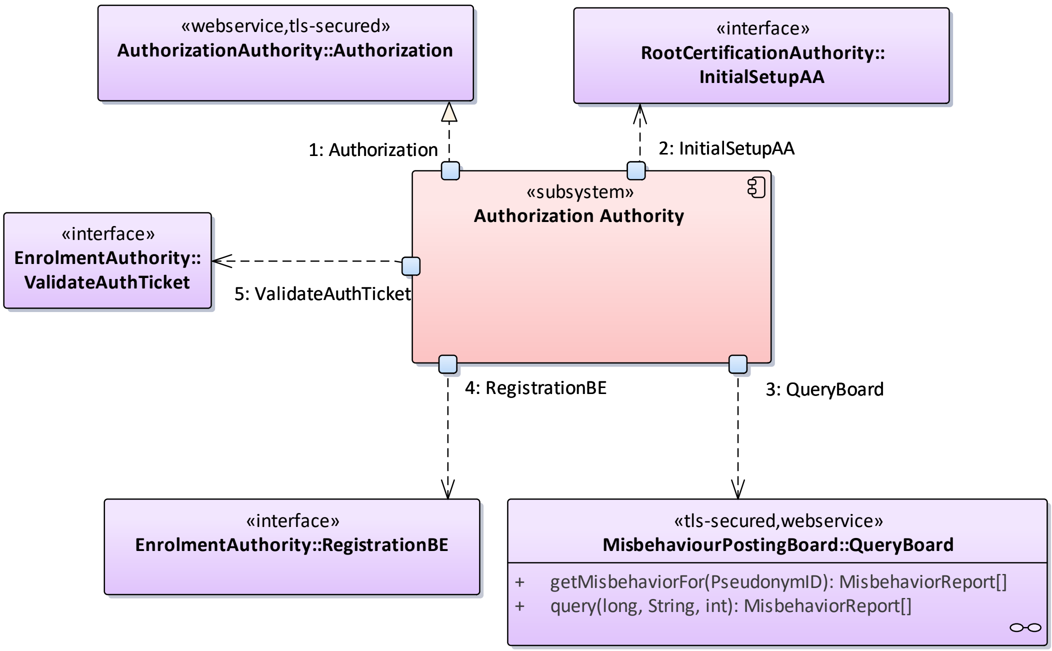


Figure 59: Authorization Authority

Like the RCA the AA can and should be implemented not only once but many times so that no single point of knowledge or failure exist.

6.2.2.1.1 Interfaces provided

Authorization

This interface connects a Service Provider (SP) to the Authorization Authority (AA). It is used in the recurring process of authorization.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 1 to «webservice» Authorization

[Direction is 'Source -> Destination'.]

6.2.2.1.2 Interfaces used

InitialSetupAA

This interface is used for initial set-up of the Authorization Authority (AA) credentials. Any AA that is acting according to the rules of the network and that is trusted by the RCA will get an AA-Certificate from the Root Certification Authority (RCA).The Information exchanged would typically at least include: AA Public Key, RCA issued AA-Certificate.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from AA to InitialSetupAA

[Direction is 'Source -> Destination'.]

QueryBoard

The QueryBoard interface allows querying the posting board to obtain information of misbehaving entities. The MPB returns the list of collected misbehavior entries that fit the request. Each entry in the list contains the information that was previously posted by the misbehavior reporter, i.e. the misbehavior record. Alternatively, the MPB rejects the query (e.g. if the requestor is not authorized).

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 2 to «tls-secured» QueryBoard

[Direction is 'Source -> Destination'.]

RegistrationBE

This interface is used in the registration process of a new Authorization Authority to obtain its initial credentials. The initial credentials are necessary for any communication whatsoever.

INCOMING STRUCTURAL RELATIONSHIPS
⇒ Realization from SP to RegistrationBE [Direction is 'Source -> Destination'.]

ValidateAuthTicket

This interface connects the Authorization Authority to the Enrolment Authority. It is required to validate Authorization Ticket request from ITS-S. Information exchanged would typically at least include: encrypted binary large object (blob) including a signature over the AT Keys and the EC-Identity, a hash over the AT Keys.

INCOMING STRUCTURAL RELATIONSHIPS
⇒ Realization from AA to ValidateAuthTicket [Direction is 'Source -> Destination'.]

6.2.2.2 Exception Posting Board (EPB)

The EPB informs other entities of the network whenever an irregular condition (service unavailability, service deletion etc.) has been reported by a Service Provider. Each Service Provider will report such exceptional conditions for its own services, so its Service Consumers are informed. The Communication Networks will also inform the Exception Posting Board when an exception regarding network functionality occurs. The EPB will perform the necessary steps to inform affected entities and solve the issue.

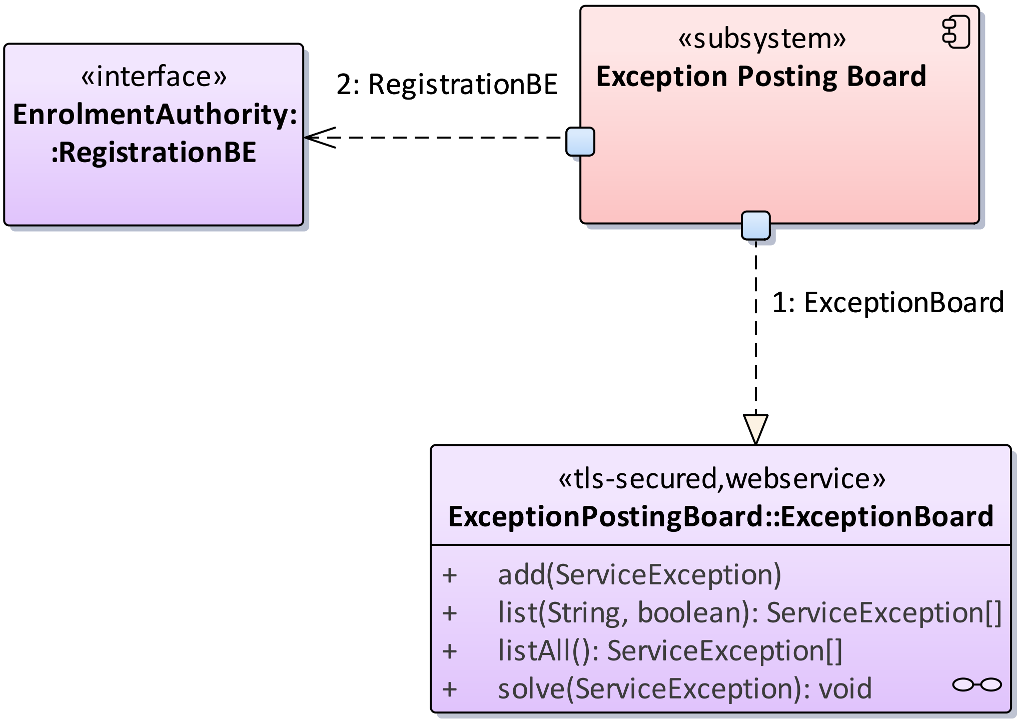

«interface»
EnrolmentAuthority::RegistrationBE
2: RegistrationBE
«subsystem»
Exception Posting Board
1: ExceptionBoard
«tls-secured,webservice»
ExceptionPostingBoard::ExceptionBoard
+ add(ServiceException)
+ list(String, boolean): ServiceException[]
+ listAll(): ServiceException[]
+ solve(ServiceException): void

Figure 60: Exception Posting Board

6.2.2.2.1 Interfaces provided

ExceptionBoard

This interface allows a Service Provider to inform other participants of the network whenever an irregular condition (service unavailability, service deletion etc.) with respect to its own services has occurred.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 1 to «tls-secured» ExceptionBoard

[Direction is 'Source -> Destination'.]

OPERATIONS

◆ add (exception : ServiceException) : Public

Adds a new exception to the board.

OPERATIONS
list (serviceURL : String , inactive : boolean) : ServiceException[] Public Returns all active (=not solved) exceptions associated with the given service.
listAll () : ServiceException[] Public Returns all exceptions currently active (= not solved) exceptions in the board.
solve (exception : ServiceException) : void Public Marks a previously posted exception as solved.

6.2.2.2.2 Interfaces used

RegistrationBE

This interface connects the Exception Posting Board (EPB) to the Enrolment Authority (EA). New EPBS joining the network use this interface during their enrolment process.

INCOMING STRUCTURAL RELATIONSHIPS
Realization from SP to RegistrationBE [Direction is 'Source -> Destination'.]

6.2.2.3 Geomessaging Proxy (GEOM-P)

The GEOM-P is the part of the geomessaging concept that is located in the backend. This is the major entry point for delivery of geomessaging data from the perspective of a C-ITS service. Through the ServiceDirectory, the GeomessagingProxy will obtain a list of GeoMessagingServers offering services for a specific geographic area. In turn, the GeomessagingProxy will offer its services to interested ServiceProviders through the ServiceDirectory including the aggregated area of coverage of the GeoMessagingServers it is connected with. The GeomessagingProxy will connect to one or many GeoMessagingServers, which take over the task to finally distribute the geomessages via different communication networks to the respective geographical areas.

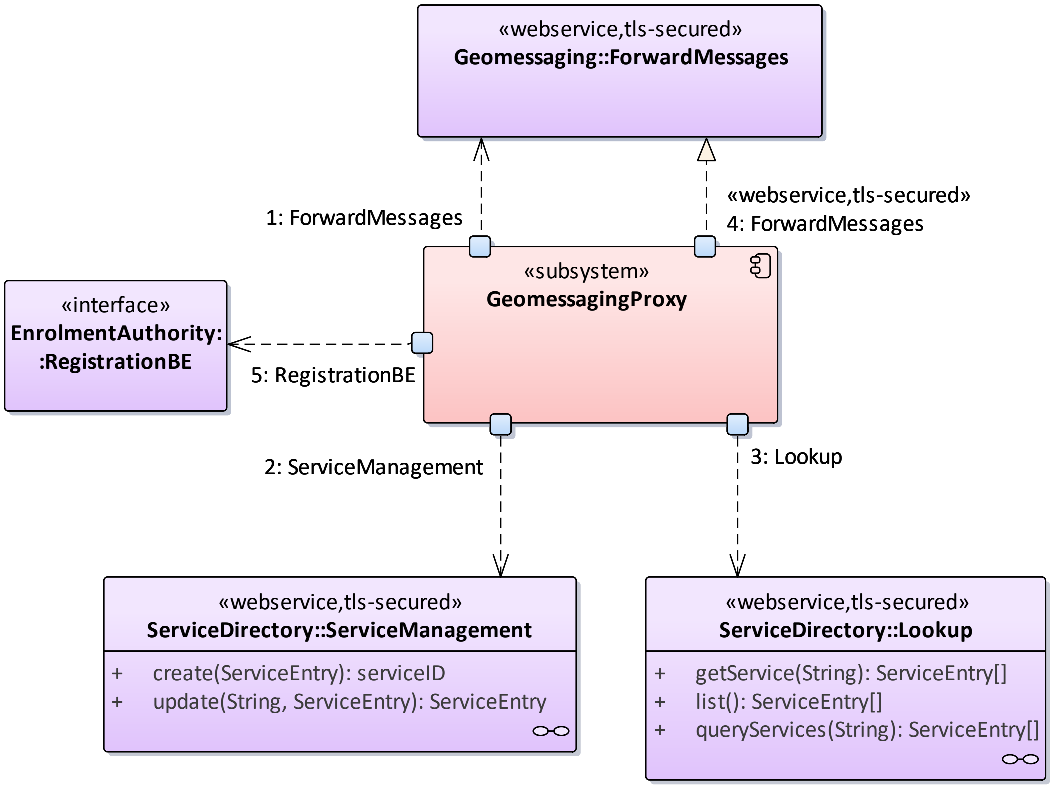


Figure 61: GeomessagingProxy

6.2.2.3.1 Interfaces provided

ForwardMessages

This interface provides the possibility for Service Providers to deliver messages to mobile terminals based on their geographical location, their attributes, or based on specific topics via the channels a Bridge provides.

Moreover, this interface provides the possibility for Geo Messaging Proxy GEOM-P services to forward messages received from Service Providers to the Bridges, which reside either in the domain of a MNO or in the domain of an IRS network. Geo Messaging Proxy GEOM-P nodes are able to register and subscribe to Bridges, using this interface.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from «webservice» 4 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from GEOM to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]

6.2.2.3.2 Interfaces used

RegistrationBE

This interface connects the Geomessaging Proxy (GEOM-P) to the Enrolment Authority (EA). It is used in the registration process of new GEOM-P joining the network.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SP to RegistrationBE [Direction is 'Source -> Destination'.]

Lookup

This service allows querying of Geomessaging Servers in the service directory based on a set of criteria.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» Lookup [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» Lookup [Direction is 'Source -> Destination'.]

ServiceManagement

This interface provides mechanisms for service management by GEOM-P, e.g. service registration, deregistration and updates.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from 2 to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]

ForwardMessages

This interface provides the possibility for Geo Messaging Proxy GEOM-P services to forward messages received from Service Providers to the Bridges, which either reside in the domain of a MNO, DAB+ or in the domain of an IRS network. Geo Messaging Proxy nodes are able to register and subscribe to Bridges, using this interface.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from «webservice» 4 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from GEOM to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]

6.2.2.4 Identity Provider (IDP)

Identity Providers manage the active users of the iKoPA system. The intent is to provide a federated approach for service providers to authenticate users (and optionally exchange user data), akin to the mechanisms provided, for example, by the OAUTH protocoll [RFC6749] or OpenID Connect.
The concept defines three roles:

- The end-user (similar to the /resource owner/ in OAUTH)
- The service provider (similar to the /client/ in OAUTH)
- The identity provider (/authorization server/ in OAUTH)

The end-user is the party which is to be authenticated or identified by the service providers. Upon successful authentication, the service providers provide some form of service to end-user, for example, a parking reservation. The identity provider serves as a trusted third party to facilitate the actual authentication between these two parties.
A precondition of an authentication sequence is that the end-user is known to an identity provider and is able to authenticate and identify himself to the identity provider. This may happen via conventional means, for example, with a username/password.
The authentication sequence between user and service provider also varies depending on the underlying authentication mechanism used by the identity provider. Here we define

two variants based on single-use pseudonym credentials and direct anonymous attestation (DAA).

An authentication sequence in the case of single-use pseudonym credential then proceeds as follows:

1. The end-user authenticates with the identity provider.
2. End-user and identity provider interactively create a pseudonym credential, for example, a private/public key pair and a certificate.
3. The end-user then uses these pseudonym credentials to authenticate with the service provider with an interactive protocol.
4. The service provider can validate these pseudonym credential, for example, by checking the certificate of the credential against a known public-key of the identity provider.

The pseudonym credentials are intended to have a short live-time / validity, which likely makes a mechanism for checking for revocation unnecessary.

In the case of DAA, the end-user created a set of long-term credentials suitable for DAA. This dispenses the need for step 1 and 2 described above, however the service provider would require some form of backchannel to the identity provider to enable the service provider to check whether this long-term credential was revoked.

An extension of this concept may also introduce a fourth role, similar to the “resource provider” in the context of OAUTH. These could provide necessary resources to the service providers, such as payment information or other necessary user data. The user would then interactively create authorization tokens with the identity providers.

These tokens could then be given to the service provider, which it then in turn can use to retrieve information from the resource providers.

Hint: in the Use Cases and some of the requirement this component is called registration service.

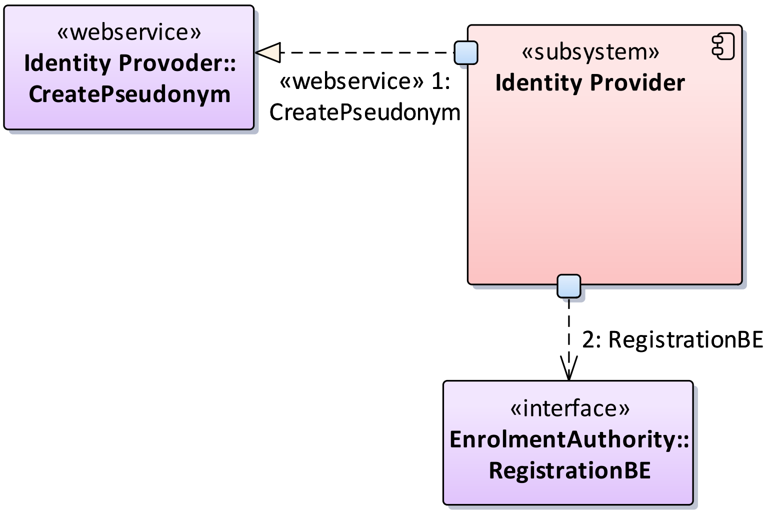


Figure 62: Identity Provider

6.2.2.4.1 Interfaces provided

CreatePseudonym

This interface connects the smartphone to the identity provider. It is used to create a pseudonym for a user within the iKoPA system.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from «webservice» 1 to «webservice» CreatePseudonym [Direction is 'Source -> Destination'.]

6.2.2.4.2 Interfaces used

RegistrationBE

This interface is used in the registration process of a new identity provider to obtain its initial credentials

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SP to RegistrationBE [Direction is 'Source -> Destination'.]

6.2.2.5 Misbehavior Posting Board (MPB)

Suspected misbehavior of any kind, detected by participants of the network will be reported to the Misbehavior Posting Board (MPB). Reports of supposed misbehavior are aggregated by the pseudonyms of both, reporting and suspected misbehaving entities, as well as their location and possibly other factors, but only those factors that are necessary to take countermeasures. In a second step, this information is used to trigger an appropriate countermeasure in order to mitigate or stop the misbehavior. The MPB itself does not perform such countermeasures, as it only provides a place for aggregated misbehavior reports. Different MPB must exchange the information so that every MPB has the same knowledge about the relevant misbehaviors. There could also exist local MPBs in different network for information that is only locally relevant.

The BPB is not able to lift the pseudonym and propose any countermeasures for any real word user. It can only provide the information that one pseudonym has misbehaved. To get the real identity of a user different service providers (e.g. REGS, RCA) have to combine shard knowledge. This is only allowed if a juridical institution (judge, Court, …) has ordered this.

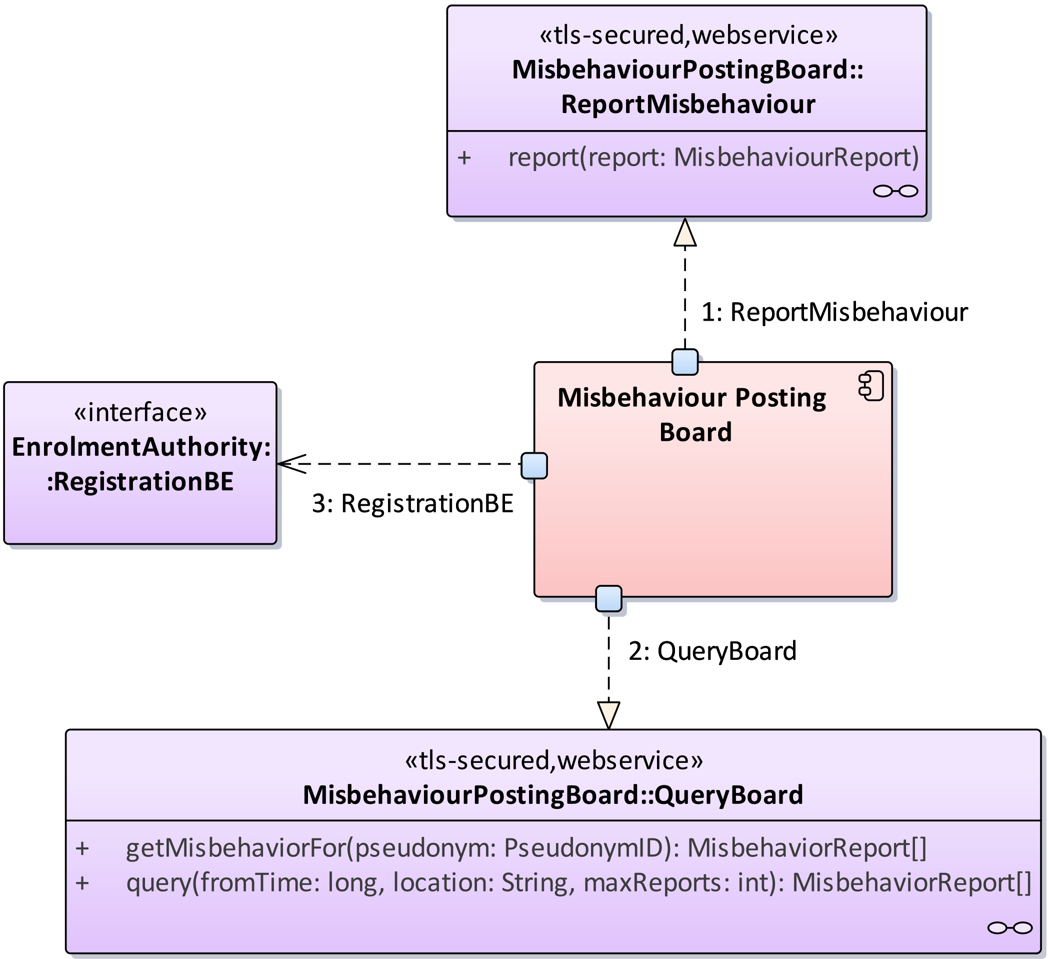

«tls-secured,webservice»
MisbehaviourPostingBoard::
ReportMisbehaviour
+ report(report: MisbehaviourReport)
1: ReportMisbehaviour
Misbehaviour Posting Board
«interface»
EnrolmentAuthority:
:RegistrationBE
3: RegistrationBE
2: QueryBoard
«tls-secured,webservice»
MisbehaviourPostingBoard::QueryBoard
+ getMisbehaviorFor(pseudonym: PseudonymID): MisbehaviorReport[]
+ query(fromTime: long, location: String, maxReports: int): MisbehaviorReport[]

Figure 63: Misbehavior Posting Board

6.2.2.5.1 Interfaces provided

QueryBoard

The QueryBoard interface allows querying the posting board to obtain reports of misbehaving entities.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from 2 to «tls-secured» QueryBoard [Direction is 'Source -> Destination'.]

