CONVERGE

COmmunication Network VEhicle Road Global Extension

Proposal for a Car2X Systems Network

Deliverable D3

Functional Requirements and Architecture Options
Appendix A Use Cases, detailed technical evaluation

Version	1.0
Dissemination Level	Public
Project Co-Ordination	HTW
Due Date	30.09.2013
Date of Preparation	30.09.2013

CONVERGE is funded and supported by

Bundesministerium für Bildung und Forschung
Bundesministerium für Wirtschaft und Technologie

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

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 (VW)

Versionsübersicht

Version	Datum	Beschreibung
1.0	30.09.2013	**Erstellung des Dokuments aus Excel Bearbeitungsdateien**

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document contains the results worked out during the generation of deliverable D3 of CONVERGE. It shows the detailed results generated in applying the concept that is described in D3 for each use case out of deliverable D1.1 of CONVERGE. The details are given in form of tables and graphs.

1 OVERVIEW

In the following chapters of this appendix document to deliverable D3 in the project CONVERGE each use case specified in D1.1 is elaborated using a certain procedure (see description in D3 main document chapter 3.1).

For each use case the made assumptions are listed at the beginning. After this the necessary actions that are forming the 3 lifecycle phases (Pre-Operation, Operation, Post-Operation) are given in form of tables and sequence diagrams. After this, the list of components necessary to provide the given use case are shown in a table. Finally the detected architecture decision points and external use cases are listed in two more tables.

Some of the use cases do not generate entries for all of the tables mentioned above. If this is the case, the tables are left empty.

2 USE CASES

2.1 UC-IVS2IVS-01

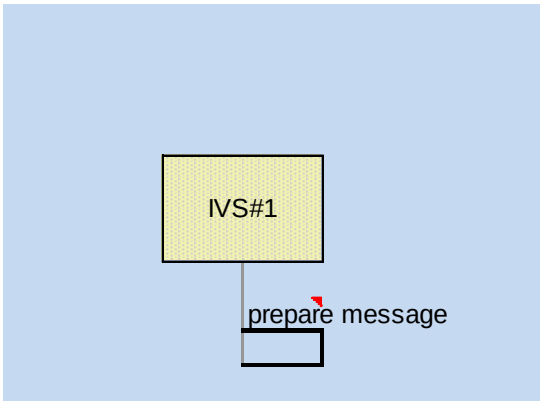
Sending message via direct communication to IVS

2.1.1 Assumptions

ID	Description
UC-IVS2IVS-01_A1	IVS#1 and IVS#2 are authorized and have valid certificates
UC-IVS2IVS-01_A2	message formats are defined and standardized

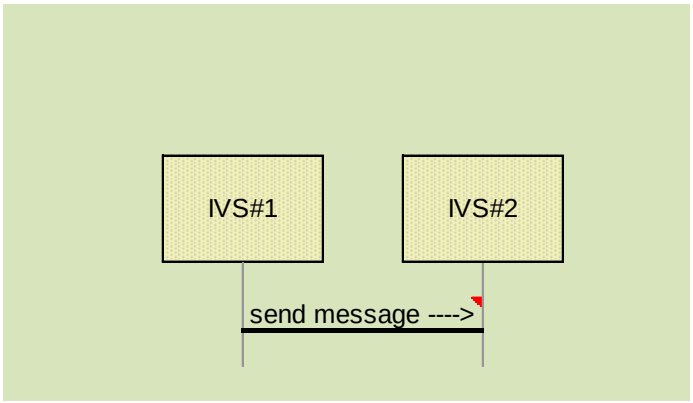
2.1.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	the message to be send is prepared and signed	



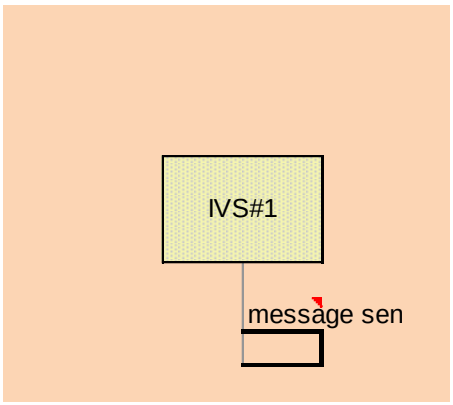
2.1.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#2	message is send directly to the receiver (f.ex. via ITS-G5)	



2.1.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	signed and validated message has been sent	



2.1.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x
IVS#2	The mobile "user" of a service, can be an vehicle or a mobile phone		x	

2.1.6 Decision Points Identified

ID	Component	Description

2.1.7 External Activities Identified

ID	Group	Description

2.2 UC-IVS2IVS-02

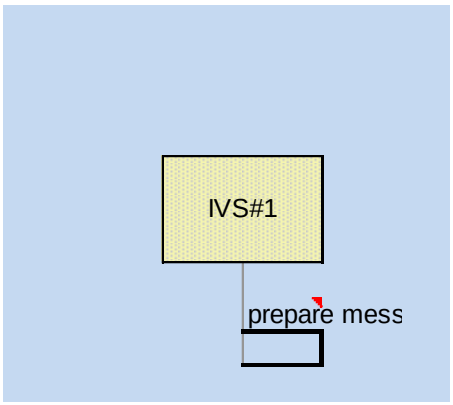
Receiving message via another IVS

2.2.1 Assumptions

ID	Description
UC-IVS2IVS-02_A1	IVS#1 and IVS#2 are authorized and have valid certificates
UC-IVS2IVS-02_A2	message formats are defined and standardized

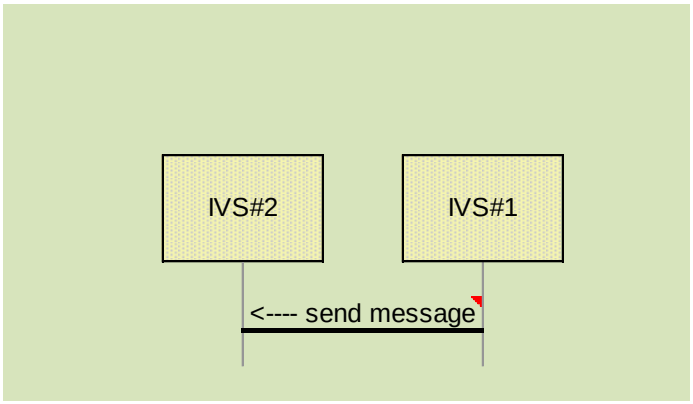
2.2.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	the message to be send is prepared and signed	



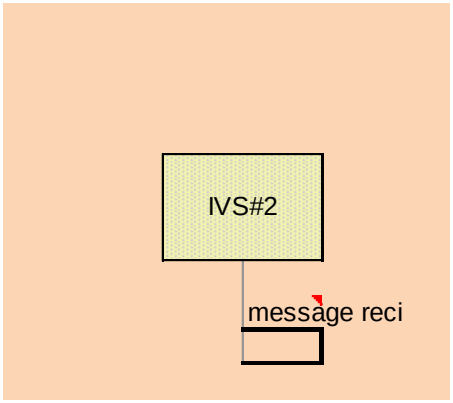
2.2.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#2	message is send directly to the receiver (f.ex. via ITS-G5)	



2.2.4 Actions Post-Operational

From	To	Description	Optional
IVS#2	IVS#2	signed and validated message has been recieved	



2.2.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	
IVS#2	The mobile "user" of a service, can be an vehicle or a mobile phone		x	x

2.2.6 Decision Points Identified

ID	Component	Description

2.2.7 External Activities Identified

ID	Group	Description

2.3 UC-IVS-01

Detection of local hazard (broken down vehicle, emergency brake). The IVS has access to needed data for the service (latitude, longitude, heading, speed, time, etc.). Sonsors information ist used to detect local hazards.

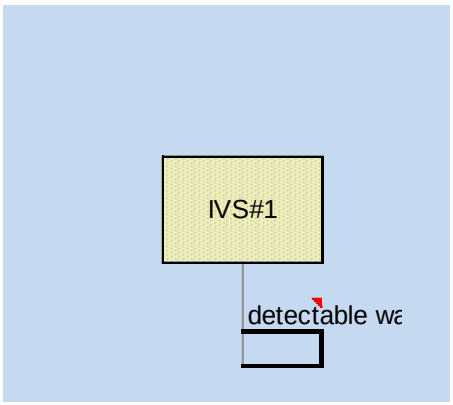
2.3.1 Assumptions

ID	Description
UC57_A1	Car is equipped with different sensors to recoqnize hazardous situations.
UC57_A2	Sensors are fully operational

2.3.2 Actions Pre-Operational

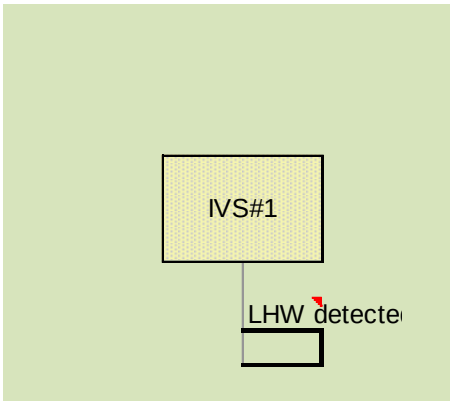
From	To	Description	Optional

IVS#1	IVS#1	occurence of detectable warning



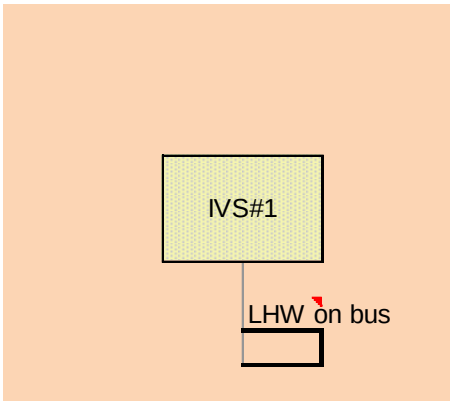
2.3.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#1	condition on vehicle bus changed	



2.3.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	LHW information can be retrieved from bus	



2.3.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x

2.3.6 Decision Points Identified

ID	Component	Description
DP-IVS-001	IVS#1	Find a way to detect hazards from sensor data

2.3.7 External Activities Identified

ID	Group	Description

2.4 UC-IVS-02

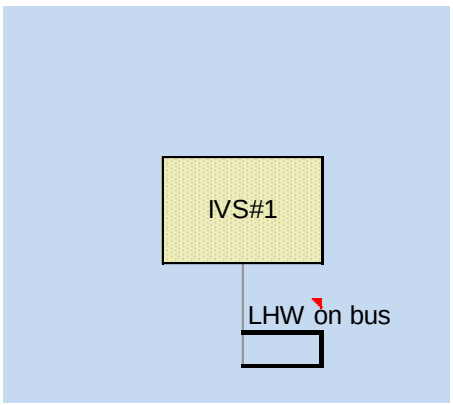
Generation of message (DENM). The IVS generates a warning message after recognizing a hazard due to sensor data.

2.4.1 Assumptions

ID	Description
UC58_A1	
UC58_A2	

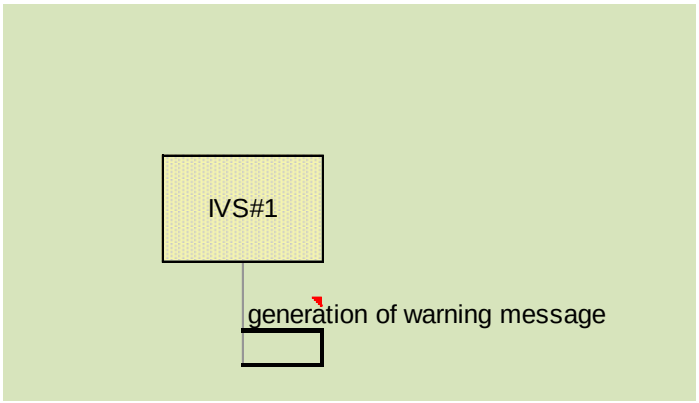
2.4.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	LHW is ready on vehicle bus	



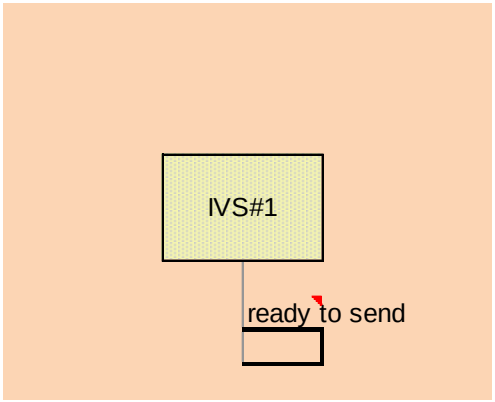
2.4.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#1	geoposition + valid certificate + message type	



2.4.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	signed & geo-referenced message is ready to be send	



2.4.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x

2.4.6 Decision Points Identified

ID	Component	Description
DP-IVS-001	IVS#1	

2.4.7 External Activities Identified

ID	Group	Description

2.5 UC-IVS-03

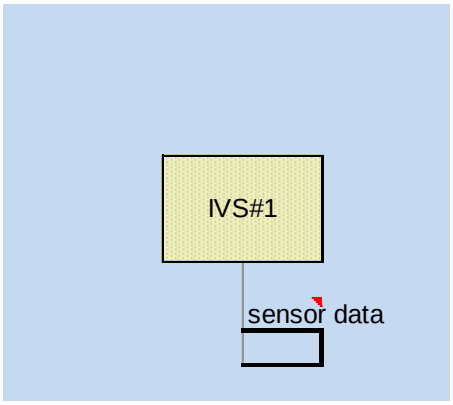
A vehicle collects sensor readings of the vehicle road environment via its integrated sensors. The data will be aggregated and anonymized.

2.5.1 Assumptions

ID	Description
UC-IVS-03_A1	The vehicle is equipped with the environment and localization sensors with data connection to IVS.
UC-IVS-03_A2	A set of sensor information to transmit is defined
UC-IVS-03_A3	A method for anonymization is defined
UC-IVS-03_A4	collected data can be realtime data or a over time collected and aggregated set

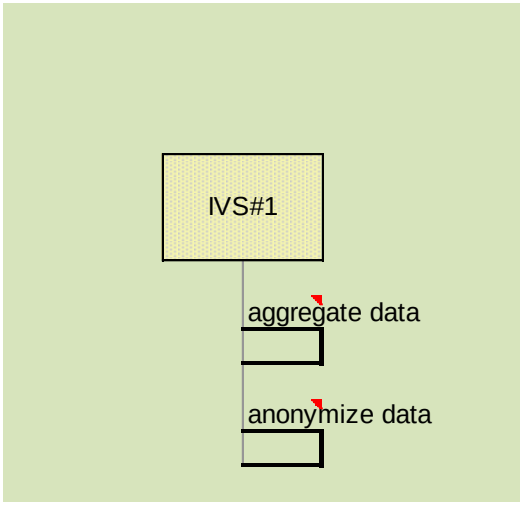
2.5.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	time- and geo-referenced data is available	



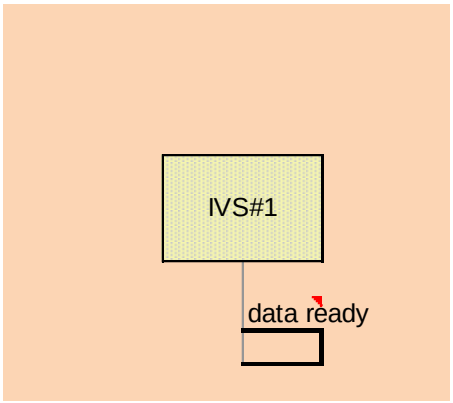
2.5.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#1	remove redundancy	
IVS#1	IVS#1	remove identifying information	



2.5.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	anonymized and aggregated data is ready to be send	



2.5.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x

2.5.6 Decision Points Identified

ID	Component	Description
DP-01	IVS	Question where the anonymisation should take place (at IVS or at backend)

2.5.7 External Activities Identified

ID	Group	Description

2.6 UC-IVS-05_01

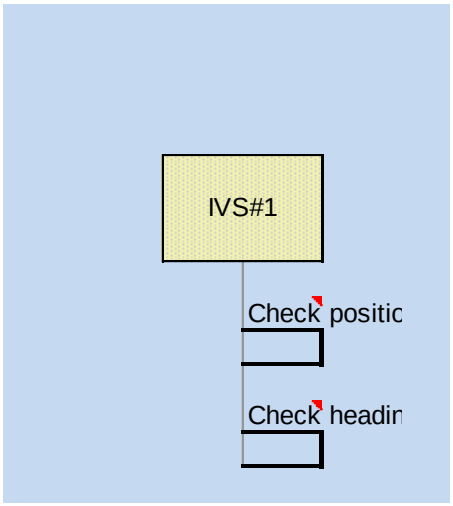
IVS checks the relevance of the incoming message with respect to its motion state IVS (message is valid for "me") consideringvehicle course (message is currently valid for IVS due to course)distance from vehicle to event location (urgency of the message)

2.6.1 Assumptions

ID	Description
UC-IVS-05_01_A1	Position and motion state of the IVS can be determined
UC-IVS-05_01_A2	Event location is known

2.6.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	Position data of the IVS is determined	
IVS#1	IVS#1	Heading information of the IVS is determined	

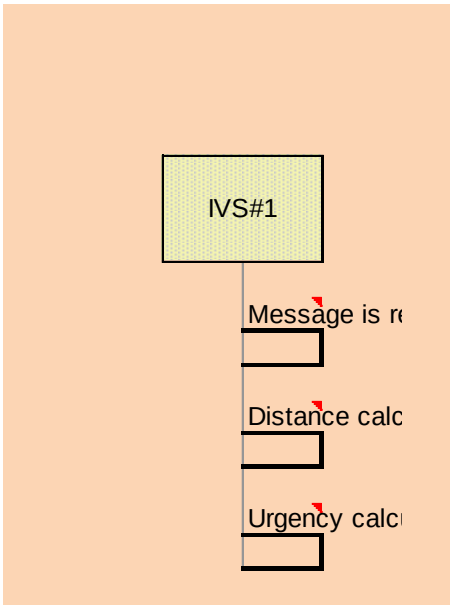


2.6.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#1	Relevance of the event information is checked depending on geographical and kinematical information of the IVS	

2.6.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	Information is relevant for the IVS	
IVS#1	IVS#1	Distrance between IVS location and event location is being computed	
IVS#1	IVS#1	Urgency of event information is computed based on IVS information and event information	



2.6.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x
IVS#2	The mobile "user" of a service, can be an vehicle or a mobile phone		x	

2.6.6 Decision Points Identified

ID	Component	Description

2.6.7 External Activities Identified

ID	Group	Description

2.7 UC-IVS-05_02

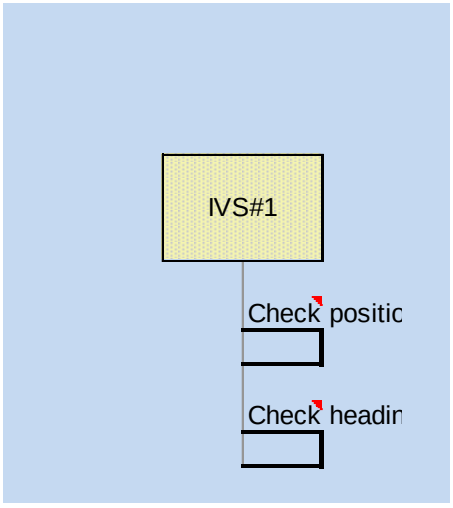
IVS checks the relevance of the incoming message with respect to vehicle course (message is currently valid for IVS due to course)

2.7.1 Assumptions

ID	Description
UC-IVS-05_02_A1	Position and motion state of the IVS can be determined
UC-IVS-05_02_A2	Event location is known

2.7.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	Position data of the IVS is determined	
IVS#1	IVS#1	Heading information of the IVS is determined	

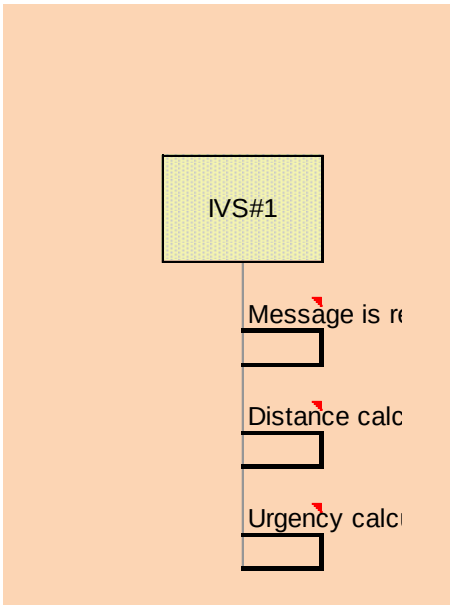


2.7.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#1	Relevance of the event information is checked depending on geographical and kinematical information of the IVS; Information is relevant if vehicle course and event location fit together	

2.7.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	Information is relevant for the IVS	
IVS#1	IVS#1	Distrance between IVS location and event location is being computed	
IVS#1	IVS#1	Urgency of event information is computed based on IVS information and event information	



2.7.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x
IVS#2	The mobile "user" of a service, can be an vehicle or a mobile phone		x	

2.7.6 Decision Points Identified

ID	Component	Description

DP-01		Message severity categorization mechanism has to be worked out

2.7.7 External Activities Identified

ID	Group	Description

2.8 UC-IVS-05_03

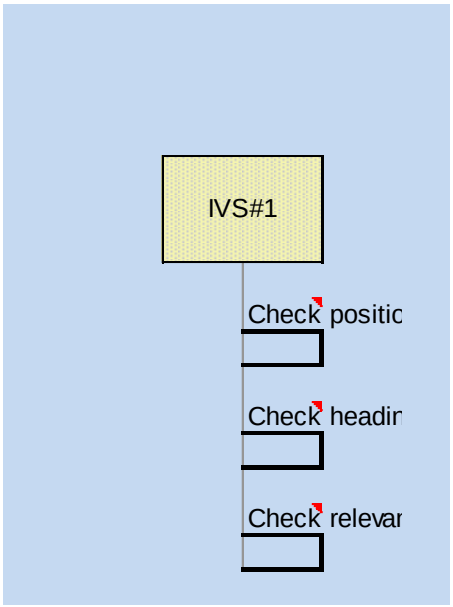
IVS checks the urgency of the incoming message with respect to distance from vehicle to event location

2.8.1 Assumptions

ID	Description
UC-IVS-05_03_A1	Position and motion state of the IVS can be determined
UC-IVS-05_02_A2	Event location is known
UC-IVS-05_02_A3	Urgency classification has been defined and is known

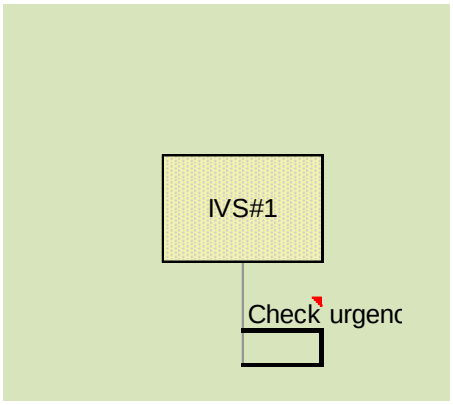
2.8.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	Position data of the IVS is determined	
IVS#1	IVS#1	Heading information of the IVS is determined	
IVS#1	IVS#1	Relevance information of the IVS is determined	



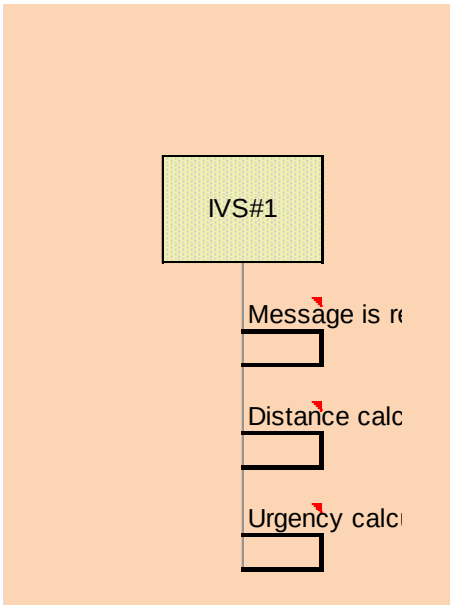
2.8.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#1	Urgency of the event information is checked depending on geographical and kinematical information of the IVS	



2.8.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	Information is relevant for the IVS	
IVS#1	IVS#1	Distrance between IVS location and event location is being computed	
IVS#1	IVS#1	Urgency of event information is computed based on IVS information and event information	



2.8.5 Components Identified

Name	Description	Involvement

		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x

2.8.6 Decision Points Identified

ID	Component	Description

2.8.7 External Activities Identified

ID	Group	Description

2.9 UC-IVS-05_0f

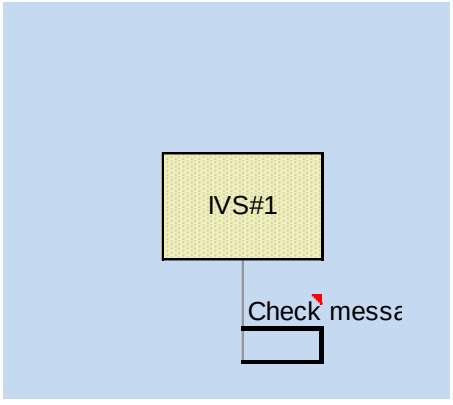
Further processing of the incoming message according to the type of the hazard

2.9.1 Assumptions

ID	Description
UC-IVS-05_0f_A1	Each interpreted message is linked to a specific application in the vehicle
UC-IVS-05_0f_A2	Applications have been defined

2.9.2 Actions Pre-Operational

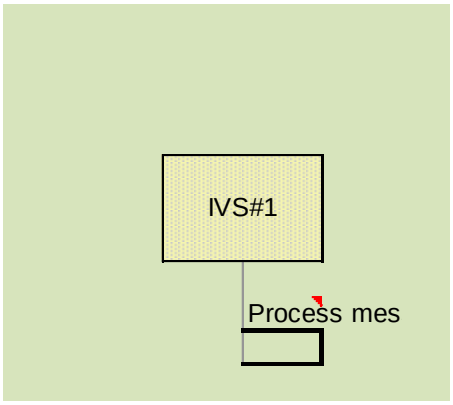
From	To	Description	Optional
IVS#1	IVS#1	Message type is determined	



2.9.3 Actions Operational

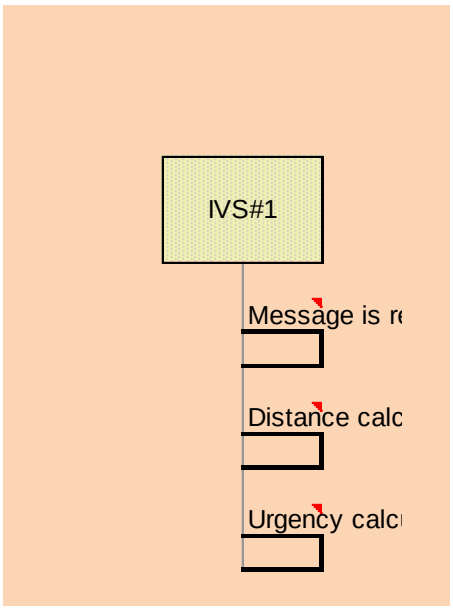
From	To	Description	Optional

IVS#1	IVS#1	Message is being processed at IVS level: e. g. applications are started or intermediate processing results are determined



2.9.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	Specialized information was determined; defined applications are started	



2.9.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x

2.9.6 Decision Points Identified

ID	Component	Description

2.9.7 External Activities Identified

ID	Group	Description

2.10 UC-IVS-06

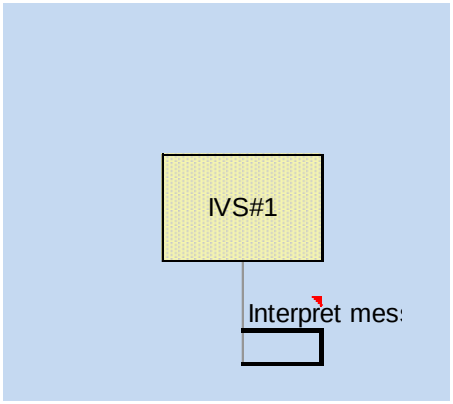
Display the warning in the HMI according to the urgency (info, warning)

2.10.1 Assumptions

ID	Description
UC-IVS-06_A1	HMI concept is defined
UC-IVS_06_A2	Urgency classification is known

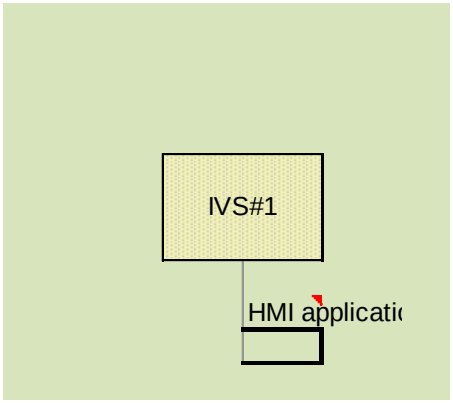
2.10.2 Actions Pre-Operational

From	To	Description	Optional
IVS#1	IVS#1	Message information (relevance, urgency) is retrieved	



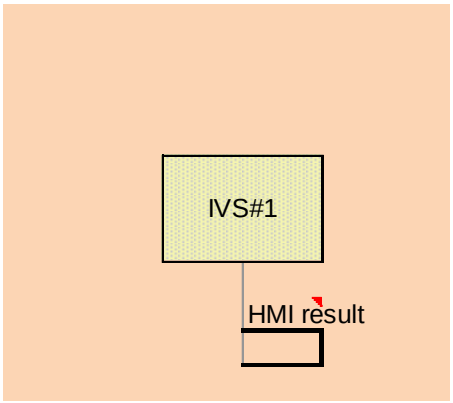
2.10.3 Actions Operational

From	To	Description	Optional
IVS#1	IVS#1	HMI application is started depending on the urgency of the message	



2.10.4 Actions Post-Operational

From	To	Description	Optional
IVS#1	IVS#1	Message information is being provided to the user of the IVS	



2.10.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS#1	The mobile "user" of a service, can be an vehicle or a mobile phone	x	x	x

2.10.6 Decision Points Identified

ID	Component	Description

2.10.7 External Activities Identified

ID	Group	Description

2.11 UC-Noname#01

Local-Hazard-Warning (LHW) data constitutes a certain dangerous event situation which has been captured by the sensor systems of one vehicle (IVS, brand #1) and is to be communicated to the OEM #1 Backend. At the #1 Backend it is decided to share this information with vehicles of other brands. Hence the LHW event notification, once being recognized at the OEM #1 Backend, enters an event-driven procedure for sharing it with the OEM Backends of OEM #2 and OEM #3

2.11.1 Assumptions

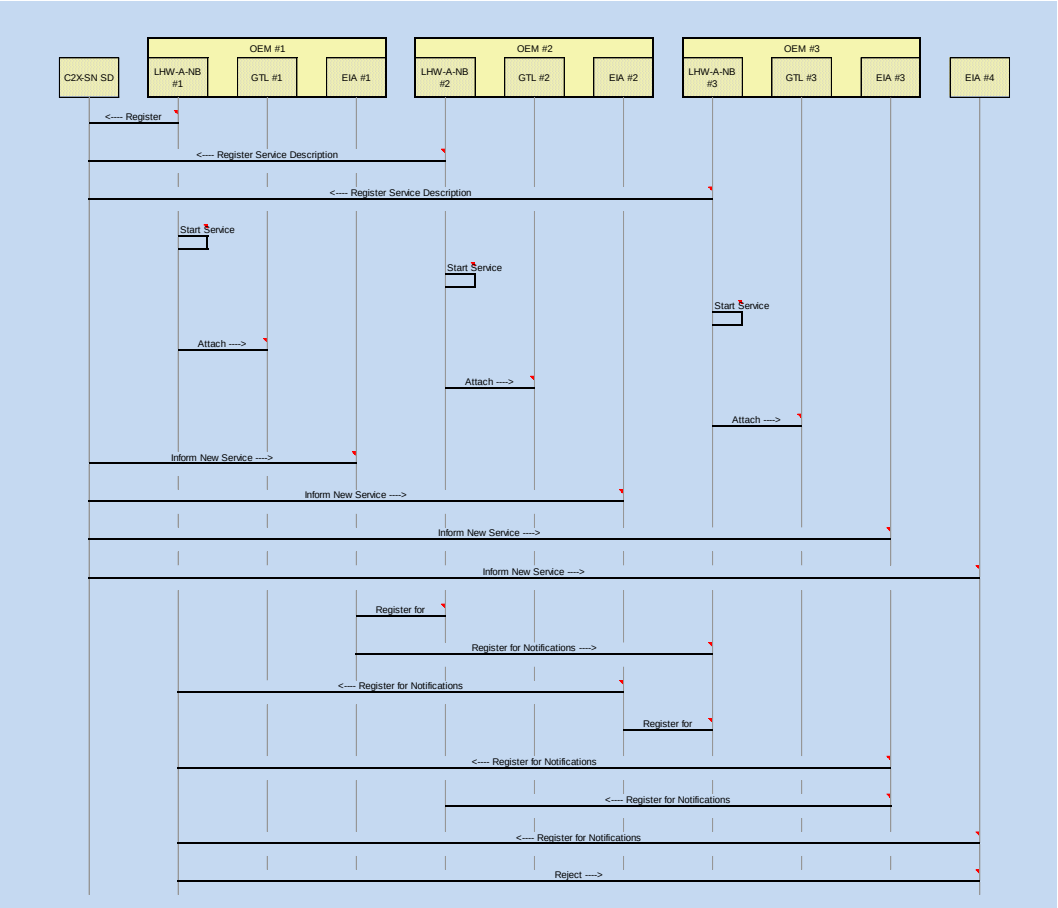
ID	Description
UC1_A1	The communication channel between IVSs and the OEMs Backends have been registered and established (è separate user-story!) and "behaves transparent" within "User-Story-1
UC1_A2	The specific LHW message has been categorized as LHW type-A at the IVSs, indicating that this is a message to be send to the OEMs Backends
UC1_A3	The OEMs #1, #2, #3 have agreed and signed a contract to share LHW Messages of Type A
UC1_A4	OEMs #1, #2 and #3 have been registered with the C2X-SN as "Service Providers, Type X" and hence have received C2X-SN access premising certificate (APC_sn) (è separate user-story!)
UC1_A5	The LHW Type A message sharing service has been agreed to be called "LHW-A-Notification-Board" (LHW-A-NB)

2.11.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite#1		A human readable document (e.g. HTML-text document), describing the characteristics of LHW Type A messages, their information quality and uncertainties, is available for human inspection	
Prerequisite#2		An Software readable interface description (e.g. XMP, WSDL Web Service description file) of the LHW-A-NB service is available	
Prerequisite#3		A C2X-SN internal Service Directory service (e.g. UDDI) including a C2X-SN internal Service-Provider notification mechanism (-> other user story!) is available and the way to contact this Service Directory service is known to all C2X-SN participants (-> other user story!)	
Prerequisite#4		Each OEM Backend 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 (-> other user story)	

Prerequisite#5		Each OEM Backend has a generic, Event Incoming Alert service (e.g. EIA_#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		An LHW-A-NB specific service access certificate, called APC_sn_LHW-A-NB, has been issued to OEMs #1, #2, #3
LHW-A-NB #1	C2X-SN SD	OEM #1 registers its WSDL description for service LHW-A-NB #1 at C2X-SN Service Directory Server, together with APC_sn_LHW-A-NB certificate
LHW-A-NB #2	C2X-SN SD	OEM #2 registers its WSDL description for service LHW-A-NB #2 at C2X-SN Service Directory Server, together with APC_sn_LHW-A-NB certificate
LHW-A-NB #3	C2X-SN SD	OEM #3 registers its WSDL description for service LHW-A-NB #3 at C2X-SN Service Directory Server, together with APC_sn_LHW-A-NB certificate
LHW-A-NB #1	LHW-A-NB #1	OEM #1 starts its Web Service LHW-A-NB #1 at its OEM Backend server farm
LHW-A-NB #2	LHW-A-NB #2	OEM #2 starts its Web Service LHW-A-NB #2 at its OEM Backend server farm
LHW-A-NB #3	LHW-A-NB #3	OEM #3 starts its Web Service LHW-A-NB #3 at its OEM Backend server farm
LHW-A-NB #1	GTL #1	OEM #1 attaches its Generic Transaction Logging (GTL_#1) service with its LHW-A-NB service and re-configure s their firewalls to permit access for requests, authorized via certificate APC_sn_LHW-A-NB
LHW-A-NB #2	GTL #2	OEM #2 attaches its Generic Transaction Logging (GTL_#2) service with its LHW-A-NB service and re-configure s their firewalls to permit access for requests, authorized via certificate APC_sn_LHW-A-NB
LHW-A-NB #3	GTL #3	OEM #3 attaches its Generic Transaction Logging (GTL_#3) service with its LHW-A-NB service and re-configure s their firewalls to permit access for requests, authorized via certificate APC_sn_LHW-A-NB
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs OEM #1 that a new service has registered itself, by posting OEM #1 EIA event reception point, providing its WSDL and its textual descriptions

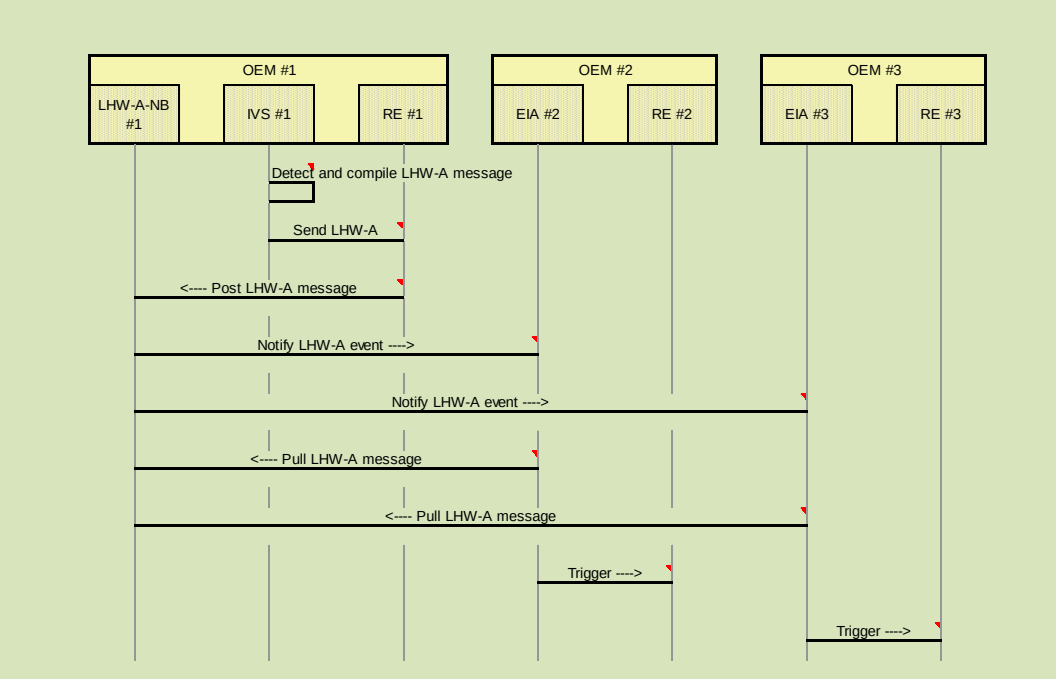
C2X-SN SD	EIA #2	The Notification Service attached to the Service Directory server informs OEM #2 that a new service has registered itself, by posting OEM #2 EIA event reception point, providing its WSDL and its textual descriptions
C2X-SN SD	EIA #3	The Notification Service attached to the Service Directory server informs OEM #3 that a new service has registered itself, by posting OEM #3 EIA event reception point, providing its WSDL and its textual descriptions
C2X-SN SD	EIA #4	The Notification Service attached to the Service Directory server informs OEM #4 that a new service has registered itself, by posting OEM #4 EIA event reception point, providing its WSDL and its textual descriptions
EIA #1	LHW-A-NB #2	OEM #1 EIA_#1 contacts LHW-A-NB_#2, presenting its certificate APC_sn_LHW-A-NB, to register itself as receiver of LHW Type A message notifications.
EIA #1	LHW-A-NB #3	OEM #1 EIA_#1 contacts LHW-A-NB_#3, presenting its certificate APC_sn_LHW-A-NB, to register itself as receiver of LHW Type A message notifications.
EIA #2	LHW-A-NB #1	OEM #2 EIA_#2 contacts LHW-A-NB_#1, presenting its certificate APC_sn_LHW-A-NB, to register itself as receiver of LHW Type A message notifications.
EIA #2	LHW-A-NB #3	OEM #2 EIA_#2 contacts LHW-A-NB_#3, presenting its certificate APC_sn_LHW-A-NB, to register itself as receiver of LHW Type A message notifications.
EIA #3	LHW-A-NB #1	OEM #3 EIA_#3 contacts LHW-A-NB_#1, presenting its certificate APC_sn_LHW-A-NB, to register itself as receiver of LHW Type A message notifications.
EIA #3	LHW-A-NB #2	OEM #3 EIA_#3 contacts LHW-A-NB_#2, presenting its certificate APC_sn_LHW-A-NB, to register itself as receiver of LHW Type A message notifications.
EIA #4	LHW-A-NB #1	OEM #4 EIA_#4 contacts LHW-A-NB_#1, presenting its certificate APC_sn_LHW-A-NB, to register itself as receiver of LHW Type A message notifications.
LHW-A-NB #1	EIA #4	OEM #1 LHW-A-NB #1 detects the invalidity of the certificate of OEM #4 and rejects the registration



2.11.3 Actions Operational

From	To	Description	Optional
Prerequisite#7		All OEMs that have agreed to exchange LHW Type A messages have registered their LHW-A-NB “brand xyz” service, attached their transaction logging service with their LHW-A-NB, have registered their EIA services with their contract partner’s Backend LHW-A-NB Services and are ready for operation	
IVS #1	IVS #1	A vehicle of brand #1 (IVS_#1) has recognized the situation of being faced with a LHW Type A sensor-data-consolidation situation. A dedicated message of Type A, i.e. LHW-A_#1_message-content, has ben compiled	
IVS #1	RE #1	The IVS platform sends the message LHW-A_#1_message-content to the OEM #1 Backend. The communication path between the #1 IVS and the #1 Backend is fully transparent, as seen from a IVS sensor data processing platform perspective	

RE #1	LHW-A-NB #1	The OEM #1 internal message processing rule engine RE (è separate user story!) detects that LHW-A_#1_message-content is to be shared via the LHW-A-NB_#1 service. Hence LHW-A_#1_message-content gets posted to the LHW-A-NB_#1 service
LHW-A-NB #1	EIA #2	The server LHW-A-NB_#1 issues an LHW-A_Event_Notification(ID) message with all event receivers which had been registered with LHW-A-NB_#1 beforehand as receivers of LHW Type A events. Hence LHW-A-NB_#1 sends the message LHW-A_Event_Notification(ID) to EIA_#2
LHW-A-NB #1	EIA #3	The server LHW-A-NB_#1 issues an LHW-A_Event_Notification(ID) message with all event receivers which had been registered with LHW-A-NB_#1 beforehand as receivers of LHW Type A events. Hence LHW-A-NB_#1 sends the message LHW-A_Event_Notification(ID) to EIA_#3
EIA #2	LHW-A-NB #1	Alerted via the incoming heads-up notification, the EIA_#2 pulls for the message(ID) from to LHW-A-NB_#1
EIA #3	LHW-A-NB #1	Alerted via the incoming heads-up notification, the EIA_#3 pulls for the message(ID) from to LHW-A-NB_#1
EIA #2	RE #2	OEM #2 triggers its local Backend rule engine with the newly available LHW Type A message LHW-A_#1_message-content which was originating from IVS_#1. Further processing and actions are with #2
EIA #3	RE #3	OEM #3 triggers its local Backend rule engine with the newly available LHW Type A message LHW-A_#1_message-content which was originating from IVS_#1. Further processing and actions are with #3

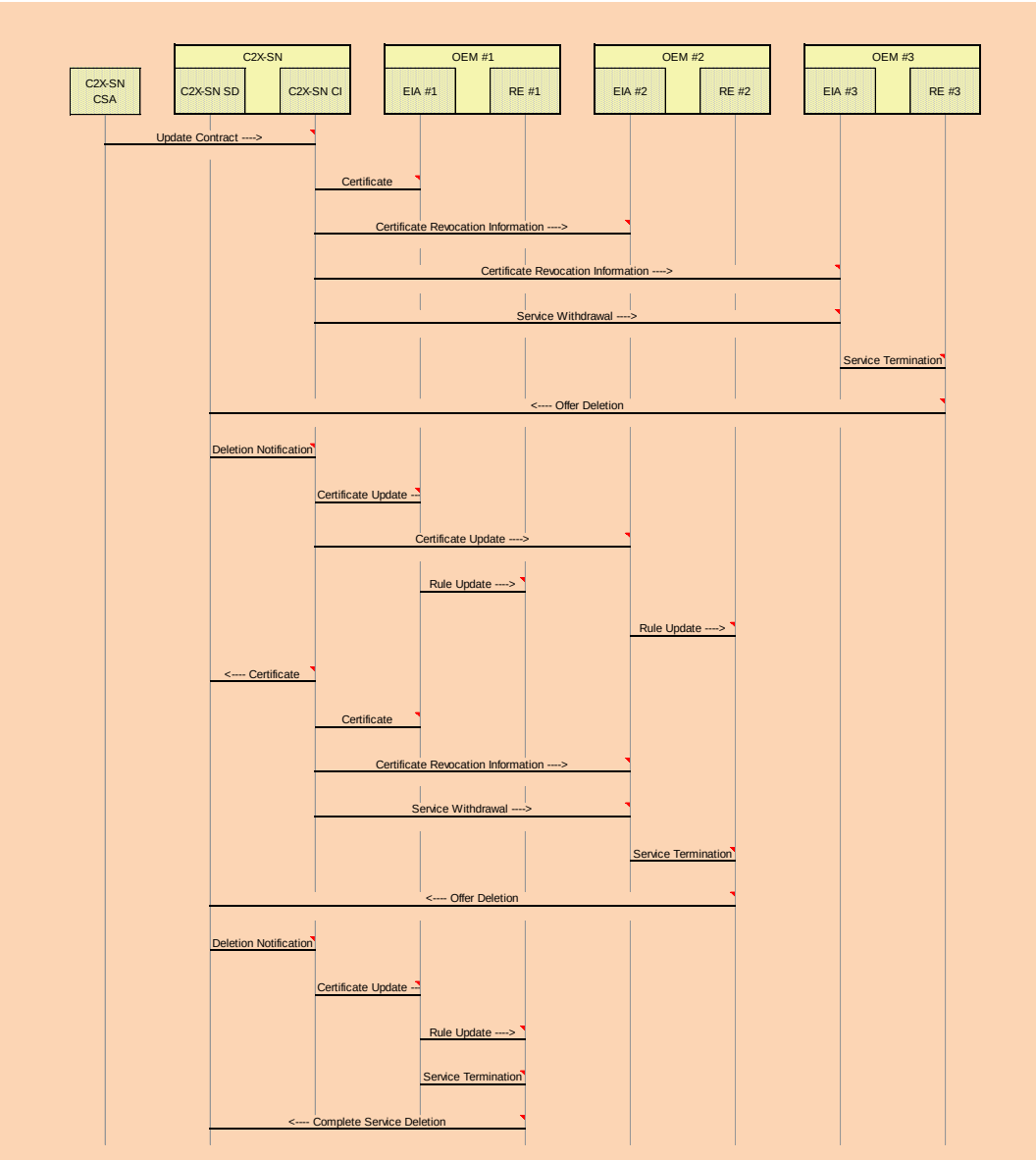


2.11.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#8		All LHW-A_NB and EIA services at #1, #2, #3 are ready to serve the next event	
Prerequisite#9		OEM #3 has terminated the LHW-A_NB contract and notified the C2X-SN Contract Supervision Authority	
Prerequisite#10		OEM #2 has terminated the LHW-A_NB contract and notified the C2X-SN Contract Supervision Authority. The Post-Operation (a) "#2 withdraws" has taken place	
Prerequisite#11		OEM #1 has terminated the LHW-A_NB contract and notified the C2X-SN Contract Supervision Authority. #1 had been the only LHW-A-NB service provider left at the C2X-SN and decided to revoke that offer. Hence the LHW-A-NB service shall disappear as if it had never been launched	
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of #1 to inform that the Certificate APC_sn_LHW-A-NB has been revoked. #1 updates its local certification management	

C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of #2 to inform that the Certificate APC_sn_LHW-A-NB has been revoked. #2 updates its local certification management
C2X-SN CI	EIA #3	The C2X-SN Certification-Issuer contacts the EIA receptor of #3 to inform that the Certificate APC_sn_LHW-A-NB has been revoked. #3 updates its local certification management
C2X-SN CI	EIA #3	The C2X-SN Certification-Issuer contacts the EIA receptors of #3 to inform that #3 has withdrawn from service LHW-A-NB
EIA #3	RE #3	EIA_#3 trigges its local RE with the update request. #3 purges it entire LHW-A-NB service configuration and terminates LHW-A-NB_#3
RE #3	C2X-SN SD	RE #3 contacts the C2X-SN Service Directory server and requests the deletion of the LHW-A-NB #3 service offer
C2X-SN SD	C2X-SN CI	C2X-SN Service Directory informs C2X-SN Certification Issuer that the LHW-A-NB #3 Service is deleted
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer generates a new certificate APC_sn_LHW-A-NB -2 and contacts the EIA receptor of #1 inform that the new certificate APC_sn_LHW-A-NB-2, associated with service LHW-A-NB has been activated and that #3 has withdrawn from service LHW-A-NB
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer generates a new certificate APC_sn_LHW-A-NB -2 and contacts the EIA receptor of #2 inform that the new certificate APC_sn_LHW-A-NB-2, associated with service LHW-A-NB has been activated and that #3 has withdrawn from service LHW-A-NB
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of #1 updates its event notification rules (i.e. #1 deletes #3 from its notification list.)
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of #2 updates its event notification rules (i.e. #2 deletes #3 from its notification list.)

