Milestone 4 - Next steps for Hybrid communication

Version number:	1.0
Main author:	Igor Passchier
Dissemination level:	PU
Lead contractor:	NMIE-R
Due date:	
Delivery date:	31/07/2019
Delivery date updated document:	

Co-financed by the European Union
Connecting Europe Facility

Grant Agreement No:
INEA/CEF/TRAN/M2015/1143833
Action No: 2015-EU-TM-0159-S

CONTROL SHEET

Version history			
Version	**Date**	**Main author**	**Summary of changes**
0.1	22/10/2018	Igor Passchier	Initial draft, table of contents
0.11	26/10/2018	Igor Passchier	Deployment models added.
0.12	10/11/2018	Paul Spaanderman, Igor Passchier	Introduction and Process. Deployment models, technical challenges
0.16	18/01/2019	Igor Passchier, Suku Phull, Marie Christine Esposito, Gilles Ampt, Darren Handley, Anne Verwimp	Review and major additions
0.17	04/02/2019	Igor Passchier, Anne Verwimp, Marie Christine Esposito, Gilles Ampt	Review and major additions
0.20	15/02/2019	Houda Labiod, Gilles Ampt, Darren Handley	Rework of security models
0.22	14/06/2019	Igor Passchier	Final internal draft
0.23	01/07/2019	Igor Passchier	Final draft
0.24	06/07/2019	Igor Passchier	Inclusion of consortium comments
1.0	31/07/2019	Igor Passchier	Inclusion of QA review
	Name		**Date**
Prepared	**Igor Passchier**		**01/07/2019**
Reviewed	**Core Management Team, Advisory Committee & General Assembly**		**15/07/2019**
Authorised	**Ronald Adams (NMIE-R)**		**31/07/2019**
Circulation			

Recipient	Date of submission
INEA	**31/07/2019**
InterCor consortium	**31/07/2019**

Authors (full list):

Igor Passchier (Siemens), Paul Spaanderman (PaulsConsultancy), Marcel van Sambeek (TNO), Peter Lewyllie (AWV Vlaanderen), Marie-Christine Esposito (MTES), Cliff Lunnon (Highways England), Suku Phull (UK DfT), Gilles Ampt (DITCM), Darren Handley(UK DfT), Anne Verwimp (AWV Vlaanderen), Houda Labiod (Telecom ParisTech)

Project Coordinator

Ronald Adams

Rijkswaterstaat

Office address: Toekanweg 7, 2035 LC, Haarlem (NL)

Postal address: Postbus 2232, 3500 GE, Utrecht (NL)

Mobile:+31 6 518 480 77

Email: ronald.adams@rws.nl

Legal Disclaimer

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Acronyms and abbreviations

Acronym / Abbreviation	Definition
AA	Authorization Authority
AC	Advisory Committee
AL	Activity Leader
AMQP	Advanced Message Queuing Protocol
ASN.1	Abstract Syntax Notation One
ASR	Action Status Report
C2C-CC	CAR 2 CAR Communication Consortium
CA	Certificate Authority
CAM	Cooperative Awareness Message (message type)
CCAM	Cooperative Connected and Automated Mobility
CEF	Connecting Europe Facility
CEN	Commission for European Normalization
C-ITS	Cooperative Intelligent Transport System
CP	Certificate Policy
CPOC	C-ITS Point Of Contact
CMT	Core Management Team
CPU	Central Processing Unit
DAB	Digital Audio Broadcast
DENM	Decentralized Environmental Notification Message
DP	Data Provider
DSMIP	Dual Stack Mobile IP
DSRC	Dedicated Short Range Communication
EA	Enrolment Authority
EC	European Commission
ECTL	European Certificate Trust List
ETA	Estimated Time of Arrival
ETSI	European Telecommunications Standards Institute
FNTP	Fast Networking & Transport Layer Protocol
GA	Grant Agreement
GLOSA	Green Light Optimal Speed Advisory
HTTP, HTTPS	HyperText Transfer Protocol, Secured
IEEE	Institute of Electrical and Electronics Engineers
IF	Interface (in this document referred to IF1, IF2, IF3)
INEA	Innovation and Networks Executive Agency
IPR	Intellectual Property Right
IP, IPv4, IPv6	Internet Protocol (version 4, version 6)
IPSec	Internet Protocol Security
ISO	International Standards Organization
ITS	Intelligent Transport System
ITS-G5	OSI layer 1 and 2 technology specified in ETSI EN 302 663

IVI	In-Vehicle Information (message type: IVIM)
IVS	In-Vehicle Signage
LAT	Latitude
LON	Longitude
LTE	Long Term Evolution (4th generation mobile networks, 4G)
LTE-D	LTE-Direct
MAP/MAPEM	Road/lane topology and traffic manoeuvre message (message type: MAPEM)
MCTO	Multi-modal Cargo Transport Optimization
ML	Milestone Leader
MQ	Message Queue
MQTT	Message Queuing Telemetry Transport
MS	Member State
Nfr-ITS-S	French National ITS station
OAUTH	Open ID authorization protocol
OBU	On-Board Unit
OSI	Open Systems Interconnection
PC	Project Coordinator
POI	Point Of Interest
PER	Packet encoding rules
PKI	Public Key Infrastructure
PVD	Probe Vehicle Data
RLAN	Radio Local Area Network
RIS	Roadside ITS Station
RSU	Roadside Unit
RWW	Road Works Warning
SASL	Simple Authentication and Security Layer
SP	Service Provider
SPAT/SPATEM	Signal Phase and Time (message type: SPATEM)
SRM	Signal Request Message (message type)
SSM	Signal Status Message (message type)
TCC	Traffic Control Centre
TCP	Transmission Control Protocol
TIC	Technical & Interoperability Coordinator
TLC	Traffic Light Controller
TLEX	Traffic Light Exchange
TLM	Trust List Manager
TLS	Transport Layer Security
TTL	Time to live
UPER	Unaligned packed encoding rules
UWB	Ultra-Wide Band
VPN	Virtual Private Network
VRU	Vulnerable Road User
WAS	Wireless Access Systems
WAVE	Wireless Access in Vehicular Environments

WSMP	WAVE Short Message Protocol

1 Executive summary

InterCor has developed, implemented and tested the specifications for information exchange via back-office systems enabling internationally interoperable hybrid communication. To progress the usability of these specifications, several aspects need to be further defined and tested. This document addresses two important aspects outlined hereafter.

The specifications of IF2 (i.e. the back-office interface) leave it open *how* these specifications will be implemented. Three implementation models are discussed for the implementation of IF2. These models mainly differ on how data is aggregated and distributed amongst Member States: services providers can obtain the data from the country of origin, a single point of contact per country can aggregate all data from other Member States and forward it to its local service providers, or a single central aggregation point can be established where all data from all Member States comes together, and is redistributed to all services providers. The models are not mutually exclusive, and mixed forms can also be implemented. Various advantages and disadvantages have been discussed. Within InterCor, no decision has been made on what is the preferred implementation model.

The second important aspect covered in this document is how trust in the messages distributed via IF2 can be established. For this aspect, two trust models are presented and discussed that can be used to establish the required level of trust in cellular communication in the context of hybrid communication. Descriptions of these models are provided, including some of the identified strengths and weaknesses. Practical examples of two implementations have been described as well. Existing security and communication standards need to be further optimized in order to support an interoperable and harmonized solution over IF2 to deploy hybrid based C-ITS services in the context of the InterCor project. Therefore, no final decision is taken on the preferred trust model to use for IF2. What ultimately is required is a solution that is optimised for hybrid communication, where stations can either implement only ITS-G5 communication, only cellular communication, or a combination of both.

2 Introduction

One of the objectives of InterCor is to provide C-ITS services on a broader scale by specifying, using and advancing a hybrid communication approach to utilise a combination of cellular (network-based) communication and direct (localized) communication. InterCor focuses on realizing international interoperability of C-ITS services based on hybrid communication solutions. In contrast, InterCor does not focus on the improved quality of service itself by combining multiple networks, but extending the geographical availability of services for end-users by connecting hybrid solutions in different countries.

Hybrid communication in InterCor is further reduced in scope by only considering ITS-G5 and currently available cellular technologies: other communication technologies and future extensions of these two technologies are not (explicitly) considered.

2.1 Purpose of this document

Based on this scope, InterCor has developed, implemented and tested the specifications for information exchange via back-office systems [1, 8] enabling internationally interoperable hybrid communication.