OPERATIONS

getMisbehaviorFor (pseudonym : PseudonymID) : MisbehaviorReport[] Public

Returns all reports reported for a given pseudonym.

query (fromTime : long , location : String , maxReports : int) : MisbehaviorReport[] Public

Query the board for entries, which match the given parameters.

ReportMisbehavior

A MBP-client is able to post information about observed misbehavior to the MBP via this interface.

INCOMING STRUCTURAL RELATIONSHIPS

Realization from 1 to «tls-secured» ReportMisbehaviour

[Direction is 'Source -> Destination'.]

OPERATIONS

report (report : MisbehaviourReport) : Public

Submit the given report to the posting board.

6.2.2.5.2 Interfaces used

RegistrationBE

This interface is used in the registration process of a new Misbehavior Posting Board to obtain its initial credentials.

INCOMING STRUCTURAL RELATIONSHIPS

Realization from SP to RegistrationBE

[Direction is 'Source -> Destination'.]

6.2.2.6 Reservation Service (RESS)

The reservation service manages the occupation of the available charging as well as parking lots. Therefore, it is connected with the charger and the local parking system at the different car parks. In order to make reservation the reservation service provides suitable interfaces e.g. to the HMI.

The request and conformation are separated because of the asynchronous communication. In the real word this can be implemented as one interface but logically this is distributed. The user requests a reservation and gets an indication back. This indication can be used to confirm the reservation. The reservation server forwards the request to the car park. The car park confirms the reservation due to the current schedule and the current occupancy of the requested parking lot.

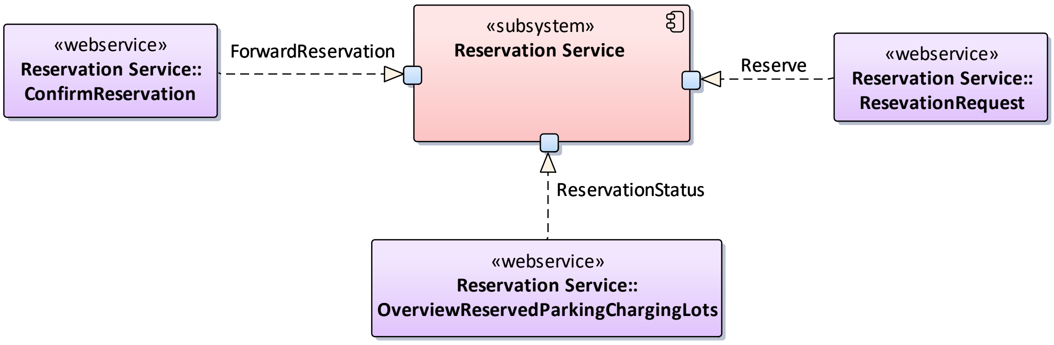


Figure 64: Reservation Service

6.2.2.6.1 Interfaces provided

ConfirmReservation

With this interface the reservation services confirms a reservation request. The interface can also be used to confirm a desired time slot at the charger the other way round. It is also used for e.g. an car park to confirm the validity of an reservation ticket.

OUTGOING STRUCTURAL RELATIONSHIPS

Realization from «webservice» ConfirmReservation to ForwardReservation

[Direction is 'Source -> Destination'.]

OverviewReservedParkingChargingLots

This interface provides the occupancy status of available parking and charging lots at the moment as well as within the next 24 hours.

OUTGOING STRUCTURAL RELATIONSHIPS
Realization from «webservice» OverviewReservedParkingChargingLots to ReservationStatus [Direction is 'Source -> Destination'.]

ResevationRequest

With the help of this interface, the booking of parking/charging lots can be requested. It is possible to make reservations for time slots up to 24 hours in prior or to check the current availability. Especially for the charging lots further information like the required charging plug space for the car have to be defined. The result is an reservation information indication.

OUTGOING STRUCTURAL RELATIONSHIPS
Realization from «webservice» ResevationRequest to Reserve [Direction is 'Source -> Destination'.]

6.2.2.6.2 Interfaces used

None

6.2.2.7 Service Directory (SD)

The Service Directory provides an overview of the entities available in the network. These entities are mainly services, communication networks, Geomessaging-Servers and other SD instances. Special extensions will feature specific concepts of certain technologies, like DAB and TPEG, to include them fully into the Service Directory concept.

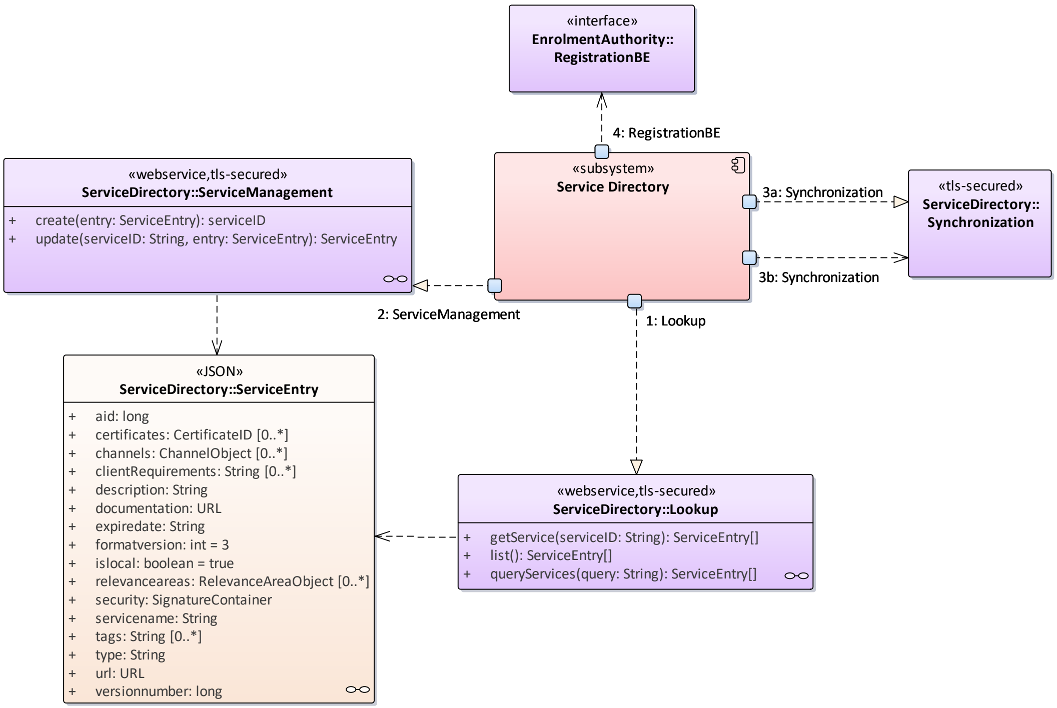


Figure 65: Service Directory

6.2.2.7.1 Interfaces provided

Lookup

This service allows querying of the service entries in the service directory based on a - still to be defined - set of criteria.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» Lookup [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» Lookup [Direction is 'Source -> Destination'.]

OPERATIONS
◆ getService (serviceID : String) : ServiceEntry[] Public Query the directory for a service with given ID, which also matches the query.

OPERATIONS

list () : ServiceEntry[] Public

Lists the whole directory.

queryServices (query : String) : ServiceEntry[] Public

Query the directory for a service, which matches the query.

ServiceManagement

This interface provides mechanisms for service management by Service Providers, e.g. service registration, deregistration and updates.

INCOMING STRUCTURAL RELATIONSHIPS

Realization from SD to «webservice» ServiceManagement

[Direction is 'Source -> Destination'.]

Realization from 2 to «webservice» ServiceManagement

[Direction is 'Source -> Destination'.]

OPERATIONS

create (entry : ServiceEntry) : serviceID Public

Create a new service entry.

update (serviceID : String , entry : ServiceEntry) : ServiceEntry Public

Updates the given service entry and returns the old entry.
Only allowed for service owner.

Synchronization

This interface is used by Service Directory instances to share information of its entries. It allows one SD to inform another SD of new services, requests information of services or communicate a change of a service.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 3a to «tls-secured» Synchronization

[Direction is 'Source -> Destination'.]

6.2.2.7.2 Interfaces used

RegistrationBE

This interface is used in the registration process of a new Service Directory entity to obtain its initial credentials.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from SP to RegistrationBE

[Direction is 'Source -> Destination'.]

Synchronization

This interface is used by Service Directory instances to share information of its entries. It allows one SD to inform another SD of new services, requests information of services or communicate changes of a service.

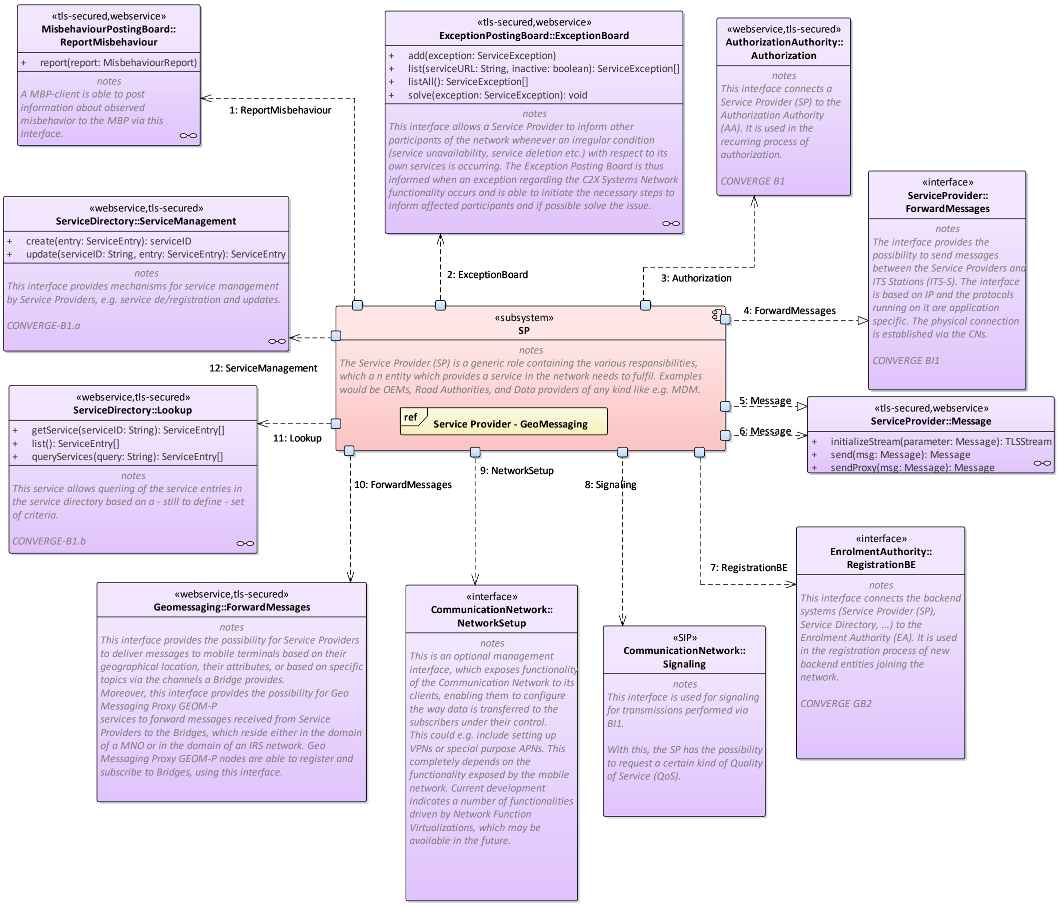
INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 3a to «tls-secured» Synchronization

[Direction is 'Source -> Destination'.]

6.2.2.8 Service Provider (SP)

The Service Provider (SP) is a generic role. It represents the responsibilities, which a service providing entity in the network needs to fulfil. Examples of such an entity can be found in section 6.3.3.


«tls-secured,webservice»
MisbehaviourPostingBoard::
ReportMisbehaviour
+ report(report: MisbehaviourReport)
notes

A MBP-client is able to post information about observed misbehavior to the MBP via this interface.

«tls-secured,webservice»
ExceptionPostingBoard::ExceptionBoard
+ add(exception: ServiceException)
+ list(serviceURL: String, inactive: boolean): ServiceException[]
+ listAll(): ServiceException[]
+ solve(exception: ServiceException): void
notes

This interface allows a Service Provider to inform other participants of the network whenever an irregular condition (service unavailability, service deletion etc.) with respect to its own services is occurring. The Exception Posting Board is thus informed when an exception regarding the C2X Systems Network functionality occurs and is able to initiate the necessary steps to inform affected participants and if possible solve the issue.

This interface connects a Service Provider (SP) to the Authorization Authority (AA). It is used in the recurring process of authorization.

CONVERGE B1

The interface provides the possibility to send messages between the Service Providers and ITS Stations (ITS-S). The interface is based on IP and the protocols running on it are application specific. The physical connection is established via the CNs.

CONVERGE BI1

«webservice,tls-secured»
ServiceDirectory::ServiceManagement
+ create(entry: ServiceEntry): serviceID
+ update(serviceID: String, entry: ServiceEntry): ServiceEntry
notes

This interface provides mechanisms for service management by Service Providers, e.g. service de/registration and updates.

CONVERGE-B1.a

The Service Provider (SP) is a generic role containing the various responsibilities, which a n entity which provides a service in the network needs to fulfil. Examples would be OEMs, Road Authorities, and Data providers of any kind like e.g. MDM.

This service allows queriing of the service entries in the service directory based on a - still to define - set of criteria.

CONVERGE-B1.b

«tls-secured,webservice»
ServiceProvider::Message
+ initializeStream(parameter: Message): TLSStream
+ send(msg: Message): Message
+ sendProxy(msg: Message): Message
«interface»
EnrolmentAuthority::
RegistrationBE
notes

This interface connects the backend systems (Service Provider (SP), Service Directory, ...) to the Enrolment Authority (EA). It is used in the registration process of new backend entities joining the network.

CONVERGE GB2

This interface provides the possibility for Service Providers to deliver messages to mobile terminals based on their geographical location, their attributes, or based on specific topics via the channels a Bridge provides.
Moreover, this interface provides the possibility for Geo Messaging Proxy GEOM-P
services to forward messages received from Service Providers to the Bridges, which reside either in the domain of a MNO or in the domain of an IRS network. Geo Messaging Proxy GEOM-P nodes are able to register and subscribe to Bridges, using this interface.

This is an optional management interface, which exposes functionality of the Communication Network to its clients, enabling them to configure the way data is transferred to the subscribers under their control.
This could e.g. include setting up VPNs or special purpose APNs. This completely depends on the functionality exposed by the mobile network. Current development indicates a number of functionalities driven by Network Function Virtualizations, which may be available in the future.

This interface is used for signaling for transmissions performed via BI1.

With this, the SP has the possibility to request a certain kind of Quality of Service (QoS).

Figure 66: Service Provider

6.2.2.8.1 Interfaces provided

ForwardMessages

This interface provides the possibility to send messages between the Service Providers and ITS Stations (ITS-S). The interface is based on IP and the protocols running on it are application specific. The physical connection is established via the CNs.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from 4 to ForwardMessages [Direction is 'Source -> Destination'.]

Message

This interface is used by various SP instances to communicate in a messages based way, analogues to packet-based data, e.g. like UDP.

INCOMING STRUCTURAL RELATIONSHIPS

Realization from 5 to «tls-secured» Message

[Direction is 'Source -> Destination'.]

Realization from 5 to «tls-secured» Message

[Direction is 'Source -> Destination'.]

OPERATIONS

initializeStream (parameter : Message) : TLSStream Public

Use by a SP to initialize a, TLS-secured, stream connection between him and another SP.

send (msg : Message) : Message Public

Used to send a message to a SP.

sendProxy (msg : Message) : Message Public

Send a message to a SP which should be delivered to another SP, e.g. as it is acting as a bridge.

6.2.2.8.2 Interfaces used

NetworkSetup

This is an optional interface, which may be used to configure the way data is transferred in the communication networks. For example, this could include the setup of the network. The functionality of this interface purely depends on the functionality exposed by the network.

INCOMING STRUCTURAL RELATIONSHIPS

Realization from SETUP to NetworkSetup

[Direction is 'Source -> Destination'.]

Signaling

This interface is used to signal the transmissions performed via the communication networks. A SP or other users of the network, has the possibility to request a certain Quality of Service (QoS).

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from SIP to «SIP» Signaling

[Direction is 'Source -> Destination'.]

ReportMisbehaviour

This interface is used to report a detected misbehavior to the MBP.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 1 to «tls-secured» ReportMisbehaviour

[Direction is 'Source -> Destination'.]

RegistrationBE

This interface is used in the registration process of a new Service Provider to obtain its initial credentials.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from SP to RegistrationBE

[Direction is 'Source -> Destination'.]

Authorization

This interface connects a Service Provider (SP) to the Authorization Authority (AA). It is used in the recurring process of authorization, primarily to obtain the short-term pseudonym tickets.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 1 to «webservice» Authorization

[Direction is 'Source -> Destination'.]

Lookup

This service allows querying of the service entries in the service directory based on a set of criteria. It may be used by an SP instance to find other SP’s. This is especially useful for providing ‘composition Service Providers’ which combine two or more services to provide a new service.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» Lookup [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» Lookup [Direction is 'Source -> Destination'.]

ServiceManagement

This interface provides mechanisms for service management by Service Providers, e.g. service de/registration and updates. It is used by the various SP instances to make sure the directory reflects the state of the SP.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]
⇨ Realization from 2 to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]

ForwardMessages

This interface provides the possibility for Service Providers to deliver messages to mobile terminals based on their geographical location, their attributes, or based on specific topics via the channels a Geomessaging Server provides.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from «webservice» 4 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from GEOM to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]

ExceptionBoard

This interface allows a Service Provider to inform other participants of the network whenever an irregular condition (service unavailability, service deletion etc.) with respect to its own services is occurring. The Exception Posting Board is thus informed when an exception regarding the network functionality occurs and is able to initiate the necessary steps to inform affected participants and if possible solve the issue.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 1 to «tls-secured» ExceptionBoard

[Direction is 'Source -> Destination'.]

6.2.2.9 TimeSynchronization (TSS-B)

This is the Time synchronization Server for the backend services and server. All servers must be synchronous for security, registration, reservation and billing purposes.

6.2.2.9.1 Interfaces provided

None other than standard protocols like NTP.

6.2.2.9.2 Interfaces used

RegistrationBE

This interface connects the TimeSynchronization (TSS-B) to the Enrolment Authority (EA). It is used in the registration process of new TSS-B joining the network.

OUTGOING STRUCTURAL RELATIONSHIPS

⇦ Delegate from RegistrationBE to RegistrationBE

[Direction is 'Source -> Destination'.]

6.2.3 Communication Network plane

The Communication Network Plane provides the connectivity between services providers and service users. This includes for example geographically based information distribution.

6.2.3.1 Entities

The communication network in the iKoPA project is realized in four networks: RFID, DAB, IRS and cellular. The architecture explicitly allows adding new communication networks. The aforementioned networks and their interfaces are described in the next sections.