C2X-SN CI	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_LHW-A-NB-3, associated with service LHW-A-NB, has been activated, replacing certificate APC_sn_LHW-A-NB-2
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of #1 to inform that the Certificate APC_sn_LHW-A-NB has been revoked. #1 updates its local certification management
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of #2 to inform that the Certificate APC_sn_LHW-A-NB has been revoked. #2 updates its local certification management
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptors of #2 to inform that #2 has withdrawn from service LHW-A-NB
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. #2 purges it entire LHW-A-NB service configuration and terminates LHW-A-NB_#2
RE #2	C2X-SN SD	RE #2 contacts the C2X-SN Service Directory server and requests the deletion of the LHW-A-NB #2 service offer
C2X-SN SD	C2X-SN CI	C2X-SN Service Directory informs C2X-SN Certification Issuer that the LHW-A-NB #2 Service is deleted
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer generates a new certificate APC_sn_LHW-A-NB -4 and contacts the EIA receptor of #1 inform that the new certificate APC_sn_LHW-A-NB-4, associated with service LHW-A-NB has been activated and that #2 has withdrawn from service LHW-A-NB
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of #1 updates its event notification rules (i.e. #1 deletes #2 from its notification list.)
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. #1 purges it entire LHW-A-NB service configuration and terminates LHW-A-NB_#1
RE #1	C2X-SN SD	#1's RE contacts the C2X-SN Service Directory server and requests the deletion of the LHW-A-NB_#1 service offer



2.11.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x

C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		x
GTL #1	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x		
IVS #1			x	
LHW-A-NB #1	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 services/information. This can be inside the C2X-SN itself and/or 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	
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x

GTL #2	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x		
LHW-A-NB #2	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 services/information. This can be inside the C2X-SN itself and/or 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		
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
GTL #3	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x		
LHW-A-NB #3	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 services/information. This can be inside the C2X-SN itself and/or 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		
RE #3	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #4	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.11.6 Decision Points Identified

ID	Component	Description

DP-SD	C2X-SN SD	Find a way to realize the C2X-SN Service Directory
DP-TL	GTL #1	Find a way to realize transaction logging to support charging, KPI supervision, security inspection

2.11.7 External Activities Identified

ID	Group	Description
UST-ComCh	OEMs	Registration and establishment of the communication channel between IVS and the OEM Backend
UST-SPReg	OEMs	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)
UST-SPNM	C2X-SN	Notification Mechanism for notifying service participants about changes in a service they have been registered to
UST-SPCM	C2X-SN	Contact mechanism to reach the C2X-SN Service Description ("yellow pages") Service
UST-KPISV	C2X-SN	Interface service to support charging, KPI supervision or security inspection functions
UST-RE	IS-Backend	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

2.12 US-RWW1

Set up of the blocking trailer; Configuration update of blocking trailer; Information distribution to other vehicles and traffic center/service provider; Information update during operation (Wanderbaustelle); Clearing up of road works

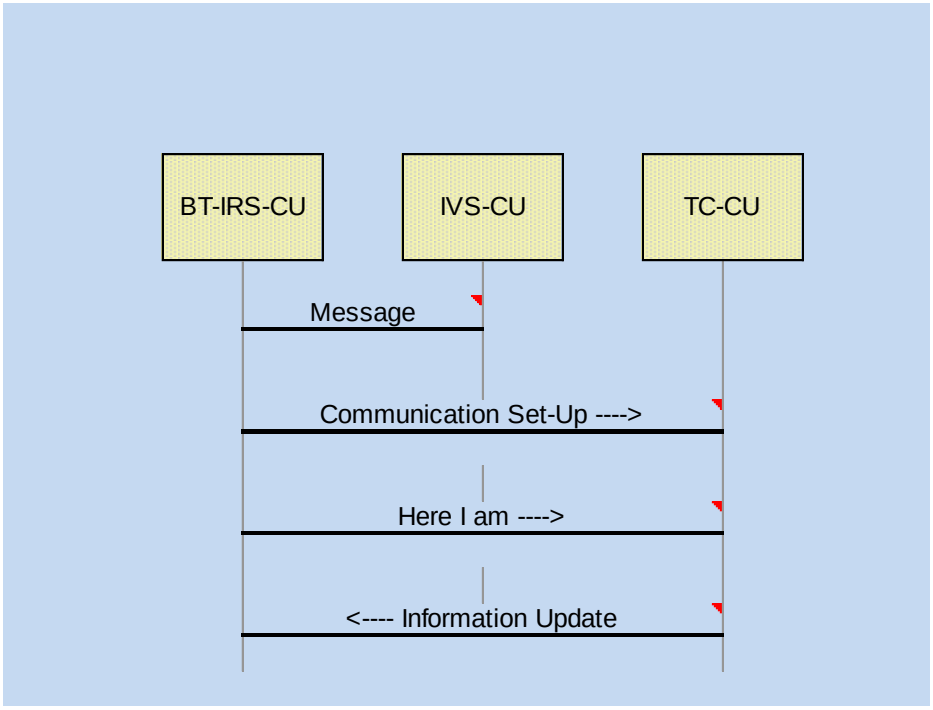
2.12.1 Assumptions

ID	Description
US-RWW-A1	Information about the communication end point (traffic center) ist known to the blockin trailer
US-RWW-A2	The initial information (message content) that the blocking trailer has to distribute has been defined and is availlable at the blocking trailer communication device (IRS)
US-RWW-A3	The blocking trailer IRS has information available about the accurate position and time
US-RWW-A4	The blocking trailer hast means to communicate with the infrastructure (traffic center) and vehicles. This includes cellular radio and ETSI ITS G5

US-RWW-A5The blocking trailer IRS has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
US-RWW-A6A road works warning database hast been started and initialized at the traffice center

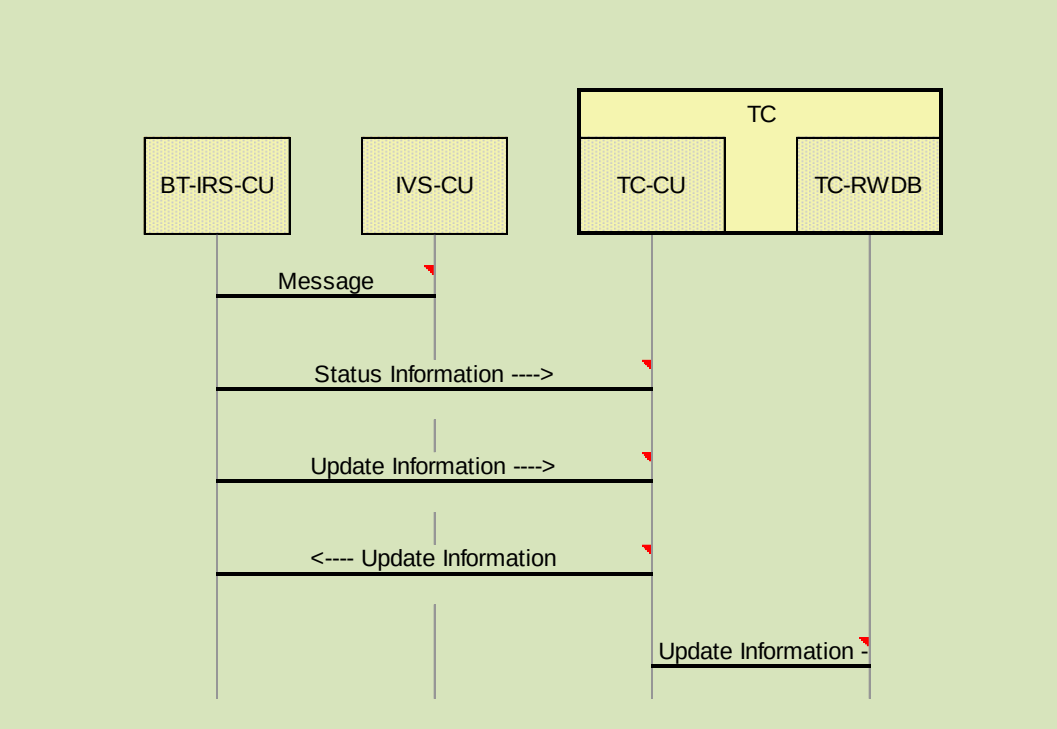
2.12.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1			
Prerequisite-2		Bob is pushing a button or flips up the traffic sign (manual activation)	
BT-IRS-CU	IVS-CU	The blocking trailer takes the initial information available, generates a broadcast message (ETSI ITS G5) and periodically sends it out	
BT-IRS-CU	TC-CU	The blocking trailer sets up the communication to its traffice center communication end point	
BT-IRS-CU	TC-CU	The blocking trailer registers at its traffic center and sends its initial information (single message, reliable, authentic, integer, confidential, not time critical)	
TC-CU	BT-IRS-CU	The traffic center sends (optional) updated information about the details of the road works to the blocking trailer (single message, reliable, authentic, integer, confidential, not time critical)	



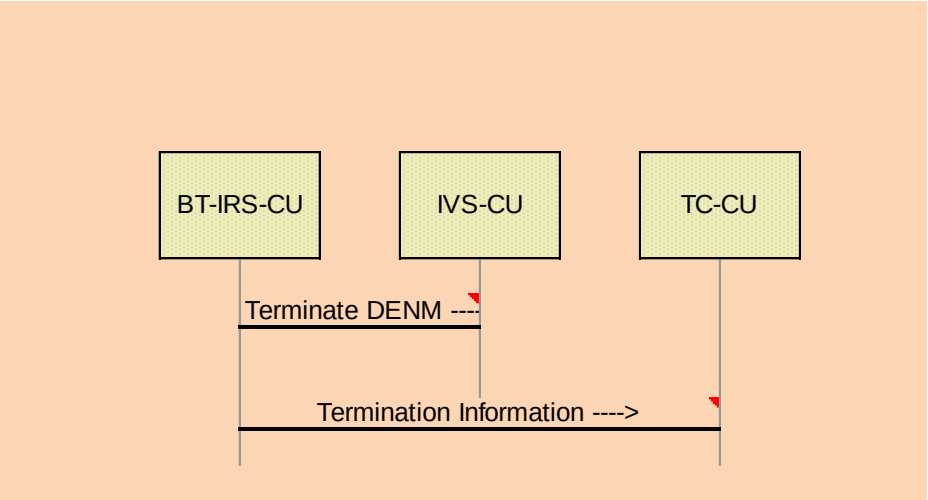
2.12.3 Actions Operational

From	To	Description	Optional
Description-1		There are 4 general action lines: - periodic distribution of actual configuration information via ETSI ITS G5 - no change in configuration, traffic center needs to get information about the status of the blocking trailer on regular basis or event driven - blocking trailer has detected a change in its configuration (e.g. position change) - traffic center updates information to the blocking trailer	
BT-IRS-CU	IVS-CU	The blocking trailer takes the actual information available, generates a broadcast message (ETSI ITS G5) and periodically sends it out	
BT-IRS-CU	TC-CU	the blocking trailer sends regular or event driven the actual trailer information	
BT-IRS-CU	TC-CU	The blocking trailer has detected a change in its configuration (e.g. position change) and sends an update message to its traffic center and updates its configuration information record	
TC-CU	BT-IRS-CU	The traffic center sends updated information about the details of the road works to the blocking trailer (single message, reliable, authentic, integer, confidential, not time critical)	
TC-CU	TC-RWDB	The traffic center updates its current database of road works events	



2.12.4 Actions Post-Operational

From	To	Description	Optional
Description-1		Construction site is terminated, Blocking trailer gets shut down, traffic center is informed about construction termination, G5 broadcast is terminated by termination DENM	
Prerequisite-1		Bob has finalized construction works and deactivates the blocking trailer.	
BT-IRS-CU	IVS-CU	a special message is sent via ETSI ITS G5 that informs the vehicles about the premature expiration of the previous DENM	
BT-IRS-CU	TC-CU	the blocking trailer sends a messge with information about the road works end to the traffic center	



2.12.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
BT-IRS-CU	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.	x	x	x
IVS-CU	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.	x	x	x
TC-CU	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.	x	x	x
TC-RWDB	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.		x	

2.12.6 Decision Points Identified

ID	Component	Description

DP-RWW-1	TC-CU	Find best way to communicate the "here I am" message from the blocking trailer to its communication end point. Possible decission to be taken: - acknowledged - repeating on transport level or aplicaton level - mechanism for confidentiality (tunnel, "cable", message based)
DP-RWW-2	BT-IRS-CU	Determine exact mechanism to exchange the operational status of the blocking trailer to its traffic center - Push or Pull

2.12.7 External Activities Identified

ID	Group	Description
US-RWW-E1		A way to inform the blocking trailer about its infrastructure communication end point has to be specified in detail
US-RWW-E2		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 (Button that Bob is pushing) or from an external entity
US-RWW-E3		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
US-RWW-E4	IRS	The IRS hast 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 have changed
US-RWW-E5	TC	The mechanism to start up all components at the TC backend has to be described

2.13 US-RWW2

OEM Backend sends RWW message to all its related vehicles in a certain defined area;
the area is defined in the message content

2.13.1 Assumptions

ID	Description
US-RWW2-A1	OEM Backend is registered as recipient for road works warning messages issued by a certain service provider
US-RWW2-A3	At the OEM Backend there is an incoming event alert service (IEA) available
US-RWW2-A4	OEM Backend has available a contract relationship with a certain mobile

network operator (MNO)
US-RWW2-A5The MNO offers the possibility to dissemminate message to communication end points based on geocast
US-RWW2-A6The OEM Backend has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
US-RWW2-A7Each IVS has a geomessaging client installed and active
US-RWW2-A8The IVS has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)

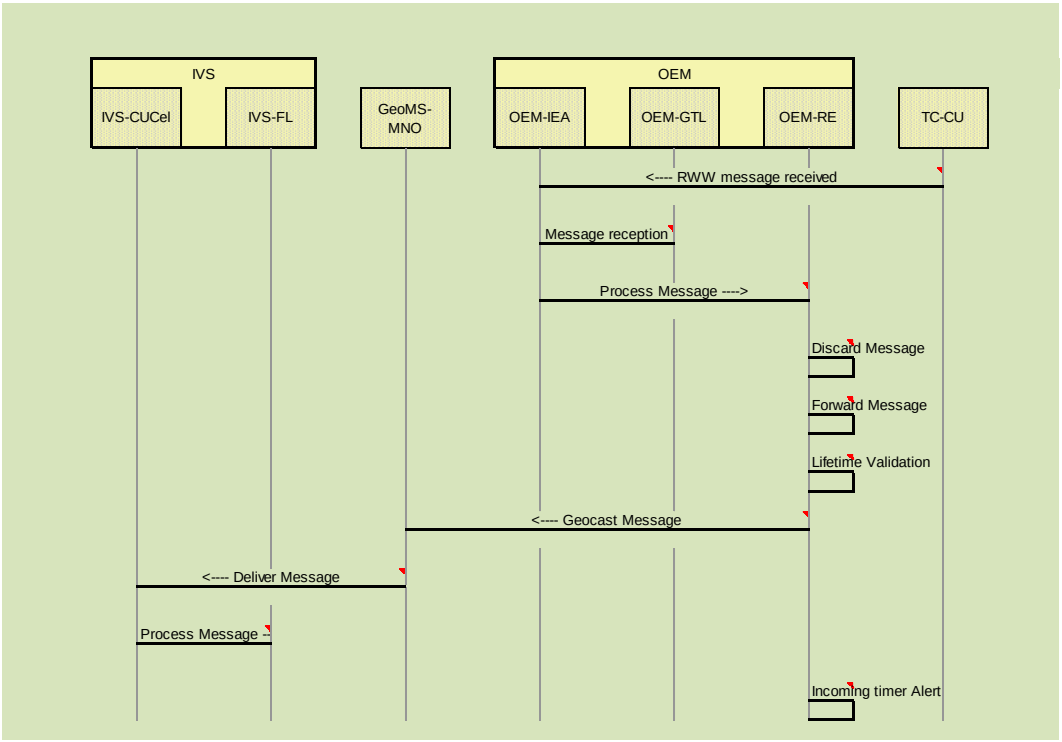
2.13.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		The OEM hast registered itself for reception of RWW messages from TCs	
Prerequisite-2		There is at least on service provider (TC) that offers a RWW message service and has announced it	
Prerequisite-3		Each OEM Backend 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 (-> other user story)	
Prerequisite-4		Each OEM Backend 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-5		Each OEM Backend has a generic rule engine (RE) service running at its backend. The RE processes icoming events according to local policies.	
Prerequisite-6		A message about a RWW event has been received from the TC and been posted to the IEA	

2.13.3 Actions Operational

From	To	Description	Optional
TC-CU	OEM-IEA	A message about a RWW has been received from the TC and been posted to the IEA	
OEM-IEA	OEM-GTL	The availability of the RWW message is logged at the OEM backend	

OEM-IEA	OEM-RE	The IEA informs the RE about the reception of a RWW message and triggers the further processing at the RE
OEM-RE	OEM-RE	The RE decides that the received message should not be distributed
OEM-RE	OEM-RE	The RE decides that the received message has to be distributed
OEM-RE	OEM-RE	Optional: In case the lifetime of the incoming message is beyond the local maximum "lifetime without validation" a "rule engine reminder" timer is set and the message is kept in an internal storage and if the time is expired, the OEM-RE Geocast Message is resent.
OEM-RE	GeoMS-MNO	The RE forwards the RWW message to the Geo messaging server (GeoMS) of its associated MNO(s).
GeoMS-MNO	IVS-CUCel	The Geo-MS-MNO sends the RWW to all receivers of the OEM in the given target region.
IVS-CUCel	IVS-FL	The cellular communication unit in the IVS forwards the message to the facility layer (IVS-FL) for futher processing
OEM-RE	OEM-RE	The given time set in the timer for "lifetime without validation" for a given message is expired and the vlidation procedure is started



2.13.4 Actions Post-Operational

From	To	Description	Optional
Description-1		After the TC receives the "road works finalized" message from the blocking trailer it informs the OEM Backend via normal update message.	

2.13.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS-CUCel	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.		x	
IVS-FL	Processing steps for messages inside an IVS/IRS, that are application independent (e.g. Message distribution or CAM creation)		x	
GeoMS-MNO	Server in the C2X-SN and/or SP and /or CN that distributes information to clients in a geographical area.		x	
OEM-GTL	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.		x	
OEM-IEA	Running on all communication endpoint entities. It represents the SAP for all incoming messages.		x	
OEM-RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	
TC-CU	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.		x	

2.13.6 Decision Points Identified

ID	Component	Description

2.13.7 External Activities Identified

ID	Group	Description

UST-GeoCast		A mechanism has to be provided by the overall system that allows to transmit 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
UST-Sec		A mechanism has to be provided that allows to generate and distribute security data (keys, certificates) to all participants of the C2X-SN
UST-OEM-RWW-Setup		The detailed setup procedure for the RWW service at the OEM has to be described.

2.14 UC-IVS2SP-04

A vehicle detects a change in one of the traffic signs that it has in its own map and informs SP about this change

2.14.1 Assumptions

ID	Description
UC-IVS2SP-04_A1	

2.14.2 Actions Pre-Operational

From	To	Description	Optional

2.14.3 Actions Operational

From	To	Description	Optional

2.14.4 Actions Post-Operational

From	To	Description	Optional

2.14.5 Components Identified

Name	Description	Involvement		
		Pre-	Operation	Post-

		Operation		Operation

2.14.6 Decision Points Identified

ID	Component	Description

2.14.7 External Activities Identified

ID	Group	Description

2.15 UC-IVS-04

IVS decodes received message

2.15.1 Assumptions

ID	Description
UC-IVS-04_A1	Message is valid

2.15.2 Actions Pre-Operational

From	To	Description	Optional

2.15.3 Actions Operational

From	To	Description	Optional

2.15.4 Actions Post-Operational

From	To	Description	Optional

2.15.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.15.6 Decision Points Identified

ID	Component	Description

2.15.7 External Activities Identified

ID	Group	Description

2.16 UC-IVS2SP-02

The service provider receives sensor readings of IVSs, checks the access rights of the IVS and validates the data. The service provider aggregates, advertises and provides the data to other service providers and/or the MDM. In addition the service provider presents the results via remote-GUI to web-clients for project evaluation.If necessary the service provider can request sensor data from IVSs in a specific area of interest.Reception of vehicle detected data will be acknowledged to the IVS

2.16.1 Assumptions

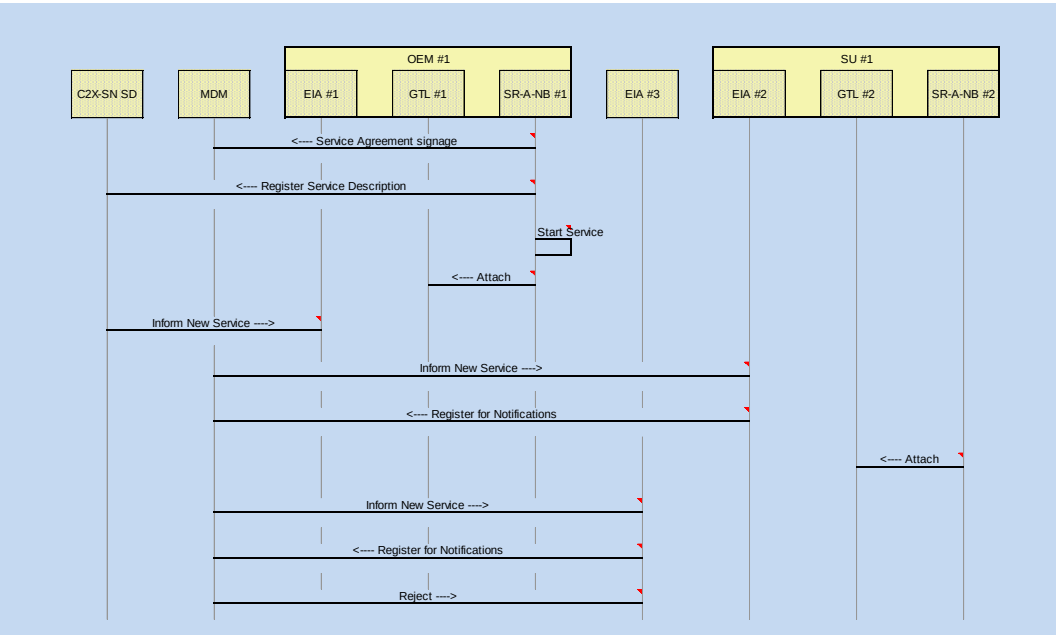
ID	Description
UC-IVS2SP-02_A1	The communication channel between IVSs and the OEMs Backends have been registered and established (-> separate user-story!) and “behaves transparent” within UC-IVS2SP-02
UC-IVS2SP-02_A2	The respective IVSs have agreed and signed a contract to share sensor readings information with the service provider. The details of the provided sensor readings have been agreed and documented.
UC-IVS2SP-02_A3	The respective IVSs have been registered with the C2X-SN as "Service Providers" for sensor readings and hence have received C2X-SN access premising certificate (APC-sn) (-> separate user-story)
UC-IVS2SP-02_A4	The service provider has regsitered itself with MDM as provider of aggregated data based on sensor readings from IVSs (-> separate user story)
UC-IVS2SP-02_A5	The Sensor Readings Type A message distribution service has been agreed to be called "SR-A-Notification Board (SR-A-NB)"

2.16.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite#1		A human readable document (e.g. HTML-text document), describing the characteristics of the SR-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 SR-A-NB service is available
Prerequisite#3		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#4		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, Event Incoming Alert service (e.g. EIA_#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 Sensor Readings specific service access certificate, called APC_sn_SR-A-NB, has been issued to all OEMs providing the service. The certificate is not only bound to the service but also allows to distinguish between different service providers
Prerequisite#7		Each service provider that wants to share aggregated sensor readings data via MDM registers itself to MDM and provides the necessary information about the aggregated sensor readings service (ASR-A) type A to MDM (-> separate user story)
SR-A-NB #1	MDM	OEM #1 aggrees with MDM about exchange of aggregated sensor readings data via MDM (-> separate user story)
SR-A-NB #1	C2X-SN SD	OEM #1 registers its WSDL description for service SR-A-NB #1 at C2X-SN Service Directory Server, together with APC_sn_SR-A-NB certificate
SR-A-NB #1	SR-A-NB #1	OEM #1 starts its Web Service SR-A-NB #1 at its OEM Backend server farm
SR-A-NB #1	GTL #1	OEM #1 attaches its Generic Transaction Logging (GTL_#1) service with its SR-A-NB service and re-configure s their firewalls to permit access for requests, authorized via certificate APC_sn_SR-A

C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs OEM #1 that a new service has registered itself, by posting OEM #1 EIA event reception point, providing its WSDL and its textual descriptions
MDM	EIA #2	The MDM informs SU #1 that a new service has registered itself (-> separate user story).
EIA #2	MDM	SU #1 EIA_#2 contacts MDM (-> separate user story), presenting its certificate APC_sn_SR-A, to register itself as receiver of Sensor Reading Type A message notifications.
SR-A-NB #2	GTL #2	SU #1 attaches its Generic Transaction Logging (GTL_#2) service with its SR-A-NB service and re-configure s their firewalls to permit access for requests, authorized via certificate APC_sn_SR-A
MDM	EIA #3	The MDM informs OEM #3 that a new service has registered itself (-> separate user story).
EIA #3	MDM	OEM #2 EIA_#2 contacts MDM (-> separate user story), presenting its certificate APC_sn_SR-A, to register itself as receiver of Sensor Reading Type A message notifications.
MDM	EIA #3	MDM (-> separate user story) detects the invalidity of the certificate of OEM #2 and rejects the registration



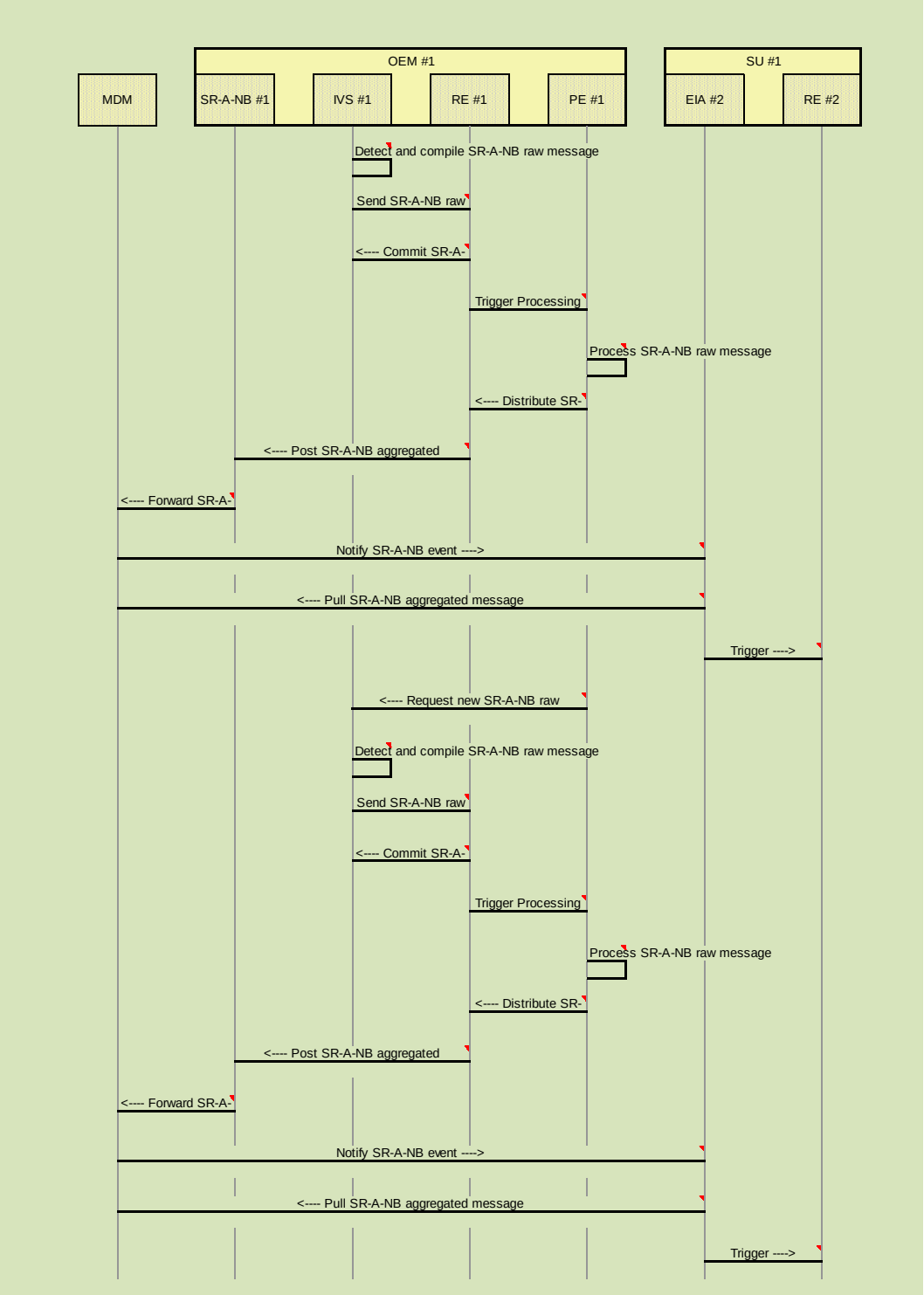
2.16.3 Actions Operational

From	To	Description	Optional

Prerequisite#8		All OEMs that have agreed to exchange Sensor Reading Type A messages have registered their Sensor Reading-A “brand xyz” service, attached their transaction logging service with their Sensor Reading-A, have registered their EIA services with their contract partner’s Backend Sensor Reading-A Services and are ready for operation
IVS #1	IVS #1	A vehicle of brand #1 (IVS_#1) has new Sensor Reading Type A sensor-data. A dedicated message of Type A, i.e. SR-A_#1_raw_message-content, has been compiled
IVS #1	RE #1	The IVS platform sends the message SR-A_#1_raw_message-content to the OEM #1 Backend. The communication path between the #1 IVS and the #1 Backend is fully transparent, as seen from a IVS sensor data processing platform perspective
RE #1	IVS #1	The OEM #1 internal message processing rule engine RE (-> separate user story) checks the SR-A-NB raw message (authenticity, correctness, format, …) from the IVS #1 and, if the message is correct, sends a confimation back to the IVS #1
RE #1	PE #1	The OEM #1 internal message processing rule engine RE (-> separate user story) detects that SR-A-NB #1 message content has to be further processed (checked, aggregated, …) to contribute to the SR-A-NB #1 service provided to other service users. Thus it hands the new message to the OEM #1 processing engine for further processing
PE #1	PE #1	The OEM #1 internal processing engine further processes (checks, aggregates, …) the new SR-A-NB #1_raw_message content and generates a new SR-A-NB #1_aggregated_message content (-> separate user story)
PE #1	RE #1	The OEM #1 internal processing engine sends the new SR-A-NB #1_aggregated_message internally to the OEM #1 message processing rule engine
RE #1	SR-A-NB #1	The OEM #1 internal message processing rule engine RE (-> separate user story!) detects that SR-A_#1_aggregated_message-content is to be shared via the SR-A_#1 service. Hence SR-A_#1_aggregated_message-content gets posted to the SR-A_#1 service
SR-A-NB #1	MDM	The server SR-A-NB #1 forwards the new SR-x A_#1_aggregated_message-content to the MDM (-> separate user story)

MDM	EIA #2	MDM issues an SR-A_Event_Notification(ID) message (-x > separate user story) with all event receivers which had been registered with SR-A_#1 beforehand as receivers of Sensor Reading Type A events. Hence MDM sends the message SR-A_Event_Notification(ID) to EIA_#2
EIA #2	MDM	Alerted via the incoming heads-up notification, the EIA_#2x pulls for the message(ID) from MDM (-> separate user story)
EIA #2	RE #2	SU #1 triggers its local Backend rule engine with thex newly available Sensor Reading Type A message SR-A_#1_aggregated_message-content which was originating from IVS_#1. Further processing and actions are with #3
PE #1	IVS #1	The OEM #1 internal processing engine needs additionalx information for further processing of the SR-A-NB messages it therefore requests the IVS #1 to send additional SR-A-NB raw message-content information
IVS #1	IVS #1	IVS_#1 gets the request from PE #1 and compiles newx Sensor Reading Type A sensor-data. A dedicated message of Type A, i.e. SR-A_#1_raw_message-content, has been compiled
IVS #1	RE #1	The IVS platform sends the message SR-x A_#1_raw_message-content to the OEM #1 Backend. The communication path between the #1 IVS and the #1 Backend is fully transparent, as seen from a IVS sensor data processing platform perspective
RE #1	IVS #1	The OEM #1 internal message processing rule engine REx (-> separate user story) checks the SR-A-NB raw message (authenticity, correctness, format, …) from the IVS #1 and, if the message is correct, sends a confimation back to the IVS #1
RE #1	PE #1	The OEM #1 internal message processing rule engine REx (-> separate user story) detects that SR-A-NB #1 message content has to be further processed (checked, aggregated, …) to contribute to the SR-A-NB #1 service provided to other service users. Thus it hands the new message to the OEM #1 processing engine for further processing
PE #1	PE #1	The OEM #1 internal processing engine further processesx (checks, aggregates, …) the new SR-A-NB #1_raw_message content and generates a new SR-A-NB #1_aggregated_message content (-> separate user story)

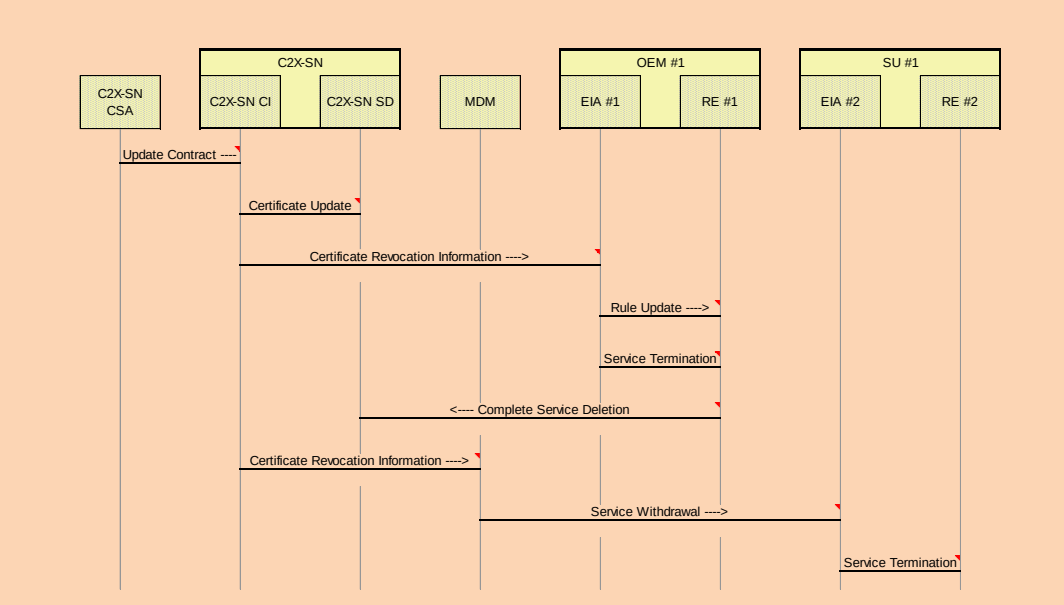
PE #1	RE #1	The OEM #1 internal processing engine sends the newx SR-A-NB #1_aggregated_message internally to the OEM #1 message processing rule engine
RE #1	SR-A-NB #1	The OEM #1 internal message processing rule enginex RE (-> separate user story!) detects that SR-A_#1_aggregated_message-content is to be shared via the SR-A_#1 service. Hence SR-A_#1_aggregated_message-content gets posted to the SR-A_#1 service
SR-A-NB #1	MDM	The server SR-A-NB #1 forwards the new SR-x A_#1_aggregated_message-content to the MDM (-> separate user story)
MDM	EIA #2	MDM issues an SR-A_Event_Notification(ID) message (-x > separate user story) with all event receivers which had been registered with SR-A_#1 beforehand as receivers of Sensor Reading Type A events. Hence SR-A_#1 sends the message SR-A_Event_Notification(ID) to EIA_#2
EIA #2	MDM	Alerted via the incoming heads-up notification, the EIA_#3x pulls for the message(ID) from MDM (-> separate user story)
EIA #2	RE #2	SU #1 triggers its local Backend rule engine with thex newly available Sensor Reading Type A message SR-A_#1_aggregated_message-content which was originating from IVS_#1. Further processing and actions are with #3



2.16.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All SR-A-NB and EIA services at OEM #1, and SU #1 are ready to serve the next event	

Prerequisite#10		OEM #1 has terminated the SR-A-NB contract and notified the C2X-SN Contract Supervision Authority. OEM #1 had been the only SR-A-NB service provider left at the C2X-SN and decided to revoke that offer. Hence the SR-A-NB service shall disappear as if it had never been launched
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SR-A-NB-3, associated with service SR-A-NB, has been activated, replacing certificate APC_sn_SR-A-NB-2
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of #1 to inform that the Certificate APC_sn_SR-A-NB has been revoked. #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of #1 updates its event notification rules (i.e. #1 deletes #2 from its notification list.)
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. #1 purges it entire SR-A-NB service configuration and terminates SR-A-NB_#1
RE #1	C2X-SN SD	#1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SR-A-NB_#1 service offer
C2X-SN CI	MDM	The C2X-SN Certification-Issuer contacts the MDM (->x separate user story) to inform that the Certificate APC_sn_SR-A-NB has been revoked. MDM updates its local certification management
MDM	EIA #2	MDM contacts (-> separate user story) the EIA receptorsx of SU #1 to inform that SU #1 has withdrawn from service SR-A-NB
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SR-A-NB service configuration and terminates SR-A-NB_#2



2.16.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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	Entity for data exchange and data format translation. A special SP for SP to SP traffic related information distribution.	x	x	x
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		x
GTL #1	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x		
IVS #1			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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.		x	
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SR-A-NB #1	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 services/information. This can be inside the C2X-SN itself and/or 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	
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
GTL #2	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x		
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SR-A-NB #2	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 services/information. This can be inside the C2X-SN itself and/or 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		

2.16.6 Decision Points Identified

ID	Component	Description
DP-SD	C2X-SN SD	Find a way to realize the C2X-SN Service Directory
DP-TL	GTL #1	Find a way to realize transaction logging to support charging, KPI supervision, security inspection
DP-AGG	PE #1	Find a way to reasonably aggregate raw sensor readings data in order to generate usable service data information
DP-MDM	MDM	Find the best way to provide and use services via MDM

2.16.7 External Activities Identified

ID	Group	Description
UST-ComCh	OEMs	Registration and establishment of the communication channel between IVS and the service provider
UST-SPReg	OEMs	Registration of IVSs with the C2X-SN as “Service Providers" for sensor readings data and reception of C2X-SN access premising certificate (APC_sn)
UST-SPNM	C2X-SN	Notification Mechanism for notifying service participants about changes in a service they have been registered to

UST-SPCM	C2X-SN	Contact mechanism to reach the C2X-SN Service Description ("yellow pages") Service
UST-KPISV	C2X-SN	Interface service to support charging, KPI supervision or security inspection functions
UST-RE	IS-Backend	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	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-AGG	OEMs	Aggregation an processing of sensor reading data

2.17 UC-IVS2SP-03

The service provider receives a service request and checks the access rights of requesting IVS. The service provider selects the data corresponding to the request, calculates waypoints (with descriptions) guiding to the free parking and finally sends it to the IVS.

2.17.1 Assumptions

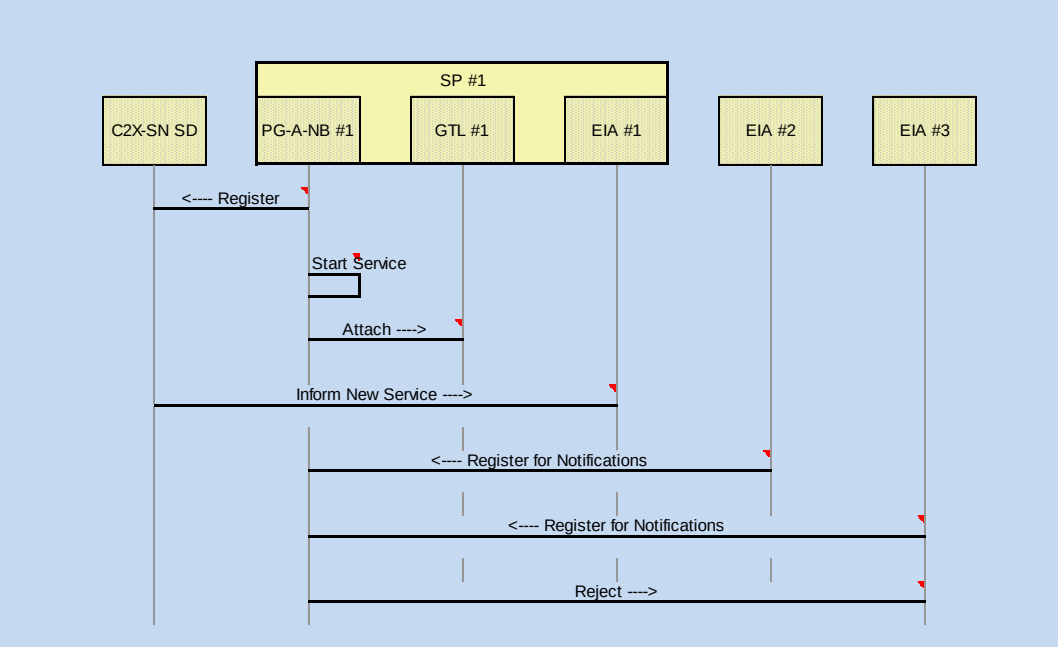
ID	Description
UC-IVS2SP-03_A1	The communication channel between IVSs and the OEMs Backends have been registered and established (-> separate user-story!) and “behaves transparent” within UC-IVS2SP-03
UC-IVS2SP-03_A2	The respective IVSs have aggreed and signed a contract to use the parking guide service with the respective service provider
UC-IVS2SP-03_A3	The service provider has registered with C2X-SN as a "Service Provider" for parking guide information and hence has received C2X-SN access premising certificate (APC_sn) (-> separate user story)
UC-IVS2SP-03_A4	The parking guide information Type A message service has been agreed to be called "PG-A-Notification Board (PG-A-NB)"
UC-IVS2SP-03_A5	The service provider has a data base that holds actual parking information in order to provide the service PG-A-NB (-> separate user story)

2.17.2 Actions Pre-Operational

From	To	Description	Optional

Prerequisite#1		A human readable document (e.g. HTML-text document), describing the characteristics of the PG-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 PG-A-NB service is available
Prerequisite#3		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#4		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, Event Incoming Alert service (e.g. EIA_#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 Sensor Readings specific service access certificate, called APC_sn_PG-A-NB, has been issued to all SUs providing the service. The certificate is not only bound to the service but also allows to distinguish between different service providers
PG-A-NB #1	C2X-SN SD	SP #1 registers its WSDL description for service PG-A-NB #1 at C2X-SN Service Directory Server, together with APC_sn_PG-A-NB certificate
PG-A-NB #1	PG-A-NB #1	SP #1 starts its Web Service PG-A-NB #1 at its SU Backend server farm
PG-A-NB #1	GTL #1	SP #1 attaches its Generic Transaction Logging (GTL_#1) service with its PG-A-NB service and re-configures its firewalls to permit access for requests, authorized via certificate APC_sn_PG-A-NB
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions

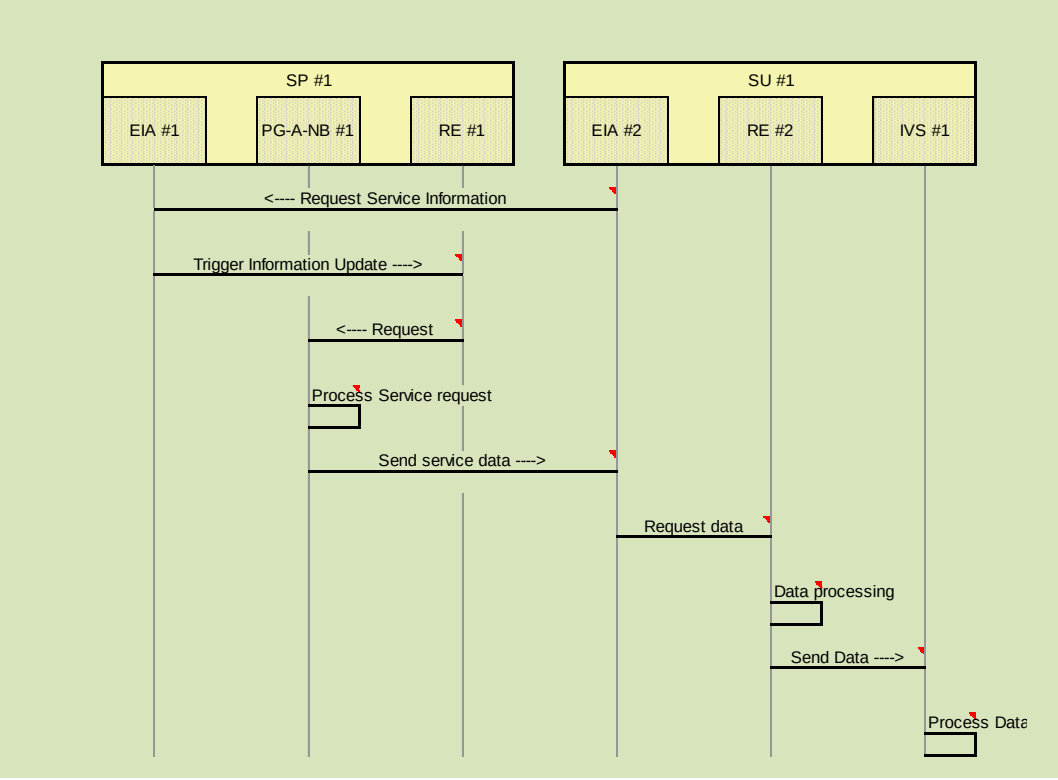
EIA #2	PG-A-NB #1	SU #1 EIA_#2 contacts PG-A-NB_#1, presenting its certificate APC_sn_PG-A-NB, to register itself as receiver of LHW Type A message notifications.
EIA #3	PG-A-NB #1	SU #2 EIA_#3 contacts PG-A-NB_#1, presenting its certificate APC_sn_PG-A-NB, to register itself as receiver of LHW Type A message notifications.
PG-A-NB #1	EIA #3	SP #1 PG-A-NB #1 detects the invalidity of the certificate of SU #2 and rejects the registration



2.17.3 Actions Operational

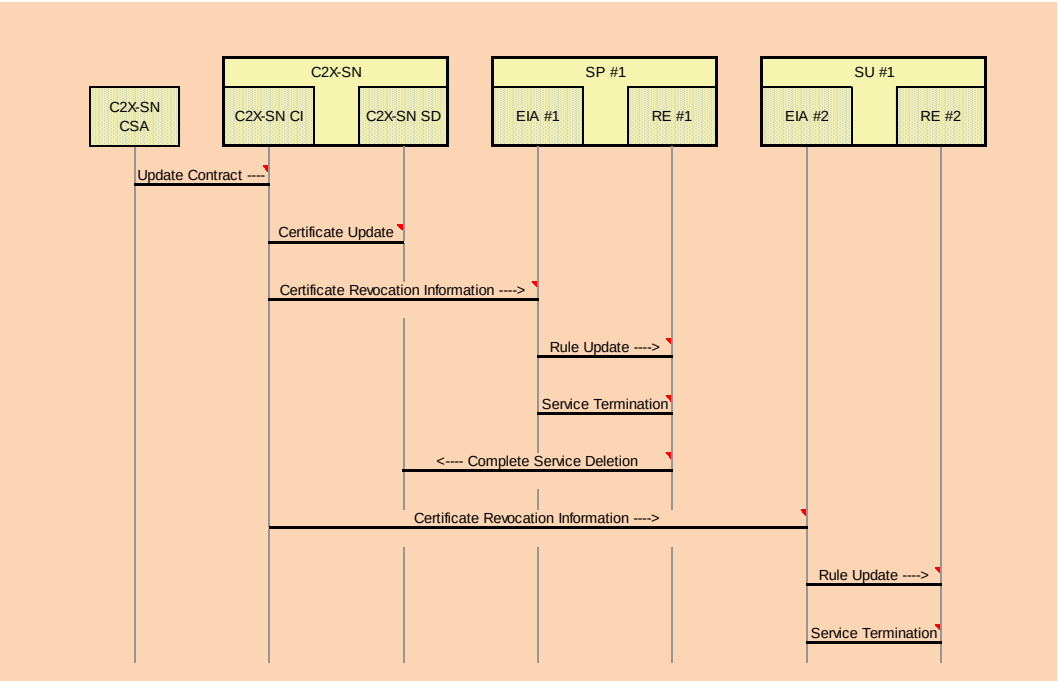
From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the PG Type A information has registered its PG-A-NB service, attached its transaction logging service with its PG-A-NB and is ready for service	
Prerequisite#8		Each service user that wants to use the PG-A service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new parking guide information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	
RE #1	PG-A-NB #1	The rue engine is requesting the service module for PG-A-NB #1 service to process the service request	

PG-A-NB #1	PG-A-NB #1	The service module PG-A-NB #1 is processing the service request (-> separate user story) by checking the given information about the route and retriving information about the parking spaces along the route and further preparation of a service message that gives the necessary information to the service user
PG-A-NB #1	EIA #2	The service module PG-A-NB #1 is sending the preprocessed service information to the service user SU #1
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the PG-A-NB #1 service and triggers the respective actions (e.g. Providing the data to the IVS)
RE #2	IVS #1	The rule engine of SU #1 is sending the information derived from the service PG-A-NB #1 to the respective IVSs
IVS #1	IVS #1	The IVSs that receive the information about the parking situation along their route take further actions to e.g. inform the driver (-> separate user story)



2.17.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All PG-A-NB and EIA services at SP #1, and SU #1 are ready to serve the next event	
Prerequisite#10		SP #1 has terminated the PG-A-NB contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only PG-A-NB service provider left at the C2X-SN and decided to revoke that offer. Hence the PG-A-NB service shall disappear as if it had never been launched	
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_PG-A-NB-2, associated with service PG-A-NB, has been activated, replacing certificate APC_sn_PG-A-NB-1	
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_PG-A-NB has been revoked. SP #1 updates its local certification management	
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.	
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire PG-A-NB service configuration and terminates PG-A-NB_#1	
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the PG-A-NB_#1 service offer	
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_PG-A-NB has been revoked. SU #1 updates its local certification management	
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.	
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire PG-A-NB service configuration and terminates PG-A-NB_#1	



2.17.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
GTL #1	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x		
PG-A-NB #1	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 services/information. This can be inside the C2X-SN itself and/or 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	
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
IVS #1			x	
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.17.6 Decision Points Identified

ID	Component	Description

DP-SD	C2X-SN SD	Find a way to realize the C2X-SN Service Directory
DP-TL	GTL #1	Find a way to realize transaction logging to support charging, KPI supervision, security inspection

2.17.7 External Activities Identified

ID	Group	Description
UST-ComCh	OEMs	Registration and establishment of the communication channel between IVS and the OEM Backend
UST-SPReg	OEMs	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	C2X-SN	Notification Mechanism for notifying service participants about changes in a service they have been registered to
UST-SPCM	C2X-SN	Contact mechanism to reach the C2X-SN Service Description ("yellow pages") Service
UST-KPISV	C2X-SN	Interface service to support charging, KPI supervision or security inspection functions
UST-RE	IS-Backend	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-PGDB	SP #1	Description of the process and components to fill and maintain a database that is holding all necessary information to provice the parking guide information service
UST-PGSP	SP #1	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)
UST-PGSU	SU #1	Description of the process and components that are necessary to present the received information about parking spaces the the end user in the IVS

2.18 UC-SP-04

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 opbtained data. The service provider assigns the obtained parking space data to predefined destination categories.

2.18.1 Assumptions

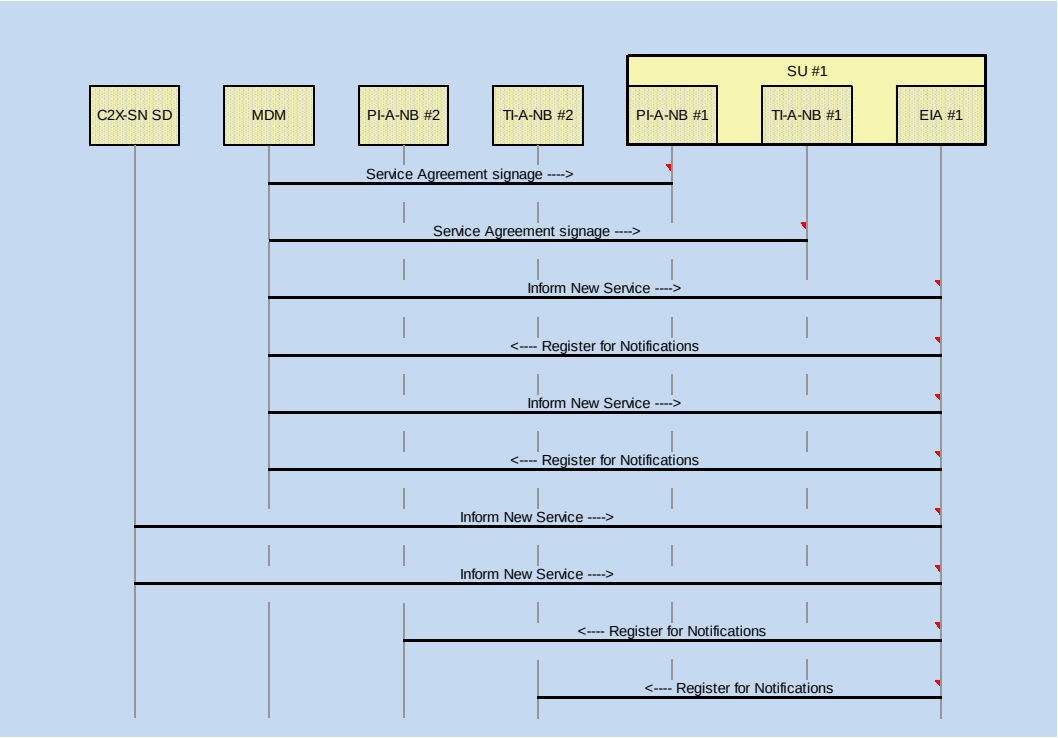
ID	Description
UC-SP-04_A1	The communication channel between IVSs and the OEMs Backends have been registered and established (-> separate user-story!) and “behaves transparent” within UC-SP-04
UC-SP-04_A2	Service providers that are delivering parking information and/or traffic information have been registered 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 premising 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 premising 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)"

2.18.2 Actions Pre-Operational

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, Event Incoming Alert service (e.g. EIA_#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)
MDM	PI-A-NB #1	service user SU #1 aggrees with MDM about exchange of parking information data via MDM (-> separate user story)
MDM	TI-A-NB #1	service user SU #1 aggrees with MDM about exchange of traffic information data via MDM (-> separate user story)
MDM	EIA #1	The MDM informs SU #1 that a new parking information service has registered itself (-> separate user story).
EIA #1	MDM	SU #1 EIA_#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	EIA #1	The MDM informs SU #1 that a new traffic information service has registered itself (-> separate user story).