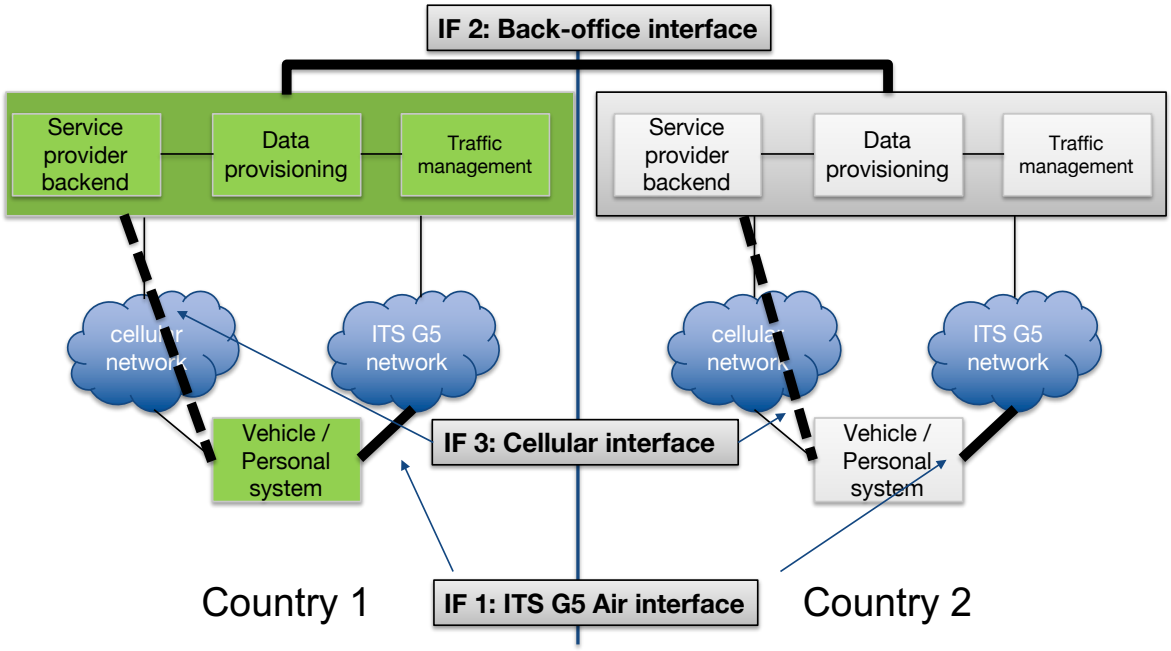

Figure 2.1: High level diagram for hybrid communication from [8].

To progress the usability of these specifications, several aspects need to be defined and tested. This document addresses two important aspects. The specifications of IF2 leave open *how* these specifications will be implemented. Several options can be considered. These are elaborated and discussed in more detail is section 4. Another important aspect is how trust in the content of messages distributed via IF2 can be established, which is the topic of section 5.

To make these aspects more concrete, section 6 provides two examples of concrete implementations where these aspects have been addressed and specific solutions have been chosen.

To place these aspects in a European C-ITS development context, an overview of the European development process for C-ITS in general and for hybrid communication in particular is provided in section 3.

2.2 InterCor Contractual References

InterCor (Interoperable Corridors) links the C-ITS corridor initiatives of the Netherlands (among which the C-ITS Corridor Netherlands-Germany-Austria), the French (among which the one defined in SCOOP@F) and extends to the United Kingdom and Belgium C-ITS initiatives.

InterCor is an action co-financed by the European Union under the Grant Agreement number INEA/CEF/TRAN/M2015/1143833. The Project duration is 36 months, effective from the 1st of September 2016 until the 31st of August 2019. It is a contract with the Innovation and Networks Executive Agency (INEA), under the powers delegated by the European Commission.

Communication details of the Agency:

Any communication addressed to the Agency by post or e-mail shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)
Department C – Connecting Europe Facility (CEF)
Unit C3 Transport
B - 1049 Brussels
Fax: +32 (0)2 297 37 27
E-mail addresses: General communication: inea@ec.europa.eu

For submission of requests for payment, reports (except ASRs) and financial statements: INEA-C3@ec.europa.eu

Any communication addressed to the Agency by registered mail, courier service or hand-delivery shall be sent to the following address:

Innovation and Networks Executive Agency (INEA)
Avenue du Bourget, 1
B-1140 Brussels (Evere)
Belgium

TEN-Tec shall be accessed via the following URL:

https://webgate.ec.europa.eu/tentec/

All communication with the INEA or the European Commission shall be done via the Project Coordinator, Mr. Ronald Adams.

3 InterCor in the context of the European C-ITS Interoperability specification process

The InterCor project has to be considered in the context of many ITS and C-ITS research and development initiatives carried out across Europe over the last three decades. In this section, the European C-ITS innovation process is sketched, and the position of InterCor in this process. To identify its influence, it is important to recognize its contribution to the overall European C-ITS objectives, relations with other initiatives and how it can be placed in C-ITS innovation process.

According to the Oxford English dictionary, innovation means introduction of something new. The National Innovation Initiative (NII) of USA defines innovation as the intersection of invention and insight, leading to the creation of social and economic value. Dr A.P.J. Abdul Kalam, the president of the Indian National Innovation Foundation pronounced “Innovation is the celebration of creativity”.

From a process perspective all the definitions direct in a practical view “Innovation = Invention + Social-Economic Exploitation”. The innovation process is the translation of a new invention into something socio-economically valuable or, in other words, it is to bring research into practical socio-economic value.

Innovation is mostly a bottom-up process, but legislation may well take the initiative by ruling societal or economic requirements (such as the reduction of CO_2 emissions). There are different types of innovations: Business, Architectural, Modular, Incremental, Radical and Novel, all having different effect on the existing situation. Differences we need to consider in the general development of C-ITS. The innovation process involves search and selection of technologies, techniques, processes and business approaches. It requires exploration and synthesis, cycles of divergence and convergence. Innovation needs at least the support from several organisational levels, and in some cases deep involvement of these levels.

3.1 The C-ITS innovation process

In the case of C-ITS, one can recognise three innovation levels as depicted in Figure 3.1.

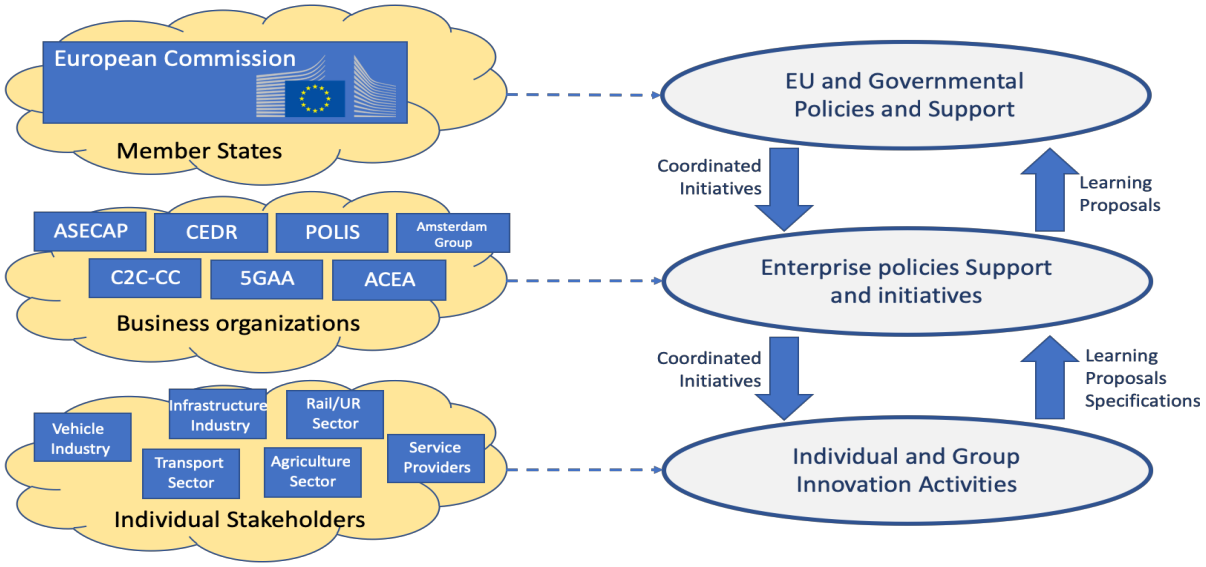

Figure 3.1: Innovation Organisation Levels in Europe.