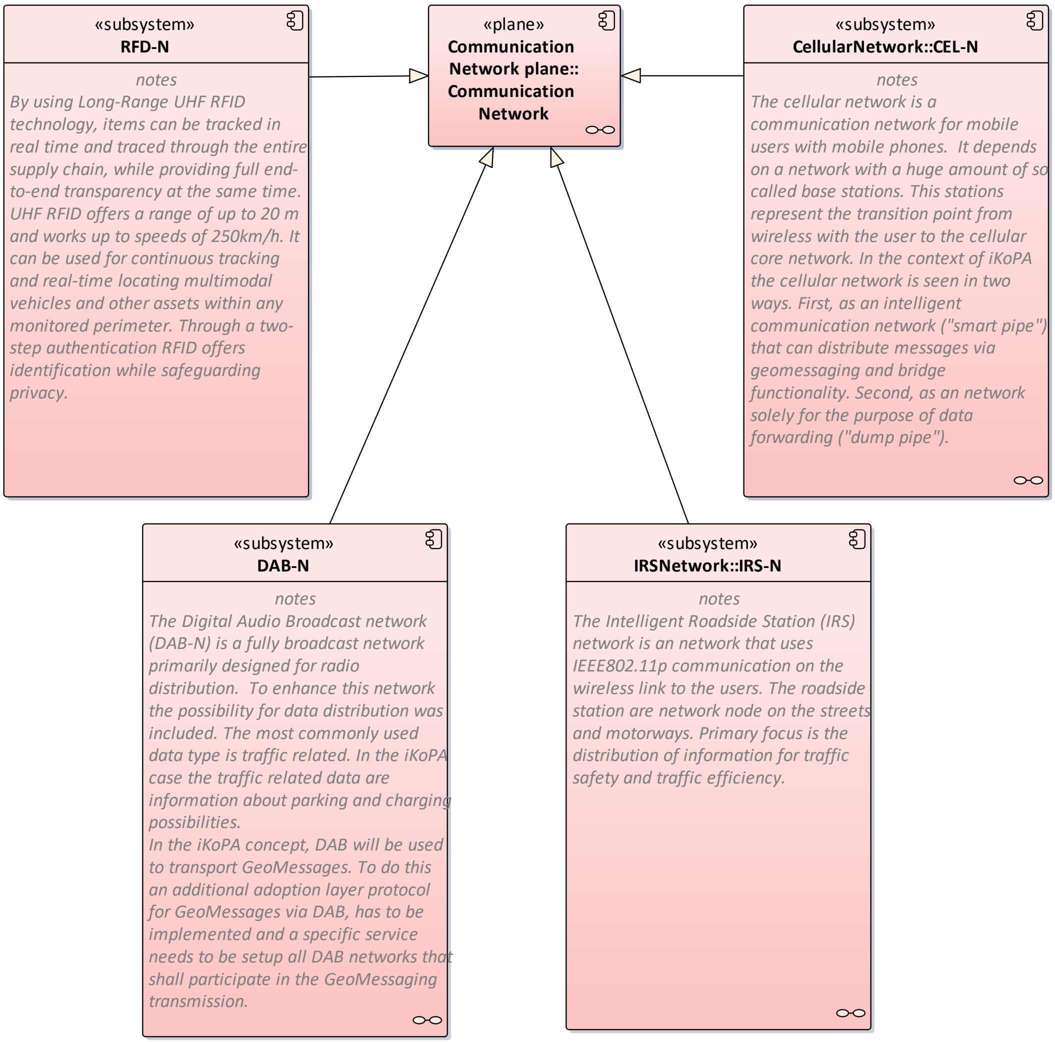

«subsystem»
RFD-N
notes
By using Long-Range UHF RFID technology, items can be tracked in real time and traced through the entire supply chain, while providing full end-to-end transparency at the same time. UHF RFID offers a range of up to 20 m and works up to speeds of 250km/h. It can be used for continuous tracking and real-time locating multimodal vehicles and other assets within any monitored perimeter. Through a two-step authentication RFID offers identification while safeguarding privacy.
«plane»
Communication Network plane:: Communication Network
«subsystem»
CellularNetwork::CEL-N
notes
The cellular network is a communication network for mobile users with mobile phones. It depends on a network with a huge amount of so called base stations. This stations represent the transition point from wireless with the user to the cellular core network. In the context of iKoPA the cellular network is seen in two ways. First, as an intelligent communication network ("smart pipe") that can distribute messages via geomessaging and bridge functionality. Second, as an network solely for the purpose of data forwarding ("dump pipe").
«subsystem»
DAB-N
notes
The Digital Audio Broadcast network (DAB-N) is a fully broadcast network primarily designed for radio distribution. To enhance this network the possibility for data distribution was included. The most commonly used data type is traffic related. In the iKoPA case the traffic related data are information about parking and charging possibilities.
In the iKoPA concept, DAB will be used to transport GeoMessages. To do this an additional adoption layer protocol for GeoMessages via DAB, has to be implemented and a specific service needs to be setup all DAB networks that shall participate in the GeoMessaging transmission.
«subsystem»
IRSNetwork::IRS-N
notes
The Intelligent Roadside Station (IRS) network is an network that uses IEEE802.11p communication on the wireless link to the users. The roadside station are network node on the streets and motorways. Primary focus is the distribution of information for traffic safety and traffic efficiency.

Figure 67: ComNet-Entities

6.2.3.1.1 Communication Network

The communication network is the generalized representation of the communication network plane. In the following subsections the interfaces of that plane are described.

INCOMING STRUCTURAL RELATIONSHIPS
➯ Generalization from «Subsystem» IRS Network to «plane» Communication Network [Direction is 'Source -> Destination'.]
➯ Generalization from «Subsystem» Cellular Network to «plane» Communication Network [Direction is 'Source -> Destination'.]

INCOMING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» DAB Network to «plane» Communication Network [Direction is 'Source -> Destination'.]
Generalization from «Subsystem» RFID to «plane» Communication Network [Direction is 'Source -> Destination'.]

6.2.3.1.1.1 Interfaces provided

NetworkSetup

This is an optional management interface, which exposes functionality of the Communication Network to its clients, enabling them to configure the way data is transferred to the subscribers under their control.

This could e.g. include setting up VPNs or special purpose APNs. This completely depends on the functionality exposed by the mobile network. Current development indicates a number of functionalities driven by Network Function Virtualizations, which may be available in the future.

INCOMING STRUCTURAL RELATIONSHIPS
Realization from SETUP to NetworkSetup [Direction is 'Source -> Destination'.]

Signaling

This interface is used to signal transmissions performed via SIP. With this, the SP has the possibility to request a certain kind of Quality of Service (QoS).

INCOMING STRUCTURAL RELATIONSHIPS
Realization from SIP to «SIP» Signaling [Direction is 'Source -> Destination'.]

ClientManagement

This interface is used to register and deregister clients of the GeomessagingServer. In addition, client send updates about their current position. In many cases, this does not have to be a precise position, but can also be a geographical area.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from GEOM to «webservice» ClientManagement [Direction is 'Source -> Destination'.]
⇨ Realization from «webservice» 5 to «webservice» ClientManagement [Direction is 'Source -> Destination'.]

6.2.3.1.1.2 Interfaces used

Lookup

This service allows querying of the service entries in the service directory based on a set of criteria. This is used by the networks to obtain entries of SP's or GEOM-P instances. Its use is mostly optional and it may be used to verify registration processes performed by the ServiceManagement interface.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» Lookup [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» Lookup [Direction is 'Source -> Destination'.]

ServiceManagement

This interface provides mechanisms for service management by Service Providers, e.g. service registration, deregistration and updates. This is used to propagate the existence of the network to Service Providers as well as the – possible – existence of the networks GEOM-instance to the various GOEM-P instances.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]
⇨ Realization from 2 to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]

ClientUpdate

This interface provides the mechanism to deliver a message to a remote station, i.e. the destination, over a cellular link. Furthermore, the mechanism to update the location and the service subscriptions of the remote station is specified here.

ForwardMessages

This interface provides the possibility for Service Providers to deliver messages to mobile terminals based on their geographical location, their attributes, or based on specific topics via the channels a Bridge provides.

Moreover, this interface provides the possibility for Geo Messaging Proxy GEOM-P services to forward messages received from Service Providers to the Bridges, which reside either in the domain of a MNO or in the domain of an IRS network. GEOM-P nodes are able to register and subscribe to Bridges, using this interface.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from «webservice» 4 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from GEOM to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]

ServiceManagement

This interface provides mechanisms for service management by Service Providers, e.g. service registration, deregistration and updates. This is used to propagate the existence of the network to Service Providers as well as the – possible – existence of the networks GEOM-instance to the various GOEM-P instances.

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Delegate from ServiceManagement to SD [Direction is 'Source -> Destination'.]

RegistrationCN

This interface is used in the registration process of a new communication network to obtain its initial credentials.

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Delegate from RegistrationCN to EA/IRS [Direction is 'Source -> Destination'.]

6.2.3.1.2 CellularNetwork (CEL-N)

The cellular network is a communication network for mobile users with mobile phones. It depends on a network with a huge amount of so-called base stations. These stations are the transition point for wireless communication with the user to the cellular core network. In the context of iKoPA the cellular network is seen in two ways. First, it is seen as an intelligent communication network ("smart pipe") that can distribute messages via geomessaging and bridge functionality. Second, it is seen as a network solely for the purpose of data forwarding ("dump pipe").

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from «Subsystem» Cellular Network to «plane» Communication Network [Direction is 'Source -> Destination'.]

6.2.3.1.2.1 Components

The following section describes the components inside a CEL-N. Only components not present in a current standard cellular network are described.

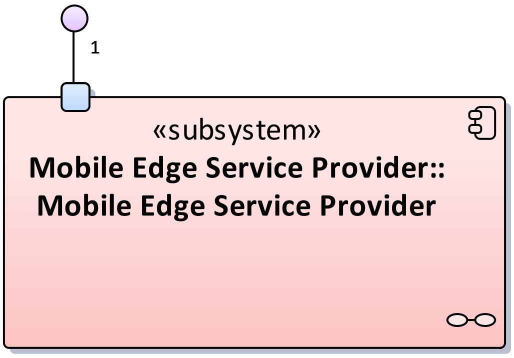


Figure 68: Cellular Network

6.2.3.1.2.1.1 Mobile Edge Service Provider

The Mobile Edge Service Provider is related to Mobile Edge Computing, which is a network architecture concept that enables cloud computing capabilities and an IT service

environment at the edge of a network. By providing services, closer to the Service Customer network congestion is reduced and applications can perform better.
The Mobile Edge Service Provider could be an independent Service Provider or a part of a Service, which consists of the Service Provider backend part and the Mobile Edge Service Provider part inside the Communication Network.

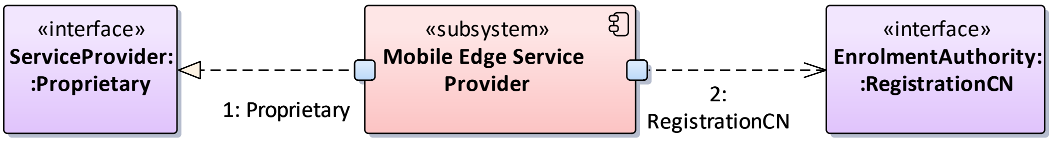


Figure 69: Mobile Edge Service Provider

6.2.3.1.2.2 Interfaces provided

Proprietary

The mobile edge Service Provider is an extension of the Service Provider inside of the communication network. The communication between the two parts depends on the service provided and the packaging of the service. For that reason, this interface is not specified, put rather solely the responsibility of the Service Provider.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from 1 to roprietary

[Direction is 'Source -> Destination'.]

6.2.3.1.2.3 Interfaces used

RegistrationCN

This interface connects the communication network entities (ITS Roadside Station (IRS), MESP, etc.) to the Enrolment Authority (EA). It is used in the registration process of new network entities joining the network.

INCOMING STRUCTURAL RELATIONSHIPS

⇨ Realization from IRS to RegistrationCN

[Direction is 'Source -> Destination'.]

6.2.3.1.3 IRS-Network (IRS-N)

The Intelligent Roadside Station (IRS) network is a network that uses IEEE802.11p communication for the wireless link to the users. The roadside stations are network nodes on the streets and motorways. Distributing information for traffic safety and traffic efficiency is the primary focus.

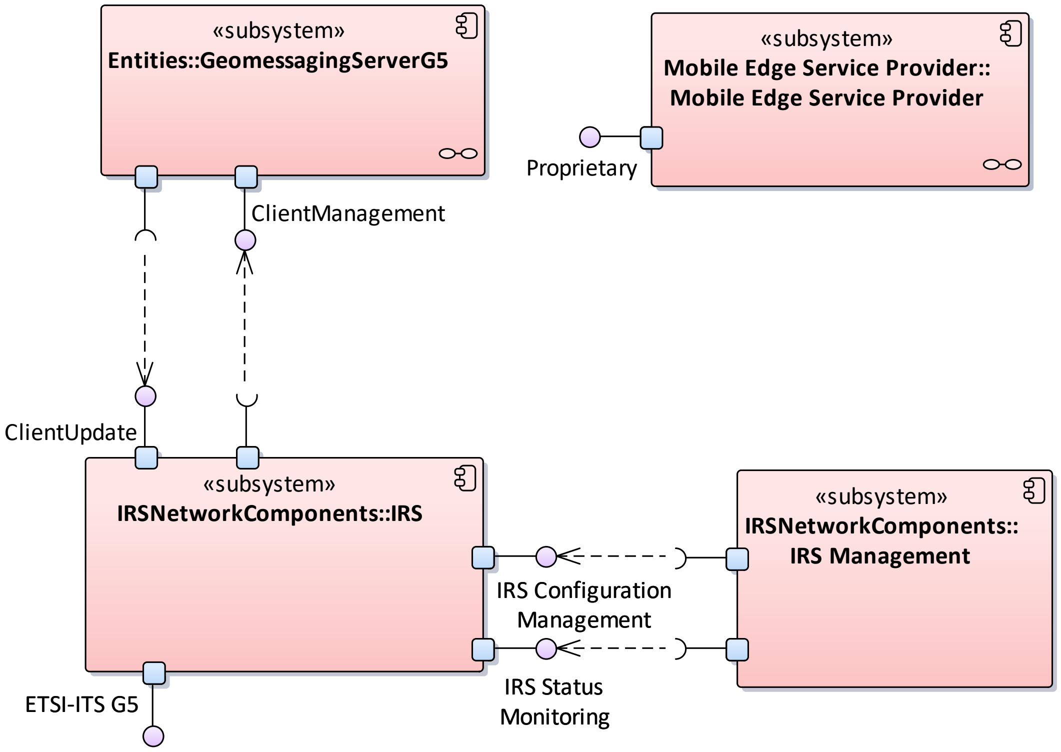


Figure 70: IRS Network

6.2.3.1.3.1 Components

In the following section, the components of the IRS Network will be described in detail. Figure 70 gives an overview of all components inside an IRS Network.

6.2.3.1.3.1.1 Geomessaging Server

Geomessaging is necessary to enable distribution of messages within a certain geographical area. This entity or hierarchy of entities can be placed at various locations within a network. All Geomessaging Server will register at the Service Directory with their area of coverage.

ClientManagement-Interface

This interface is used to register and unregister a client. The IRS as a client provides the information of its current reachable geographical area with its ETSI-ITS G5 communication technology.

STRUCTURAL PART OF ClientManagement
ClientManagement: RequiredInterface

ClientUpdate-Interface

This interface provides the mechanism to deliver a message to an IVS. The GeomessagingServer uses this interface to transfer the message via an IRS to reach an IVS in a specific geographical area.

STRUCTURAL PART OF ClientUpdate
ClientUpdate: ProvidedInterface

6.2.3.1.3.1.2 IRS

An Intelligent Roadside Station (IRS) defines an infrastructure component, which provides ETSI-ITS G5 technology for communication. An IRS therefore can be used to distribute information, mostly in regards to traffic safety and traffic efficiency, via ETSI-ITS G5 communication technology to certain vehicles.

ETSI-ITS G5-Interface

This interface offers the communication technology of ETSI-ITS G5.

STRUCTURAL PART OF ETSI-ITS G5
ETSI-ITS G5: ProvidedInterface

ClientManagement-Interface

This interface is used to register and deregister a client. The IRS as a client provides the information of its current reachable geographical area with its ETSI-ITS G5 communication technology.

STRUCTURAL PART OF ClientManagement
ClientManagement: RequiredInterface

ClientUpdate-Interface

This interface provides the mechanism to deliver a message to an IVS. The IRS provides this interface to transfer a georeferenced message inside its geographical area.

STRUCTURAL PART OF Geomessaging
ClientUpdate: RequiredInterface

IRS Configuration Management-Interface

IRSs need to have a management entity to configure and monitor the state of an IRS Network. With this interface the IRS can be configured.

STRUCTURAL PART OF IRS Configuration Management
IRS Configuration Management : ProvidedInterface

IRS Status Monitoring-Interface

This interface delivers the state of an IRS and is used to detect critical situations of an IRS or an IRS Network early. This interface offers the status of the IRS to the IRS Management component

STRUCTURAL PART OF IRS Status Monitoring
IRS Status Monitoring : ProvidedInterface

6.2.3.1.3.1.3 IRS Management

IRSs need to have a management entity to configure and monitor the state of an IRS Network.

STRUCTURAL PART OF IRS Management
IRS Configuration Management : Port
IRS Status Monitoring : Port

IRS Configuration Management-Interfaces
This interface is used to configure an IRS. Either to deploy the initial configuration or to change configuration on the fly

STRUCTURAL PART OF IRS Configuration Management
IRS Configuration Management : RequiredInterface

IRS Status Monitoring-Interface
This interface delivers the state of an IRS and is used to detect critical situations of an IRS or an IRS Network early

STRUCTURAL PART OF IRS Status Monitoring
IRS Status Monitoring : RequiredInterface

6.2.3.1.3.1.4 Mobile Edge Service Provider

The Mobile Edge Service Provider is related to Mobile Edge Computing, which is a network architecture concept that enables cloud computing capabilities and an IT service environment at the edge of a network. By providing services, closer to the Service Customer network congestion is reduced and applications can perform better. The Mobile Edge Service Provider could be an independent Service Provider or a part of a Service, which consists out of the Service Provider backend part and the Mobile Edge Service Provider part inside the Communication Network.

6.2.3.1.4 DAB Network (DAB-N)

The Digital Audio Broadcast network (DAB-N) is a broadcast network primarily designed for radio distribution. To enhance this network the possibility for data distribution was included. The most commonly used data type is traffic related. In the iKoPA case, the traffic related data are information about parking and charging possibilities.
In the iKoPA concept, DAB will be used to transport GeoMessages. To do this an additional adoption layer protocol for GeoMessages via DAB, has to be implemented and a specific service needs to be set up for all DAB networks that shall participate in the GeoMessaging transmission.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» DAB Network to «plane» Communication Network [Direction is 'Source -> Destination'.]

6.2.3.1.5 RFID (RFD-N)

By using Long-Range UHF RFID technology, items can be tracked in real time and traced through the entire supply chain, while providing full end-to-end transparency at the same time. UHF RFID offers a range of up to 20 m and works at speeds up to 250km/h. It can be used for continuous tracking and real-time location of multimodal vehicles and other assets within any monitored perimeter. By supporting a two-step authentication, RFID offers identification while safeguarding privacy. The identifications used can be changed for every usage. Meaning an identification is used only once, so no tracking is possible.

OUTGOING STRUCTURAL RELATIONSHIPS

Generalization from «Subsystem» RFID to «plane» Communication Network
[Direction is 'Source -> Destination'.]

6.2.3.2 Geomessaging

Geomessaging is necessary to enable distribution of messages within a certain geographical area. It consists out of one or more GeomessagingServer of a specific communication network and a GeomessagingProxy. A GeomessagingServer will register with its coverage area so a GeomessagingProxy can handle the distribution of a message to a destination area.

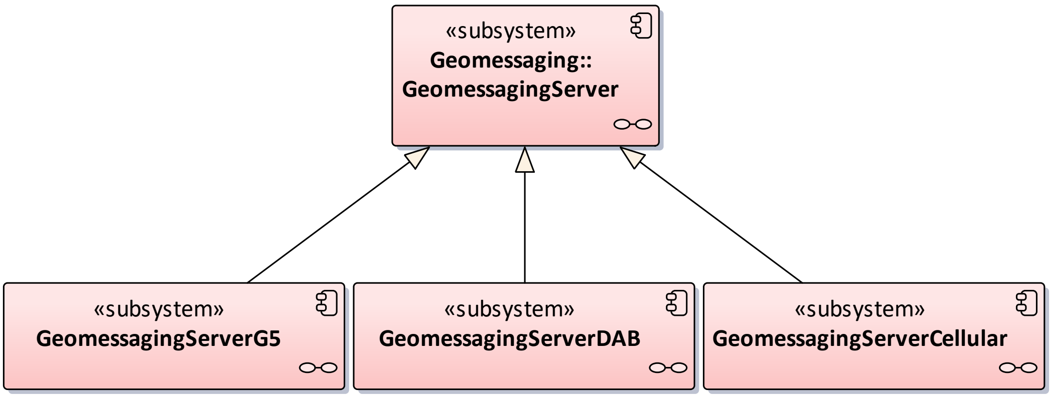


Figure 71: Geomessaging-Entities

6.2.3.2.1 GeomessagingServer (GEOMS)

Geomessaging is necessary to enable distribution of messages within a certain geographical area. This entity or hierarchy of entities can be placed at various locations within a Network. All GeomessagingServers will register at the ServiceDirectory with their area of coverage

INCOMING STRUCTURAL RELATIONSHIPS
➡ Generalization from «Subsystem» GeomessagingServerDAB to «Subsystem» GeomessagingServer [Direction is 'Source -> Destination'.]
➡ Generalization from «Subsystem» GeomessagingServerG5 to «Subsystem» GeomessagingServer [Direction is 'Source -> Destination'.]
➡ Generalization from «Subsystem» GeomessagingServerCellular to «Subsystem» GeomessagingServer [Direction is 'Source -> Destination'.]