EIA #1	MDM	SU #1 EIA_#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	EIA #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 EIA event reception point, providing its WSDL and its textual descriptions
C2X-SN SD	EIA #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 EIA event reception point, providing its WSDL and its textual descriptions
EIA #1	PI-A-NB #2	SU #1 EIA_#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.
EIA #1	TI-A-NB #2	SU #1 EIA_#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.



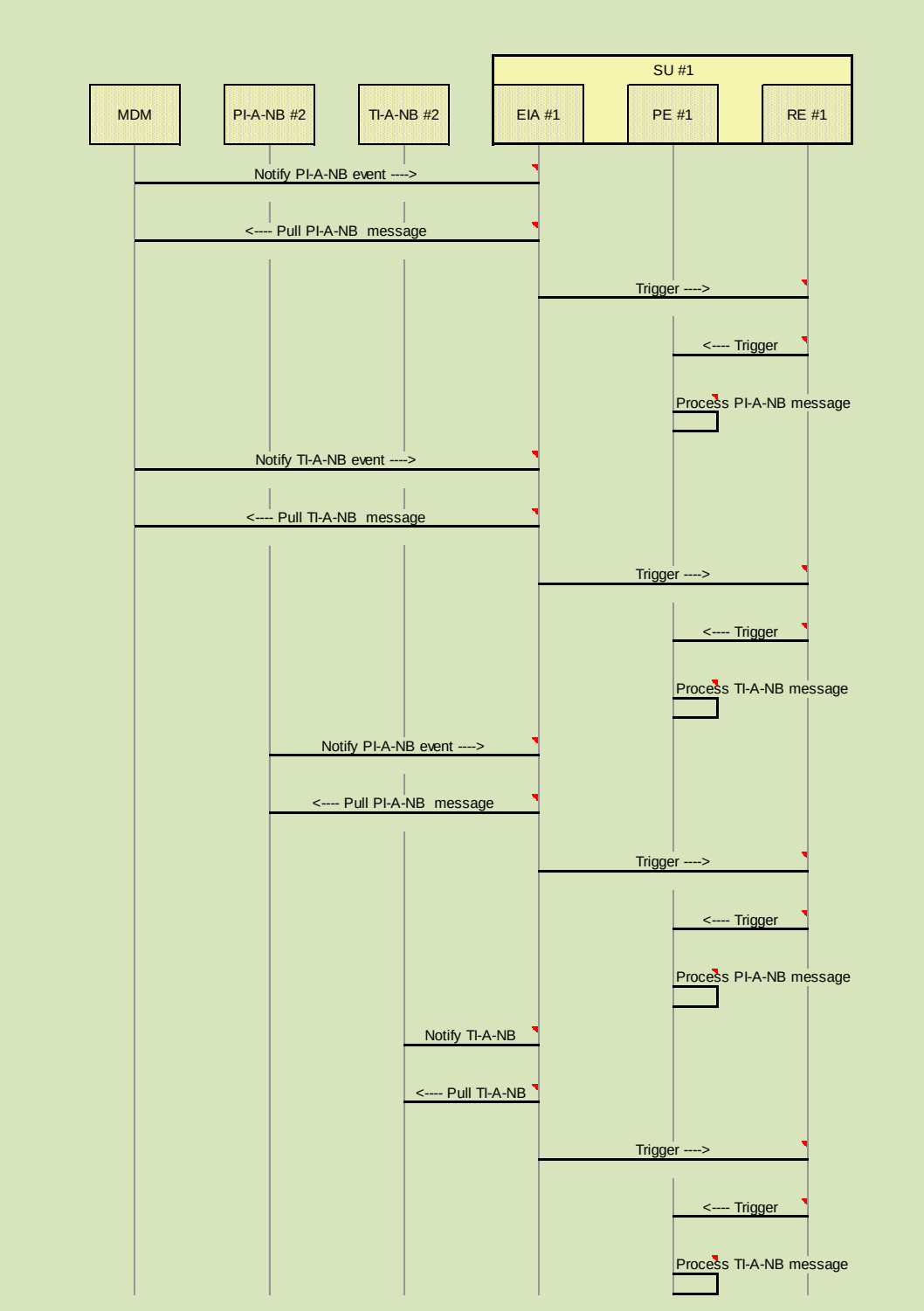
2.18.3 Actions Operational

From	To	Description	Optional

Prerequisite#10		At least on 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 EIA services with their contract partner’s Backend PI-A-NB Services and is ready for operation
Prerequisite#11		At least on 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 EIA services with their contract partner’s Backend TI-A-NB Services and is ready for operation
Prerequisite#12		At least on 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 on service provider has agreed to provide TI Type A messages via MDM and done the necessary steps to offer and provide the service
MDM	EIA #1	MDM issues an PI-A_Event_Notification(ID) message (->x 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 EIA_#1
EIA #1	MDM	Alerted via the incoming heads-up notification, the EIA_#1x pulls for the message(ID) from MDM (-> separate user story)
EIA #1	RE #1	SU #1 triggers its local Backend rule engine with thex newly available Parking Information Type A message PI-A_#1__message-content
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-x > 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
PE #1	PE #1	The SU #1 internal processing engine further processesx (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 opbtained data. The service provider assigns the obtained parking space data to predefined destination categories.

MDM	EIA #1	MDM issues an TI-A_Event_Notification(ID) message (->x 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 EIA_#1
EIA #1	MDM	Alerted via the incoming heads-up notification, the EIA_#1x pulls for the message(ID) from MDM (-> separate user story)
EIA #1	RE #1	SU #1 triggers its local Backend rule engine with thex newly available Parking Information Type A message TI-A_#1__message-content
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-x > separate user story) detects that TI-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
PE #1	PE #1	The SU #1 internal processing engine further processesx (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 opbtained data. The service provider assigns the obtained parking space data to predefined destination categories.
PI-A-NB #2	EIA #1	SP #1 issues an PI-A_Event_Notification(ID) message (->x 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 EIA_#1
EIA #1	PI-A-NB #2	Alerted via the incoming heads-up notification, the EIA_#1x pulls for the message(ID) from SP #1
EIA #1	RE #1	SU #1 triggers its local Backend rule engine with thex newly available Parking Information Type A message PI-A_#1__message-content
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-x > 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

PE #1	PE #1	The SU #1 internal processing engine further processesx (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 opbtained data. The service provider assigns the obtained parking space data to predefined destination categories.
TI-A-NB #2	EIA #1	SP #2 issues an TI-A_Event_Notification(ID) message (->x 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 EIA_#1
EIA #1	TI-A-NB #2	Alerted via the incoming heads-up notification, the EIA_#1x pulls for the message(ID) from SP #2
EIA #1	RE #1	SU #1 triggers its local Backend rule engine with thex newly available Parking Information Type A message TI-A_#1__message-content
RE #1	PE #1	The SU #1 internal message processing rule engine RE (-x > 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
PE #1	PE #1	The SU #1 internal processing engine further processesx (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 opbtained data. The service provider assigns the obtained parking space data to predefined destination categories.

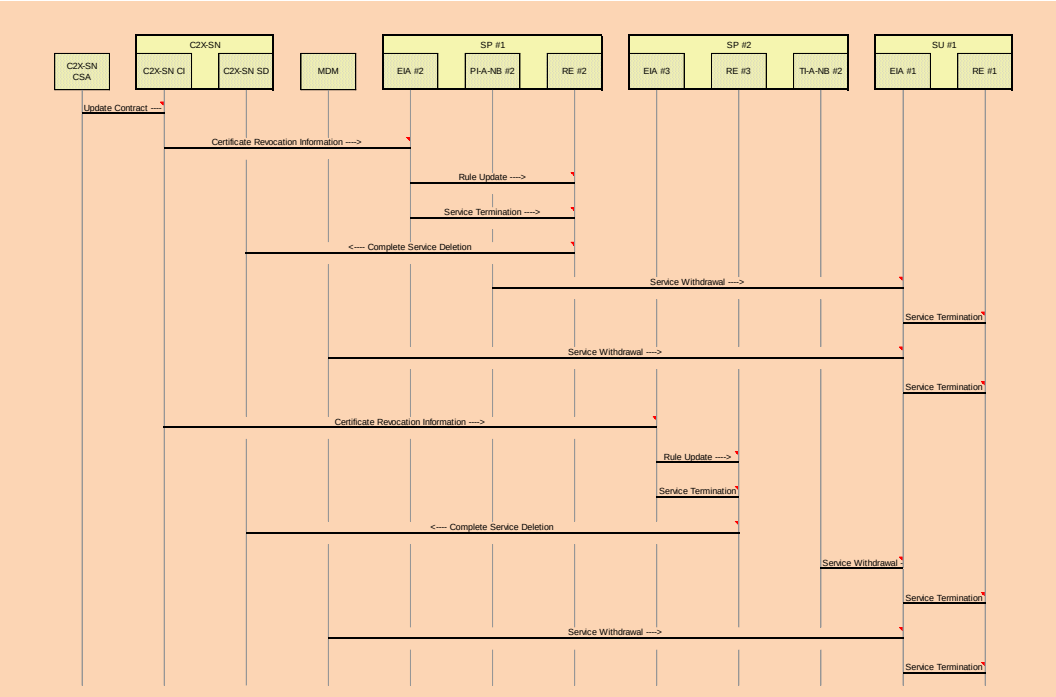


2.18.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#14		All PI-A-NB and EIA services at SU #1 are ready to serve the next event	

Prerequisite#15		All TI-A-NB and EIA 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 MDMhad 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 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	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_PI-A-NB has been revoked. SP #1 updates its local certification management
EIA #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
EIA #2	RE #2	SP #1 EIA trigges 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	EIA #1	SP #1 contacts the EIA receptors of SU #1 to inform thatx the parking information service is not available any more
EIA #1	RE #1	SU #1 EIA trigges its local RE with the update request. SU #1 purges it entire PI-A-NB service configuration and terminates PI-A-NB_#1
MDM	EIA #1	MDM contacts (-> separate user story) the EIA receptorsx of SU #1 to inform that the parking information service is not available any more
EIA #1	RE #1	SU #1 EIA trigges 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	EIA #3	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #2 to inform that the Certificate APC_sn_TI-A-NB has been revoked. SP #2 updates its local certification management
EIA #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 #2 updates its event notification rules
EIA #3	RE #3	SP #2 EIA trigges 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	EIA #1	SP #2 contacts the EIA receptors of SU #1 to inform thatx the traffic information service is not available any more
EIA #1	RE #1	SU #1 EIA trigges its local RE with the update request. SU #1 purges it entire PI-A-NB service configuration and terminates PI-A-NB_#1
MDM	EIA #1	MDM contacts (-> separate user story) the EIA receptorsx of SU #1 to inform that the traffic information service is not available any more
EIA #1	RE #1	SU #1 EIA trigges its local RE with the update request. SU #1 purges it entire TI-A-NB service configuration and terminates TI-A-NB_#1



2.18.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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	Entity for data exchange and data format translation. A special SP for SP to SP traffic related information distribution.	x	x	x
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.			x
PI-A-NB #2	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 services/information. This can be inside the C2X-SN itself and/or 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	x
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.			x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.			x
RE #3	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.			x

TI-A-NB #2	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 services/information. This can be inside the C2X-SN itself and/or 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	x
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.		x	
PI-A-NB #1	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 services/information. This can be inside the C2X-SN itself and/or 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		
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
TI-A-NB #1	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 services/information. This can be inside the C2X-SN itself and/or 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	x		

2.18.6 Decision Points Identified

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

2.18.7 External Activities Identified

ID	Group	Description
UST-ComCh	OEMs	Registration and establishment of the communication channel between IVS and the OEM Backend
UST-PIMDM	MDM	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	OEMs	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	C2X-SN	Notification Mechanism for notifying service participants about changes in a service they have been registered to
UST-SPCM	C2X-SN	Contact mechanism to reach the C2X-SN Service Description ("yellow pages") Service
UST-KPISV	C2X-SN	Interface service to support charging, KPI supervision or security inspection functions
UST-RE	IS-Backend	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	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-MDM	SP	Detailed description about providing services via C2X-SN This includes: - User registration - Service registration - Service announcement - Service information distribution - Certification management - Data distribution

2.19 UC-SP-05

The service provider receives the request (UC-IVS2SP-02_01) and checks the access rights of requesting IVS. The service provider forwards the request to the corrensponding CA.The CA validates the request and creates the certificates for the IVS and sends the certificates according to ETSI TS 102 941 back to the service provider (In UC-SP-1000). Having received, the service provider sends the certificates to the IVS.

2.19.1 Assumptions

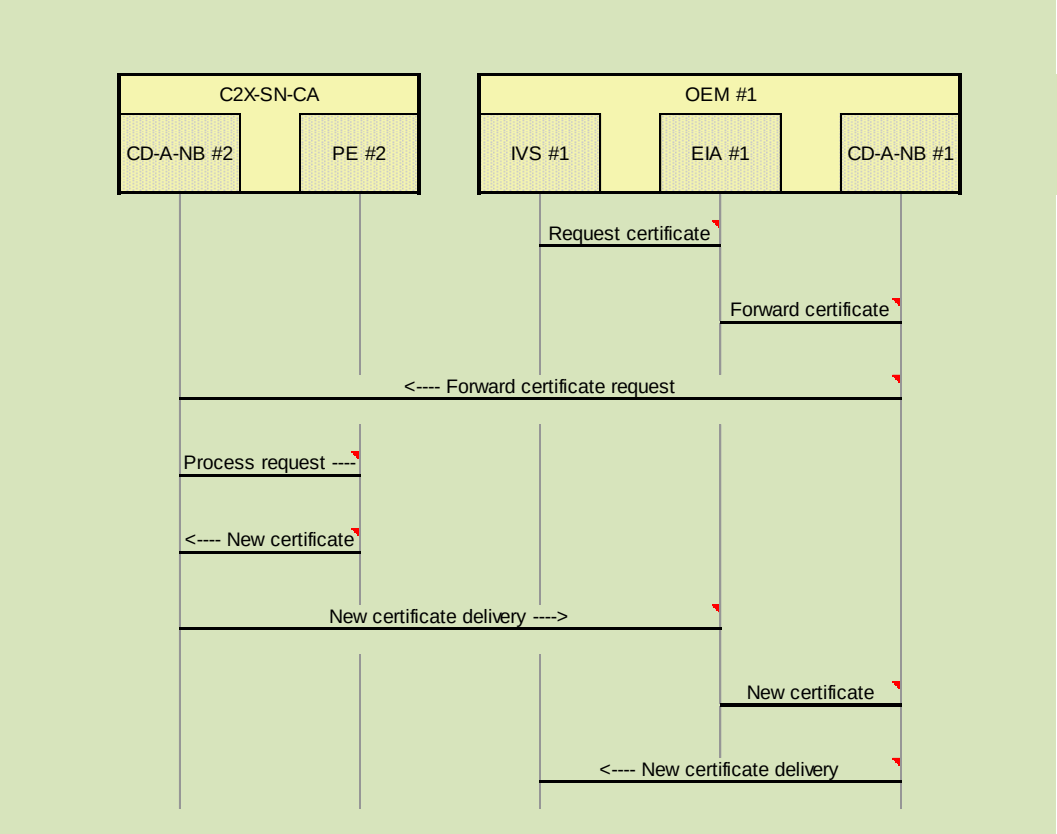
ID	Description
UC-SP-05_A1	The communication channel between IVSs and the OEMs Backends have been registered and established (-> separate user-story!) and “behaves transparent” within UC-SP-05
UC-SP-05_A2	Certification authorities (CA) are existing that are trusted by all participants of the C2X-SN (-> separate user story). The CAs are able to generate certificates that are certifying a certain user and allowing other users to check authenticity of signed messages. Furthermore the certificates are allowing to set up a secure and confiential communication between users of the C2X-SN. Eeach certificate has a certain lifety and identifies access rights that allow the certified user to use/provide certain services in the C2X-SN.
UC-SP-05_A3	A set of rules is existing that are defining how certificates are generated for users of the C2X-SN (-> separate user story). The rules are known to and accepted by all participants in the C2X-SN.
UC-SP-05_A4	The certificate distribution type A service has been agreed to be called "CD-A-Notification Board (CD-A-NB)"

2.19.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite#1		A human readable document is existing that describes the security concpet of the C2X-SN. This document can be checked and inspected by all potential users of the C2X-SN and must be accepted before taking part in the C2X-SN	
Prerequisite#2		A human readable document (e.g. HTML-text document), describing the characteristics of the CD-A-NB messages, their information quality and uncertainties, is available for human inspection.	
Prerequisite#3		A software readable interface description (e.g. XMP, WSDL, Web Service description file) of the PI-A-NB service is available	
Prerequisite#4		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#5		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#6		Each service provider has a generic, Event Incoming Alert service (e.g. EIA_#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#7		A certificate distribution specific service access certificate, called APC_sn_CD-A-NB has been issued to all users of the C2X-SN	
Prerequisite#8		The service CD-A-NB is know to all participants of the C2X-SN (-> separate user story). Each service user for CD-A-NB has set up its EIA to listen to messages of type CD-A-NB-Message and the RE of the respective service user knows how to further process incoming events of type CD-A-NB-Message. The generic transaction logging service of each service user is attached to CD-A-NB service and the firewalls of each user are configured to allow for message exchange, authorized with APC_sn_CD-A-NB.	

2.19.3 Actions Operational

From	To	Description	Optional
Prerequisite#9		All OEMs participating in the C2X-SN have registered their CD-A-NB “brand xyz” service, attached their transaction logging service with their CD-A-NB, have registered their EIA services with their contract partner’s Backend CD-A-NB Services and are ready for operation	
IVS #1	EIA #1	The IVS #1 is requesting the update of its certificates. The request contains the information about the existing status of the certificates of the IVS #1 and information about the update requested	
EIA #1	CD-A-NB #1	The CD-A-NB #1 service of OEM #1 checks the request from the respective IVS and, if the check is OK, the request is forwarded to the C2X-SN-CA	
CD-A-NB #1	CD-A-NB #2	The CD-A-NB #1 service of the OME #1 forwards the request for a new certificate to (a) CA of the C2X-SN	
CD-A-NB #2	PE #2	The C2X-SN-CA is processing the certificate renewal request. This includes checking the authenticity of the requester, the ID of the requester, validating the request (e.g. if a certain IVS is not allowed any more to participate to the C2X-SN) and checking the renewal paramters for the requesting IVS (-> separate user story).	
PE #2	CD-A-NB #2	The C2X-SN-CA processing engine (PE) is providing a new certificate to the CD-A-NB #2 service	
CD-A-NB #2	EIA #1	The C2X-SN-CA CD-A-NB #2 service is delivering the new certificate inside of a CD-A-NB-Message to the OEM #1 EIA.	
EIA #1	CD-A-NB #1	The EIA is fowarding the received new certificate to the CD-A-NB #1 service of the OEM #1	
CD-A-NB #1	IVS #1	The OEM #1 delivers the new certificate to the requesting IVS #1	



2.19.4 Actions Post-Operational

From	To	Description	Optional

2.19.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
CD-A-NB #2	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 services/information. This can be inside the C2X-SN itself and/or 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	

PE #2	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.		x	
CD-A-NB #1	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 services/information. This can be inside the C2X-SN itself and/or 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	
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.		x	
IVS #1			x	

2.19.6 Decision Points Identified

ID	Component	Description

DP-CA	Certification authorities (CA) are existing that are trusted by all participants of the C2X-SN (-> separate user story). The CAs are able to generate certificates that are certifying a certain user and allowing other users to check authenticity of signed messages. Furthermore the certificates are allowing to set up a secure and confiential communication between users of the C2X-SN. Eeach certificate has a certain lifety and identifies access rights that allow the certified user to use/provide certain services in the C2X-SN.	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 trus concept also has to be defined.
DP-CD	CD-A-NB #2	The concept of certificate distribution and renewal has to be definde 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, …)

2.19.7 External Activities Identified

ID	Group	Description
UST-ComCh	OEMs	Registration and establishment of the communication channel

		between IVS and the OEM Backend
UST-CAConcept	C2X-SN	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 ….
UST-Certificate	C2X-SN	The details of certification generation rules have to be specified
UST-CD-ServInst	C2X-SN	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.
UST-CertRen	C2X-SN	The renewal concept of certificates has to be specified in detail (e.g. renewal periods, renewal methodology, certificate distribution, …)

2.20 UC-C2X-101_01 Registration

Car2X Systems Network offers a registration for Service Providers, IVSs and Communication Network Providers.

2.20.1 Assumptions

ID	Description
US-Enter-A1.1	The supplicant is totally unknown to the Car2X systems network.
US-Enter-A1.2	

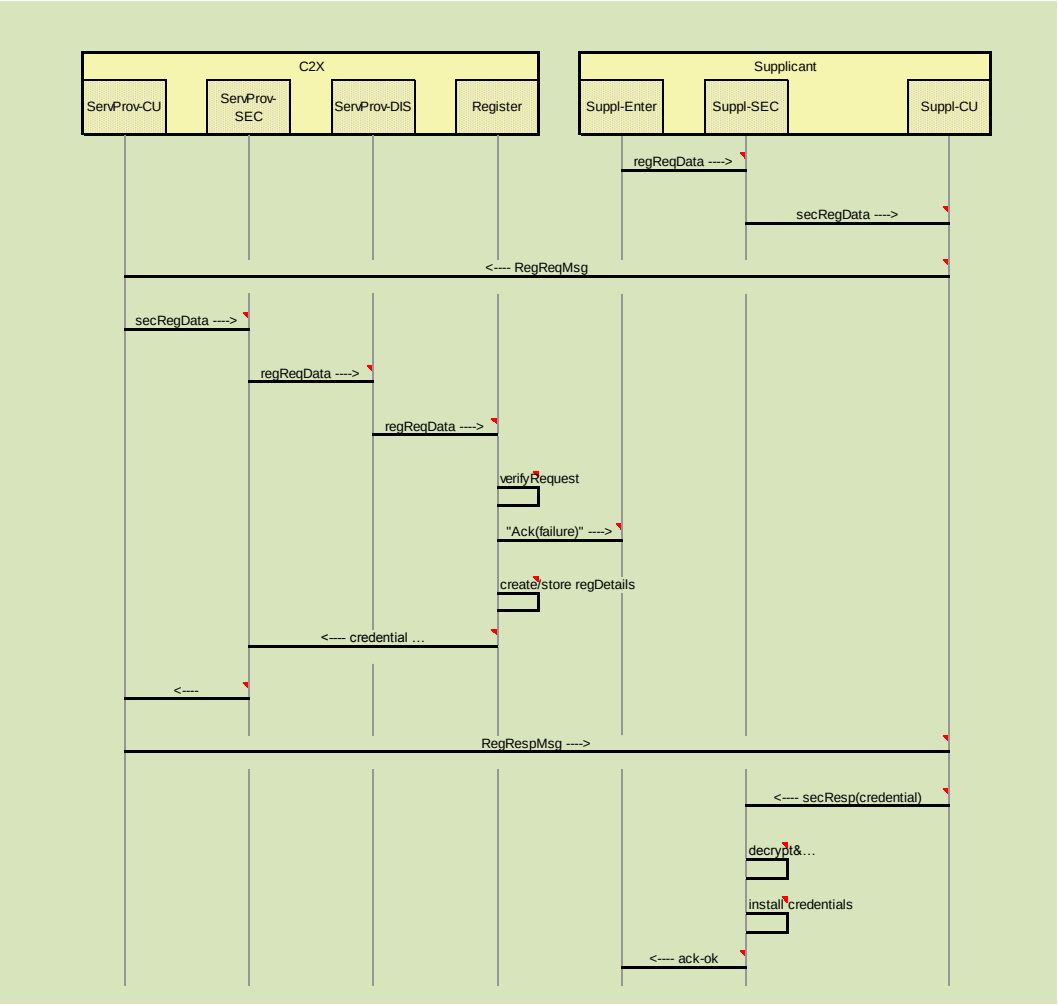
2.20.2 Actions Pre-Operational

From	To	Description	Optional
Prereq-PreOp-1.1		e.g. published on the WEB	
Prereq-PreOp-1.2		Communication means towards actor providing role "Service Provision" exists (Note 1)	
Prereq-PreOp-1.3		A supplicant wants to join the Car2X systems network	

2.20.3 Actions Operational

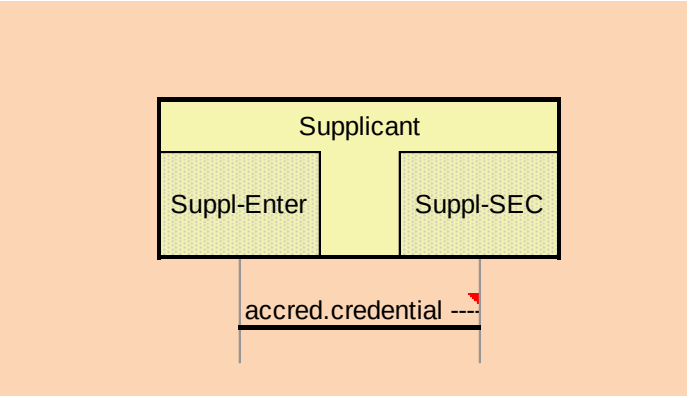
From	To	Description	Optional
Description-1		The supplicant sends an encrypted registration request to service provision. Service provision performs some security checks and forwards the request to registration body. The registration body verifies the request according to its rules and regulations. A data set of the registed user and an unpriviledged enrolment credential is created. A response is sent back to the supplicant, who installs the received credential.	
Prereq-Op-1.1		All rules and regulations required for participating in the Car2X Systems Network are defined, documented and available (=REQ-C2X-007).	
Prereq-Op-1.2		The public key for encrypting messages towards enter access is known to the supplicant.	
Suppl-Enter	Suppl-SEC	The "EnterC2X facility" provides data about itsself to be included in the registration request message.	
Suppl-SEC	Suppl-CU	The message is encryted	
Suppl-CU	ServProv-CU	The encrypted registration request message is sent to service provision	
ServProv-CU	ServProv-SEC	The encryped data are forwarded to the security component	
ServProv-SEC	ServProv-DIS	decrypt content of the registration request and forward to distributor	
ServProv-DIS	Register	the supplicant's registration request is forwarded to the registration body	
Register	Register	the register verifies the request according to its rules and regulations.	
Register	Suppl-Enter	in case the verification failed. The complete backwards is not shown.	
Register	Register	in case the verification succeeded registration data are created and stored	
Register	ServProv-SEC	unpriviledged entrolment credential (Note1) is created and included into the response together with detailed register data	
ServProv-SEC	ServProv-CU	the ack/resp. message is encrypted and signed	
ServProv-CU	Suppl-CU	the response is sent back to the supplicant	
Suppl-CU	Suppl-SEC	response msg received and forwarded to security component	

Suppl-SEC	Suppl-SEC	perform security functions (decryption, authentication, non-repudation, message plausibility checks))
Suppl-SEC	Suppl-SEC	unpriviledged enrolment credential is installed for use of suceeding UC
Suppl-SEC	Suppl-Enter	The issuer of the registration request gets the result



2.20.4 Actions Post-Operational

From	To	Description	Optional
PostCond-1.1		Supplicant is now unpriviledged (Note1) part of the Car2X systems network	



2.20.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
Register	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 services/information. This can be inside the C2X-SN itself and/or 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	
ServProv-CU	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.		x	
ServProv-DIS	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.		x	
ServProv-SEC	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.		x	
Suppl-CU	Physical/logical entity that handles communication. The CH is responsible for all outgoing communication and is the counterpart for the IEA. It		x	

	also handles Security and QoS.			
Suppl-Enter	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.		x	
Suppl-SEC	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.		x	

2.20.6 Decision Points Identified

ID	Component	Description

2.20.7 External Activities Identified

ID	Group	Description

2.21 UC-C2X-101_02 Accreditation

Car2X Systems Network offers an accreditation for Service Providers, IVSs and Communication Network Providers. (Note 1)

2.21.1 Assumptions

ID	Description
US-Enter-A2.1	
US-Enter-A2.2	

2.21.2 Actions Pre-Operational

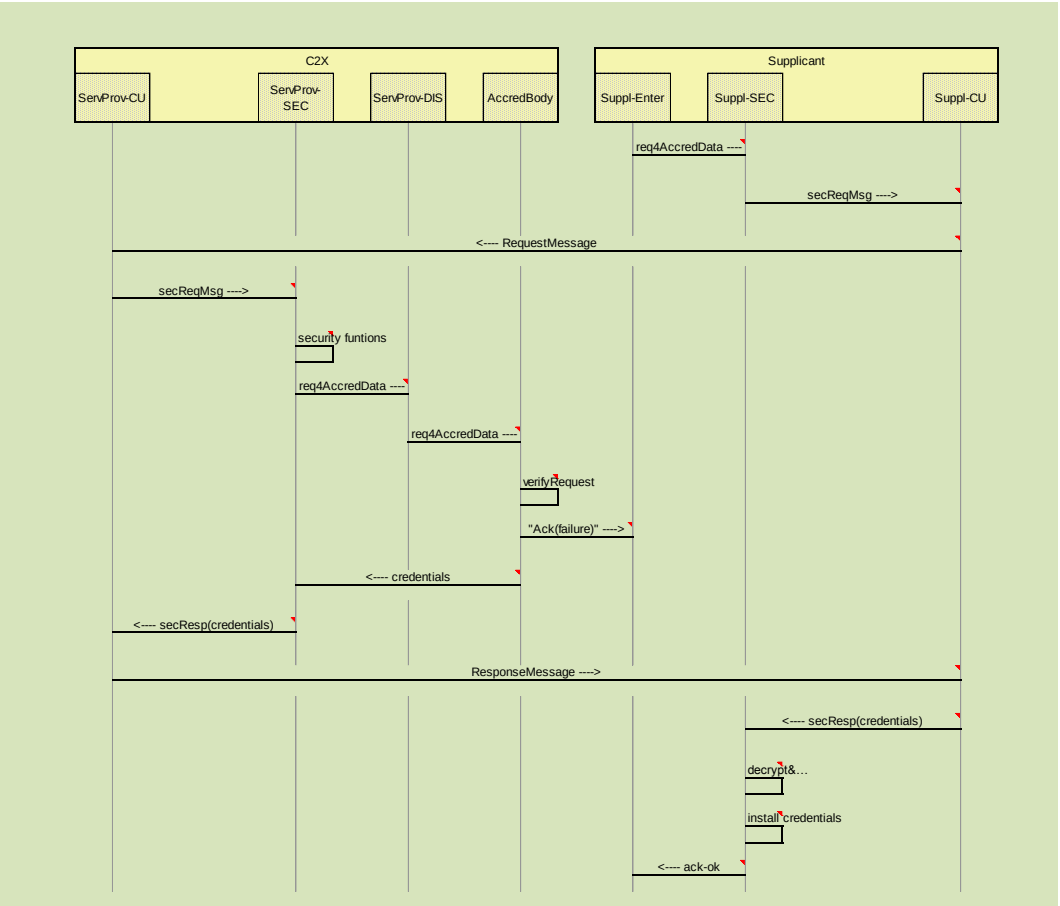
From	To	Description	Optional
Prereq-PreOp-2.1		e.g. published on the WEB (same as in UC Registration)	
Prereq-PreOp-2.2		Communication means towards Service Provision exists (as in UC Registration)	
Prereq-PreOp-2.3		The supplicant is successfully registered in the Car2X Systems network	

Prereq-PreOp-2.4	A registered supplicant wants to join the Car2X integrated system and starts the accreditation process

2.21.3 Actions Operational

From	To	Description	Optional
Description-2.1		The supplicant sends an encrypted accreditation request to service provision. Service provision performs security checks, including a check of trustworthiness of the supplicant. The request is forwarded to accreditation body. The accreditation body verifies the request according to its rules and regulations and creates a privileged enrolement credential for the succeeding UC "authentication". A response is sent back to the supplicant, who installs the received credential.	
Prereq-Op-2.1		All rules and regulations required for participating in the Car2X Systems Network are defined, documented and available (=REQ-C2X-007).	
Prereq-Op-1.2		The public key for encrypting messages towards enter access is known to the supplicant.	
Prereq-Op-1.2		unpriviliged enrolmnet certificate from preceding UC "registration" is available	
Suppl-Enter	Suppl-SEC	the "EnterC2X facility" creates data for an accreditation request	
Suppl-SEC	Suppl-CU	encrypted, certificate added, signed	
Suppl-CU	ServProv-CU	The encrypted registration request message is sent to service provision	
ServProv-CU	ServProv-SEC	The encryped and signed data are forwarded to the security component	
ServProv-SEC	ServProv-SEC	perform, decryption, authentication, non-repudation, trustworthiness of supplicant	
ServProv-SEC	ServProv-DIS	the accreditation request data are given to a distribution function	
ServProv-DIS	AccredBody	the supplicant's accreditation request data are forwarded to the registration body	
AccredBody	AccredBody	verify the request according to its rules and regulations.	
AccredBody	Suppl-Enter	in case the verification failed. The complete backwards is	

		not shown.
AccredBody	ServProv-SEC	enrolement credential created and included into the response
ServProv-SEC	ServProv-CU	the ack/resp. message is encrypted and signed
ServProv-CU	Suppl-CU	the response is sent back to the supplicant
Suppl-CU	Suppl-SEC	response msg received and forwarded to security component
Suppl-SEC	Suppl-SEC	perform security functions (decryption, authentication, non-repudation, message plausibility checks))
Suppl-SEC	Suppl-SEC	priviledged enrolment credential is installed for use in succeeding UC
Suppl-SEC	Suppl-Enter	The issuer of the accreditation request gets ok



2.21.4 Actions Post-Operational

From	To	Description	Optional

PostCond-2.1	Supplicant is now priviledged (Note1) part of the Car2X systems network

2.21.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
AccredBody	The (human) body that is responsible for 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.		x	
ServProv-CU	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.		x	
ServProv-DIS	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.		x	
ServProv-SEC	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.		x	
Suppl-CU	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.		x	
Suppl-Enter	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.		x	
Suppl-SEC	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.		x	

2.21.6 Decision Points Identified

ID	Component	Description

2.21.7 External Activities Identified

ID	Group	Description

2.22 UC-C2X-101_03_01 Authentication of accredidated participant

Car2X Systems Network offers an authentication for Service Providers, IVSs and Communication Network Providers.. (Note 1)

2.22.1 Assumptions

ID	Description
US-Enter-A3.1	Supplicant is already authenticated by the "priviled enrolement certificate" created in preceding UC "accreditation".
US-Enter-A2.2	Supplicant need authentication ticket(s) to participate in the Car2X systems network.

2.22.2 Actions Pre-Operational

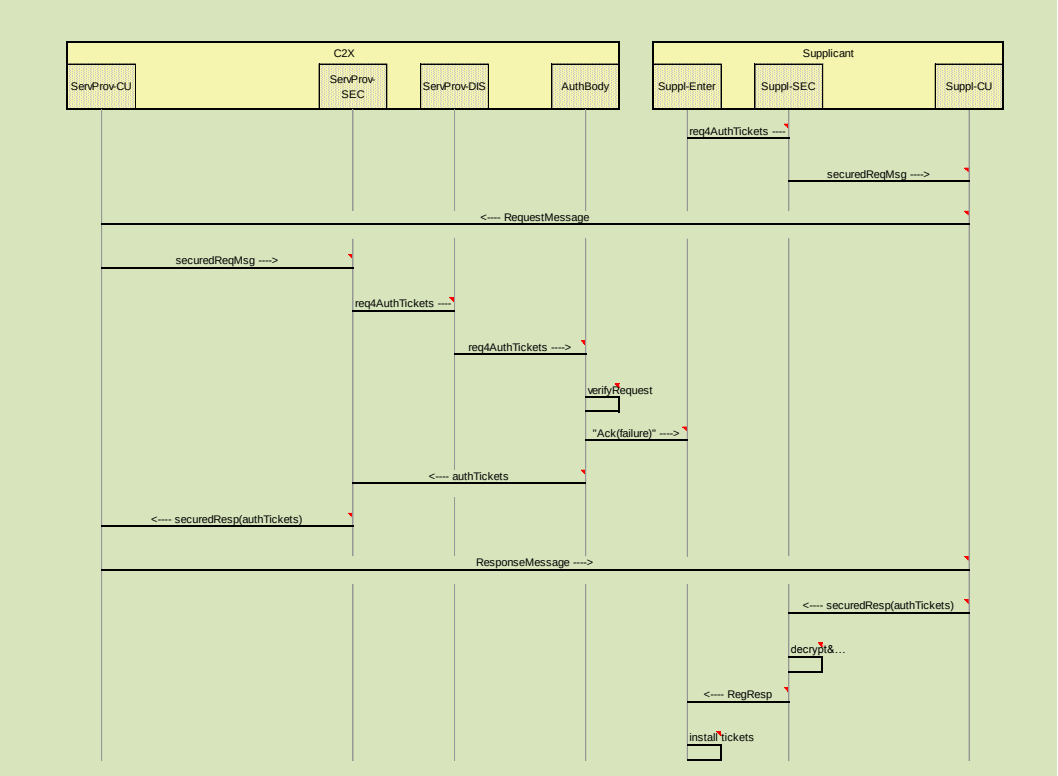
From	To	Description	Optional
Prereq-PreOp-3.1		e.g. published on the WEB	
Prereq-PreOp-3.2		Communication means towards Service Provision exists	
Prereq-PreOp-3.3		The supplicant is accredidated user of the Car2X Systems network and has an certificate (e.g. a LTC)	
Prereq-PreOp-3.4		trigger to complete the user story "entering the Car2X systems network"	

2.22.3 Actions Operational

From	To	Description	Optional

Description-3.1		The supplicant sends an encrypted accreditation request to service provision. Service provision performs security checks, including a check of trustworthiness of the supplicant. The request is forwarded to autehntication body. The accreditation body verifies the request according to its rules and regulations. Authentication tickets are created. A response is sent back to the supplicant, who installs the received credential.
Prereq-Op-3.1		All rules and regulations required for participating in the Car2X Systems Network are defined, documented and available (=REQ-C2X-007).
Prereq-Op-3.2		The public key for encrypting messages towards enter access is known to the supplicant.
Prereq-Op-3.3		The supplicant has "priviledged enrolment certiciate"availabale. (see preceding UC "accreditation")
Suppl-Enter	Suppl-SEC	the "EnterC2X facility" requests authentication tickets
Suppl-SEC	Suppl-CU	encrypted, priviledged enrolement certicate added, signed
Suppl-CU	ServProv-CU	The encrypted registration request message is sent to service provision
ServProv-CU	ServProv-SEC	The encryped and signed data are forwarded to the security component
ServProv-SEC	ServProv-DIS	decryption, authentication, non-repudation, trustworthiness of supplicant
ServProv-DIS	AuthBody	the supplicant's authentication request data are forwarded to the authentication body
AuthBody	AuthBody	verify the request according to its rules and regulations.
AuthBody	Suppl-Enter	in case the verification failed. The complete backwards path is not shown.
AuthBody	ServProv-SEC	authentication tickets created and included into the response
ServProv-SEC	ServProv-CU	the ack/resp. message is encrypted and signed
ServProv-CU	Suppl-CU	the response is sent back to the supplicant
Suppl-CU	Suppl-SEC	response msg received and forwarded to security component
Suppl-SEC	Suppl-SEC	perform security functions (decryption, authentication, non-repudation, message plausibility checks))

Suppl-SEC	Suppl-Enter	The "EnterC2X facitlity" gets the requested authentication tickets.
Suppl-Enter	Suppl-Enter	Authentication tickets available for communication



2.22.4 Actions Post-Operational

From	To	Description	Optional
PostCond-3.1		Supplicant is now user/member of the Car2X systems network	

2.22.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
AuthBody	The (human) body that is responsible for 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.		x	

ServProv-CU	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.		x	
ServProv-DIS	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.		x	
ServProv-SEC	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.		x	
Suppl-CU	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.		x	
Suppl-Enter	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.		x	
Suppl-SEC	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.		x	

2.22.6 Decision Points Identified

ID	Component	Description

2.22.7 External Activities Identified

ID	Group	Description

2.23 UC-C2X-101_03_02 Authentication of a new service

An already authorised supplicant (SP, TTC, OEM, IVS) wants to offer/use a new coopertive service. Therefore he requests for additional authentication ticket(s), which include the entitlement of the new service (see Note 1)

2.23.1 Assumptions

ID	Description
US-Enter-A3.1	User has already one or more authentication tickets for his services
US-Enter-A2.2	User need additional authentication ticket(s) for the new service.

2.23.2 Actions Pre-Operational

From	To	Description	Optional
Prereq-PreOp-3.1		Supplicant has already entered the C2X systems network	
Prereq-PreOp-3.2		Communication means towards Service Provision exists	
Prereq-PreOp-3.4		trigger to request additional authentication tickets for a new service	

2.23.3 Actions Operational

From	To	Description	Optional

2.23.4 Actions Post-Operational

From	To	Description	Optional
PostCond		Supplicant has a new authorisation ticket for new service	

2.23.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.23.6 Decision Points Identified

ID	Component	Description

2.23.7 External Activities Identified

ID	Group	Description

2.24 UC-C2X-101-04

Car2X Systems Network offers an advertisement service that enables (a) Service Provider and Communication Network Provider to advertise the services they offer (b) Service Provider and Mobile Nodes to lookup discover services offered within the C2X integrated systemC2X Systems Network.

2.24.1 Assumptions

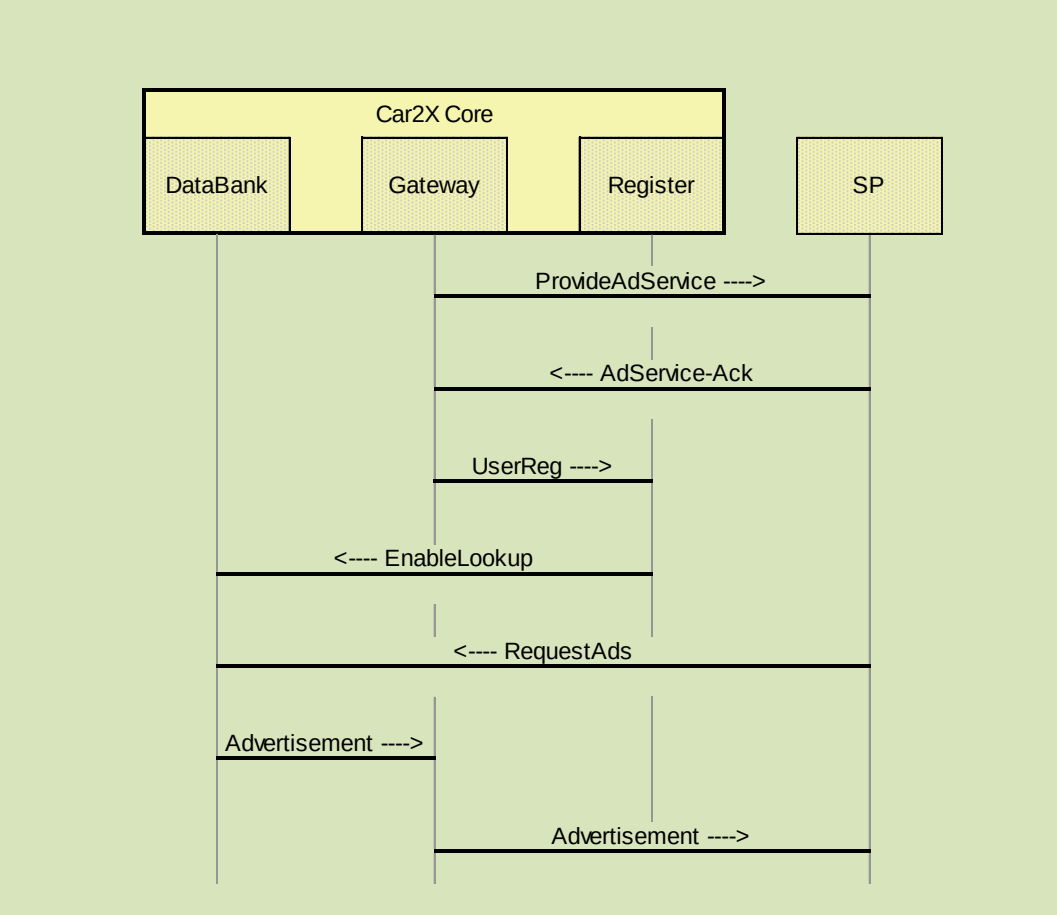
ID	Description

2.24.2 Actions Pre-Operational

From	To	Description	Optional

2.24.3 Actions Operational

From	To	Description	Optional
Gateway	SP		
SP	Gateway		
Gateway	Register		
Register	DataBank		
SP	DataBank		
DataBank	Gateway		
Gateway	SP		



2.24.4 Actions Post-Operational

From	To	Description	Optional

2.24.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

DataBank	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 services/information. This can be inside the C2X-SN itself and/or 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	
Gateway	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.		x	
Register	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 services/information. This can be inside the C2X-SN itself and/or 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	
SP	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.		x	

2.24.6 Decision Points Identified

ID	Component	Description

2.24.7 External Activities Identified

ID	Group	Description

2.25 UC-C2X-102_02

"An IVS respectively IRS is able to download the software for a (new) application.

An IVS/IRS checks for a new sw version and downloads the installation package.

Note: At least an interface is available which supports, if required, the download of application software by the (new) user of a serviceIf pseudonymous download is not allowed, privacy profile REQ-SEC-PP-006 would be required (might depend on the actual software).Only participants in a role with an appropriate authorization should be able to download the software.

Note: it is presumed, that SW update processes both at IVS/IRS and service provider are vendor specific and are to be defined by OEM/service provider. Only the procedures to check for and provide the appropriate sw packages from SP to IVS/IRS are defined here.
"

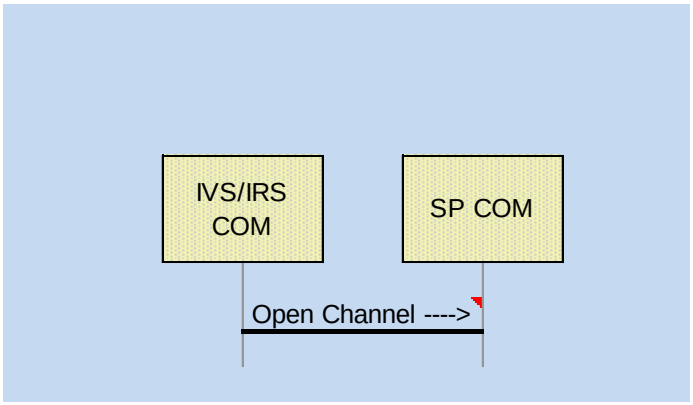
2.25.1 Assumptions

ID	Description
SW-Mgmt-AS01	IVS/IRS positively registered to SP (either self-registration or by OEM during manufacturing) for the associated service, in order to be eligible to receive SW update
SW-Mgmt-AS02	appropriate (i.e. compatible) SW object is stored at SP and has been tested to be working for specific type of service and specific IVS/IRS
SW-Mgmt-AS03	a mechanism exists inside IVS/IRS to perform all necessary steps to install new/updated SW onto itself
REQ-SEC-PP-003	The C2X-SN provides a way to obtain an "authorized pseudonym" as described in REQ-SEC-PP-003 and the IVS/IRS has been allocated with such an identity.
REQ-SEC-PS-007	all messages between IVS/IRS contain a signature and are encrypted
REQ-SEC-PA-002	not applicable

2.25.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		IVS/IRS has positively registered itself to SP for the associated service, in order to be eligible to receive SW update	
Prerequisite-2		the SW management process has been started at SP and is available	

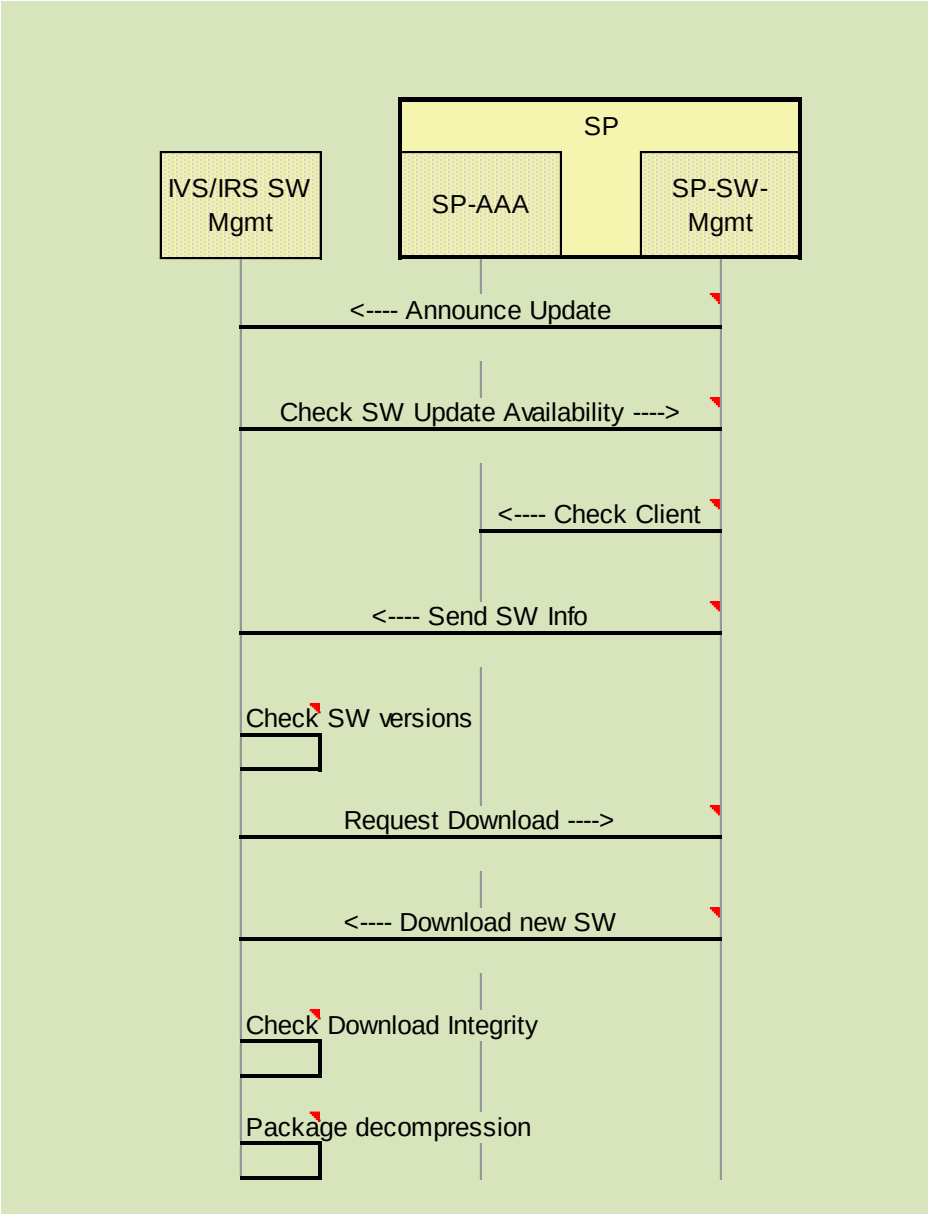
Prerequisite-3		a new/updated SW object is available at SP for download to IVS/IRS
Prerequisite-4		compatibility of new SW version towards specific IVS/IRS type and service has been tested
Prerequisite-5		IVS/IRS has been initialised and has performed self-test
Prerequisite-6		the COM module of IVS/IRS is able to establish an appropriate channel towards SP according to required QoS, either via IST-G5 or mobile communications
Prerequisite-7		internal logging - including all sw management procedures inside IVS/IRS - has been started
IVS/IRS COM	SP COM	establish a safe communication channel between IVS/IRS and SP according to required QoS, this channel is to be used (by both SW-Mgmt. handlers of IVS/IRS and SP) for sw version check and possible sw download



2.25.3 Actions Operational

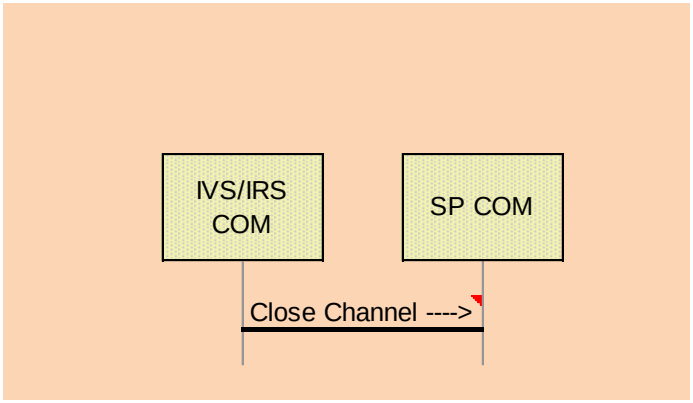
From	To	Description	Optional
SP-SW-Mgmt	IVS/IRS SW Mgmt	Optional: SP announces availability of new SW package	yes
IVS/IRS SW Mgmt	SP-SW-Mgmt	Request SP for actual SW version information for desired service [Identity(AuthPseud), ServiceId, ClientHwId, ClientSwVersion]	
SP-SW-Mgmt	SP-AAA	SP provider check eligibility of IVS/IRS to receive SW updates for requested service	
SP-SW-Mgmt	IVS/IRS SW Mgmt	SP provides information about actual SW versions and download packages for desired service [ServiceId, SwVersion, DownloadData(e.g. package size, download URL, compression info, encryption info, checksum, …)]	

IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. Handler compares client sw version with received info from SP and decides about update
IVS/IRS Mgmt	SW	SP-SW-Mgmt		IVS/IRS SW Mgmt. Handler requests download of swyes package from SP [URL] (optional: only if update is required)
SP-SW-Mgmt		IVS/IRS Mgmt	SW	SP sends SW package to IVS/IRS (optional: only if update is required)
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. Handler checks integrity of download package e.g. via checksum (optional: only if update is required)
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. Handler decompresses & decrypts downloaded installation package (if necessary)



2.25.4 Actions Post-Operational

From	To	Description	Optional
IVS/IRS COM	SP COM	Close prevoiously opened communication channel	



2.25.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS/IRS COM	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.	x		x
IVS/IRS SW Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.		x	
SP COM	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.	x		x
SP-AAA	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.		x	
SP-SW-Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.		x	

2.25.6 Decision Points Identified

ID	Component	Description
DP-01	Announce Update	Decide if announcement of new SW version by SP is needed or if pull-only mechanism by IVS/IRS is preferred

2.25.7 External Activities Identified

ID	Group	Description
US-01	IVS/IRS	Open Channel: use case to open a generic transport channel between IVS/IRS and SP
US-02	IVS/IRS	Registration of IVS/IRS for service
US-03	SP	SW management process at service provider including storage of new sw objects at SP and compatibility testing
US-04	IVS/IRS	cold start / initialisation of IVS/IRS components
US-05	IVS/IRS	IVS/IRS logging procedures
US-06	IVS/IRS	Close Channel: use case to open a generic transport channel between IVS/IRS and SP
US-07	SP	Check authorisation of client to obtain new sw, check signatures, identities, subscribed services, …

2.26 UC-C2X-102_03

"Installation of a new application / service on an IVS or IRS.