As can be seen in the case of C-ITS, a large number of authorities and stakeholder's groups, represented by business organisations, are involved. This large number of groups and organisations results in many organized and bilateral alignments, which are needed to come to the realisation of an acceptable level of interoperability of an innovative solution for all the stakeholders across all Member States.

To come to a common result, the agreement of the objectives and processes is an alignment process in itself. Starting the innovation cycle, functionality and technology generally are developed in bottom-up research processes. Investment in research starts slowly, and at the moment benefits are more visible as investments increase. While based on new service interests and introduction of new technologies, new innovation cycles are identified and started. Each of these new cycles, however, need to go through the same steps to get to maturity. The figure below identifies these steps for C-ITS.

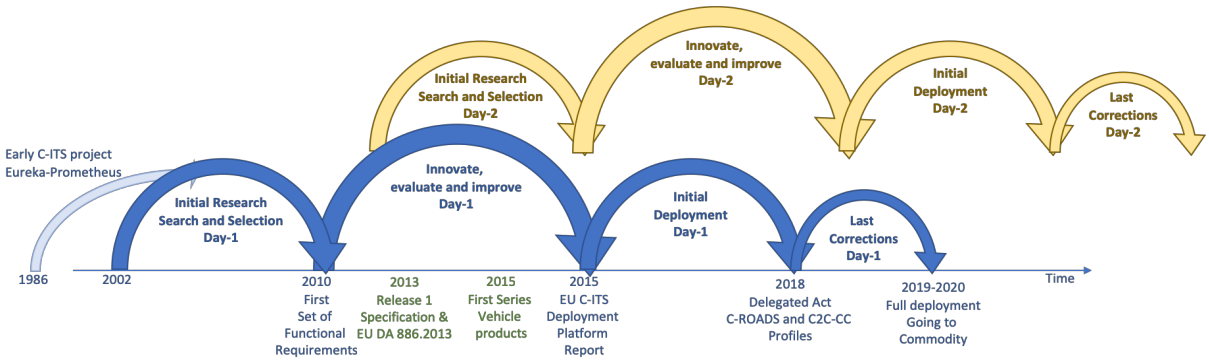

Figure 3.2: The Innovation steps in C-ITS. Note that a complete overview of all involved activities is not included.

In this innovation process, 4 stages can be identified. In the first stage, initial research is performed on a wide range of technologies to determine an initial set of candidate solutions for specific C-ITS services. In the second stage, the focus is on innovation, i.e. combining technology with socio-economic exploration to come to realistic solutions that can be deployed from both a technical perspective and a socio-economic perspective. In the third stage, initial deployments are realized to gain field operational experience with these solutions. During these initial deployments, lessons learnt on how to best deploy the services are used to fine-tune the overall solution for deploying the services in a European wide context. After this 4-step process, the services will become a commodity where all stakeholders have a common understanding on their role in the service delivery, and how to fulfil that role.

A number of ITS related services (also) using standard cellular communication technologies for their information sharing are commodity, i.e. the have reached the end of the above sketched innovation cycle. An example is the route-planner service provided by navigation systems providers. They adopt the route based on shared traffic information provided e.g. via TMC or a dedicated connection to the back-office of the navigation system provider.

For the exchange of safety related information for C-ITS services, technology based IEEE 802.11p and ETSI ITS standards was chosen after the Initial research phase. Today we are at the initial deployment stage, which is necessary to ensure interoperability and service availability, also across country borders.

The introduction shows where the ITS community stands in the C-ITS innovation process. The initiation of the C-Roads Platform (www.c-roads.eu) and implementing projects (such as InterCor) proved to be a successful approach bringing European Member States interested in C-ITS to real deployment. The development of C-ITS roadmaps was started by the Amsterdam Group and then brought to a higher level by the European Commission. The EU C-ITS Deployment Platform in its Phase-1 (2014-2016) and Phase-2 (2016-2017) led to the formulation of the first EU vision and roadmaps [10]. The reports identified Day-1, Day-1.5 and Day-2 services. To realize interoperability for these services, alignment between different stakeholder groups, C-Roads Platform, C2C-CC (www.car-2-car.org) and others is necessary. For instance, C-Roads and C2C-CC are developing their own specifications and aligning those with each other. As these groups are more and more working together, they organize common meetings to align at an early stage. It can be expected that the speed and quality of the interoperable specifications will increase as a result of the cooperation within the C-Roads Platform and between C-Roads and C2C-CC.

The projects under the umbrella of the C-Roads Platform have and will start and end at different moments. To consolidate the results of these projects in a commonly agreed solution, the C-

Roads Platform needs to be a continuous activity, and thus continue also after all projects have ended. To find the approach how to continue after all projects are ended is a task for the C-Roads Platform to realize in cooperation with the European Commission. The aim is to realize a single platform for the harmonisation and interoperability of C-ITS services at European level for all stakeholders. To make the overall process faster and more efficient, the support and stimulation of a continuing independent process where all stakeholders can realize interoperability neutrally should be stimulated for the continuity of the deployment of current and new C-ITS and CCAM services.

3.2 InterCor as part of the C-ITS innovation process

InterCor is initiated by 4 MS with funding from the EC, positioned as an initial deployment of Day-1 services, i.e. stage 3 of the innovation process. In that context, it provides and aligns its finding to the C-Roads Platform. C-Roads uses these findings to consolidate the specifications to increase the functional and cross-border interoperability of the Day-1 services and use cases. The work done in InterCor on harmonization of message definitions, ITS-G5 based implementations and PKI aspects are part of this work. These activities resulted in detailed profiles and other technical documents validated through TESTFESTs and operational pilots, whose outcomes have been provided to the C-Roads Platform for wider harmonisation.

At the same time, InterCor also addresses technical challenges for cross-border interoperability that are not yet in the third stage of the innovation process. This is particularly true for hybrid communication, which did not conclude the first two stages of this process (i.e. research and innovation). For hybrid communication, InterCor focusses specifically on the innovation step by bringing results from previous (European and national) research activities, but also considering market development.

As mentioned section 2.1, various approaches / solutions have been investigated in relation to implementation models and security models for hybrid communication[1]. The next sections present the various solutions considered and a preliminary assessment, but no position is expressed in relation to their adoption: no definitive decisions on these topics are made within InterCor. A hybrid communication roadmap is identified, leaving the next steps to C-Roads and other activities.

[1] For hybrid communication, InterCor only focusses on the international interoperability, but not on a complete solution. Therefore, these aspects are only addressed in such perspective.

4 Implementation models for the IF2 interface

4.1 Introduction

The Figure below provides a simplified functional architectural view of the use of IF2 defined within InterCor, as described in [1, 8], when a vehicle from country 1 is visiting country 2. In this simplified view, IF1 (Wi-Fi air interface) and IF3 (cellular interface) are left out. This and all other Figures in this document should be interpreted for multiple countries, multiple service providers and multiple vehicles, but for simplicity, only 2 countries, 1 vehicle and 1 service provider per country are shown. Data and service providers within each Member State may be able to use IF2 for data exchange within a single country, but this is outside the scope of this document.

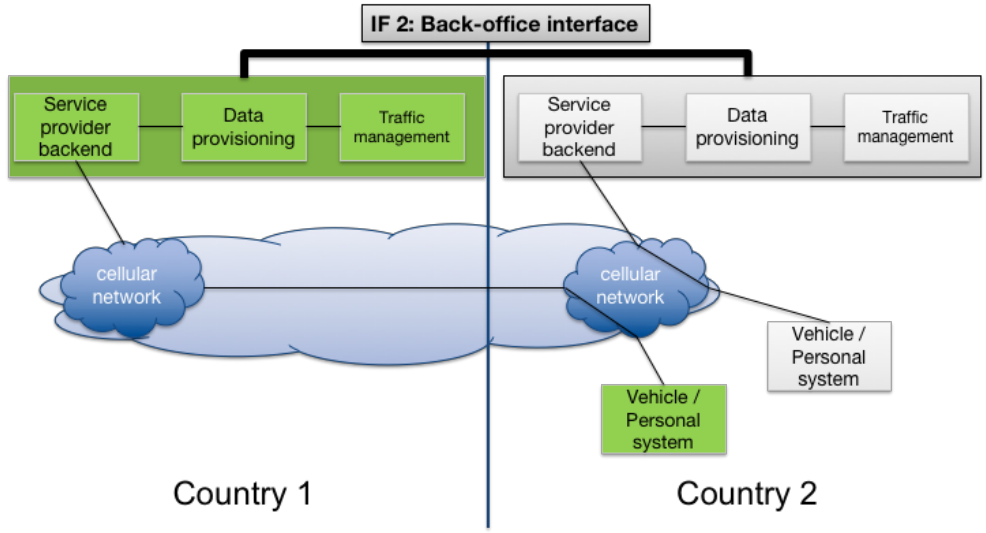

Figure 4.1: General system overview for the functional usage of IF2.