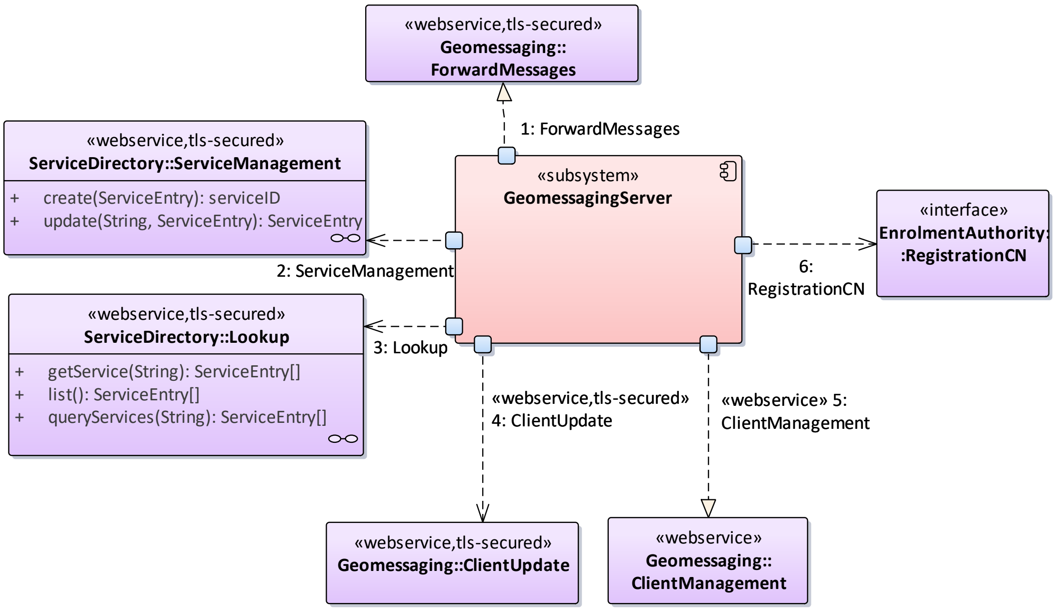


Figure 72: GeomessagingServer

6.2.3.2.1.1 Interfaces provided

ClientManagement

This interface is used to register and deregister clients of the GeomessagingServer.

INCOMING STRUCTURAL RELATIONSHIPS
➡ Realization from GEOM to «webservice» ClientManagement [Direction is 'Source -> Destination'.]

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from «webservice» 5 to «webservice» ClientManagement [Direction is 'Source -> Destination'.]

ForwardMessages

This interface provides the possibility for Service Providers to deliver messages to mobile terminals based on their geographical location, their attributes, or based on specific topics via the channels a GeomessagingServer provides.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from «webservice» 4 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]
⇨ Realization from GEOM to «webservice» ForwardMessages [Direction is 'Source -> Destination'.]

6.2.3.2.1.2 Interfaces used

RegistrationCN

This interface connects the Geomessaging Server (GEOMS) to the Enrolment Authority (EA). It is used in the registration process of new GEOMS joining the network.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from IRS to RegistrationCN [Direction is 'Source -> Destination'.]

Lookup

This interface is used for debugging purposes by verifying that the GEOMS has successfully registered.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» Lookup [Direction is 'Source -> Destination'.]
⇨ Realization from 1 to «webservice» Lookup [Direction is 'Source -> Destination'.]

ServiceManagement

This interface provides mechanisms for service management by the GEOMS. The GEOMS registers, deregisters and updates its service with information about availability, geographical region, etc.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Realization from SD to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]
⇨ Realization from 2 to «webservice» ServiceManagement [Direction is 'Source -> Destination'.]

ClientUpdate

This interface provides the mechanism to deliver a message to a remote station over a cellular link. Furthermore, the mechanism to update the location and the service subscriptions of the remote station is specified here.

6.2.3.2.2 GeomessagingServerDAB (GEOMS-D)

The GeomessagingServerDAB, will use the "GeoMessage Over DAB" protocol to transport GeoMessages via DAB. It knows about specific features and requirements of DAB and is able to handle them. It has to deal with multiplexing and data rate management, to assure the Geomessages that are pending for transmission do fit into the data rate of the predefined DAB sub channels.

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from «Subsystem» GeomessagingServerDAB to «Subsystem» GeomessagingServer [Direction is 'Source -> Destination'.]

6.2.3.2.2.1 Interfaces provided

EDI output-Interface

EDI ("Encapsulation of DAB Interfaces ") is specified in ETSI TS 102 693 and allows DAB specific protocols to be encapsulated and transmitted by using generic IP-based protocols. It is the default base interface for data provision to DAB multiplexers and to the DAB transmitters, in case that they are connected to IP-based networks (like the internet or separated dedicated IP-based contribution networks).

STRUCTURAL PART OF EDI output
ProvidedInterface : ProvidedInterface

6.2.3.2.2.2 Interfaces used

None

6.2.3.2.3 GeomessagingServerG5 (GEOMS-G)

Geomessaging is necessary to enable distribution of messages within a certain geographical area. This entity or hierarchy of entities can be placed at various locations within a network. All GeomessagingServers will register at the ServiceDirectory with their area of coverage. This is specific for an ETSI ITS-G5 communication network.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» GeomessagingServerG5 to «Subsystem» GeomessagingServer [Direction is 'Source -> Destination'.]

6.2.3.2.4 GeomessagingServerCellular (GEOMS-C)

Geomessaging is necessary to enable distribution of messages within a certain geographical area. This entity or hierarchy of entities can be placed at various locations within a network. All high level GeomessagingServer will register at the ServiceDirectories with their area of coverage. The communication from and to the clients depends on the use case. Clients always use unicast communication, but the server can use both direct communication via unicast or multicast techniques like eMBMS (evolved Multimedia Broadcast Multicast Service). To be aware where the users are in the network (their global position with an acceptable certain degree of fuzziness for privacy reasons) the clients have to update the server regularly.

OUTGOING STRUCTURAL RELATIONSHIPS

Generalization from «Subsystem» GeomessagingServerCellular to «Subsystem» GeomessagingServer
[Direction is 'Source -> Destination'.]

6.2.3.3 TimeSynchronization (TSS-C)

This is the Time Synchronization Server for the communication network services and server. All servers must be synchronous for security, registration, reservation and billing purposes.

6.2.4 Remote Station Plane

The Remote Station Plane is the plane at the bottom. It represents the user and field equipment. From a communication point of view, it is the endpoint of the communication links in the architecture. The systems in the plane only communicate with stations in the same plane or with the communication network plane.

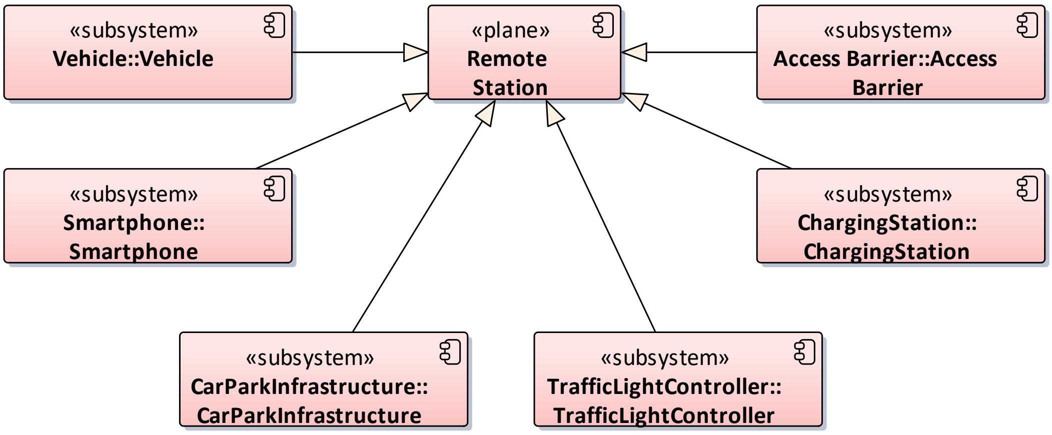


Figure 73: Remote Station

6.2.4.1 Remote Station

In iKoPA six realizations of the remote station concept are defined. However, the architecture is open for further realization in the future. The realization can be categorized in two domains: mobile stations and infrastructure stations. The mobile stations are vehicle and smartphone. The infrastructure stations are the car park infrastructure, the access barrier, the charging station, and the traffic light controller. The common interfaces are described in the next two sections. Afterwards the different realizations are explained in more detail.

INCOMING STRUCTURAL RELATIONSHIPS
⇨ Generalization from «Subsystem» V-ITS-Station to «plane» Remote Station [Direction is 'Source -> Destination'.]
⇨ Generalization from «Subsystem» Access Barrier to «plane» Remote Station [Direction is 'Source -> Destination'.]
⇨ Generalization from «Subsystem» ChargingStation to «plane» Remote Station [Direction is 'Source -> Destination'.]
⇨ Generalization from «Subsystem» TrafficLightController to «plane» Remote Station [Direction is 'Source -> Destination'.]
⇨ Generalization from «Subsystem» CarParkInfrastructure to «plane» Remote Station [Direction is 'Source -> Destination'.]
⇨ Generalization from «Subsystem» Vehicle to «plane» Remote Station [Direction is 'Source -> Destination'.]
⇨ Generalization rom «Subsystem» Smartphone to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.2.4.1.1 Interfaces provided

ClientUpdate

This interface provides the mechanism to receive a message from a Geomessaging Server. Furthermore, the mechanism to update the location and the service subscriptions of the remote station are specified here.

Coupling

The coupling connects two devices with each other. In iKoPA this are the smartphone and the vehicle. This is necessary for example, when the user reserves a parking lot and the vehicle has to authenticate itself. The coupling is done via NFC, i.e. a flavor of short-range RFID. The NFC reader is handled by the phone’s app and provides an air interface of physical type ISO/IEC 14443-2/3 Type A and a logical interface of smart card to an NFC tag.

V2X

The Vehicle-2-X (V2X) interface provides a direct communication link between two entities on the remote station plane. In iKoPA this are smartphone, vehicle, charging station, access barrier and traffic light. This list can be extended to any other systems placed on this plane. The interface is independent from the uses communication technology. This can be 802.11p, cellular direct link, RFID or other direct link communication technologies.

6.2.4.1.2 Interfaces used

Authorization

This interface connects a remote station to the Authorization Authority (AA). It is used in the recurring process of authorization, primarily to obtain the short-term pseudonym tickets.

ForwardMessages

This interface is used to send messages from the remote plane to the Service Provider. The interface is based on IP and other protocols running on it, which are application specific. The physical connection is established via the CNs.

ClientManagement

This interface is used to register and deregister clients of the GeomessagingServer. In addition, client send updates about their current position. This must not be in any case a precise position, but can also be a geographical area.

Coupling

The coupling connects two devices with each other. In iKoPA this are smartphone and the vehicle. This is necessary for example, when the user reserves a parking lot and the vehicle has to authenticate itself.

Create Pseudonym

This interface connects the remote station to the identity provider. It is used to create an pseudonym for a user within the iKoPA system.

RegistrationRS

This interface is used in the registration process of a new remote station to obtain its initial credentials.

V2X

The Vehicle-2-X (V2X) interface provides a direct communication link between two entities on the remote station plane. In iKoPA this are smartphone, vehicle, charging station, access barrier and traffic light. This list can be extended to any other systems placed on this plane. The interface is independent from the uses communication technology. This can be 802.11p, cellular direct link, RFID or other direct link communication technologies.

6.2.4.2 Components

The remote station plan can be realized by mobile stations, e.g. smartphones or vehicles, or be infrastructure stations, e.g. access barriers or charging stations. The realizations in the iKoPA architecture are shown in Figure 73 and described in the following sections.

6.2.4.2.1 Smartphone

The smartphone is an entity that connects the user (Driver) to the cloud. It is required for reservation, navigation and pairing of vehicle and user.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» Smartphone to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.2.4.2.1.1 Interfaces provided

Coupling

The coupling is done via NFC, i.e. a flavor of short-range RFID. The NFC reader is handled by the phone’s app and provides an air interface of physical type ISO/IEC 14443-2/3 Type A and logical interface of smart card to an NFC tag.

6.2.4.2.1.2 Interfaces used

CellularConnection

The air interface to the cloud is provided as Data Service application according to either of the standards 2G GSM-EDGE, 3G UMTS or 4G LTE.

CreatePseudonym

This interface connects the smartphone to the identity provider. It is used to create a pseudonym for a user within the iKoPA system.

ReservationConfirmation

After a reservation request, a Service Provider confirms or declines the reservation depending on availability and the registration status of the requester. Part of the reservation confirmation is the provision of a reservation token/key for authentication.

ReservationRequest

When the vehicle wants to use a service, which requires reservation, it sends a request to a reservation service, which grants or declines the request depending on the user registration status and availability of the service.

WLANConnection

WLAN is used to couple a smart phone device locally inside the vehicle to the vehicle's AU. It can be any of the WLAN standard flavors a, b, g, n or ac.

6.2.4.2.2 Vehicle

The vehicle is the main entity connecting the user the smartphone and the communication network. It provides the interfaces to services, to the authentication, to the user equipment and receives and sends messages.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» Vehicle to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.2.4.2.2.1 Interfaces provided

None

6.2.4.2.2.2 Interfaces used

V2X Auth

V2X Authentication uses the V2X bearer service in connection with an asymmetric key pair exchanged during reservation. The Authentication makes use of the V2X ITS G5 security standard on which it adds a layer of security. A new command type needs to be defined in ITS G5, which then has to be standardized.

RFID Auth

RFID Authentication is based on (e.g. AES128) symmetric key cryptography. The procedure follows the Long-Range RFID communication standard. It includes privacy procedures. Today, the keys are pre-configured on the RFID tag and RFID reader side. However, in the future this should be dynamically changeable.

WLANConnection

WLAN is used to couple a smart phone device locally inside the vehicle to the vehicle's AU. It can be any of the WLAN standard flavors a, b, g, n or ac.

6.2.4.2.3 CarParkInfrastructure

All elements of the car park house related to the local parking management (like single space detectors, ticket terminals, and local control system).

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» CarParkInfrastructure to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.2.4.2.4 ChargingStation

The Charging Station represents the local publicly available infrastructure for connecting and charging of electrical vehicles. It can be connected to a Charge Point Management system and be part of networks operated by e-mobility providers available for subscribed users.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» ChargingStation to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.2.4.2.5 TrafficLightController

The Traffic Light Controller switches all the traffic signals at an intersection according to a defined signal program. It has an inbuilt local intelligence and can be interfaced to centralized management systems or services as well as other local ITS-related equipment.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» TrafficLightController to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.2.4.2.6 Access Barrier

An access barrier in front of a car park (a light signal could also be a stand-in for demonstration).

ELEMENTS OWNED BY Access Barrier
RFID Reader : Component «Subsystem»

OUTGOING STRUCTURAL RELATIONSHIPS

Generalization from «Subsystem» Access Barrier to «plane» Remote Station

[Direction is 'Source -> Destination'.]

6.2.4.2.6.1 Interfaces provided

V2X Auth

V2X Authentication uses V2X bearer service in connection with an asymmetric key pair exchanged during reservation. The Authentication makes use of the V2X ITS G5 security standard on which it adds a layer of security. A new command type needs to be defined in ITS G5, which then has to be standardized.

RFID Auth

RFID Authentication is based on (e.g. AES128) symmetric key cryptography. The procedure follows the Long-Range RFID communication standard. Today, the keys are pre-configured on the RFID tag and RFID reader side. However, in the future this should be dynamically changeable.

6.2.4.2.6.2 Interfaces used

ForwardTicket

The Ticket is handled as a token and set of keys allowing access at the barrier.

6.2.4.2.6.3 Components

The access barrier has dedicated communication components for the authentication process. These are a RFID reader and a Trusted Platform Module.

6.2.4.2.6.3.1 RFID Reader

The RFID Reader or so-called interrogator is a device, which communicates through the air interface with an RFID tag. It provides three functions: First, energy supply via RF energy harvesting, the second function is the transmission of data and the third function is the reception of the tag’s response. Part of the RFID reader is also the safe container of the white list of accepted RFID tags, stored in a TPM module inside the interrogator.

ELEMENTS OWNED BY RFID Reader

TPM : Component

6.2.4.2.6.3.1.1 Interfaces provided

RFID Auth

The Authentication of the RFID communication is based on (e.g. AES128) symmetric cryptography with predefined secret key pairs. This is part of the RFID standard and cannot be modified. It uses the (in the future changeable) ID of the vehicle but is encapsulated by means of a local TPM

6.2.4.2.6.3.1.2 Interfaces used

The RFID IDENTIFCATION as given by the RFID UHF Long-range standard and implemented in the tag and in the reader

6.2.4.2.6.3.2 TPM

The TPM safeguards the identity of the user and the vehicle. It encapsulates the crypto algorithms, secret and public keys as well as a white list of registered and accepted users. It can be implemented in software on a trusted hardware or incorporated in a security hardware component.

6.2.4.2.6.3.2.1 Interfaces provided

AuthSession

AuthSession covers the interfaces for the authentication of the vehicle by the barrier. It can optionally also cover the mutual authentication of vehicle and barrier. This is useful when an automated vehicle needs to trust a car park identity before entering it. The authentication is prepared by a.) exchange of secrets during reservation (V2X case) and/or b.) pre-configurations of IDs and secret keys (RFID case)

LoadKey

Manages the asymmetric (private/public) and symmetric (secret) key handling including storage and protection.

6.2.4.2.6.3.2.2 Interfaces used

None

6.2.4.3 TimeSynchronization (TSS-R)

This is the Time Synchronization Server for the remote station services and systems. All systems must be synchronous for security, registration, reservation and billing purposes.

6.3 Low Level Concepts

This chapter describes important concepts from the high-level architecture in more detail. The concepts include more detailed descriptions of some architectural components as well as the description of important mechanisms.

6.3.1 MobileEdgeServiceProvider (MESP)

The Mobile Edge Service Provider is related to Mobile Edge Computing, which is a network architecture concept that enables cloud computing capabilities and an IT service environment at the edge of a network. By providing services closer to the Service Customer network congestion is reduced and applications can perform better. The Mobile Edge Service Provider could be an independent Service Provider or a part of a Service, which consists of the Service Provider backend part and the Mobile Edge Service Provider part inside the Communication Network.

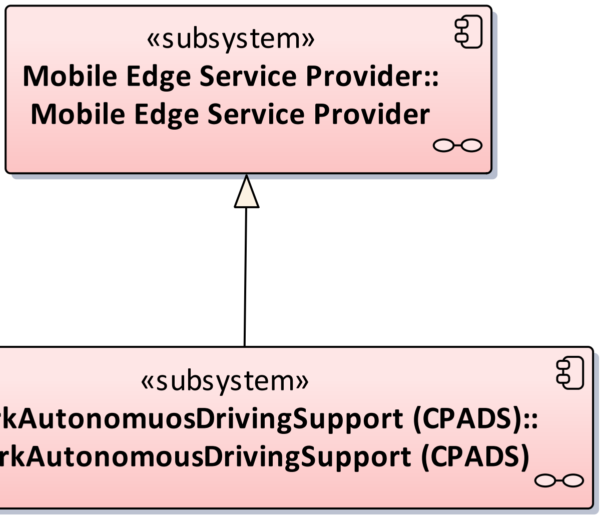

«subsystem»
Mobile Edge Service Provider::
Mobile Edge Service Provider
«subsystem»
CarParkAutonomuosDrivingSupport (CPADS)::
CarParkAutonomousDrivingSupport (CPADS)

Figure 74: MobileEdgeServiceProvider-Overview

INCOMING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» CarParkAutonomousDrivingSupport (CPADS) to «Subsystem» Mobile Edge Service Provider [Direction is 'Source -> Destination'.]

6.3.1.1 CarParkAutonomuosDrivingSupport (CPADS)

The CarParkAutonomuosDrivingSupport (CPADS) enables vehicles to drive autonomously through the car park. Therefore, CPADS provides services necessary for the route guidance and orientation of the vehicle as well as for safe-driving. It receives location information from the infrastructure of the car park like the connected camera systems and transmits them via the integrated road site unit to the cars.

