CONVERGE

CONVERGE

COmmunication Network VEhicle Road Global Extension

Proposal for a Car2X Systems Network

Deliverable D3

Functional Requirements and Architecture Options

Version	1.1
Dissemination Level	Public
Project Co-Ordination	HTW
Due Date	30.09.2013
Date of Preparation	30.09.2013

Supported by

Federal Ministry
of Education
and Research

Federal Ministry
of Economics
and Technology

on the basis of a decision by the German Bundestag

This document was prepared by the CONVERGE Project Office
(K&S GmbH Projektmanagement).

Project coordination

Prof. Dr. Horst Wieker
HTW - University of Applied Sciences
Department of Telecommunications
Campus Alt-Saarbrücken
Goebenstr. 40
D-66117 Saarbruecken
Germany

Telefon	+49 681 5867 195
Fax	+49 681 5867 122
E-mail	wieker@htw-saarland.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:

Arno Spinner	BASt
Lutz Rittershaus	BASt
Teresina Herb	BASt
Levent Ekiz	BMW
Oliver Klemp	BMW
Dennis Lenz	BMW
Kurt Eckert	Bosch
Hans Löhr	Bosch
Florian Wildschütte	Bosch
Alexander Federlin	Ericsson
Friedhelm Ramme	Ericsson
Daniel Angermaier	Fraunhofer
Alexander Kiening	Fraunhofer
Dieter Heussner	Hessen Mobil
Manuel Fünfrocken	HTW
Jonas Vogt	HTW
Matthias Mann	PTV
Carsten Büttner	Opel
Harald Berninger	Opel
Tobias Rückelt	Opel
Jürgen Caldenhoven	Vodafone
Sebastian Gräbner	Vodafone
Thomas Lang	Tactilo
Bernd Lehmann	Volkswagen

Revision and History Chart

Version	Date	Description
0.1	22.03.2013	Initial version with proposal for document structure
0.9	27.09.2013	Intermediate Version for Team Review
1.0	30.09.2013	Final Version for delivery at M1
1.1	18.10.2013	Inclusion of Inputs from final Review

Table of Content

Figures

Tables

EXECUTIVE SUMMARY

In the past years there has been tremendous progress in intelligent transport systems in the domains of traffic management, driver assistance and driver information. However most of the solutions that are existing today lack of a common overall system architecture that is providing solutions for a flexible interaction between service providers, service subscribers and the communication infrastructures in between. Scalability, IT-security, decentralization and operator openness are some of the most important properties that a technically and commercially successful solution must provide. The CONVERGE project is aiming to close this gap by defining a Car2X Systems Network architecture capable of fulfilling the aforementioned goals.

Based on the deliverable D1.1, which is defining a comprehensive set of use-cases accompanied by a few representative user stories, this document - deliverable D3 - is elaborating a more detailed view including in depth interaction sequence charts in different phases of the life cycle of the system and its components. This detailed technical view on the given use-cases is helping to further detail the overall system with respect to

- functional components that are necessary to realize the use-cases,
- technical requirements that have to be taken into account in the detailed architecture concept and
- decisions that need to be made with respect to architecture and functional options.

Building on the detected detailed requirements and components an overview of the basic architecture of the Car2X Systems Network is provided. The most important and architecture relevant technical questions are further analyzed with respect to possible solutions and the related advantages and disadvantages.

So this document provides the detailed foundation for the next steps of the definition of the detailed Car2X Systems Network architecture which are going to be performed in the course of the CONVERGE project and which will form the deliverable D4.

1 OVERVIEW

1.1 System Overview

The CONVERGE project aims to design and verify a system architecture for flexible interaction between different service providers and communications network operators in a decentralized, scalable structure.

The Car2X Systems Network will establish a completely new open communication-, services-, and organization architecture that reflects communication technologies and technologies of IT security at state of the art. Through well-defined access methods service providers like traffic control centers or vehicle manufacturers can be integrated into the open and secure system network. The ultimate goal is the decentralized and dynamic coupling of all systems and actors across national and organizational borders in an open, but secure, distributed, trans-regional/international connecting, provider-independent, scalable, flexible and hybrid communicating Car2X Systems Network.

1.2 Document Overview

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

- to introduce the Car2X Systems Network as a concept for the interconnection of Mobile Nodes using different access technologies on the one hand and service providers and users of ITS systems on the other hand,
- to provide a set of architectural and technical requirements,
- to present constraints considered from different viewpoints as the vehicle side, service operators, operational aspects, standardization and regulation and security,
- to present architecture options and
- to introduce the reference architecture for the Car2X Systems Network in CONVERGE.

Figure 1shows the process for work package WP2 and the interaction with other WPs according to the description of work. As can be seen the output of WP2 are technical constraints, architecture options and the reference architecture which will be used as input for further activities in WP2 to WP8. This output is provided by WP2 and documented in Deliverable D3. The delivery of D3 is part of the first milestone in the CONVERGE project.

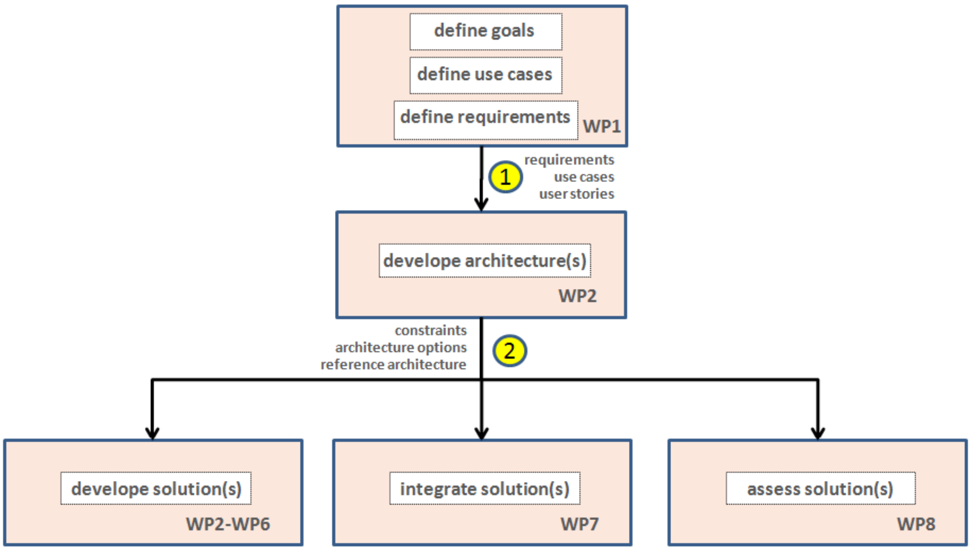

Figure 1: Process Overview

1.2.1 Document Structure

This document is arranged as follows:

- **Chapter 2** - gives an introduction into the architecture understanding within the CONVERGE project, the used methodology and tools for the description of the architecture as well as the interfaces to and working assumptions for interfacing with other work packages.
- **Chapter 3** - lists the architectural constraints and technical requirements including the general approach taken for the definition of technical requirements based on a list of functional requirements, the architectural constrains and the technical requirements.
- **Chapter 4** - presents different options for the CONVERGE architecture reflecting the given requirements and state of the art and applicability of the different solutions.
- **Chapter 5** - provides an overview of the chosen reference architecture and therefore is the basis for the implementation work in WP2 to WP6.

2 INTRODUCTION

2.1 Architecture understanding in CONVERGE

Before the details of the overall system architecture of the C2X systems network ("C2X Systemverbund") can be specified, it is very important to get a common clear understanding of the meaning and the properties of architecture in the CONVERGE context.

The remainder of this subchapter depicts this common understanding that has been elaborated as one of the first activities in the workflow of WP2.

There are different models existing that define the concept of system architecture. Based on these existing models we will figure out the way we are going to define the system architecture concept for CONVERGE.

2.1.1 Architecture concept in the V-Model

One of the existing models is the V-Model (see details at: "http://v-modell.iabg.de/v-modell-xt-html-english/index.html" and the overview in Figure 2). In this model the definition of the system architecture is part of the system design which is based on the output of the system specification process. Besides the creation of the system architecture system design additionally specifies concepts for implementation, integration and test.

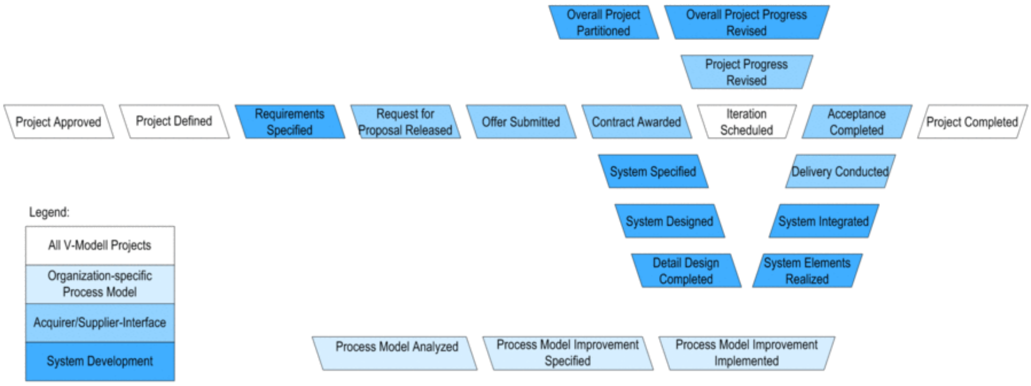

Figure 2: V-Model Decision Gates and Project Execution Strategies [Source: V-Model Description]

The system architecture itself in this model consists of the following elements:

- Architecture principals and design alternatives:
  Architecture principals are requirements that are important for the architecture design. This could be e.g. the decision for a distributed system or the overall security concept.
  Design Alternatives are describing different possibilities of the decomposition of the system in segments (hardware components, software components, external components). The architecture design has to take into account these alternatives and make a decision on the most suitable ones for the given system.

- System decomposition:
  This is the definition of the static structure of the system. It describes the breakdown of the system into segments and of the segments into elements and their interactions and relationships.

- Cross sectional system properties:
  The cross sectional properties of software systems are e.g. transaction requirements, data persistence, requirements for tracing and logging.

- Interface Overview:
  Gives an overview of all interfaces of the overall system. Interfaces of different levels of the system are taken into account:
  - Interfaces between systems or interfaces of one system to the outside world.
  - Interfaces between segments inside the system.
  - Interfaces between elements inside of a segment.

- Overall data catalogue:
  Systems and system elements are exchanging data in communicating with each other. The overall data catalogue of the system describes all data structures and signals which are exchanged via interfaces. It also describes possible data values and constraints.

- Design verification:
  After having decided on a reference architecture the design verification is proving that the chosen system architecture is implementing the given requirements.

- System elements to be specified:
  For the more complex system elements it is necessary to add a detailed specification for each of those elements.

The creation of the system architecture itself is an iterative process which is shown in Figure 3:

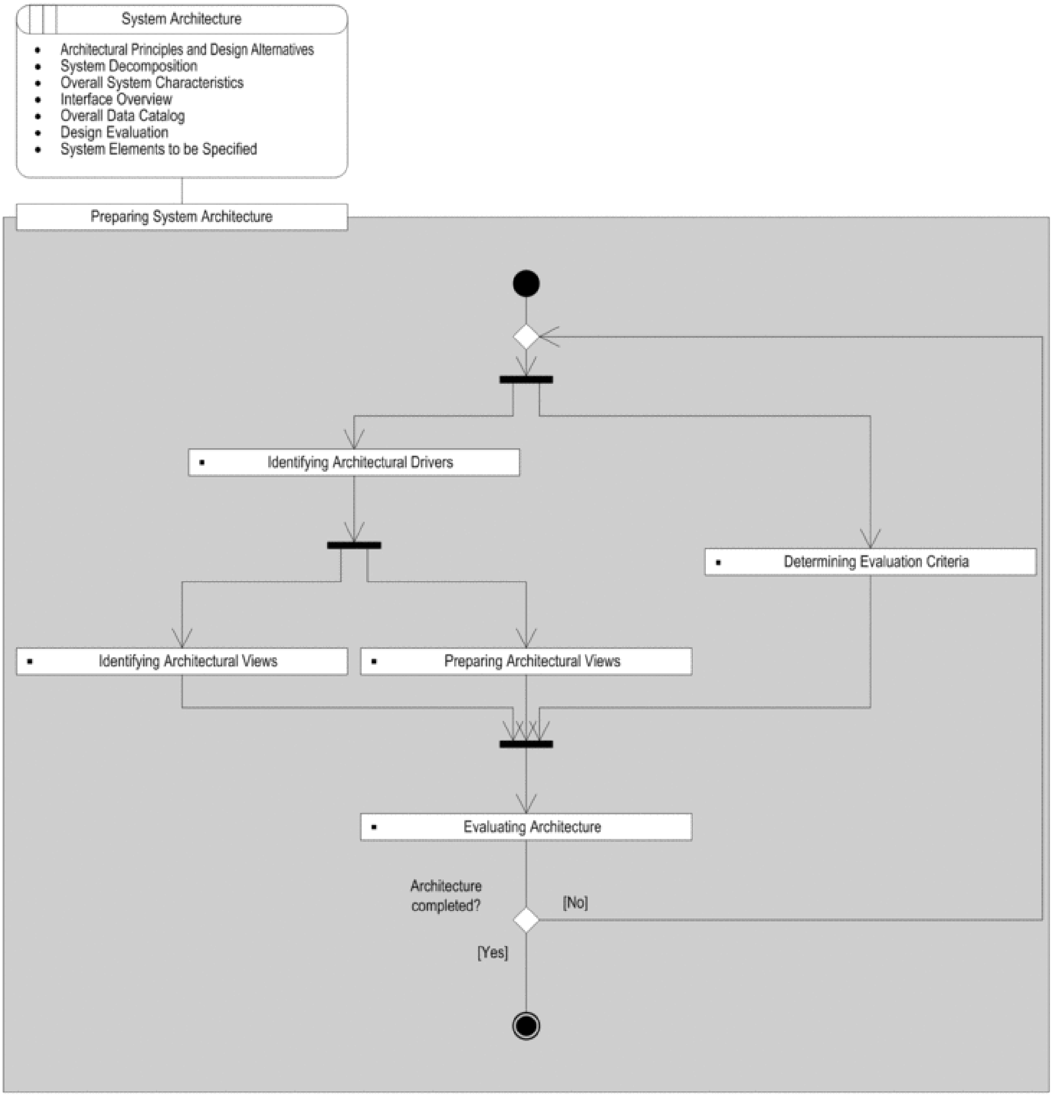
System Architecture
Architectural Principles and Design Alternatives
System Decomposition
Overall System Characteristics
Interface Overview
Overall Data Catalog
Design Evaluation
System Elements to be Specified
Preparing System Architecture
Identifying Architectural Drivers
Determining Evaluation Criteria
Identifying Architectural Views
Preparing Architectural Views
Evaluating Architecture
Architecture completed?
[No]
[Yes]

Figure 3: V-Model System Architecture Preparation [Source: V-Model Description]

First there is the identification of architecture drivers (e.g. reusability, system type, life cycle) and evaluation criteria. In the next step architecture views (e.g. logical and physical system structure view, view of the dynamic behavior) are identified and generated. These views are evaluated according to the given criteria and if necessary improved in subsequent iteration cycles.

The CONVERGE architecture will be developed according to the methodology described in the V-Model. The activities and tasks of the different V-model phases will be applied to the CONVERGE system, results will be both the CONVERGE architecture and the architectural description of the C2X systems network as eminent part of the CONVERGE system. The V-Model is reflected in the different CONVERGE work packages and the project plan.

2.1.2 Architecture concept in open distributed processing (ODP)

The open distributed processing reference model (specified in ISO-Norm ISO/IEC 10746) is a meta-model for the description of information systems.

This model is describing a system by several defined views that are used to describe different aspects of the overall architecture of the system:

- Enterprise viewpoint:
  Describes the purpose, roles, use cases, interactions and policies of the system (e.g. roles related to data collection, data processing, service presentation).

- Information viewpoint:
  Describes the semantic of static information, information processing and data formats.

- Computational viewpoint:
  Provides the functional decomposition of the system and objects interacting at interfaces.

- Engineering viewpoint:
  Describes the distribution of processing that provides the system functionality (e.g. data transfer supported by messages and protocols).

- Technology viewpoint:
  Describes the technologies used for processing and presentation of the information (e.g. used hardware and software).

So the ODP Model can serve as a model of standardized views on a distributed information system and thus could be used in the definition and generation of architectural views in the generation step of the V-Model.

ODP provides a framework for the description of different architectural viewpoints. CONVERGE will mainly focus on the Enterprise, Information, Computational and Engineering viewpoint. The Technology viewpoint will correspond with the documentation of the implementations that are part of CONVERGE. All viewpoints will be developed and maintained as products of the V-Model phases.

2.2 Used methodology and tools for architecture description

2.2.1 Architecture description languages

There are several languages, platforms and tools available that can be used for the description of system architectures. As in the past few years UML has proven to get more and more an industry standard, UML will be used as a base for describing the architecture in this project. SysML is on one hand a subset of the UML diagrams that are suitable for system design an on the other hand an extension as well as some new diagrams are added to the standard UML ones. Some of the UML diagrams are adapted in SysML. Figure 4 gives an overview on the diagram types.

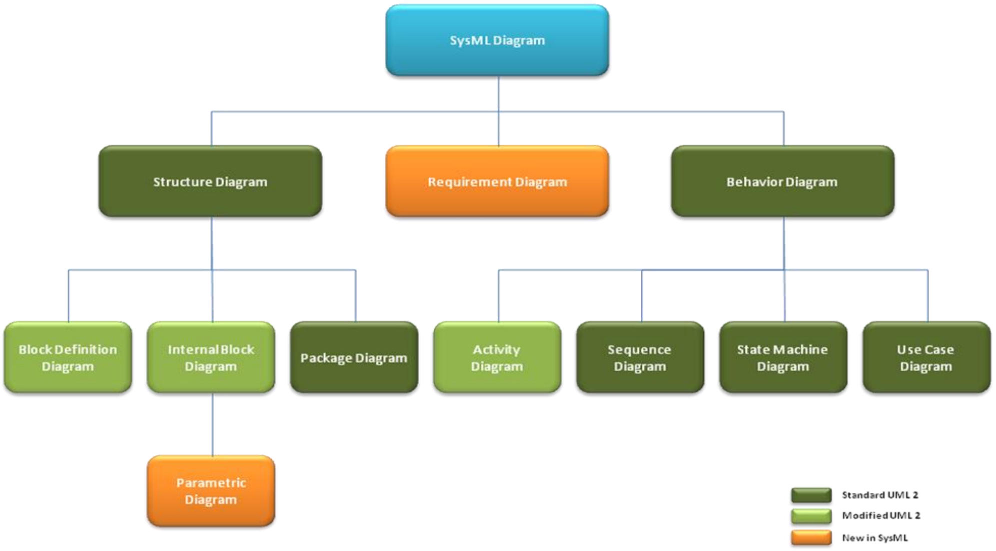

Figure 4: Overview SysML Components

2.2.2 Architectural viewpoints

As described before, it is necessary to take up different positions in order to fully describe complex system architectures. The following defines the viewpoints that will be taken into account in the activity of WP2 system architecture design. For each viewpoint an example will be given of how the description of the viewpoint and its visualization will look like. UML and SysML are used for the visualization of the views.

Generally there are two major types of viewpoints that are used in the description of a system. One is the structural viewpoint and the other is the behavior viewpoint. Both are needed in order to fully describe the system and the way it acts. In addition to those major elements there are requirements that form the major input for the definition of the system and parametric descriptions like e.g. equations used in the system.

Structural viewpoints

Package Diagram

Package Diagrams will be used to give overviews on the overall system or subsystems. They can be used to represent the system or parts of it from different viewpoints (e.g. Logical View, Physical View, Data Model View …).

Package diagrams shall be used for an overview on the system (e.g. logical view, physical view, data model view) and for each subsystem that is identified.

Block Diagram

Blocks are basic structural components that describe the structure of an element or system. As in the package diagram blocks can provide different views (e.g. physical blocks, software blocks, data blocks …). Each block can have different compartments that are used to describe block characteristics. Examples for characteristics of a block are constraints, satisfied requirements, values or properties.

An internal block diagram describes the internal structure of a block consisting of parts. An internal block shows different parts (atomic functional components) and their internal behavior inside a block.

For each of the packages identified a block diagram shall be derived. The decomposition in parts shall be done as long as it is needed to provide an understanding of the system. It might be possible to stop at a certain level of detail and hand over to other WPs (WP3 – WP6) for further detail elaboration.

Behavioral viewpoints

Activity Diagram

Activities describe the transformation of inputs of a system or parts of it through a controlled sequence of actions. An action can have two types of flows:

- control flow
  input that controls the way an action is performed and output that is used to e.g. control other actions
- data flow
  mandatory or optional data that is entering (input) and leaving (output) the action block

An activity diagram shall be generated for the overall system, each subsystem and each block defined in the structural decomposition.