The IF2 interface is identified as the interface between road authorities, data providers and service providers, in any combination, to support data distribution via cellular IP-based networks to satisfy the specific C-ITS services of interest to road operators and services providers ensuring cross border service availability. The interface specifications are given in [8]. At the current state the supported services within InterCor are RWW, IVS, PVD, and GLOSA. Additional services are expected in near future, but it cannot be anticipated that the current specifications support them. For the four InterCor services above, the data messages originate from the road operator (or a third party on behalf of the road operator) or a vehicle, and the information needs to be provided to a system in the vehicle to provide the service to the driver of the vehicle or to the road operator. The receiving actor should be able to identify who the data/service owner is and who provided (delivered) the data, if the (optional) header on IF2 has been filled in.

The IF2 interface specifications themselves only specify the technical details of the interface itself, but not the complete system in which the interface will be implemented. For the pilot operation phase, a specific implementation model (possibly different for each InterCor Member State) needs to be selected. The choice of a specific model for pilot operation will be influenced also by what implementation model is foreseen in the long term, extending the services deployment after the completion of InterCor. In the following section, three implementation models are described. It is also possible to mix these models, however for clarity this document focuses on the advantages and disadvantages of the separate models. An assessment of the models will be given in section 4.3.

4.2 Implementation model descriptions

4.2.1 Implementation model based on national nodes for national data only

In this model A (Service Provider (SP) oriented), every country has a national node that services only national data (i.e. C-ITS related information). Service providers from different countries all connect directly to the broker in this national node. Every national node will have to serve all service providers with vehicles in their country, and each service provider will need to connect to brokers in all countries where it has customers. This situation is depicted in the figure below, with the national node depicted as 'broker' for data provisioning and interfaces to a 'client' in service provider back-end systems in each country, marked with black and orange arrows.

In this model, there is no need to connect the different national nodes to each other.

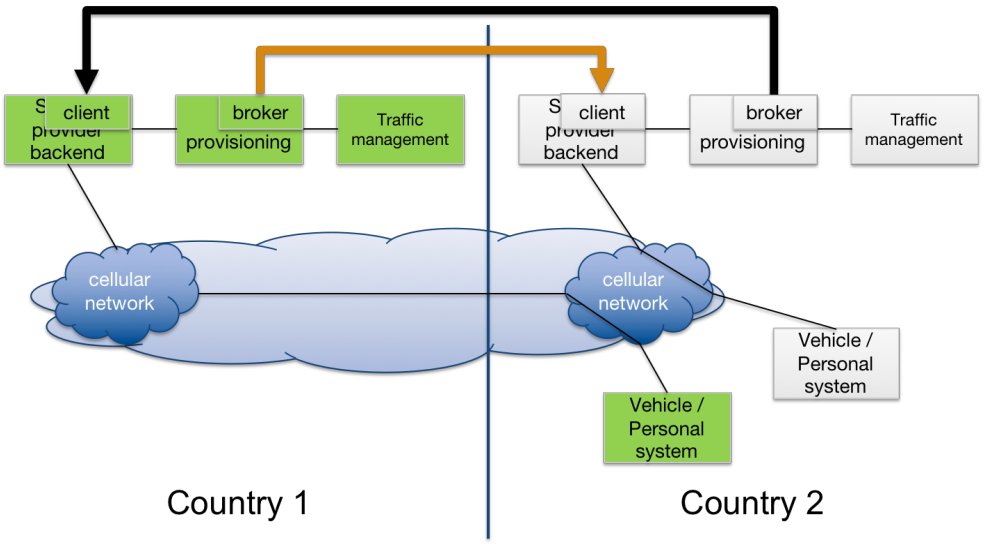

Figure 4.2: Model A: deployment model based on national nodes that only serve national data. The bold lines are implementations of IF2, where the broker and client boxes refer to the broker and client implementations of IF2. The arrows indicate the direction of the data streams for the current services.

4.2.2 Implementation model based on national nodes exchanging data

In this model B (national node (NN) oriented), the NNs are interconnected with each other, and the service providers will (only) need to connect to a single NN. Every NN will connect to every other NN and processes all data from the other NNs to to serve it to the connected service providers[2]. This situation is depicted in the figure below.

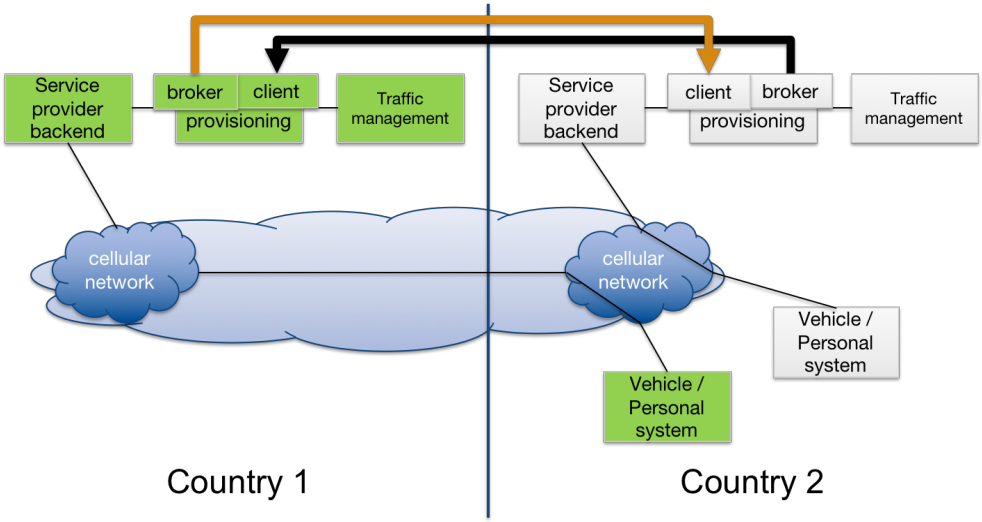

Figure 4.3: Model B: deployment model based on national nodes exchange all data. The bold lines are implementations of IF2, where the broker and client boxes refer to the broker and client implementations of IF2. The black arrows indicate the direction of the data streams for supporting vehicle from country 1 in country 2, and the orange arrows for vehicles from country 2 in country 1.

4.2.3 Implementation model based on a central EU node

In this model C (EU central node (CN) oriented), the national nodes all forward their data to a central EU broker, and all service providers connect to the central broker node[3]. The EU central node can connect as a client to all brokers in all national nodes, and the service providers can connect as client to the broker in the EU central node. This situation is depicted in the figure below.

[2] This implies that service providers only connect to a specific national node, which might not be the case for internationally operating service providers. For simplicity, this is not taken into account here.
[3] Possibly they also connect to their national node, but that is out of scope of InterCor.

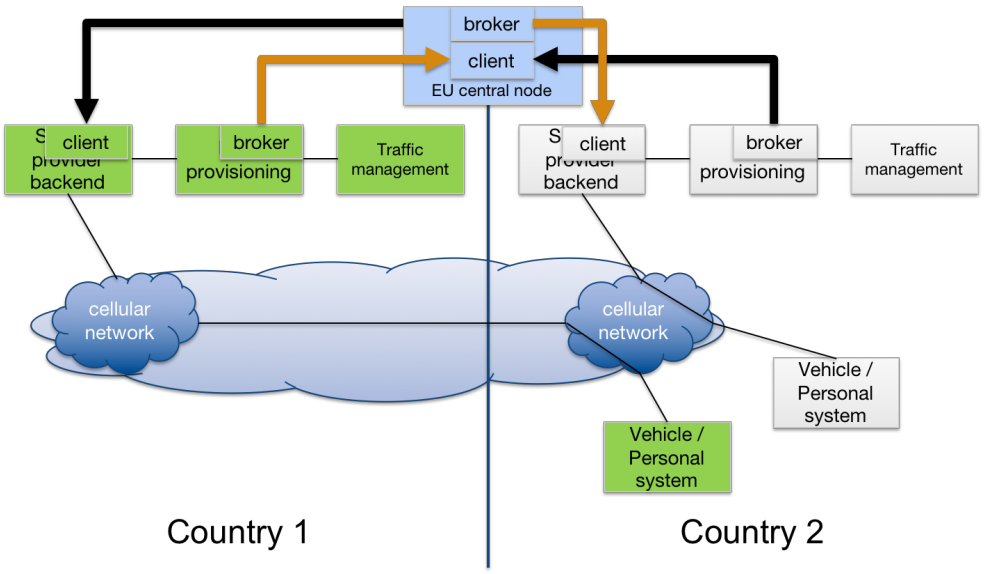

Figure 4.4: Model C: deployment model based on a central EU node. The bold lines are implementations of IF2, where the broker and client boxes refer to the broker and client implementations of IF2. The black arrows indicate the direction of the data streams for supporting vehicle from country 1 in country 2, and the orange arrows for vehicles from country 2 in country 1.