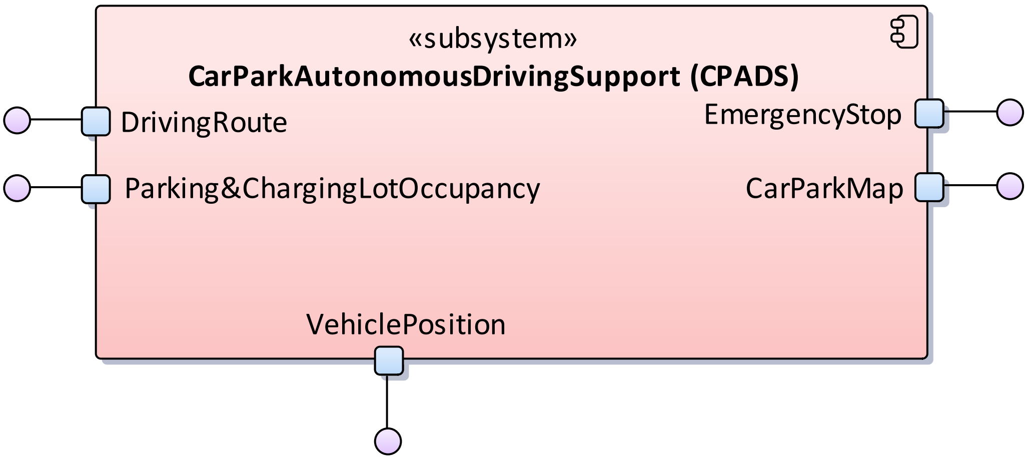

«subsystem»
CarParkAutonomousDrivingSupport (CPADS)
DrivingRoute
Parking&ChargingLotOccupancy
EmergencyStop
CarParkMap
VehiclePosition

Figure 75: CarParkAutonomousDrivingSupport (CPADS)

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» CarParkAutonomousDrivingSupport (CPADS) to «Subsystem» Mobile Edge Service Provider [Direction is 'Source -> Destination'.]

STRUCTURAL PART OF CarParkAutonomousDrivingSupport (CPADS)
CarParkMap : Port
DrivingRoute : Port
EmergencyStop : Port
Parking&ChargingLotOccupancy : Port
VehiclePosition : Port

6.3.1.1.1 Interfaces

CarParkMap

Via this interface, the connected cars receive the map of the car park with the driving lanes and the parking and charging lots. Beside the geographical representation of the map, a routable graph for emergency cases is provided.

DrivingRoute

The car park provides a pre-calculated route that the vehicle has to use to reach the final parking or charging spot.

EmergencyStop

Over this bidirectional interface, each site can inform the other one in case of an emergency stop. If the car park sends the EmergencyStop the car has to stop immediately. The carpark can also be informed by the vehicle that it stops for whatever reasons. This is a time-critical connection and therefore only a short delay is acceptable.

Parking&ChargingLotOccupancy

The interface provides an overview about the current occupancy status of the car park.

VehiclePosition

Over this interface, the autonomous car receives the immediate position as a GPS replacement in a very short succession. This is a time-critical connection and therefore only a short delay is acceptable.

6.3.2 ServiceDirectory (SD)

The Service Directory provides an overview of the entities available in the network. These entities are mainly services, communication networks, Geomessaging-Servers and other SD instances. Special extensions will feature specific concepts of certain technologies, like DAB and TPEG, to include them fully into the Service Directory concept.

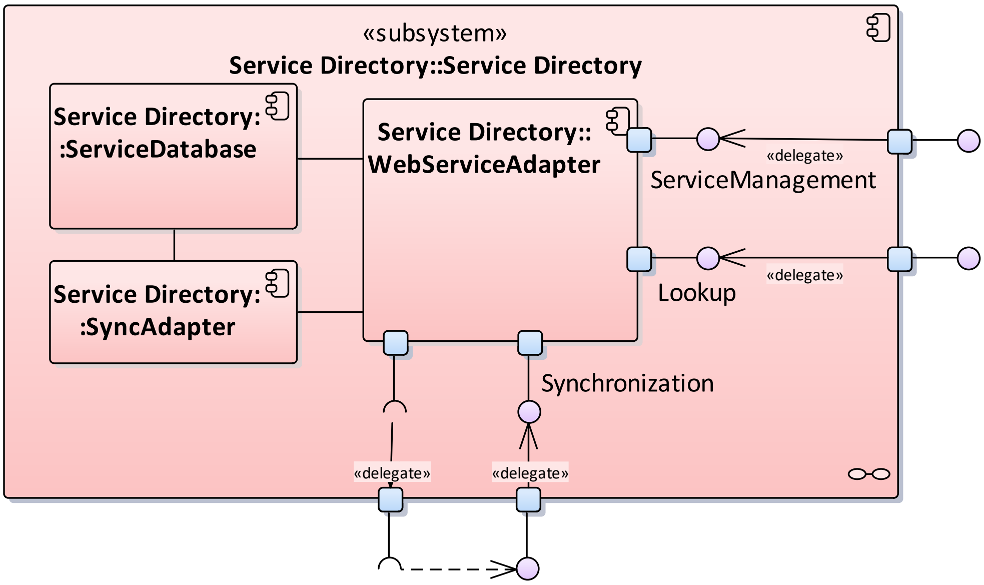


Figure 76: ServiceDirectory - Neighborhood

ELEMENTS OWNED BY Service Directory
ServiceDatabase : Component «Subsystem»
SyncAdapter : Component «Subsystem»
WebServiceAdapter : Component «Subsystem»

STRUCTURAL PART OF Service Directory
Lookup : Port
Service Management : Port
Synchronization (a) : Port
Synchronization (b) : Port

6.3.2.1.1 Interfaces

Lookup

This service allows to query of the service entries in the service directory based on a set of criteria. It is provided by the SD to its clients, to allow them to obtain entries out of the Service Directory.

INCOMING STRUCTURAL RELATIONSHIPS
Delegate from SD to Lookup [Direction is 'Source -> Destination'.]

CONNECTORS
Dependency Source -> Destination From: Lookup : RequiredInterface, Public To: Lookup : ProvidedInterface, Public
Delegate Source -> Destination From: SD : Port, Public To: Lookup : ProvidedInterface, Public
Dependency Source -> Destination From: SDLookup : RequiredInterface, Public To: Lookup : ProvidedInterface, Public

ServiceManagement

This interface provides mechanisms for service management by Service Providers, e.g. service registration, deregistration and updates. It is used by Service Providers to create the entries, which can be obtained by the lookup interfaces mentioned above.

INCOMING STRUCTURAL RELATIONSHIPS
Delegate from SD to ServiceManagement [Direction is 'Source -> Destination'.]

CONNECTORS
Dependency Source -> Destination From: SDServiceManagement : RequiredInterface, Public To: ServiceManagement : ProvidedInterface, Public

CONNECTORS
Delegate Source -> Destination From: SD : Port, Public To: ServiceManagement : ProvidedInterface, Public
Dependency Source -> Destination From: ServiceManagement : RequiredInterface, Public To: ServiceManagement : ProvidedInterface, Public

Synchronization

This interface is used by the Service Directory instances to share information about service. It allows one SD to inform another SD of new services, requests information of services or communicate a change about a service. Therefore, it is provided as well as consumed by each Service Directory instance.

CONNECTORS
Dependency Source -> Destination From: Synchronization : RequiredInterface, Public To: Synchronization : ProvidedInterface, Public

6.3.2.1.2 Components

In the following, the inner components of the SD are described.

6.3.2.1.2.1 ServiceDatabase

This database contains a listing of all ServiceEntries known to the ServiceDirectory.

ASSOCIATIONS	
Source: Public (Component) ServiceDatabase	Target: Public (Component) WebServiceAdapter
Source: Public (Component) ServiceDatabase	Target: Public (Component) SyncAdapter

6.3.2.1.2.2 SyncAdapter

This adapter implements the synchronization facilities of the ServiceDirectory.

ASSOCIATIONS	
Source: Public (Component) WebServiceAdapter	Target: Public (Component) SyncAdapter
Source: Public (Component) ServiceDatabase	Target: Public (Component) SyncAdapter

6.3.2.1.2.3 WebServiceAdapter

The WebServiceAdapter adapts the ServiceDatabase to the WebService interface.

STRUCTURAL PART OF WebServiceAdapter
Lookup : Port
Mgmt : Port
SYN-OUT : Port
Sync : Port

ASSOCIATIONS	
Source: Public (Component) WebServiceAdapter	Target: Public (Component) SyncAdapter
Source: Public (Component) ServiceDatabase	Target: Public (Component) WebServiceAdapter

6.3.2.1.2.4 Interfaces

Lookup

This service allows to query the service entries in the service directory based on a - still to be defined - set of criteria. It is the SD internal implementation of the corresponding interface described in section 6.3.2.1.1.

Mgmt (ServiceManagement)

This interface provides mechanisms for service management by Service Providers, e.g. service registration, deregistration and updates. It is the SD internal implementation of the corresponding interface described in section 6.3.2.1.1.

SYN-OUT (Synchronization)

This interface is used by other Service Directory instances to share information of their services with the own SD instance and to access information of the own SD instance. It is the SD internal implementation of the corresponding interface described in section 6.3.2.1.1.

Sync (Synchronization)

This interface is used by other Service Directory instances to share information of their services with the own SD instance and to access information of the own SD instance. It is the SD internal implementation of the corresponding interface described in section 6.3.2.1.1.

6.3.3 ServiceProvider (SP)

The Service Provider (SP) is a generic role. It represents the responsibilities, which a service providing entity in the network needs to fulfil. In the low-level architecture, more specific SP instances have been defined to allow a more detailed specification of the various functionalities of SP's in the architecture. The provided SP are only examples. More SP can be added to the system and every SP can exist in more than one instance by more than one institution providing the service.

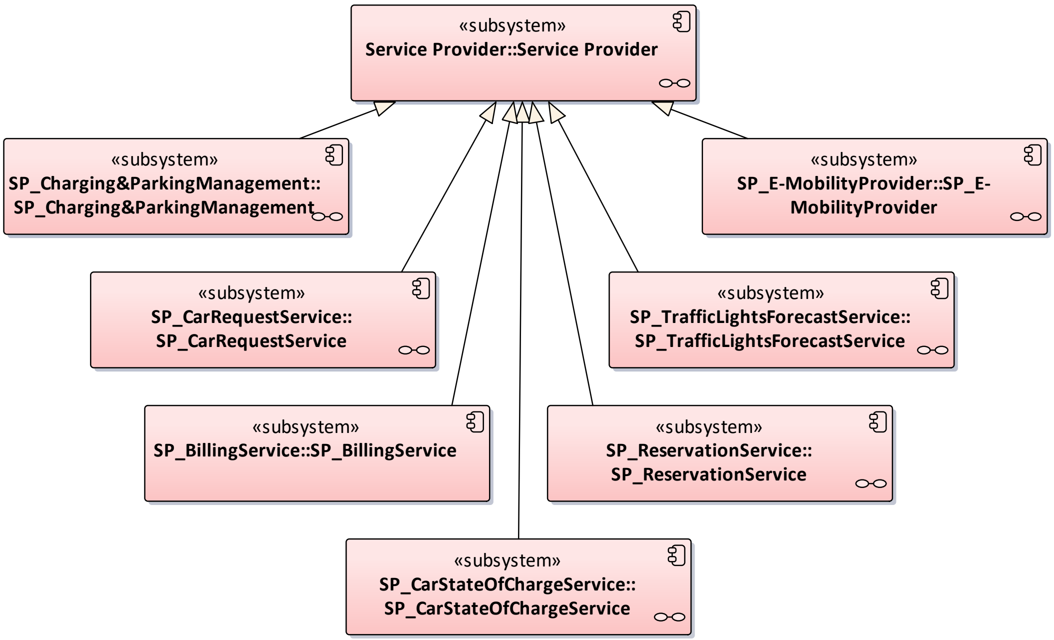

«subsystem»
Service Provider::Service Provider
«subsystem»
SP_Charging&ParkingManagement::
SP_Charging&ParkingManagement
«subsystem»
SP_E-MobilityProvider::SP_E-MobilityProvider
«subsystem»
SP_CarRequestService::
SP_CarRequestService
«subsystem»
SP_TrafficLightsForecastService::
SP_TrafficLightsForecastService
«subsystem»
SP_BillingService::SP_BillingService
«subsystem»
SP_ReservationService::
SP_ReservationService
«subsystem»
SP_CarStateOfChargeService::
SP_CarStateOfChargeService

Figure 77: SP Overview

6.3.3.1 SP_BillingService

The SP_BillingService provider provides the means to process the billing information for the parking and charging. As such, it serves as a trusted party for the car park, providing methods of confirming the validity of billing information and the transmission of billing information. Other billing provides can be integrated for lesser traceability and more services.

STRUCTURAL PART OF SP_BillingService
BillParking : Port
ConfirmBillable : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_BillingService to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.3.1.1 Interfaces

BillParking
This interface is used to transmit the information relevant for billing the parking, such as the duration of the parking and charging.

ConfirmBillable
This interface is used to confirm the validity of billing information.

6.3.3.2 SP_CarRequestService

The CarRequestServiceProvider, gives the Driver the ability to request its vehicle to drive to a specific position via a personal device, which is coupled with the vehicle. Therefor the CarRequestServiceProvider handles the registration of the Driver and its related personal device and its vehicle, the actual request of the vehicle to drive to a requested position and the forwarding of the request to the vehicle itself.

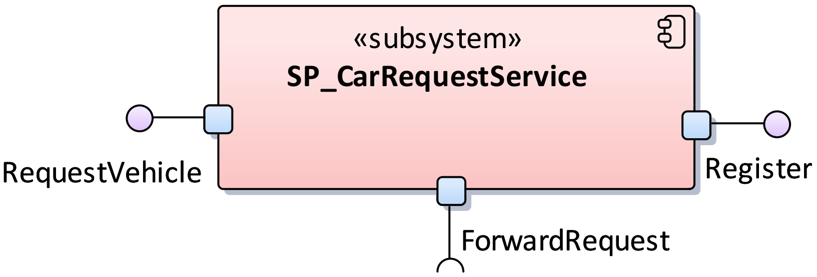


Figure 78: SP_CarRequestService

STRUCTURAL PART OF SP_CarRequestService
⚙ ForwardRequest : Port
⚙ Register : Port
⚙ RequestVehicle : Port

OUTGOING STRUCTURAL RELATIONSHIPS
⇦ Generalization from «Subsystem» SP_CarRequestService to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.3.2.1 Interfaces

ForwardRequest

This interface is used to forward the vehicle request to the vehicle.

Register

A user has to register to the service first to use the Request Service. This should include a unique identifier of a personal device, in most cases a smartphone, and a unique identifier of the vehicle. Those identifiers are unique only for this one transaction. For the next transaction different identifiers should be generated so that neither the vehicle nor the smartphone can the traced.

RequestVehicle

This interface is used to handle requests of vehicle requests.

6.3.3.3 SP_CarStateOfChargeService

The SP_CarStateofChargeService gives the Driver the ability to request the charging state of his vehicle via a personal device, which has to be coupled with the vehicle. The SP_CarStateofChargeService handles the registration of the Driver and its related personal device and vehicle.

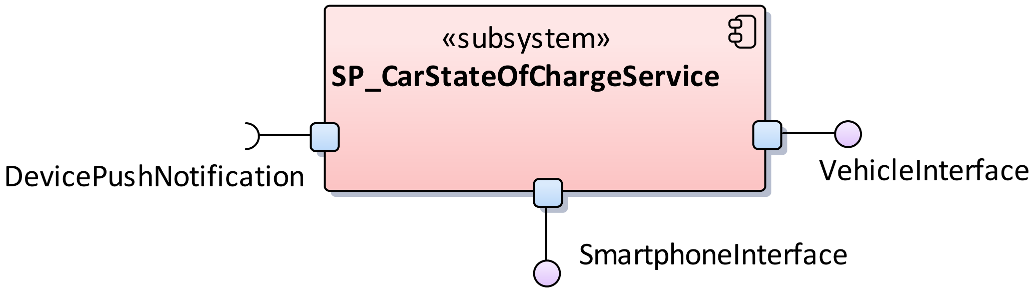


Figure 79: SP_CarStateOfChargeService

STRUCTURAL PART OF SP_CarStateOfChargeService
DevicePushNotification : Port
SmartphoneInterface : Port
VehicleInterface : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_CarStateOfChargeService to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.3.3.1 Interfaces

DevicePushNotification

The DevicePushNotification interface is used to output push messages to a personal device.

SmartphoneInterface

The SmartphoneInterface is used to interact with a personal device (e.g. a smartphone).

VehicleInterface

The VehicleInterface is used to interact with a coupled vehicle.

6.3.3.4 SP_Charging&ParkingManagement

Charging & Parking Management is a service that exists in the backend plane. It combines the functionalities of a Charge Point Management with classical citywide parking guidance and additional premium services (like remote charging/parking spot reservation). It provides an interface between electric mobility Service Providers and park-house infrastructure equipped with charging stations.

ELEMENTS OWNED BY SP_Charging&ParkingManagement
Charge Point Management : Component «Subsystem»
Parking Infrastructure Status Monitor : Component «Subsystem»
Reservation Handler : Component «Subsystem»

STRUCTURAL PART OF SP_Charging&ParkingManagement
Broadcast interface : Port
Charge Point Interface : Port
EMP interface : Port
Parking control interface : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_Charging&ParkingManagement to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.3.4.1 Interfaces

Broadcast interface

The interface is used to inform services (TPEG/DAB, mobile) about charge spot availability.

Charge Point Interface

This interface is used to connect to remote charging stations.

EMP interface
This interface is used to connect to e-mobility Service Providers.

Parking control interface
This interface is used to connect to local Car Park management system.

6.3.3.4.2 Components

The Charging & Parking Management cloud service contains the following logical components that account for interaction with external systems and perform use case specific tasks.

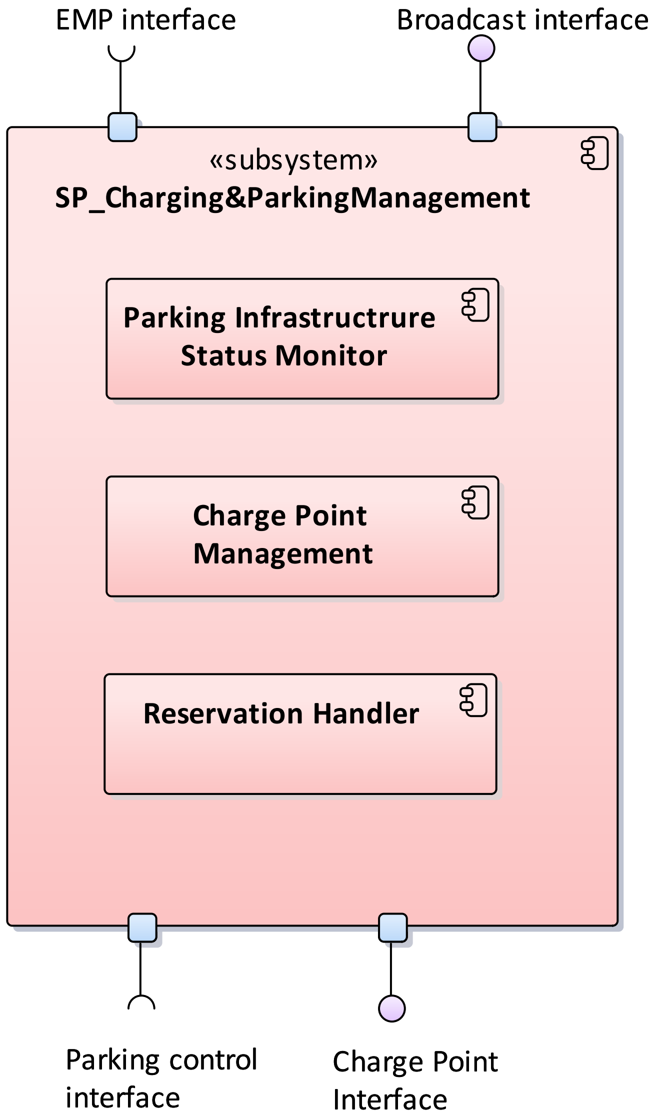


Figure 80: SP_Charge&ParkManagementService internal overview

6.3.3.4.2.1 Charge Point Management

This is a component that manages the remote connected charging station infrastructure from an operational and technical point of view (i.e. access control, management, data collection, maintenance).

6.3.3.4.2.2 Parking Infrastructure Status Monitor

A component that monitors the status of connected remote park-house facilities through an interface with their local control systems. Acquired status updates concerning the current park-house utilization are used to indicate availability of free parking lots to parking guidance sub-systems or broadcasting services.