Sequence Diagram

Sequence diagrams are helping to describe the interaction between parts based on messages. They can help to understand the behavior of complex scenarios by providing reference sequences, a control logic and a lifeline decomposition.

Sequence diagrams shall be used when the dynamic complexity of a block makes it necessary to describe the behavior of blocks.

State Machine Diagram

State machine diagrams are typically used to show the lifecycle of a block. They mainly support asynchronous (event driven) behavior and are able to take into account transitions and states. It is also possible to send signals from one block to another during e.g. state transitions.

State machine diagrams shall be used when the dynamic complexity of a block makes it necessary to describe the behavior of blocks.

2.3 Interfaces and working assumptions for interfacing with other work packages

WP2 will define the overall architecture of the CONVERGE C2X systems network. However it is not going to specify architectural details (implementation) of each of the subsystems in the overall system. Details for certain subsystems will be given by other working packages. The rest of the document gives an overview of the system from a functional point of view and depicts the interfaces and borders of the work done in WP2.

3 ARCHITECTURAL CONDITIONS AND TECHNICAL REQUIREMENTS

3.1 Derivation of technical requirements from functional requirements

The base for the complete architecture are the user stories and use cases defined in deliverable D1.1 in WP1 of the project. In this document a definition of 4 so called user stories has been done (after finalization of D1.1 two more user stories have been added which are marked with a * in the list below).

- Mobile road works
- Local hazard warning
- Communication of OEM backend with vehicle
- Short distance public transport
- Wrong way driver warning*
- Logistics scenario*

A user story is describing a complete application of the Car2X Systems Network from a functional point of view.

Each user story is decomposed into atomic functional blocks so called use cases which describe a certain part of the user story in a more generic way so that a use case can be part of several user stories. The so defined set of generic use cases is providing the complete set of building blocks defining the system architecture and allows to generate different kinds of additional other user stories to be covered by the Car2X Systems Network defined in CONVERGE. The two additional user stories mentioned above have been analyzed with respect to the needed use cases for their realization, and it has been deduced that both can be realized with the already existing architecture relevant use cases (only some functional parts have to be defined additionally). So it can be stated that the existing use cases from D1.1 are forming a complete set of inputs for the definition of the system architecture.

In a first step a dedicated approach and methodology has been worked out to systematically derive the technical requirements from the use cases and user stories pointed out in the deliverable D1.1. The determination of this methodology has been done in a core team consisting of experts from the different project partners. The chosen approach has been evaluated by applying it on one user story in an exemplified way. After some fine tuning, this verified approach has been used to transform each use case into a dedicated technical specification. To further formalize and optimize the process, some tools have been developed based on spreadsheets.

The basic outcomes of this process are three major kinds of information:

- A list of technical requirements
- A list of questions that need further detailed analysis and decisions to be made from an architecture point of view
- A list of functional architecture components that are needed in order to realize the given use cases

One of the major goals of the project is the generation of an overall system architecture that is open for users, providers and operators contributing to the system. This means that actors, services or functions should be able to appear and vanish without any influence on the operation and functionality of the overall system.

Therefore the major cornerstones of the deduced approach where, on one hand, the separation of the procedure into single atomic steps and on the other hand the split in three phases:

- Pre-operation phase (bootstrap)
- Operation phase (execution)
- Post-operation phases (suspension phases).

The phases are covering the complete life cycle of a certain use-case. If there are external dependencies or actions needed, this is noted, but not further detailed in the workflow of a single atomic step.

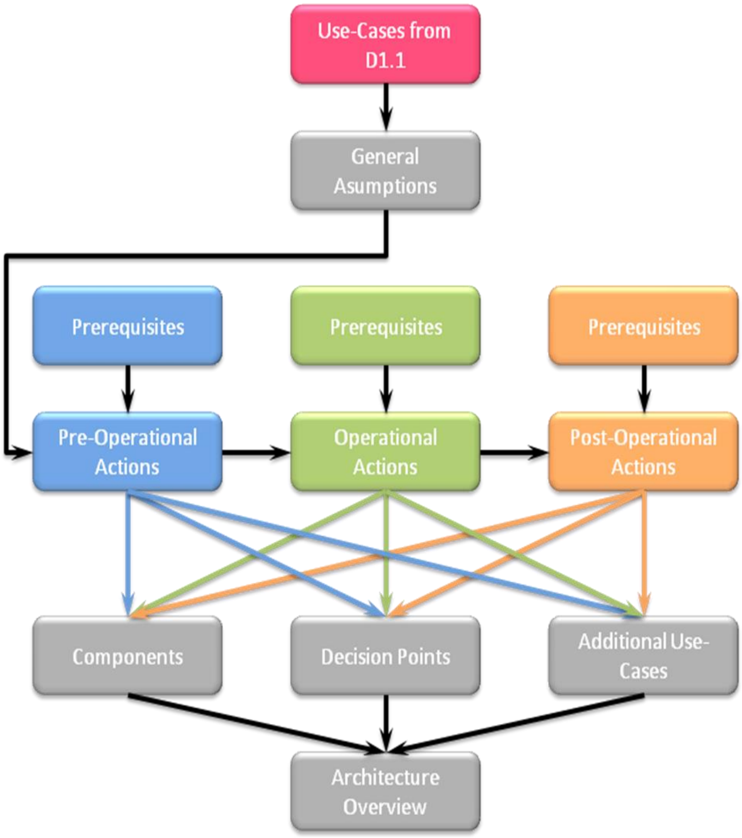

Figure 5: Overview of used Approach

Each use case is split into a number of actions that are necessary to prepare and initialize, operate and decompose the involved system components. After all three phases for a given use case have been performed in the system, it must not have any remaining components or data left and thus the use case has to be completely vanished. Especially the pre-operation and the suspension phases also have to be analyzed with respect to contractual issues besides the more technical ones.

For each of the phases in turn pre- and post-conditions are specified in order to ensure a seamless integration of the given functionality in the overall system and its lifecycle.

Figure 5 is illustrating the developed approach.

3.1.1 Explanation of the used approach in an exemplified use case

In this chapter the described approach for detection of technical requirements, open architecture questions and needed architectural components is shown in detail for one exemplified use case. A summary of all processed use cases is shown in Appendix A.

The use case that is taken here for explanation is just an arbitrarily selected one and does not have any special importance. The case chosen is UC-SP-04. This use case is one sub cases of the user story about parking space management. See chapter (4.1.4) of the deliverable D1.1 (Deliverable D1.1). For a description of the abbreviations used in the tables in this chapter please refer to Table 5: Components Detected in Descriptive Example.

Description (as given in D1.1):

The service provider collects periodically up to date parking space availability (parking information system) and traffic data (IGLZ) via the MDM or directly. The service provider calculates the zone approach route and creates a parking space prediction based on the obtained data. The service provider assigns the obtained parking space data to predefined destination categories.

Assumptions and Prerequisites:

In order to start from a well defined base of conditions a number of assumptions have been taken as prerequisites. These assumptions are not part of the analysis of the use case, but can be fulfilled by another use case or are a general assumption. Table 1 lists assumptions for this example use case.

Table 1: Assumptions in Descriptive Example

ID	Description
UC-SP-04_A1	The communication channel between IVSs and the OEMs Backends have been registered and established (-> separate user-story!) and “behaves transparent” within UC-SP-04
UC-SP-04_A2	Service providers that are delivering parking information and/or traffic information have been registered at the MDM so that parking information and traffic data services are available via the MDM (-> separate user story)
UC-SP-04_A3	The service provider has registered itself with MDM as receiver of parking space information and traffic data (-> separate user story)
UC-SP-04_A4	A service provider that is providing parking information via C2X-SN has been registered with the C2X-SN and hence has received C2X-SN access promising certificate (APC-SN) (-> separate user story)
UC-SP-04_A5	A service provider that is providing traffic information via C2X-SN has been registered with the C2X-SN and hence has received C2X-SN access promising certificate (APC-SN) (-> separate user story)
UC-SP-04_A6	The Parking Information Type A message distribution service has been agreed to be called "PI-A-Notification Board (PI-A-NB)"
UC-SP-04_A7	The Traffic Information Type A message distribution service has been agreed to be called "TI-A-Notification Board (TI-A-NB)"

Actions in pre-operation phase:

The first phase that is analyzed and detailed is the pre-operation phase. In this part of the analysis all actions necessary to bring the system in a state that allows the operational work of the given use case are worked out. Some prerequisites that are necessary for this phase (and not for the use case as a whole) are given at the beginning of the list. Following these prerequisites a list of actions is specified that are necessary to complete the pre operation phase. The columns that are indicated as “From” and “To” are listing the components that are belonging to a certain action (which component is communicating with which other component for the given action). The column “Optional” is used to indicate whether the given action is mandatory or optional. Components that are special in this use case get a certain prefix (PI for parking information or TI for traffic information)

Table 2: Actions of Pre-Operational Phase

From	To	Description	Optional
Prerequisite#1		A human readable document (e.g. HTML-text document), describing the characteristics of the PI-A-NB messages, their information quality and uncertainties, is available for human inspection	
Prerequisite#2		A software readable interface description (e.g. XMP, WSDL, Web Service description file) of the PI-A-NB service is available	
Prerequisite#3		A human readable document (e.g. HTML-text document), describing the characteristics of the TI-A-NB messages, their information quality and uncertainties, is available for human inspection	
Prerequisite#4		A software readable interface description (e.g. XMP, WSDL, Web Service description file) of the TI-A-NB service is available	
Prerequisite#5		A C2X-SN internal Service Directory service (e.g. UDDI) including a C2X-SN internal Service-Provider notification mechanism (-> separate user story!) is available and the way to contact this Service Directory service is known to all C2X-SN participants (-> separate user story!)	
Prerequisite#6		Each service provider has a generic, local, transaction logging service available which can be bound to a specific interface service to support charging, KPI supervision or security inspection functions (-> separate user story)	
Prerequisite#5		Each service provider has a generic, Incoming Event Alert service (e.g. IEA_#1) running at its Backend server farm in order to receive subscribed event notifications from any valid C2X-SN source. These services have been registered to the Service Directory.	
Prerequisite#6		A parking Information specific service access certificate, called APC_SN_PI-A-NB, has been issued to all SPs providing the service. The certificate is not only bound to the service but also allows to distinguish between different service providers	
Prerequisite#7		A traffic Information specific service access certificate, called APC_SN_TI-A-NB, has been issued to all SPs providing the service. The certificate is not only bound to the service but also allows to distinguish between different service providers	
Prerequisite#8		Each service provider that wants to share parking information data via MDM registers itself to MDM and provides the necessary information about the Parking Information service to MDM (-> separate user story)	
Prerequisite#9		Each service provider that wants to share traffic information data via MDM registers itself to MDM and provides the necessary information about the traffic information service to MDM (-> separate user story)	

From	To	Description	Optional
MDM	PI-A-NB #1	service user SU #1 agrees with MDM about exchange of parking information data via MDM (-> separate user story)	
MDM	TI-A-NB #1	service user SU #1 agrees with MDM about exchange of traffic information data via MDM (-> separate user story)	
MDM	IEA #1	The MDM informs SU #1 that a new parking information service has registered itself (-> separate user story).	
IEA #1	MDM	SU #1 IEA_#1 contacts MDM (-> separate user story), presenting its certificate APC_SN_PI-A, to register itself as receiver of Parking Information Type A message notifications.	
MDM	IEA #1	The MDM informs SU #1 that a new traffic information service has registered itself (-> separate user story).	
IEA #1	MDM	SU #1 IEA_#1 contacts MDM (-> separate user story), presenting its certificate APC_SN_TI-A, to register itself as receiver of Traffic Information Type A message notifications.	
C2X-SN SD	IEA #1	The Notification Service attached to the Service Directory server informs SU #1 that a new service (PI-A-NB) has registered itself, by posting SU #1 IEA event reception point, providing its WSDL and its textual descriptions	
C2X-SN SD	IEA #1	The Notification Service attached to the Service Directory server informs SU #1 that a new service (TI-A-NB) has registered itself, by posting SU #1 IEA event reception point, providing its WSDL and its textual descriptions	
IEA #1	PI-A-NB #2	SU #1 IEA_#1 contacts PI-A-NB_#2, presenting its certificate APC_SN_PI-A-NB, to register itself as receiver of Parking Information Type A message notifications.	
IEA #1	TI-A-NB #2	SU #1 IEA_#1 contacts TI-A-NB_#2, presenting its certificate APC_SN_TI-A-NB, to register itself as receiver of Traffic Information Type A message notifications.	

This process is illustrated in the sequence diagram in Figure 6.

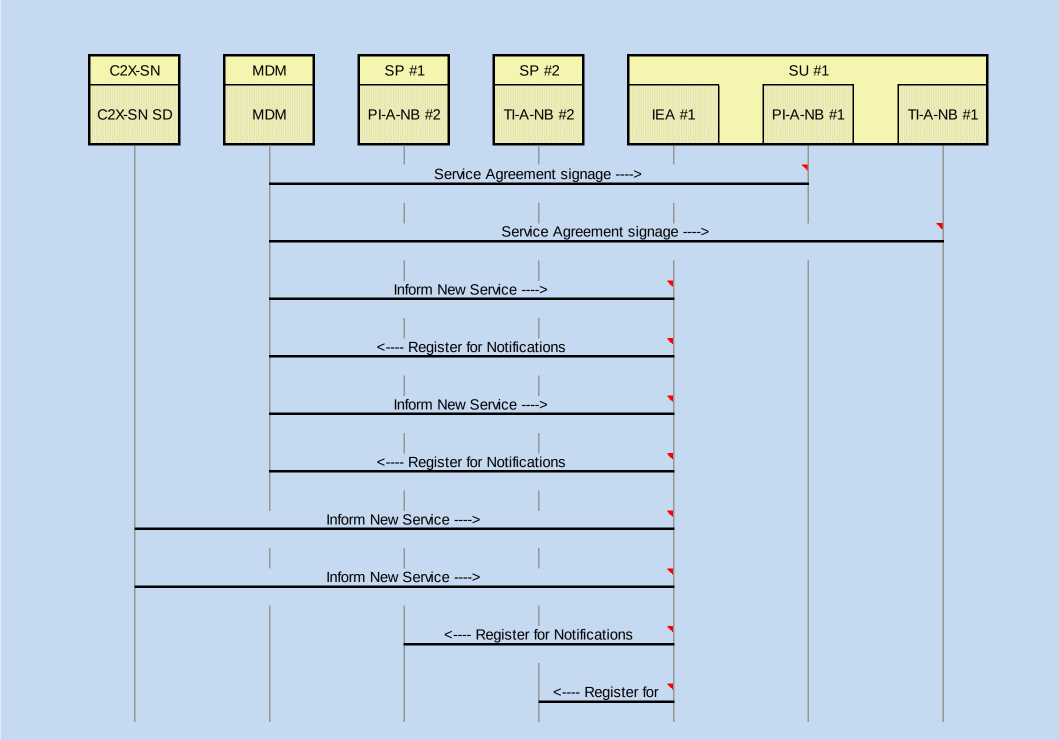

Figure 6: Sequence Diagram of Pre-Operational Phase

Actions in operational phase:

The prerequisites and actions of the operational phase are specified in the same way as explained for the pre-operational phase before and are shown in the Table 3 and sequence chart of Figure 7. This phase is dedicated to all activities that are necessary to operate the system for the given use case. All activities that are needed to carry out the use case are listed.

Table 3: Actions in Operational Phase

From	To	Description	Optional
Prerequisite#10		At least one service provider SP #1 that has agreed to exchange PI Type A messages has registered its PI-A-NB “brand xyz” service, attached their transaction logging service with their PI-A-NB, have registered their IEA services with their contract partner’s Backend PI-A-NB Services and is ready for operation	
Prerequisite#11		At least one service provider SP #1 that has agreed to exchange TI Type A messages has registered its TI-A-NB “brand xyz” service, attached their transaction logging service with their TI-A-NB, have registered their IEA services with their contract partner’s Backend TI-A-NB Services and is ready for operation	
Prerequisite#12		At least one service provider has agreed to provide PI Type A messages via MDM and done the necessary steps to offer and provide the service	
Prerequisite#13		At least one service provider has agreed to provide TI Type A messages via MDM and done the necessary steps to offer and provide the service	
MDM	IEA #1	MDM issues an PI-A_Event_Notification(ID) message (-> separate user story) with all event receivers which had been registered with PI-A_#1 beforehand as receivers of Parking Information Type A events. Hence MDM sends the message PI-A_Event_Notification(ID) to IEA_#1	x
IEA #1	MDM	Alerted via the incoming heads-up notification, the IEA_#1 pulls for the message(ID) from MDM (-> separate user story)	x
IEA #1	RE #1	SU #1 triggers its local Backend rule engine with the newly available Parking Information Type A message PI-A_#1__message-content	x
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-> separate user story) detects that PI-A-NB #2 message content has been received from either MDM or SP #1. It detects that there is a need for further processing (checking, aggregation, …), thus it hands the new message to the SU #1 processing engine for further processing	x
PE #1	PE #1	The SU #1 internal processing engine further processes (checks, aggregates, …) the new PI-A-NB #2_message content and calculates the zone approach route and creates a parking space prediction based on the obtained data. The service provider assigns the obtained parking space data to predefined destination categories.	x
MDM	IEA #1	MDM issues an TI-A_Event_Notification(ID) message (-> separate user story) with all event receivers which had been registered with TI-A_#1 beforehand as receivers of Parking Information Type A events. Hence MDM sends the message TI-A_Event_Notification(ID) to IEA_#1	x
IEA #1	MDM	Alerted via the incoming heads-up notification, the IEA_#1 pulls for the message(ID) from MDM (-> separate user story)	x
IEA #1	RE #1	SU #1 triggers its local Backend rule engine with the newly available Parking Information Type A message TI-A_#1__message-content	x
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-> separate user story) detects that TI-A-NB #2 message content has been received from either MDM or SP #1. It detects that	x

From	To	Description	Optional
		there is a need for further processing (checking, aggregation, …), thus it hands the new message to the SU #1 processing engine for further processing	
PE #1	PE #1	The SU #1 internal processing engine further processes (checks, aggregates, …) the new TI-A-NB #2_message content and calculates the zone approach route and creates a parking space prediction based on the obtained data. The service provider assigns the obtained parking space data to predefined destination categories.	x
PI-A-NB #2	IEA #1	SP #1 issues an PI-A_Event_Notification(ID) message (-> separate user story) with all event receivers which had been registered with PI-A_#1 beforehand as receivers of Parking Information Type A events. Hence SP #1 sends the message PI-A_Event_Notification(ID) to IEA_#1	x
IEA #1	PI-A-NB #2	Alerted via the incoming heads-up notification, the IEA_#1 pulls for the message(ID) from SP #1	x
IEA #1	RE #1	SU #1 triggers its local Backend rule engine with the newly available Parking Information Type A message PI-A_#1__message-content	x
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-> separate user story) detects that PI-A-NB #1 message content has been received from either MDM or SP #1. It detects that there is a need for further processing (checking, aggregation, …), thus it hands the new message to the SU #1 processing engine for further processing	x
PE #1	PE #1	The SU #1 internal processing engine further processes (checks, aggregates, …) the new PI-A-NB #1_message content and calculates the zone approach route and creates a parking space prediction based on the obtained data. The service provider assigns the obtained parking space data to predefined destination categories.	x
TI-A-NB #2	IEA #1	SP #2 issues an TI-A_Event_Notification(ID) message (-> separate user story) with all event receivers which had been registered with TI-A_#1 beforehand as receivers of Parking Information Type A events. Hence SP #2 sends the message TI-A_Event_Notification(ID) to IEA_#1	x
IEA #1	TI-A-NB #2	Alerted via the incoming heads-up notification, the IEA_#1 pulls for the message(ID) from SP #2	x
IEA #1	RE #1	SU #1 triggers its local Backend rule engine with the newly available Parking Information Type A message TI-A_#1__message-content	x
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-> separate user story) detects that TI-A-NB #1 message content has been received from either MDM or SP #1. It detects that there is a need for further processing (checking, aggregation, …), thus it hands the new message to the SU #1 processing engine for further processing	x
PE #1	PE #1	The SU #1 internal processing engine further processes (checks, aggregates, …) the new TI-A-NB #1_message content and calculates the zone approach route and creates a parking space prediction based on the obtained data. The service provider assigns the obtained parking space data to predefined destination categories.	x