4.3 Assessment of the deployment models

The three models described in the previous section, will be assessed based on the technical complexity for the service provider and national node implementations, for their scalability, and on their organisational complexity.

Table 4.1: Assessment of the three deployment models.

Aspect	Model A (SP oriented)	Model B (NN oriented)	Model C (CN oriented)
Description	SPs connect to all national nodes	SP connects to one national node (NN). National nodes exchange data with each other.	SP connects to a single central EU node
SP technical complexity	SPs have as many different connections as countries in which they are providing services to their customers.	SPs have access to all information available via a single connection.	SPs have access to all information available via a single connection.
National node technical complexity	National nodes only have to serve data for their own country. They will have many more clients than in the other models, as all SPs from all countries will connect to them. This also	The number of clients is limited, and changes to this list will happen less frequently. The national node has to process all data from all countries involved. The IF2 specs	National nodes only have to serve data for their own country. They will have a single client, the EU central node.

Aspect	Model A (SP oriented)	Model B (NN oriented)	Model C (CN oriented)
	creates a more dynamic operational environment for the national node.	assume that the client knows the area of interest, but the national node will not have this information automatically. If it does not know the area of relevance, it always has to gather all data from all countries. Connecting on demand could be implemented as well.	
Scalability	National nodes have to serve more clients than in the other models, and therefore have higher scalability requirements. Overall, however, the scalability is better, as all clients know what data is relevant, and thus are capable of filtering on the relevant data.	The number of clients is limited per broker, but all data need to be distributed to all national nodes. So scalability on number of clients is good, on the amount of data is poor. Note, that a lot of data is being distributed, which is not used in practise.	The full scalability requirements are placed on the EU central node. This node will have to process all data from all countries and has many clients. Due to the fact that these stringent requirements are all placed on a single entity, it requires constructing a single, highly scalable instance.
Reliability/ Latency	As this is a locally managed solution latency and reliability to the SP can be monitored and managed at a practicable level. As there is no physical international connection and possible roaming delays it may be difficult in this solution to manage services to international users.	Each national node will be providing services to each other national node. This would be an unwieldy service to manage as the incoming data from each national node could be of variable quality. If there was an issue with a data provider the issue could be difficult to resolve as it is a parallel relationship.	Although as in model B there could be variable quality of service from different national nodes as this is centrally managed by an overriding authority this could be an easier system to manage.
Consistency of service	As each national road operator is responsible for their own data, they will have local knowledge and context. The service they are able to provide should be easier to manage and	International consistency is managed locally in this model and so obliging road operators to agree and commit to providing international service for vehicles	As all services are fed from and to through the European node this will provide the same service to the service provider where ever the vehicles are based and travelling.

Aspect	Model A (SP oriented)	Model B (NN oriented)	Model C (CN oriented)
	provide a national consistency. Internationally consistency could be an issue as the service provider will have a separate connection to the local service the vehicle is travelling.	travelling in other countries than their home. As such this creates a technically accountable system.	
Organisational complexity	For a small number of countries participating, the organisational complexity is limited. However, if the number of countries and or SPs that participate increase, the complexity increases rapidly. A central repository or marketplace where the details of all national nodes and/or SPs can be found would be beneficial.	The organisational complexity is limited. National nodes only have to deal with local customers, and with a (limited) set of other national nodes. The legal responsibility for the data provided could become an issue, as national nodes will serve data from many sources, also sources that they have no contact with directly themselves[4].	*After* an EU central node has been organized the organisational complexity is limited. National nodes only have to deal with the central EU node. The legal responsibility for the data provided could become an issue, as the EU node will serve data from many sources, sources that they have no contact with directly themselves.
Business model aspects	This model focusses on a service provider-oriented solution: the service providers decide what data is interesting for them, and only those data will be gathered, at the national node where the data is originating.	It is unclear who pays the costs for data exchange and management of non-national data by the national node operators. This model is more country oriented, instead of service provider/data provider oriented.	The EU central node needs to be developed and operated by someone. At the moment, it is unclear who could fill in this role. This would need further collaboration with other Member States and the EC to setup such a central node.

Depending on how strict the models will be implemented by different Member States, it is possible to have deployments based on the different models and still have international interoperability. Model A is the base model or starting point that needs to be supported by

[4] See next section on a more detailed discussion of “trust”, which can also help to overcome this legal issue.

individual Member State to provide data from road authorities on a central level per Member State.

The models B and C can be deployed in time and are based on model A. It should be noted that pan-European service providers are not tied to a single country and are free to connect to multiple national nodes. The aggregation of data by national nodes (supported by local government) can be offered by either each national node (model B) or by a central node (model C). The functionality of the EU central node may also be provided by commercial providers e.g. data aggregation providers to other service providers. For example, if a MS implements model B in addition to model A for their existing service providers, i.e. provide data from their own country and also from other selected Member States, via IF2 to their existing service providers, this will be at the same time attractive to provide the data from that Member State to new a service provider.

Multiple models based on model A will likely evolve and can be deployed and supported at the same time. Consequently, it will become more complex to figure out what information can be obtained where. Also, if information will be provided at different places, service providers subscribing to this information need to ensure that they are able to identify duplicates and ensure they can handle that correctly.

Therefore, it might be preferable to have a common approach for selecting one of the deployment models B or C, at least for the long term. Support for multiple models could be a good way to start off, as long as it is unclear what that common approach should be and migrate in a later stage. Also, model C can be treated as a development of model A or B to simplify the data distribution on a larger (European) scale. The move from model A to B or C will depend on the benefits for both national nodes to distribute data and for services providers to collect data (and vice versa for probe vehicle data). The EC could stimulate the use of pan-European ITS safety services by giving support to an EU node.

When scaling up to a larger deployment, it can be considered to add a control layer to the currently defined operational layer. Such a control layer would facilitate dynamic requests of technical details about where to get access to what data. This could be implemented as a kind of market place, as investigated in e.g. the Mobinet project. Another option would be to standardize a control layer where every application that wants to connect via IF2 first addresses a central server with the details of the information that is required/provided (message type, geographical region of interest, etc.), and based on that receives the details (IP address, credentials, etc.) of an IF2 implementation to connect to. This approach has been implemented already in the Talking Traffic project. When a market place or control layer would

be added, it is not necessary anymore to make a single, EU-wide decision on which of the models, or combination of models, will be supported.

For the testing and piloting phase in the frame of InterCor, the participating Member States (France, Belgium/Flanders, Netherlands, and the United Kingdom) have chosen to support multiple implementation models to realize international interoperability. This does not reflect the preferred long-term solution. At this moment, InterCor does not provide a preferred implementation model in the long-term perspective. This issue needs to be addressed in a larger context, as consensus is required on a European level. This issue could therefore be further addressed in the C-Roads Platform and/or other European C-ITS deployment projects.

5 Realization of trust in messages exchanged via IF2

An important aspect for message exchange over IF2 is how to ensure trust. Ultimately, the system receiving messages needs to be able to verify the authenticity and integrity of the received messages. Only if the receiving system trusts the content of a C-ITS message, it can use this message in the services it provides.

To establish trust within a particular domain, agreements, processes and procedures need to be established and translated into policies and standards. These put legal and technical requirements to all participants within the trust domain. Specifications are essential as they clearly specify the requirements on messages that are transmitted in the context of the trust domain. These requirements are covered in standards, and complemented by profiles, which are currently being investigated by a.o. InterCor, the C2C CC and the C-Roads Platform. Also, a compliance assessment procedure shall be in put place to ensure that the standards and profiles are properly implemented by transmitting systems, but this is out of the scope of InterCor and will not be treated here.