6.3.3.4.2.3 Reservation Handler

A component that manages reservation requests received by external EMPs or other 3rd party Service Providers. The reservation request is processed and the requested charging station is booked until the validity of the time slot expires or is consumed by an authorized user

6.3.3.5 SP_E-MobilityProvider

An entity that sells e-mobility services to end customers. Such services include seamless and possibly payment free access to charging stations from different charging station operators. Additional services like parking, electricity supply and others might also be included in the contract.

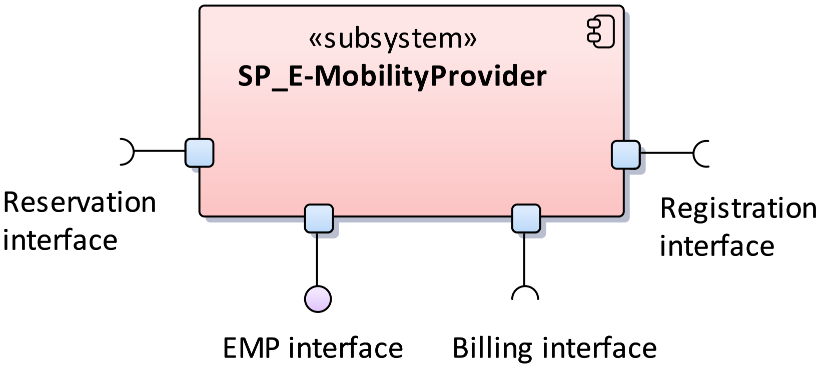


Figure 81: SP_E-MobilityProvider

STRUCTURAL PART OF SP_E-MobilityProvider
Billing interface : Port

STRUCTURAL PART OF SP_E-MobilityProvider
EMP interface : Port
Registration interface : Port
Reservation interface : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_E-MobilityProvider to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.3.5.1 Interfaces

Billing interface

This interface is used to send service consumption data to a Billing Service, which is responsible for clearing/payments.

EMP interface

This interface is used to connect with other E-Mobility Providers in order to allow roaming of the services delivered to the end customer. The same interface can be used also for a connection with the SP_Charging&ParkingManagement service in order to enable premium features like charging/parking lot availability status and reservation.

Registration interface

This interface is used to connect to an external identity provider that accounts for registering and authenticating end users of a 3rd party e-mobility service.

Reservation interface

This interface is used to connect to an external Reservation Service that accounts for initiating reservation requests for a parking/charging spot by end users of a 3rd party e-mobility service.

6.3.3.6 SP_ReservationService

The reservation service manages reservation requests.

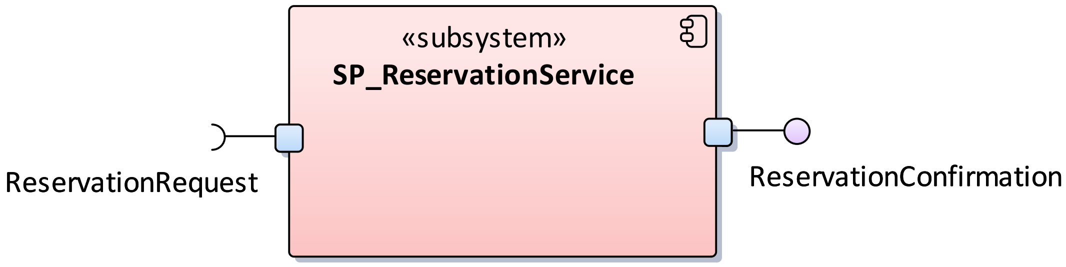


Figure 82: SP_ReservationService

STRUCTURAL PART OF SP_ReservationService
ReservationConfirmation : Port
ReservationRequest : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_ReservationService to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.3.6.1 Interfaces

ReservationConfirmation
This interface relays reservation confirmations.

ReservationRequest
This interface is used for reservation requests.

6.3.3.7 SP_TrafficLightsForecastService

This is a service that predicts traffic signal timings. It is based on current and historic status of an intersection. The final information comes in the form of a standard SPAT/MAP message. Dissemination may happen locally (e.g. over 802.11p) or centrally (over mobile operator networks or DAB/TPEG). SPAT/MAP messages are used by onboard systems or a mobile app. E.g. to display (TTG - time to green) or (GLOSA - Green Light Optimal Speed Advisory). The TLF service runs centrally in the backend plane.

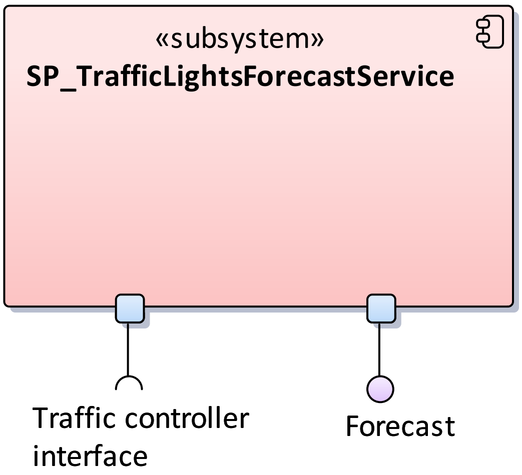


Figure 83: SP_TrafficLightsForecastService

STRUCTURAL PART OF SP_TrafficLightsForecastService
Forecast : Port
Traffic controller interface : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_TrafficLightsForecastService to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.3.7.1 Interfaces

Forecast

The forecast interface is used to output forecast messages in a standard SPAT/MAP format.

Traffic Controller Interface

The interface links a remote traffic controller to the Traffic Lights Forecast Service. The interface provides exchange of signals timing and traffic condition data from the controller to the TLF central server. It is used to get input on current signal state/detection from intersections

6.3.4 Ticket Authentication System

The Ticket Authentication System details the architecture used to authenticate vehicles in front of access barriers (e.g. in front of the car park or charging station). The user's smartphone creates "pseudonym" with the identity provider. Tickets serve as a single use pseudonym for the smartphone and in turn as an authentication method (without revealing the actual identity within the iKoPA System).

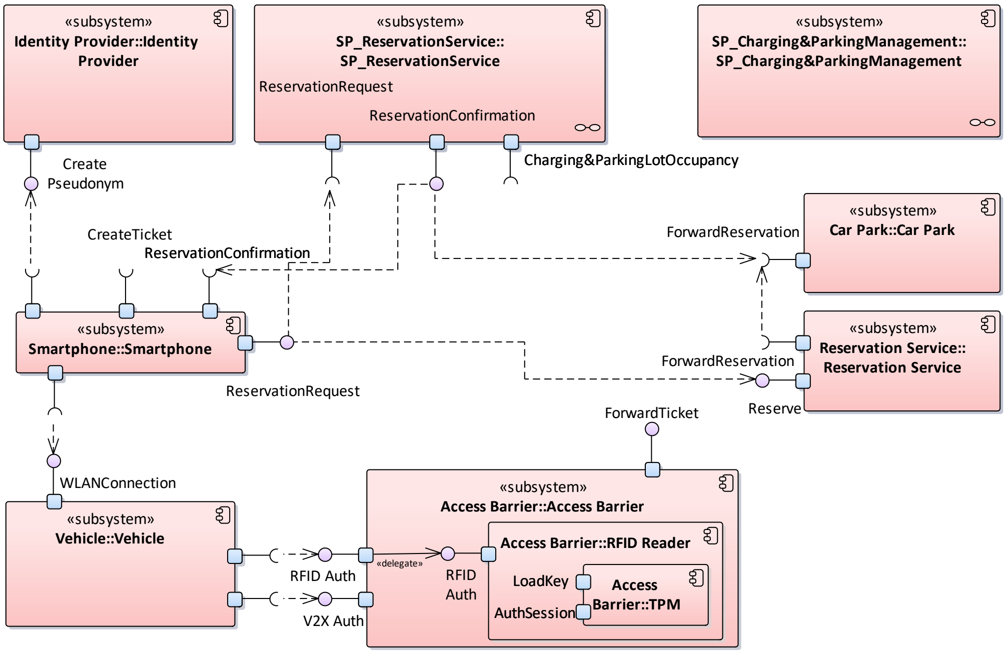


Figure 84: Ticket Authentication System

6.3.4.1 Components

The core components involved are the user's smartphone, the vehicle, the registration and reservation services, and an access barrier.

6.3.4.1.1 Reservation Service

The Reservation Service forwards the reservation requests and tickets to the appropriate car park backend.

STRUCTURAL PART OF Reservation Service
ForwardReservation : Port
Reserve : Port

6.3.4.1.1.1 Interfaces

ForwardReservation

The Reservation Service uses this interface to forward reservation requests to the correct car park backend

Reserve

The smartphone uses this interface to place a reservation request.

6.3.4.1.2 Identity Provider

The Identity Provider manages the active users of the iKoPA system and serves as a trusted third party to authenticate users.

STRUCTURAL PART OF Identity Provider
CreatePseudonym: Port «webservice»

6.3.4.1.2.1 Interfaces

CreatePseudonym

This interface connects the smartphone to the Identity Provider. A pseudonym for a user within the iKoPA system is created via this interface.

6.3.4.1.3 Access Barrier

This is an access barrier in front of a car park.

ELEMENTS OWNED BY Access Barrier
RFID Reader : Component «Subsystem»

STRUCTURAL PART OF Access Barrier
V2X : Port

STRUCTURAL PART OF Access Barrier
ForwardTicket : Port
RFID : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» Access Barrier to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.3.4.1.3.1 Interfaces

V2X Auth

This interface is used by vehicles to authenticate via V2X.

ForwardTicket

This interface provides means to forward the ticket information required to authenticate vehicles (either via V2X or RFID).

RFID Auth

This interface is used by vehicles to authenticate via RFID. It delegates to the RFID Auth interface of the RFID Reader.

6.3.4.1.3.2 Components

The access barrier contains an RFID reader.

6.3.4.1.3.2.1 RFID Reader

The RFID Reader is used to communicate with the RFID tags of the vehicle during the authentication. A TPM is used as a secure element for processing authentication keys.

ELEMENTS OWNED BY RFID Reader
TPM : Component

STRUCTURAL PART OF RFID Reader
RFID Auth : Port

6.3.4.1.3.2.1.1 Interfaces

RFID Auth

This RFID interface is used to authenticate a RFID tag of the vehicle.

6.3.4.1.3.2.1.2 Components

The RFID reader contains a TPM to load and use secret keys for the authentication

6.3.4.1.3.2.1.2.1 TPM

The TPM is used by the RFID reader as a secure element for the keys involved in the authentication process. The ticket includes information about the RFID tags of the car. A secret authentication key is part of this and used during the RFID authentication.

STRUCTURAL PART OF TPM
AuthSession : Port
LoadKey : Port

6.3.4.1.3.2.1.2.1 Interfaces

AuthSession

This interface is used to perform the authentication with loaded keys.

LoadKey

The secret key used during the RFID authentication is loaded into the TPM with this interface.

6.3.4.1.4 SP_Charging&ParkingManagement

Charging & Parking Management is a service that exists in the backend plane. It combines the functionalities of a Charge Point Management with classical citywide parking guidance and additional premium services (like remote charging/parking spot reservation). It provides an interface between electric mobility Service Providers and park-house infrastructure equipped with charging stations.

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_Charging&ParkingManagement to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.4.1.5 Car Park

This component is a stand-in for the car park's backend infrastructure.

STRUCTURAL PART OF Car Park
ForwardReservation : Port

6.3.4.1.5.1 Interfaces

ForwardReservation

The car park receives reservation requests from the reservation service via this interface.

6.3.4.1.6 SP_ReservationService

The reservation service manages reservation requests.

STRUCTURAL PART OF SP_ReservationService
ReservationConfirmation : Port
ReservationRequest : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» SP_ReservationService to «Subsystem» Service Provider [Direction is 'Source -> Destination'.]

6.3.4.1.6.1 Interfaces

ReservationConfirmation

This interface relays reservation confirmations.

ReservationRequest

This interface is used for reservation requests.

6.3.4.1.7 Vehicle

The vehicle needs to be authenticated in front of an access barrier, either via RFID or via V2X. In the case of RFID, an RFID tag attached to the vehicle is authenticated. In the case of V2X, the vehicle relays the authentication information to the user's smartphone.

STRUCTURAL PART OF Vehicle
V2X : Port
RFID : Port
WLANConnection : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» Vehicle to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.3.4.1.7.1 Interfaces

V2X (V2X Auth)

This interface is used to authenticate with the access barrier via V2X.

RFID (RFID Auth)

This interface is used to authenticate with the access barrier via RFID.

WLANConnection

The WLAN Connection is an interface for the smartphone to the vehicle, used to relay authentication information.

6.3.4.1.8 Smartphone

In this case, the smartphone is used during registration, reservation and authentication. During registration, an account is created. With an account, tickets are created. Tickets in turn serve as an authentication method during reservation and in front of the access barrier when V2X authentication is used.

STRUCTURAL PART OF Smartphone
CreatePseudonym : Port
ReservationConfirmation : Port
Reserve : Port
WLANConnection : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» Smartphone to «plane» Remote Station [Direction is 'Source -> Destination'.]

6.3.4.1.8.1 Interfaces

CreatePseudonym
This interface is used by the smartphone to create a Pseudonym for the iKoPA system.

ReservationConfirmation
Confirmation for a reservation is passed over this interface.

Reserve (ReservationRequest)
This interface is used to perform a reservation with the Reservation Service Provider.

WLANConnection
The WLAN Connection is an interface between the smartphone and the vehicle, used to relay authentication information.

6.3.5 Traffic Message Distribution

The Traffic Message Distribution uses the concept of GeoMessages known from the CONVERGE architecture, to combine protocols and concepts from the V2X sector and the broadcast sector. Besides other content and protocols, TPEG is transported via GeoMessages and within the field of GeoMessages lies the responsibility to route the data to the appropriate carriers, regions and receivers. They include DAB as another carrier for GeoMessages, which is a concept that is not known from the CONVERGE architecture. In iKoPA a new adaption layer is needed to tunnel and transport GeoMessages via DAB and to fulfill the specific requirements and concepts of DAB. Via different carriers, the information is distributed as GeoMessages, to the receiver, where it is unpacked, decoded and used as a source of information.

6.3.5.1 Traffic Message Distribution DAB

The Traffic Message Distribution via DAB, has its source at the GeomessagingServerDAB, which is the DAB specific instance of the Geomessaging Server. It is aware of DAB specific concepts, such as DAB specific protocols and services and it provides a stream based input for one or multiple DAB Multiplexers, by using the EDI encapsulation protocol. The DAB Multiplexer must be preconfigured, to accept the data and include it in a specific predefined DAB service, which needs booked capacity and a coordinated service identifier, provided by regulatory authorities. To transport GeoMessages via DAB a specific adaption layer is needed, thus, a new protocol in the DAB specification must be created, that allows setup of DAB services, able to transport GeoMessages on-demand. As soon as the DAB multiplexer has merged the service with the overall DAB ensemble, the chain follows the classic DAB mechanisms. The DAB ensemble data stream is forwarded to one or multiple DAB Transmitter stations at different locations, where the high frequency signal is created and put “on air” via broadcast antennas. All such DAB transmitters, supplied by one DAB Multiplexer, do broadcast on the same frequency, forming a so called “single frequency network” (SFN), that can be received by an unlimited number of DAB receivers, e.g. in vehicles.

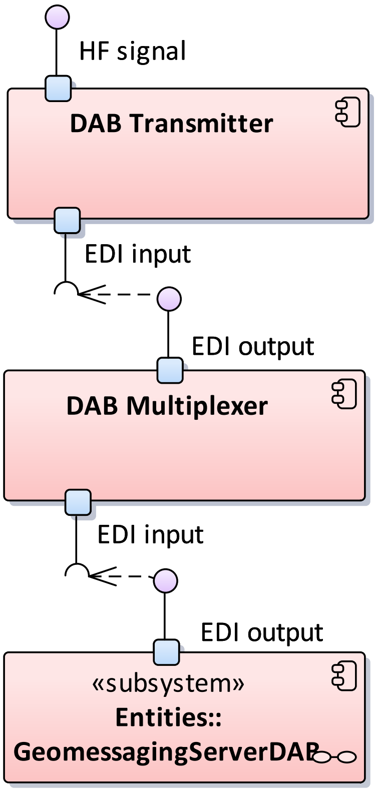


Figure 85: Traffic Message Distribution - DAB

6.3.5.1.1 Components

Both the DAB Transmitter and the DAB Multiplexer are commonly known components in the field of DAB broadcast and are already in use for different operative DAB networks in several countries. The new concept in iKoPA is, to include an adaption layer and protocol to encapsulate GeoMessages in a way that is suitable to be transported via DAB mechanisms. This is done by the GeomessagingServerDAB, which is a variety of the GeomessagingServer, but with enhancement to do the specific DAB handling and encoding. The EDI protocol provided is a common encapsulation mechanism, which is typical for DAB Multiplexers. The DAB Multiplexer combines multiple such inputs to a DAB ensemble by using a given configuration, including identifiers for DAB services.

6.3.5.1.1.1 DAB Transmitter

The DAB transmitter creates the HF (high frequency) signal and is located near the broadcast antenna.

STRUCTURAL PART OF DAB Transmitter
EDI input : Port
HF signal : Port

6.3.5.1.1.1.1 Interfaces

EDI input

EDI ("Encapsulation of DAB Interfaces ") is specified in ETSI TS 102 693 and allows DAB specific protocols to be encapsulated and transmitted by using generic IP-based protocols. It is the default base interface for data provision to DAB multiplexers and to the DAB transmitters, in case that they are connected to IP-based networks (like the internet or separated dedicated IP-based contribution networks).

HF signal

It is a high frequency signal that is broadcasted over the air, using an antenna. The receivers will use an antenna to receive this HF signal and decode it. . For DAB typically multiple transmitters at different locations using the same broadcast frequency form a so called “single frequency network”.

6.3.5.1.1.2 DAB Multiplexer

A DAB multiplexer aggregates and combines various input data streams into one homogenous so-called "DAB ensemble". The combined data stream, containing the DAB ensemble is then contributed to one or more DAB transmitters.

STRUCTURAL PART OF DAB Multiplexer
EDI input : Port
EDI output : Port

6.3.5.1.1.2.1 Interfaces

EDI input

EDI ("Encapsulation of DAB Interfaces ") is specified in ETSI TS 102 693 and allows DAB specific protocols to be encapsulated and transmitted by using generic IP-based protocols. It is the default base interface for data provision to DAB multiplexers and to the DAB transmitters, in case that they are connected to IP-based networks (like the internet or separated dedicated IP-based contribution networks).

EDI output

EDI ("Encapsulation of DAB Interfaces ") is specified in ETSI TS 102 693 and allows DAB specific protocols to be encapsulated and transmitted by using generic IP-based protocols. It is the default base interface for data provision to DAB multiplexers and to the DAB transmitters, in case that they are connected to IP-based networks (like the internet or separated dedicated IP-based contribution networks).

6.3.5.1.1.3 Geomessaging Server DAB

The GeomessagingServerDAB will use the "GeoMessage over DAB" protocol to transport GeoMessages via DAB. It knows about specific features and requirements of DAB and is able to handle them. It has to deal with multiplexing and data rate management, to assure that the GeoMessages that are pending for transmission do fit into the data rate of the predefined DAB sub channels.

STRUCTURAL PART OF GeomessagingServerDAB
EDI output : Port

OUTGOING STRUCTURAL RELATIONSHIPS
Generalization from «Subsystem» GeomessagingServerDAB to «Subsystem» GeomessagingServer [Direction is 'Source -> Destination'.]

ASSOCIATIONS	
Source: Public (Component) GeomessagingServerDAB «Subsystem»	Target: Public (Component) DAB
Source: Public (Component) GeomessagingServerDAB «Subsystem»	Target: Public (Component) GeoMessage Over DAB «protocol»
Source: Public (Component) multiplex & datarate management	Target: Public (Component) GeomessagingServerDAB «Subsystem»

6.3.5.1.1.3.1 Interfaces

EDI output

EDI ("Encapsulation of DAB Interfaces ") is specified in ETSI TS 102 693 and allows DAB specific protocols to be encapsulated and transmitted by using generic IP-based protocols. It is the default base interface for data provision to DAB multiplexers and to the DAB transmitters, in case that they are connected to IP-based networks (like the internet or separated dedicated IP-based contribution networks).

6.3.5.2 Traffic Message Distribution TPEG

The classic concept to distribute TPEG into the vehicle would be to directly insert it into a DAB ensemble. The new idea in the iKoPA approach is, to encapsulate the TPEG into GeoMessages, which are then transported via DAB. This allows a combination of the classical TPEG/DAB approach and the GeoMessages, including all other related protocols and content. The benefit of using GeoMessages is to create a common base to support TPEG through various carriers, not only DAB, but also V2X typical bidirectional and local transmissions. In addition, GeoMessages provide some mechanics to route the content through the appropriate carriers and entities, to reach the vehicle, following a “push on-demand concept”, rather than a “repeated broadcast and re-broadcast” as currently in DAB.