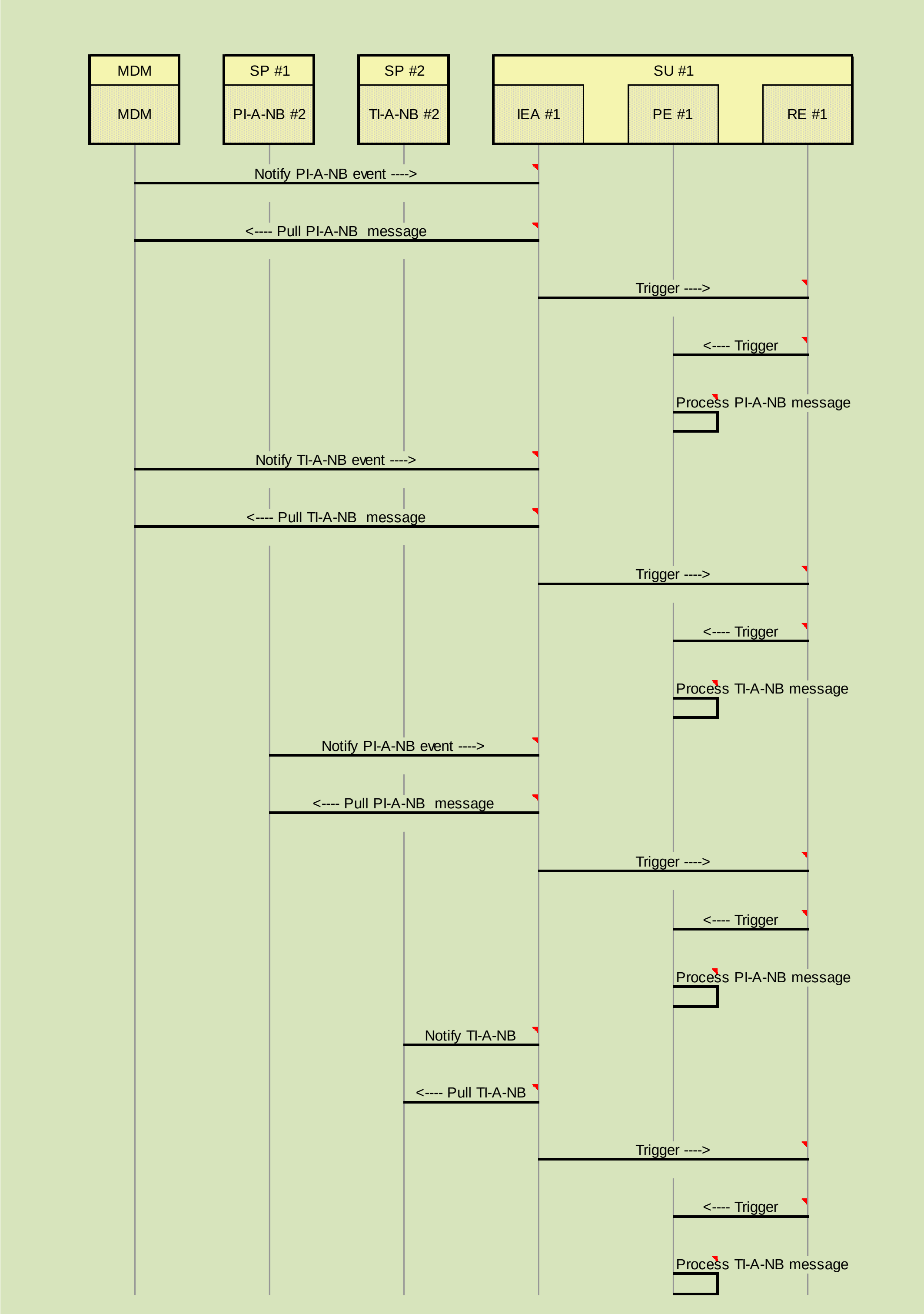

Figure 7: Sequence Diagram of Operational Phase

Actions in post-operational phase:

The prerequisites and actions of the post-operational phase are specified in the same way as explained for the pre-operational phase and are shown in

and in the sequence chart Figure 8. In this phase of the life cycle of the use case all actions necessary to stop and remove this use case and the underlying data and components are listed.

Table 4: Actions in Post-Operational Phase

From	To	Description	Optional
Prerequisite#14		All PI-A-NB and IEA services at SU #1 are ready to serve the next event	
Prerequisite#15		All TI-A-NB and IEA services at SU #1 are ready to serve the next event	
Prerequisite#16		SP #1 or MDM has terminated the PI-A-NB contract and notified the C2X-SN Contract Supervision Authority. SP #1 or MDM had been the only PI-A-NB service provider left at the C2X-SN and decided to revoke that offer. Hence the PI-A-NB service shall disappear as if it had never been launched	
Prerequisite#17		SP #2 or MDM has terminated the TI-A-NB contract and notified the C2X-SN Contract Supervision Authority. SP #2 or MDM had been the only TI-A-NB service provider left at the C2X-SN and decided to revoke that offer. Hence the TI-A-NB service shall disappear as if it had never been launched	
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority e.g. Web-HMI is filled with the contract relation update information and a Certification-Update-Request message is posted to the C2X-SN Certification-Issuer	
C2X-SN CI	IEA #2	The C2X-SN Certification-Issuer contacts the IEA receptor of SP #1 to inform that the Certificate APC_SN_PI-A-NB has been revoked. SP #1 updates its local certification management	
IEA #2	RE #2	SP #1 rule engine updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules	
IEA #2	RE #2	SP #1 IEA triggers its local RE with the update request. SP #1 purges it entire PI-A-NB service configuration and terminates PI-A-NB_#1	
RE #2	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the PI-A-NB_#1 service offer	
PI-A-NB #2	IEA #1	SP #1 contacts the IEA receptors of SU #1 to inform that the parking information service is not available any more	x
IEA #1	RE #1	SU #1 IEA triggers its local RE with the update request. SU #1 purges it entire PI-A-NB service configuration and terminates PI-A-NB_#1	
MDM	IEA #1	MDM contacts (-> separate user story) the IEA receptors of SU #1 to inform that the parking information service is not available any more	x
IEA #1	RE #1	SU #1 IEA triggers its local RE with the update request. SU #1 purges it entire PI-A-NB service configuration and terminates PI-A-NB_#1	
C2X-SN CI	IEA #3	The C2X-SN Certification-Issuer contacts the IEA receptor of SP #2 to inform that the Certificate APC_SN_TI-A-NB has been revoked. SP #2 updates its local certification management	
IEA #3	RE #3	SP #2 rule engine updates its local certification management and triggers its local RE with the update request. The RE of SP	

From	To	Description	Optional
		#2 updates its event notification rules	
IEA #3	RE #3	SP #2 IEA triggers its local RE with the update request. SP #2 purges it entire PI-A-NB service configuration and terminates TI-A-NB_#1	
RE #3	C2X-SN SD	SP #2's RE contacts the C2X-SN Service Directory server and requests the deletion of the TI-A-NB_#1 service offer	
TI-A-NB #2	IEA #1	SP #2 contacts the IEA receptors of SU #1 to inform that the traffic information service is not available any more	X
IEA #1	RE #1	SU #1 IEA triggers its local RE with the update request. SU #1 purges it entire PI-A-NB service configuration and terminates PI-A-NB_#1	
MDM	IEA #1	MDM contacts (-> separate user story) the IEA receptors of SU #1 to inform that the traffic information service is not available any more	x
IEA #1	RE #1	SU #1 IEA triggers its local RE with the update request. SU #1 purges it entire TI-A-NB service configuration and terminates TI-A-NB_#1	

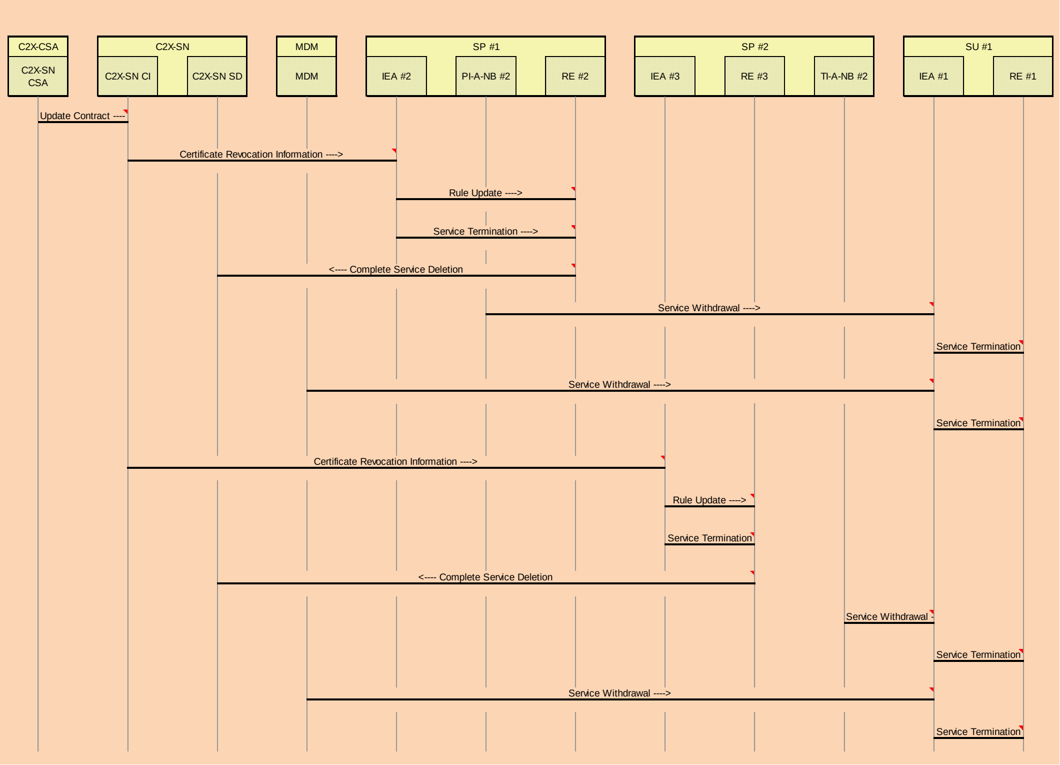

Figure 8: Sequence Diagram in Post-Operational Phase

Detected components:

In the actions identified before, there are always certain functional components involved. These **components are needed to start the given use case, operate it and have it vanish from the** system. Table 5 is a list of the components involved in the use case analyzed here. Some components exist in more than one instance. For the final decomposition of the architecture of the system network those components are taken into account only once of course.

Table 5: Components Detected in Descriptive Example

Name	Description	Involvement		
		Pre-Op.	Operation	Post-Op.
C2X-SN CSA	The (human) body (person) that is responsible for the generation, supervision and revocation of certificates used to access the C2X Systems Network. It also regulates the legal part and ensures that all participants meet the necessary requirements.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that a systems network CA and SP-internal CA exists. This can be for example for OEM, so that they can attach certificates to their cars or non-free services so that service users can get a certificate to access the service. The CA is also responsible for certificate revocation.			x
C2X-SN SD	An electronic "yellow page" like service (e.g. UDDI) that holds, maintains and shares detailed information about all services that are available and their operational status. In addition on an SP side it can hold the information about the registered mobile nodes and their services. It also informs registered user about new available messages. This can be inside the C2X-SN itself and inside a SP. The SP part can hold information about registered clients and information and can than distribute all or a subset of this information to the "global" SD in the C2X-SN	x		x
MDM	Special SP for data exchange (Mobility Data Marketplace, see MDM Description).	x	x	x
IEA #2	Running on all communication entities; the SAP for all incoming messages from the C2X-SN and the MN			x
PI-A-NB #2	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtypes like client (incl. installation), server, application repository, etc.	x	x	x
RE #2	A Software component that is able to handle and process messages that are sent through the C2X-SN			x
IEA #3	The SAP for all incoming messages from the C2X-SN and the MN; Running on all communication entities			x
RE #3	A Software component that is able to handle and process messages that are sent through the C2X-SN			x
TI-A-NB #2	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtypes like client (incl. installation), server, application repository, etc.	x	x	x

Name	Description	Involvement		
IEA #1	Running on all communication entities; the SAP for all incoming messages from the C2X-SN and the MN	x	x	x
PE #1	A component that performs service specific actions (e.g. provide a warning message to the driver of a car via HMI) There are different subtype like RWW, LHW, CAM-sending, etc.		x	
PI-A-NB #1	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtypes like client (incl. installation), server, application repository, etc.	x		
RE #1	A Software component that is able to handle and process messages that are sent through the C2X-SN		x	x
TI-A-NB #1	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtypes like client (incl. installation), server, application repository, etc.	x		

Detected decision points:

During the work out of the use case details there might be some tasks that allow different kinds of realization, so called decision points. These decision points may or may not result in the definition of alternative architectural solutions and need to be further examined. All those questions that are arising in the course of use case processing are listed and taken into account in the further analysis (see 3.3). Here the focus is on certain functions or system behavior detected as necessary parts of the overall system (e.g. realization of the functional component service directory). Those functions might be realized in different ways and with different approaches.

Table 6 shows the decision points detected here.

Table 6: Decision Points Detected in Descriptive Example

ID	Component	Description
DP-SD	C2X-SN SD	Find a way to realize the C2X-SN Service Directory

Detected additional use cases:

Another kind of information as shown in Table 7 that is generated in the specification process of the technical details of each use case are actions that are not belonging to the use case itself but are necessary to make the use case working. In order not to overload the description and to keep focus on the use case itself, those so called external use-cases are noted and treated in a separate step (see 3.3). The focus here is not on single functional or behavioral questions but on certain blocks including sequences of actions that are needed in order to let the overall system get into function (e.g. registration procedure for a service provider at the external MDM).

Table 7: New Use-Cases Detected in Descriptive Example

ID	Description
UST-ComCh	Registration and establishment of the communication channel between IVS and the OEM Backend
UST-PIMDM	Description how service providers that are delivering parking information and/or traffic information can be registered at the MDM so that parking information and traffic data services are available via the MDM
UST-SPReg	Registration of SP #1 with the C2X-SN as “Service Provider, Type X” and reception of C2X-SN access premising certificate (APC_SN)
UST-SPNM	Notification Mechanism for notifying service participants about changes in a service they have been registered to
UST-SPCM	Contact mechanism to reach the C2X-SN Service Description ("yellow pages") Service
UST-KPISV	Interface service to support charging, KPI supervision or security inspection functions
UST-RE	Component that is able to process all messages that are distributed in the C2X-SN. For each message the Rule Engine (RE) has to know the steps to be taken for further processing
UST-MDM	Detailed description about providing and using services via MDM. This includes: - User registration - Service registration - Service announcement - Service information distribution - Certification management - Data distribution
UST-C2XSN	Detailed description about providing services via C2X-SN This includes: - User registration - Service registration - Service announcement - Service information distribution - Certification management - Data distribution

After having performed the use cases according to the method explained before, all remaining decision points and external use cases have been summarized and answered or treated as to be answered in the further course of the detailed architecture elaboration. The result of this analysis is given in the following chapters.

The detected architectural components have also been summarized, double entries have been deleted and the components are listed in a summary list (see 4.1). This list is one of the main inputs for the generation of the first architecture view given in chapter 5.

3.2 Overview on treated use cases

Figure 9, Figure 10 and Figure 11 gives an overview on the use cases that are generated in D1.1, the related requirements and the dependency of the different use cases from each other. It also indicates security relevant use cases and the network layer each use case is related to. This might serve as help to quickly get a view on the classification of a certain use case when further reading the document.