For messages exchanged via IF1 (i.e. via ITS-G5), a European C-ITS Trust model has been developed [11], defining the trusted C-ITS communications system. This model is based on Public Key Infrastructure [12] within the scope of the overall EU C-ITS Security Credential Management System (EU CCMS).

To be able to realize C-ITS services based on hybrid communication, an integrated solution for realizing trust in the complete hybrid system is required. Based on the current status, an overview will be given of trust models that could be used as part of the cellular communication channel. As a second step, these models are evaluated in the context of hybrid communication.

A complicating factor is that the trust needs to be ensured for specific end-to-end services, using a specific communication channel, or even for a complete architecture, whereas InterCor only defines the interoperability interfaces, and not the overall architecture or communication chain. Therefore, only an overview of possible solution directions is provided and assessed here in the context of IF2.

In the next sub-section two trust models are described and discussed. Although they are discussed separately, in practice they can also be used in combined fashion.

5.1 Trust model based on individually end-to-end signed messages

Early 2014 the European Commission decided to take a more prominent role in the deployment of connected driving by setting up a C-ITS Deployment Platform [10]. The EU C-ITS Platform

was conceived as a cooperative framework including national authorities, C-ITS stakeholders to develop a shared vision on the interoperable deployment of C-ITS in the EU.

Among other aspects, the security of V2X communications has been covered by the EU C-ITS Platform. A security architecture with support of a Public Key Infrastructure (PKI) using commonly changing pseudonym certificates has been eventually developed [11, 12].

The common C-ITS Certificate Policy [13] defines the European C-ITS trust model based on Public Key Infrastructure. It defines legal and technical requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe. The PKI is composed at its highest level by a set of Root Certificate Authorities (RCAs) “enabled” by a Trust List Manager (TLM), i.e. whose certificates are listed in a European Certificate Trust List (ECTL) defined and published by the central entity TLM.

Figure 5.1 provides a pictorial description of the C-ITS trust model architecture. The Policy Authority appoints the TLM and therefore provides trust in the operation of the TLM to all PKI participants. The Policy Authority approves the Root CA operation and confirms that the TLM can trust the Root CA(s). The TLM issues the ECTL that provides trust in the approved Root CAs to all PKI participants. The Root CA issues certificates to the Enrolment Authority (EA) and Authorisation Authority (AA) and hence provides trust to their operation. The EA issues Enrolment Certificates to the sending and relaying ITS station (as End-Entity), providing trust in its operation. The AA issues Authorization Tickets to the ITS stations based on the trust from the EA.

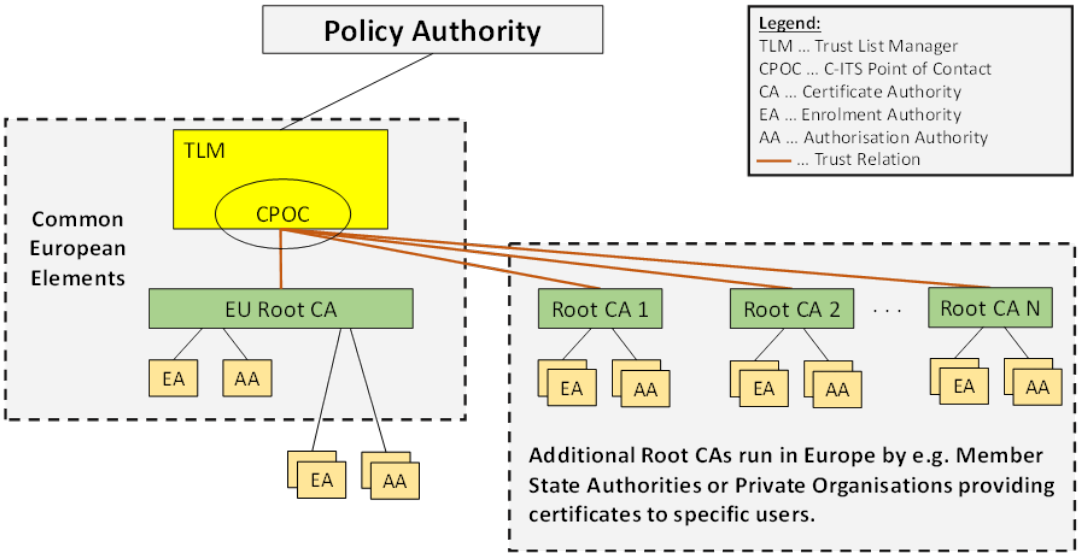

Figure 5.1: High level overview of the organisation of the European C-ITS trust model.

The C-ITS trust model is based on a multiple Root CA architecture and is composed of the following main components:

- **The Policy Authority:** The Policy Authority is a role composed by the representatives of public and private stakeholders (e.g. Member States, Vehicle Manufacturers, etc.) participating to the C-ITS trust model, where a consensus based voting scheme applies. The Policy Authority is the main decision body that guarantees the trust and interoperability between the participating members states PKIs.
- **The Trust List Manager (TLM):** The TLM is a unique entity appointed by the Policy Authority. The Trust List Manager is responsible for operation of the ECTL according to the common valid CP and regular activity reporting to the policy authority for the overall secure operation of C-ITS trust model.
- **The C-ITS Point of Contact (CPOC):** It is the responsibility of the Policy Authority to authorize the CPOC to fulfil some main tasks to secure communication exchange between all entities of the C-ITS trust model including the transmission of the Root CA certificates to the TLM as well as the publication of the ECTL.
- **The Accredited Auditor:** The Accredited Auditor is responsible for performing or organizing audits of root CAs, notifying to the Policy Authority on the successful or unsuccessful execution of an audit either initial or periodic and assessing compliance of CPSs to the CP.
- **Members States PKIs elements**: Each Member State is responsible of managing its own PKI composed of Root CAs, EAs and AAs. The certificates of the Root CAs are transmitted periodically to the CPOC through a secure protocol (which is under construction by the EC).

To apply this model for IF2 as it has been defined for ITS-G5 Day-1 services, the following requirements need to be respected:

- A sending ITS station acquires rights to broadcast an authorized set of ITS messages from Enrolment Authority, negotiates rights to invoke ITS services from Authorization Authority and sends single-hop and/or relayed signed broadcast messages.
- A relaying ITS station (Forwarding ITS station) receives broadcast messages from the sending ITS-S and forwards them to the receiving ITS station if required.
- A receiving ITS station receives signed broadcast messages from the sending or relaying ITS station.
- Following the certificates management procedures as they have been defined in the Certificate Policy (CP) in terms of time of validity of certificates, signature algorithms and cryptographic requirements, verification of signature, generation of keys for signature and encryption, etc.

End-to-end signed messages are transmitted, forwarded and delivered to destinations. At destination, the forwarded messages should be verified thanks to the use of signature and Authorization Tickets in order to guarantee interoperability. Signature of data messages is done at Geonet layer respecting the reference ETSI communication architecture model and based on the security profile of messages as defined in the ETSI security standards.

Advantages of this model are that it can be integrated relatively easy with ITS-G5 based communication, that it does not put strong trust requirement on any relay station, and that it is already accepted by many stakeholders in the C-ITS domain. However, several difficulties have been encountered when applying this model to cellular technology:

- The current C-ITS security standards and EC CP have been mainly focused so far on ITS-G5 access technology; hence the signature has been set at the network layer, necessary for this type of technology. However, for IP based links based on another transmission paradigm, carrying message signature at the Geonet layer may appear as not relevant and restrictive.
- End-to-end data message signature is required for trust and message integrity and message authorisation verification; this must be kept, but maybe without the complete structure of Geonet Secured Message for C-ITS based cellular communications. ETSI is working on a ITS standard to allow message signatures on the facility layer or application layer instead of the Geonet layer. This could be useful for long-range, cellular-only communications.
- In order to provide service interoperability between Member States, harmonisation should be done to integrate into one solution different signing approaches (occurring at facility layer, at network layer or at application layer) taking into account the constraints of communicating end user vehicles performance (hardware security modules cannot sign many messages per second) as well as C-ITS services performance constraints.
- Another difficulty on the hybrid link is that the information can be more widespread than on ITS-G5 and the reciprocity of the exchange of information might be requested by different stakeholders. However, the European C-ITS trust model allows a “club of senders” to send messages but doesn’t prevent others outside the club to receive and use the messages.