Note: No communication, hence only generic security requirements apply.

Note: it is presumed, that SW update processes both at IVS/IRS and service provider are vendor specific and are to be defined by OEM/service provider. Only the procedures to check for and provide the appropriate sw packages from SP to IVS/IRS are defined here.

Note: It might be neccessary/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)"

2.26.1 Assumptions

ID	Description
SW-Mgmt-AS01	a mechanism exists inside IVS/IRS to perform all necessary steps to install new/updated SW onto itself and to initialise new SW accordingly
SW-Mgmt-AS02	a mechanism exists inside IVS/IRS to create a backup of an existing sw installation for the purpose of emergency fall-back in case of sw installation

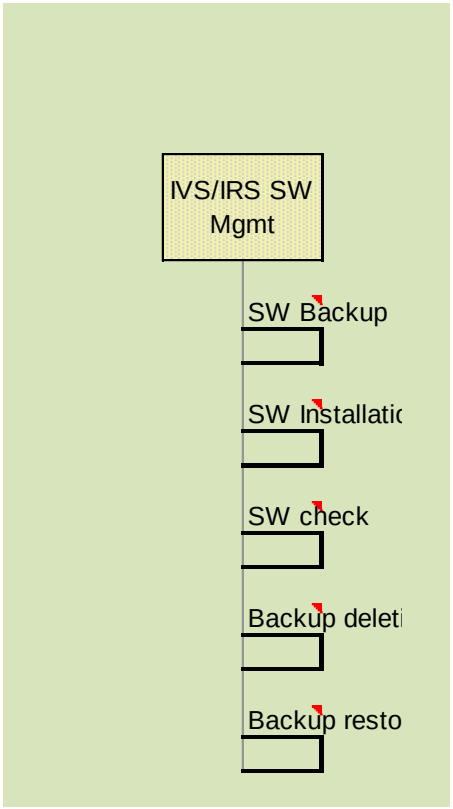
	failure

2.26.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		IVS/IRS has successfully downloaded new sw package as in UC-C2X-102_02	
Prerequisite-2		new sw package has been decompressed/unzipped successfully after download and is ready to be installed	
Prerequisite-3		compatibility of new SW version towards specific IVS/IRS type and service has been tested	
Prerequisite-4		internal logging - including all sw management procedures inside IVS/IRS - has been started	

2.26.3 Actions Operational

From	To	Description	Optional
IVS/IRS SW Mgmt	IVS/IRS SW Mgmt	IVS/IRS SW Mgmt. handler creates back-up of existing sw version for emergency fall-back	
IVS/IRS SW Mgmt	IVS/IRS SW Mgmt	IVS/IRS SW Mgmt. Handler triggers internal sw update procedure	
IVS/IRS SW Mgmt	IVS/IRS SW Mgmt	IVS/IRS SW Mgmt. Handler checks integrity of installation (e.g. via checksums friom file system)	
IVS/IRS SW Mgmt	IVS/IRS SW Mgmt	if "SW check" successfull: IVS/IRS SW Mgmt. Handleryes deletes previously created backup of outdated sw version	
IVS/IRS SW Mgmt	IVS/IRS SW Mgmt	if "SW check" fails: IVS/IRS SW Mgmt. Handler restoresyes previously created backup of outdated sw version and disables/deletes downloaded package	



2.26.4 Actions Post-Operational

From	To	Description	Optional

2.26.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS/IRS SW Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.		x	

2.26.6 Decision Points Identified

ID	Component	Description
DP-01	SW Backup	Is a backup of previously installed (older/working) sw version necessary before installation of new sw? What happens if sw install fails?

DP-02	It might be neccessary/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)

2.26.7 External Activities Identified

ID	Group	Description

2.27 UC-C2X-102_04

"Activation of the installed software.

Note: it is presumed, that SW update processes both at IVS/IRS and service provider are vendor specific and are to be defined by OEM/service provider. Only the procedures to check for and provide the appropriate sw packages from SP to IVS/IRS are defined here.
"

2.27.1 Assumptions

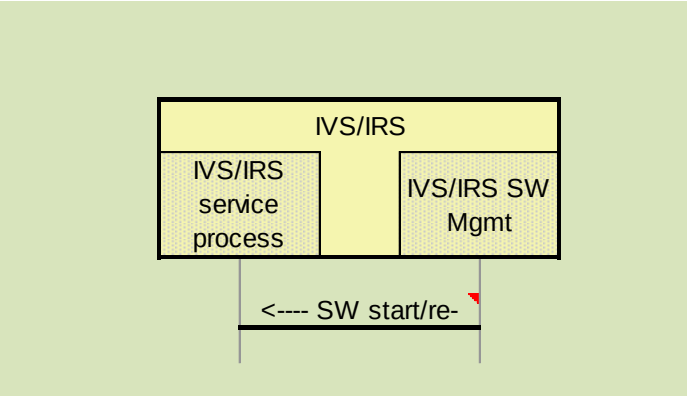
ID	Description
SW-Mgmt-AS03a	mechanism exists inside IVS/IRS to perform all necessary steps to initialise new/updated sw version

2.27.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		IVS/IRS has successfully downloaded new sw package as in UC-C2X-102_02	
Prerequisite-2		IVS/IRS has successfully installed new sw package as in UC-C2X-102_03	
Prerequisite-3		compatibility of new SW version towards specific IVS/IRS type and service has been tested	
Prerequisite-4		internal logging - including all sw management procedures inside IVS/IRS - has been started	

2.27.3 Actions Operational

From	To	Description	Optional
IVS/IRS SW Mgmt	IVS/IRS service process	IVS/IRS SW Mgmt. Handler (re-)starts newly installed sw	



2.27.4 Actions Post-Operational

From	To	Description	Optional

2.27.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS/IRS service process	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.		x	
IVS/IRS SW Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.		x	

2.27.6 Decision Points Identified

ID	Component	Description
DP-01	SW start/re-start	Sind besondere Maßnahmen notwendig vor der Aktivierung der neuen SW? (z.B. nur in Werkstatt erlaubt, Triggerung nur manuell, …)

2.27.7 External Activities Identified

ID	Group	Description

US-01	IVS/IRS	IVS/IRS sw package download
US-02	IVS/IRS	IVS/IRS sw package install
US-03	IVS/IRS	IVS/IRS logging procedures
US-04	SP	SW management process at service provider including storage of new sw objects at SP and compatibility testing
US-05	IVS/IRS	sw initialisation process (IVS/IRS vendor specific)

2.28 UC-C2X-102_07

"Software belonging to an application or service running on an IVS or IRS is completely removed.

Note: No communication, hence only generic security requirements apply.

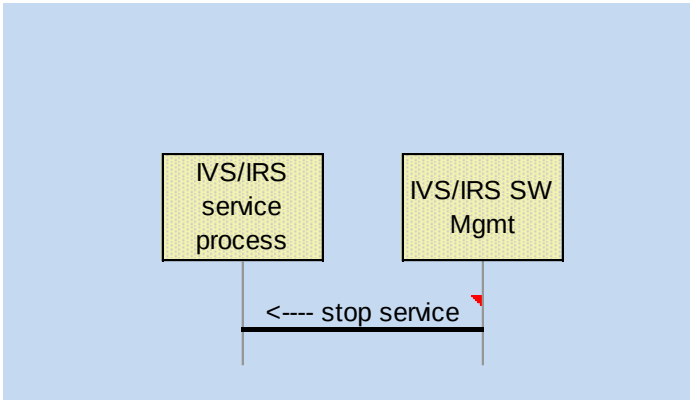
Note: it is presumed, that SW update processes both at IVS/IRS and service provider are vendor specific and are to be defined by OEM/service provider. Only the procedures to check for and provide the appropriate sw packages from SP to IVS/IRS are defined here.
"

2.28.1 Assumptions

ID	Description
SW-Mgmt-AS01a	mechanism exists inside IVS/IRS to perform all necessary steps to uninstall outdated sw

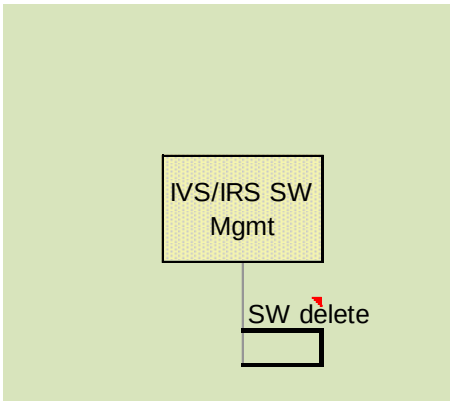
2.28.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		IVS/IRS has successfully de-registered from service atyes SP	
Prerequisite-2		internal logging - including all sw management procedures inside IVS/IRS - has been started	
Prerequisite-3		the COM module of IVS/IRS is able to establish an appropriate channel towards SP according to required QoS, either via IST-G5 or mobile communications	
IVS/IRS Mgmt	SW process	IVS/IRS servicesignal to internal process handler to stop service	



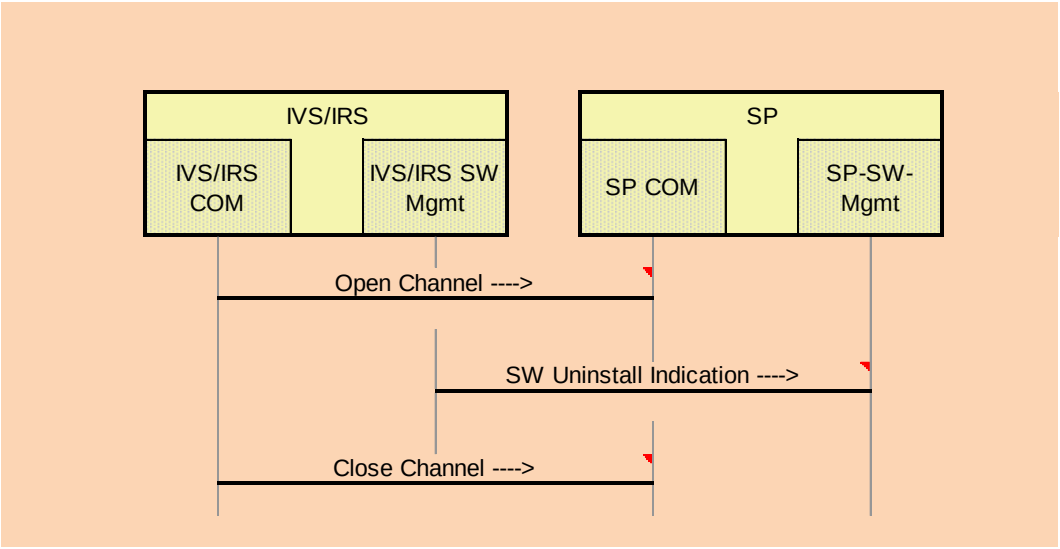
2.28.3 Actions Operational

From	To	Description	Optional
IVS/IRS SW Mgmt	IVS/IRS SW Mgmt	IVS/IRS SW Mgmt. handler deletes sw package	



2.28.4 Actions Post-Operational

From	To	Description	Optional
IVS/IRS COM	SP COM	establish a safe communication channel between IVS/IRS and SP according to required QoS, this channel is to be used (by both SW-Mgmt. handlers of IVS/IRS and SP) for sw version check and possible sw download	
IVS/IRS SW Mgmt	SP-SW-Mgmt	Indicate to SP that sw has been uninstalled andyes deactivated for desired service [Identity, ServiceId, ClientHwId, ClientSwVersion]	
IVS/IRS COM	SP COM	Close prevoiously opened communication channel	



2.28.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS/IRS COM	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.			x
IVS/IRS service process	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.	x		
IVS/IRS SW Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.	x	x	x
SP COM	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.			x
SP-SW-Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.			x

2.28.6 Decision Points Identified

ID	Component	Description
DP-01	SW Uninstall Indication	Is it neccessary to inform SP about sw uninstallation at IVS/IRS?

2.28.7 External Activities Identified

ID	Group	Description
US-01	IVS/IRS	IVS/IRS component uninstall sw procedure (vendor specific)
US-02	IVS/IRS	service de-registration
US-03	IVS/IRS	IVS/IRS logging procedures
US-04	IVS/IRS	Open Channel: use case to open a generic transport channel between IVS/IRS and SP
US-05	IVS/IRS	Close Channel: use case to open a generic transport channel between IVS/IRS and SP

2.29 UC-C2X-101-04

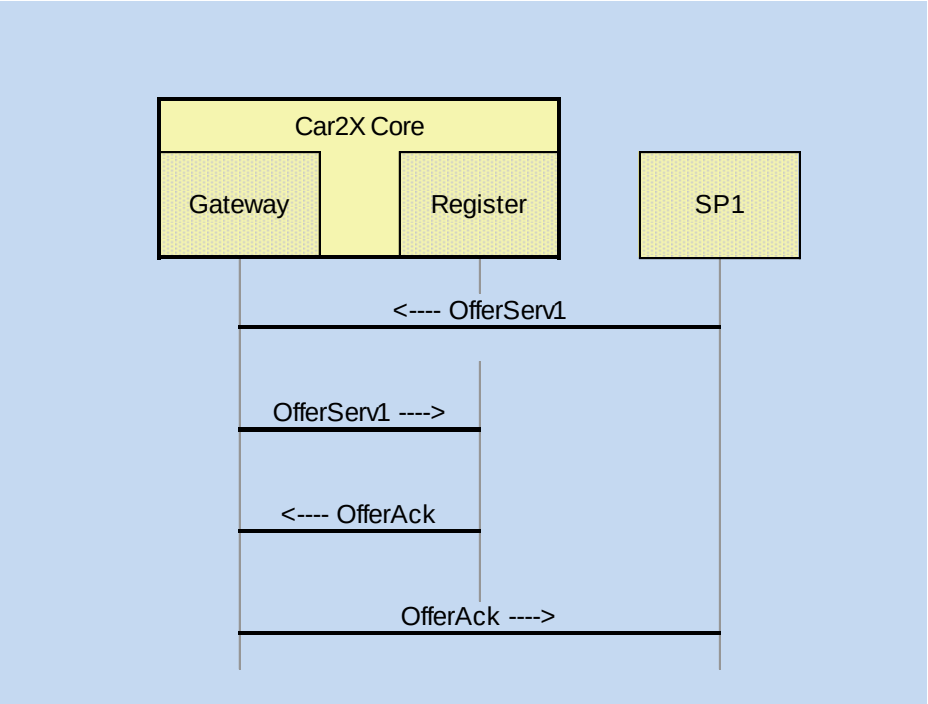
Car2X Systems Network offers an advertisement service that enables (a) Service Provider and Communication Network Provider to advertise the services they offer (b) Service Provider and Mobile Nodes to lookup discover services offered within the C2X integrated systemC2X Systems Network.

2.29.1 Assumptions

ID	Description

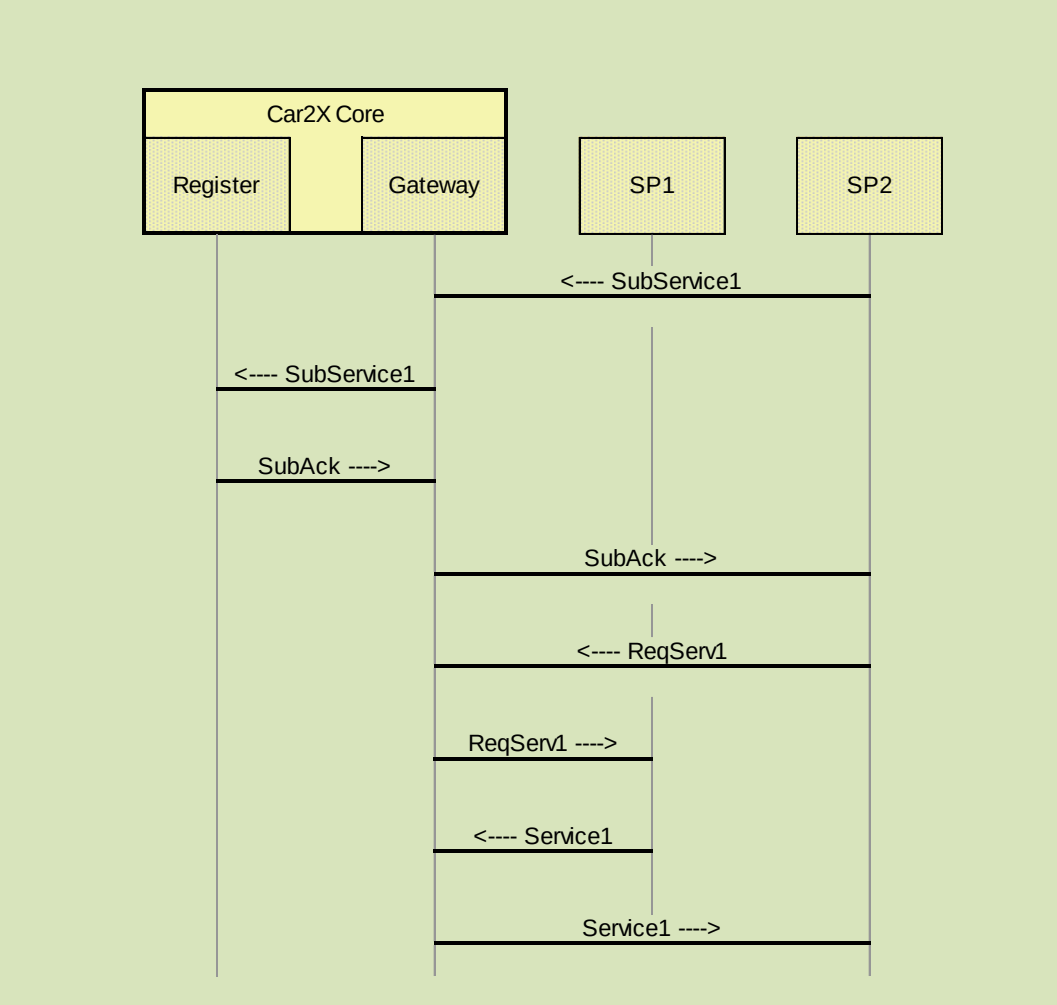
2.29.2 Actions Pre-Operational

From	To	Description	Optional
SP1	Gateway		
Gateway	Register		
Register	Gateway		
Gateway	SP1		



2.29.3 Actions Operational

From	To	Description	Optional
SP2	Gateway		
Gateway	Register		
Register	Gateway		
Gateway	SP2		
SP2	Gateway		
Gateway	SP1		
SP1	Gateway		
Gateway	SP2		



2.29.4 Actions Post-Operational

From	To	Description	Optional

2.29.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
Gateway	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.	x	x	

Register	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 services/information. This can be inside the C2X-SN itself and/or 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	
SP1	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.	x	x	
SP2	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.		x	

2.29.6 Decision Points Identified

ID	Component	Description

2.29.7 External Activities Identified

ID	Group	Description

2.30 UC-C2X-101-04

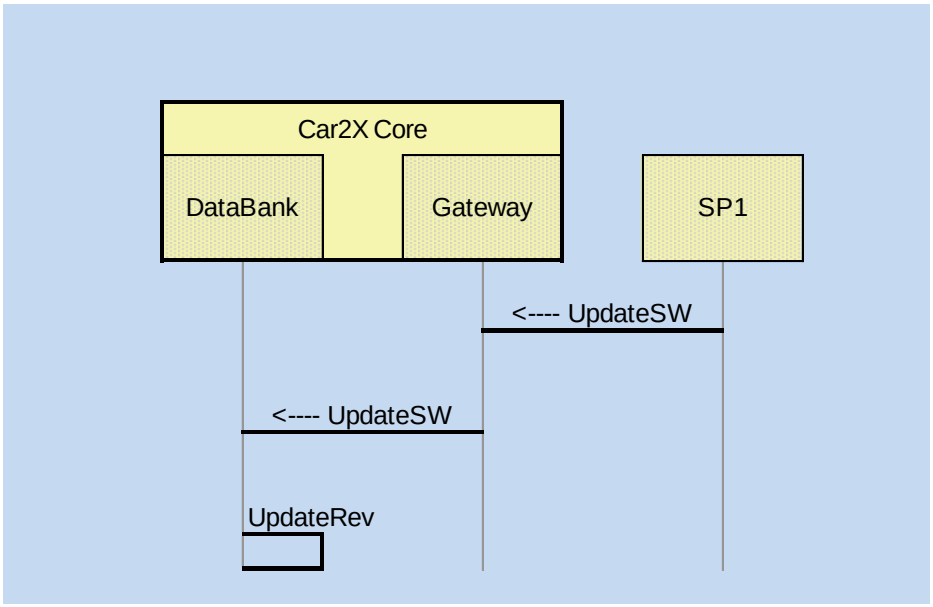
Car2X Systems Network offers an advertisement service that enables (a) Service Provider and Communication Network Provider to advertise the services they offer (b) Service Provider and Mobile Nodes to lookup discover services offered within the C2X integrated systemC2X Systems Network.

2.30.1 Assumptions

ID	Description

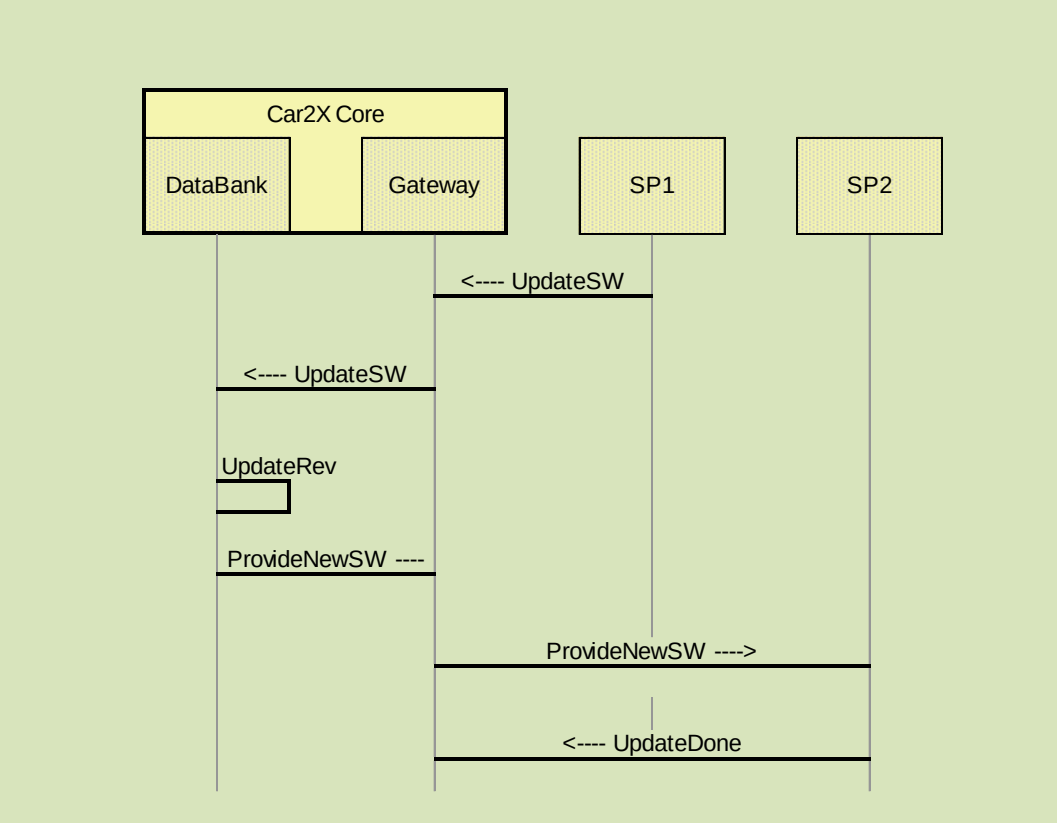
2.30.2 Actions Pre-Operational

From	To	Description	Optional



2.30.3 Actions Operational

From	To	Description	Optional
SP1	Gateway		
Gateway	DataBank		
DataBank	DataBank		
DataBank	Gateway		
Gateway	SP2		
SP2	Gateway		



2.30.4 Actions Post-Operational

From	To	Description	Optional

2.30.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
DataBank	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 services/information. This can be inside the C2X-SN itself and/or 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	

Gateway	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.	x	x	
SP1	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.	x	x	
SP2	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.		x	

2.30.6 Decision Points Identified

ID	Component	Description

2.30.7 External Activities Identified

ID	Group	Description

2.31 UC-C2X-101-04

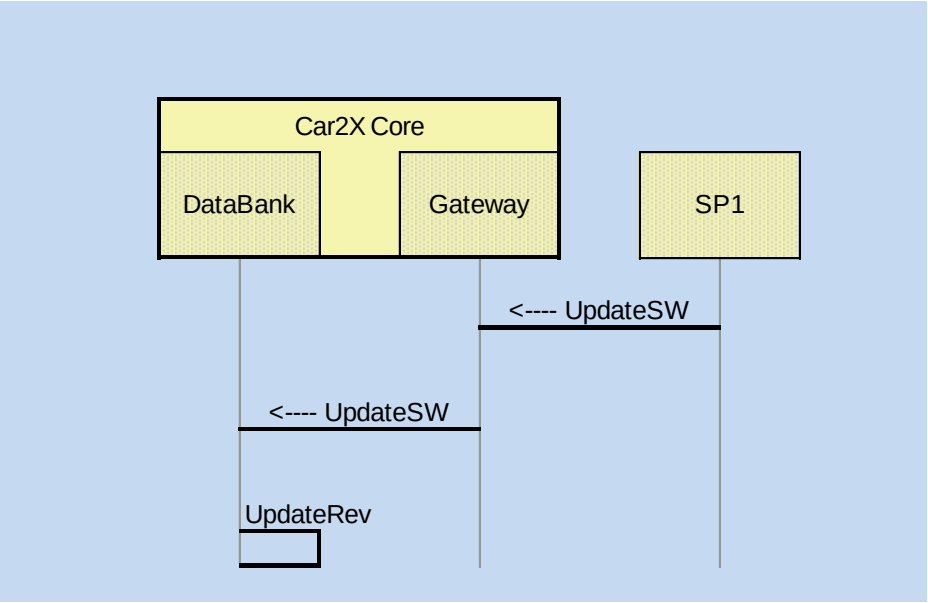
Car2X Systems Network offers an advertisement service that enables (a) Service Provider and Communication Network Provider to advertise the services they offer (b) Service Provider and Mobile Nodes to lookup discover services offered within the C2X integrated systemC2X Systems Network.

2.31.1 Assumptions

ID	Description

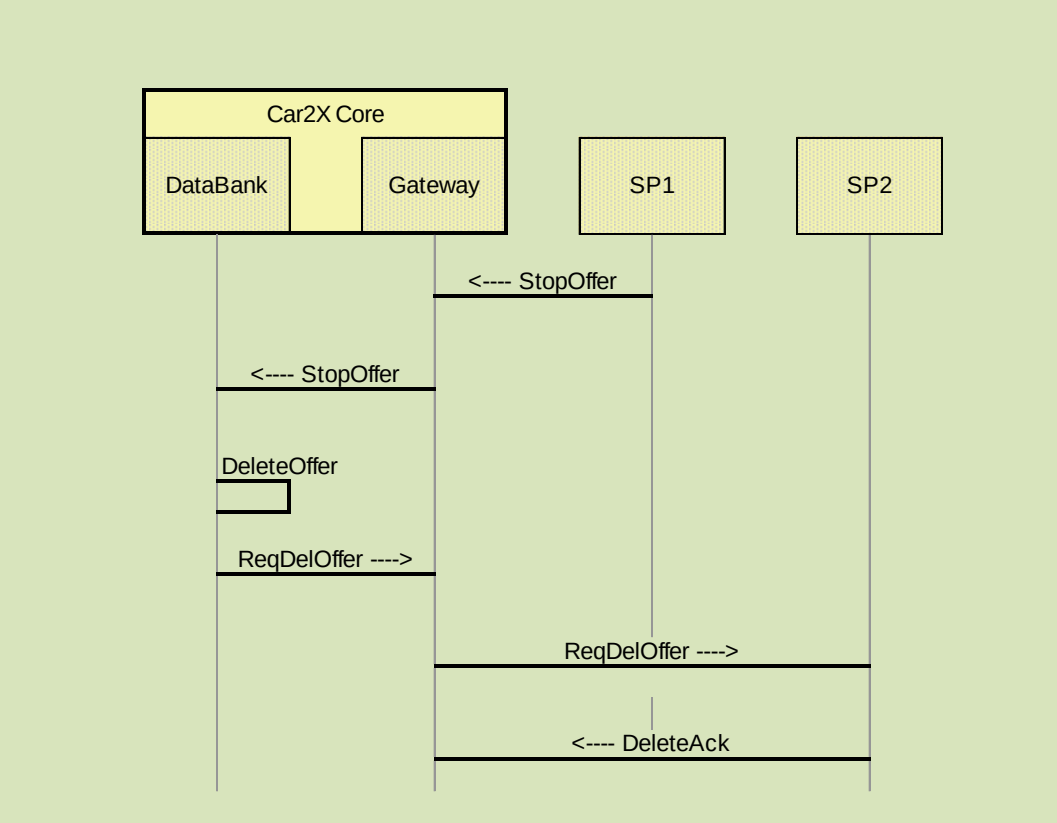
2.31.2 Actions Pre-Operational

From	To	Description	Optional



2.31.3 Actions Operational

From	To	Description	Optional
SP1	Gateway		
Gateway	DataBank		
DataBank	DataBank		
DataBank	Gateway		
Gateway	SP2		
SP2	Gateway		



2.31.4 Actions Post-Operational

From	To	Description	Optional

2.31.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
DataBank	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 services/information. This can be inside the C2X-SN itself and/or 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	

Gateway	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.	x	x	
SP1	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.	x	x	
SP2	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.		x	

2.31.6 Decision Points Identified

ID	Component	Description

2.31.7 External Activities Identified

ID	Group	Description

2.32 UC-C2X-101-04

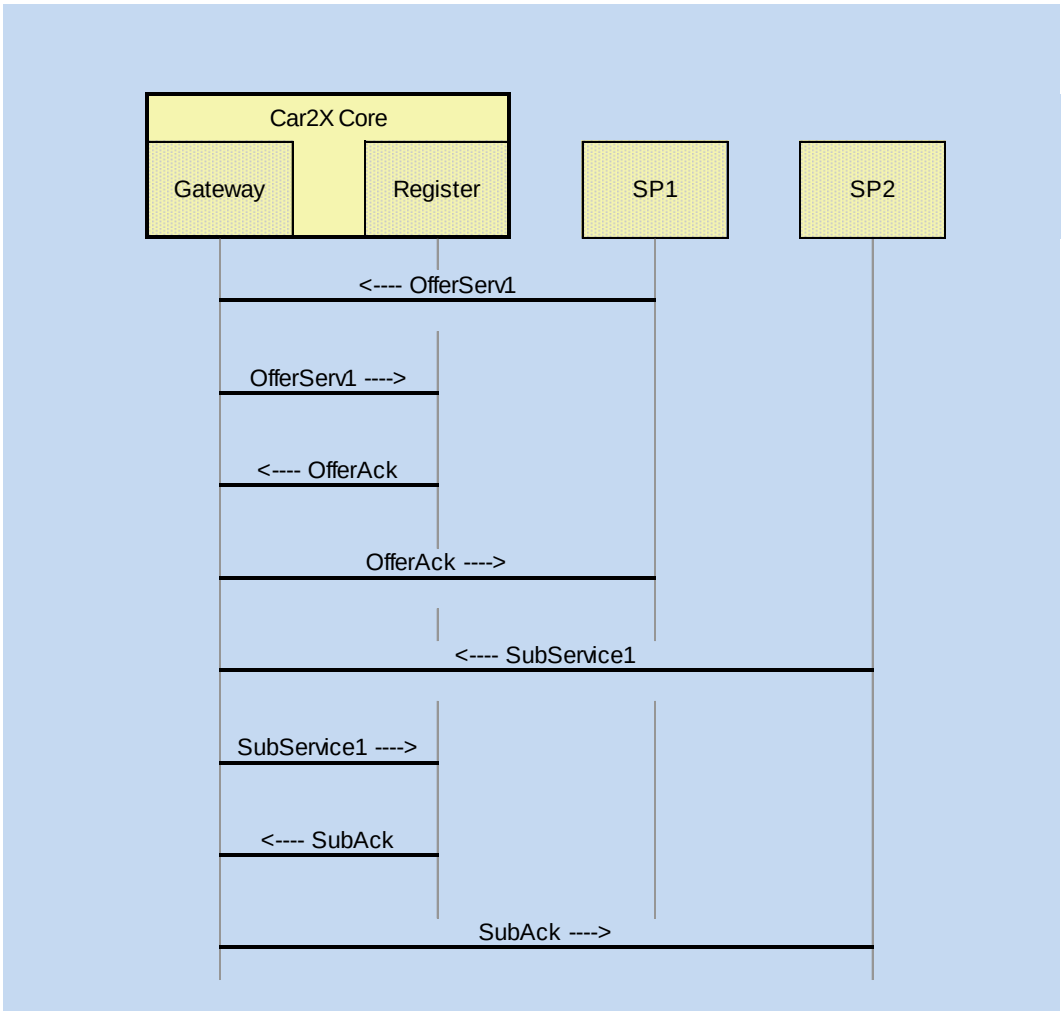
Car2X Systems Network offers an advertisement service that enables (a) Service Provider and Communication Network Provider to advertise the services they offer (b) Service Provider and Mobile Nodes to lookup discover services offered within the C2X integrated systemC2X Systems Network.

2.32.1 Assumptions

ID	Description

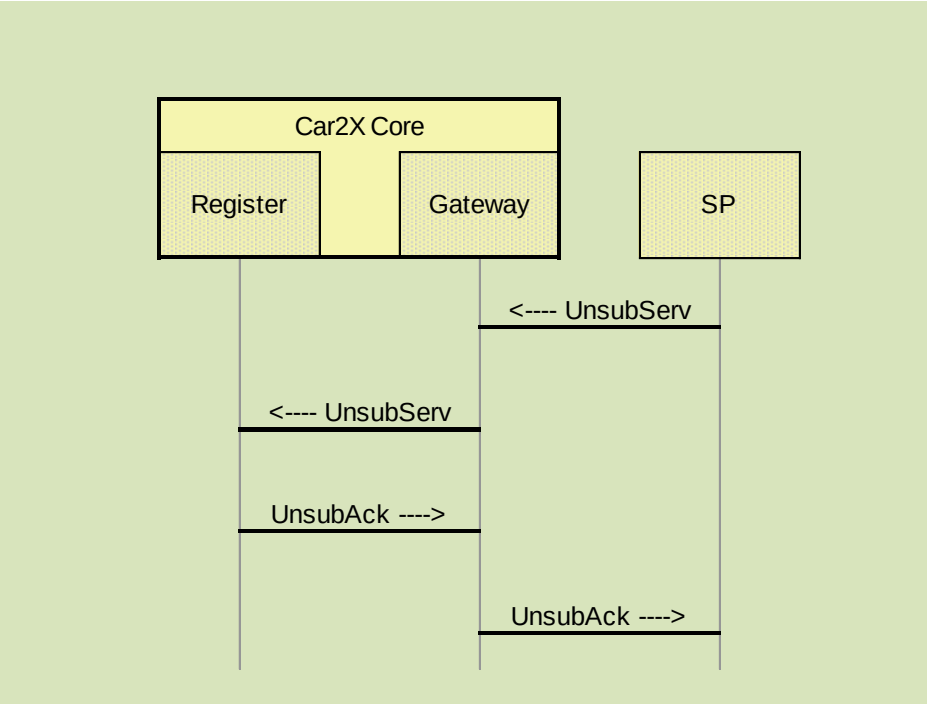
2.32.2 Actions Pre-Operational

From	To	Description	Optional



2.32.3 Actions Operational

From	To	Description	Optional
SP	Gateway		
Gateway	Register		
Register	Gateway		
Gateway	SP		



2.32.4 Actions Post-Operational

From	To	Description	Optional

2.32.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
Gateway	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.	x	x	
Register	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 services/information. This can be inside the C2X-SN itself and/or 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	x	x	

	C2X-SN			
SP	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.	x	x	

2.32.6 Decision Points Identified

ID	Component	Description

2.32.7 External Activities Identified

ID	Group	Description

2.33 UC-SEC-004_05 Revoke authentication

Based on misbehaviour reports the UC first decides if a participant of the C2X system network shall be excluded.

2.33.1 Assumptions

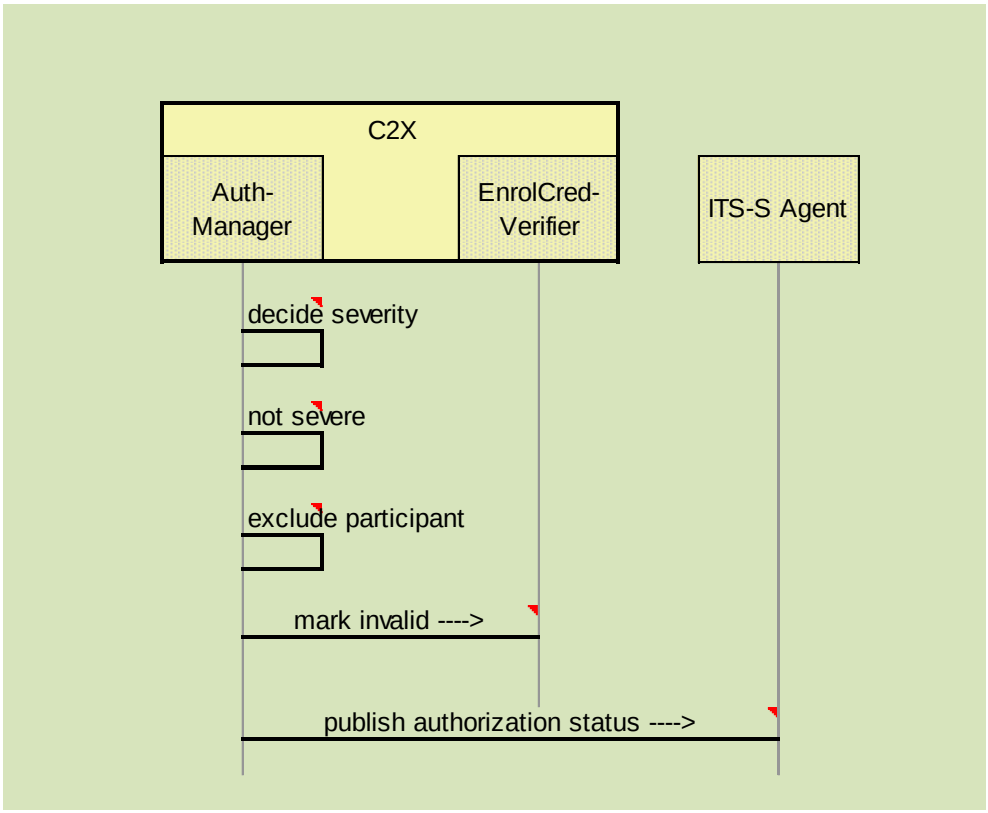
ID	Description
US-Exclude-A1	Misbehaviour reports a sent cyphered
US-Exclude-A2	Mobile Network operator does not perform misbehaviour detection based on message payload

2.33.2 Actions Pre-Operational

From	To	Description	Optional
Prereq-PreOp-1		A msibehaviour rpoert has been received	
Auth-Manager	Auth-Manager	perform security functions (decryption, authentication, non-repudation)	

2.33.3 Actions Operational

From	To	Description	Optional
Description-1			
Auth-Manager	Auth-Manager	the severity of the reported misbehaviour report is decided	
Auth-Manager	Auth-Manager	result: participant shall yet not be excluded	
Auth-Manager	Auth-Manager	result: participant shall be excluded from C2X systems network	
Auth-Manager	EnrolCred-Verifier	the certiciate of the pariticipant is marked as compromised	
Auth-Manager	ITS-S Agent	if the compromised participant is not an IVS, then the security service "publish authorisation status" is executed (see ETSI TS 102 731)	conditional



2.33.4 Actions Post-Operational

From	To	Description	Optional

2.33.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
Auth-Manager	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an certificate to access the service. The CA is also responsible for certificate revocation.		x	
EnrolCred-Verifier	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an certificate to access the service. The CA is also responsible for certificate revocation.		x	
ITS-S Agent	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.		x	

2.33.6 Decision Points Identified

ID	Component	Description

2.33.7 External Activities Identified

ID	Group	Description

2.34 UC-C2X-101-04

Car2X Systems Network offers an advertisement service that enables (a) Service Provider and Communication Network Provider to advertise the services they offer (b)

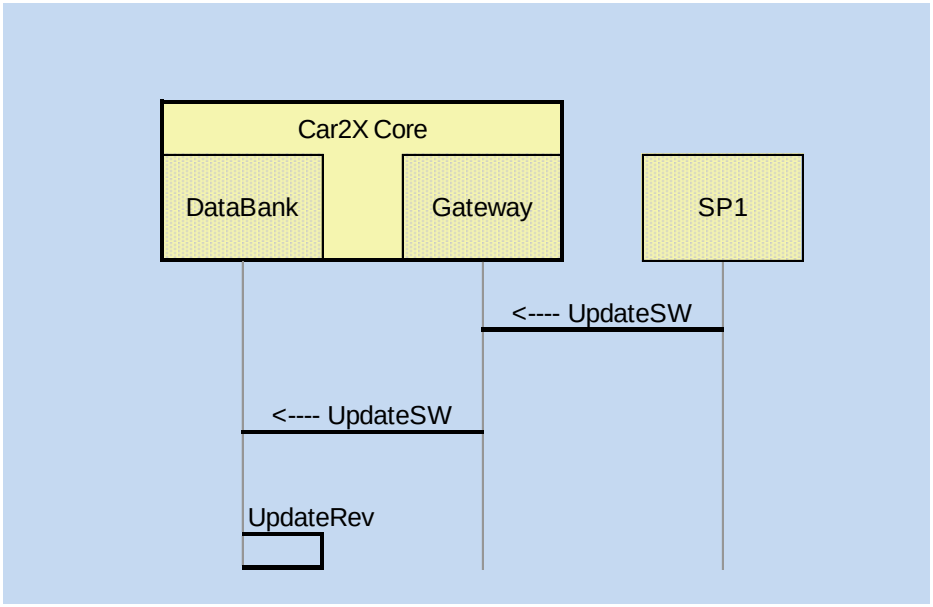
Service Provider and Mobile Nodes to lookup discover services offered within the C2X integrated systemC2X Systems Network.

2.34.1 Assumptions

ID	Description

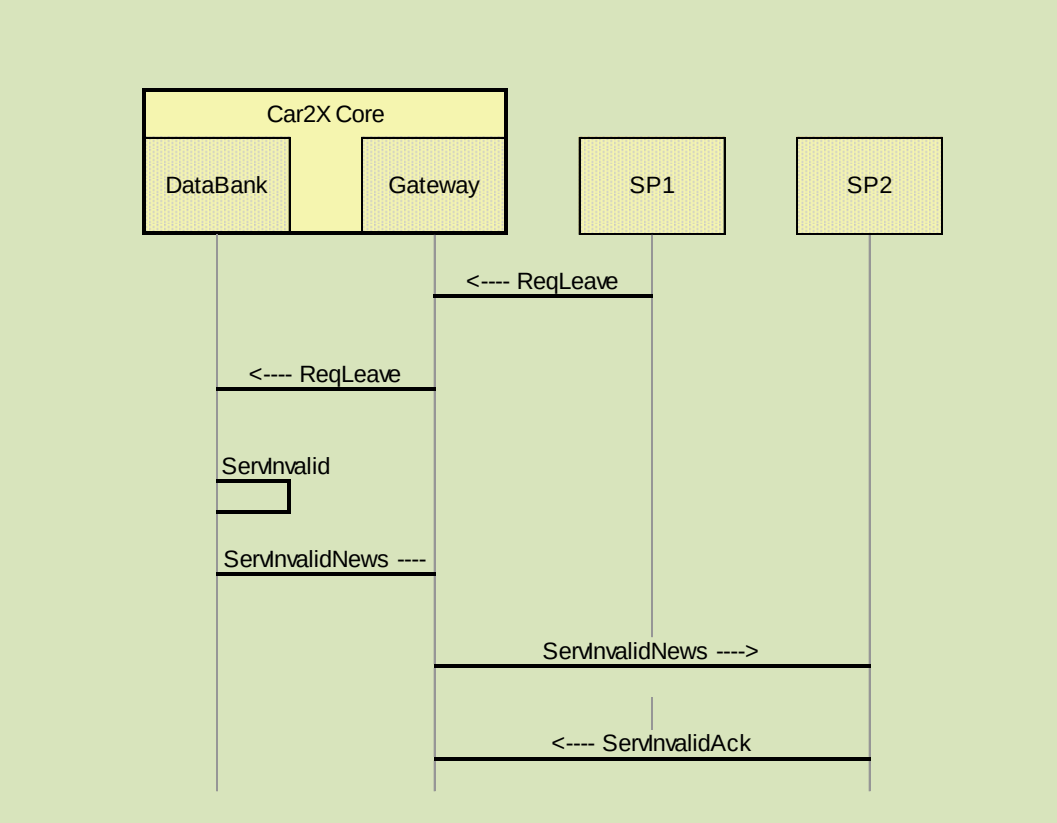
2.34.2 Actions Pre-Operational

From	To	Description	Optional



2.34.3 Actions Operational

From	To	Description	Optional
SP1	Gateway		
Gateway	DataBank		
DataBank	DataBank		
DataBank	Gateway		
Gateway	SP2		
SP2	Gateway		



2.34.4 Actions Post-Operational

From	To	Description	Optional

2.34.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
DataBank	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 services/information. This can be inside the C2X-SN itself and/or 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	

Gateway	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.	x	x	
SP1	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.	x	x	
SP2	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.		x	

2.34.6 Decision Points Identified

ID	Component	Description

2.34.7 External Activities Identified

ID	Group	Description

2.35 UC-C2X-105

"Data sinks are able to assess the quality of perceived data based on a predefined set of quality metrics.

Precondition: Predefined set of data quality metrics including relevant information from originating sensor.For some use cases, a standardized interpretation of data quality is required (e. g. in case of safety-relevant information).

Note: In case of safety-relevant information, information regarding applied data processing algorithms needs to be made available to the receiver in order to reproduce the interpretation of data."

2.35.1 Assumptions

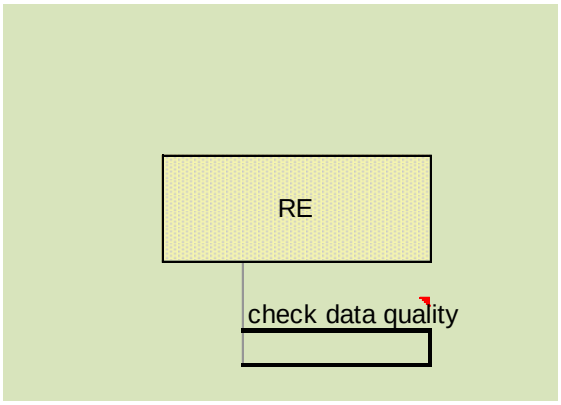
ID	Description
AS#1	The Rule Engine has a set of quality metric to assess the received data

2.35.2 Actions Pre-Operational

From	To	Description	Optional
Pre-requisite#1		The Rule Engine has a set of quality metric to assess the received data	
Pre-requisite#2		The received data includes a standard reference	
Pre-requisite#3		The received data includes information about the sender, time stamp and signature.	

2.35.3 Actions Operational

From	To	Description	Optional
RE	RE	The Rule Engine has a set of quality metric to assess the received data	



2.35.4 Actions Post-Operational

From	To	Description	Optional

2.35.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	

2.35.6 Decision Points Identified

ID	Component	Description
DP-01	check data quality	A set of quality mertrics needs to be defined, which describe the quality of the received data (e.g. originator, type of sensor, type of processing algorithm, timestamp, signature, …)

2.35.7 External Activities Identified

ID	Group	Description

2.36 UC-C2X-106

"The IVS/IRS respectively IRS observes the communication environment, identifies available access points / networks selects the appropriate according to a predefined set of criteria (e.g. application, costs, contract, bandwith, QoS, …).