3.2.1 Use Cases related to Layers above Network Layer

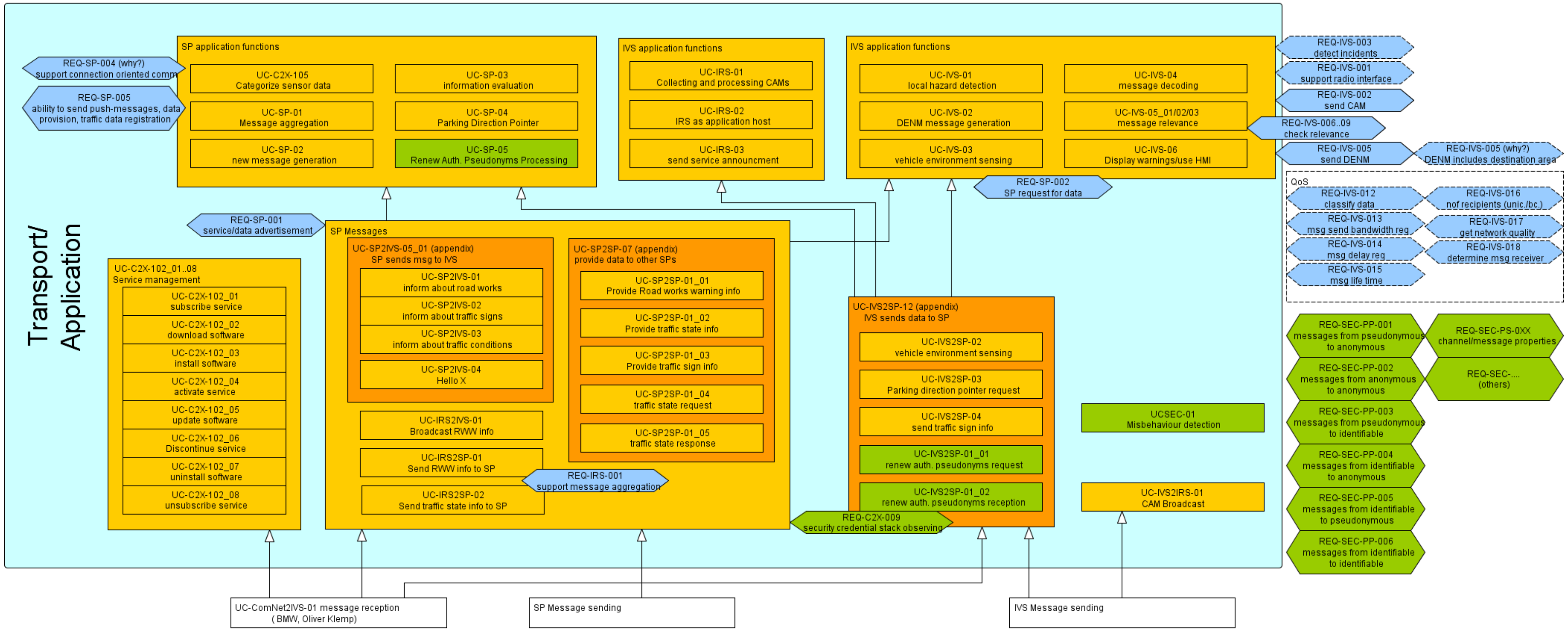

Figure 9: Use Cases Related to Layers above Network Layer

3.2.2 Use Cases related to Network Layer

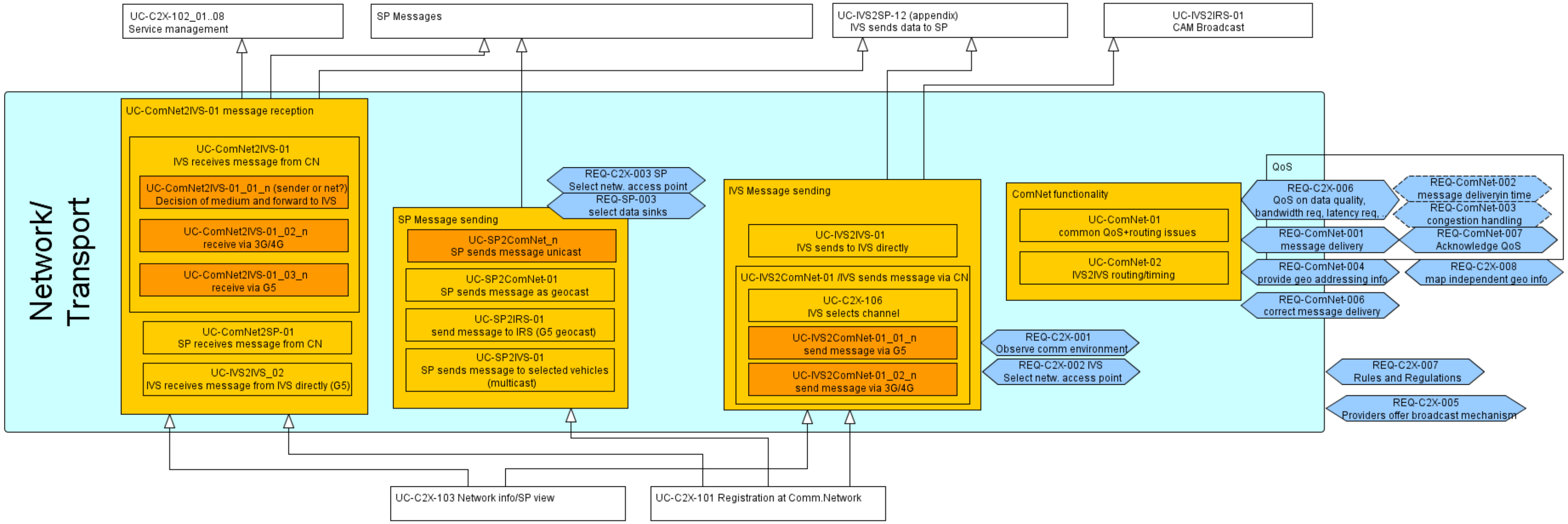

Figure 10: Use Cases Related to Network Layer

3.2.3 Use Cases related to Layers below Network Layer

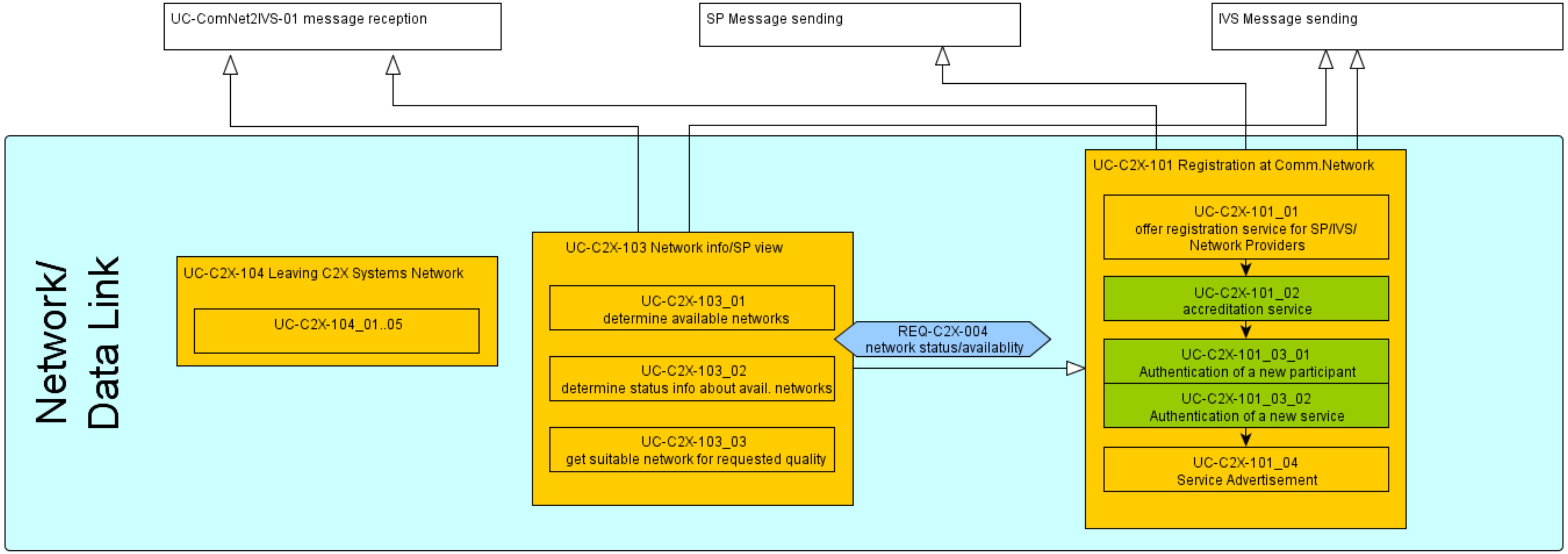
UC-ComNet2IVS-01 message reception
SP Message sending
IVS Message sending
Network/
Data Link
UC-C2X-104 Leaving C2X Systems Network
UC-C2X-104_01..05
UC-C2X-103 Network info/SP view
UC-C2X-103_01
determine available networks
UC-C2X-103_02
determine status info about avail. networks
UC-C2X-103_03
get suitable network for requested quality
REQ-C2X-004
network status/availablity
UC-C2X-101 Registration at Comm.Network
UC-C2X-101_01
offer registration service for SP/IVS/
Network Providers
UC-C2X-101_02
accreditation service
UC-C2X-101_03_01
Authentication of a new participant
UC-C2X-101_03_02
Authentication of a new service
UC-C2X-101_04
Service Advertisement

Figure 11: Use Cases Related to Layers below Network Layer

3.3 Requirements and decision points

The detailed technical analysis of the given use cases from D1.1 have led to a number of requirements, decision points and questions which have been analyzed in a more detailed way. To do this analysis in an efficient way, the open points have been split in several groups with regards to content. In the following subchapters the details are presented. In order to give a complete overview on the work done, all requirement and decision points are listed even though some of them might not be architecture relevant and are only needed to complete the use case functionality. The requirements and decision points that are not architecture relevant are indicated with a lighter text color.

3.3.1 Requirements for the communication

One of the classes identified are questions and decision points that are related to communication issues. The following tables are summarizing the questions and feedback generated during the analysis process.

Use case: UC-C2X-106		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Use case describing the different QoS requirements of the applications (and the mechnism of requestion QoS from CU)	mobile network: - packet bearer (including QoS parameters) - TCP - IP - HTTP IRS Network: - packet based connection - IP) or GeoNetwork - TCP/UDP	No additional usecase. Describe connection setup and tear down in mobile network and IRS network
Question:	**Points to be considered:**	**Proposed way forward:**
A set of quality mertrics needs to be defined, which both accomodates the application layer requirements regarding QoS as well as the LTE modem and ITS-G5 modem QoS parameterization capabilities. Perhaps a mapping is necessary to project application layer QoS requirements differently onto hw/network capabilities depending on both the nature of the specific use case as well as the nature of the communication network (e.g. latency requirements may be viewed in a different way for LTE and IST-G5). These quality parameters need to be incorporated into the "decision maker" (Entscheider) accordingly.	- BMW Paper (see BMW): cooperative experience map as possible additional criteria - Take application requirements into account - in which scenarios do we really have to decide? E.g. depending on application - Which parameters would make sense to be provided by the network (e.g. depending on current direction of travel, and expected network load/quality in that direction)	discuss within AP3, AP4, AP5, AP6
Question:	**Points to be considered:**	**Proposed way forward:**
It has to be decided how the CU shall determine the "status" of a possible communication network and which parameters shall be measured (which, how often …) and how these are to be taken into account by the decision maker -> “decision maker” Discussions in AP6, to be extended to AP6.	- BMW Paper (see BMW): cooperative experience map as possible additional criteria - Take application requirements into account - in which scenarios do we really have to decide? E.g. Depending on application - Which parameters would make sense to be provided by the network (e.g. depending on current direction of travel, and expected network load/quality in that direction)	discuss within AP3, AP4, AP5, AP6
Question:	**Points to be considered:**	**Proposed way forward:**
It has to be decided how the RE shall handle cases, where the requested QoS cannot be met by the available communication networks	In case of LTE a new connection with different QoS class has to be requested. Decision how to continue may be dependent on requesting application the same applies for IRS networks	describe current procedure within mobile network

Use case: UC-ComNet-01		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Gathers information and calculates the currently available QoS.	It is Communication Network (cellular and IRS) internal functionality to determine the current QoS status of the network, so that it can be presented to users (SP or IVS) which want to use the communication network. It is network specific. But a comparable set of QoS parameters must be defined and available.	No additional use case, but definition of a set of necessary parameter.
Question:	**Points to be considered:**	**Proposed way forward:**
How is the addressing done? How gets the server the information about the clients?	explain GLM proposal (mobile network) / eMBMS Address AP5 for IRS, already an research point for AP5	provide description of Ericsson's and HTW GLM proposal, converge and enhance solution (AP4 & AP5 together)
Question:	**Points to be considered:**	**Proposed way forward:**
Do we have a feedback if the QoS was met?	QoS on mobile radio network can be guaranteed. Other QoS (end-to-end) cannot be guaranteed, feedback on actual QoS is not given IRS Network: No QoS feedback is defined and given, and in general QoS cannot be guaranteed (only in some special situations)	provide description of QoS mechanisms in mobile networkand IRS Network
Question:	**Points to be considered:**	**Proposed way forward:**
Do we send a feedback, if the message can be send via the backbone network? And do we send a feedback, if the message was delivered successfully or unsuccessfully to the next network?	IRS Network: Since the last step of the transmission via ETSI ITS G5 is not confirmed, higher layers are responsible for acknowledgments if a message could be delivered or not.	no action

Use case: UC-IRS-02		
Question:	**Points to be considered:**	**Proposed way forward:**
Specification of communication to service provider	IRS Network: The communication between IRS and an SP must be specified.	IRS Network: AP5 discussion

Use case: UC-IRS2SP-02		
Question:	**Points to be considered:**	**Proposed way forward:**
The requirements for the connection have to be defined. (Reliable, connectionless or connection oriented, etc.)	IRS Network: This applies only, if more than one backbone connection is available, which should be normal priorization	no action.

Use case: UC-IVS2SP-01_01 Renew Authorized Pseudonyms – Request		
Question:	**Points to be considered:**	**Proposed way forward:**
It is assumed that a supervision of correct message delivery is the task of the subsequent UCs. ETSI TS 102 941 has not defined an Ack mechanism.	This is kind of a deadlock. The CN cannot guarantee a message delivery, because the SP is not in the CN. So the Security application is responsible to send a message again, if no reply is received in a certain amount of time.	To be discussed between AP4, AP5, AP6, AP0.4

Use case: UC-SP2IVS-03		
Question:	**Points to be considered:**	**Proposed way forward:**
It has to be defined, when a message will be discarded.	SP specific: Forward to AP3	SP specific: Forward to AP3

Use case: UC-LHW		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Registration and establishment of the communication channel between IVS and the OEM Backend	mobile network: - packet bearer (including QoS parameters) - TCP - IP - HTTP IRS Network: - packet based connection - IP or GeoNetwork - TCP/UDP	No additional use case. Describe connection setup and tear down in mobile network and IRS network

Use case: US-RWW1		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The IVS has to detect which communication channels are available for communication with the infrastructure end point, select one or several according to local policies. This setup has to be updated whenever a change in the conditions that influence the communication was detected	"Decision maker" discussion.	No additional use case. Continue decision maker discussion in AP2 to AP6

Use case: US-RWW2		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A mechanism has to be provided by the overall system that allows transmitting messages with geocast. This has to be taken into account both communication network operator (MNO, IRS) side and on a global side across communication network operator	No dedicated use case needed. Description of existing proposals in AP2	provide description of Ericsson's and HTW GLM proposal, converge and enhance solution (AP4 & AP5 together)

Use case: UC-IVS2SP-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Registration and establishment of the communication channel between IVS and the service provider	mobile network: - packet bearer (including QoS parameters) - TCP - IP - HTTP IRS Network: - packet based connection - IP or GeoNetwork - TCP/UDP	No additional use case. Describe connection setup and tear down in mobile network and IRS network

Use case: UC-C2X-102_02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Open Channel: use case to open a generic transport channel between IVS/IRS and SP	mobile network: - packet bearer (including QoS parameters) - TCP - IP - HTTP IRS Network: - packet based connection - IP or GeoNetwork - TCP/UDP	No additional use case. Describe connection setup and tear down in mobile network and IRS network
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Close Channel: use case to open a generic transport channel between IVS/IRS and SP	mobile network: - packet bearer (including QoS parameters) - TCP - IP - HTTP IRS Network: - packet based connection - IP or GeoNetwork - TCP/UDP	No additional use case. Describe connection setup and tear down in mobile network and IRS network

Use case: UC-ComNet2SP-01		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A use case describing the set of QoS parameters (and its adoption), which both accommodates the application layer requirements regarding QoS as well as the LTE modem and ITS-G5 modem QoS parameterization capabilities. Perhaps a mapping is necessary to project application layer QoS requirements differently onto hw/network capabilities depending on both the nature of the specific use case as well as the nature of the communication network (e.g. latency requirements may be viewed in a different way for LTE and ITS-G5).	description of Application requirements and QoS mechanisms in existing networks - not necessarily own UC	create a list of application requirements and QoS mechanisms in mobile networks

Use case: UC-IVS2ComNet-01		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
use case specifically describing the regularly transmission of CAM messages (or similar) to cover REQ-IVS_006 (see Deliverable D1.1)	Discuss within AP4: do we need this on mobile networks (e.g. selective intersection assistant)? AP5: this includes the "classic" ITS functions. For IRS that means forwarding and processing.	probably not a UC, but a closer look at special scenarios (e.g. geo-selective intersection assistant via LTE) might be needed For IRS: also no use case but a general discussion about the abilities and responsibilities of an IRS

Use case: UC-IVS2SP-01_02 Renew Certificates - Reception		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
IVS receiving message via backbone communication infrastructure	general reception of messages from IRS: UC ComNet2IVS-01 (see Deliverable D1.1)	no action

3.3.2 Requirements for external access (MDM)

A connection to the external MDM is required for some use cases. The following tables are summarizing the questions and feedback generated during the analysis process.

Use case: UC-IVS2SP-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Detailed description about providing and using services via MDM. This includes: - User registration - Service registration - Service announcement - Service information distribution - Certification management - Data distribution	Find the best way to provide and use services via MDM	see chapter 4.2.6
Question:	**Points to be considered:**	**Proposed way forward:**
Find the best way to provide and use services via MDM	Information available from MDM documentation	get MDM documentation

Use case: UC-SP-04		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Description how service providers that are delivering parking information and/or traffic information can be registered at the MDM so that parking information and traffic data services are available via the MDM	Find the best way to provide and use services via MDM	see chapter 4.2.6

3.3.3 Requirements from functional point of view

The functional requirements are necessary to realize the given use cases, however those requirements do not generate major architectural influence. The following tables are summarizing the questions and feedback generated during the analysis process.

Use case: UC-IVS-01		
Question:	**Points to be considered:**	**Proposed way forward:**
Find a way to detect hazards from sensor data	Hazards should also be triggered manually (e.g. by Converge Smartphone-App). Some cars have e.g. Crash-sensors integrated, should be used in AP6 in the VAPI. Define classes of hazards	Define Sensor Data in AP6 for VAPI. Define hazards catalogue.

Use case: US-RWW1		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A way to inform the blocking trailer about its infrastructure communication end point has to be specified in detail	BT has a cellular uplink and an ITS-G5 unit. The "communication-box" is pre-provisioned with the addresses of its service provider. By going online via cellular tech., it establishes a link to its SP.	Specify detailed communication for the RWW use case in AP2 (e.g. Sequence-diagram), depending on the architecture options.
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Methods for transferring the initial information that the blocking trailer has to distribute to the "blocking trailer communication device" (IRS) have to be defined. This information can be derived from the blocking trailer itself or from an external entity	Both should be possible. The RWW message to be sent must be defined.	Add to message catalogue
Question:	**Points to be considered:**	**Proposed way forward:**
Find best way to communicate the "here I am" message from the blocking trailer to its communication end point. Possible decision to be taken: - acknowledged - repeating on transport level or application level - mechanism for confidentiality (tunnel, "cable", message based)	Communication also depends on the architecture of the whole system. Is it a "converge-enabled" blocking trailer or is it maintained by a service provider, which is then the communication endpoint? Are the messages geo-referenced? Should they be, or raw? Which geo-referencing system has to be used?	Define Middleware or Communication Protocol in AP2 with regards to Security group, also depending on the yet-to-be-defined system architecture. A message-catalogue has to be defined.
Question:	**Points to be considered:**	**Proposed way forward:**
Determine exact mechanism to exchange the operational status of the blocking trailer to its traffic center - Push or Pull	Push and Pull should both be supported. The protocol has still to be defined.	Define Middleware or Communication Protocol in AP2 with regards to Security group, also depending on the yet-to-be-defined system architecture. A message-catalogue has to be defined.

Use case: UC-IVS2SP-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Aggregation and processing of sensor reading data	Methods and algorithms for aggregation must be found	This is not part of CONVERGE.
Question:	**Points to be considered:**	**Proposed way forward:**
Find a way to reasonably aggregate raw sensor readings data in order to generate usable service data information	Different sensors with different quality and different accuracy have to be merged. Algorithms are mostly very special. Where should the data be aggregated?	Research regarding sensor data fusion has to be done. Metrics have to be defined

Use case: UC-IRS2SP-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Module which recognize the topology and analyzed the traffic condition around the IRS	Hessen Mobil already automatically analyzes traffic by different sensor data (input regarding data and methods). Where is this recognition done, backend or IRS or a combination with pre-filtering?	Define Method for gathering this information by CAM-Messages. Ask Hessen Mobil for current methods.
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The traffic center has a module, which gather traffic data from different sensors (e.g. IRS) and calculates an overall traffic situation.	Hessen Mobil already automatically analyzes traffic by different sensor data (input regarding data and methods). Where is this recognition done, backend or IRS or a combination with pre-filtering?	Define Method for gathering this information by CAM-Messages. Ask Hessen Mobil for current methods.
Question:	**Points to be considered:**	**Proposed way forward:**
How often and in which quality should the analyzed data be sent to the TC.	Raw or aggregated data? Message Life-Time. On-demand notification.	Message-catalogue must be defined, also maybe some kind of relationship or ontology between the data

Use case: UC-SP2IVS-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
How will the TC be informed about RWW.	Depending on the architecture (BT is maintained and pre-provisioned by the TC or its 3rd party with own SP).	Define communication protocol and messages (AP2)
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Use case for generation of unique message ids for reference used in update messages.	Maybe some standard like UUID (RFC 4122)	Find use case, where this is necessary. Define the standard to use. (AP2)
Question:	**Points to be considered:**	**Proposed way forward:**
Threshold for the live time validation.	Hazards could have limited lifetime, must be defined as a property of the messages.	Message-catalogue must be defined, also maybe some kind of relationship or ontology between the data

Use case: US-RWW2		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The detailed setup procedure for the RWW service at the OEM has to be described.	Error cases (no cellular link) must be handled.	Specify detailed communication for the RWW use case in AP2 (e.g. Sequence-diagram), depending on the architecture options.

Use case: UC-IVS2SP-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Description of the process and components to fill and maintain a database that is holding all necessary information to provide the parking guide information service	Define requirements for the parking house. Will this information be provided via an ITS-G5 unit at the house? Maybe some kind of indoor Navigation necessary?	Define a Service Provider for this user story. Define responsible AP, maybe in AP-Leader meeting.
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Description of the process of generating the PG-A service data message from the given input of the requesting service user and the information available in the parking guide database (see above)	Free parking spaces should be markable as reserved for tour planning. This must be considered in the database an in the communication protocol.	Define a Service Provider for this user story. Define responsible AP, maybe in AP-Leader meeting.
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Description of the process and components that are necessary to present the received information about parking spaces the end user in the IVS	Automatic guidance in combination with navigation in-car system, but also maybe some other variant for smart phones (geo-referenced position or plain number,…)	Define a Service Provider for this user story. Define responsible AP, maybe in AP-Leader meeting.

Use case: UC-IRS-01		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Connection between Blocking Trailer and IRS.	Some old blocking trailers have only analogue speed limit signs, should they be considered?	Ask Hessen Mobil how the digital speed limit signs are connected. Define physical and logical interface between "communication box" and other components at the blocking trailer

Use case: UC-SP-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A CONVERGE message must be specified with a certain message type. Such a message contains data description and data source.	A set of metadata has to be defined, which covers all user stories and use cases. Also maybe some kind of ontology between messages (context-aware computing)	The "CONVERGE communication protocol" has to be defined with its messages and interfaces (also serialization, binary, xml, extensions for existing formats,…) (AP2)

3.3.4 General requirements

The requirements that are not able to be assigned to one of the other classes are summarized in this chapter. The following tables are summarizing the questions and feedback generated during the analysis process.

Use case: UC-LHW		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Component that is able to process all messages that are distributed in the C2X-SN. For each message the Rule Engine (RE) has to know the steps to be taken for further processing	Very general component for message processing and distribution in den SN context. Is available on SP and IVS/IRS. Important are interfaces and protocols.	To be discussed in the APs context with AP3/AP5/AP6
Question:	**Points to be considered:**	**Proposed way forward:**
Find a way to realize transaction logging to support charging, KPI supervision, security inspection	This is from an architectural point of view out of scope for CONVERGE, it must only be guaranteed that such a thing exists (replicability, auditability)	forward to AP3, AP5, AP6 for CONVERGE solution

Use case: UC-C2X-105		
Question:	**Points to be considered:**	**Proposed way forward:**
A set of quality metrics needs to be defined, which describe the quality of the received data (e.g. originator, type of sensor, type of processing algorithm, timestamp, signature, …)	Definition of data types (e.g. from a vehicle) and suitable quality values, this is for IVS<->SP but also for IVS<->IVS and IVS<->IRS	forward to AP3 and AP6 (AP5)

Use case: UC-IRS-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The status/logging/fault information must be forwarded to a central monitoring	This is linked to UC-C2X-102_02 US-05	forward to AP5
Question:	**Points to be considered:**	**Proposed way forward:**
Specification of communication with management (log/fault/conf/status)	A defined interface and protocol for the management (how the information is transmitted to the management) have to be defined.	forward to AP5

Use case: UC-SP-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The logging of data in a non-repudiation manner is needed. This has to define the log format, the information to be logged, the logging mechanism and storage of the logs, which guarantee, that the log cannot be tampered.	This is the same as for UC-SP2IVS-03 SP-LOG	forward to AP3

Use case: UC-SP-03		
Question:	**Points to be considered:**	**Proposed way forward:**
The call-hierarchy and the result propagation must be specified (especially which component calls the MessageChecker and which component receives the result).	this is from an architectural point of view out of scope for CONVERGE	forward to AP3 for CONVERGE solution

Use case: US-RWW1		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The mechanism to start up all components at the TC backend has to be described	All prerequisites that have to be considered for blocking trailer management and "ITS communication" have to be established. Only the external interfaces should be defined not the internal structure	forward to AP3

Use case: UC-C2X-102_02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
cold start / initialization of IVS/IRS components	This includes self tests and initial contact to management instance	forward to AP5 (for IRS) and AP6 (for IVS)
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
IVS/IRS logging procedures	A defined interface for application (how application can access the logging) and for the management (how the logging information is transmitted to the central system management) have to be defined.	forward to AP5 (for IRS) and AP6 (for IVS, here maybe the management part is out of scope for CONVERGE)

Use case: UC-IVS2SP-01_02 Renew Certificates - Reception		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
IVS decodes received message	For Sec and at least ITS safety applications a general message format (e.g. in ASN.1) end encoding must be defined.	forward to AP0.4 (for sec) and AP5/AP6 (for safety messages)

Use case: UC-SP2IVS-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Logging for SPs.	this is from an architectural point of view out of scope for CONVERGE, it must only guaranteed that such a thing exists (replicability, auditability)	no action needed

Use case: UC-SP2IVS-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Description of the startup and shutdown routines of all modules of a SP backend.	Definition of all services and interfaces that must be available for a SP to communicate with the SN (and so with other SP, CN or IVS/IRS)	forward to AP3

Use case: UC-C2X-103_01-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
IEA mechanism at SP backends	this is the interface (including data format) definition and the definition of the communication (protocol, coding, push/pull, ...)	forward to AP3

3.3.5 Security requirements

Security is a very important part of the Car2X Systems Network and thus a number of points related to IT security have been detected during the work out of the use cases. The following tables are summarizing the questions and feedback generated during the analysis process.