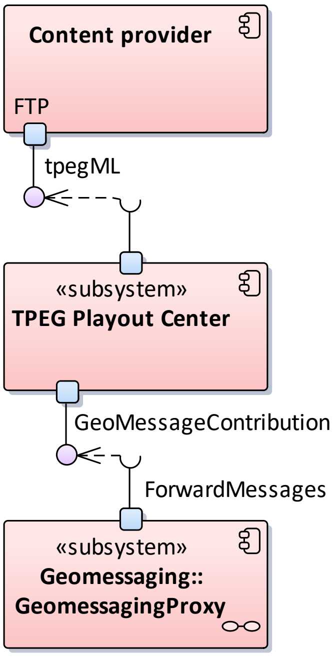


Figure 86: Traffic Message Distribution TPEG

6.3.5.2.1 Components

The classical format used by a content provider (the editorial authority) is tpegML, which is then provided to the TPEG Playout Center that does the binary encoding and the multiplexing strategy. Up to now, the TPEG Playout Center would forward a continuous stream to a DAB multiplexer, but in the iKoPA approach, the TPEG Playout Center provides separated binary objects, each representing one self-contained TPEG based information, enclosed in a single TPEG transport frame. In addition, meta-information is used to tell the GeomessagingProxy about the targeted geolocation. This is necessary, as the GeomessagingProxy shall handle the TPEG transport frame as a black box (BLOB), without the need to decode and to look for location information in it. Therefore, the TPEG Playout Center supports the GeomessagingProxy by giving it straight forward a command where to distribute the given BLOB.

6.3.5.2.2 Content provider

A Content Provider that contributes to a TPEG Service may be any kind of authority or business partner that has valuable information. In terms of TPEG, the Content provider holds responsible for the editorial decisions and is owner of the “originator service identifier”, describing a specific data pool that is managed and maintained by this content provider.

STRUCTURAL PART OF Content provider
⚙ FTP : Port

6.3.5.2.2.1 Interfaces

FTP (tpegML)

The content provider describes its information by using “tpegML”, which is a XML file based on the TPEG data model. These files can be transferred, typically by simple FTP (or similar means) to the TPEG Playout Center.

6.3.5.2.3 TPEG Playout Center

The TPEG Playout Center requires tpegML files and converts it into GeoMessageContribution objects to be used by GeoMessagingProxy.

STRUCTURAL PART OF TPEG Playout Center
⚙ FTP : Port

STRUCTURAL PART OF TPEG Playout Center
GeoMessageContribution : ProvidedInterface

6.3.5.2.3.1 Interfaces

GeoMessageContribution

The idea is to, not only provide the GeoMessages payload as BLOBs, but additional header information, including the targeted region. The TPEG Playout Center therefore makes the decision, which region shall be supplied with the included TPEG information in the BLOB. The GeoMessagingProxy just follows this command, but knows for itself, which means of transport are available for which region and which receivers. To do this, the GeoMessagingProxy does not need to decode the BLOB but just forwards it, and uses the data from the header to make the routing decisions.

FTP (tpegML)

The TPEG Playout Center accepts XML files, following the TPEG model. Each provider maintains message identifiers and version numbers. The TPEG Playout Center creates binary objects, manages them and merges them into combined services and data streams.

6.3.5.2.4 GeomessagingProxy

The GEOM-P is the part of the geomessaging concept that is located in the backend. This is the major entry point for delivery of geomessaging data from the perspective of a C-ITS service. Through the ServiceDirectory, the GeomessagingProxy will obtain a list of GeoMessagingServers offering services for a specific geographic area. In turn, the GeomessagingProxy will offer its services to interested ServiceProviders through the ServiceDirectory including the aggregated area of coverage of the GeoMessagingServers it is connected with. The GeomessagingProxy will connect to one or many GeoMessagingServers, which take over the task to finally distribute the geomessages via different communication networks to the respective geographical areas.

STRUCTURAL PART OF GeomessagingProxy
ForwardMessages : Port

6.3.5.2.4.1 Interfaces

ForwardMessages

The GeomessagingProxy accepts GeoMessages and treats the payload from the TPEG Playout Center as not decodable BLOB data.

6.3.6 Vehicle ITS Station

In the following, the Vehicle ITS Station will be described. This includes a more detailed view of the internal processors, as well as a logical outside view of the component. The V-ITS-Station is the logical unit, which resides in the vehicle and controls the access of the vehicle internals, manages the different communication technologies and provides an application platform. Additionally the vehicle system contains a unit for executing automated driving functions.

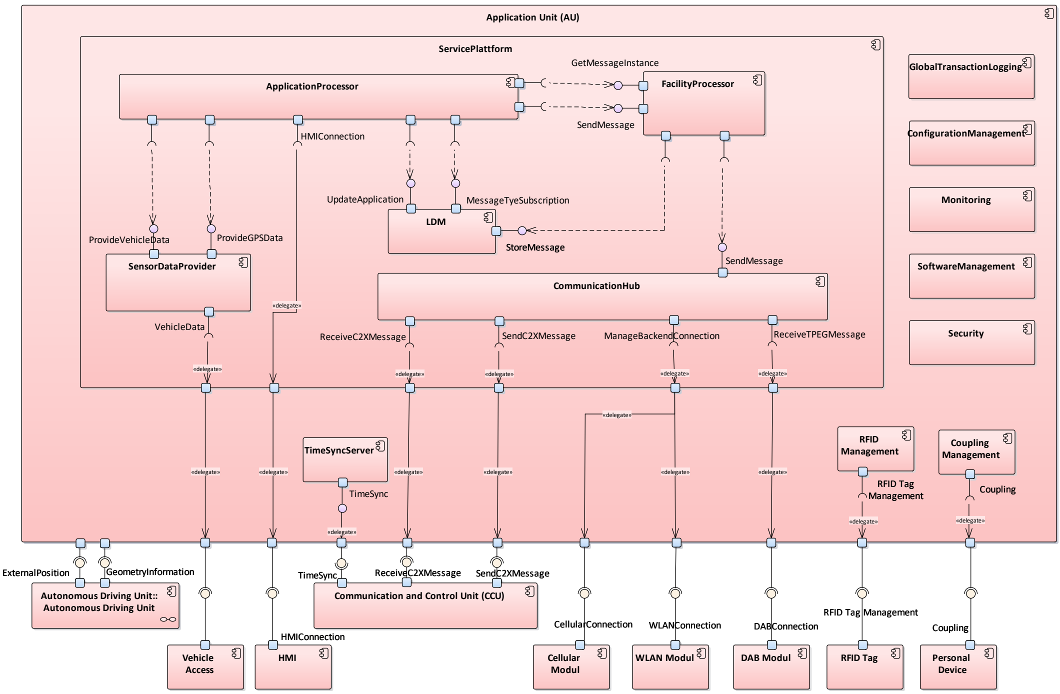


Figure 87: V-ITS-Station

6.3.6.1 Autonomous Driving Unit

The Autonomous Driving Unit is the central unit, which assumes all duties of the human Driver in a manually driven vehicle. It consists of the following four internal components: Collision Check, Position Estimator, Real Time Control Box and Trajectory Calculator. These components will be explained below. The Autonomous Driving Unit receives on one hand information about the driving route and additional sensor data and provides on the other hands commands for steering and acceleration via the interfaces.

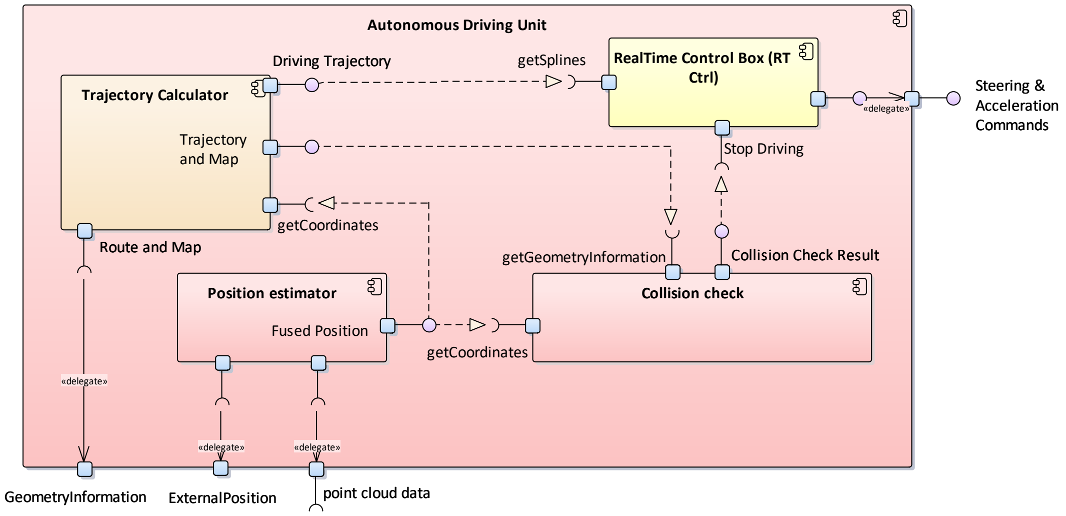


Figure 88: Autonomous Driving Unit

ELEMENTS OWNED BY Autonomous Driving Unit
Collision check : Component
Position estimator : Component
RealTime Control Box (RT Ctrl) : Component
Trajectory Calculator : Component

STRUCTURAL PART OF Autonomous Driving Unit
ExternalPosition : Port
GeometryInformation : Port
Point cloud data : Port
Steering & Acceleration Commands : Port
StopDriving : Port

6.3.6.1.1 Interfaces

ExternalPosition

Via this interface, the Autonomous Driving Unit receives the external position of the vehicle provided by the camera system of the car park as a GPS supplement.

GeometryInformation

Via this interface, the car park provides via this interface the route the vehicle has to drive o parking or charging lot as well as information about the geometrical structure of the car park, like the position of the walls, obstacles, lanes etc.

Point cloud data

This interface provides additional sensor data, e.g. from a Lidar system.

Steering & Acceleration Commands

This interface provides the commands, which directly influences the accelerator pedal, brake pedal and steering.

StopDriving

Over this bidirectional interface, each site can inform the other one in case of an emergency stop. If the car park sends the EmergencyStop the car has to stop immediately. In case the car has to stop for whatever reason, the carpark is informed.

6.3.6.1.2 Components

6.3.6.1.2.1 Collision Check

Based on the current position this component permanently observes the driveway and obstacles in the surrounding.

STRUCTURAL PART OF Collision check
⚙ Collision Check Result : Port
⚙ Fused Position : Port
⚙ Trajectory and Map : Port

6.3.6.1.2.1.1 Interfaces

Collision Check Result (Stop-Driving)
If the CollisionCheck notice a potential crash with an obstacle or other car in the surrounding the Stop-Driving signal will be sent.

Fused Position (getCoordinates)
The unit continuously receives the precise position of the vehicle fused from the external position calculation and from the vehicle's own calculated position information.

Trajectory and Map (getGeometryInformation)
In order to observe the distance to walls and other structural circumstances the Collision Check unit requires the geometry information of the car park.

6.3.6.1.2.2 Position Estimator

The Position Estimator calculates the position of the vehicle based on the Lidar-sensors, odometry system and the external position provided by the cameras of the car park.

STRUCTURAL PART OF Position estimator
External position : Port
Fused Position : Port
Point cloud data : Port

6.3.6.1.2.2.1 Interfaces

External position (getExternalPosition)
The position information of the car detected from the camera system of the car park is received.

Fused Position (setCoordinates)
Precise position of the vehicle based on a sensor fusion of external and internal position values will be sent to other components of the Autonomous Driving Unit.

Point cloud data (ProtocolBuffer)
Point cloud data is received from the Lidar system.

6.3.6.1.2.3 RealTime Control Box (RT Ctrl)

The RealTime Control Box guides the vehicle on the pre-calculated trajectory and ensures the safe drivability. In case of deviations between the current position and pre-calculated trajectory, it steers the vehicle with appropriate control commands back on the optimal track. Furthermore, the RealTime Control Box monitors the proper function of all other components of the Autonomous Driving Unit.

STRUCTURAL PART OF RealTime Control Box (RT Ctrl)
⚙ Collision Check Result : Port
⚙ Driving Trajectory : Port
⚙ Steering & Acceleration Commands : Port

6.3.6.1.2.3.1 Interfaces

Collision Check Result (Stop Driving)

If the Stop-Driving signal is set the RealTime Control Box brakes the vehicle immediately to a standstill and passes the information back to the Car Park Autonomous Driving System (CPADS).

Driving Trajectory (getSplines)

Via this interface the car receives the trajectory consisting of a series of subsequent splines the car has to follow.

Steering & Acceleration Commands

The RealTime Control Box provides via this interface the real commands for steering and acceleration of the car.

6.3.6.1.2.4 Trajectory Calculator

Based on the pre-calculated route the driving trajectory will be identified. The trajectory consists of a series of subsequent splines taking all physical parameters of this particular vehicle into account.

STRUCTURAL PART OF Trajectory Calculator
⚙ Driving Trajectory : Port

STRUCTURAL PART OF Trajectory Calculator
Fused position : Port
Route and Map : Port
Trajectory and Map : Port

6.3.6.1.2.4.1 Interfaces

Driving Trajectory (setSplines)
Based on the pre-calculated route from CPADS the Trajectory Calculator takes all physical parameters of this particular vehicle into account and calculates a trajectory consisting of a series of subsequent splines the car has to follow.

Fused position (getCoordinates)
Via this interface the Trajectory Calculator receives the precise position in geographical coordinates from the Position Estimator.

Route and Map (getGeometryInformation)
The route and the map of the car park is received via this interface.

Trajectory and Map (setGeometryInformation)
This interface passes the calculated trajectory together with the map of the car park to the collision check.

6.3.6.2 Application Unit (AU)

The Application Unit is the core logic component of the V-ITS-Station. It provides a service platform for hosting different services, has several interfaces to different sensors of the vehicle and describes the core communication component of a V-ITS-Station.

ELEMENTS OWNED BY Application Unit (AU)
Coupling Management : Component
Linux OS : Component

ELEMENTS OWNED BY Application Unit (AU)
RFID Management : Component
Security : Component
ServicePlattform : Component

STRUCTURAL PART OF Application Unit (AU)
CellularConnection : Port
Coupling : Port
DABAccess : Port
HMIConnection : Port
provideExternalPosition : Port
provideGeometryInformation : Port
ReceiveV2XMessage : Port
RFID Tag Management : Port
SendV2XMessage : Port
timeSync : Port
VehicleData : Port
WLANConnection : Port

6.3.6.2.1 Interfaces

CellularConnection

This interface is used for connections via a cellular network.

Coupling

The coupling interface lets a user link a personal device with its vehicle.

DABAccess

Interface for DAB+ data access.

HMIConnection

The interface is used to display information to a Human Machine Interface (HMI).

provideExternalPosition

The interface provides the GPS position to other components of the vehicle systems such as the AD Box and the CCU.

provideGeometryInformation

The interface provides geometry information of the car park.

ReceiveV2XMessage

This is an interface to receive V2X messages via the CCU received by ITS G5.

RFID Tag Management

RFID Tags can be managed through this interface. In most cases, this will be adding or changing an RFID Tag to the system.

SendV2XMessage

This interface is used to send V2X Messages via the CCU.

timeSync (provideTimeSync)

This interface provides time synchronization to other subsystems of the vehicle system.

VehicleData

This interface gets vehicle data of a specific interface of the vehicle, like CAN bus.

WLANConnection

This is the interface for IEEE 802.11a/b/g/n/ac Wi-Fi connections.

6.3.6.2.2 Components

6.3.6.2.2.1 Coupling Management

This component manages the coupling of the personal device of a Driver and the vehicle.

STRUCTURAL PART OF Coupling Management
⚙ Coupling : Port

6.3.6.2.2.1.1 Interfaces

Coupling

The coupling interface lets a user link a personal device with its vehicle.

6.3.6.2.2.2 BackendConnectionManager

The BackendConnectionManager handles the routing of the backend connection. In iKoPA a “handover” between mobile communication and standard WLAN will be done by this component.

STRUCTURAL PART OF BackendConnectionManager
⚙ ManageBackendConnection : Port
⚙ SendAndReceive Cellular : Port
⚙ SendAndReceive WLAN : Port

6.3.6.2.2.2.1 Interfaces

ManageBackendConnection

This is the interface used to register and unregister backend connections.

SendAndReceive Cellular

This is the interface to send and receive via cellular communication.

SendAndReceive WLAN

This Interface is used to send and receive signals via standard WLAN.

6.3.6.2.2.3 Configuration Management

This component will handle the configuration of the vehicle system.

6.3.6.2.2.4 DAB Middleware

The DAB Middleware provides an easy way to access DAB and the included TPEG data.

STRUCTURAL PART OF DAB Middleware
⚙ ProvideTPEGMessage : Port
⚙ ReceiveDABStream : Port

6.3.6.2.2.4.1 Interfaces

ProvideTPEGMessage

This interface provides access to TPEG messages received via DAB.

ReceiveDABStream

This interface provides access to the raw DAB stream as received via the DAB receiver. It can be used if other than TPEG messages are included in the DAB stream.

6.3.6.2.2.5 GlobalTransactionLogging

This component offers a global logging of transaction of the system. This includes but is not limited to message sending and receiving, user interactions, vehicle data…

6.3.6.2.2.6 Monitoring

This component will allow the monitoring of the system to detect errors.

6.3.6.2.2.7 SoftwareManagement

The SoftwareManagement component will handle installation and updates of the system.

6.3.6.2.2.8 TimeSyncServer

This component provides a time synchronization mechanism to the system.

STRUCTURAL PART OF TimeSyncServer
provideTimeSync : Port
receiveTime : Port

6.3.6.2.2.8.1 Interfaces

provideTimeSync (TimeSync)

Provides time synchronization to other subsystems of the vehicle system.

6.3.6.2.2.9 RFID Management

This component handles the RFID Tag, which should be coupled to the system.

STRUCTURAL PART OF RFID Management
RFID Tag Management : Port

6.3.6.2.2.9.1 Interfaces

RFID Tag Management

RFID Tags can be managed through this interface. In most cases, this will be done by adding or changing (the identification of) a RFID Tag to the system.

6.3.6.2.2.10 Security

This component should provide security related services and enforce a system wide security policy. It should be present at any time.

6.3.6.2.2.11 ServicePlattform

The ServicePlattform provides a service-oriented environment for applications to interact with the system.

ELEMENTS OWNED BY ServicePlattform
ApplicationProcessor : Component

ELEMENTS OWNED BY ServicePlattform
CommunicationHub : Component
FacilityProcessor : Component
GeomessagingClient Cellular : Component
LDM : Component
SensorDataProvider : Component
TimeSyncProxy : Component

STRUCTURAL PART OF ServicePlattform
BackendConnection : Port
HMIConnection : Port
ReceiveV2XMessage : Port
SendV2XMessage : Port
timeSync : Port
VehicleData : Port

6.3.6.2.2.11.1 Interfaces

BackendConnection

This interface provides a backend connection to the services.

HMIConnection

This interface is used to control what should be displayed on an HMI and to interact with the user.

ReceiveV2XMessage

This interface is used to receive V2X Messages via the CCU.

SendV2XMessage

This interface is used to send V2X Messages via the CCU.

VehicleData

This interface is used to receive vehicle specific data.

6.3.6.2.2.11.2 Components

In the following section, the components of the service platform are described.

6.3.6.2.2.11.2.1 ApplicationProcessor

The application processor describes a logical component, which unifies all services or applications.

STRUCTURAL PART OF ApplicationProcessor
GetMessageInstance : Port
GPSData : Port
HMIConnection : Port
MessageTypeSubscription : Port
SendMessage : Port
UpdateApplication : Port
VehicleData : Port

6.3.6.2.2.11.2.1.1 Interfaces

GetMessageInstance
This interface is used to get message containers of various types, like CAM, DENM, SAM etc.

GPSData
Through this interface, GPS (GNSS) data is provided to the services.

HMIConnection
This interface is used to control what should be displayed on an HMI.

MessageTypeSubscription
To receive a specific message type the service needs to subscribe at the Local Dynamic Map (LDM). The LDM will then trigger the service at every new incoming message of the subscribed type.

SendMessage
This interface is used to send a message.

UpdateApplication
As described for the interface MessageTypeSubscription, this is the interface to push the new incoming message to message subscribers.

VehicleData
This interface is used to get vehicle specific data, like speed, heading etc.

6.3.6.2.2.11.2.2 CommunicationHub

Controls which way a message will take. It will handle incoming message of all technologies and controls via which communication technology a message will be sent.