Note: The SP selects the appropriate communication access point / network according to a predefined set of criteria (e.g. application, costs, contract, bandwith, QoS, IVS/IRS access availability, …). This part is handled in UC-C2x-103_01-03"

2.36.1 Assumptions

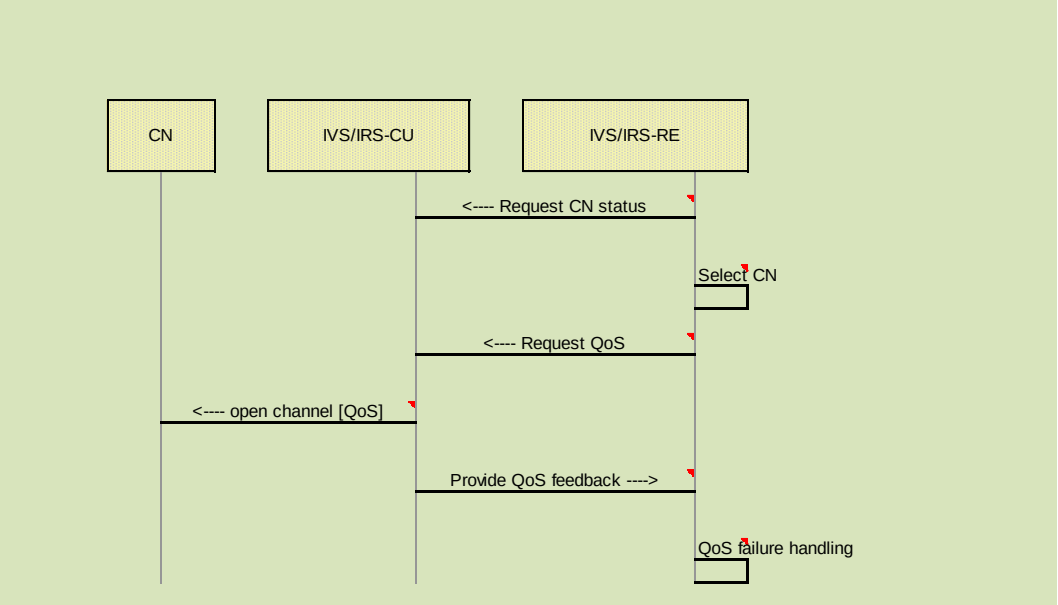
ID	Description

2.36.2 Actions Pre-Operational

From	To	Description	Optional
Pre-Requiste#1		IVS/IRS needs different communication units (G5A/B, MNO 1/2/3) including authentication	
Pre-Requiste#2		IVS/IRS needs to be in communication range (stationary or moving)	
Pre-Requiste#3		SP needs access to C2X communication networks to IVS/IRS	
Pre-Requiste#4		The IVS/IRS has a "decision maker" to select a communication link and protocol type	
IVS/IRS-APP	IVS/IRS-RE	The Application/service provides the selection criteria (e.g. QoS)	

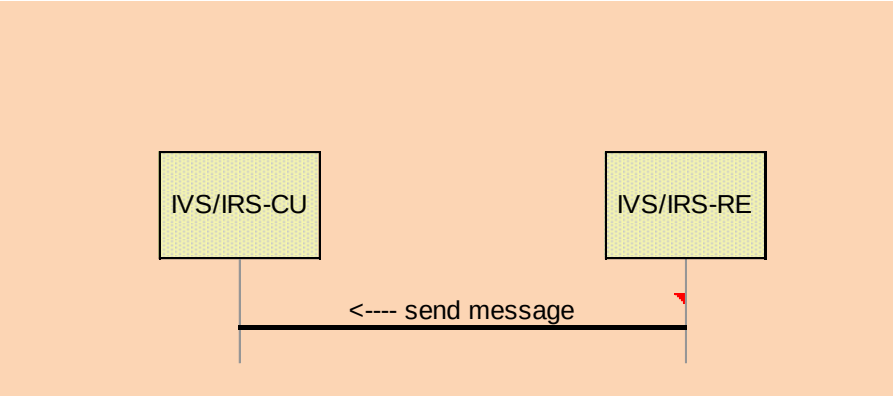
2.36.3 Actions Operational

From	To	Description	Optional
IVS/IRS-RE	IVS/IRS-CU	Rule engine detects status of both mobile network and G5	
IVS/IRS-RE	IVS/IRS-RE	Rule engine selects communication network depending on criteria	
IVS/IRS-RE	IVS/IRS-CU	rule engine request communication channel with a certain QoS	yes
IVS/IRS-CU	CN	IVS/IRS-CU request communication channel with requested QoS	yes
IVS/IRS-CU	IVS/IRS-RE	CU informs RE about the success/failure of QoS request	yes
IVS/IRS-RE	IVS/IRS-RE	optional: in case the QoS requirements can not be met RE decides about further actions	yes



2.36.4 Actions Post-Operational

From	To	Description	Optional



2.36.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
CN	The CN provides communication capacity for all kind of other services		x	
IVS/IRS-CU			x	x
IVS/IRS-RE			x	x

2.36.6 Decision Points Identified

ID	Component	Description
DP-01	Select CN	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 IST-G5 modem qos parametrization 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). These quality parameters need to be incorporated into the "decision maker" (Entscheider) accordingly.
DP-02	Request CN status	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 **-> Entscheider Diskussion in AP6, ggfs ausweiten auf AP5?**
DP-03	QoS failure handling	it has to be decided how the RE shall handle cases, where the requested qos can not be met by the available communication networks

2.36.7 External Activities Identified

ID	Group	Description
US-01	Provide QoS requirements	Suse case describing the different qos requirements of the applications (and the mechnism of requestion qos from CU)

2.37 UC-ComNet-01

"Message reception and processing by the communication network

A message has been received by a termination point of the infrastructure-based communication network that is assigned to the source-region of the message. The message is being forwarded through the backbone network to a termination point of the instrastructure-based communication network that is assigned to the sink-region of the message. Since the mobile network operators of source- and sink region do not necessarily need to be the same, specific service level agreements (e. g. QoS control, payment charges) need to be in place."

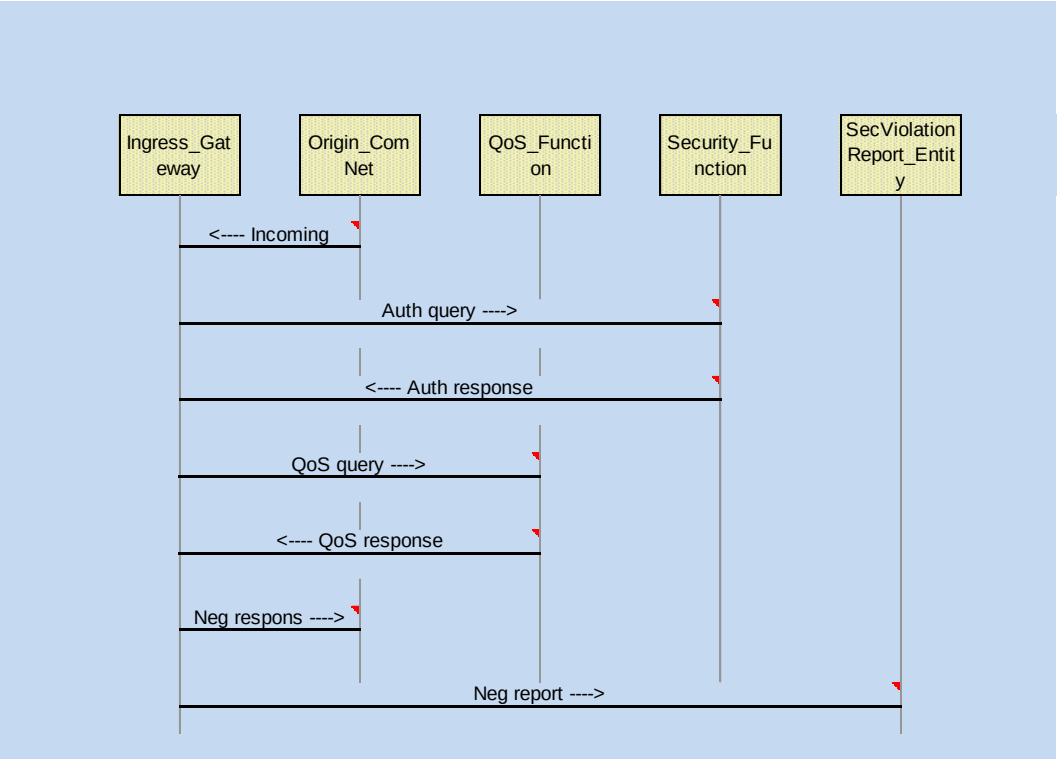
2.37.1 Assumptions

ID	Description
UC-ComNet-01-A1	A message is available
UC-ComNet-01-A2	A message has been processed in the communication network and can be forwarded
UC-ComNet-01-A3	While for the sending of messages requirements can be defined, at the reception spot there is only a verification of security. Due to that the reception-aspect is omitted. While processing the privacy of the sending entities has to be protected (aggregation).
UC-ComNet-01-A4	The network operators share known agreements and specifications according protocols, QoS, etc.
UC-ComNet-01-A5	REQ-SEC-PS-015 Authorization: Senders of messages shall be authorized to send these messages for this use case.

2.37.2 Actions Pre-Operational

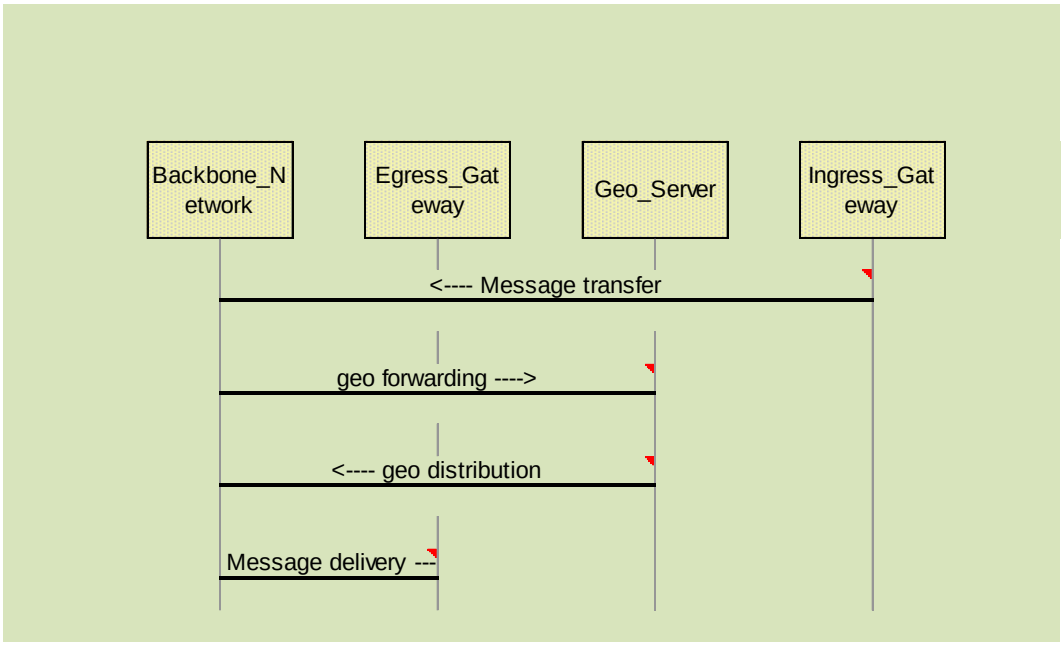
From	To	Description	Optional
Origin_ComNet	Ingress_Gateway	The message to be forwarded by the backbone communication network.	
Ingress_Gateway	Security_Function	Query the information if the sender was authorized to send the message.	
Security_Function	Ingress_Gateway	Result of the authorization check.	
Ingress_Gateway	QoS_Function	Query if the claimed QoS is currently	

		available.
QoS_Function	Ingress_Gateway	Result of the QoS query.
Ingress_Gateway	Origin_ComNet	If the auth or the QoS query was negative,x the sender network is informed.
Ingress_Gateway	SecViolationReport_Entity	If the auth query was negative, the securityx violation entity is informed.



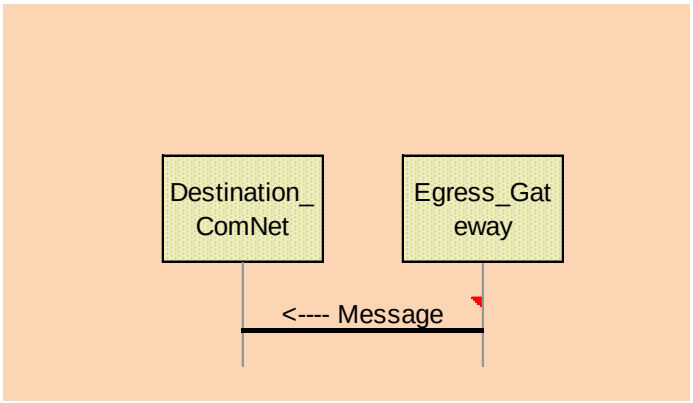
2.37.3 Actions Operational

From	To	Description	Optional
Ingress_Gateway	Backbone_Network	The message is forwarded to the actual backbone network.	
Backbone_Network	Geo_Server	If the destination address is not known, thex message is forwarded to the GeoServer, which queries for corresponding addresses.	
Geo_Server	Backbone_Network	If nodes are found in the specified geografic area,x the message is forwarded with the corresponding adress to the backbone network.	
Backbone_Network	Egress_Gateway	The message is forwarded to the egress gateway.	



2.37.4 Actions Post-Operational

From	To	Description	Optional
Egress_Gateway	Destination_ComNet	The message is delivered to the destination communciation network.	



2.37.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Po Oper
Backbone_Network	The CN provides communication capacity for all kind of other services		x	
Destination_ComNet	The CN provides communication capacity for all kind of other services			

Egress_Gateway	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.		x	
Geo_Server	Server in the C2X-SN and/or SP and /or CN that distributes information to clients in a geographical area.		x	
Ingress_Gateway	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.	x	x	
Origin_ComNet	The CN provides communication capacity for all kind of other services	x		
QoS_Function	The QF is responsible for all kind of QoS related data gathering and adjustments.	x		
Security_Function	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.	x		
SecViolationReport_Entity	Entity that is informed about any security and service misbehavior. It will take or initiate the necessary measure (caution or throw out participants | technical or legal) depending on the amount and severity of the misbehavior.	x		

2.37.6 Decision Points Identified

ID	Component	Description
DP-01	Geo_Server	How is the adressing done? How gets the server the information about the clients?
DP-02	QoS_Function	Do we have a feedback if the QoS was met?
DP-03	Ingress_Gateway	Do we send a feedback, if the message can be send via the backbone network? And dowe send a feedback, if the message was delived successfully or unsuccessfully to the next network?

2.37.7 External Activities Identified

ID	Group	Description
US-01	SecViolationReport_Entity	What is done with security violations?
US-02	QoS_Function	Gathers information and calculates the currently available QoS.

2.38 UC-ComNet2IVS-01

IVS Receiving message fromvia backbone communication infrastructure

2.38.1 Assumptions

ID	Description

2.38.2 Actions Pre-Operational

From	To	Description	Optional

2.38.3 Actions Operational

From	To	Description	Optional

2.38.4 Actions Post-Operational

From	To	Description	Optional

2.38.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.38.6 Decision Points Identified

ID	Component	Description

2.38.7 External Activities Identified

ID	Group	Description

2.39 UC-ComNet2SP-01

"Message reception at SP

Use-case seems to be already covered by LHW-UC ""CONVERGE_LHW_D3_TechnicalRequirement_v03.xls"" from first AP2 workshop!! Use-case is unclear, therefore it needs to be ""interpreted""...

Interpretation (GB): a (local) road hazard warning is generated by an IVS and sent to its OEM backend/SP through the communication network the lhw message is received at the OEM backend/SP.

Precondition: The message to be distributed includes a georeferenced relevance, such as a LHW warning.The SP knows the location of the communication partner (geoserver, etc.)The SP knows the destination area of the message to be distributed.The SP has registered to deliver the LHW messages (e. g. filtering the Car2X System Network for LHW messages).

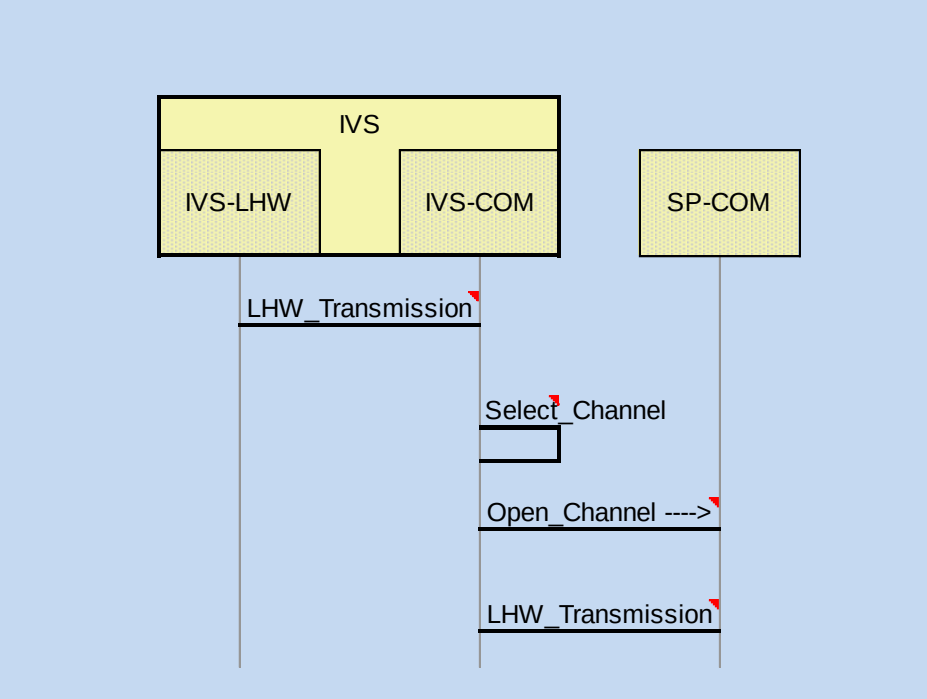
Postcondition: Routing of a road hazard warning message through the core network to the back end of a service provider.All recipients within the given destination area have been identified"

2.39.1 Assumptions

ID	Description
MsgRecSP-01	IVS has generated a valid lhw message, including a valid geo-reference
MsgRecSP-02	OEM Backend is registered as recipient for road works warning messages issued by a certain service provider
MsgRecSP-03	At the OEM Backend there is an incoming event alert service (IEA) available
MsgRecSP-04	OEM Backend has available a contract relationship with a certain mobile network operator (MNO)
MsgRecSP-05	OEM Backend has available a contract relationship with a certain ITS-G5 provider
MsgRecSP-06	The OEM Backend has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
MsgRecSP-07	a mechanism exists within OEM backend/SP to check authentication, authorization and validity if incoming message via certifaction authorities etc.
MsgRecSP-08	The IVS has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
MsgRecSP-09	The SP knows the location of the communication partner (geoserver, etc.
MsgRecSP-10	The SP knows the destination area of the message to be distributed
MsgRecSP-11	The OEM backend/SP has registered to deliver the LHW messages to other recipients (mobile nodes and/or other SPs)

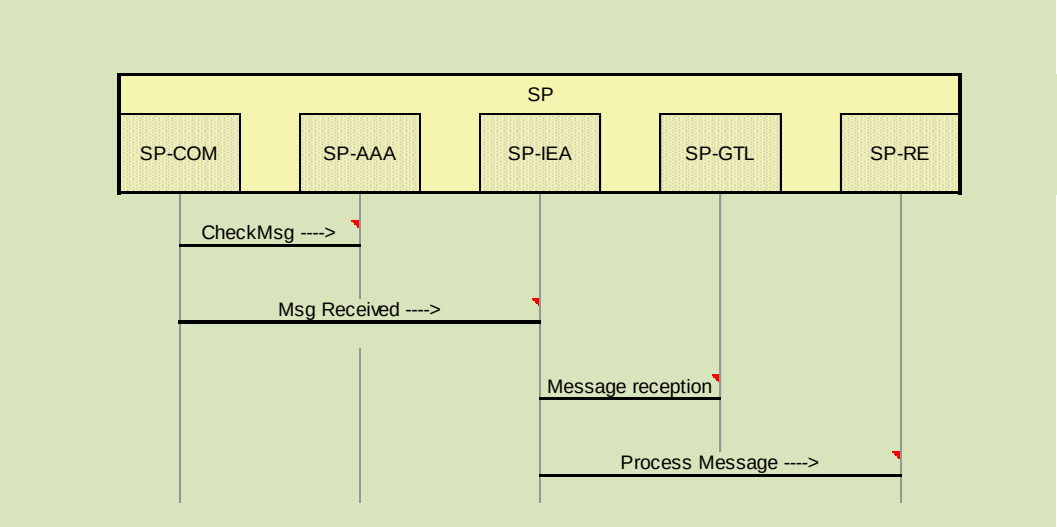
2.39.2 Actions Pre-Operational

From	To	Description	Optional
IVS-LHW	IVS-COM	IVS-LHW process requests transmission of LHW message to backend/SP [LHWmsg, QoS]	
IVS-COM	IVS-COM	IVS-COM determines best communications channel (e.g. IST-G5/cellular) via "Entscheider"	
IVS-COM	SP-COM	IVS-COM opens connection with requested QoS [QoS]	
IVS-COM	SP-COM	IVS-COM send LHW message to SP-COM [LHWmsg]	



2.39.3 Actions Operational

From	To	Description	Optional
SP-COM	SP-AAA	SP-COM checks incoming msg for authenticity, validity etc.	
SP-COM	SP-IEA	if check successful: SP-COM posts message to associated IEA board	
SP-IEA	SP-GTL	The availability of the RWW message is logged at the SP	
SP-IEA	SP-RE	The IEA informs the RE about the reception of a message	



2.39.4 Actions Post-Operational

From	To	Description	Optional

2.39.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS-COM	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.	x		
IVS-LHW	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.	x		
SP-AAA	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.		x	
SP-COM	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.	x	x	

SP-GTL	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.		x	
SP-IEA	Running on all communication endpoint entities. It represents the SAP for all incoming messages.		x	
SP-RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	

2.39.6 Decision Points Identified

ID	Component	Description
DP-01		see LHW/RWW descriptions
DP-02	Select_Channel	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 IST-G5 modem qos parametrization 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).

2.39.7 External Activities Identified

ID	Group	Description
US-01		see LHW/RWW descriptions
US-02	Select_Channel	A use-case describing the set of qos parameters (and its adoption), which both accomodates the application layer requirements regarding qos as well as the LTE modem and IST-G5 modem qos parametrization 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).

2.40 UC-IRS-01

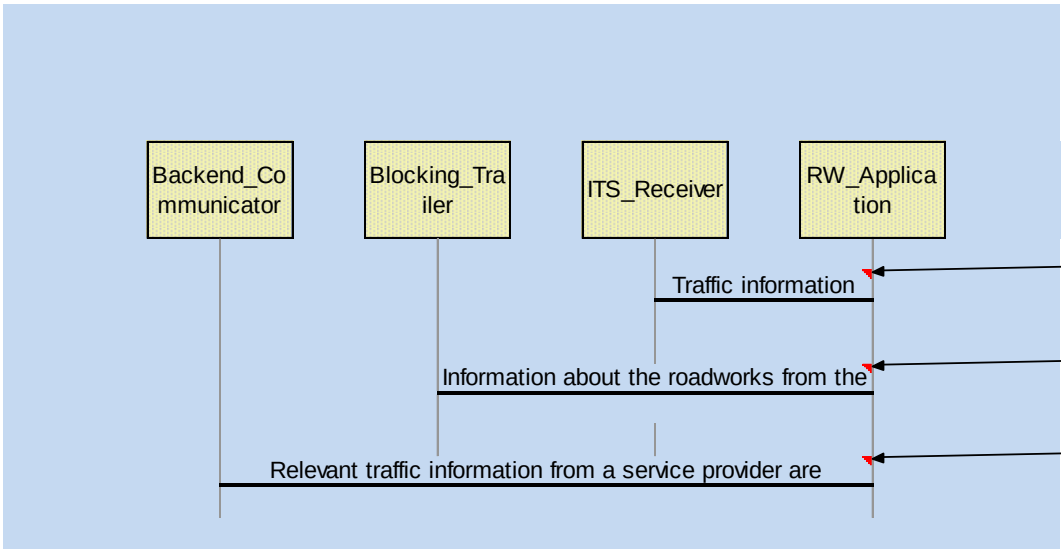
Blocking trailer collects information about the actual traffic condition and processes it

2.40.1 Assumptions

ID	Description
UC-IRS-01-A1	• UC-IVS2IRS-01 • A subset of vehicles in the vicinity of the blocking trailer send ETSI G5 messages • Privacy of the drivers is secured • Blocking trailer is able to pre-process traffic information using ETSI G5 messages from the other vehicles
UC-IRS-01-A2	Blocking Trailer is aware of the traffic in its environment depending on the wireless coverage and UC-IRS2SP-02 is enabled
UC-IRS-01-A3	The blocking trailer is not the initiating element of the collection/reception of information but the sending traffic component (IVS). That means no security-requirements are raised towards the trailer according to message-reception. It is however the initiating element according to further processing so the security-requirements reference to that aspect of the use-case. Sending or forwarding of information is not included. While processing the privacy of the CAM-sending entities has to be protected (aggregation).

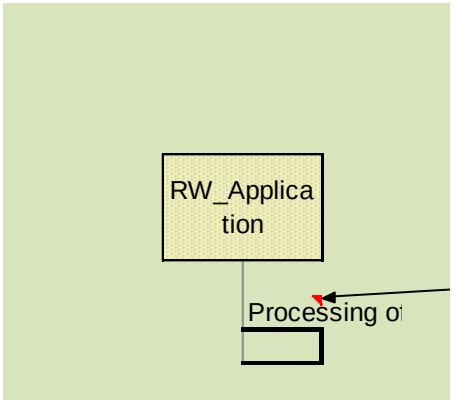
2.40.2 Actions Pre-Operational

From	To	Description	Optional
ITS_Receiver	RW_Application	The IVS send information about the track history driven by the vehicle. Additionally detected traffic signs in the vicinity of the roadworks are send.	
Blocking_Trailer	RW_Application	The blocking trailer send periodically the current state of the sign and the roadworks from the trailer to the IRS and so to the application.	
Backend_Communicator	RW_Application	The services provider send inforamtion about the current traffic in the area to support the roadworks application in buildung a correct traffic situation.	



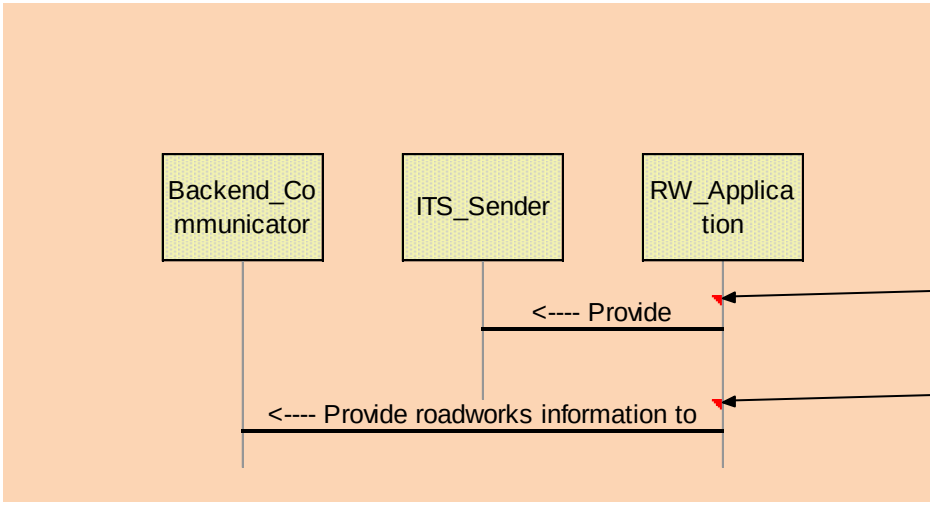
2.40.3 Actions Operational

From	To	Description	Optional
RW_Application	RW_Application	The application evaluates the received information and processes them for the following tasks - determination of the current traffic state - calculation of the roadworks geometry and position - determine the traffic signs of the roadworks and the upstream traffic area	



2.40.4 Actions Post-Operational

From	To	Description	Optional
RW_Application	ITS_Sender	The processed information are forwarded to the IVS in the area to provide information about the roadworks and the respective traffic state.	
RW_Application	Backend_Communicator	The processed information are forwarded to the service provider to provide information about the roadworks and the respective traffic state.	



2.40.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Pos Opera
Backend_Communicator	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.	x		x
Blocking_Trailer		x		
ITS_Receiver	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		
ITS_Sender	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.			x
RW_Application	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.	x	x	x

2.40.6 Decision Points Identified

ID	Component	Description

2.40.7 External Activities Identified

ID	Group	Description

UC-IRS-01-EUS-1	Connection between Blocking Trailer and IRS.

2.41 UC-IRS-02

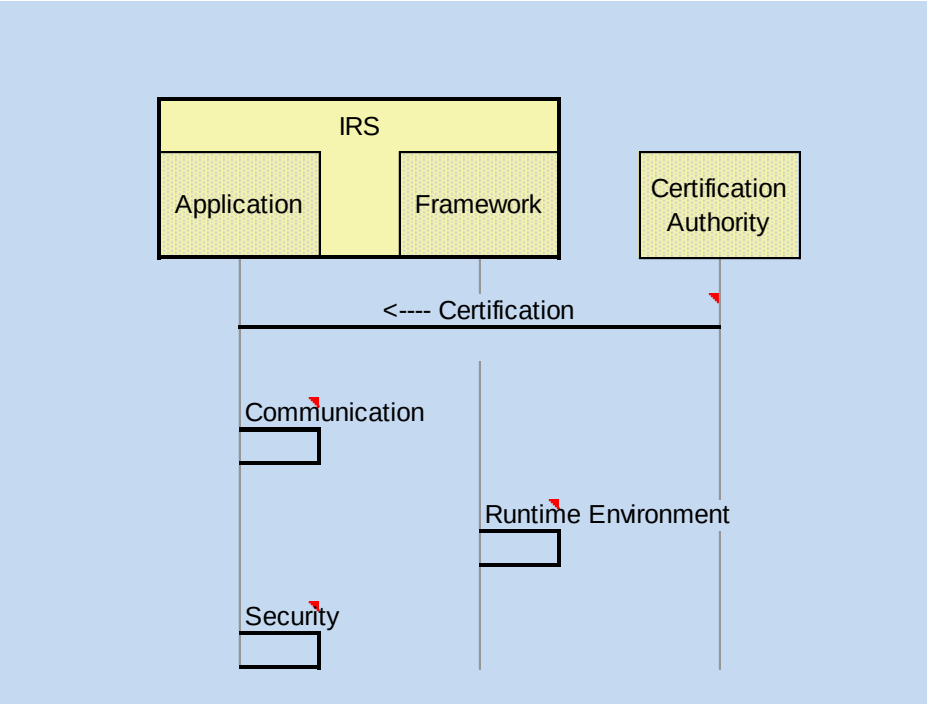
The IRS may serve as a host for applications. Those applications may be part of a service provider or provide services themselves.

2.41.1 Assumptions

ID	Description
UC_IRS-02_A1	The IRS provider has a business relation to the owner of the application.The application fulfils the requirements the IRS provider has set. (QoS, reliability, security)
UC_IRS-02_A2	The remote installtion/update/deinstallation of application on an IRS is defined and possible (OWN USE CASE)
UC_IRS-02_A3	A central application repository exist. (OWN USE CASE)
UC_IRS-02_A4	Security requirements regarding communication shall be elaborated in an own use case.

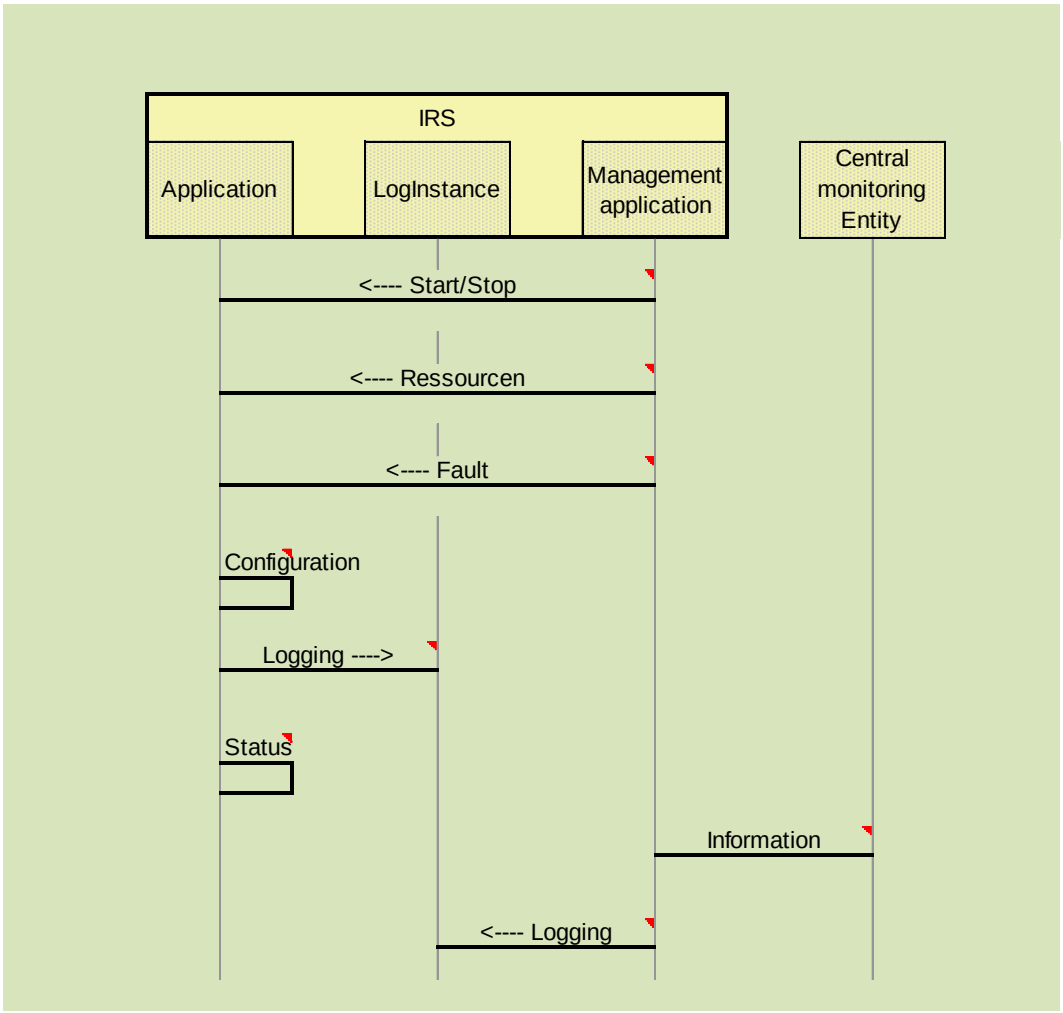
2.41.2 Actions Pre-Operational

From	To	Description	Optional
CertificationAuthority	Application	The application has been certified for the C2X systems network. (OWN USE CASE)	
Application	Application	Communication Interfaces for Mobile Node and Service Provider Communication are established.	
Framework	Framework	A runtime environment for the applications is working properly.	
Application	Application	The communication between applications and the storage of data have to be regualted/secured.	



2.41.3 Actions Operational

From	To	Description	Optional
Management application	Application	Start/Stop Application	
Management application	Application	Ressourcen Management (Space/Power/CPU/RAM/Comm)	
Management application	Application	Fault Management monitors the application, and acts on detected malfunctions.	
Application	Application	The Application must be remotely configurable. (OWN USE CASE)	
Application	LogInstance	Application entities shall log in the configured manner.	
Application	Application	The Application must provide an interface for status information.	
Management application	Central monitoring Entity	The status/logging/fault information must be forwarded to a central monitoring. (OWN USE CASE)	
Management application	LogInstance	Management entities shall log in the configured manner.	



2.41.4 Actions Post-Operational

From	To	Description	Optional

2.41.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
Application	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.	x	x	

Framework	The platform on an IRS/IVS or SP where the actual ApP are running and where they are managed.	x	X	
LogInstance	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.		x	
Management application	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 platform it is running.	X	x	
Central monitoring Entity	Monitoring component for IRS/IVS, SP, …, not a centralized monitoring		x	
CertificationAuthority	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an certificate to access the service. The CA is also responsible for certificate revocation.	x		

2.41.6 Decision Points Identified

ID	Component	Description
UC-IRS_02_DC_1	Management application	specification of communication with management (log/fault/conf/status)
UC-IRS_02_DC_2	Application	specification of communication to service provider

2.41.7 External Activities Identified

ID	Group	Description
UC_IRS-02_EUS_1		The remote installtion/update/deinstallation of application un an IRS is definde an possible
UC_IRS-02_EUS_2		The application has been certified for the C2X systems network
UC_IRS-02_EUS_3		The Application must be remotely configurable.
UC_IRS-02_EUS_4		A remote management must be able to administrate, install/uninstall, configure and monitor appilcation on an IRS application plattform.

UC_IRS-02_EUS_5	A central application repository exist.(For all application or only for an IRS network, or…)
UC_IRS-02_EUS_6	The status/logging/fault information must be forwarded to an central monitoring
UC_IRS-02_EUS_7	The requirements (including the defined security req for this UC) for the application running on the IRS must be defined in an own use case: Applications running on the IRS communicate with the vehicles and a service provider.

2.42 UC-IRS2SP-01

Blocking trailer informs the service provider about the start of RWW with all the information that is required by the SP in order to identify the Road Works

2.42.1 Assumptions

ID	Description
US-RWW-A1	Information about the communication end point (traffic center) ist known to the blockin trailer
US-RWW-A2	The initial information (message content) that the blocking trailer has to distribute has been defined and is availlable at the blocking trailer communication device (IRS)
US-RWW-A3	The blocking trailer IRS has information available about the accurate position and time
US-RWW-A4	The blocking trailer hast means to communicate with the infrastructure (traffic center) and vehicles. This includes cellular radio and ETSI ITS G5
US-RWW-A5	The blocking trailer IRS has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
US-RWW-A6	A road works warning database hast been started and initialized at the traffice center
US-RWW-A7	All sended 5G messages will be c

2.42.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1			
Prerequisite-2		Bob is pushing a button or flips up the traffic sign (manual activation)	
BT-IRS-CU	IVS-CU	The blocking trailer takes the initial information available, generates a broadcast message (ETSI ITS G5) and periodically sends it out	

BT-IRS-CU	TC-CU	The blocking trailer sets up the communication to its traffic center communication end point	
BT-IRS-CU	TC-CU	The blocking trailer registers at its traffic center and sends its initial information (single message, reliable, authentic, integer, confidential, not time critical)	
TC-CU	BT-IRS-CU	The traffic center sends (optional) updated information about the details of the road works to the blocking trailer (single message, reliable, authentic, integer, confidential, not time critical)	X

2.42.3 Actions Operational

From	To	Description	Optional
Description-1		There are 4 general action lines: - periodic distribution of actual configuration information via ETSI ITS G5 - no change in configuration, traffic center needs to get information about the status of the blocking trailer on regular basis or event driven - blocking trailer has detected a change in its configuration (e.g. position change) - traffic center updates information to the blocking trailer	
BT-IRS-CU	IVS-CU	The blocking trailer takes the actual information available, generates a broadcast message (ETSI ITS G5) and periodically sends it out	
BT-IRS-CU	TC-CU	the blocking trailer sends regular or event driven the actual trailer information	
BT-IRS-CU	TC-CU	The blocking trailer has detected a change in its configuration (e.g. position change) and sends an update message to its traffic center and updates its configuration information record	
TC-CU	BT-IRS-CU	The traffic center sends updated information about the details of the road works to the blocking trailer (single message, reliable, authentic, integer, confidential, not time critical)	X
TC-CU	TC-RWDB	The traffic center updates its current database of road works events	

2.42.4 Actions Post-Operational

From	To	Description	Optional
Description-1		Construction site is terminated, Blocking trailer gets shut down, traffic center is informed about construction termination, G5 broadcast is terminated by termination DENM	
Prerequisite-1		Bob has finalized construction works and deactivates the blocking trailer.	
BT-IRS-CU	IVS-CU	a special message is sent via ETSI ITS G5 that informs the vehicles about the premature expiration of the previous DENM	
BT-IRS-CU	TC-CU	the blocking trailer sends a messge with information about the road works end to the traffic center	

2.42.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.42.6 Decision Points Identified

ID	Component	Description
DP-RWW-1	TC-CU	Find best way to communicate the "here I am" message from the blocking trailer to its communication end point. Possible decission to be taken: - acknowledged - repeating on transport level or aplicaton level - mechanism for confidentiality (tunnel, "cable", message based)
DP-RWW-2	BT-IRS-CU	Determine exact mechanism to exchange the operational status of the blocking trailer to its traffic center - Push or Pull

2.42.7 External Activities Identified

ID	Group	Description
US-RWW-E1		A way to inform the blocking trailer about its infrastructure communication end point has to be specified in detail

US-RWW-E2		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 (Button that Bob is pushing) or from an external entity
US-RWW-E3		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
US-RWW-E4	IVS	The IVS hast 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 have changed
US-RWW-E5	TC	The mechanism to start up all components at the TC backend has to be described

2.43 UC-IRS2SP-02

Blocking trailer informs SP about the actual traffic condition using the best available network technology (see UC-IRS2SP-01)

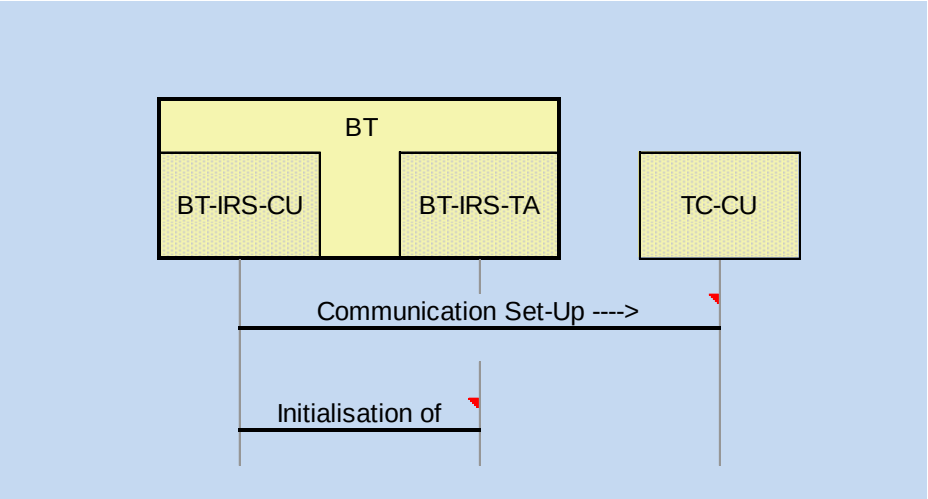
2.43.1 Assumptions

ID	Description
UC-IRS2SP-02-A1	Information about the communication end point (traffic center) ist known to the blockin trailer
UC-IRS2SP-02-A2	The blocking trailer IRS has information available about the accurate position and time
UC-IRS2SP-02-A3	The blocking trailer hast means to communicate with the infrastructure (traffic center) and vehicles. This includes cellular radio and ETSI ITS G5
UC-IRS2SP-02-A4	The blocking trailer IRS has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
UC-IRS2SP-02-A5	A traffic analyzing module has been started at the traffic center.
UC-IRS2SP-02-A7	There are Vehicles, which have ETSI ITS G5 communikation technology on board.

2.43.2 Actions Pre-Operational

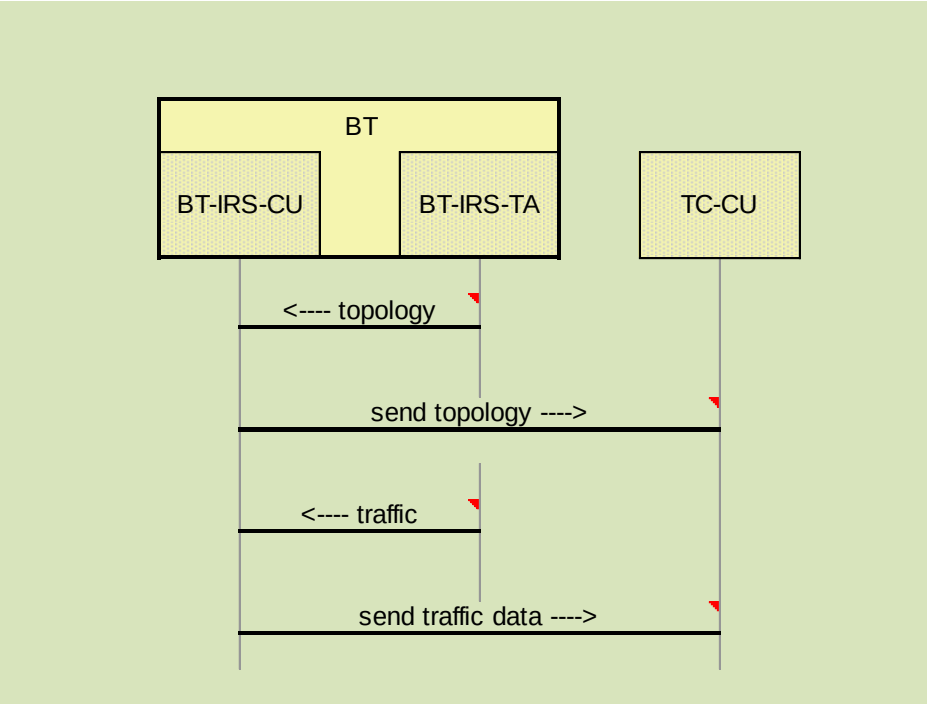
From	To	Description	Optional
Prerequisite-1		Bob is pushing a button or flips up the traffic sign (manual activation)	
Prerequisite-2		Only messages from the G5 interface which are authentic will forwarded to the functions.	

Prerequisite-3		All necessary components at TC have to be started.
BT-IRS-CU	TC-CU	The blocking trailer sets up the secure communication to its traffic center communication end point
BT-IRS-CU	BT-IRS-TA	Initialize the traffic analyzer of the IRS. The analyzer determine the topolgy of the lanes around the IRS using CAMs and DENMs.



2.43.3 Actions Operational

From	To	Description	Optional
Description-1		There are two task: 1) Update the topology if necessary 2) Analyze traffic flow	
Prerequisit-1		Only messages from the G5 interface which are authentic will forwarded to the functions.	
BT-IRS-TA	BT-IRS-CU	Due to a position change of the BT, the topology have to be updated.	
BT-IRS-CU	TC-CU	BT sends topology information to the TC everey time, when a change occured	
BT-IRS-TA	BT-IRS-CU	The BT-IRS analyze the traffic around the BT using CAMs and DENMs.	
BT-IRS-CU	TC-CU	The BT sends the analyzed traffic data to the TC in specific time schedule	



2.43.4 Actions Post-Operational

From	To	Description	Optional
Description-1		Construction site is terminated, Blocking trailer gets shut down, traffic center will be informed about the terminated analyzing service.	
Prerequisite-1		Bob has finalized construction works and deactivates the blocking trailer.	
BT-IRC-CU	TC-CU	BT informs the TC about the stop of the analyzing process	

2.43.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
BT-IRS-CU	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.	x	x	

BT-IRS-TA	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.	x	x	
TC-CU	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.	x	x	

2.43.6 Decision Points Identified

ID	Component	Description
UC-IRS2SP-02-DP1	BT-IRS-CU	How often and in which quality should the analyzed data send to the TC.
UC-IRS2SP-02-DP2	BT-IRS-CU	What means secure in this UseCase.
UC-IRS2SP-02-DP3	BT-IRS-CU	The requirements for the connection have to be defines. (reliable, connectionless or connection oriented, etc.)

2.43.7 External Activities Identified

ID	Group	Description
UC-IRS2SP-02-E1		A way to inform the blocking trailer about its infrastructure communication end point has to be specified in detail
UC-IRS2SP-02-E2		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
UC-IRS2SP-02-E3	BT	The IVS hast 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 have changed
UC-IRS2SP-02-E4	TC	The mechanism to start up all components at the TC backend has to be described
UC-IRS2SP-02-E5	BT	There is a security mechanism, which checks the autenticity of G5-Messages.
UC-IRS2SP-02-E6	BT	Module which recognise the topology and analyzed the traffic condition around the IRS
UC-IRS2SP-02-E7	TC	The traffic center has a module, which gather traffic data from different sensors (e.g. IRS) and calculates a over all traffic situation.

2.44 UC-IRS-03

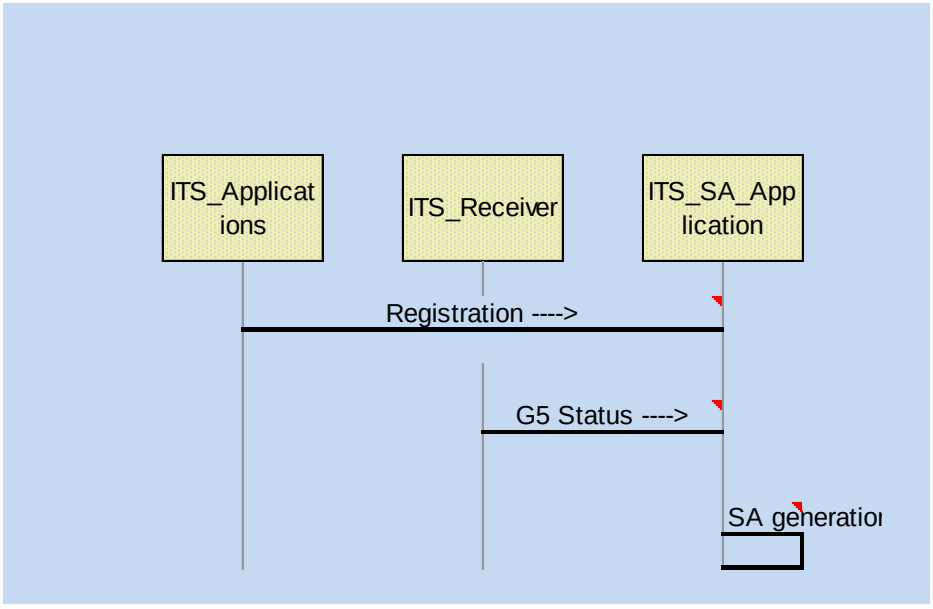
The IRS will announce the services which it provides via ITS G5.

2.44.1 Assumptions

ID	Description
UC-IRS-03-A1	On the IRS are one or more running services.
UC-IRS-03-A2	Passing IVS are informed about services on the IRS.
UC-IRS-03-A3	Only certified applications are allowned on the IRS.
UC-IRS-03-A4	Only the Service announcement application is allowed and able to send service announcement messages.

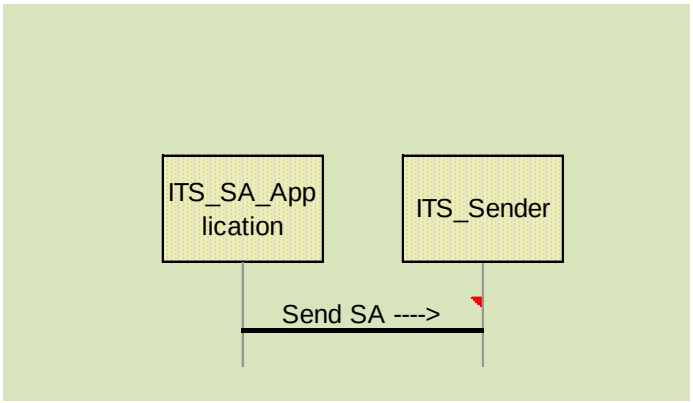
2.44.2 Actions Pre-Operational

From	To	Description	Optional
ITS_Applications	ITS_SA_Application	The ITS applications register by the service announcement application in order to be propagated.	
ITS_Receiver	ITS_SA_Application	The SA application collects information about the current status of the G5 network and the utilization of the available channels.	
ITS_SA_Application	ITS_SA_Application	The collected information and registrations are processed, the SA message is generated and the channels are selected.	