Use case: UC-SP-05		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The general concept of security has to be described. This includes: - general trust concept - architecture of security concept - threat analysis and security features - certification formats, features	This is not a use case, but a requirement covered by the security requirements.	no further action needed
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The details of certification generation rules have to be specified	This is not a use case, but a requirement covered by the security requirements.	no further action needed
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The renewal concept of certificates has to be specified in detail (e.g. renewal periods, renewal methodology, certificate distribution, …)	This is not a use case, but a requirement covered by the security requirements.	no further action needed
Question:	**Points to be considered:**	**Proposed way forward:**
Definition of the general set up of CA(s). For example it has to be defined if there is one central CA or if there are several CAs. The general trust concept also has to be defined.	The CAs will form a hierarchy: a basic "Root CA" will form the central root of trust and is thus at the top of the hierarchy. The certificate of this root CA has to be installed into all participants of the C2X-SN. Below this CA, there are several sub-CAs: * LTCA: Long-term CA, this CA manages the long term identities of IVS-Ss. * PCA: Pseudonym CA, provides short term certificates for IVS-Ss to serve as pseudonyms. * optional: SPCA: Service Provider CA, manages long term identities of service providers * optional: IRSCA: IRS CA, provides long term certificates for road side infrastructure In order to allow a "provider open" operation, there multiple Root CAs are possible. The certificates of all Root CAs has to be installed into all participants to serve as roots of trust (if a Root CAs certificate is not known to a participant, the participant cannot trust any certificate	Details to be worked out in the security task force

Use case: UC-SP-05		
	provided by all of the Root CA's sub-CAs. An option to avoid the installation of all Root CA certificates is cross-certification. A participant can trust a Root CA certificate if it is signed by a known and already trusted CA.	
Question:	**Points to be considered:**	**Proposed way forward:**
The concept of certificate distribution and renewal has to be defined in detail (e.g. how are renewed certificates made know to participants of the C2X-SN, how often is a renewal required, which conditions lead to renewal, …)	New certificates do not need to be "made known" to the C2X-SN. They are generated by the corresponding CA, signed by it and installed into the requesting participant. If this participant uses this certificate to ensure trust in transmitted messages, the recipient of such messages can verify this trust if it trusts the issuing CA or the issuing CA's Root CA. The method used to request pseudonym certificates is the procedure proposed by the C2C CC. The method of how to deploy certificates of long term certificates is left open as this may vary for each participating company. Certificate revocation: * Pseudonym certificates: there is such a huge number of certificates in the field that revocation does not make sense. This would also dramatically increase the computational costs of checking the validity of incoming messages at an IVS if the message's signing certificate has also to be checked if it is within a potentially very long certificate revocation list (CRL). * Long term certificates for IVSs: they have to revoked. But as they are only needed during for the request of pseudonym certificates, the CRL has only to be checked by the CAs * Long term certificates for SPs: As they have communication relationships with IVSs, they have to be revoked and the CRLs have to be distributed throughout the C2X-SN (including the IVSs).	Details to be worked out in the security task force

Use case: UC-IRS2SP-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
There is a security mechanism, which checks the authenticity of G5-Messages.	Covered by the security requirements.	no further action needed
Question:	**Points to be considered:**	**Proposed way forward:**

Use case: UC-IRS2SP-02		
What means secure in this Use Case.	This depends on which data is collected, processed and sent to the SP. The fulfillment of any security requirements is possible. The protocol intended for secure communication (ETSI TS 103 097) supports message authenticity and integrity. Optionally, it also supports confidentially.	Details to be worked out in the security task force

Use case: UC-SEC-001 Misbehavior Detection		
Question:	**Points to be considered:**	**Proposed way forward:**
There is a central component within the C2X System network that further handles reports on misbehavior detections.	There is one (or maybe several) Misbehavior Posting Boards (MPB) to collect pseudonymous data indicating misbehavior of participants. This MPB corresponds with the misbehaving entities' CAs to resolve their true identities. With these identities the CSA will be notified to decide whether to exclude the misbehaving participant from the C2X-SN.	Details to be worked out in the security task force

Use case: UC-SP-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A credential authority exists to enable CONVERGE entities to verify security credentials.	CONVERGE entities do not require a credential authority to verify credentials. Instead, each entity can check the validity of certificate chains on its own. However, root of trust authorities are needed to create these chains.	no further action needed
Question:	**Points to be considered:**	**Proposed way forward:**
The used algorithms and methods for message encryption, authenticity and integrity must be specified.	The used algorithms are specified in ETSI TS 103 097: * SHA256 * ECDSA with NIST P-256 curves * AES-128 CCM * ECIES with certain parameters	no further action needed

Use case: UC-LHW		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Registration of OEMs #1, #2 and #3 with the C2X-SN as “Service Providers, Type X” and reception of C2X-SN access premising certificate (APC_SN)	Covered by UC-C2X-101_01 and following	no further action needed

Use case: UC-LHW		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Interface service to support charging, KPI supervision or security inspection functions	The misbehavior detection part is covered by UC-SEC-001	no further action needed

Use case: US-RWW1		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The mechanism to generate and distribute security information (e.g. certificates, encryption keys) from a certification body to the blocking trailer have to be defined and implemented	This is not a use case, but a requirement covered by the security requirements.	no further action needed

Use case: US-RWW2		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A mechanism has to be provided that allows to generate and distribute security data (keys, certificates) to all participants of the C2X-SN	Identical to the previous use case.	no further action needed

Use case: UC-C2X-102_02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Check authorization of client to obtain new sw, check signatures, identities, subscribed services, …	This is either covered by general ITS security OR by service-specific security mechanisms.	no further action needed

Use case: UC-ComNet-01		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
What is done with security violations?	This is outside the scope of the security group, but it is a valid use case.	no further action needed

Use case: UC-IRS-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The application has been certified for the C2X systems network	Covered by UC-C2X-101_02	no further action needed

3.3.6 Service management requirements

As it is foreseen to keep the system flexible, there is a need to define a framework that is dealing with the management of services in the Car2X Systems Network. The following tables are summarizing the questions and feedback generated during the analysis process.

Use case: UC-LHW		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Notification Mechanism for notifying service participants about changes in a service they have been registered to	Possible solutions are proposed in D3	To be worked out in further detail in D4
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Contact mechanism to reach the C2X-SN Service Description ("yellow pages") Service	Possible solutions are proposed in D3	To be worked out in further detail in D4
Question:	**Points to be considered:**	**Proposed way forward:**
Find a way to realize the C2X-SN Service Directory	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-SP-03		
Question:	**Points to be considered:**	**Proposed way forward:**
Methods to ensure service availability are in place.	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-IVS2SP-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Registration of IVSs with the C2X-SN as “Data Providers" for sensor readings data and reception of C2X-SN access premising certificate (APC_SN)	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-IVS2SP-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Registration of SP #1 with the C2X-SN as “Service Provider, Type X” and reception of C2X-SN access premising certificate (APC_SN)	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-SP-05		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
It has to be specified in detail, how the initial set-up of the service CD-A-NB is done at all participants of the C2X-SN (via installation in SW, via bootstrap mechanism, …). This ensures that all participants of the C2X-SN are able to at least use generic initial security services.	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-C2X-102_02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Registration of IVS/IRS for service	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-C2X-102_07		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
service de-registration	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-IRS-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Services provided via backend communication are announced to the service provider or communication networks.	Possible solutions are proposed in D3	To be worked out in further detail in D4
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
Restrict specific ITS functionalities to dedicated services.	Possible solutions are proposed in D3	To be worked out in further detail in D4

Use case: UC-C2X-103_01-03		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The directory service has to be provided by the overall system.	Possible solutions are proposed in D3	To be worked out in further detail in D4

3.3.7 Software and device management requirements

As the system should be able to be extended and modified during its lifetime, there is a certain need for introduction of software and device management. The following tables are summarizing the questions and feedback generated during the analysis process.

Use case: UC-C2X-102_02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
SW management process at service provider including storage of new sw objects at SP and compatibility testing	OEM/vendor specific, not to be defined as normative in CONVERGE -> no additional use case, but prerequisite on SP side (the SW Mgmt process at SP has to exist and been started)	no action needed
Question:	**Points to be considered:**	**Proposed way forward:**
Decide if announcement of new SW version by SP is needed or if pull-only mechanism by IVS/IRS is preferred	Service specific, not to be defined as normative in CONVERGE -> optional for reduced traffic load	no action needed

Use case: UC-C2X-102_03		
Question:	**Points to be considered:**	**Proposed way forward:**
Is a backup of previously installed (older/working) sw version necessary before installation of new sw? What happens if sw install fails?	OEM/vendor specific, not to be defined as normative in CONVERGE -> backup recommended for communication firmware updates in order to prevent "bricking" of communication modules; a fallback onto old firmware version ensures sustainability of communication link	no action needed
Question:	**Points to be considered:**	**Proposed way forward:**
It might be necessary/useful to describe different sw management procedures for the various number of system components (e.g. different procedure for LTE modem fw update and application sw)	Vodafone recommend usage of "Lightweight M2M standard" for device management of LTE modules. This standard is also feasible for sw updates of application layer modules	no action needed

Use case: UC-C2X-102_04		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
IVS/IRS sw package download	use case already exists: UC-C2X-102_02	no action needed
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
IVS/IRS sw package install	use case already exists: UC-C2X-102_03	no action needed
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
sw initialization process (IVS/IRS vendor specific)	part of initialization procedure of IVS/IRS	no action needed

Use case: UC-C2X-102_04		
Question:	**Points to be considered:**	**Proposed way forward:**
Are there special treatments necessary before the SW is activated (e.g. only allowed at workshop, trigger only manually, …)	OEM/vendor specific, not to be defined as normative in CONVERGE	no action needed

Use case: UC-C2X-102_07		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
IVS/IRS component uninstall sw procedure (vendor specific)	OEM/vendor specific, not to be defined as normative in CONVERGE -> no additional use case, but prerequisite on SP side (a procedure has to exist, which installs/uninstalls sw packages within IVS/IRS)	no action needed
Question:	**Points to be considered:**	**Proposed way forward:**
Is it necessary to inform SP about sw uninstallation at IVS/IRS?	OEM/vendor specific, not to be defined as normative in CONVERGE	no action needed

Use case: UC-IRS-02		
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The remote installation/update/deinstallation of application in an IRS is defined and possible	use case already exists: UC-C2X-102_02/03/04/07	no action needed
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
The Application must be remotely configurable.	OEM/vendor specific, not to be defined as normative in CONVERGE -> depending on specific application; if the app needs to be configured it makes sense to have it done remotely.	no action needed
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A remote management must be able to administrate, install/uninstall, configure and monitor application on an IRS application platform.	generic use case already exists: UC-C2X-102_02/03/04/07 -> can be used for all types of applications, not only for monitoring applications	no action needed
Missing Detail:	**Points to be considered:**	**Proposed way forward:**
A central application repository is needed. (For all application or only for an IRS network, or…)	OEM/vendor specific, not to be defined as normative in CONVERGE	no action needed

4 ARCHITECTURE OPTIONS

4.1 Definition of architecture blocks

Based on the technical requirements and reviewed user stories several functional blocks and interfaces were identified. A functional block is a logical entity which is implantation dependent and could also be distributed over various HW entities. The following list summarizes the blocks identified during the review. Thereby different user stories and requirements produced equal blocks with different names and also blocks with (early) equal names but different functionalities. To overcome these differences and to produce a consistent view for the architecture a set of blocks was created that summarizes and equalizes the identified blocks for systems network architecture.

4.1.1 Definition of Blocks

Table 8 shows the most important and defining blocks and provides a brief description for each block. In addition the abbreviation for each block is given.

Table 8: List of Detected Components

Functional Block	Abbreviation	Description
Application Processing	ApP	A component that performs service specific actions (e.g. provide a warning message to the driver of a car via HMI). There are different subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.
C2X Initialization Body	C2X-IB	An institution that is responsible for the set-up of contractual frameworks and dedicated contracts for services and access inside of the C2X Services Network
Certification Authority	CA	Certification instance for service and service provider certification. The term CA is used as a generalization of the more specific terms LTCA, PCA and RootCA.
Communication Hub	CH	Physical/logical entity that handles communication. The CH is responsible for all outgoing communication and is the counterpart for the IEA. It also handles Security and QoS.
Communication Network	CN	The CN provides communication capacity for all kind of other services
Contract Supervision Authority	CSA	The (human) body that is responsible for authorizing the generation, supervision and revocation of certificates used to access the C2X-SN. It also regulates the legal part and ensures that all participants meet the necessary requirements.
Exception Posting Board	EPB	Entity that is informed when an exception regarding the C2X-SN functionality occurs. This instance should also initiates the necessary steps to inform affected participants and if possible solves the issue.
Facility Processing	FAC	Processing steps for messages inside an IVS/IRS, that are application independent (e.g. Message distribution or CAM creation)
Geomessaging Function	GEOM	Server in the C2X-SN and/or SP and /or CN that distributes information to clients in a geographical area.
Global Transaction Logging	GTL	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for

Functional Block	Abbreviation	Description
		security reasons (e.g. repudiation), fault management or billing constrains.
Incoming Event Alert	IEA	Running on all communication endpoint entities. It represents the SAP for all incoming messages.
ITS Roadside Station	IRS	Communication equipment on the roadside for vehicle to infrastructure communication. IRS can be located for example on gentries, traffic light or blocking trailer.
ITS Vehicle Station	IVS	The mobile "user" of a service, can be a vehicle or a mobile phone
Long Term CA	LTCA	Providing long term certificates to the participants used to obtain pseudonyms.
Management Console	MC	Management Interface for e.g. human interaction (e.g. for services start/stop, services installation). In addition MC also monitors the services and resources on the running platform.
Misbehavior Posting Board	MPB	Entity that is informed about any security and service misbehavior. It will take or initiate the necessary technical or legal measure (caution or exclude participants) depending on the amount and severity of the misbehavior.
Mobility Data Marketplace	MDM	Entity for data exchange. A special SP for SP to SP traffic related information distribution (see MDM Description).
Monitoring	Mon	Monitoring component for IRS/IVS, SP, …, not a centralized monitoring
Pseudonym CA	PCA	CA providing valid pseudonyms to the participants used for actual communication with other participants
QoS Function	QF	The QF is responsible for all kind of QoS related data gathering and adjustments.
Root CA	RootCA	Main CA signing certificates for all CAs in the hierarchy.
Rule Engine	RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN according to certain rules.
Security Processing	SecP	Message en/decryption and signing/verification process (on SP and IVS/IRS). The SecP is involved in all kind of communication (IVS to SP, SP to SP, …) and also handles the certification management.
Sensor Data Provider	SDP	Entity that collects information from sensors, GNSS positioning data, … on IVS/IRS
Service Announcement	SerAnn	SerAnn sends announcements to services clients to inform them about available services. This can be done e.g. as part of the SD in SP-related services, or as IVS/IRS related with IVS/IRS services (e.g. from an IRS)
Service Directory	SD	An electronic "yellow Page" like service (e.g. UDDI) that holds, maintains and shares detailed information about all services that are available and their operational status. In addition on an SP side it can hold the information about the registered IVS and their services. It also informs registered user about new available services/information. This can be inside the C2X-SN itself and/or inside a SP. The SP can distribute all or a subset of this information to the "global" SD in the C2X-SN
Service Platform	ServP	The platform on an IRS/IVS or SP where the actual ApP is running and where they are managed.
Service Provider	SP	An entity that provides a service to other entities. In the

Functional Block	Abbreviation	Description
		CONVERGE architecture SP is only the SP directly connected to the C2X-SN, not the IVS or IRS as they are mobile and not always connected.
Service Test and Certification Institution	STC-I	Human and electronic instance that is responsible for the test and certification of safety relevant application.
Service Usage Agreement	SU-A	Legal instance for bilateral contracts between SP; used for non-free accessible services.
Software Management	SWM	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtypes like client (incl. installation), server, application repository, etc.

4.1.2 Classification of Blocks

Table 9 classifies the blocks into three different categories.

Placement

The columns 3 – 7 (red) in the table identify in which part of the CONVERGE system the block can exist. An ‘x’ represents the existence of a block in this system part. A ‘(x)’ represents the possible existence in this system part. This is only relevant for communication networks (CN), as this strongly depends of the actual design of the CN. The last red column ‘external’ is for blocks not inside the CONVERGE system. Such a block can be for example a legal institution for services agreements.

Existence constraints

The columns 8-10 (green) indicate the existence of conditions for a block. There are the following three alternatives

- **Mandatory**: This block has to be present in all manifestations of this block and in all before mentioned system parts. Additionally ‘mandatory’ means that there are fixed conditions, functions and interfaces for this block, which have to be fulfilled.
- **Optional**: This block may not be present in an actual system, but during the design of the architecture these blocks were found very helpful.
- **Conditional mandatory**: This block has to be present but only the features are mandatory, the actual interface and implementation are open and can be vendor specific.

Block type

The columns 11-13 (cyan) specify what kind of block it is. There are three characteristics:

- **Component**: Actual technical component that has a well-defined purpose, but not necessarily a piece of hardware or software.
- **Interface**: Public Interface between participants of the systems network (IVS, IRS, CN, SP)
- **Functionality**: Functionality inside a component or system part (IVS/IRS, CN, SP), not necessarily a component or interface.

The last column (orange) informs about the work packages (WP) of the CONVERGE project in which the block will be specified in detail.

Table 9: Classification of Detected Components

Functional Block	Abbreviation	IVS/IRS	SP	CN	C2X-SN	External	Mandatory	Optional	Conditional mandatory	Component	Interface	Functionality	WP
Application Processing	ApP	x	x	(x)					x	x			3/5/6
C2X Initialization Body	C2X-IB					x	x					x	2
Certification Authority	CA		x	x	x	x	x			x	x		3
Communication Hub	CH	x	x						x			x	3/5/6
Communication Network	CN			x			x				x	x	4/5
Contract Supervision Authority	CSA					x			x			x	2
Exception Posting Board	EPB	x	x	x	x				x		x	x	2
Facility Processing	FAC	x						x		x			5/6
Geomessaging Function	GEOM		x	x	x				x	x	x		2/3/4/5
Global Transaction Logging	GTL	x	x	(x)					x			x	3/4/5/6
Incoming Event Alert	IEA	x	x				x				x		3/5/6
ITS Roadside Station	IRS	x					x			x			5
ITS Vehicle Station	IVS	x					x			x			4
Long Term Certification Authority	LTCA				x		x			x	x		3
Management Console	MC	x	x	x				x				x	3/4/5/6
Misbehavior Posting Board	MPB		x		x				x		x	x	2
Mobility Data Marketplace	MDM		x		x			x		x	x		3
Monitoring	Mon	x	x	x					x			x	3/4/5/6
Pseudonym Certification Authority	PCA				x		x			x	x		3
QoS Function	QF			x					x		x	x	4/5
Root Certification Authority	RootCA				x		x				x	x	3
Rule Engine	RE	x	x					x				x	3/4/5/6
Security Processing	SecP	x	x				x				x	x	3/4/5/6
Sensor Data Provider	SDP	x							x			x	5/6
Service Announcement	SerAnn	x	x	(x)			x					x	2/3/4/5/6
Service Directory	SD		x		x		x			x	x		2/3
Service Platform	ServP	x	x						x			x	3/5/6
Service Provider	SP		x				x			x			3
Service Test and Certification Institution	STC-I					x			x	x		x	2
Service Usage Agreement	SU-A					x			x			x	2
Software Management	SWM	x	x	(x)				x				x	3/5/6

4.2 Description of architecture options for given requirements

During the detailed analysis of the use cases specified in D1.1 a number of architecture decision points have been identified which are of major relevance for the architecture of the Car2X-SN and which therefore need a more detailed evaluation in terms of possible solutions and their suitability for the given use cases. Those issues are described in detail in this chapter together with possible implementation options.