STRUCTURAL PART OF CommunicationHub
⚙ ManageBackendConnection : Port
⚙ ReceiveV2XMessage : Port
⚙ ReceiveTPEGMessage : Port
⚙ SendV2XMessage : Port

STRUCTURAL PART OF CommunicationHub
SendMessage : Port

6.3.6.2.2.11.2.3 Interfaces

ManageBackendConnection
This interface manages over which backend connection the message can be sent. This should be done in a best effort way.

ReceiveV2XMessage
This interface is used to receive V2X Messages via the CCU.

ReceiveTPEGMessage
This interface is used to receive TPEG Messages.

SendV2XMessage
This interface is used to send V2X Messages via the CCU.

SendMessage
Through this interface, a message is given to the CommunicationHub for sending a message.

6.3.6.2.2.11.2.4 FacilityProcessor

This component manages messages, e.g. the creation of messages and storing them in an LDM. Furthermore, it provides some protocol logic for further message processing.
.

STRUCTURAL PART OF FacilityProcessor
GetMessageInstance : Port
SendMessage : Port
SendMessage : Port
StoreMessage : Port

6.3.6.2.2.11.2.4.1 Interfaces

GetMessageInstance
This is an interface, which provides a specific message instance, like CAM or DENM, to a service with pre-filled values.

SendMessage
This interface is used to receive message from applications to be pre-processed and forwarded to the communication hub.

SendMessage
This is an interface, which sends the message to the communication hub for further sending.

StoreMessage
This is an interface to store an incoming message in the LDM.

6.3.6.2.2.11.2.5 LDM

The Local Dynamic Map stores incoming messages and provides an interface to subscribe to a specific message type.

STRUCTURAL PART OF LDM
MessageTypeSubscription : Port
StoreMessage : Port
UpdateApplication : Port

6.3.6.2.2.11.2.5.1 Interfaces

MessageTypeSubscription
To receive a specific message type a service needs to subscribe at the LDM. The LDM will then trigger the service at every new incoming message of the subscribed type.

StoreMessage
This interface is provided to the FacilityProcessor to store incoming messages.

UpdateApplication

This interface is used to trigger an application/service when a new message was received of the subscribed type.

6.3.6.2.2.11.2.6 SensorDataProvider

The SensorDataProvider is an entity to collect sensor data of the vehicle and provides that information to the system and the services.

STRUCTURAL PART OF SensorDataProvider
ProvideGPSData : Port
ProvideVehicleData : Port
vehicleData : Port

6.3.6.2.2.11.2.6.1 Interfaces

ProvideGPSData

This interface is used to provide GPS (GNSS) data to all services.

ProvideVehicleData

This interface is used to provide vehicle data to all services

vehicleData

Through this interface the vehicle data is collected by the ServiceDataProvider.

6.3.6.3 Cellular Module

This hardware component is used for cellular communication.

STRUCTURAL PART OF Cellular Module
CellularConnection : Port

6.3.6.3.1 Interfaces

CellularConnection

Interface to describe the cellular connection of the system.

6.3.6.4 Communication and Control Unit (CCU)

The Communication and Control Unit handles the V2X communication. Therefore, it is able to send and receive V2X Messages.

STRUCTURAL PART OF Communication and Control Unit (CCU)
ReceiveV2XMessage : Port
SendV2XMessage : Port
TimeSync : Port

6.3.6.4.1 Interfaces

ReceiveV2XMessage

This is an interface to receive V2X Messages.

SendV2XMessage

This is an interface to send V2X Messages.

TimeSync

This is an interface to synchronize the time between the systems.

6.3.6.5 DAB+ Modul

This is the hardware DAB+ Module. This component is used to receive DAB+ streams and to subscribe to a TPEG services.

STRUCTURAL PART OF DAB Modul
DAB+Connection : Port

6.3.6.5.1 Interfaces

DAB+Connection

This is an interface to describe the DAB+ connection.

6.3.6.6 HMI

The Human Machine Interface is a component to display information to the Driver and lets the Driver actively interact with the vehicle system.

STRUCTURAL PART OF HMI
HMIConnection : Port

6.3.6.6.1 Interfaces

HMIConnection

This is an interface to receive Driver interactions and to display important information to the Driver.

6.3.6.7 Personal Device

This is a Personal Device of the Driver. In most cases, this will be a smartphone.

STRUCTURAL PART OF Personal Device
Coupling : Port

6.3.6.7.1 Interfaces

Coupling

This interface is used to couple the personal device with the vehicle to have a unique and clear connection.

6.3.6.8 RFID Tag

This component is the hardware RFID Tag. Currently this is a one-time preconfigured tag. In the future, this will be a programmable tag with dynamically changed identifications.

STRUCTURAL PART OF RFID Tag
RFID Tag Management : Port

6.3.6.8.1 Interfaces

RFID Tag Management

This interface is used to manage RFID Tags. This should be used to couple decoupled RFID tags to the system. In the future, this should be used as an API for RFID Tag programming.

6.3.6.9 Vehicle Access

This is a component, which handle the access of vehicle data.

STRUCTURAL PART OF Vehicle Access
VehicleAccessControl: Port

6.3.6.9.1 Interfaces

VehicleAccessControl

This interface is used to control and receive vehicle data of the vehicle

6.3.6.10 WLAN Module

This is a standard IEEE 80.11 Wi-FI Module.

STRUCTURAL PART OF WLAN Modul
WLANConnection : Port

6.3.6.10.1 Interfaces

WLANConnection

This is an interface to describe the WLAN connection.

7 CONCLUSION

To sum up the architecture document of iKoPA, a technical summary is presented emphasizing the key points of the proposed architecture. But first a short synopsis about the current legal framework from a data protection point of view is presented.

7.1 Data protection and the architecture

A data protection preserving integration of services in the ecosystem of automated and connected vehicles has to comply with the relevant data protection laws, particularly the General Data Protection Regulation (EU) 2016/679[21] (GDPR). The GDPR is the new legal framework that lays down rules for the protection of natural persons with regard to the processing of their personal data and has been directly applicable in all European Member States since 25 May 2018.

Whenever personal data is involved, the controller of a processing activity must comply with the requirements of the GDPR. In the context of connected vehicles, personal data covers all vehicle data that can be linked to an identified or identifiable person (e.g. driver, vehicle owner, passenger or even a person outside the vehicle). In particular, all messages containing a unique identifier such as authorization certificates or a header with timestamp and location can be linked to a natural person and therefore the majority of vehicle data must be considered personal data.[22] Even technical data that describes the state of the vehicle or its parts, including data relating to the wear of the vehicle (such as the age of vehicle parts or the mileage of the engine), often reveal information about using habits (e.g. the driving style) that can be attributed to the owner and can constitute a behavior profile. Biometric data of drivers or geolocation data can also be used to identify persons and compile movement profiles.

The GDPR mandates to identify, analyze, assess, and mitigate the risks to the rights and freedoms of individuals posed by each processing operation on personal data. This risk-based approach primarily concerns the fundamental rights to data protection and informational self-determination (Articles 7 and 8 of the Charter of Fundamental Rights of the EU). Even legitimate data processing may pose risks for individuals, especially when

[21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[22] Article 29 Data Protection Working Party, Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS), Working Paper 252, online: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47888

new technologies or forms of communication are involved, as is the case for connected vehicles.

Controllers who process personal data shall implement technical and organizational measures to achieve and demonstrate compliance with the GDPR (Articles 24, 25, 32 GDPR). The basic data protection principles to be applied are set out in Article 5 (1) GDPR. Personal data shall be processed lawfully, fairly and transparently, collected for specified, explicit and legitimate purposes, based on accurate data, protected against loss, destruction or damage, and handled in a way that ensures their integrity and confidentiality. Articles 12–22 grant certain rights to data subjects, such as the right to erasure (Article 17 GDPR) or the right to data portability (Article 20 GDPR). Furthermore, the GDPR requires to implement appropriate measures already in the design phase in order to safeguard the right to informational self-determination and the data protection principles (data protection by design (Article 25 (1) GDPR) and that default settings foresee that only the necessary personal data are processed (Data Protection by Default, Article 25 (2) GDPR).

The GDPR states requirements at a high level of abstraction such that a transformation to the operational level is necessary. Therefore, the methodology of the Standard Data Protection Model [23] (SDM) was employed to identify appropriate risk mitigation measures. The Conference of the German Independent Data Protection Authorities of the Bund and the Länder has formally recommended the SDM. The SDM categorizes the different measures based on protection goals that meet the required standards of the GDPR. [24] Seven fundamental protection goals have been identified, namely data minimization as the underlying principle, availability, integrity, confidentiality, unlinkability, transparency, and intervenability.[25] Based on these protection goals, the possible sources of risks were identified. Also, the levels of interference and necessary protection were investigated. On this basis, the necessary requirements in section 5 were developed.

A data protection enhancing solution should support anonymization and pseudonymization to the extent possible and where implementation is not possible now foresee this as relevant option for the future. Using purpose-specific pseudonyms

[23] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Das Standard Datenschutzmodell Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V 1.1 – Erprobungsfassung; also available English translation: DSK, The Standard Data Protection Model (SDM), V.1.0 – Trial Version; latest versions and translations online at: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/.

[24] DSK, SDM, V.1.0, 23 ff.

[25] DSK, SDM, V.1.0, 25 f.

supports unlinkability. The implementation of privacy-preserving attribute-based credentials (privacy-ABCs) mitigates the inherent risk of abuse by trusted third parties and should be favored when possible. When a trusted party is involved, its trustworthiness shall be regulated and monitored.

To fully support the rights of the individuals and fulfil the obligations of the controller under the GDPR, a data protection preserving system design of an integrated service minimizes the risk of privacy breaches, informs vehicle users about basic data protection related aspects, enables them to gain self-determined control over the access to their data, and minimizes the access to vehicle generated data. Therefore, data minimization shall proactively be exercised by not collecting in the first place or erasing personal data as soon as possible and thus effectively reducing the volume and storage duration of data. Data protection preserving design also ensures protection against unauthorized modifications and deletion, as well as unlawful processing. It ensures secure authentication and encryption of data at rest, in use, and in transit. Transparency requires that any information and communication relating to the processing of personal data be easily accessible and easy to understand ("concise, transparent, intelligible", Article 12 GDPR) and that clear and plain language be used. It can be presented in writing or by other means, including – were appropriate – by electronic means in a machine-readable format and provided free of charge. Standardized icons could be used to give an easily intelligible and meaningful overview of the intended processing (Article 12 (7) GDPR). Provisions in support of the data subjects' rights to intervene must be implemented. Operational possibilities are for example the rights of access, rectification, erasure, restriction, and data portability (Articles 16 – 20 GDPR) as well as differentiated options for consent, withdrawal of consent (Article 7 GDPR), and objection (Article 21 GDPR).

The legal considerations summarized above have been laid forth in German language in the iKoPA-Document "D3: Datenschutzanalyse und Handlungsempfehlungen", foreseen for publication in 2018.

7.2 Résumé

The research project iKoPA aims to design a secure and data-protection friendly ITS architecture. This architecture should incorporated different communication technologies and also fulfill the needs of applications in the context of electric mobility and connected and automated driving (CAD).

With the visionary scenario, a starting point to visualize the application families that should be addresses with the architecture was created. This scenario includes automated driving, interaction between the vehicle and the (traffic) infrastructure and the role of the human driver resp. vehicle passenger. Also the communication requirements were addressed in the scenario. In the end, all major project goals could be included. Twelfth use case were derived from the scenario. The use cases include detailed description about the involved actors, technical components and the steps that have to be taken, to conclude the use case.

In the next step, the use cases were analyzed regarding their communication requirements. Following, the status quo of the communication architectures (the CONVERGE architecture in particular, because iKoPA is an extension of the CONVERGE architecture), communication technology, security and electric mobility was surveyed. Those information in combination with use cases were the basis to formulate the requirements. In total, 156 requirements were defined within three categories: privacy, security and architecture. It has to be noted that requirements that have already be addressed by the CONVERGE architecture were not formulated again.

Finally, the iKoPA architecture was defined. It was specified in two layers: a high-level architecture to provide an overview and a low-level architecture to provide more detailed information. The architecture includes concepts for secure communication and pseudonymous service usage. Different communication technologies like IEEE802.11p automotive wireless LAN, cellular communication, RFID communication and communication via DAB+ were also included, and the architecture is also open to facilitate more and different communication technologies. Additionally, concepts for geographical message distribution were extended. The aforementioned security and privacy concepts were included from the start so that components and interfaces have been design directly with these topics in mind. This should guarantee that all system components are designed in such a way, that security and privacy are an inherent part of the system by default.

The architecture was starting point for the implementation of a real world demonstration scenario. The experiences with the architecture during the implementation phase were collected and necessary changes were included in the current version of the architecture as described in this document.

Concluding, the iKoPA architecture combines modern communication technologies, security mechanisms and privacy concepts. To implement this architecture further work is necessary, due to the fact that not all interface and components are defined in total and to the bit. Nevertheless, the architecture is big step forward for an all secure, privacy-friendly, state of the art ITS communication architecture.

8 BIBLIOGRAPHY

[1] „CONVERGE Deliverable D4.3 "Architecture of the Car2X Systems Network“," CONVERGE, 2015.

[2] B. W. Kroeger und P. J. Peyla, „Compatibility of FM hybrid in-band on-channel (IBOC) system for digital audio broadcasting,“ In IEEE Trans. on Broadcast. 43 (4), pp. 421–430., DOI: 10.1109/11.664025, 1997.

[3] „What is DAB Digital Radio Tutorial,“ Electronics Notes, https://www.electronics-notes.com/articles/audio-video/broadcast-audio/digital-radio-audio-broadcasting-dab-tutorial.php, 2016.

[4] W. Hoeg und T. Lauterbach, „Digital audio broadcasting. Principles and applications,“ John Wiley & Sons Ltd, West Sussex PO19 8SQ, England, 2003.

[5] T. T. a. S. Committee, „TPEG - What is it all about? A guideline for understanding TPEG quickly!,“ TISA, http://tisa.org/wp-content/uploads/documents/TISA14001TPEGWhatisitallabout2014.pdf, 2014.

[6] C. Gemini, „TPEG VERSUS RDS-TMC: THE TRUTH IS OUT THERE…,“ Traffic technology international, Surrey, UK : UK & International Press, 1999.

[7] R. Goel, „Implementation of a TPEG Decoder, Master Thesis,“ Universität zu Lübeck, Arbeitsbereich Softwaresysteme, https://www.ifis.uni-luebeck.de/~moeller/publist-sts-pw-and-m/source/papers/2006/goel06.pdf, 2006.

[8] Wikipedia, „IEEE 802.11p,“ Wikimedia Foundation, Inc., https://en.wikipedia.org/wiki/IEEE_802.11p, 2017.

[9] ETSI, „ETSI EN 302 665 - Intelligent Transport Systems (ITS); Communication Architecture,“ ETSI , Sophia Antipolis Cedex, France, 2010.

[10] N. Semiconductors, „SL3S5002N0FUD: UCODE DNA,“ NXP Semiconductors, http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/ucode-dna/ucode-dna:SL3S5002N0FUD, 2017.

[11] N. Semiconductors, „UCODE(C) DNA,“ NXP Semiconductors, http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/ucode-dna:MC_1436185909808, 2017.

[12] W. Arthur, D. Challener und W. K. Goldman, A Practical Guide to TPM 2.0, Apress, 2015.

[13] A. J. Menezes, S. A. Vanstone und P. C. Oorschot, Handbook of Applied Cryptography, CRC Press, Inc., 1996.

[14] A. Greenberg, „Radio Attack Lets Hackers Steal 24 Different Car Models,“ https://www.wired.com/2016/03/study-finds-24-car-models-open-unlocking-ignition-hack/, 2016.

[15] B. B. d. E.-. u. Wasserwirtschaft, „BDEW Codes,“ https://bdew-codes.de/Codenumbers/EMobilityId/OperatorIdList, 2017.

[16] „Global EV outlook 2016, Global EV outlook 2015,“ International Energy Agency: IEA, www.iea.org, 2016.

[17] „Overview of electromobility standards,“ Deutsches Institut für Normung e.V. DIN, www.din.de, 2016.

[18] „Standardization of EV Recharging Infrastructures,“ North Sea Region Electric Mobility Network, www.e-mobility-nsr.eu, 2013.

[19] „Project Site,“ Chademo allIanz, 2016. [Online]. Available: www.chademo.com.

[20] „Design Guide,“ The Charging Interface Initiative: CharIN e.V., www.charinev.org.

[21] „The V2G interface according to ISO/IEC 15118, Deliverable FP7-314151,“ EMERALD Project, www.fp7-emerald.eu, 2016.

[22] „ACEA position and recommendations for the standardization of the charging of electrically chargeable vehicles (Ref.ACEA 20120501att01),“ European Automobile Manufacturers Association, https://www.acea.be, 2012.

[23] „Deploying publicly accessible charging infrastructure for electric vehicles: how to organise the market?,“ The Union of the Electricity Industry: EURELECTRIC, www.eurelectric.org, 2013.

[24] „Protocols OCPP,“ Open Charge Alliance, http://www.openchargealliance.org.

[25] „Open Clearing House Protocol Dokumentation,“ Open Clearing House, www.ochp.eu.

[26] „Protocols OSCP,“ Open Charge Alliance, http://www.openchargealliance.org.

[27] „General Procurement Guidance for electric vehicle charge points,“ UK Electric Vehicle Supply Equipment Association, www.ukevse.org.uk.

[28] A. T. d. K. d. u. D. d. B. u. d. Länder, „Das Standard-Datenschutzmodell,“ AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, https://datenschutzzentrum.de/artikel/954-.html, 2016.

[29] M. Hansen, M. Jensen und M. Rost, „Protection Goals for Privacy Engineering,“ IEEE, IEEE Security and Privacy Workshops, San Jose, CA, 2015.

[30] S. Bradner, „Key words for use in RFCs to Indicate Requirement Levels,“ Network Working Group , https://www.ietf.org/rfc/rfc2119.txt, 1997.

[31] ETSI, „ETSI EN 300401 - Radio Broadcasting Systems; Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers,“ ETSI, http://www.etsi.org/deliver/etsi_en/300400_300499/300401/01.04.01_60/en_300401v010401p.pdf, 2006.

[32] E. W. Schuster, S. J. Allen und D. L. Brock, „Global RFID. The value of the EPCglobal Network for supply chain management,“ KY: Springer, Berlin, Lexington, 2010.

[33] 9. K. d. u. D. d. B. u. d. Länder, „Das Standard-Datenschutzmodel,“ AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der , Schwerin, 2016.

9 TERMS AND ABBREVIATIONS

Term & Abbreviation	
AA	Authorization Authority
AU	Application Unit
BLOB	A message for that the content is not known and has not to be known. Some kind of black box.
BYOD	Bring Your Own Device
C2X-IX	Car2X Initialization Body
CA	Certificate Authority
CAM	Cooperative Awareness Message
CCU	Communication and Control Unit
CEL-N	Cellular Network
CN	Communication Network
CPADS	Car Park Autonomous Driving Support
CSA	Contract Supervision Authority
DAB	Digital Audio Broadcast
DAB-N	DAB Network
DENM	Decentralized Environmental Notification Message
eMBMS	evolved Multimedia Broadcast Multicast Service
EA	Enrolment Authority
EPB	Exception Posting Board
ETSI ITS-G5	European Telecommunications Standards Institute ITS G5, European IEEE 1609 equivalent for V2X communication via wireless LAN
EV	Electric Vehicles
ETA	Estimated Time of Arrival
GEOM-P	Geo Messaging Proxy
GEOM-S /GEOMS	Geo Messaging Server (-D = DAB, -G = ITS G5, -C = Cellular)
HTTP	Hyper Text Transfer Protocol
IDP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
iKoPA	Integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge
IRS	Roadside ITS station
IRS-N	IRS Network
ITS	Intelligent Transportation Systems
IVS	Vehicle ITS station
LAN	Local Area Network
LDM	Local Dynamic Map
LTCA	Long Term CA
MESP	Mobile Edge Service Provider
MPB	Misbehavior Posting Board
PCA	Pseudonym CA
RCA	Root CA
RESS	Reservation Service
RFD-N	RFID Network
RFID	Radio-frequency Identification
RT Ctl	Real Time Controller
SD	Service Directory
SP	Service Provider
STC-I	Service Test and Certification Institute
TISA	Traveller Information Services Association
TLF	Traffic Light Forecast
TPEG	Transport Protocol Experts Group from the TISA
TPEG-EMI	Electric mobility Information
TPEG-PKI	Parking information application

TPEG-TEC	Traffic event compact application
TSS	Time synchronization server (-B = Backend, -C = Communication Network, -R = Remote Station)
V2X	Vehicle to X communication (comprises Vehicle to Vehicle (V2V) and Vehicle to Infrastructure communication (V2I), sometime also the terms C2C, C2I and C2X are used, whereby C stands for Car)
Wi-Fi	Wireless Fidelity. Technology for wireless local area networking based on the standard IEEE 802.11.