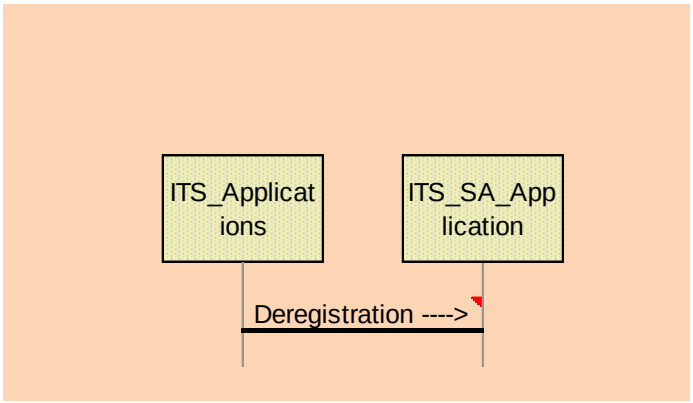
2.44.3 Actions Operational

From	To	Description	Optional
ITS_SA_Application	ITS_Sender	The created SA is send via G5 control channel.	



2.44.4 Actions Post-Operational

From	To	Description	Optional
ITS_Applications	ITS_SA_Application	The ITS applications deregister their service. If the last service is deregistered, no more SA is send.	



2.44.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
ITS_Applications	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.	x		x
ITS_Receiver	Running on all communication endpoint entities. It	x		

	represents the SAP for all incoming messages.			
ITS_SA_Application	SerAnn send 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)	x	x	x
ITS_Sender	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.		x	

2.44.6 Decision Points Identified

ID	Component	Description

2.44.7 External Activities Identified

ID	Group	Description
UC-IRS-03-EUS-1		Services provided via backend communication are announced to the service provider or communicaction networks.
UC-IRS-03-EUS-2		Restrict specific ITS functionalities to dedicated services.

2.45 UC-IVS2ComNet-01

"Sending message via backbone network infrastructure

The IVS supports infrastructure-based transmission mode.The IVS is registered to and certified for the Car2X Systems NetworkThe communication system is able to deliver messages to the desired recipients.

Note: Whole use case seems to be covered by UC-C2X_106 - clarification required"

2.45.1 Assumptions

ID	Description
REQ-ComNet-002	##
REQ-IVS_006	The IVS shall send its motion data (latitude, longitude, heading, speed, etc.) and time stamp as a message on a regular basis
REQ-IVS_008	In case of a hazard situation a specific (standard compliant) message containing

relevant data shall be sent.
REQ-IVS_022The communication system is able to determine the recipient of the message
REQ-SEC-PS-001The initiating actor shall use an authorized pseudonym. All other participating entities shall remain anonymous.
REQ-SEC-PP-003The initiating actor shall use an authorized pseudonym. All other participating entities shall be identifiable using their real identity.

2.45.2 Actions Pre-Operational

From	To	Description	Optional

2.45.3 Actions Operational

From	To	Description	Optional

2.45.4 Actions Post-Operational

From	To	Description	Optional

2.45.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.45.6 Decision Points Identified

ID	Component	Description

2.45.7 External Activities Identified

ID	Group	Description
US-01	IVS	use case specifically describing the regularly transmission of CAM messages (or similar) to cover REQ-IVS_006

2.46 UC-IVS2IRS-01

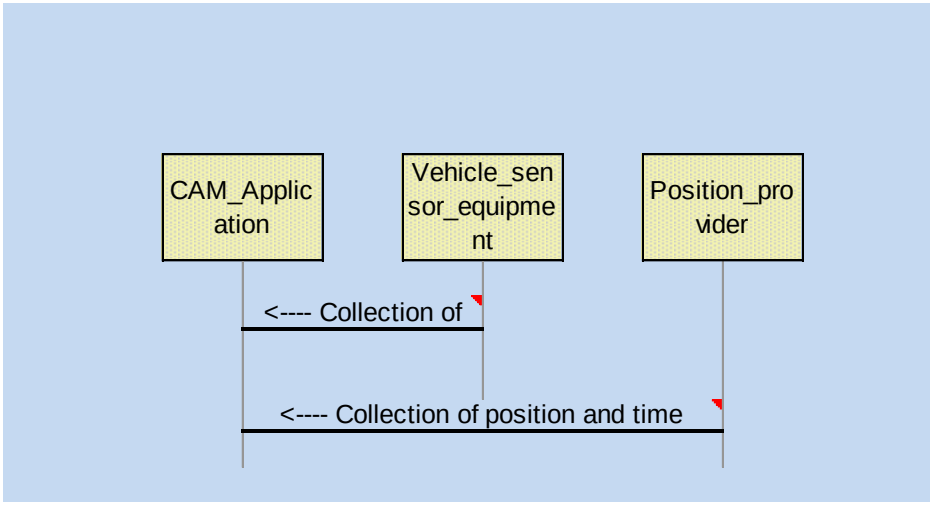
IVS respectively IRS sends CAMs to IRS respectively IVS

2.46.1 Assumptions

ID	Description
UC-IVS2IRS-01-A1	Both IVS and IRS supports direct transmission mode.
UC-IVS2IRS-01-A2	CAM is available at data sink.
UC-IVS2IRS-01-A3	The CAM matches the ETSI norm EN 302 637-2
UC-IVS2IRS-01-A4	The CAM application is aware whether it is running on an IRS or an IVS
UC-IVS2IRS-01-A5	Mechanisms to provide vehicle-specific data as well as position and time date are in place.

2.46.2 Actions Pre-Operational

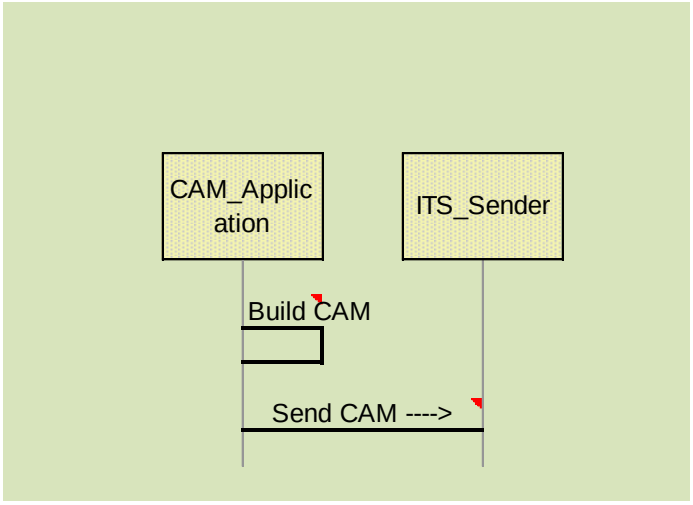
From	To	Description	Optional
Vehicle_sensor_equipment	CAM_Application	The vehicles sensors supply information for the CAM (VAPI).	
Position_provider	CAM_Application	Collection of position and time information for the CAM.	



2.46.3 Actions Operational

From	To	Description	Optional
CAM_Application	CAM_Application	The previously collected information are used to build a CAM, if one of the defined conditions is fullfilled (The trigger conditions are defined within the CAM standard).	

CAM_Application	ITS_Sender	The CAM is send via ITS G5 immidiately after it is build.



2.46.4 Actions Post-Operational

From	To	Description	Optional

2.46.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	P Ope
CAM_Application	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.	x	x	
ITS_Sender	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.		x	
Position_provider	Entity that collects information from sensors, gnss positioning data, … on IVS/IRS	x		
Vehicle_sensor_equipment	Entity that collects information from sensors, gnss positioning data, … on IVS/IRS	x		

2.46.6 Decision Points Identified

ID	Component	Description

2.46.7 External Activities Identified

ID	Group	Description

2.47 UC-IVS2SP-01_02 Renew Certificates - Reception

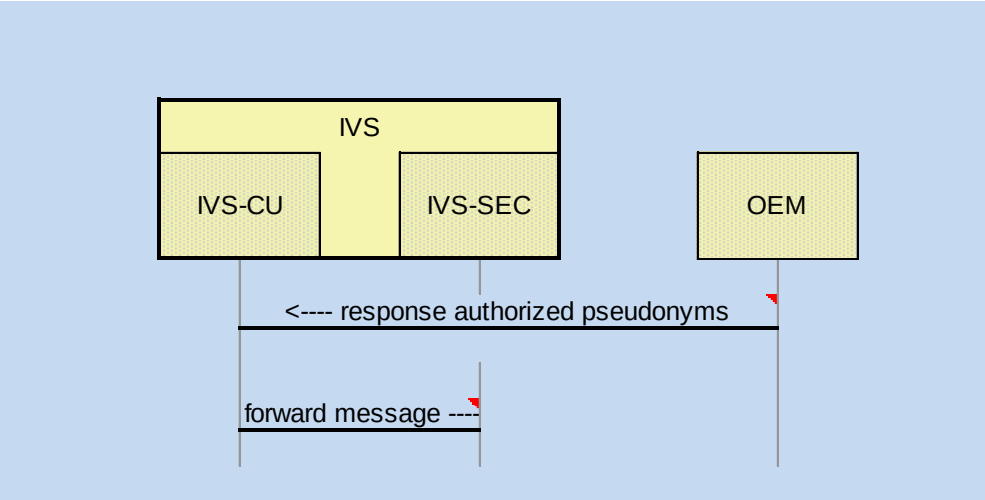
The IVS receives, checks, and stores the authorized pseudonyms on board.

2.47.1 Assumptions

ID	Description
Assumption-1	From the IVS point of view the OEM is its Authorization Authority (AA)
Terminology-1	The term "authorized pseudonyms" is used instead of certificates.

2.47.2 Actions Pre-Operational

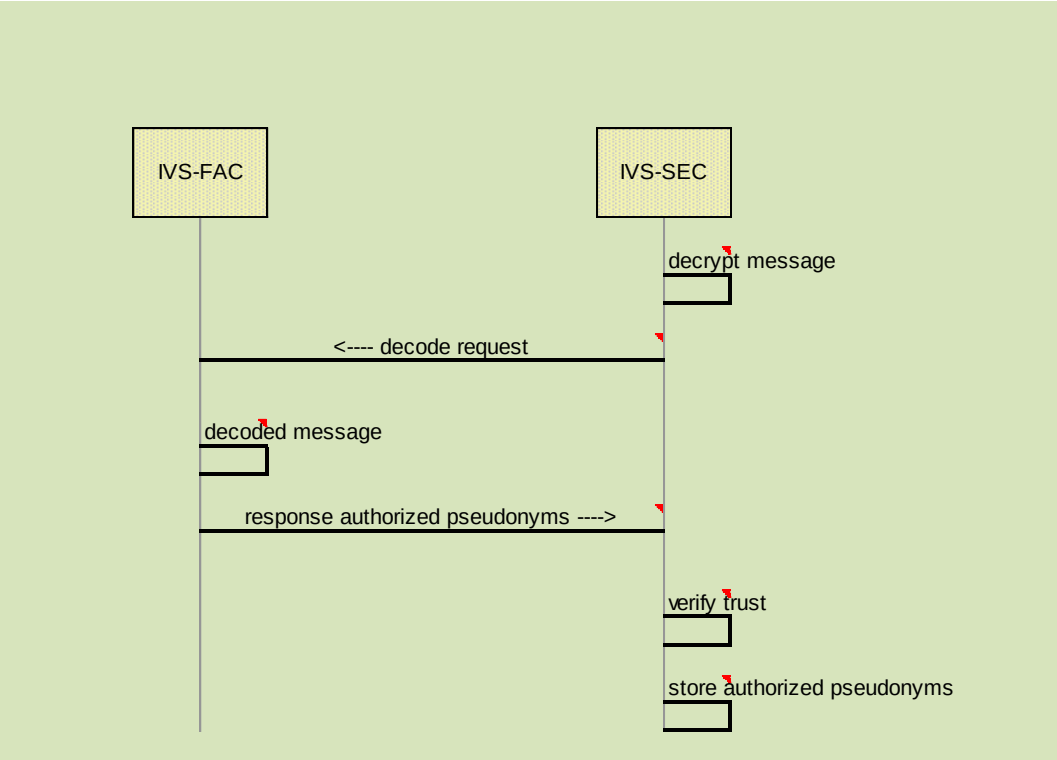
From	To	Description	Optional
OEM	IVS-CU	The IVS has physically received the ITS-S AuthorizationResponse message(see UC-ComNet2IVS-01)	
IVS-CU	IVS-SEC	The encrypted message is forwarded to security functions	



2.47.3 Actions Operational

From	To	Description	Optional
IVS-SEC	IVS-SEC	The message is decrypted with the IVS long term secret key.	

IVS-SEC	IVS-FAC	The decoded message is sent to the facility layer for decoding	
IVS-FAC	IVS-FAC	The IVS decodes the message (see UC-IVS-04)	
IVS-FAC	IVS-SEC	The IVS triggers the handling of the received authorization content	
IVS-SEC	IVS-SEC	The IVS checks f it can trust the message content	optional
IVS-SEC	IVS-SEC	The IVS adds the received authorization tickets to the set of available tickets.	



2.47.4 Actions Post-Operational

From	To	Description	Optional

2.47.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

IVS-CU	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.	x		
IVS-FAC	Processing steps for messages inside an IVS/IRS, that are application independent (e.g. Message distribution or CAM creation)		x	
IVS-SEC	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.	x	x	
OEM	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.	x		

2.47.6 Decision Points Identified

ID	Component	Description

2.47.7 External Activities Identified

ID	Group	Description
Ext-1	IVS	IVS receiving message via backbone communication infrastructure
Ext-2	IVS	IVS decodes received message

2.48 UC-IVS2SP-01_01 Renew Suthorized Pseudonyms - Request

An IVS observes that it is running out of authorized pseudonyms. The IVS creates a message to request authorized pseudonyms according to ETSI TS 102941 (Authorization Request Message), which shall be sent to the OEM. The IVS forwards this message to the subsequent use case, which will select a communication channel and send the message

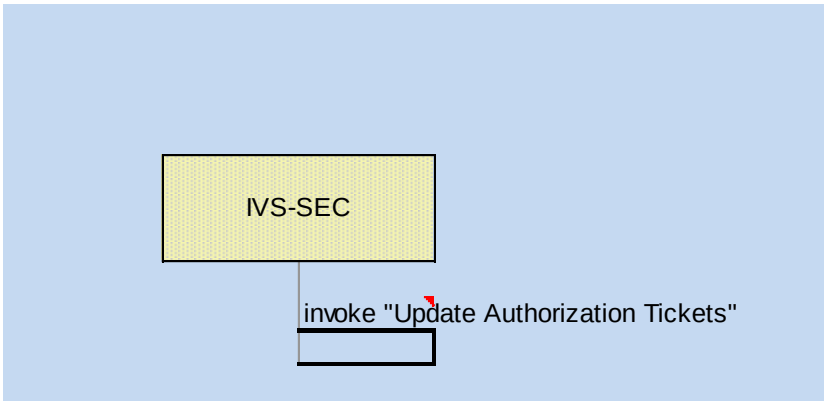
2.48.1 Assumptions

ID	Description

Assumption-1	From the IVS point of view the OEM is its Authorization Authority (AA)
Terminology-1	In CONVERGE AP1 the term "authorized pseudonyms" is used. It has the same meaning as the term "authorization ticket" which is defined in ETSI TS 102 731 and used in other specifications, esp. in ETSI TS 102940. In ETSI TS 102 942 the term "authorization ceriticate" is used.

2.48.2 Actions Pre-Operational

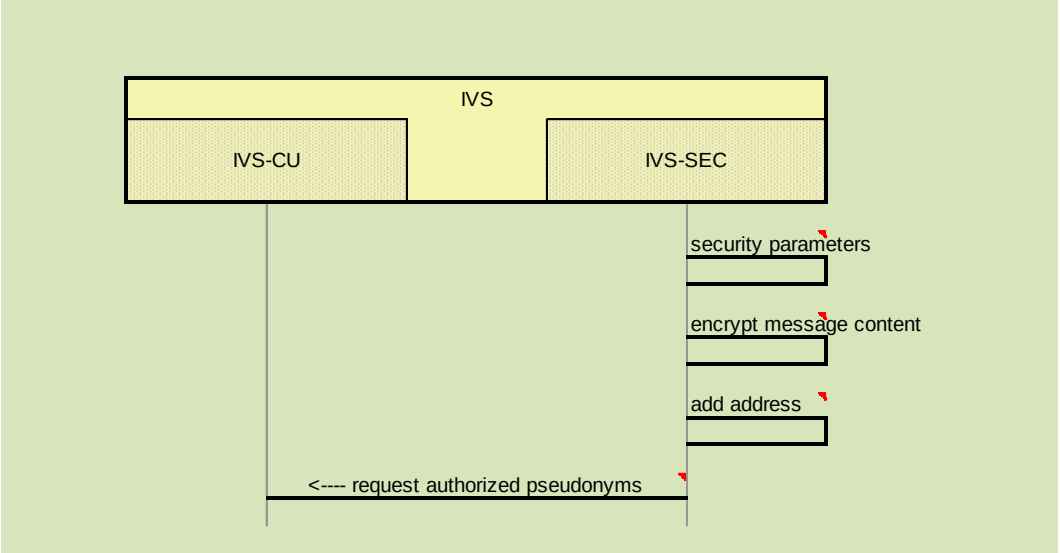
From	To	Description	Optional
Prereq-Pre-1		The IVS is a user of the Car2X Systems network and has a stock of authorized pseudonyms.	
Prereq-Pre-2		The IVS continuously monitors the amount of authorized pseudonyms, which are still available for the communication with other users of the Car2X systems network.	
Prereq-Pre-3		There is a predefined "renewal time period"	
IVS-SEC	IVS-SEC	The IVS detects that the amount of available authorized pseudonyms might be exhausted within the predefined "renewal time period". The security service "Update Authorized Pseudonyms" is triggered.	



2.48.3 Actions Operational

From	To	Description	Optional
IVS-SEC	IVS-SEC	The IVS generates security parameters, i.e. public keys and other information, which shall be authorized (certified).	
IVS-SEC	IVS-SEC	The message content is encrypted with the long term secret key of the IVS.	

IVS-SEC	IVS-SEC	The addressee OEM is added to the message
IVS-SEC	IVS-CU	The CU is asked to send the request message to the OEM (see UC- C2X-106)



2.48.4 Actions Post-Operational

From	To	Description	Optional

2.48.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS-CU	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.		x	
IVS-SEC	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.	x	x	

2.48.6 Decision Points Identified

ID	Component	Description

DP-1	IVS-CU	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.

2.48.7 External Activities Identified

ID	Group	Description

2.49 UC-SEC-001 Misbehaviour Detection

Plausibility checks on a received message concludes that the sender of the message misbehaves. This issue is reported to an authority for further action/decision.

2.49.1 Assumptions

ID	Description
US-Exclude-A1	Misbehaviour reports are sent cyphered
US-Exclude-A2	Mobile Network operator does not perform misbehaviour detection based on message payload

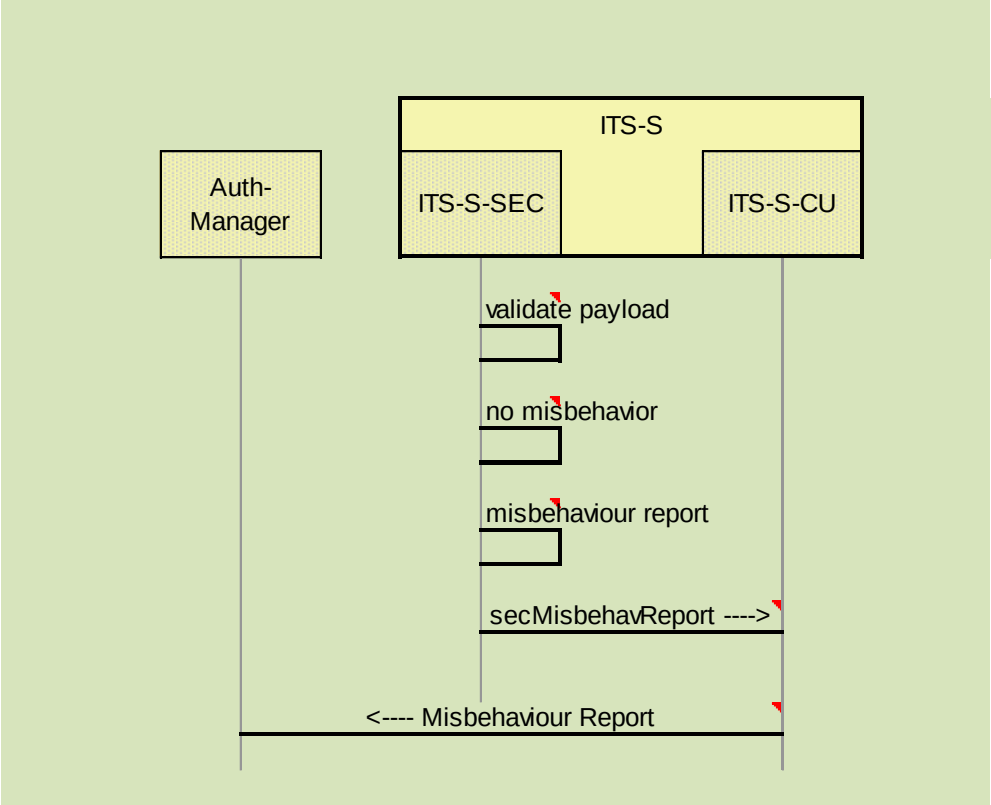
2.49.2 Actions Pre-Operational

From	To	Description	Optional
Prereq-PreOp-1		- C-ITS message has been received - message decrypted (if needed) - message sender authenticated - integrity validated Note 1	
Prereq-PreOp-2		-	
Prereq-PreOp-3		the message receiver decides to check the plausibility of the message content Note 2	

2.49.3 Actions Operational

From	To	Description	Optional
Description-1			
ITS-S-SEC	ITS-S-SEC	After basic security checks the security service "Validate Data Plausibility" is executed.	

ITS-S-SEC	ITS-S-SEC	The message is encryted
ITS-S-SEC	ITS-S-SEC	generate payload for reporting misbehaviour
ITS-S-SEC	ITS-S-CU	encrypted, certificate added, signed
ITS-S-CU	Auth-Manager	A report on a detected misbehaviour is send to the Authentication Status Manager



2.49.4 Actions Post-Operational

From	To	Description	Optional

2.49.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

Auth-Manager	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an certificate to access the service. The CA is also responsible for certificate revocation.		x	
ITS-S-CU	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.		x	
ITS-S-SEC	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.		x	

2.49.6 Decision Points Identified

ID	Component	Description
Decision 1		There is a central component within the C2X System network that further handles reports on misbehaviour detections.

2.49.7 External Activities Identified

ID	Group	Description

2.50 UC-SP2IVS-03

SP informs selected vehicles about the RWs and traffic conditions nearby

2.50.1 Assumptions

ID	Description
UC-SP2IVS-03-A1	OEM Backend is registered as recipient for road works warning messages issued by a certain service provider
UC-SP2IVS-03-A2	At the OEM Backend there is an incoming event alert service (IEA) available
UC-SP2IVS-03-A3	OEM Backend has available a contract relationship with a certain mobile network operator (MNO)
UC-SP2IVS-03-A4	The MNO offers the possibility to dissemminate message to communication end points based on geocast
UC-SP2IVS-03-A5	The OEM Backend has the security data (e.g. certificate, encryption key)

available (e.g. pre-loaded)
UC-SP2IVS-03-A6Each IVS has a geomessaging client installed and active
UC-SP2IVS-03-A7The IVS has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
UC-SP2IVS-03-A8OEM is termination point for its cellular connected vehicles
UC-SP2IVS-03-A9The Backend is already started.
UC-SP2IVS-03-A10All recieved messages can be new events or event updates which referes to old events.

2.50.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		The OEM hast registered itself for reception of RWW messages from TCs	
Prerequisite-2		There is at least on service provider (TC) that offers a RWW message service and has announced it	
Prerequisite-3		Each OEM Backend 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 (-> other user story)	
Prerequisite-4		Each OEM Backend 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-5		Each OEM Backend has a generic rule engine (RE) service running at its backend. The RE processes icoming events according to local policies.	
Prerequisite-6		A message about a RWW event has been received from the TC and been posted to the IEA of the OEM	

2.50.3 Actions Operational

From	To	Description	Optional
TC-UC	OEM-IEA	A message about a RWW has been received from the TC and been posted to the IEA	
OEM-IEA	OEM-GTL	The availability of the RWW message is logged at the OEM backend	

OEM-IEA	OEM-RE	The IEA informs the RE about the reception of a RWW message and triggers the further processing at the RE	
OEM-RE	OEM-RE	The RE decides that the received message should not be distributed	X
OEM-RE	OEM-RE	The RE decides that the received message has to be distributed	
OEM-RE	OEM-RE	Optional: In case the lifetime of the incoming message is beyond the local maximum "lifetime without validation" a "rule engine reminder" timer is set and the message is kept in an internal storage and if the time is expired, the OEM-RE Geocast Message is resent.	X
OEM-RE	MNO-GeoMS	The RE forwards the RWW message to the Geo messaging server (GeoMS) of its associated MNO(s).	
MNO-GeoMS	IVS-CUCel	The Geo-MS-MNO sends the RWW to all receivers of the OEM in the given target region.	
IVS-CUCel	IVS-FL	The cellular communication unit in the IVS forwards the message to the facility layer (IVS-FL) for futher processing	
OEM-RE	OEM-RE	The given time set in the timer for "lifetime without validation" for a given message is expired and the vlidation procedure is started	X

2.50.4 Actions Post-Operational

From	To	Description	Optional

2.50.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.50.6 Decision Points Identified

ID	Component	Description
UC-SP2IVS-03-DP1	OEM-RE	It have to be defined, when a message will be discarded.

UC-SP2IVS-03-DP2	OEM-RE	Threshold for the live time validation.

2.50.7 External Activities Identified

ID	Group	Description
UST-GeoCast		A mechanism has to be provided by the overall system that allows to transmit 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
UST-Sec		A mechanism has to be provided that allows to generate and distribute security data (keys, certificates) to all participants of the C2X-SN
UST-OEM-RWW-Setup		The detailed setup procedure for the RWW service at the OEM has to be described.
TC-BT		How will the TC be informed about RWW.
SP-LOG		Logging for SPs.
SP-BackendSUP		Description of the startup and shutdown routines of the all modules of the SP backend.
MSG-ID		Use case for generation of unique message ids for reference used in update messages.

2.51 UC-SP2IVS-04

A service provider (OEM Backend) sends a greeting message via Converge platformCar2X Services Network to a set of IVS (e.g. all IVS or a specific subset i.e. Opel) in a specific area).

2.51.1 Assumptions

ID	Description

2.51.2 Actions Pre-Operational

From	To	Description	Optional

2.51.3 Actions Operational

From	To	Description	Optional

2.51.4 Actions Post-Operational

From	To	Description	Optional

2.51.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.51.6 Decision Points Identified

ID	Component	Description

2.51.7 External Activities Identified

ID	Group	Description

2.52 UC-SP2SP-01_04

SP request more information about traffic condition in a specific area from another SP (See UC-SP2SP-01_01)

2.52.1 Assumptions

ID	Description

2.52.2 Actions Pre-Operational

From	To	Description	Optional

2.52.3 Actions Operational

From	To	Description	Optional

2.52.4 Actions Post-Operational

From	To	Description	Optional

2.52.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation

2.52.6 Decision Points Identified

ID	Component	Description

2.52.7 External Activities Identified

ID	Group	Description

2.53 UC-SP2SP-01_05

"SP response to requesting SP with more information about traffic condition in a specific area

Note: use case makes only sense in combination with UC-SP2SP-01_04 and needs to be defined accordingly, use case is NOT fully defined yet!!"

2.53.1 Assumptions

ID	Description
	AS#1SP has traffic conditions in a specific area
	AS#2SP#1 and SP#2 has a contractrual agreement in place

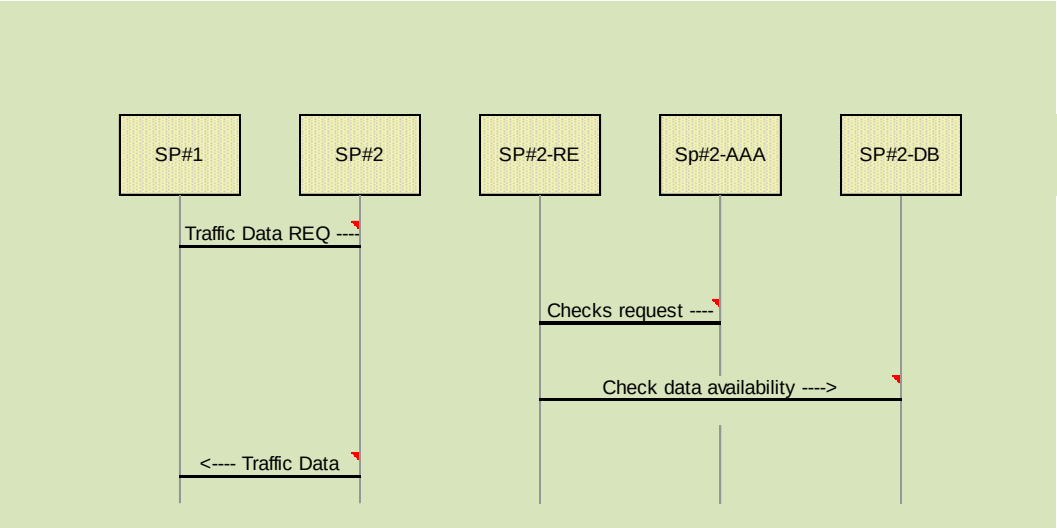
2.53.2 Actions Pre-Operational

From	To	Description	Optional

2.53.3 Actions Operational

From	To	Description	Optional

SP#1	SP#2	SP requests information about traffic condition in a specific area
SP#2-RE	Sp#2-AAA	RE checks eligibility of the rquest (authentication, etc.)
SP#2-RE	SP#2-DB	RE checks SP#2 own database for availability of requested data
SP#2	SP#1	SP#2 response to SP#1 with information in a specifc areayes [data]



2.53.4 Actions Post-Operational

From	To	Description	Optional

2.53.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
SP#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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.		x	
SP#2	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		x	

	the IVS/IRS/Smartphone or the Service Provider side.			
Sp#2-AAA	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.		x	
SP#2-DB	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 services/information. This can be inside the C2X-SN itself and/or 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	
SP#2-RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	

2.53.6 Decision Points Identified

ID	Component	Description

2.53.7 External Activities Identified

ID	Group	Description

2.54 UC-SP-03

Service Provider evaluates and validates the information coming from vehicles.This also includes that the authenticity of the message sender, the integrity and confidentiality of the data, non repudiation of the message, and pseudonymity of the vehicle are satisfied.

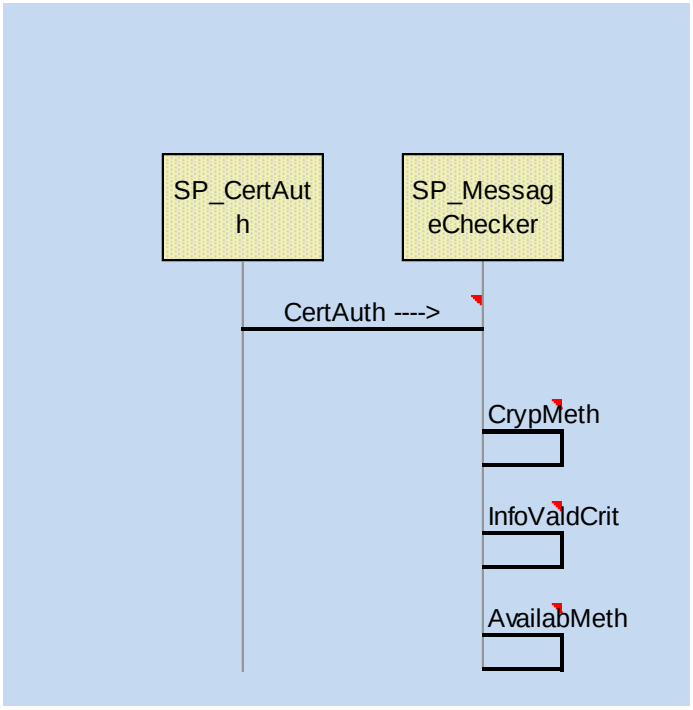
2.54.1 Assumptions

ID	Description
UC-SP-03_A1	A message from a vehicle is already received.

	UC-SP-03_A2A root certificate from a trusted authority is available as a base of trust in the certificate-chain
	UC-SP-03_A3The communication process fulfills the requirements for the pseudonymity for the sender.

2.54.2 Actions Pre-Operational

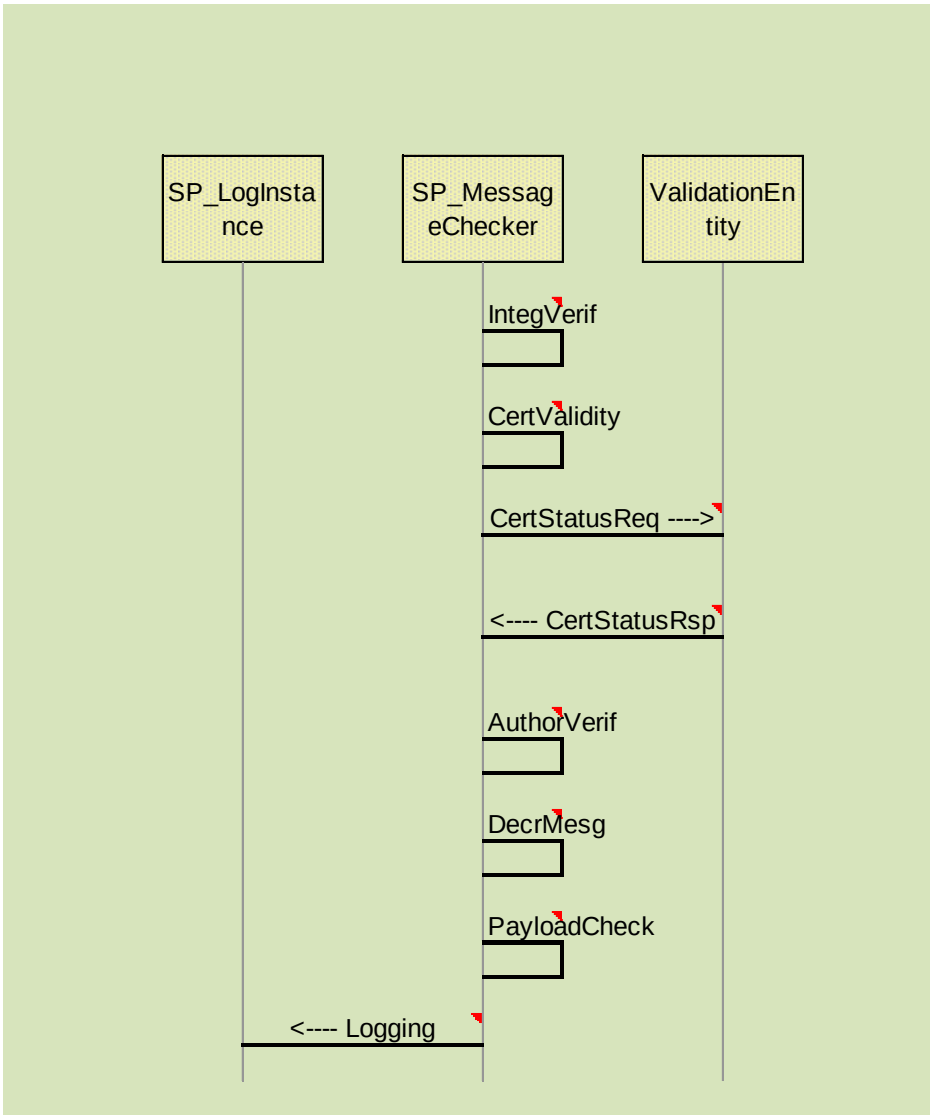
From	To	Description	Optional
SP_CertAuth	SP_MessageChecker	The root certificate has been received from the Certificate authority.	
SP_MessageChecker	SP_MessageChecker	The cryptografical methods to process a certain message of an specific type are known.	
SP_MessageChecker	SP_MessageChecker	The criteria for the evaluation of the payload (transmitted information) are defined.	
SP_MessageChecker	SP_MessageChecker	Methods to ensure the MessageCheckers availability are in place.	



2.54.3 Actions Operational

From	To	Description	Optional
SP_MessageChecker	SP_MessageChecker	The integrity of the message is verified.	
SP_MessageChecker	SP_MessageChecker	Verify the validity of the received certificate.	
SP_MessageChecker	ValidationEntity	Request (Certificate status - revoked/expired/valid/...)	

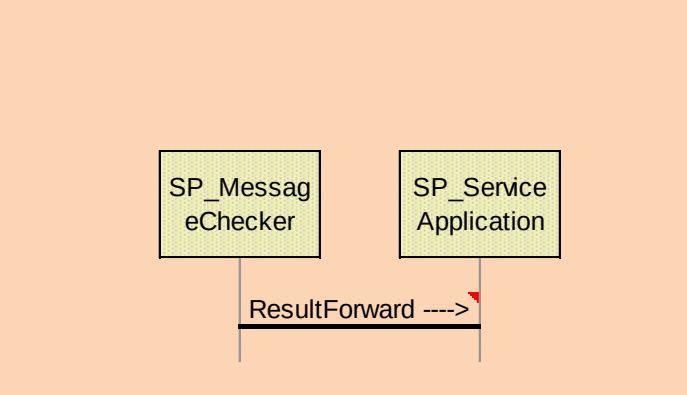
ValidationEntity	SP_MessageCheckerResponse (Certificate status)	
SP_MessageChecker	SP_MessageChecker	The authorization of the sender to send theX message is verified.
SP_MessageChecker	SP_MessageChecker	The cryptical methods are utilized to decrypt the messages payload (confidentialitiy).
SP_MessageChecker	SP_MessageChecker	The messages payload is evaluated according to the specified criteria.
SP_MessageChecker	SP_LogInstance	Log the received Message details, so that the non-repudiation criteria is fulfilled.



2.54.4 Actions Post-Operational

From	To	Description	Optional
SP_MessageChecker	SP_ServiceApplication	The data validation	

	result for the given message will be forwarded to the calling entity.



2.54.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
SP_CertAuth			x	
SP_LogInstance	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.			x
SP_MessageChecker	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.	x	x	x

SP_ServiceApplication	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.		x
ValidationEntity			x

2.54.6 Decision Points Identified

ID	Component	Description
UC_SP_03_DC_1	SP_MessageChecker	Methods to ensure service availability are in place.
UC_SP_03_DC_2	SP_MessageChecker	The call-hierarchy and the result propagation must be specified (especially which component calls the MessageChecker and which component receives the result).
UC_SP_03_DC_3	ValidationEntity	It has to be decided whether to verify a certificates status per direct request or by checking a certificate revocation list.

2.54.7 External Activities Identified

ID	Group	Description
UC_SP-03_EUS_1		A CONVERGE message must be specified with a certain message type. Such a message contains data description and data source.
UC_SP-03_EUS_2		The logging of data in a non-repudiation manner is needed. This has to define the log format, the information to be logging, the logging mechanism and storage of the logs, which guarantee, that the log cannot be tampered.

2.55 UC-C2X-102_02, UC-C2X-102_03, UC-C2X-102_04 combined

"An IVS/IRS downloads, checks & installs and activates the software for a (new) application. This is the combination of use cases UC-C2X-102_02/03/04.

Note: At least an interface is available which supports, if required, the download of application software by the (new) user of a serviceIf pseudonymous download is not allowed, privacy profile REQ-SEC-PP-006 would be required (might depend on the actual software).Only participants in a role with an appropriate authorization should be able to download the software.

Note: it is presumed, that SW update processes both at IVS/IRS and service provider are vendor specific and are to be defined by OEM/service provider. Only the procedures to check for and provide the appropriate sw packages from SP to IVS/IRS are defined here.
"

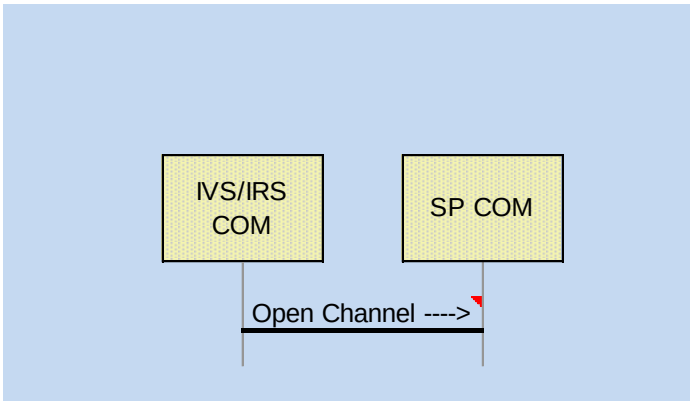
2.55.1 Assumptions

ID	Description
SW-Mgmt-AS01	IVS/IRS positively registered to SP (either self-registration or by OEM during manufacturing) for the associated service, in order to be eligible to receive SW update
SW-Mgmt-AS02	appropriate (i.e. compatible) SW object is stored at SP and has been tested to be working for specific type of service and specific IVS/IRS
SW-Mgmt-AS03	a mechanism exists inside IVS/IRS to perform all necessary steps to install new/updated SW onto itself
SW-Mgmt-AS04	a mechanism exists inside IVS/IRS to perform all necessary steps to initialise new/updated sw version
SW-Mgmt-AS05	a mechanism exists inside IVS/IRS to create a backup of an existing sw installation for the purpose of emergency fall-back in case of sw installation failure
REQ-SEC-PP-003	The C2X-SN provides a way to obtain an "authorized pseudonym" as described in REQ-SEC-PP-003 and the IVS/IRS has been allocated with such an identity.
REQ-SEC-PS-007	all messages between IVS/IRS contain a signature and are encrypted
REQ-SEC-PA-002	not applicable

2.55.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		IVS/IRS has positively registered itself to SP for the associated service, in order to be eligible to receive SW update	
Prerequisite-2		the SW management process has been started at SP and is available	
Prerequisite-3		a new/updated SW object is available at SP for download to IVS/IRS	

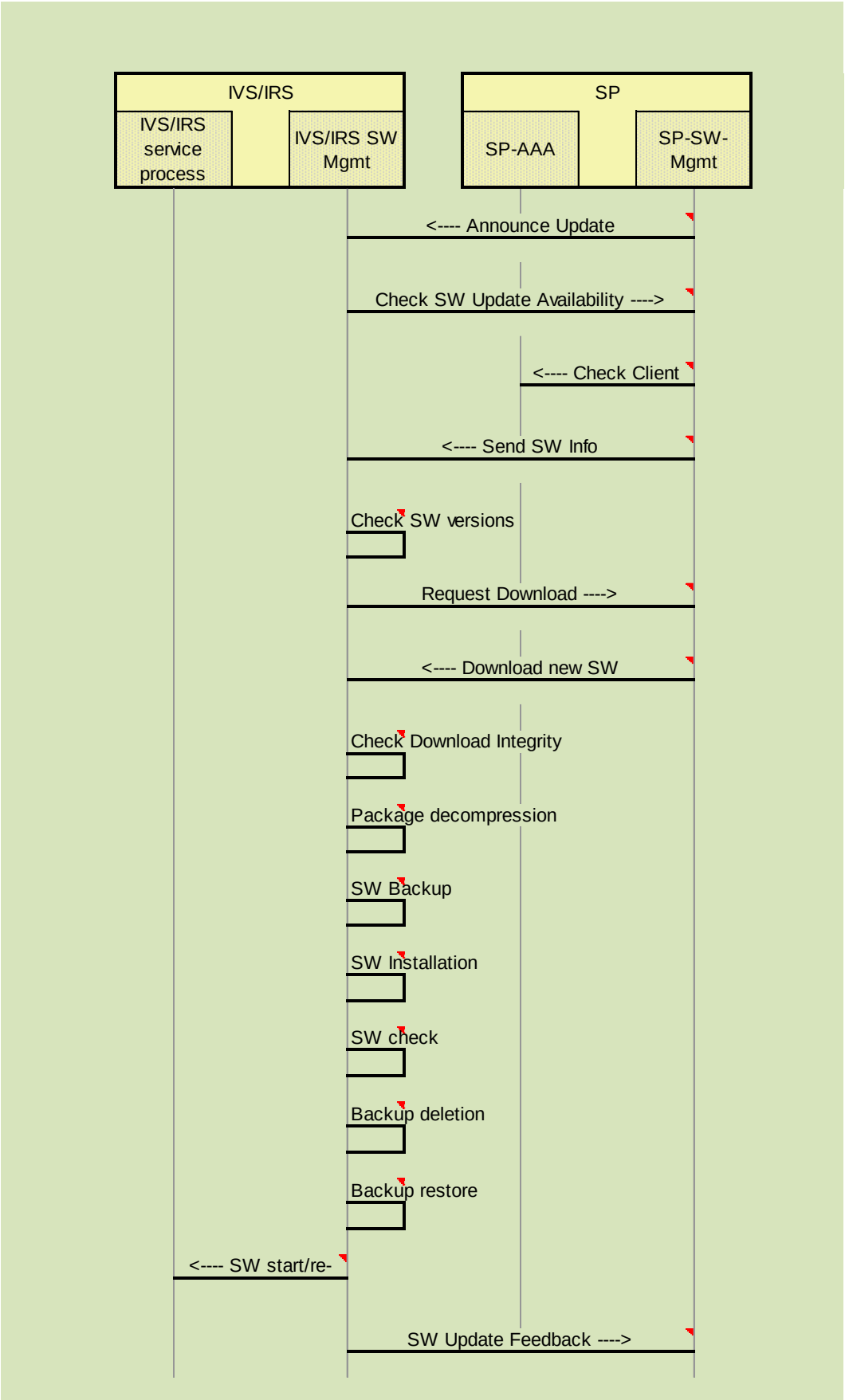
Prerequisite-4		compatibility of new SW version towards specific IVS/IRS type and service has been tested
Prerequisite-5		IVS/IRS has been initialised and has performed self-test
Prerequisite-6		the COM module of IVS/IRS is able to establish an appropriate channel towards SP according to required QoS, either via IST-G5 or mobile communications
Prerequisite-7		internal logging - including all sw management procedures inside IVS/IRS - has been started
IVS/IRS COM	SP COM	establish a safe communication channel between IVS/IRS and SP according to required QoS, this channel is to be used (by both SW-Mgmt. handlers of IVS/IRS and SP) for sw version check and possible sw download



2.55.3 Actions Operational

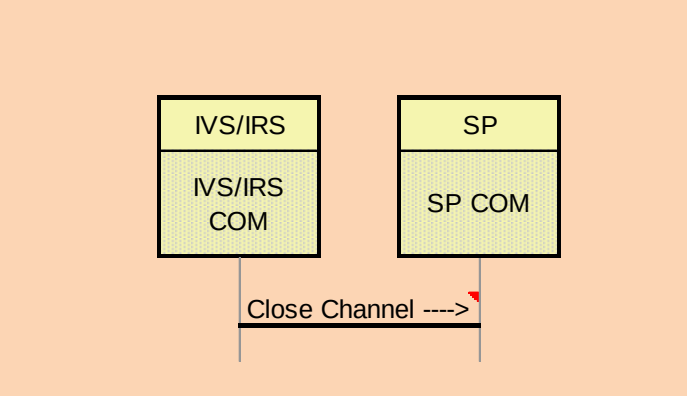
From	To	Description	Optional
SP-SW-Mgmt	IVS/IRS SW Mgmt	Optional: SP announces availability of new SW package	yes
IVS/IRS SW Mgmt	SP-SW-Mgmt	Request SP for actual SW version information for desired service [Identity(AuthPseud), ServiceId, ClientHwId, ClientSwVersion]	
SP-SW-Mgmt	SP-AAA	SP provider check eligibility of IVS/IRS to receive SW updates for requested service	
SP-SW-Mgmt	IVS/IRS SW Mgmt	SP provides information about actual SW versions and download packages for desired service [ServiceId, SwVersion, DownloadData(e.g. package size, download URL, compression info, encryption info, checksum, …)]	
IVS/IRS SW Mgmt	IVS/IRS SW Mgmt	IVS/IRS SW Mgmt. Handler compares client sw version with received info from SP and decides about update	

IVS/IRS Mgmt	SW	SP-SW-Mgmt		IVS/IRS SW Mgmt. Handler requests download of swyes package from SP [URL] (optional: only if update is required)	
SP-SW-Mgmt		IVS/IRS Mgmt	SW	SP sends SW package to IVS/IRS (optional: only if update is required)	
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. Handler checks integrity of download package e.g. via checksum (optional: only if update is required)	
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. Handler decompresses & decrypts downloaded installation package (if necessary)	
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. handler creates back-up of existing sw version for emergency fall-back	
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. Handler triggers internal sw update procedure	
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	IVS/IRS SW Mgmt. Handler checks integrity of installation (e.g. via checksums friom file system)	
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	if "SW check" successfull: IVS/IRS SW Mgmt. Handleryes deletes previously created backup of outdated sw version	
IVS/IRS Mgmt	SW	IVS/IRS Mgmt	SW	if "SW check" fails: IVS/IRS SW Mgmt. Handler restoresyes previously created backup of outdated sw version and disables/deletes downloaded package	
IVS/IRS Mgmt	SW	IVS/IRS service process		IVS/IRS SW Mgmt. Handler (re-)starts newly installed sw	
IVS/IRS Mgmt	SW	SP-SW-Mgmt		IVS/IRS gives feedback about SW update outcomeyes [ServiceId, HwId, authPseudonym, success/unsuccess, SWVersion]	


IVS/IRS
IVS/IRS service process
IVS/IRS SW Mgmt
SP
SP-AAA
SP-SW-Mgmt
<---- Announce Update
Check SW Update Availability ---->
<---- Check Client
<---- Send SW Info
Check SW versions
Request Download ---->
<---- Download new SW
Check Download Integrity
Package decompression
SW Backup
SW Installation
SW check
Backup deletion
Backup restore
<---- SW start/re-
SW Update Feedback ---->

2.55.4 Actions Post-Operational

From	To	Description	Optional
IVS/IRS COM	SP COM	Close prevoiously opened communication channel	



2.55.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
IVS/IRS COM	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.	x		x
IVS/IRS service process	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.		x	
IVS/IRS SW Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.		x	
SP COM	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.	x		x
SP-AAA	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.		x	

SP-SW-Mgmt	The SWM is responsible for all application installed on a device, including services, runtime environments, operating systems and firmware. There are different subtype like client (incl. installation), server, application repository, etc.		x	

2.55.6 Decision Points Identified

ID	Component	Description
DP-01	Announce Update	Decide if announcement of new SW version by SP is needed or if pull-only mechanism by IVS/IRS is preferred
DP-02	SW Backup	Is a backup of previously installed (older/working) sw version necessary before installation of new sw? What happens if sw install fails?
DP-03	general	It might be neccessary/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)
DP-04	SW start/re-start	Sind besondere Maßnahmen notwendig vor der Aktivierung der neuen SW? (z.B. nur in Werkstatt erlaubt, Triggerung nur manuell, …)

2.55.7 External Activities Identified

ID	Group	Description
US-01	IVS/IRS	Open Channel: use case to open a generic transport channel between IVS/IRS and SP
US-02	IVS/IRS	Registration of IVS/IRS for service
US-03	SP	SW management process at service provider including storage of new sw objects at SP and compatibility testing
US-04	IVS/IRS	cold start / initialisation of IVS/IRS components
US-05	IVS/IRS	IVS/IRS logging procedures
US-06	IVS/IRS	Close Channel: use case to open a generic transport channel between IVS/IRS and SP
US-07	SP	Check authorisation of client to obtain new sw, check signatures, identities, subscribed services, …
US-08	IVS/IRS	sw initialisation process (IVS/IRS vendor specific)

2.56 UC-C2X-103_01-03

"Old description: The Car2X Systems Network determines all available communication networks. (SP which are able to reach mobile nodes)

The Car2X Systems Network determines the status (e.g. availability, supported bandwidth, communication costs) of a selected communication network.

The Car2X Systems Network determines which communication network is best suited to provide the requested quality.