4.2.1 Quality of Service provisioning and differentiation

Quality of Service (QoS) for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical application. The goal of QoS is to provide preferential delivery service for the applications that need it by ensuring parameters like sufficient bandwidth, controlling latency and jitter and reducing data loss. Since the QoS measurements are related to the performance of networking applications, these parameters could be grouped in three categories: timeliness (delay, response time, jitter...), bandwidth (throughput, transaction time...) and reliability (packet loss rate, bit error rate, percentage of time available, mean time to failure, mean time to repair, mean time between failures...). Among them, the most widely used for communication systems are delay, jitter, throughput and packet loss rate. The typical mechanisms to handle these parameters and provide QoS are admission control and traffic control (or a combination of them). The former one, determines which applications and users are entitled to network resources, answering questions like: how, when And by whom network resources on a network segment can be used? Traffic control regulates data flows by classifying, scheduling and marking packets based on priority and by shaping traffic. Once agreed a QoS, diagnosis of violations can be made with rule-based methods which require clear margins of QoS parameters in asserting a QoS violation. Other alternatives could make use of more complex techniques like neural networks, logic regression, expert systems and data mining.

The most common QoS measurement architecture includes: measurement points (located at nodes), traffic measurement tool (captures packets and collects information of the desired traffic flow), QoS analysis tool (analyzes the collected data and calculates the actual QoS statistics) and QoS database (gather the information). The complexity of QoS measurements and accuracy increases with the number of measurement points, e.g. only single point measurement are simple, the information provided is very limited as well as the accuracy.

End-to-end QoS in Cellular Networks

A driver to introduce QoS is to ensure that speech calls in packet-switched systems continue to be available at the same or a higher quality level as in the circuit-switched systems. It must be possible to prioritize emergency calls (and possibly other priority traffic such as hazard warnings) to ensure that even if the networks are heavily loaded, e.g. at New Year’s Eve, this data is transmitted with sufficient quality. Therefore 3GPP defines mechanisms to ensure a specific quality of service (QoS) according to the individual service requirements. The QoS mechanisms defined for 3G networks were advanced and further improved in the specifications of LTE.

QoS handling in LTE networks is network-controlled. Requests for altering the QoS levels can however be made by both, the network servers and the User equipment (UE). The network element responsible for handling QoS requests is the Policy and Charging Resource Function (PCRF). A standardized application function (AF) using the PCRF is the IP Multimedia Subsystem (IMS) system, see IP Multimedia Subsystem (IMS), which handles the application-layer session setup and can use the PCRF to ensure the data associated to that session is properly treated in the network.

Granted QoS requests then lead to the establishment of a bearer with certain characteristics, or to the modification of an existing bearer.

The implementation of the QoS mechanisms in the network depends on the specific cellular network technology. The QoS concept standardized in 3GPP Release 8 is leveraging the so called “bearer” mechanism (see Figure 12), which uniquely identifies the packet flows having the same QoS parameters. Packet filters on the UE and in the PDN-GW/GGSN ensure that the packets are associated to the correct bearer. In the downlink (i. e. at the PDN-GW) it is also possible to use more advanced traffic classification methods such as deep packet inspection.

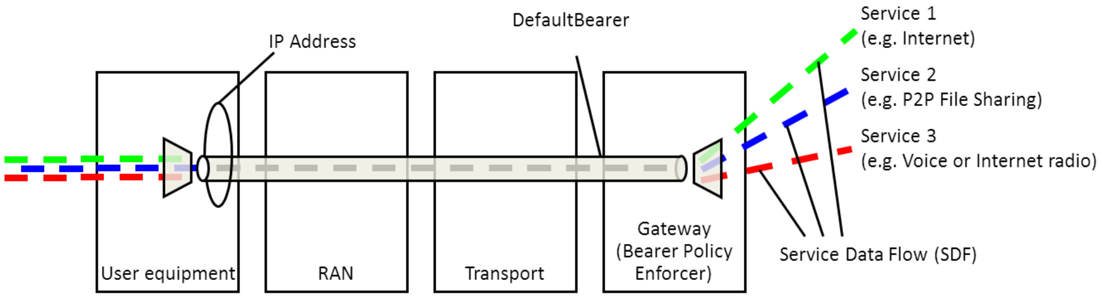

Figure 12: Overview on QoS Mechanisms

Figure 12 also clearly shows that end-to-end quality of service involves number of network elements, i. e. in order to ensure end-to-end QoS, it is not enough to only consider QoS parameters on the radio link.

IP Multimedia Subsystem (IMS)

With UMTS Release 5 and with the accelerating development towards an all-IP core network design, a call and session control system called the IP Multimedia Subsystem was introduced. IMS supports IP-based multimedia and voice applications and is designed for both wireless and wire line networks. It is based on IETF protocols such as the Session Initiation Protocol (SIP) or Diameter, which have been extended for the use in 3GPP networks. IMS simplifies the establishment and handling of end-to-end IP sessions, across multi-user shared radio and wire line links. As side effect, and with particular relevance for automotive use cases, it supports service oriented billing and service oriented QoS assignments by relating different service groups (like telematics safety services and infotainment services) to different IMS sessions.

IMS initiated QoS requests are processed and implemented by the PCRF, described above. Depending on current system load, established QoS requests, QoS classes and priority schemas, the PCRF responds to the requesting system node. Most modern PCRFs are multi tenancy capable so that it can support 3GPP cellular networks with and without IMS extensions at the same time.

Network performance indicators

All mobile network operators use Key Performance Indicators (KPIs) to judge their network performance and evaluate the Quality of Service (QoS) regarding end user perspective. All the events having occurred over radio interface are triggering different counters in the network e.g. NodeB. The KPIs are derived with the help of these counters using different formulations. The observations will lead to RF optimization, which affect the performance, and QoS of an operational cellular network. Normally this optimization is a regular task which is done day by day.

However, the actions described above must not be confused with the highly dynamic allocation and setup of (Radio-) Resources with changing characteristics during the day due to changing traffic situations, busy hours and other scenarios which have impact on load in radio cells and other instants in a network. In this dynamic traffic environment the network measures, evaluates, controls and allocates the available resources based on ongoing measurements and QoS requirements. The KPIs are rather used to optimize and improve the handling and allocation of these resources in order to use the resources more efficiently with regards to the required QoS (e.g. latency, priority, bandwidth, …).

ETSI G5 QoS mechanism

Due the intrinsic characteristics of the ITS G5 network (multichannel, connectionless, frequent topology changes, high channel load...) some typical problems that can come up are a high number of collisions, high packet losses and data load on the wireless channel exceeding the available capacity. This makes necessary a decentralized mechanism to prevent congestion. For that purpose ITS G5 uses a Distributed Congestion Control (DCC) and a Transmit Power Control (TPC) mechanism. On the other hand, it is important to point out that typical parameters used to evaluate the QoS in the group of reliability have to be analyzed and to be chosen carefully, since as it was mentioned before a high packet loss rate is typical from the network and not necessarily means a violation of the QoS agreed.

4.2.2 Geo-addressing / Geo-messaging

Messages of particular services, e.g. Road Hazard Warnings (RHW), have to be delivered to all mobile participants located inside a certain geographical area. This is referred to as geo-messaging. In mobile networks this can be accomplished by means of point to point-to-point (i.e. unicast) or point-to-multipoint (i.e. broadcast/multicast) transmissions.

Both modes require a backend service (i.e. ITS service) that keeps track of the location of mobile participants to guarantee message delivery to all subjects in the addressed area. The unicast mode is always used for the uplink regardless of the downlink mode.

In the case of a service using unicast, the ITS service addresses all the concerned vehicles and infrastructure nodes individually when distributing the message. In order to perform the geo-messaging, the ITS server has to select the recipients based on their location. To this purpose, the ITS service needs some kind of location information about every single user in the service area. One approach to obtain such a user context is that all equipped cars send regularly their status, containing identification, location, heading, speed, etc. to the service. Another approach could make use of network-based positioning to obtain the location information.

The use of multicast and/or broadcast for geo-messaging needs to be further analyzed. In general it can be said that broadcast approaches in mobile networks do not discriminate between certain users. Users/devices listen to different broadcast “channels” and it is in the responsibility of the user to check the relevance of broadcasted data. The network cannot restrict the broadcasted data to the concerned nodes. Therefore it seems necessary to implement encryption of the broadcasted data to cover the case of a restricted (e.g. paid) service using geo messaging or general broadcast.

Geo-messaging approach from CoCarX project

The GeoMessaging function developed in CoCar and CoCarX uses a grid-based algorithm to enable scalable, real-time data delivery to specific geographical area (see Figure 13). The details of this approach can be found in ETSI Technical Report TR 102962 .

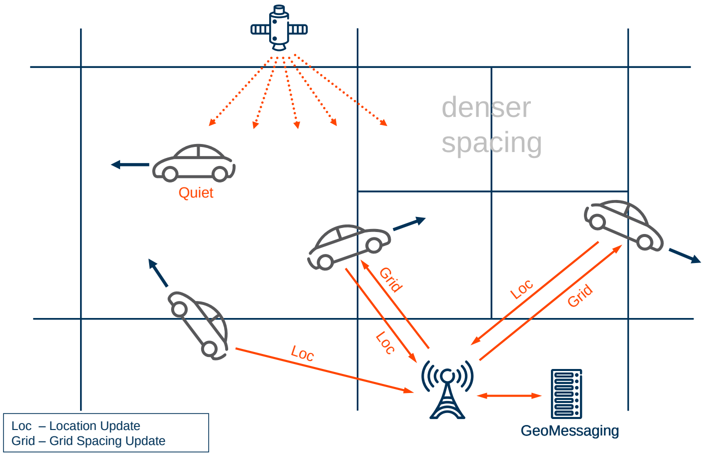

Figure 13: Geo Messaging Concept in CoCarX

The server adds an overlay of square tiles to the map of the coverage area. When clients initially register to the geo-location messaging server (GLM), they report their GPS position. The server associates the respective client with the tile it is located in, saves it in its database and returns the tile borders to the client. The client can then remain quiet until it has crossed the tile border. Then it reports its position again and receives the borders of the new tile. As a result, the server has a complete overview of the client location, however only on a per-tile basis.

Geo-messaging approach from sim^{TD} project

In sim^{TD} there was no priority on developing an optimized way for geocasting. The main focus was to ensure the functioning of C2X application during the field operational trail with about 120 vehicles. So the choice here was a simple but robust concept with not too many modifications necessary in the vehicle system. The chosen approach therefore was to place a central server in the system which has been reachable from each vehicle at any point in time via cellular radio.

Each vehicle station was implementing a special kind of “here I am” message (an adapted CAM message take from the ETSI ITS G5 specification) which was sent periodically to the GeoServer. This message contained information about the current position of the vehicle. This allowed the server to keep a database with the current positions and IP addresses of all vehicles involved in the system.

The destination address for a geocast C2X message to be sent from either a vehicle or a central component was the GeoServer. Inside of the GeoServer each safety relevant message received was checked and compared to the known vehicle positions from the position database.geoserver. The Geo Server compared the locations of the tracked vehicles with the addressed area to identify the desired recipients. Thus the message could be converted into a number of unicast messages and sent out to all vehicles in the area specified in the geocast message. All messages coming from the vehicle side were forwarded to the central side including non-safety messages like vehicle history data (PVD – probe vehicle data).

Figure 14 and Figure 15 shows the overall concept and the message protocol format used compared to the one used in ETSI ITS G5 communication.

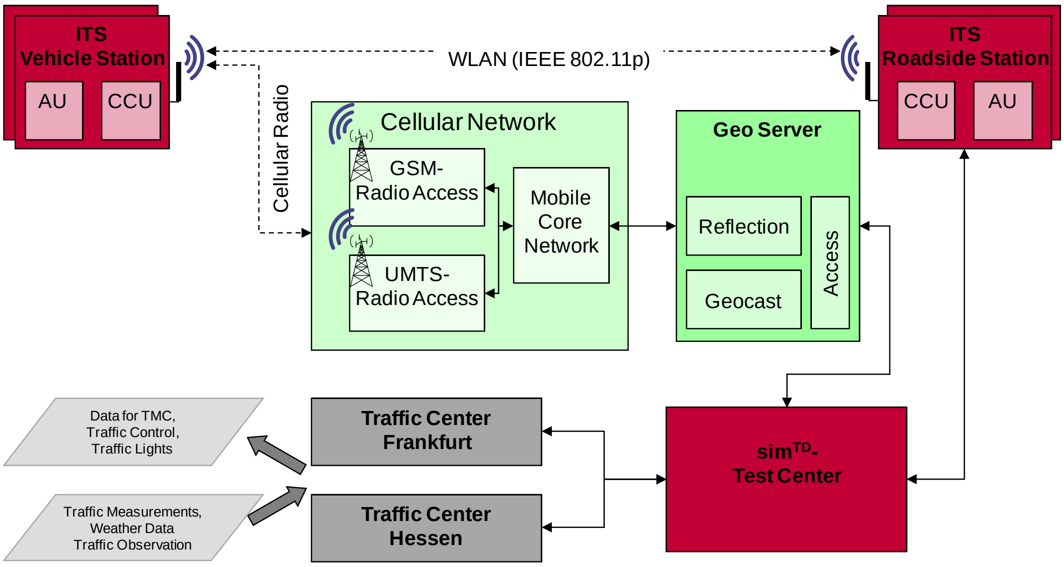

Figure 14: Geo Messaging Concept in sim^TD

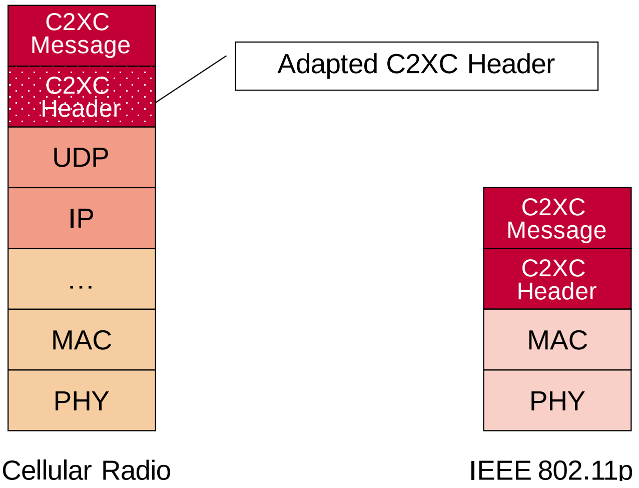

Figure 15: Message Layers in sim^TD

Alternative options of geo-messaging infrastructure placement

Three alternatives for the disposition of the geo-location messaging infrastructure components have been identified. These alternatives need to be examined further in the course of the CONVERGE research activities. In addition, a concept implementing a hierarchical combination of two or more of the following alternatives may have to be considered. The alternatives are shown by comparison of views on parts of the overall architecture (see chapter 5) using the UML format that is also used for the overall architecture view in chapter 5 (see Figure 16, Figure 17 and Figure 18).

Geo-location Messaging Server located in MNO

Pros/Cons

- best propagation strategy can be chosen (unicast/multicast/broadcast)
- Info about location of client is known to MNO anyway – no additional party in the knowledge chain
- SP needs to take care of contacting different GLMs to guarantee maximum spread

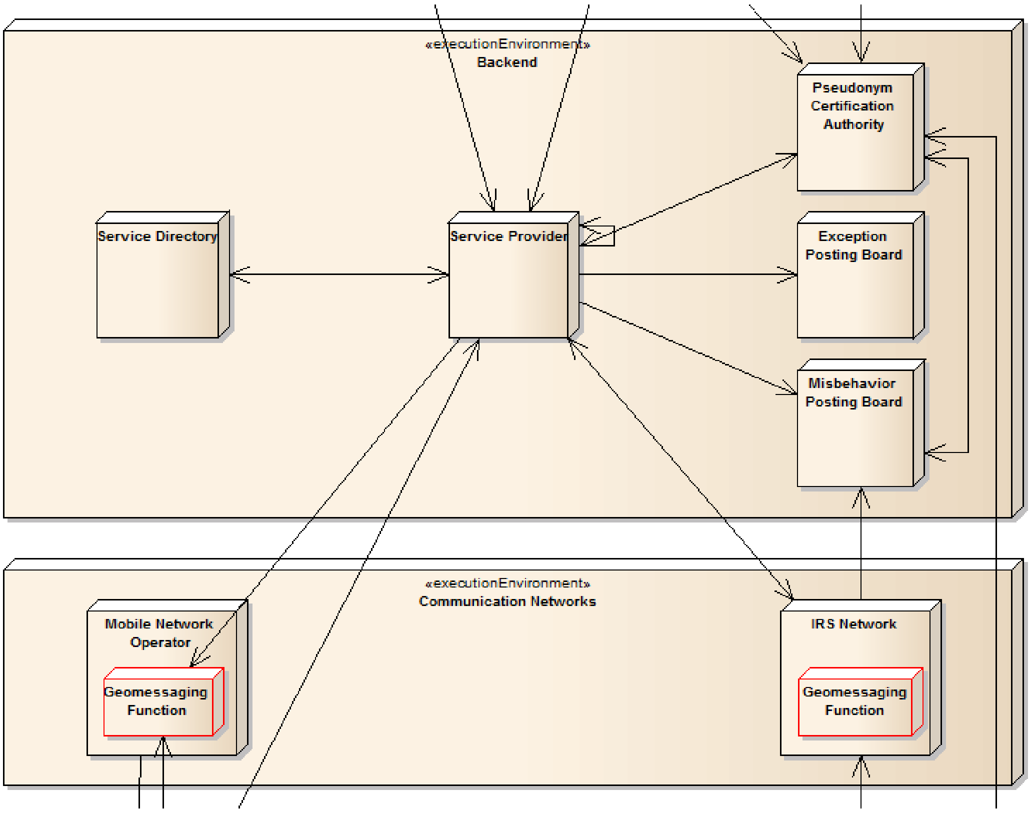

Figure 16: Geo Messaging located in MNO

Geo-location Messaging Server as separate service provider

Pros/Cons

- SP just needs to contact one GLM in order to reach all clients
- MNO cannot leverage broadcast
- Additional party has knowledge about client location

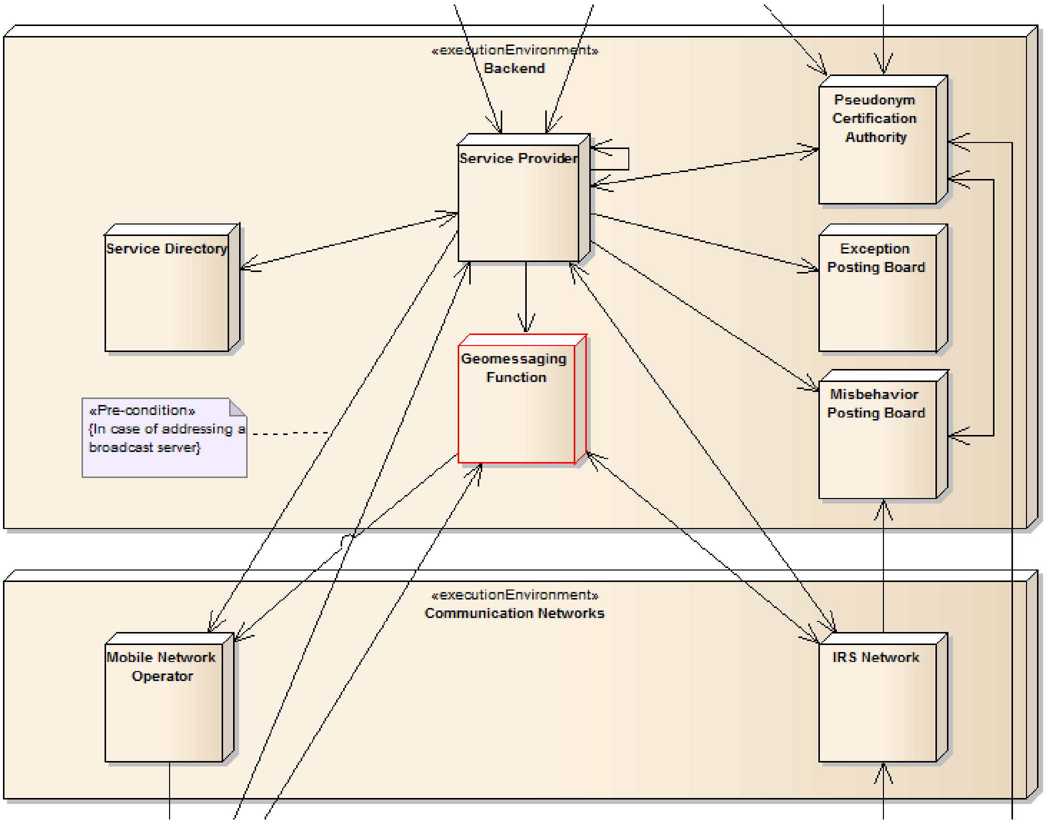

Figure 17: Geo Messaging as separate Service

Geo-location Messaging Server located at each SP

__Pros/Cons__

- SP knows which of its customers should receive the information (have booked the service)
- MNO cannot leverage broadcast
- Additional party has knowledge about client location
- High effort for each SP to implement GLM
- Client needs to keep several GLMs updated about its position