5.2 Trust models used for (mobile) internet services

A common model to realize trust in the context of internet services is via a so-called chain of trust. In this model, information is exchanged between peers that have an established relation with each other. For every relation, it is agreed what information is exchanged, and what standards and profiles are adhered to. Part of the agreement will also include how peers’ proof

that they adhere to these standards and profiles. In the operational phase, at a minimum, it is required that it can be established that the communication is taking place with the correct peer, i.e. the peer is identified in the operational phase.

In the complete implementation of a service, information can flow via systems of multiple entities, where every peer to peer communication is governed by an established relation with a related level of trust. In this way, a chain of trust is formed between the originating source of information and the final destination. As a baseline, the level of trust will generally only decrease when it flows via the chain. However, it is possible that a node in the chain can increase the level of trust by e.g. combining information from multiple sources, or by other means to validate the information in the messages.

The peer-to-peer trust relations can be established in many ways and at different layers in the OSI communication stack. For the end-to-end trust, it is not required that the same mechanism is used at every peer-to-peer connection in the full chain. At the lowest layer, physically secured network connections can be used, typically for connections within a single entity. At higher layers, Virtual Private Networks (VPN), IP Security (IPSec), or Transport Layer Security (TLS) can be applied. At higher levels in the OSI stack, authentication mechanisms based on simple username/password authentication, OAUTH, or SASL can be used. In the end, based on the specific technology and implementation details, a certain level of trust can be realized between peers, and in that way end-to-end.

The advantages of this model is that technical solutions can be optimized based on specific needs of specific stakeholders, and it is not required to agree on an overall solution with all stakeholders before services can be implemented. This model is well accepted in the mobile internet domain in general, but not yet applied to mobile C-ITS services specifically. As the end-to-end trust is build-up of the trust on every peer-to-peer connection in the chain, every intermediate (relay) node needs to be trusted as well: relaying via untrusted nodes is not possible[5]. Furthermore, integration with ITS-G5 trust model to come to a truly hybrid model might prove difficult.

For the chain-of-trust model, it is unclear how to convert specific technology solutions to trust levels. This is required to determine the overall end-to-end trust level. Technical specifications of the European C-ITS trust domain are to a large extent finished and implementation is underway; the chain of trust has a lot of freedom for implementation. It could be useful to investigate to what extent the architecture, trust model, and/or technical specifications of the

[5] In this context, only nodes that operate on the level where the trust is technically implemented are considered; so, if the trust is realized on the application level, intermediate nodes on the network level (e.g. routers) are not considered to be part of the chain of trust.

European C-ITS trust domain as developed for ITS-G5 communication could be used also for the chain of trust. For example, it could be investigated whether the Certificate Policy of this trust domain can be used when providing certificates that are used in VPN or TLS implementations. This would most likely require modifications of the Certificate Policy, but would allow operating in the same trust domain, independently from whether individual messages are signed based on TS 103 097 or the connection between peers is secured via VPN or TLS.

6 Example solutions currently defined and/or implemented

6.1 SCOOP@F solution, mixing chain of trust and signed messages

For the French C-ITS projects (SCOOP@F, C-Roads France, InterCor), a complete and harmonised C-ITS hybrid architecture has been developed. It makes sure that the same message going through different channels of communication can be understood. The functional links are shown in the figure below.

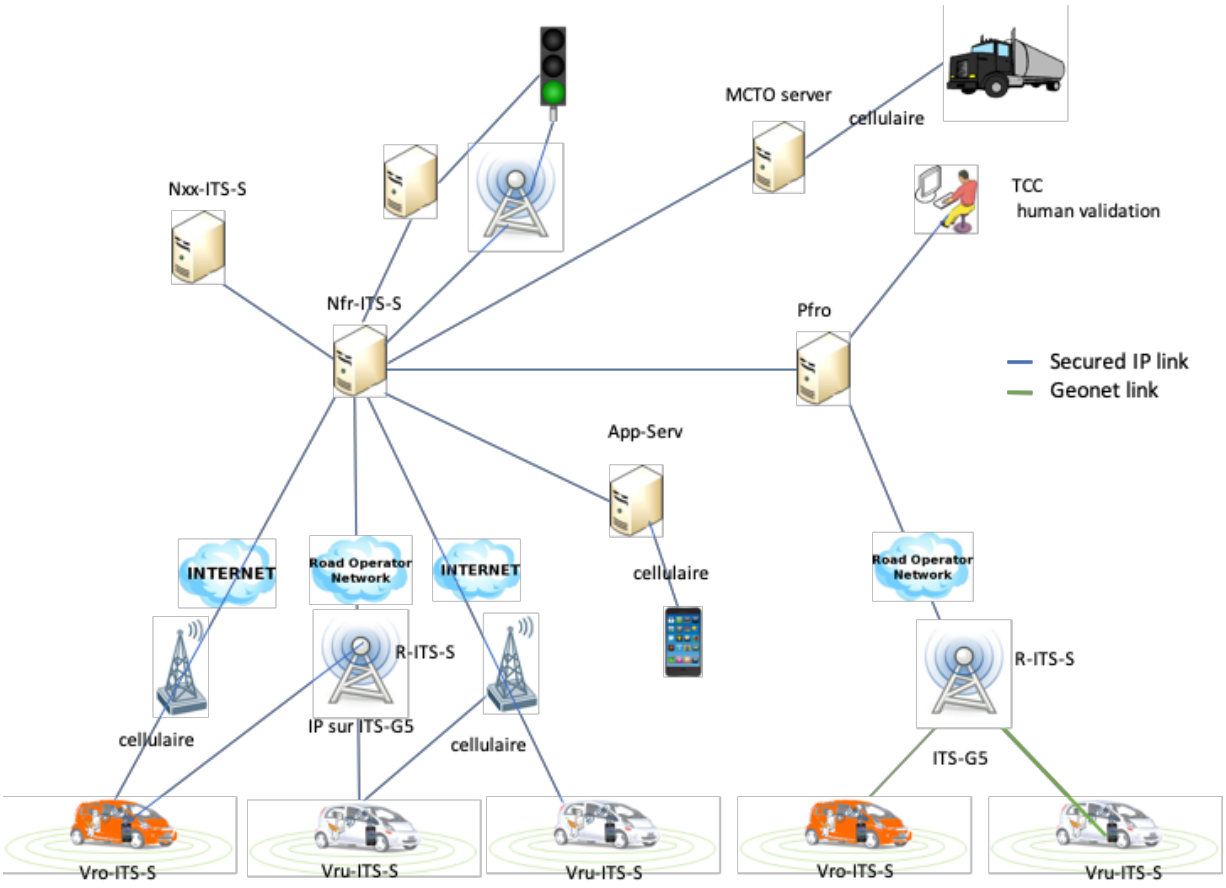

Figure 6.1: Functional diagram of the French hybrid architecture.

The Nfr-ITS-S is the French National ITS station. As any C-ITS station, it is enrolled in the French PKI.

It has two main functions:

- Router for any C-ITS message, with notably geographical filtering functionality; it also implements the IF2 to communicate with any back-end server, including foreign C-ITS stations;

- Receiver of Datex II messages and building C-ITS messages from them (functions for road operators), like any roadside ITS station in France; it also works the other way around; furthermore, it adds some specific road operator functions, such as the aggregation of CAM messages.

The detail of the messages exchanged between the Nfr-ITS-S and other servers is shown in the figure here below.

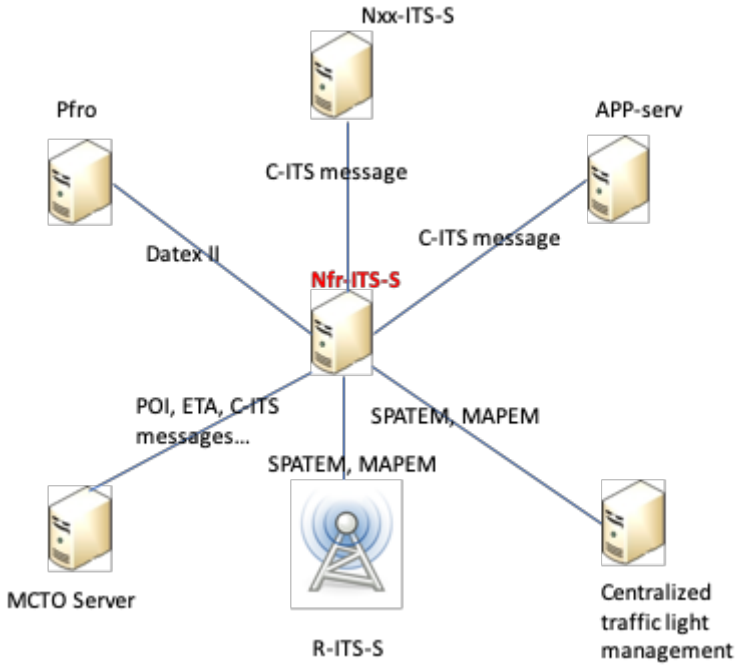

Figure 6.2: Messages exchanged between the Nfr-ITS-S and other servers.