New Proposal:

A SP wants to know the possible recieving SPs/backends for a certain type of message/service (e.g. HessenMobil wants to distribute LHW messages and needs to know where to send these messages(other receiving SPs))

The Rule engine (RE) determines how to handle the message according to the criteria

Note: We assume that CN providers are a subset of a SP. That means that only the SP decides about the used means of communication towards its recepients. -> Reference: RWW User Story/Use-Case

Note: The Car2X Systems Network provides information on all available communication networks which can be used by the applications.

Postcondition: The party interested in knowing the available communication networks has all relevant information for further processing."

2.56.1 Assumptions

ID	Description
UC-C2X-103_01-03_A1	The C2X-SN provides a directory service, where all receiving SPs are registered
UC-C2X-103_01-03_A2	SP Backend is registered as recipient for a Service(e.g. road works warning messages) issued by a certain service provider
UC-C2X-103_01-03_A3	At the SP Backend there is an incoming event alert service (IEA) available
UC-C2X-103_01-03_A4	SP Backend has available a contract relationship with a certain Network Operator(e.g. mobile network operator (MNO))
UC-C2X-103_01-03_A5	The CN offers the possibility to dissemminate message to communication end points based on geocast

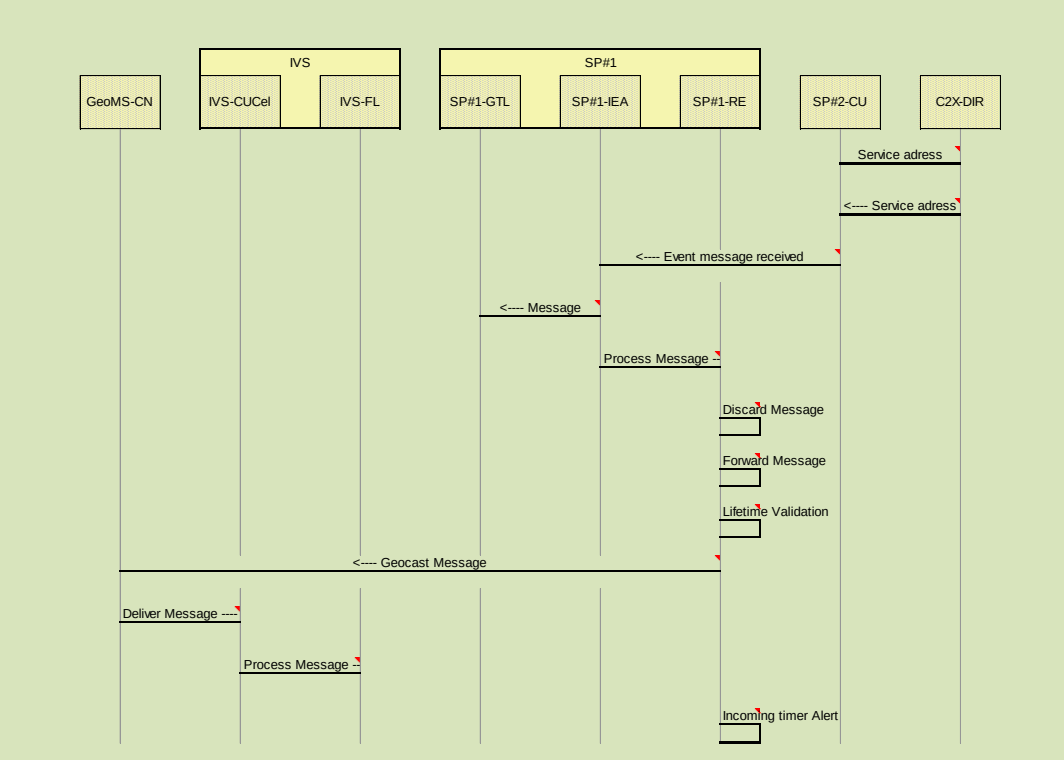
03_A6	UC-C2X-103_01-The SP Backend has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
03_A7	UC-C2X-103_01-Each IVS has a geomessaging client installed and active
03_A8	UC-C2X-103_01-The IVS has the security data (e.g. certificate, encryption key) available (e.g. pre-loaded)
03_A9	UC-C2X-103_01-The IVS shall observe the communication environment to identify the available access points and networks.
03_A10	UC-C2X-103_01-The IVS shall select the appropriate access point / network according to a predefined set of criteria (e.g. application, costs, contract, bandwidth, QoS, …).
03_A11	UC-C2X-103_01-The SP shall select the appropriate communication access point / network according to a predefined set of criteria (e.g. application, costs, contract, bandwidth, QoS, IVS access, availability, …).
03_A12	UC-C2X-103_01-**UNKNOWN!!**

2.56.2 Actions Pre-Operational

From	To	Description	Optional
Prerequisite-1		The SP#1(OEM) has registered itself for reception of Service messages from SP#2 (e.g.TCs)	
Prerequisite-2		There is at least one service provider (TC) that offers a message service and has announced it	
Prerequisite-3		Each SP Backend 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 (-> other user story)	
Prerequisite-4		Each SP Backend 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-5		Each SP Backend has a generic rule engine (RE) service running at its backend. The RE processes incoming events according to local policies.	
Prerequisite-6		A message about an event has been received from the SP#2 and been posted to the IEA	

2.56.3 Actions Operational

From	To	Description	Optional
SP#2-CU	C2X-DIR	SP requests other interested SPs from C2X-SN directory service	
C2X-DIR	SP#2-CU	C2X-SN directory provides interested SP communication endpoints	
SP#2-CU	SP#1-IEA	A message about an event has been received from the SP#2 and been posted to the IEA	
SP#1-IEA	SP#1-GTL	The availability of the event message is logged at the SP#1 backend	
SP#1-IEA	SP#1-RE	The IEA informs the RE about the reception of a event message and triggers the further processing at the RE	
SP#1-RE	SP#1-RE	The RE decides that the received message should not be distributed	
SP#1-RE	SP#1-RE	The RE decides that the received message has to be distributed	
SP#1-RE	SP#1-RE	Optional: In case the lifetime of the incoming message is beyond the local maximum "lifetime without validation" a "rule engine reminder" timer is set and the message is kept in an internal storage and if the time is expired, the OEM-RE Geocast Message is resent.	
SP#1-RE	GeoMS-CN	The RE forwards the event message to the Geo messaging server (GeoMS) of its associated MNO(s).	
GeoMS-CN	IVS-CUCel	The Geo-MS-MNO sends the event message to all receivers of the SP#1 in the given target region.	
IVS-CUCel	IVS-FL	The cellular communication unit in the IVS forwards the message to the facility layer (IVS-FL) for futher processing	
SP#1-RE	SP#1-RE	The given time set in the timer for "lifetime without validation" for a given message is expired and the vlidation procedure is started	



2.56.4 Actions Post-Operational

From	To	Description	Optional

2.56.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
GeoMS-CN	Server in the C2X-SN and/or SP and /or CN that distributes information to clients in a geographical area.		x	
IVS-CUCel	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.		x	
IVS-FL	Processing steps for messages inside an IVS/IRS, that are application independent (e.g. Message distribution or CAM creation)		x	

SP#1-GTL	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.		x	
SP#1-IEA	Running on all communication endpoint entities. It represents the SAP for all incoming messages.		x	
SP#1-RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	
SP#2-CU	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.		x	
C2X-DIR	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 services/information. This can be inside the C2X-SN itself and/or 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	

2.56.6 Decision Points Identified

ID	Component	Description
DP-01	general	new interpretation of use-case seems neccessary
DP-02		see also LHW/RWW use cases for decision points

2.56.7 External Activities Identified

ID	Group	Description
UST-GeoCast		A mechanism has to be provided by the overall system that allows to transmit 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
C2X-DIR		The directory service has to be provided by the overall system.
UST-ComCh	OEMs	Registration and establishment of the communication channel between IVS and the OEM Backend

UST-SPReg	OEMs	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)
UST-SPCM	C2X-SN	Contact mechanism to reach the C2X-SN Service Description (directory service) Service
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-IEA	SPs / OEMs	IEA mechanism at SP backends

2.57 UC-C2X-102_06 (130708_CONVERGE_SP_Client-lifecycle_mgmt)

SP-Alpha Client lifecycle mgmt

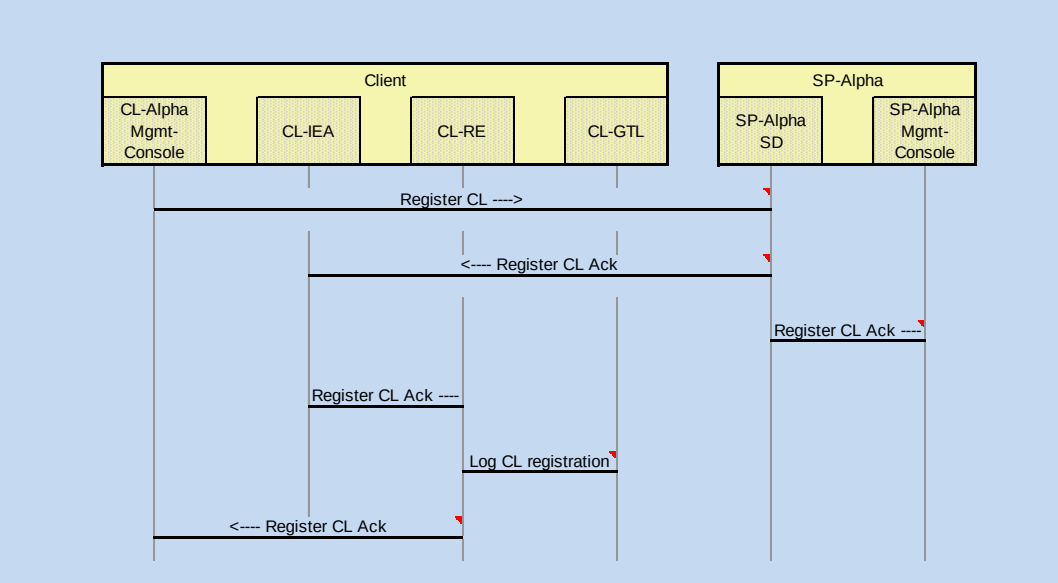
2.57.1 Assumptions

ID	Description

2.57.2 Actions Pre-Operational

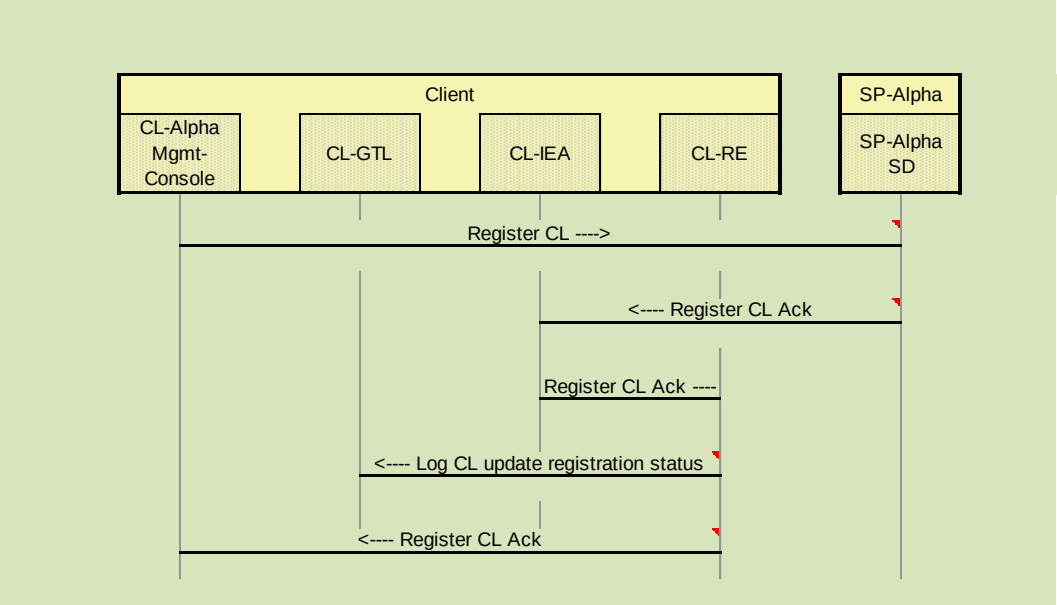
From	To	Description	Optional
Prerequisite#1		The Client CL-Alpha shall join the customer group of SP-Alpha as new member and therefore has estabished its "registration description". The Client registration description contains the following mandatory information sections: a) NAME: CL-Alpha (a unique CL-ID) b) CL class: e.g IVS of OEM-Alpha c) CL descrip: A human readable description of the CL nature d) Certificate: A CL certificate stating CL-Alpha has been granted SP-Alpha membership by an SP LegalBody (or manufacturing process body) after assessing its integrity e) CL-IEA: A Unique SW reference to the Client IEA access point (incoming communication access point at IVS or IRS) in the CL-to-SP-Alpha relationship Further optional information sections are: A) Geo-Area: A description of which geographic area is serviced by CL-Alpha (e.g. geo-serving area of an IRS)	
Prerequisite#2		Prior to executing the Client registration at SP-Alpha the CL-Alpha has obtained an electronic certificate to proof it is entitled to join the SP-Alpha client community as approved and integer member (see UC-C2X-101_03_02)	

Prerequisite#3		The SP-Alpha has an Alpha-CL-IEA service up an running and ready to be accessed from within the SP-Alpha Client community
Prerequisite#4		The SP-Alpha has a SP specific Mgmt-Console Server-Process available to initiatate and to visulalize all SP specific adminstratation activities.
Prerequisite#5		The SP-Alpha has a Client specific Rule-Engine CL-RE (SP-Alpha CL-RE) available to process all its Client events and to interact with the Alpha overall SP-RE (Alpha-RE, the one that is being concerned with C2X-SN communication).
Prerequisite#6		The SP-Alpha has a Client specific Global-Transaction-Logging service CL-GTL available to log all its Client events.
Prerequisite#7		The CL-Alpha has an CL-IEA service up an running and ready to be accessed from the SP-Alpha, serving as unique access point for communication to the Client.
Prerequisite#8		The CL-Alpha has a local Rule-Engine CL-RE available to process all its Client events.
Prerequisite#9		The CL-Alpha has a CL specific Mgmt-Console Server-Process available to initiatate and to visulalize all CL specific adminstratation activities.
CL-Alpha Mgmt-Console	SP-Alpha SD	Register CL-Alpha information with unique CL-Alpha ID name and with its CL description (see Pre#1) at the SP-Alpha service directory. As part of the CL description also the CL-IEA is being registered as confirmation address.
SP-Alpha SD	CL-IEA	Notify CL about registeration result.
SP-Alpha SD	SP-Alpha Mgmt-Console	Notify SP about CL registeration result.
CL-IEA	CL-RE	
CL-RE	CL-GTL	Log CL registration status result
CL-RE	CL-Alpha Mgmt-Console	Mark Status CL registration accordingly at the CL console process.



2.57.3 Actions Operational

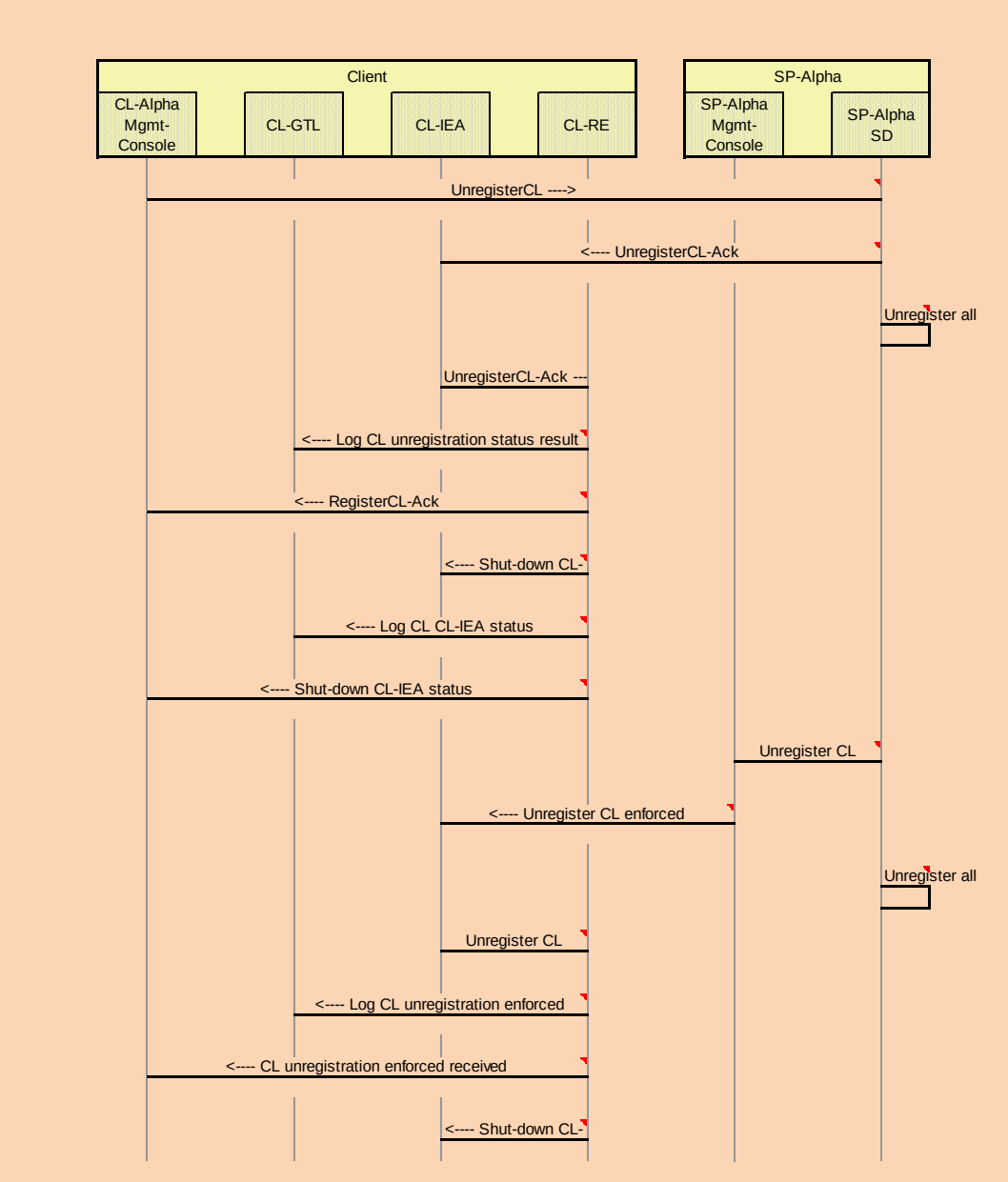
From	To	Description	Optional
Prerequisite#1		CL-Alpha has successfully registered itself at the SP-Alpha service directory. The SP-Alpha has a mgmt console service, a SP-Alpha CL-IEA, SP-Alpha CL-RE, and SP-Alpha CL-GTL service up and running	
Prerequisite#2		The CL-Alpha has a CL mgmt console service, a CL-IEA, CL-RE, and CL-GTL service up and running	
Prerequisite#3		An update (of any kind) to the CL-Alpha registration description shall be filed with the SP-Alpha Service Directory (including SP-Alpha Client devices). The update communication is initiated by the Client, e.g. as result of a CL SW update.	
CL-Alpha Mgmt-Console	SP-Alpha SD	Register CL-Alpha update-information with its (former) unique ID name and with its new CL description (see Pre#3) at the SP-Alpha service directory.	
SP-Alpha SD	CL-IEA	Notify about CL update registeration result.	
CL-IEA	CL-RE		
CL-RE	CL-GTL	Log CL update registration update status result	
CL-RE	CL-Alpha Mgmt-Console	Mark Update-Status CL registration accordingly at the CL console process.	



2.57.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#1		A Client (e.g. IVS, IRS) at SP-Alpha wants to unregister itself from the SP-Alpha and will terminate its accessability to the SP-Alpha afterwards. This is the controlled shut-down rather than a sudden CL death process.	
CL-Alpha Mgmt-Console	SP-Alpha SD	Unregister the Client at the SP-Alpha, using its corresponding unique CL name-ID and CL-IEA.	
SP-Alpha SD	CL-IEA	Notify Client about CL unregisteration result.	
SP-Alpha SD	SP-Alpha SD	Unregister all Client services and Alpha (Update Alpha internal DB).	
CL-IEA	CL-RE		
CL-RE	CL-GTL	Log CL unregistration status result	
CL-RE	CL-Alpha Mgmt-Console	Mark Status CL unregistration accordingly at the CL console process.	
CL-RE	CL-IEA	Shut down the CL-IEA	
CL-RE	CL-GTL	Log CL CL-IEA operation status after shut-down advise	
CL-RE	CL-Alpha Mgmt-Console	Mark Status CL-IEA shut-down status at Mgmt Console.	

SP-Alpha Mgmt-Console	SP-Alpha SD	Ultimately cut-off the Client from the SP-Alpha. Unregister the Client at the SP-Alpha, using its corresponding unique CL name-ID and CL-IEA.
SP-Alpha Mgmt-Console	CL-IEA	Ultimately cut-off the Client from the SP-Alpha. Unregister the Client at the SP-Alpha, using its corresponding unique CL name-ID and CL-IEA.
SP-Alpha SD	SP-Alpha SD	Unregister all Client services and Alpha (Update Alpha internal DB).
CL-IEA	CL-RE	Process Unregister CL enforced
CL-RE	CL-GTL	Log CL unregistration enforced received
CL-RE	CL-Alpha Mgmt-Console	CL unregistration enforced received
CL-RE	CL-IEA	Shut down the CL-IEA enforced



2.57.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
CL-Alpha Mgmt-Console	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 platform it is running.	X	X	X

CL-GTL	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x	x	x
CL-IEA	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
CL-RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.	x	x	x
SP-Alpha Mgmt-Console	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 platform it is running.	x		x
SP-Alpha 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 services/information. This can be inside the C2X-SN itself and/or 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	x

2.57.6 Decision Points Identified

ID	Component	Description

2.57.7 External Activities Identified

ID	Group	Description

2.58 UC-C2X-102_06 (130708_CONVERGE_C2X-SN_SP_Client-lifecycle_mgmt)

C2X-SN SP lifecycle mgmt

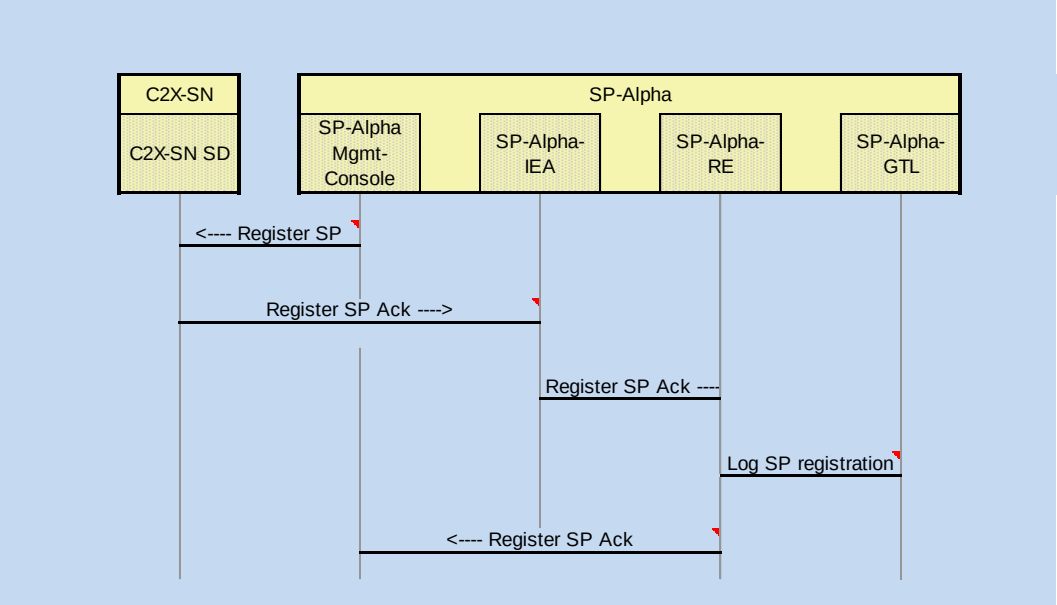
2.58.1 Assumptions

ID	Description

2.58.2 Actions Pre-Operational

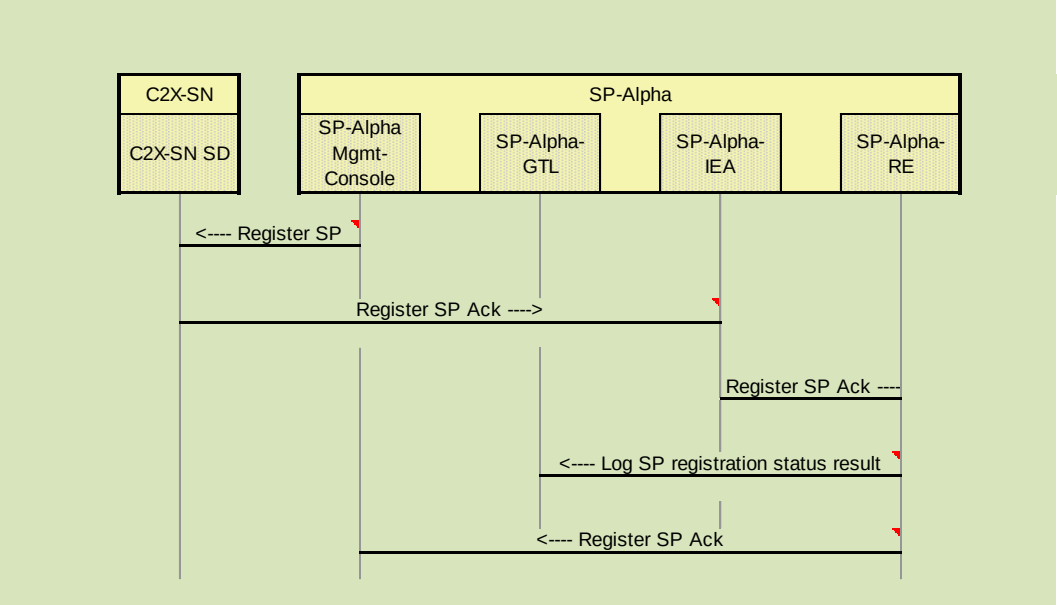
From	To	Description	Optional

Prerequisite#1		The SP-Alpha shall join the C2X-SN as new member and therefore has established its "registration description". This SP registration description contains the following mandatory information sections: a) NAME: SP-Alpha (a unique SP-ID) b) SP class: e.g. CommunicationChannel c) SP descrip: A human readable description of the SP nature d) Certificate: A SP certificate, stating SP-Alpha has been granted C2X-SN membership by an external LegalBody after assessing its integrity e) Alpha-IEA: A Unique SW reference to the C2X-SN-to-Alpha access point of SP-Alpha Further optional information sections are: A) Geo-Area: A description of which geographic area is being served by SP-Alpha
Prerequisite#2		Prior to executing the C2X-SN registration act the SP-Alpha has obtained an electronic certificate to proof it is entitled to join the C2X-SN as approved and integer member (see UC-C2X-101_01)
Prerequisite#3		The SP-Alpha has an Alpha-IEA service up an running and ready to be accessed from within the C2X-SN
Prerequisite#4		The SP-Alpha has a SP specific Mgmt-Console Server-Process (SP-Alpha Mgmt-Console) available to initiatate and to visulalize all SP specific adminstratation activities.
SP-Alpha Mgmt-Console	C2X-SN SD	Register SP-Alpha information with unique ID name and with it SP description (see Pre#1) at the C2X-SN service directory. As part of the SP description also the Alpha-IEA is being registered as confirmation address.
C2X-SN SD	SP-Alpha-IEA	Notify about registeration result.
SP-Alpha-IEA	SP-Alpha-RE	
SP-Alpha-RE	SP-Alpha-GTL	Log SP registration status result
SP-Alpha-RE	SP-Alpha Mgmt-Console	Mark Status SP registration accordingly at the SP console process.



2.58.3 Actions Operational

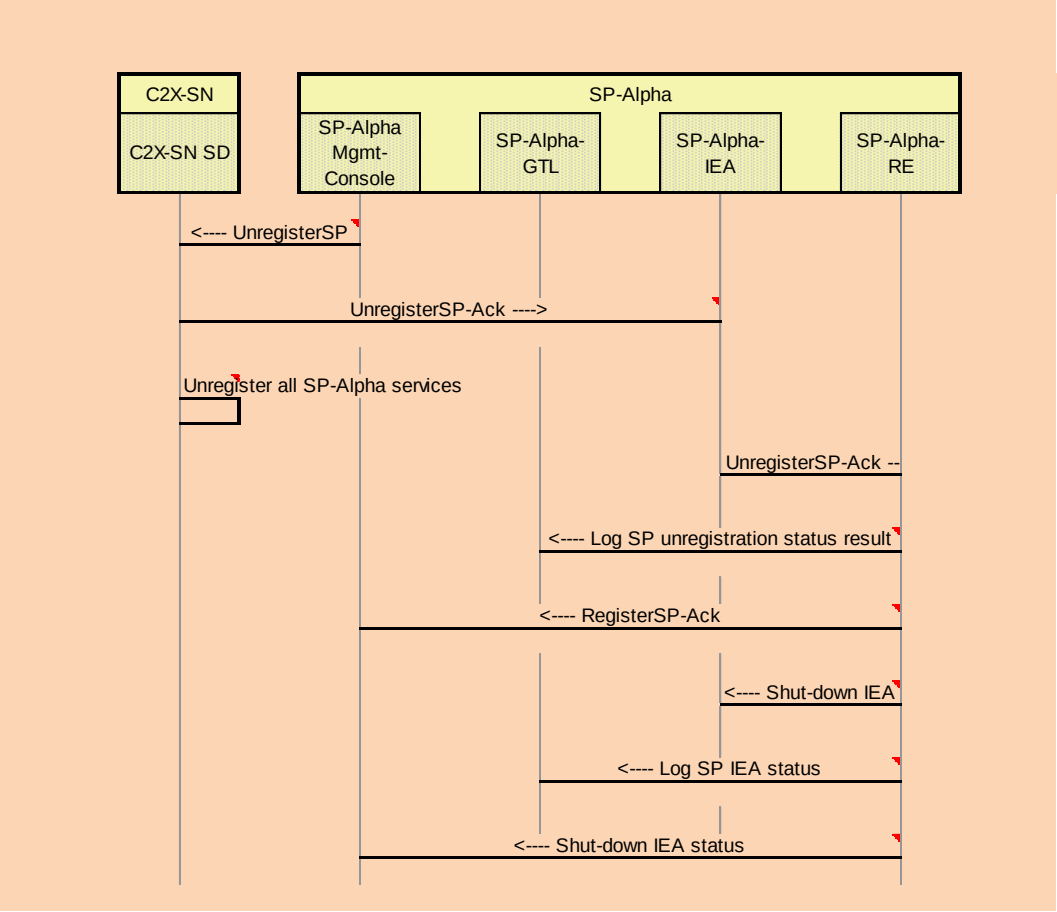
From	To	Description	Optional
Prerequisite#1		SP-Alpha has successfully registered itself at the C2X-SN, has a mgmt conole service, an IEA, RE, and GTL service for C2x-SN interactions up and running.	
Prerequisite#2		An update (of any kind) to the SP-Alpha registration description shall be filed with the C2X-SN directory service. A noticifation of this update shall be provided to ALL C2X-SN SPs afterwards.	
SP-Alpha Mgmt-Console	C2X-SN SD	Register SP-Alpha update-information with its (former) unique ID name and with its new SP description (see Pre#2) at the C2X-SN service directory.	
C2X-SN SD	SP-Alpha-IEA	Notify about registeration result.	
SP-Alpha-IEA	SP-Alpha-RE		
SP-Alpha-RE	SP-Alpha-GTL	Log SP registration update status result	
SP-Alpha-RE	SP-Alpha Mgmt-Console	Mark Update-Status SP registration accordingly at the SP console process.	



2.58.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#1		SP-Alpha wants to unregister itself from the C2X-SN and will terminate its accessability to the C2X-SN afterwards. This is the controlled shut-down rather than a sudden death process.	
SP-Alpha Mgmt-Console	C2X-SN SD	Unregister the service povider Alpha at the C2X-SN, using its corresponding unique SP name-ID and SP-Alpha-IEA.	
C2X-SN SD	SP-Alpha-IEA	Notify about the unregisteration result.	
C2X-SN SD	C2X-SN SD	Unregister all SP-Alpha-services (Update internal DB) and issue service update notifications to all C2X-SN service providers, according to their event notification filter setting.	
SP-Alpha-IEA	SP-Alpha-RE		
SP-Alpha-RE	SP-Alpha-GTL	Log SP unregistration status result	
SP-Alpha-RE	SP-Alpha Mgmt-Console	Mark Status SP unregistration accordingly at the SP console process.	
SP-Alpha-RE	SP-Alpha-IEA	Shut down the SP-Alpha-IEA	
SP-Alpha-RE	SP-Alpha-GTL	Log SP IEA operation status after shut-down advise	

SP-Alpha-RE	SP-Alpha Mgmt-Console	Mark Status SP IEA shut-down status at Mgmt Console.



2.58.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
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 services/information. This can be inside the C2X-SN itself and/or 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	x

SP-Alpha-Mgmt-Console	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 platform it is running.	x	x	x
SP-Alpha-GTL	A service that runs at each C2X-SN participant that is involved in the communication. This entity is responsible for the logging for security reasons (e.g. repudiation), fault management or billing constrains.	x	x	x
SP-Alpha-IEA	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
SP-Alpha-RE	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.	x	x	x

2.58.6 Decision Points Identified

ID	Component	Description

2.58.7 External Activities Identified

ID	Group	Description

2.59 UC-SP2SP2-01_02

SP informs all interested and authorized SPs about the traffic condition

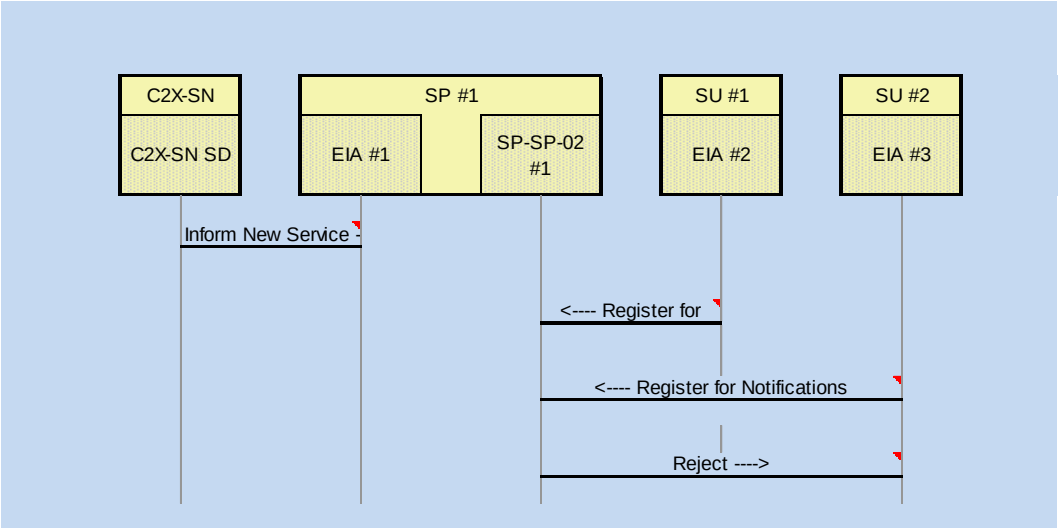
2.59.1 Assumptions

ID	Description
UC-SP2SP-01_02_A1	The communication channel between sending SP and the receiving SP have been registered and established.
UC-SP2SP-01_02_A2	The SP selects the most appropriate communication channel(s) for the message containing the additional information.
UC-SP2SP-01_02_A3	The SP has registered with C2X-SN as a "Service Provider" and hence has received a C2X-SN a permission certificate.
UC-SP2SP-01_02_A4	The SP has a data base that holds actual and accurate information about change in traffic condition.

2.59.2 Actions Pre-Operational

From	To	Description	Optional

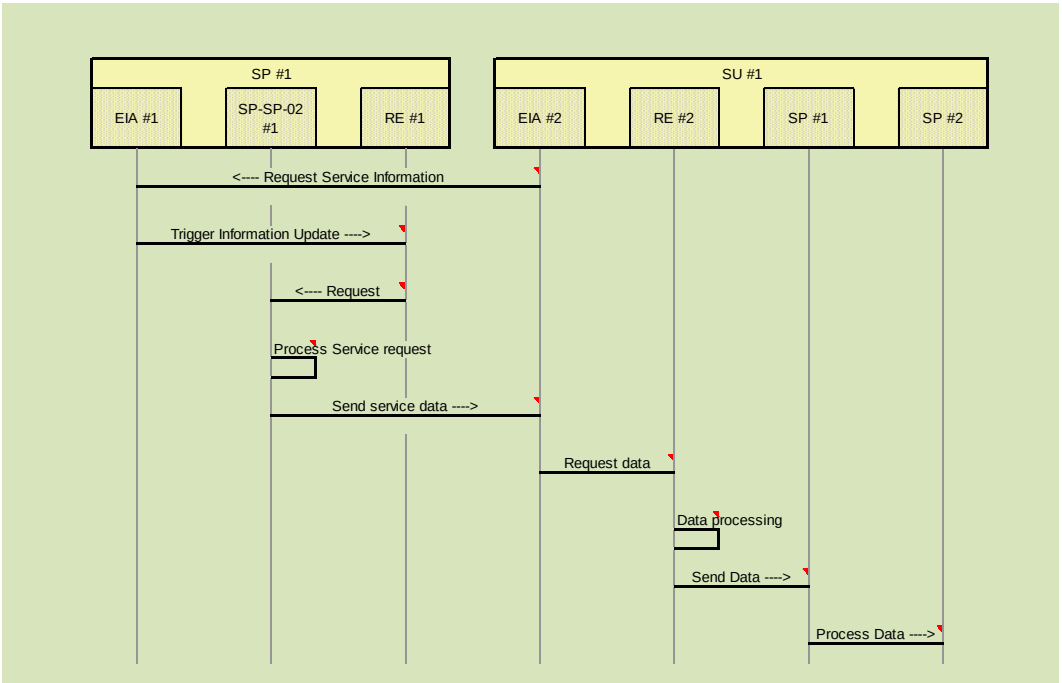
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions
EIA #2	SP-SP-02 #1	SU #1 EIA_#2 contacts SP-SP-02_#1, presenting its certificate APC_sn_SP-SP-02, to register itself as receiver of message notifications.
EIA #3	SP-SP-02 #1	SU #2 EIA_#3 contacts SP-SP-02_#1, presenting its certificate APC_sn_SP-SP-02, to register itself as receiver of message notifications.
SP-SP-02 #1	EIA #3	SP #1 SP-SP-02 #1 detects the invalidity of the certificate of SU #2 and rejects the registration



2.59.3 Actions Operational

From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the additional information has registered its SP-SP-02 service, attached its transaction logging service with its SP-SP-02 and is ready for service	
Prerequisite#8		Each service user that wants to use the SP-SP-02 service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	

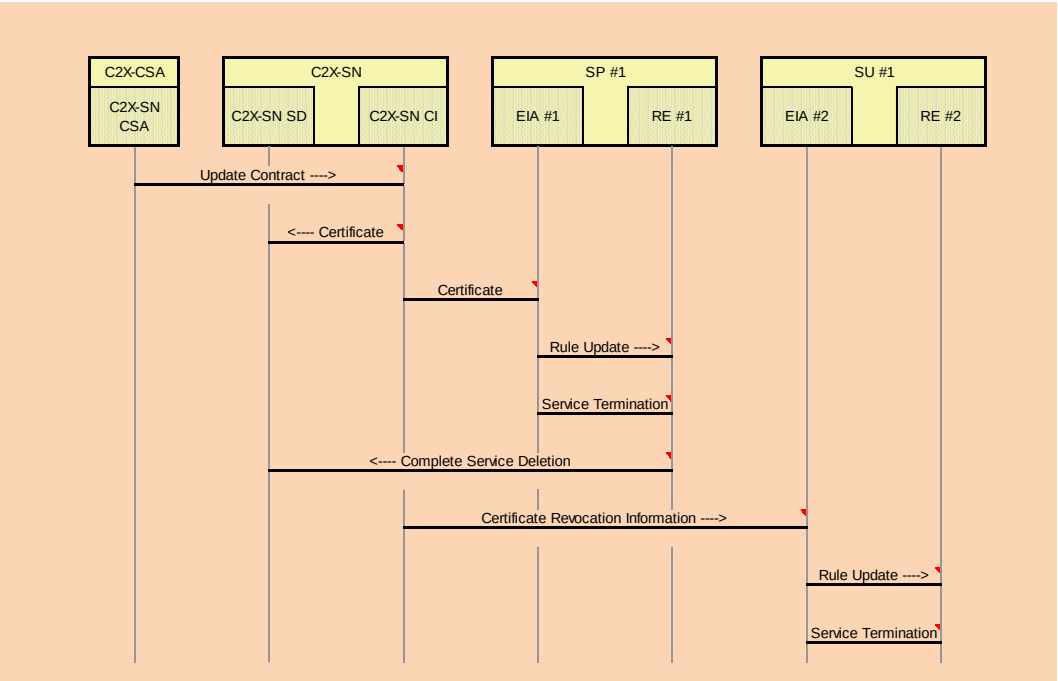
RE #1	SP-SP-02 #1	The rule engine is requesting the service module for SP-SP-02 #1 service to process the service request
SP-SP-02 #1	SP-SP-02 #1	The service module SP-SP-02 #1 is processing the service requestby checking the information received and retrieving information and further preparation of a service message that gives the necessary information to the service user
SP-SP-02 #1	EIA #2	The service module SP-SP-02 #1 is sending the preprocessed service information to the service user SU #1
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the SP-SP-02 #1 service and triggers the respective actions (e.g. Providing the data to the IVS)
RE #2	SP #1	The rule engine of SU #1 is sending the information derived from the service SP-SP-02 #1 to the respective SPs
SP #1	SP #2	The SPs that receive the information take further actions to e.g. inform the driver.



2.59.4 Actions Post-Operational

From	To	Description	Optional

Prerequisite#9		All SP-SP-02 and EIA services at SP #1, and SU #1 are ready to serve the next event
Prerequisite#10		SP #1 has terminated theSP-SP-02 contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only SP-SP-02 service provider left at the C2X-SN and decided to revoke that offer. Hence the SP-SP-02 service shall disappear as if it had never been launched
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SP-SP-02-2, associated with service SP-SP-02, has been activated, replacing certificate APC_sn_SP-SP-02-1
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_SP-SP-02 has been revoked. SP #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire SP-SP-02 service configuration and terminates SP-SP-02_#1
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SP-SP-02_#1 service offer
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_SP-SP-02 has been revoked. SU #1 updates its local certification management
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SP-SP-02 service configuration and terminates SP-SP-02_#1



2.59.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP-SP-02 #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.	x	x	
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.		x	
SP #2	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.		x	
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.59.6 Decision Points Identified

ID	Component	Description

2.59.7 External Activities Identified

ID	Group	Description

2.60 UC-SP2SP2-01_01

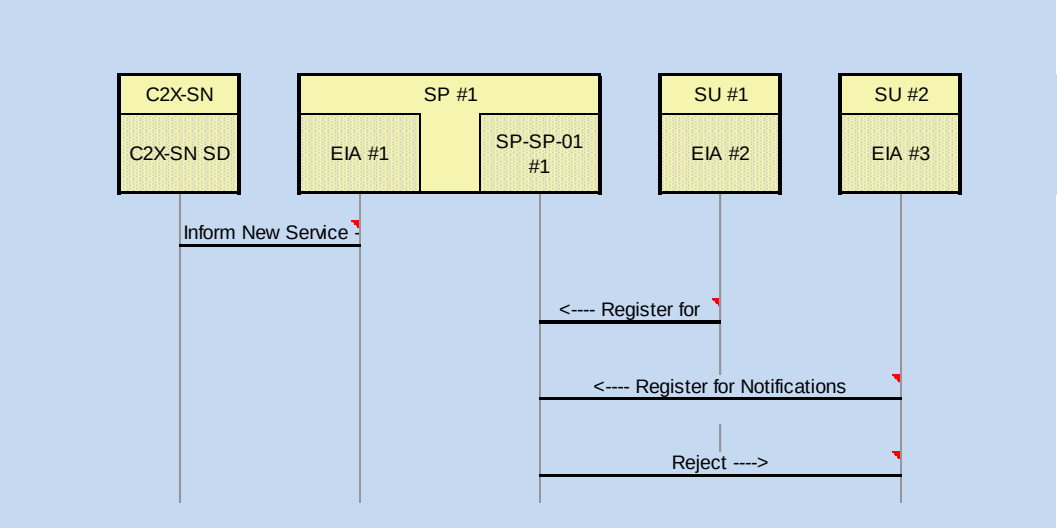
SP provides information about Road Works to other SPs

2.60.1 Assumptions

ID	Description
UC-SP2SP-01_01_A1	The communication channel between sending SP and the receiving SP have been registered and established.
UC-SP2SP-01_01_A2	The SP selects the most appropriate communication channel(s) for the message containing the additional information.
UC-SP2SP-01_01_A3	The SP has registered with C2X-SN as a "Service Provider" and hence has received a C2X-SN a permission certificate.
UC-SP2SP-01_01_A4	The SP has a data base that holds actual and accurate information about RW.

2.60.2 Actions Pre-Operational

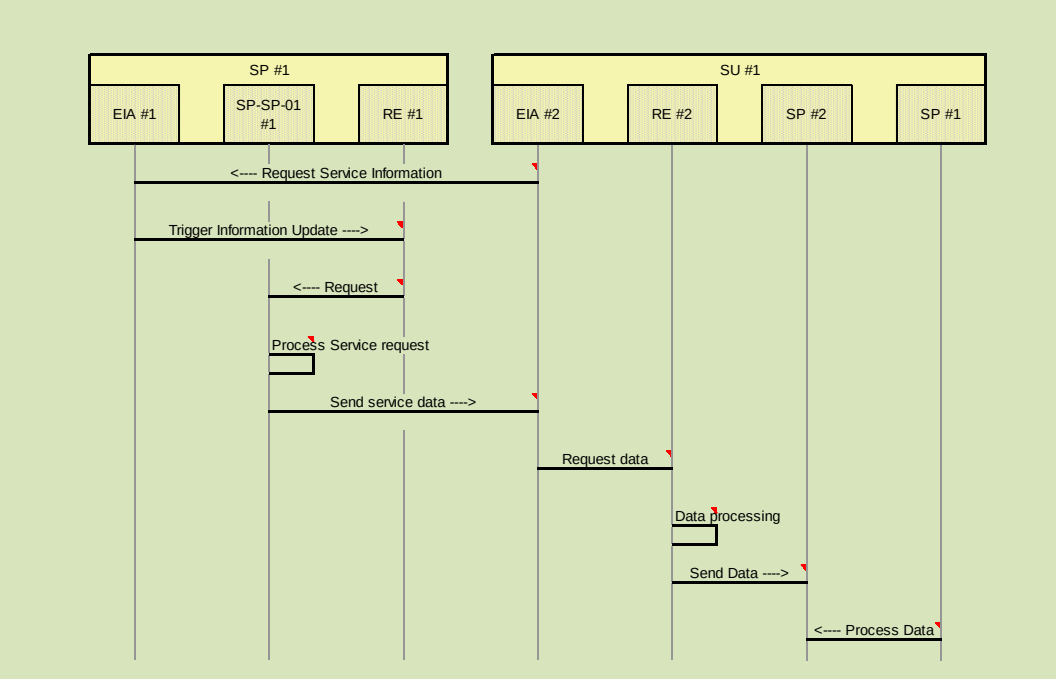
From	To	Description	Optional
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions	
EIA #2	SP-SP-01 #1	SU #1 EIA_#2 contacts SP-SP-01_#1, presenting its certificate APC_sn_SP-SP-01, to register itself as receiver of message notifications.	
EIA #3	SP-SP-01 #1	SU #2 EIA_#3 contacts SP-SP-01_#1, presenting its certificate APC_sn_SP-SP-01, to register itself as receiver of message notifications.	
SP-SP-01 #1	EIA #3	SP #1 SP-SP-01 #1 detects the invalidity of the certificate of SU #2 and rejects the registration	



2.60.3 Actions Operational

From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the additional information has registered its SP-SP-01 service, attached its transaction logging service with its SP-SP-01 and is ready for service	
Prerequisite#8		Each service user that wants to use the SP-SP-01 service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	
RE #1	SP-SP-01 #1	The rule engine is requesting the service module for SP-SP-01 #1 service to process the service request	
SP-SP-01 #1	SP-SP-01 #1	The service module SP-SP-01 #1 is processing the service requestby checking the information received and retrieving information and further preparation of a service message that gives the necessary information to the service user	
SP-SP-01 #1	EIA #2	The service module SP-SP-01 #1 is sending the preprocessed service information to the service user SU #1	
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2	

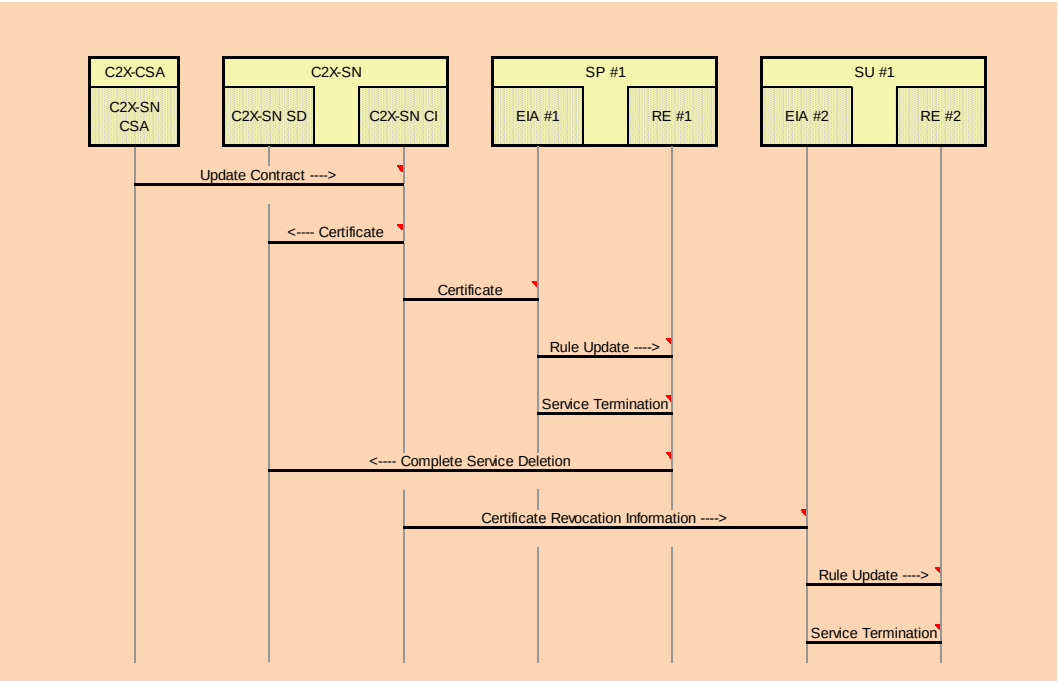
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the SP-SP-01 #1 service and triggers the respective actions (e.g. Providing the data to the IVS)
RE #2	SP #2	The rule engine of SU #1 is sending the information derived from the service SP-SP-01 #1 to the respective SPs
SP #1	SP #2	The SPs that receive the information take further actions to e.g. inform the driver.