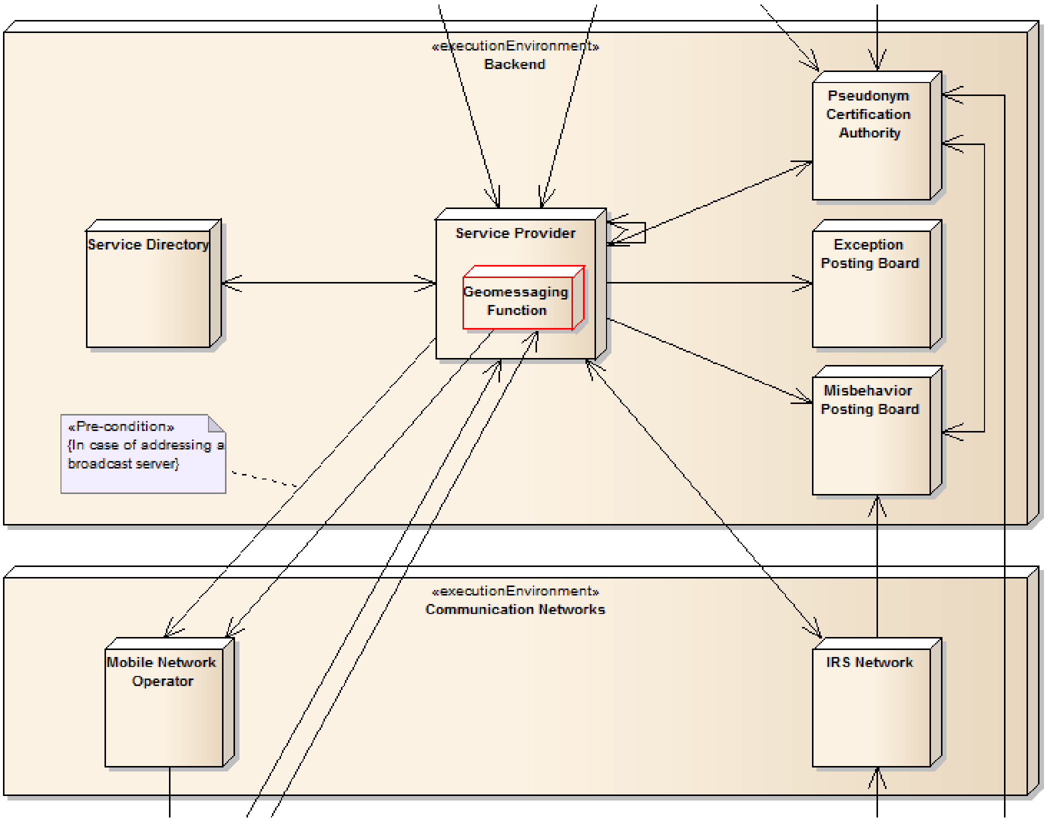

Figure 18: Geo Messaging at each Service Provider

4.2.3 Network Access Selection and Message Distribution

Problem description

The distribution of messages in a hybrid communication network can differ depending on the type of the message and the application. How do multiple radio access technologies (RATs) influence this distribution and how could *cooperative decision* components be useful regarding economics in the whole system network? An efficient distribution to a pre-defined number of message recipients with optimum performance indicators is key necessity in driver assistance oriented message delivery with stringent delay constraints. Since a heterogeneous communication system spans multiple dissemination paths with individual traffic characteristics, a key decision that needs to be taken is the selection of the most appropriate route for message distribution. In addition to this, traffic attributes like *directionality* (up- or downlink information) as well as the *number of message sources* and the *number of traffic recipients* define relevant aspects as for the selection of suitable message distribution protocols. Application characteristics such as e. g. tolerances with regards to *delay jitter*, interpretation of multiple communication links carrying identical information (path diversity), etc. also need to be taken into consideration.

Where should such a decision component be placed in the network? To answer this question the relationship between the source and the sink of a message can be examined (see Figure 19).

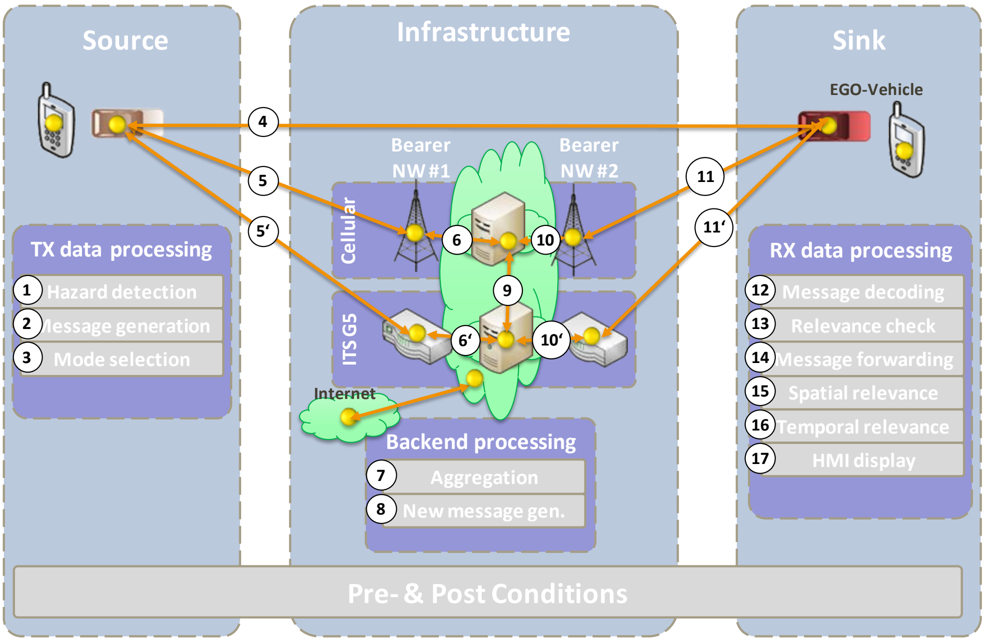

Figure 19: Relationship between source and sink of a message

Status information of the individual RATs such as the availability, robustness, link quality, historical information regarding, e.g. lost connections at specific geo-coordinates, etc. define additional aspects that need to be taken into consideration during network selection.

This leads to the centralized question where to locate relevant decision components in the network. Additionally, in case multiple selection entities are located in the entire network, it needs to be clarified if and how to establish feed-back mechanisms among them in order to allow for synchronous and adapted network selection.

It seems useful to use such decision components not only on the terminal side but also at other nodes within the whole system network (see Figure 20). Also it obviously makes sense to distribute decisions about network selections and their reasons towards other nodes in a cooperative way, in order to facilitate the same decisions at other nodes. This feedback could help to reach a certain "awareness" about the communication environment within and between the nodes and to select the appropriate network technology not only for the moment but also for the immediate future, resulting in reduced network load, less communication errors and higher overall system reliability.

From this point of view new questions arise:

- Where will the decision components be placed inside the system?
- How and what feedback has to be exchanged between these components?
- What are the strategic goals?
  - Cost reduction
  - Load balancing
  - Quality of Service
- Are there applications or application classes, which influence the decision?
  - Simultaneous use of all possible RATs?
  - Dedicated RATs for special applications?

- Which classes allow for intelligent data planning?
- What are the communication concepts?
  - Push/pull
  - Unicast / Multicast / Broadcast

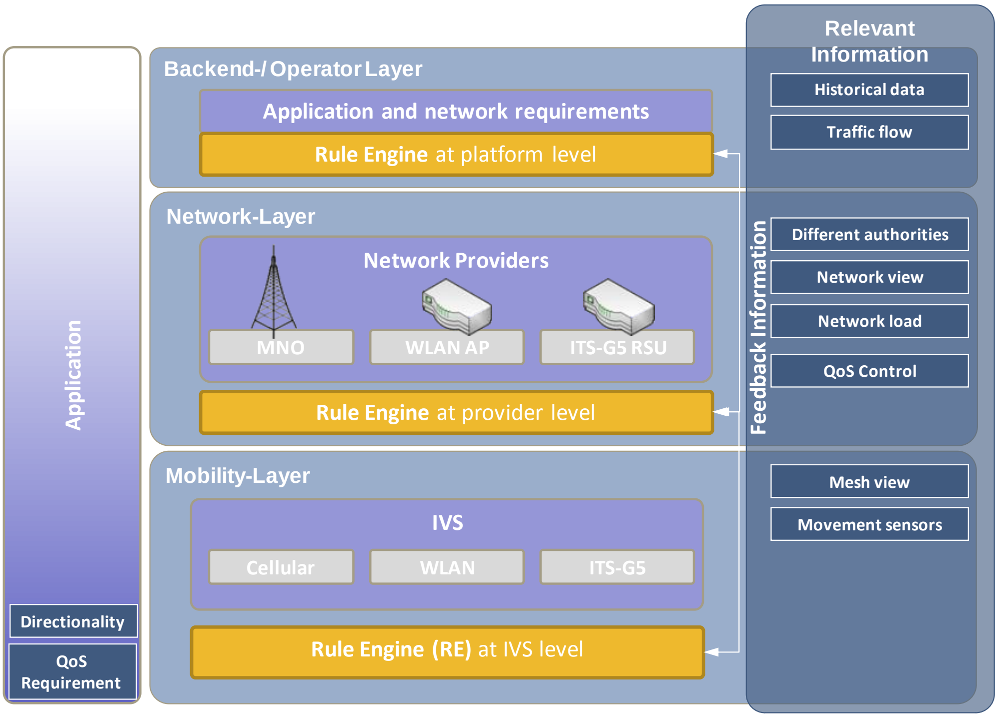

Figure 20: Partitioning of Decision

Definition of reference scenarios and network performance simulation

The aforementioned questions shall be examined by network performance simulations based on defined reference scenarios which include all relevant constraints (e.g. traffic conditions, network load …).

With the simulation results the efficiency of the communication protocols and the optimal distribution of the decider components will be evaluated. Depending on the defined architecture for the overall system network as well as the individual components, different results can be expected and the comparison of multiple simulations might be necessary in order to determine the optimal layout of the decision components.

4.2.4 Data quality

Problem description

Different sources and sinks of information exist in a system network. Information passes different stations, is aggregated and modified. The category of mobility data depends on the *source, data format* and the *geo-refencing technique*. At first, it has to be determined from which source the data are generated (“sensor source”) and in which format they are presented. Here, different sensor classes shall be distinguished (e. g. on-board vehicle sensor, aftermarket device, Smartphone sensor).

The data has to be analyzed and interpreted (e. g. determination of data format in case multiple data formats will be allowed, lane assignment of mobility data), if the data is based on a simple geo-referencing technique with GPS coordinates. In case of geo-referencing data based on “map-matching", it is required to have information about the used map-matching approach. The map-matching approach is necessary in order to allow a comparison of geo-referenced information generated by different sources.

The quality of the sensors generating the messages differ (Smartphone, Car …) from each other. As for the *data format* of mobility data, it shall be differentiated between *raw data* and *aggregated data*. Here, aggregated data means, if additional sensor information from the sensor device has been used to modify, change or improve the data.

For this reason different questions have to be answered:

- What kinds of sources for information exist?
- Does the sink have to perform plausibility checks even if there is a high level of confidence in the source?
- Which source can be trusted and up to which extend?
  - E.g. Full Trust: Vehicle is always confident in its OEM backend
- Which confidence levels have to be defined?
  - Just yes/no or are there steps in between?
- Is confidence related/bound to use cases
  - E.g.: Are safety critical functions only possible based on fully trusted information (e.g. from OEM own backend)
- How many pieces of redundant information from different sources are necessary to reach a certain confidence level
- Do messages need the underlying confidence level as integral part
- How are certificates for confidentiality generated
- General way to "transport" confidentiality information
  - Similar way as trust certificates for IT security
- Should there be sender oriented confidentiality or message based confidentiality or a combination of both.

First steps

To answer the questions above, first existing ways of message distribution and trust will be analyzed. Some of the possible questions that might be checked e.g. for the case of a wrong-way driver warning are listed below.

- How is the existing procedure e.g. for wrong-way driver warning (when distributed via radio stations)?
  - Is there a confidence interval existing (e.g. is the message distributed even if there is only 10% confidence)?
  - What is the validity period of the message?
  - Who decides about invalidity of existing messages?

4.2.5 Service management

CONVERGE will provide an easy to use way to offer services to participants in the Car2X Systems Network. A participant, who offers a service, acts as *Service Provider (SP)*. To publish their services, SPs contact a logical service called *Service Directory (SD)* to register the respective service information in a lookup database. The SD serves as a database which allows different search patterns to look up available services. The SD database stores only substantial information about the published services and acts as a broker between service users and service providers.

Figure 21 shows the relationship of SPs, SD and IVS. The interactions between participants and the required interfaces are described in the following paragraphs.

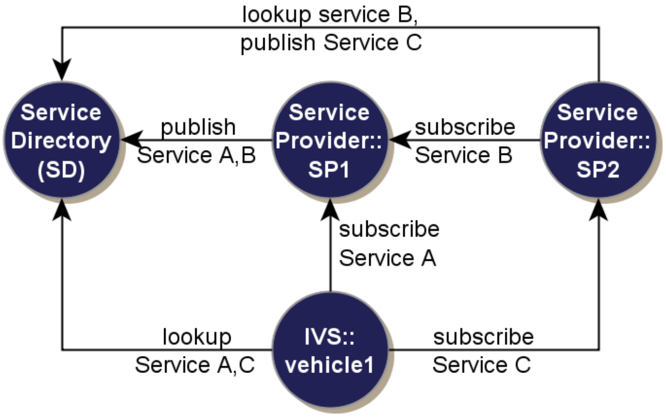

Figure 21: Relationship of Participants in Service Management

4.2.5.1 Usage Principles

Service Publish

Publishing is the process in which a Service Provider is announcing a new service to the Car2X Systems Network defined in CONVERGE. Therefore, an SP has to implement a dedicated interface which will be defined by CONVERGE in form of an API. The SP sends basic information about the new service to a Service Directory (SD). This information contains at least the service name, a brief description, categorization tags, cost and contract information, target group and a link to the Service Provider (SP) to allow unmediated communication. The SD checks the information and the service characteristics and grants the publishing if the service meets all requirements. These requirements have to be defined. The SD returns a unique service ID on grant which is used to identify the service later on. The service information is integrated into the Service Directory database.

Service Lookup

Services which have been published are available and can be found via SD. Services can either be designed for service users which are other SPs, customers in vehicles with an IVS or other connected devices (e.g. Smartphones). Service users are able to send queries towards a SD to find an appropriate service. For the query an interface defined by CONVERGE is used, which may include one or more parts of the information (including tags, name, target group, cost and contract, etc). The SD accesses its data base and returns a list of appropriate services to the inquiring participant including at least service name, service ID, contract information and the link to the service provider (SP). The ITS services network provides an interface to request additional information about the service directly from the SP to provide more details to the service user.

Service Subscription

Knowing the service ID and a link to the service at the SP, the participant is able to subscribe to the service in order to use it. Subscription may be of various forms, depending on the requirements of the service provider. Therefore, all parts of the subscription are optional from a CONVERGE point of view and are only applied if desired. It may contain a registration of the node at the SP for participant specific service, a conclusion of a contract and a software installation. Especially the process of conclusion of contracts has to be supported by the CONVERGE Contract Supervision Authority (CSA). The contracting process shall include a certificate of the SD which verifies that the service has been granted and was not modified since. For contract cancelation, the service can be unsubscribed to finish its use. Software and service specific data is removed on demand.

Service specific Data Transfer

Provider and consumer both offer reliable and unreliable push and pull interfaces to communicate with each other. Interfaces are provided by the Car2X Systems Network via a communication library. This communication is controlled by the services and the local Car2X Systems Network system logic.

Involved components

Service Directory (SD)

The Service Directory (SD) is a service provided by a Car2X Systems Network internal functional component. It is used to publish new services and provides a database to find services in the Car2X Systems Network. It is responsible for granting the publishing of only such services that fulfill the requirements and rules of the Car2X Systems Network. It offers a lookup interface for participants of the systems network, which allows directed and vague search patterns using categories, tags etc.

The Service Directory may be realized in a decentralized structure in which most nodes hold only a subset of service entries and collaborative searches are applied over a couple of nodes. Moreover, good algorithms for distribution of the data bases of granted services and for efficient search have to be applied. This decentralized organization allows for a provider open organization, redundancy and a hierarchical overall configuration of the SD service.

Service Consumption Interfaces

Client Interfaces of the Service Management include service lookup request and service subscription. These interfaces will be offered by a generic Service Consumption API which has to be used by all service consumers.

Service Provision Interfaces

A Service Provider additionally implements Service Provision Interfaces, which are defined in the architecture of the Car2X Systems Network and are provided by a separate Service Provision API. It includes service publishing as well as a service subscription provider interface. A service can furthermore be announced via locally operated IRS on ITS-G5 WLAN with limited bandwidth. An announcement includes at least the information, which is provided by SD on request. Additional bandwidth for public use has to be reserved.

Contracts:

If a contract is required for subscription, the Contract Supervision Authority (CSA) has to be involved into the process. In this process, contract information has to be passed to both parties: to the SD to verify that contract properties are equal to the granted properties and to the CSA which acts as a trustee. The possibilities of how service subscription is accomplished introduce minor options to the architecture and to the functional requirements of components.

The message sequence of publishing, lookup, detail request, contracting and service data transfer is shown in an exemplified way in Figure 22.

Two different options are proposed for contract conclusion. In the first, the SP is responsible for preparing the contract. It is verified by the CSA using information about the service from an independent SD. Most competences lie at the service provider.

Another variant is shown below. Due to contract preparation and conclusion using SD and CSA, the competence is taken away from the SP. The remaining task of the SP is to verify and sign the contract. This way, several details about the user can be hidden from the Service Provider in order to keep the service user anonymous while the Service Directory acts as additional trustee. This may offer additional business models. Besides these two proposals others are possible too and will be further analyzed in the course of the project.

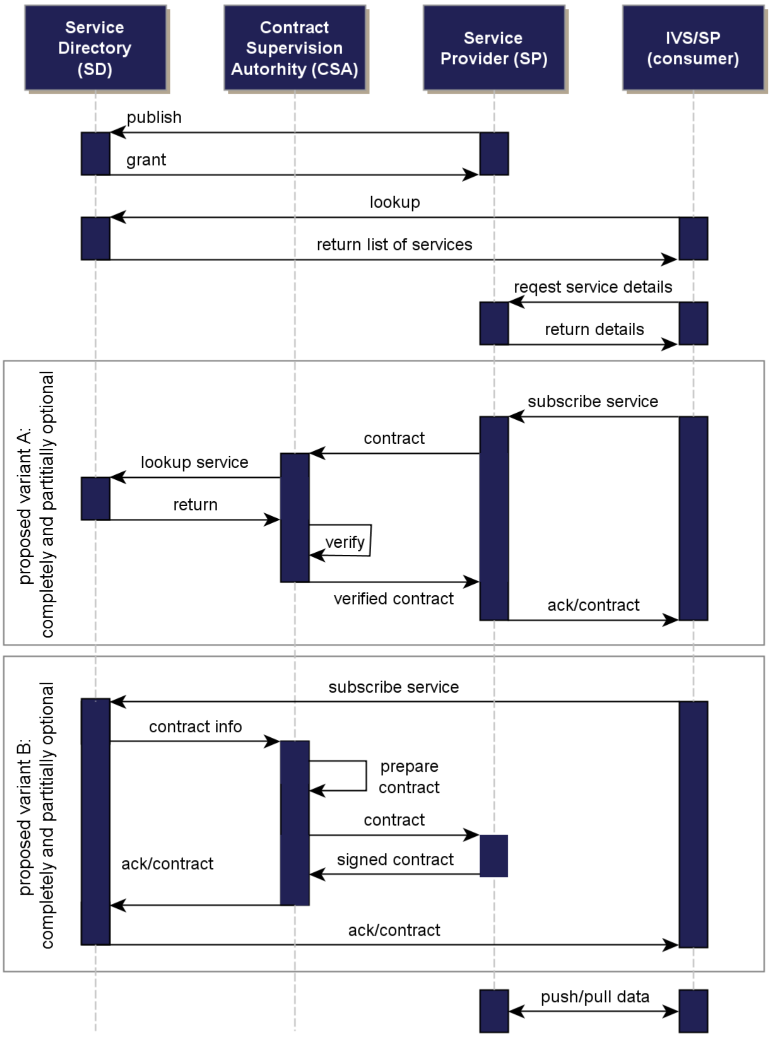

Figure 22: Exemplified Sequence Diagram

4.2.6 External Connections (MDM)

The main external data connection that was identified in the specification of the details of the use-cases was the connection to the so called mobility data marketplace (MDM). The following gives an overview on MDM.