2.60.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All SP-SP-01 and EIA services at SP #1, and SU #1 are ready to serve the next event	
Prerequisite#10		SP #1 has terminated theSP-SP-01 contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only SP-SP-01 service provider left at the C2X-SN and decided to revoke that offer. Hence the SP-SP-01 service shall disappear as if it had never been launched	
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SP-SP-01-2, associated with service SP-SP-01, has been activated, replacing certificate APC_sn_SP-SP-01-1
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_SP-SP-01 has been revoked. SP #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire SP-SP-01 service configuration and terminates SP-SP-01_#1
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SP-SP-01_#1 service offer
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_SP-SP-01 has been revoked. SU #1 updates its local certification management
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SP-SP-01 service configuration and terminates SP-SP-01_#1



2.60.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP-SP-01 #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.	x	x	
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.		x	
SP #2	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.		x	
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.60.6 Decision Points Identified

ID	Component	Description

2.60.7 External Activities Identified

ID	Group	Description

2.61 UC-SP2IVS-03

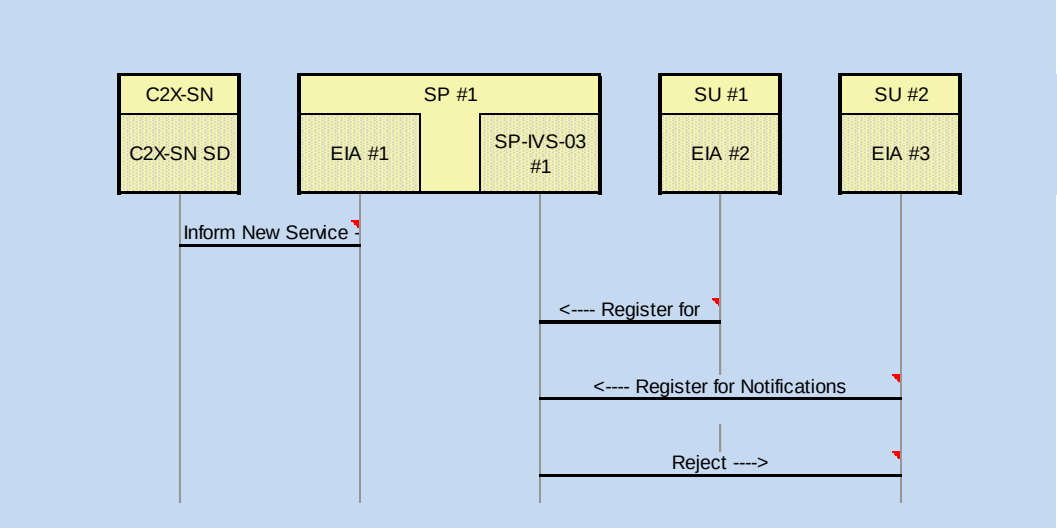
SP informs selected vehicles about the RWs and traffic conditions nearby

2.61.1 Assumptions

ID	Description
UC-SP2IVS-02_A1	The communication channel between sending SP and the receiving IVS have been registered and established.
UC-SP2IVS-02_A2	The SP selects the most appropriate communication channel(s) for the message containing the additional information. Sending the same message via different channels may be required.
UC-SP2IVS-02_A3	The SP has registered with C2X-SN as a "Service Provider" and hence has received a C2X-SN a permission certificate.
UC-SP2IVS-02_A4	The SP has a data base that holds actual and accurate information about change in traffic sign.

2.61.2 Actions Pre-Operational

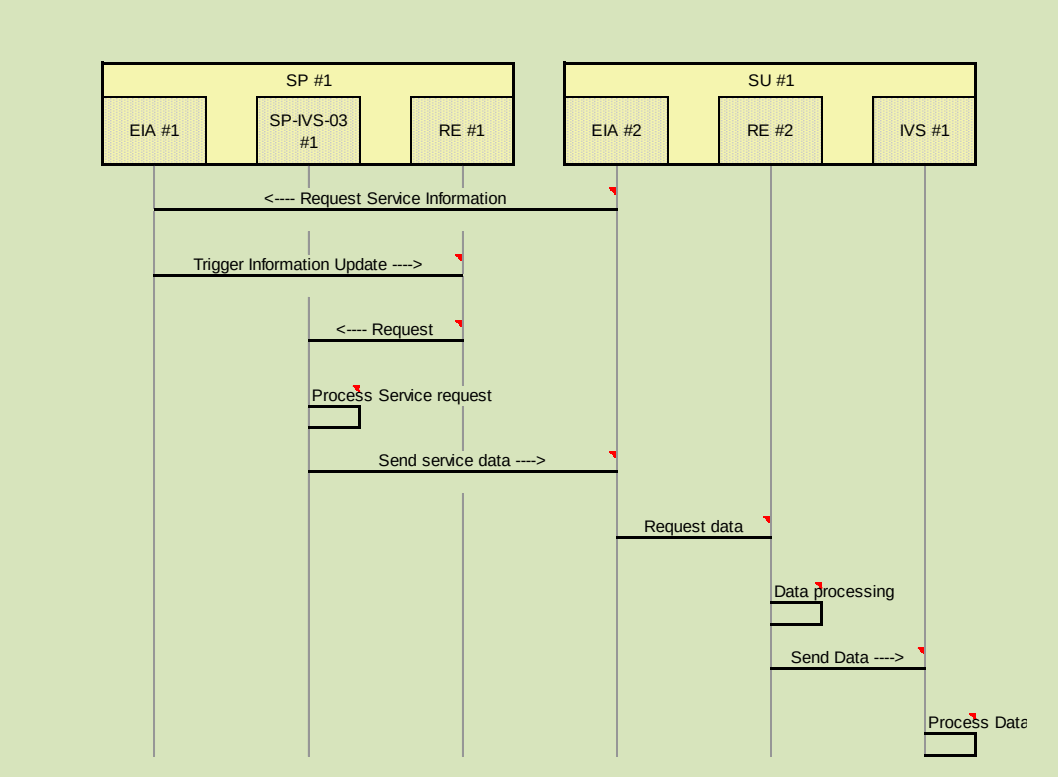
From	To	Description	Optional
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions	
EIA #2	SP-IVS-03 #1	SU #1 EIA_#2 contacts SP-IVS-03_#1, presenting its certificate APC_sn_SP-IVS-03, to register itself as receiver of message notifications.	
EIA #3	SP-IVS-03 #1	SU #2 EIA_#3 contacts SP-IVS-03_#1, presenting its certificate APC_sn_SP-IVS-03, to register itself as receiver of message notifications.	
SP-IVS-03 #1	EIA #3	SP #1 SP-IVS-03 #1 detects the invalidity of the certificate of SU #2 and rejects the registration	



2.61.3 Actions Operational

From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the additional information has registered its SP-IVS-03 service, attached its transaction logging service with its SP-IVS-03 and is ready for service	
Prerequisite#8		Each service user that wants to use the SP-IVS-03 service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	
RE #1	SP-IVS-03 #1	The rule engine is requesting the service module for SP-IVS-03 #1 service to process the service request	
SP-IVS-03 #1	SP-IVS-03 #1	The service module SP-IVS-03 #1 is processing the service requestby checking the information received and retrieving information and further preparation of a service message that gives the necessary information to the service user	
SP-IVS-03 #1	EIA #2	The service module SP-IVS-03 #1 is sending the preprocessed service information to the service user SU #1	
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2	

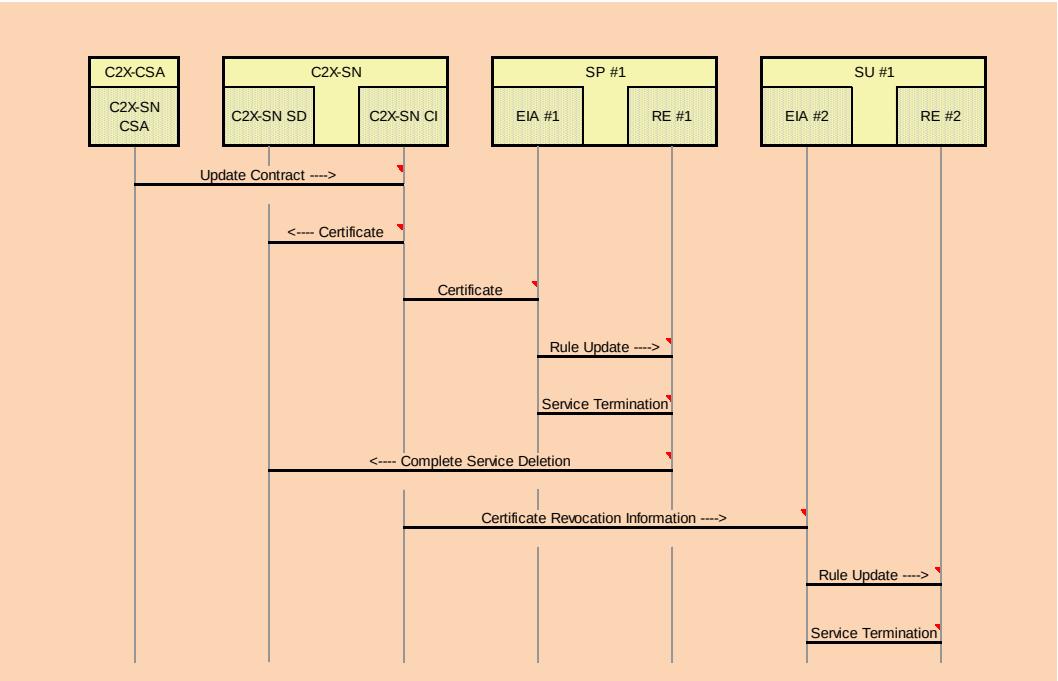
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the SP-IVS-03 #1 service and triggers the respective actions (e.g. Providing the data to the IVS)
RE #2	IVS #1	The rule engine of SU #1 is sending the information derived from the service SP-IVS-03 #1 to the respective IVSs
IVS #1	IVS #1	The IVSes that receive the information take further actions to e.g. inform the driver.



2.61.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All SP-IVS-03 and EIA services at SP #1, and SU #1 are ready to serve the next event	
Prerequisite#10		SP #1 has terminated theSP-IVS-03 contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only SP-IVS-03 service provider left at the C2X-SN and decided to revoke that offer. Hence the SP-IVS-03 service shall disappear as if it had never been launched	

C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SP-IVS-03-2, associated with service SP-IVS-03, has been activated, replacing certificate APC_sn_SP-IVS-03-1
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_SP-IVS-03 has been revoked. SP #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire SP-IVS-03 service configuration and terminates SP-IVS-03_#1
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SP-IVS-03_#1 service offer
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_SP-IVS-03 has been revoked. SU #1 updates its local certification management
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SP-IVS-03 service configuration and terminates SP-IVS-03_#1



2.61.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP-IVS-03 #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.	x	x	
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
IVS #1			x	
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.61.6 Decision Points Identified

ID	Component	Description

2.61.7 External Activities Identified

ID	Group	Description

2.62 UC-SP2IVS-02

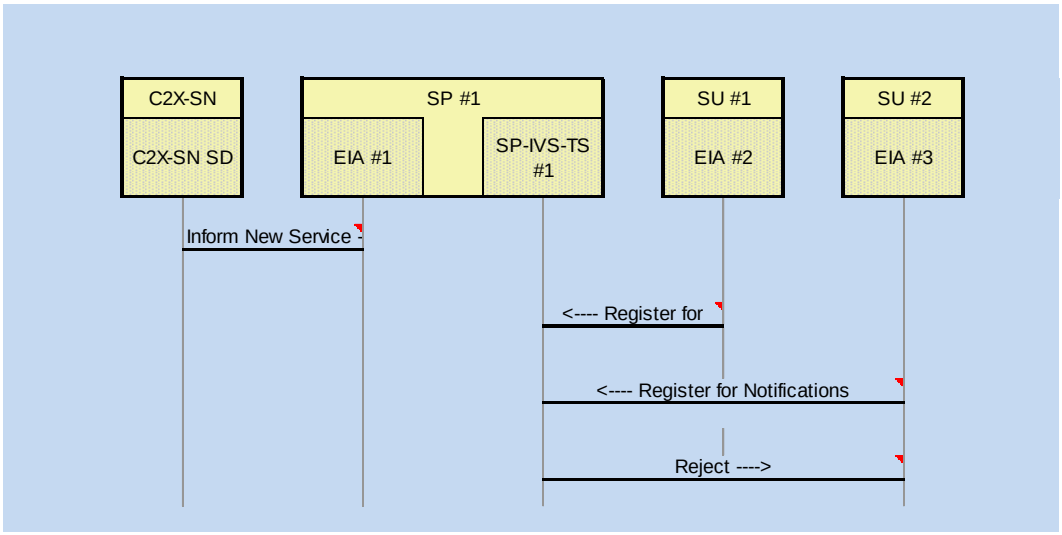
SP informs selected vehicles about the change in traffic sign (see UC-SP2IVS-01)

2.62.1 Assumptions

ID	Description
UC-SP2IVS-02_A1	The communication channel between sending SP and the receiving IVS have been registered and established.
UC-SP2IVS-02_A2	The SP selects the most appropriate communication channel(s) for the message containing the additional information. Sending the same message via different channels may be required.
UC-SP2IVS-02_A3	The SP has registered with C2X-SN as a "Service Provider" and hence has received a C2X-SN a permission certificate.
UC-SP2IVS-02_A4	The SP has a data base that holds actual and accurate information about change in traffic sign.

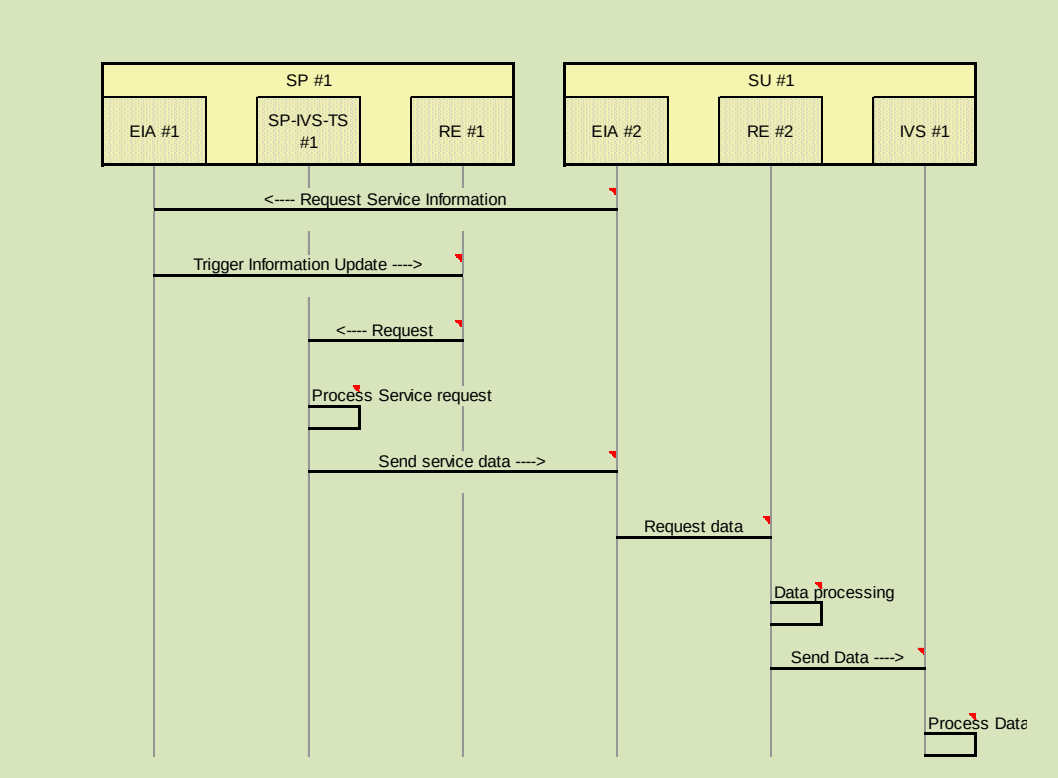
2.62.2 Actions Pre-Operational

From	To	Description	Optional
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions	
EIA #2	SP-IVS-TS #1	SU #1 EIA_#2 contacts SP-IVS-TS_#1, presenting its certificate APC_sn_SP-IVS-TS, to register itself as receiver of message notifications.	
EIA #3	SP-IVS-TS #1	SU #2 EIA_#3 contacts SP-IVS-TS_#1, presenting its certificate APC_sn_SP-IVS-TS, to register itself as receiver of message notifications.	
SP-IVS-TS #1	EIA #3	SP #1 SP-IVS-TS #1 detects the invalidity of the certificate of SU #2 and rejects the registration	



2.62.3 Actions Operational

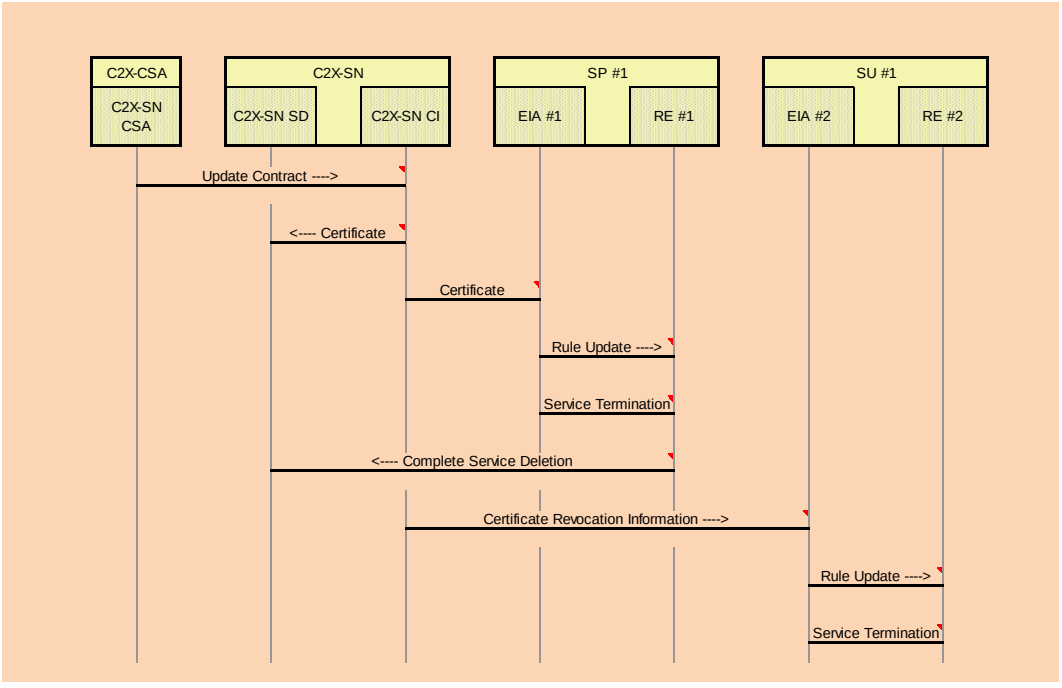
From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the additional information has registered its SP-IVS-TS service, attached its transaction logging service with its SP-IVS-TS and is ready for service	
Prerequisite#8		Each service user that wants to use the SP-IVS-TS service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	
RE #1	SP-IVS-TS #1	The rule engine is requesting the service module for SP-IVS-TS #1 service to process the service request	
SP-IVS-TS #1	SP-IVS-TS #1	The service module SP-IVS-TS #1 is processing the service requestby checking the information received and retrieving information and further preparation of a service message that gives the necessary information to the service user	
SP-IVS-TS #1	EIA #2	The service module SP-IVS-TS #1 is sending the preprocessed service information to the service user SU #1	
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2	
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the SP-IVS-TS #1 service and triggers the respective actions (e.g. Providing the data to the IVS)	
RE #2	IVS #1	The rule engine of SU #1 is sending the information derived from the service SP-IVS-TS #1 to the respective IVSs	
IVS #1	IVS #1	The IVSes that receive the information take further actions to e.g. inform the driver.	



2.62.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All SP-IVS-TS and EIA services at SP #1, and SU #1 are ready to serve the next event	
Prerequisite#10		SP #1 has terminated theSP-IVS-TS contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only SP-IVS-TS service provider left at the C2X-SN and decided to revoke that offer. Hence the SP-IVS-TS service shall disappear as if it had never been launched	
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SP-IVS-TS-2, associated with service SP-IVS-TS, has been activated, replacing certificate APC_sn_SP-IVS-TS-1	

C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_SP-IVS-TS has been revoked. SP #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire SP-IVS-TS service configuration and terminates SP-IVS-TS_#1
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SP-IVS-TS_#1 service offer
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_SP-IVS-TS has been revoked. SU #1 updates its local certification management
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SP-IVS-TS service configuration and terminates SP-IVS-TS_#1



2.62.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP-IVS-TS #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.	x	x	
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
IVS #1			x	

RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.62.6 Decision Points Identified

ID	Component	Description

2.62.7 External Activities Identified

ID	Group	Description

2.63 UC-SP2IVS-01

SP informs selected vehicles about the RWs

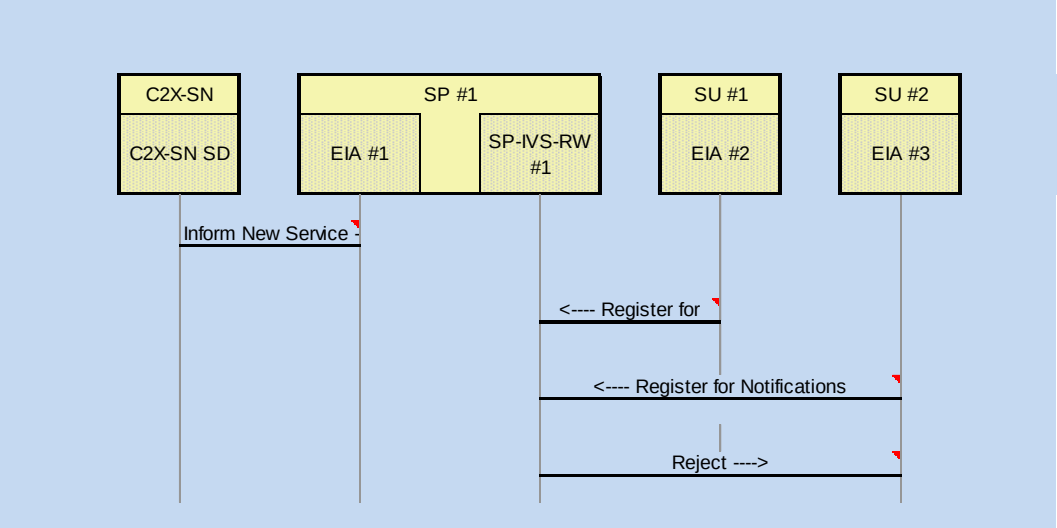
2.63.1 Assumptions

ID	Description
UC-SP2IVS-01_A1	The communication channel between sending SP and the receiving IVSes in the geographical area of reference have been registered and established.
UC-SP2IVS-01_A2	The SP selects the most appropriate communication channel(s) for the message containing the additional information. Sending the same message via different channels may be required.
UC-SP2IVS-01_A3	The SP has registered with C2X-SN as a "Service Provider" and hence has received a C2X-SN a permission certificate.
UC-SP2IVS-01_A4	The SP has a data base that holds actual and accurate information about RWW in the area of intereested.

2.63.2 Actions Pre-Operational

From	To	Description	Optional
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions	
EIA #2	SP-IVS-RW #1	SU #1 EIA_#2 contacts SP-IVS-RW_#1, presenting its certificate APC_sn_SP-IVS-RW, to register itself as receiver of message notifications.	

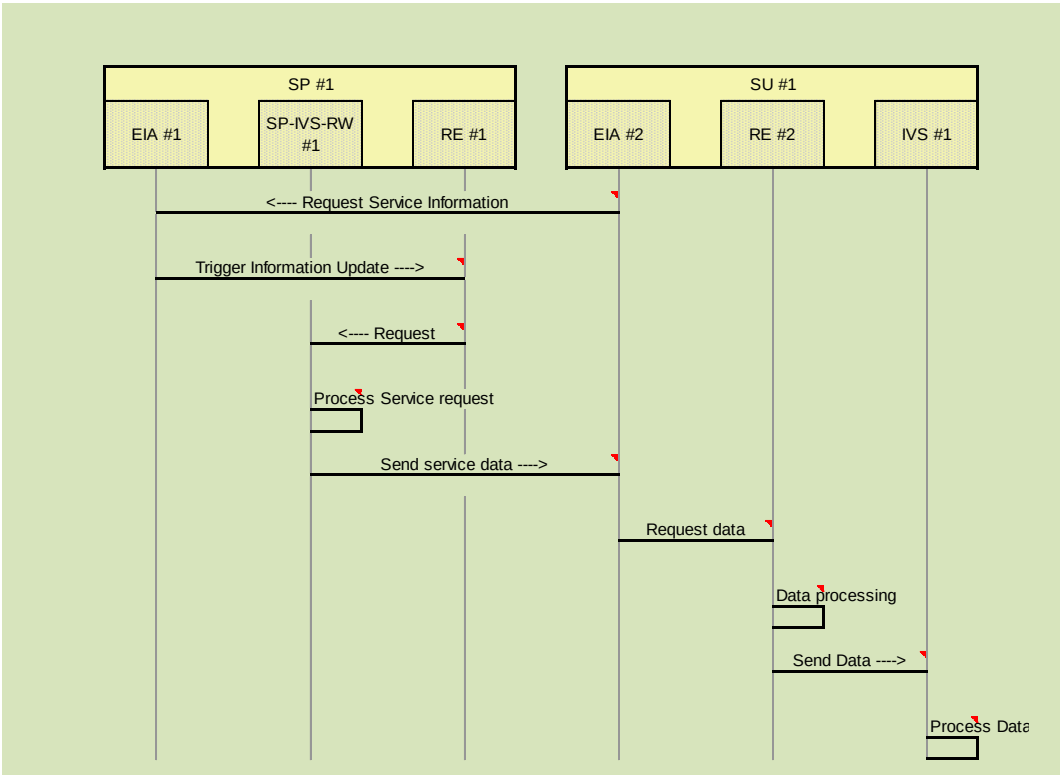
EIA #3	SP-IVS-RW #1	SU #2 EIA_#3 contacts SP-IVS-RW_#1, presenting its certificate APC_sn_SP-IVS-RW, to register itself as receiver of message notifications.
SP-IVS-RW #1	EIA #3	SP #1 SP-IVS-RW #1 detects the invalidity of the certificate of SU #2 and rejects the registration



2.63.3 Actions Operational

From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the additional information has registered its SP-IVS-RW service, attached its transaction logging service with its SP-IVS-RW and is ready for service	
Prerequisite#8		Each service user that wants to use the SP-IVS-RW service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	
RE #1	SP-IVS-RW #1	The rule engine is requesting the service module for SP-IVS-RW #1 service to process the service request	
SP-IVS-RW #1	SP-IVS-RW #1	The service module SP-IVS-RW #1 is processing the service requestby checking the information received and retrieving information and further preparation of a service message that gives the necessary information to the service user	

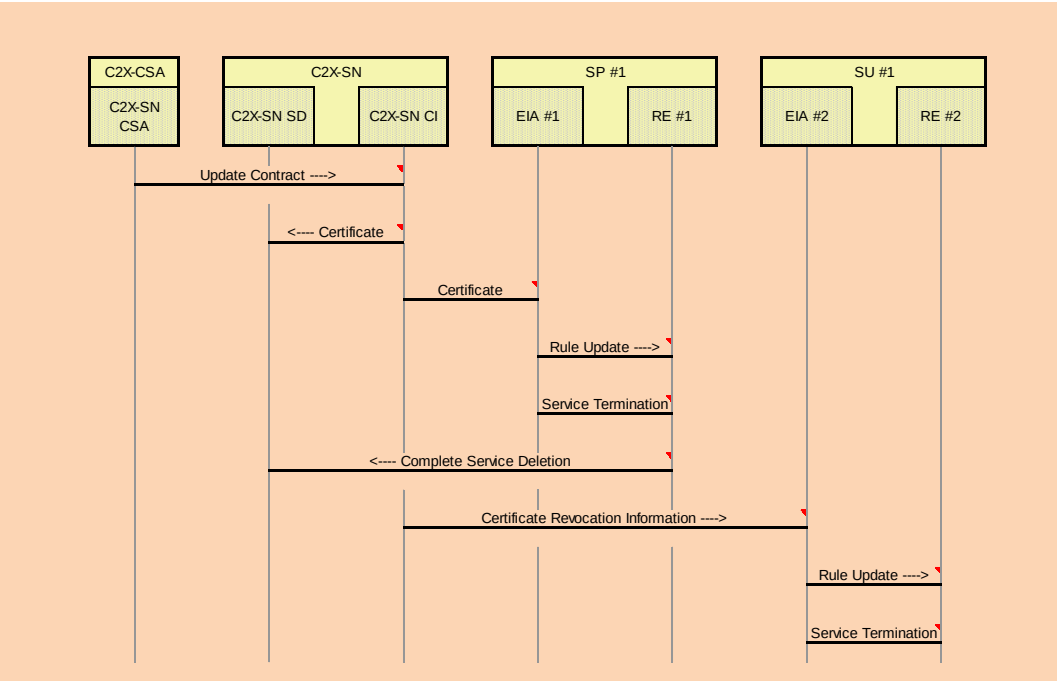
SP-IVS-RW #1	EIA #2	The service module SP-IVS-RW #1 is sending the preprocessed service information to the service user SU #1
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the SP-IVS-RW #1 service and triggers the respective actions (e.g. Providing the data to the IVS)
RE #2	IVS #1	The rule engine of SU #1 is sending the information derived from the service SP-IVS-RW #1 to the respective IVSs
IVS #1	IVS #1	The IVSes that receive the information take further actions to e.g. inform the driver.



2.63.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All SP-IVS-RW and EIA services at SP #1, and SU #1 are ready to serve the next event	

Prerequisite#10		SP #1 has terminated theSP-IVS-RW contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only SP-IVS-RW service provider left at the C2X-SN and decided to revoke that offer. Hence the SP-IVS-RW service shall disappear as if it had never been launched
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SP-IVS-RW-2, associated with service SP-IVS-RW, has been activated, replacing certificate APC_sn_SP-IVS-RW-1
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_SP-IVS-RW has been revoked. SP #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire SP-IVS-RW service configuration and terminates SP-IVS-RW_#1
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SP-IVS-RW_#1 service offer
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_SP-IVS-RW has been revoked. SU #1 updates its local certification management
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SP-IVS-RW service configuration and terminates SP-IVS-RW_#1



2.63.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP-IVS-RW #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.	x	x	
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
IVS #1			x	
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.63.6 Decision Points Identified

ID	Component	Description

2.63.7 External Activities Identified

ID	Group	Description

2.64 UC-SP2IRS-01

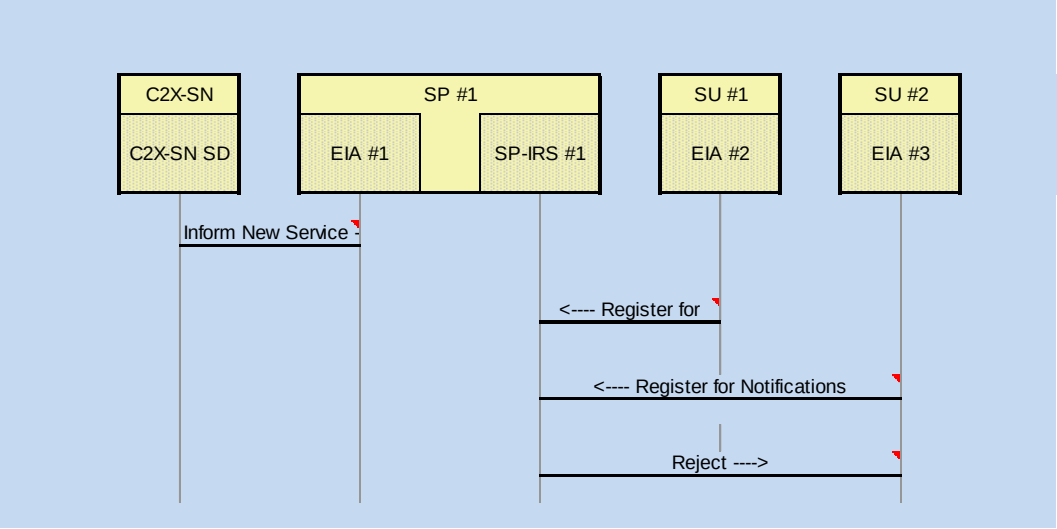
Service provider provides additional information to IRS (e.g. at a blocking trailer), which was not available before (e.g. blocked lanes, duration of the Road Works, speed limits and topology)

2.64.1 Assumptions

ID	Description
UC-SP2IRS-01_A1	The communication channel between sending SP and the receiving IRS have been registered and established.
UC-SP2IRS-01_A2	The SP selects the most appropriate communication channel(s) for the message containing the additional information. Sending the same message via different channels may be required.
UC-SP2IRS-01_A3	The SP has registered with C2X-SN as a "Service Provider" and hence has received a C2X-SN a permission certificate.
UC-SP2IRS-01_A4	The SP has a data base that holds actual and accurate additional information for IRS.

2.64.2 Actions Pre-Operational

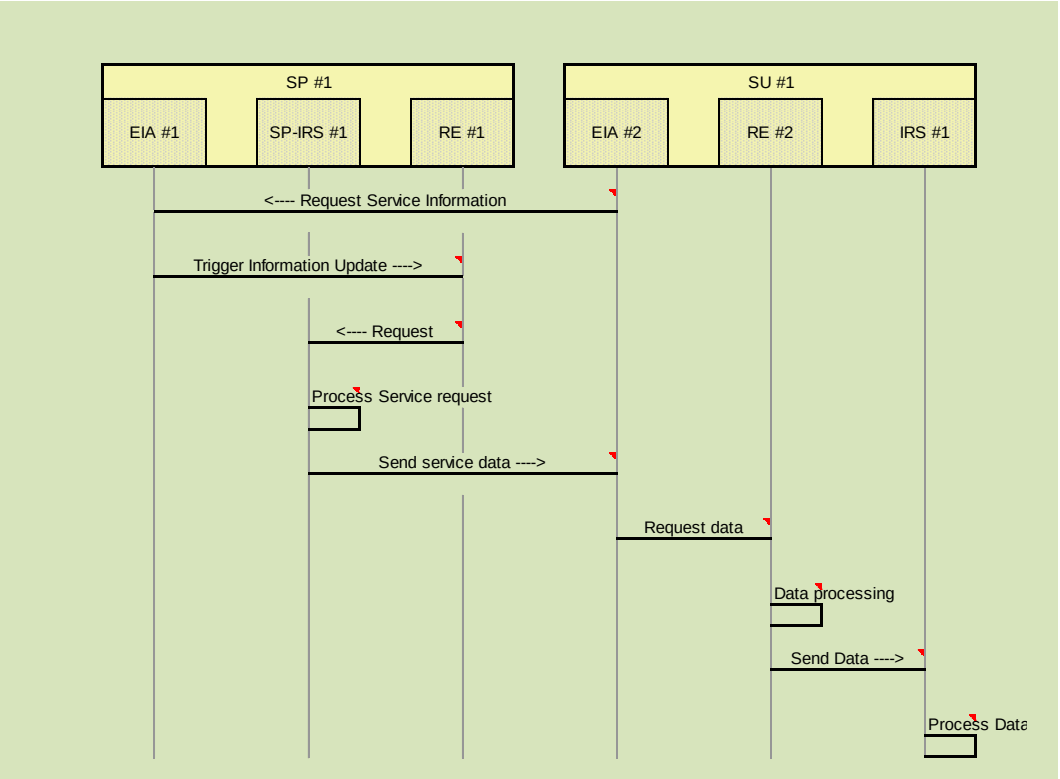
From	To	Description	Optional
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions	
EIA #2	SP-IRS #1	SU #1 EIA_#2 contacts SP-IRS_#1, presenting its certificate APC_sn_SP-IRS, to register itself as receiver of message notifications.	
EIA #3	SP-IRS #1	SU #2 EIA_#3 contacts SP-IRS_#1, presenting its certificate APC_sn_SP-IRS, to register itself as receiver of message notifications.	
SP-IRS #1	EIA #3	SP #1 SP-IRS #1 detects the invalidity of the certificate of SU #2 and rejects the registration	



2.64.3 Actions Operational

From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the additional information has registered its SP-IRS service, attached its transaction logging service with its SP-IRS and is ready for service	
Prerequisite#8		Each service user that wants to use the SP-IRS service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	
RE #1	SP-IRS #1	The rule engine is requesting the service module for SP-IRS #1 service to process the service request	
SP-IRS #1	SP-IRS #1	The service module SP-IRS #1 is processing the service requestby checking the information received and retrieving information and further preparation of a service message that gives the necessary information to the service user	
SP-IRS #1	EIA #2	The service module SP-IRS #1 is sending the preprocessed service information to the service user SU #1	
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2	

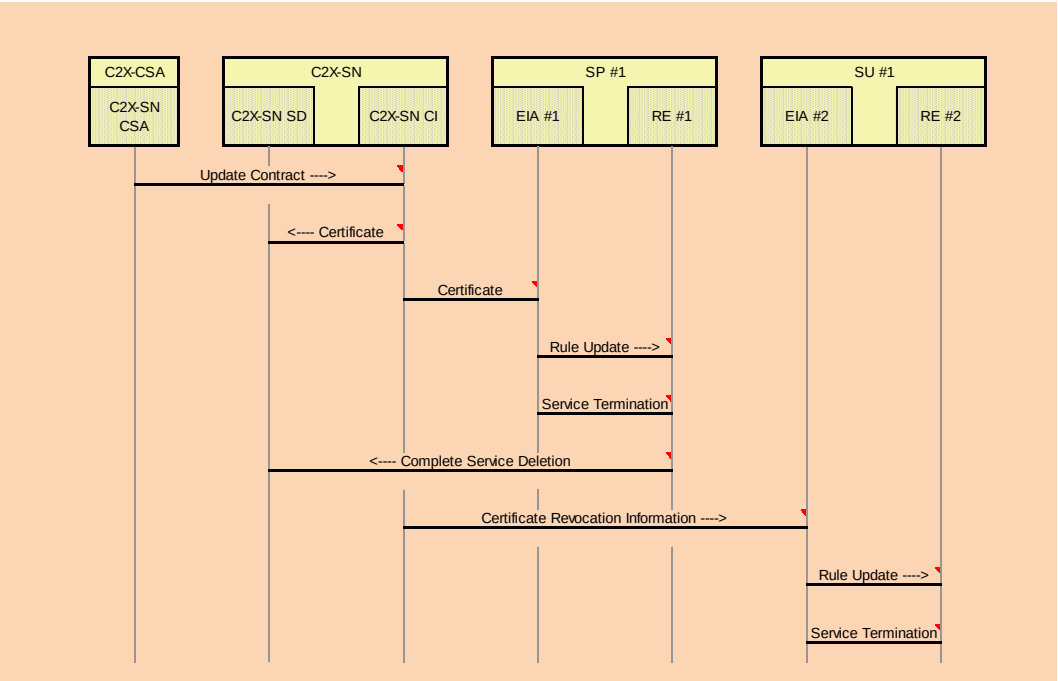
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the SP-IRS #1 service and triggers the respective actions (e.g. Providing the data to the IVS)
RE #2	IRS #1	The rule engine of SU #1 is sending the information derived from the service SP-IRS #1 to the respective IVSs
IRS #1	IRS #1	The IRSes that receive the information take further actions to e.g. inform the driver.



2.64.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All SP-IRS and EIA services at SP #1, and SU #1 are ready to serve the next event	
Prerequisite#10		SP #1 has terminated theSP-IRS contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only SP-IRS service provider left at the C2X-SN and decided to revoke that offer. Hence the SP-IRS service shall disappear as if it had never been launched	
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SP-IRS-2, associated with service SP-IRS, has been activated, replacing certificate APC_sn_SP-IRS-1
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_SP-IRS has been revoked. SP #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire SP-IRS service configuration and terminates SP-IRS_#1
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SP-IRS_#1 service offer
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_SP-IRS has been revoked. SU #1 updates its local certification management
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SP-IRS service configuration and terminates SP-IRS_#1



2.64.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP-IRS #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.	x	x	
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
IRS #1	The mobile "user" of a service, can be an vehicle or a mobile phone		x	
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.64.6 Decision Points Identified

ID	Component	Description

2.64.7 External Activities Identified

ID	Group	Description

2.65 UC-SP2ComNet-01

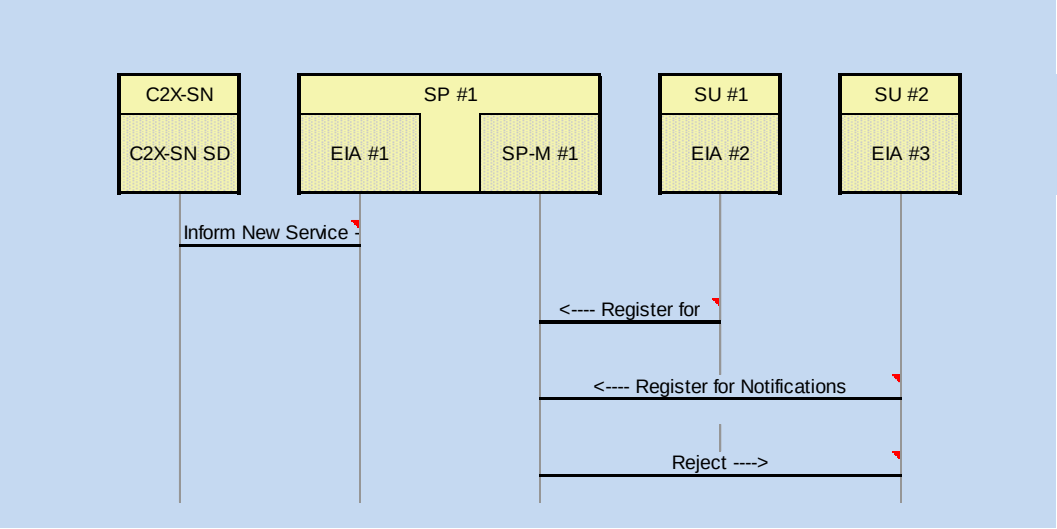
Sending message to the communication partner in the destination area by the SP

2.65.1 Assumptions

ID	Description
UC-SP2ComNet-01_A1	The communication channel between sending SP and the communication partners in the destination area have been registered and established.
UC-SP2ComNet-01_A2	The SP selects the most appropriate communication channel(s) for the given message. Sending the same message via different channels may be required.
UC-SP2ComNet-01_A3	The SP has registered with C2X-SN as a "Service Provider" and hence has received a C2X-SN a permission certificate.
UC-SP2ComNet-01_A4	The SP has a data base that holds actual and accurate information about current communication partners (e.g. V-ITS-S) in the desired destaination area.

2.65.2 Actions Pre-Operational

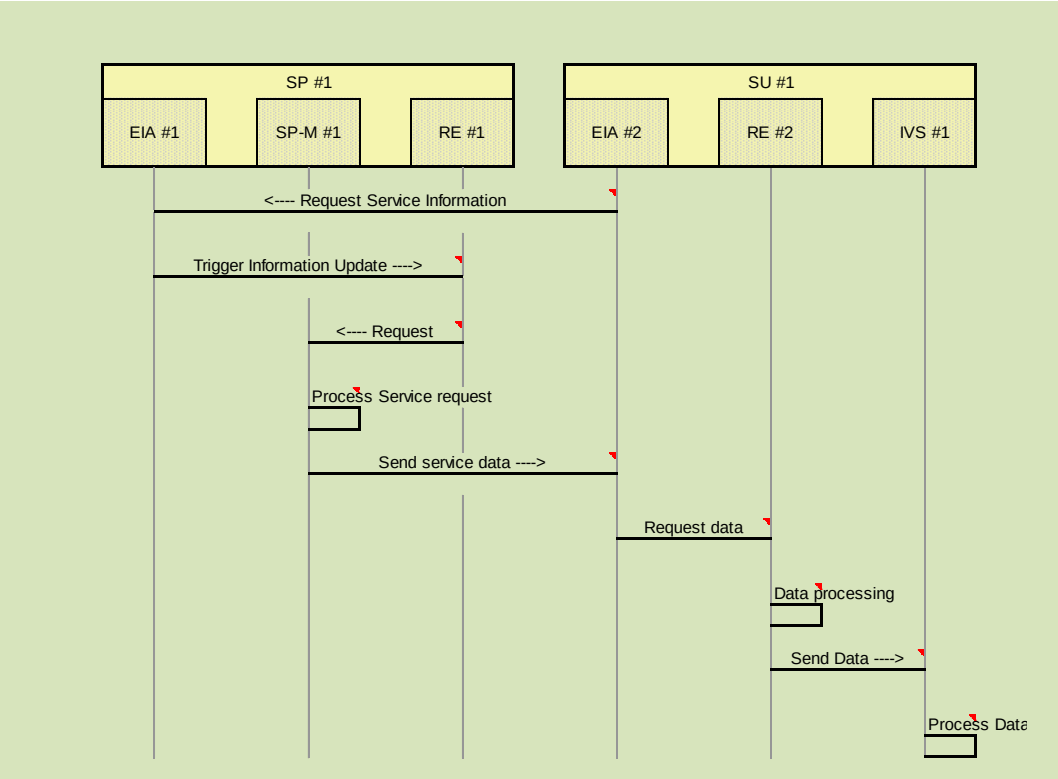
From	To	Description	Optional
C2X-SN SD	EIA #1	The Notification Service attached to the Service Directory server informs SP #1 that a new service has registered itself, by posting SP #1 EIA event reception point, providing its WSDL and its textual descriptions	
EIA #2	SP-M #1	SU #1 EIA_#2 contacts SP-M_#1, presenting its certificate APC_sn_SP-M, to register itself as receiver of message notifications.	
EIA #3	SP-M #1	SU #2 EIA_#3 contacts SP-M_#1, presenting its certificate APC_sn_SP-M, to register itself as receiver of message notifications.	
SP-M #1	EIA #3	SP #1 SP-M #1 detects the invalidity of the certificate of SU #2 and rejects the registration	



2.65.3 Actions Operational

From	To	Description	Optional
Prerequisite#7		The service provider(s) that want to provide the information has registered its SP-M service, attached its transaction logging service with its SP-M and is ready for service	
Prerequisite#8		Each service user that wants to use the SP-M service has registered its EIA service with its service provider	
EIA #2	EIA #1	The service user SU #1 requests new information from the service provider SP #1	
EIA #1	RE #1	The rule engine of SP #1 gets the information from the event incoming alert service of SP #1 that a new request is to be prepared	
RE #1	SP-M #1	The rule engine is requesting the service module for SP-M #1 service to process the service request	
SP-M #1	SP-M #1	The service module SP-M #1 is processing the service requestby checking the information received and retrieving information and further preparation of a service message that gives the necessary information to the service user	
SP-M #1	EIA #2	The service module SP-M #1 is sending the preprocessed service information to the service user SU #1	
EIA #2	RE #2	The SU #1 event incoming alert service EIA #2 detects that the incoming message and forwards it to the rule engine RE #2	

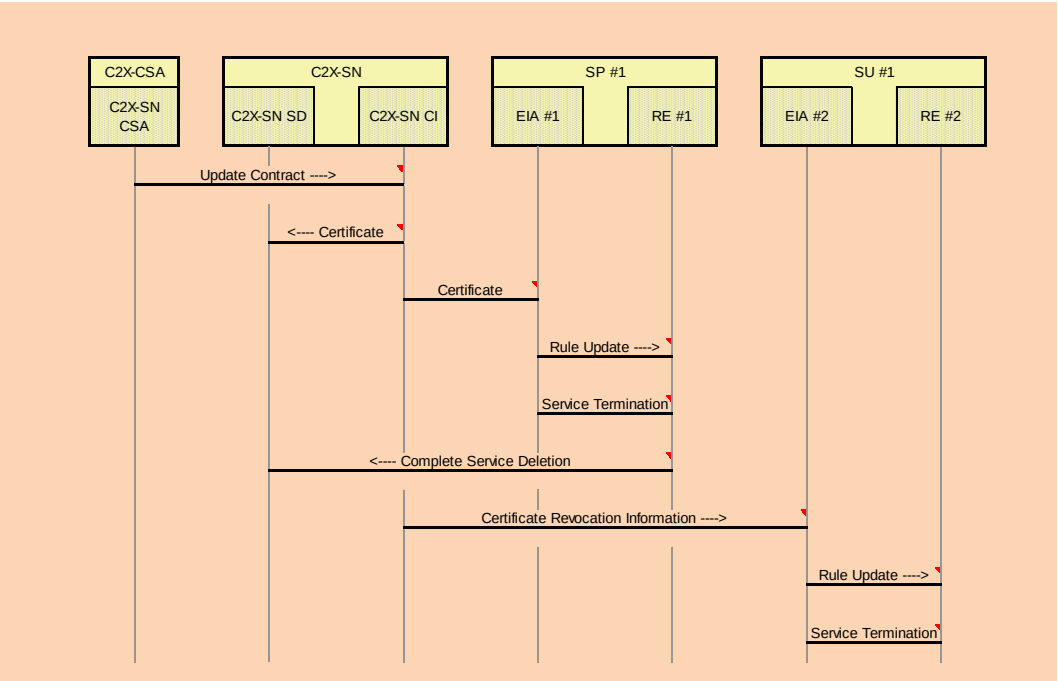
RE #2	RE #2	The rule engine of SU #1 is further processing the information of the SP-M #1 service and triggers the respective actions (e.g. Providing the data to the IVS)
RE #2	IVS #1	The rule engine of SU #1 is sending the information derived from the service SP-M #1 to the respective IVSs
IVS #1	IVS #1	The IVSes that receive the information take further actions to e.g. inform the driver.



2.65.4 Actions Post-Operational

From	To	Description	Optional
Prerequisite#9		All SP-M and EIA services at SP #1, and SU #1 are ready to serve the next event	
Prerequisite#10		SP #1 has terminated theSP-M contract and notified the C2X-SN Contract Supervision Authority. SP #1 had been the only SP-M service provider left at the C2X-SN and decided to revoke that offer. Hence the SP-M service shall disappear as if it had never been launched	
C2X-SN CSA	C2X-SN CI	The C2X-SN Contract Supervision Authority 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	C2X-SN SD	The C2X-SN Certification-Issuer contacts the C2X-SN Service Directory service (associated with the Service Directory) to inform that the new certificate APC_sn_SP-M-2, associated with service SP-M, has been activated, replacing certificate APC_sn_SP-M
C2X-SN CI	EIA #1	The C2X-SN Certification-Issuer contacts the EIA receptor of SP #1 to inform that the Certificate APC_sn_SP-M has been revoked. SP #1 updates its local certification management
EIA #1	RE #1	EIA #1 updates its local certification management and triggers its local RE with the update request. The RE of SP #1 updates its event notification rules.
EIA #1	RE #1	EIA_#1 trigges its local RE with the update request. SP #1 purges it entire SP-M service configuration and terminates SP-M_#1
RE #1	C2X-SN SD	SP #1's RE contacts the C2X-SN Service Directory server and requests the deletion of the SP-M_#1 service offer
C2X-SN CI	EIA #2	The C2X-SN Certification-Issuer contacts the EIA receptor of SU #1 to inform that the Certificate APC_sn_SP-M has been revoked. SU #1 updates its local certification management
EIA #2	RE #2	EIA #2 updates its local certification management and triggers its local RE with the update request. The RE of SU #1 updates its event notification rules.
EIA #2	RE #2	EIA_#2 trigges its local RE with the update request. SU #1 purges it entire SP-M service configuration and terminates SP-M_#1



2.65.5 Components Identified

Name	Description	Involvement		
		Pre-Operation	Operation	Post-Operation
C2X-SN CSA	The (human) body that is responsible for 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.			x
C2X-SN CI	Certification instance for service and service provider certification. Hierarchical structure for the CA, so that an systems network CA and SP-internal CA can exist and be interconnected. This can be for example for OEM, so that they can attach certificates to their cars or for non-free services so that service users can get an 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 services/information. This can be inside the C2X-SN itself and/or 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
EIA #1	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
RE #1	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
SP-M #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 subtypes like ETA, WWD, RWW, LHW, CAM-sending, etc. on either the IVS/IRS/Smartphone or the Service Provider side.	x	x	
EIA #2	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x	x	x
IVS #1			x	
RE #2	A Software component inside a communication endpoint that is able to handle and process messages that are sent through the C2X-SN.		x	x
EIA #3	Running on all communication endpoint entities. It represents the SAP for all incoming messages.	x		

2.65.6 Decision Points Identified

ID	Component	Description

2.65.7 External Activities Identified

ID	Group	Description

LITERATURE

Reference documents can be seen in the main document of deliverable D3

ABBREVIATIONS

Abbreviations can be seen in the main document of deliverable D3 (components list and abbreviations chapter)