Introduction

The Mobility Data Marketplace was developed and introduced for the exchange of dynamic data relating to road traffic between the centers / back-ends of organizations from the public road operators, private traffic data suppliers as well as traffic information and navigation services.

The goal of the Mobility Data Marketplace (MDM) is to support the exchange of data between data suppliers and data subscribers (B-to-B) with the help of interfaces. At the same time, the MDM forms a central portal where the information about the available online traffic data of individual data providers is collected.

In this way MDM enables its users to offer, find and subscribe to traffic-related data online without a lengthy search for the relevant data and without a complex technical and organizational bilateral agreement between data subscribers and data suppliers. The data exchange is processed via standardized interfaces. As a result the business processes should be simplified for all participants and the potential of the existing data sources should be developed.

In the foreground of the CONVERGE project is the development of open communication, service and organizational architecture. To this the exchange and sharing of online data will play an important role as well. For the data communication between back-ends the MDM is an existing solution which is to be tested in the CONVERGE project in terms of its potential contribution towards achieving the objectives. This document describes the basic architecture of the MDM and its interfaces.

Detailed information can be found on the help page of the MDM: http://hilfe.mdm-portal.de/

System Architecture

The system architecture of the MDM platform is based on a service delivery platform (product name: MACS) developed by the same software producer of the MDM, MATERNA GmbH, which provides components for the aggregation, distribution and marketing of digital content as well as subscription management. Thus the MACS already support the essential applications of the specified MDM platform. The basic product with its fundamental architecture has proved itself in other similar projects and is well equipped for the regular operation of the MDM in terms of the scalability of the used technologies.

Figure 23 shows how the MACS platform has been extended to the MDM platform by using specific project components. Here, a logical definition of the components is shown.

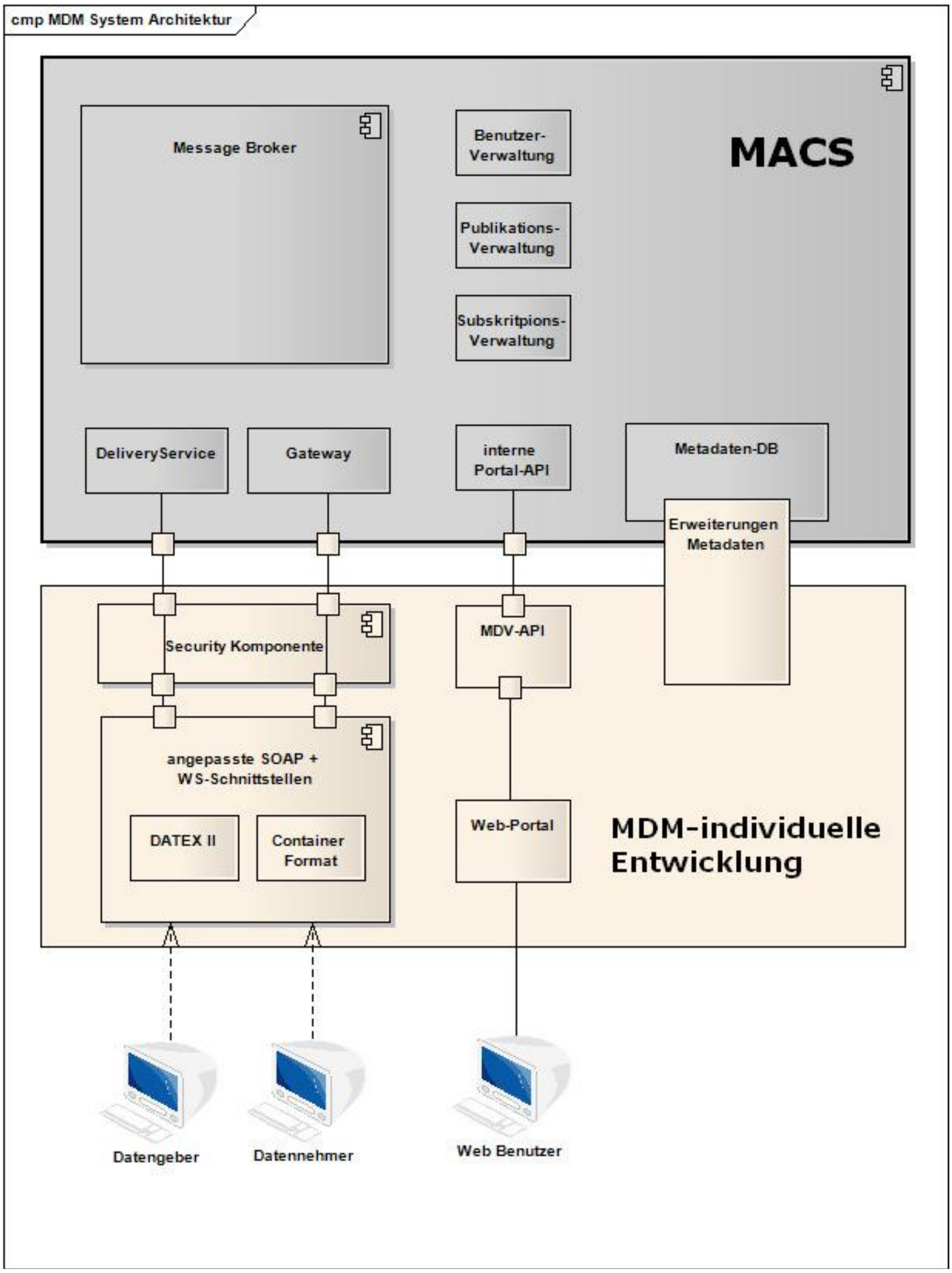

Figure 23: System architecture (source: Materna GmbH)

Security Architecture

The MDM provides authentication, by means of X.509 compliant certificates, for both the users of the web interfaces as well as the machines that handle the M2M communication. The user or machine certificates can either be assigned by the operator of the MDM (current procedure) or can be provided by the users themselves.

The security components include in particular the authentication of data supplier systems and data subscriber systems that want to communicate with the MDM platform.

The origins of the data packets have to be checked before being accepted by the MDM platform. This includes the authentication of the data packet's associated data supplier system by means of a digital certificate. Each data supplier system must have a valid certificate with which it can log on to the platform.

Before a data packet is sent to a data subscriber system the identity of the data subscriber system has to be checked. Each data subscriber system must be authenticated by the MDM platform by means of a digital certificate.

The confidentiality of communications between the MDM and his participants have to be ensured with the exclusive use of a SSL/TLS transport encryption.

The connection between data suppliers and data subscribers is using HTTPS connections and X.509v3 certificates for authentication. The presented certificates will be checked for validity against a revocation list.

If the MDM platform acts as a web client in the M2M communication, it will authenticate itself with its server certificate in case the web server has activated this option on the data supplier and data subscriber sides.

The platform will only accept requests from systems that are registered in the metadata directory. The machine can be assigned to an organisation because of its certificate. Furthermore, it can be checked whether the organization is the owner of the publication or subscription for which an exchange of data is to take place.

MDM Interfaces

The services for data collection and delivery are offered under defined and unified URLs.

For the communication with the broker system a DATEX II format or a container format specially defined for the MDM is used.

The data transfer between the MDM platform can be carried out through SOAP-based web services or simple HTTPS-GET/POST requests. Additionally the OTS 2 protocol is supported for the DATEX II format.

Compressed HTTPS data transmission to the MDM is possible but not mandatory while compressed data transmission from the MDM is allways used.

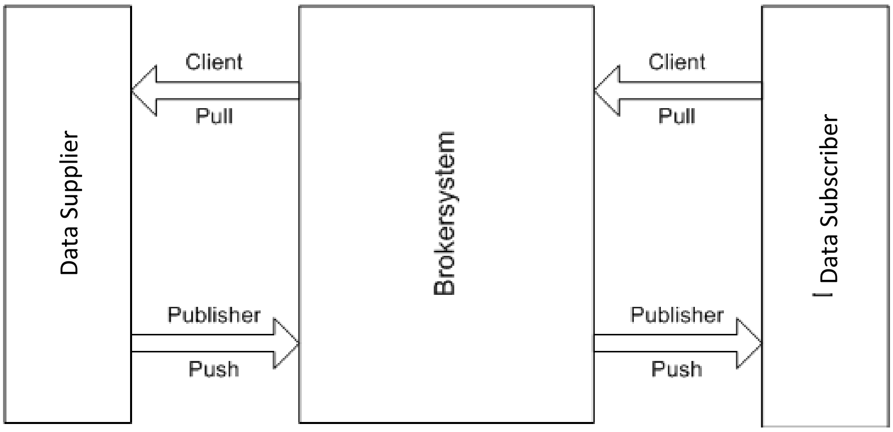

Figure 24: Interfaces between data supplier, broker and data subscriber

As intermediary between the data supplier system and the data subscriber system the MDM broker system takes on the role of the client or that of the server. For the communication either the PUSH/PULL or the publish/subscribe pattern can be used.

Figure 24 illustrates the possible paths available for data packet transmission between

When using the HTTPS or SOAP protocol, there are three different modes of operation for the exchange of data, all of which are supported by the MDM platform:

MDM Usage

It is necessary to register at the MDM before it can be used for the exchange of data. As part of the registration process new users are provided with user certificates and, if needed, machine certificates as well. All functions of the MDM web portal are described in the user manual (download available (only in German) on the MDM Help Page http://hilfe.mdm-portal.de/). In particular, the functions "Create and Manage Publications" and "Creating a Subscription" are of importance for potential data suppliers and subscribers.

Data supplier and data subscription systems must be able to use the interfaces offered by the MDM. The specifications of these interfaces can be found in the Technical Interface Description of the MDM (download available (only in German) on the MDM Help Page).

The MDM is operated 24/7, here the availability of the broker service is 99.6%.

With regards to the "real time" capability of the MDM the SLAs require that 99% of the data packets must have passed the MDM in less than 10 seconds (scalable, currently designed for a load of 50 transactions per second).

Other parameters to the SLAs can be found in the Terms and Conditions of the MDM (download available (only in German) on the MDM website http://service.mdm-portal.de).

5 OVERVIEW ON REFERENCE ARCHITECTURE

The UML diagrams in this section show an overview of the architecture of the Car2X Systems Network. The focus of this chapter resides in the introduction of functional blocks which have been identified so far as necessary to meet the requirements described in previous sections. The functional blocks have been grouped to four headings which are briefly described below.

The arrows connecting the different blocks define the logical connections between the functional blocks.

Note that functional blocks may be distributed over several physical entities, so the UML description neither implies a centralistic nor a distributed architectural approach.

5.1 Governance

The header Governance contains the agreement to basic rules and strategies to ensure security and privacy (see Figure 25).

In order to instantiate the general rules for the Car2X Systems Network, a so-called “Car2X Initialization Body” is introduced which is a kind of players’ agreement on a legal framework. A “Contract Supervision Authority” (CSA) is taking stewardship of this legal framework. If a new player (Service Provider, Communication Network Provider joins the Car2X Systems Network, ground rules have to be acknowledged and committed to.

Most important will be the enabling of the trustful exchange of information between players within the Car2X Systems Network. To achieve this trustful exchange a Public Key Infrastructure (PKI) will be implemented. The PKI is shown here in the form of various Certification Authorities (CA) such as Root CA, Long Term CA and Pseudonym CA.

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

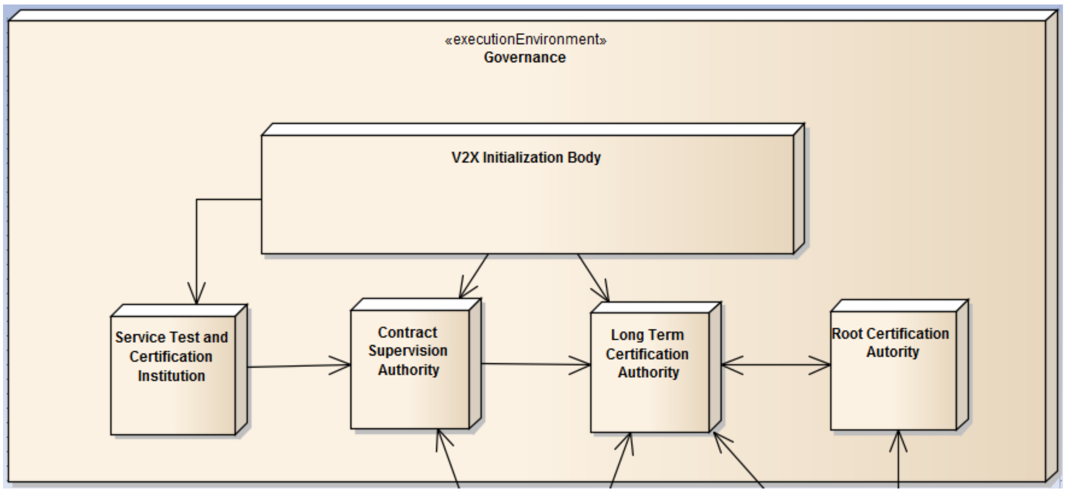
«executionEnvironment»
Governance
V2X Initialization Body
Service Test and Certification Institution
Contract Supervision Authority
Long Term Certification Authority
Root Certification Autority

Figure 25: Overview on Governance Architecture

5.2 Backend /Backbone level

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 (see Figure 26). Examples would be: OEMs, Road Authorities, Communication Network Providers, Data providers of any kind like e.g. MDM.

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.

Additionally it is necessary to become aware of temporary disruption or complete discontinuation of a service it is necessary to have an “Exception Posting Board” as a central entity to which exceptions 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 in different entities within the system.

Another important entity is the “Misbehavior Posting Board” (MPB) to which detected misbehavior of any kind within the Car2X Systems Network can be reported. In a next step this information can be used to trigger an appropriate countermeasure in order to mitigate or stop the misbehavior.

The “Geomessaging” function is necessary to enable distribution of messages to end-users within a certain geographical area. This entity (or hierarchy of entities) can be placed at various locations within the Car2X Systems Network (see 4.2.2).

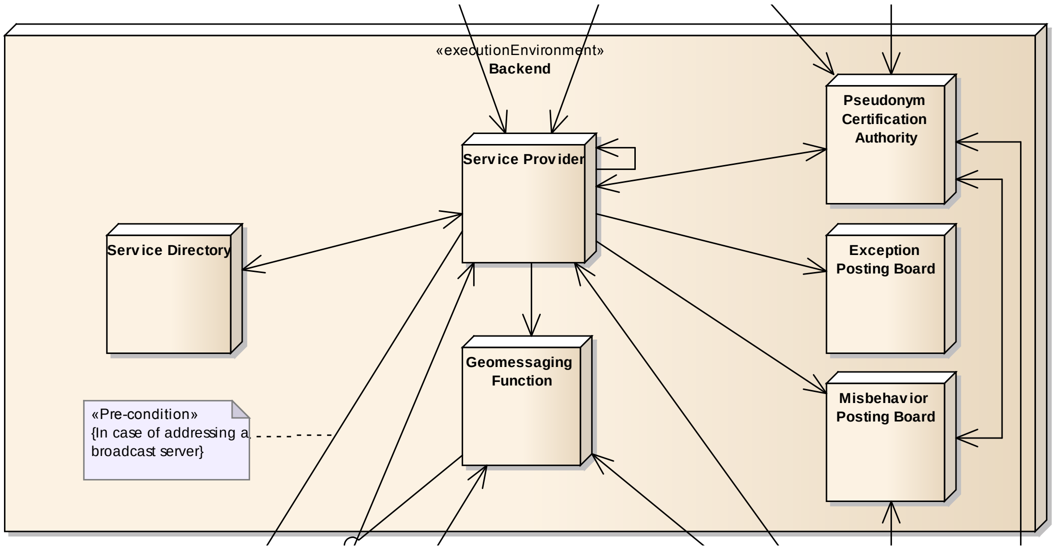

Figure 26: Overview on Backend Architecture

5.3 Communication Networks

Two Communication Networks are examined in the scope of the CONVERGE project: IRS Networks and cellular mobile networks (see Figure 27). These entities can take on several roles within the Car2X Systems Network. One role is of course the one providing transport of information between the Service Providers and the ITS-Station. Communication networks themselves can have certain attributes and can act as Service Providers themselves. The representation of these functional blocks in the UML diagrams is owing to this duality in nature.

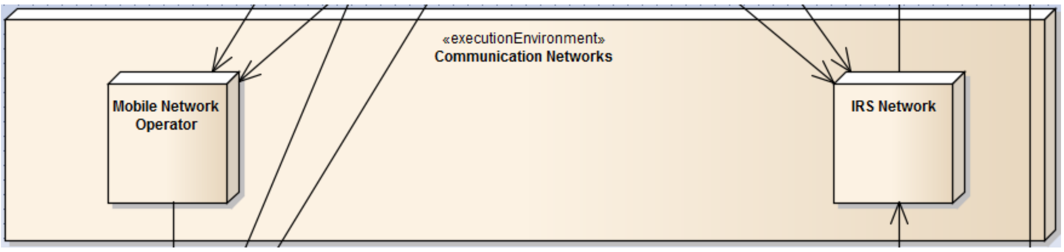

Figure 27: Overview on Communication Networks Architecture

5.4 ITS Stations

There are two types of ITS-Stations distinguished in these UML diagrams: IVS and IRS. The IVS is integrated into a car or is an application on a smart device. The IRS is a unit which permanently or semi-permanently installed on the road side. An example is a blocking trailer present at a road works site.

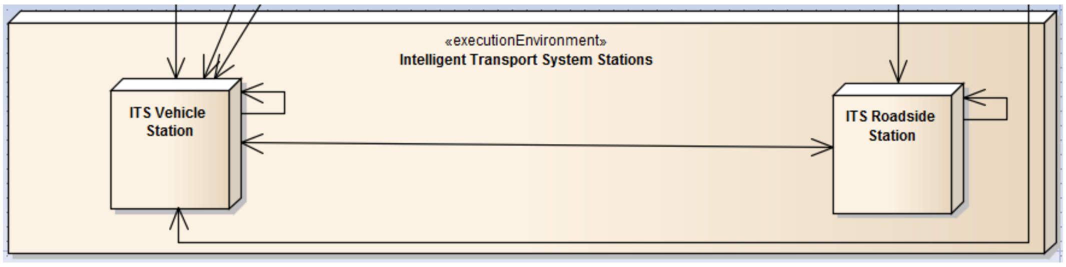

Figure 28: Overview on Mobility Layer Architecture

LITERATURE

CONVERGE Consortium (2013) Converge Deliverable D1.1, Link in Project Place

CONVERGE Consortium (2013) Converge Terms and Abbreviations, Link in Project Place

sim^{TD} (2013) sim^{TD} D21.2 konsolidierter Systemarchitekturentwurf, Link auf sim^{TD} Webseite

BMW (2013) Potential of Cooperative Information for Vertical Handover Decision Algorithms, 16th International IEEE Conference on Intelligent Transportation Systems, Levent Ekiz, Christian Lottermann, David Öhmann, Thang Tran, Oliver Klemp, Christian Wietfeld and Christoph Mecklenbräuker

ETSI (2012) TR 102962 V1.1.1 Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS), Link in ETSI

V-Model Description see web page at http://v-modell.iabg.de/v-modell-xt-html-english/index.html

MDM Description see web page at http://hilfe.mdm-portal.de/

ABBREVIATIONS

See the CONVERGE CONVERGE Consortium and the components list in chapter 4 of this document for the major amount of abbreviations. The following is extending those abbreviations as used in this document.

3GPP	3rd Generation Partnership Project
AP	Arbeitspacket
C2X-SN	Car2X Services Network
DCC	Distributed Congestion Control
eMBMS	Enhanced Multimedia Broadcast Multicast Service
GGSN	Gateway GPRS Support Node
GLM	Geo-Location Messaging Server
IMS	IP Multimedia Subsystem
KPI	Key Performance Indicator
MN	Mobile Node
MNO	Mobile Network Operator
ODP	Open Distributed Processing
PCRF	Policy and Charging Resource Function
PDN-GW	Packet Data Network Gateway
QoS	Quality of Service
RAT	Radio Access Technology
RHW	Road Hazard Warning
SAP	Service Access Point
SDF	Service Data Flow
STCI	Service Test and Certification Institute
SysML	Systems Modeling Language
TPC	Transmit Power Control
UML	Unified Markup Language
WP	Work Package

APPENDIX A: DETAILS OF THE USE CASE ANALYSIS

The details of the analysis of the use cases that is described in chapter (see 3.1) are put to a separate document that can be found at (Link to Document in Project Place) or in the attached appendix.