The trust is established at two levels between the different entities:

- on the C-ITS links:
  - on the link itself: TLS 1.2 is used with the exchange of x509 certificates;
  - for each message: messages are exactly the same ones signed on the ITS-G5 link (including the Geonet header) within the C-ITS trust domain – the Nfr-ITS-S verifies each message that arrives before forwarding it (or publishing it) on every link;
- on the non C-ITS links: specific bilateral solutions between the French Ministry and road operators have been defined.

The figure below illustrates the definition of the technical interfaces.

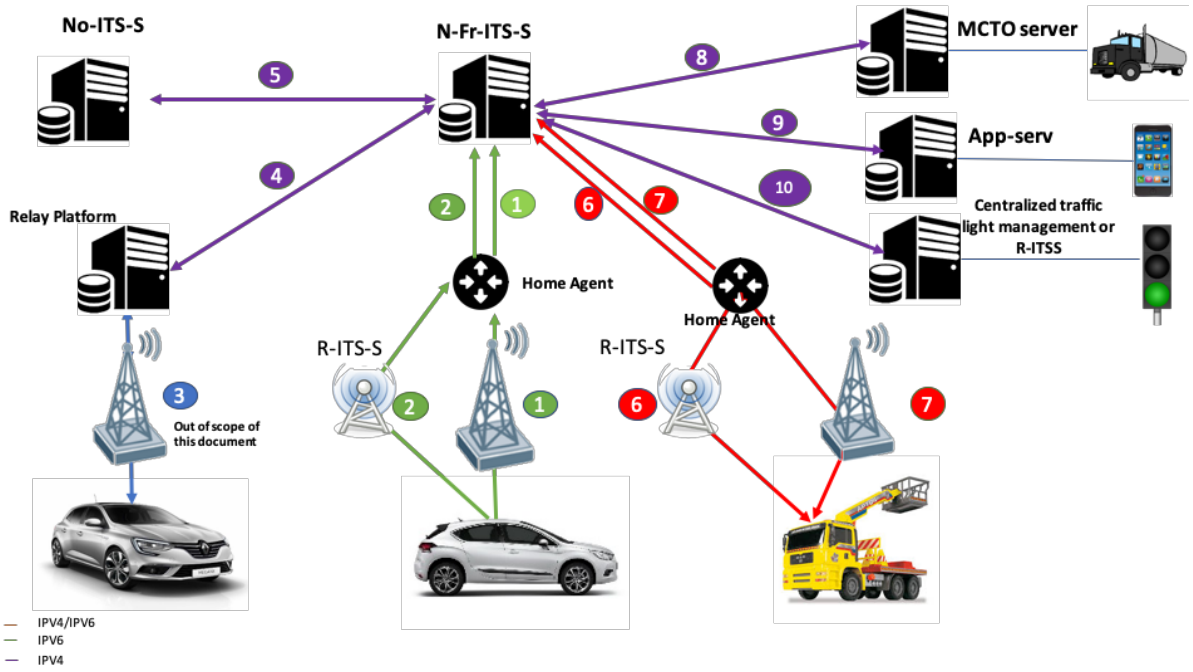

Figure 6.3: Definition of the technical interface for the harmonized French hybrid C-ITS architecture.

The choice was made to secure C-ITS messages for the interfaces numbered 1, 2, 4, 6 and 7 by using signature at Geonet layer and to use DSMIP tunnels for IPv6.

This choice was made because for now the standards allow only such implementation. It was also difficult for the vehicles to sign twice and some vehicles were directly connected to the Nfr-ITS-S.

Table 6.1: Summary of the communication stacks used on the interfaces of the French harmonized hybrid architecture.

Interface	Communication stack	Downlink messages	Uplink messages
1	ASN1 u-per / BTP / Geonet / TCP / IPv6 / cellular security at Geonet level implementation of DSMIP tunnel	DENM IVI SPATEM MAPEM POI	CAM , DENM
2	ASN1 u-per / BTP / Geonet / TCP / IPv6 / ITS-G5 security at Geonet level	DENM IVI SPATEM MAPEM POI	CAM and DENM
3	Out of scope		
4	IF2 from InterCor ASN1 u-per / AMQP / TCP / IPv4 security at Geonet level	DENM	DENM IVI SPATEM MAPEM POI

Interface	Communication stack	Downlink messages	Uplink messages
5	IF2 from InterCor ASN1 u-per / AMQP / TCP / IPv4	DENM IVI SPATEM MAPEM POI	DENM IVI SPATEM MAPEM POI
6	ASN1 u-per / BTP / Geonet / TCP / IPv6 or IPv4 / ITS-G5 security at Geonet level	DENM IVI SPATEM MAPEM POI	CAM and DENM
7	ASN1 u-per / BTP / Geonet / TCP / IPv6 or IPv4 / cellular security at Geonet level implementation of DSMIP tunnel if using IPv6 link	DENM IVI SPATEM MAPEM POI	CAM et DENM
8	IF2 from InterCor ASN1 u-per / AMQP / TCP / IPv4 security at Geonet level	DENM IVI POI	DENM POI ETA information
9	IF2 from InterCor ASN1 u-per / AMQP / TCP / IPv4 security at Geonet level	DENM IVI SPATEM MAPEM POI	DENM
10	IF2 from InterCor ASN1 u-per / AMQP / TCP / IPv4 security at Geonet level		SPATEM, MAPEM

6.2 GLOSA solution by Talking Traffic, based on chain of trust

The Dutch project Talking Traffic has developed specifications and implementations C-ITS services based on cellular communication. One set of services are related to signalized intersections, see figure below.

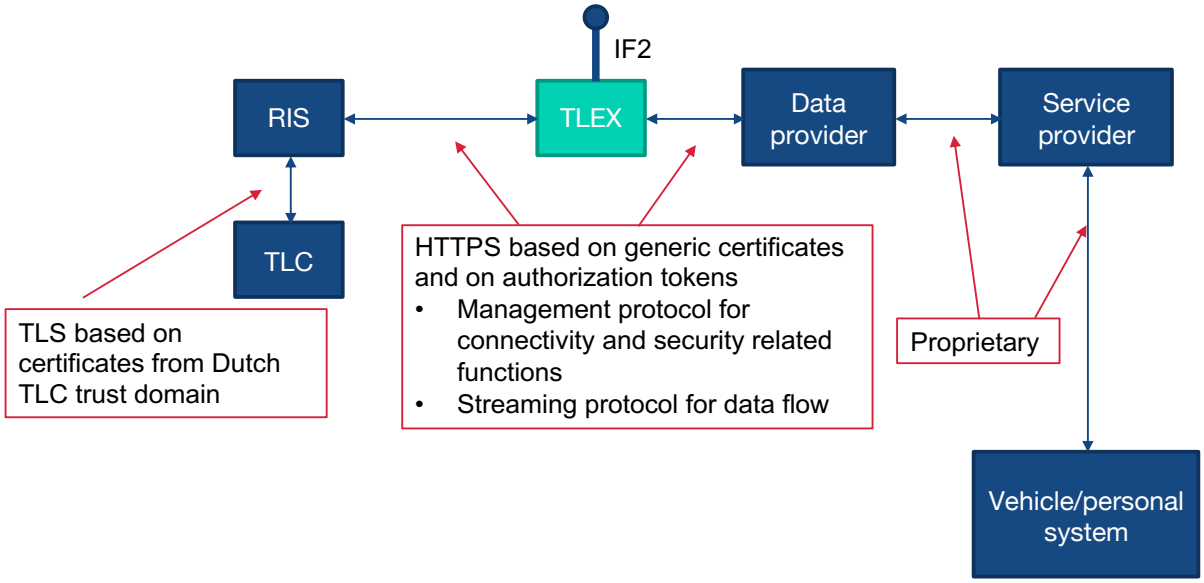

Figure 6.4: Schematic overview of the systems used in the Talking Traffic project for signalized intersection based services.

A new architecture and interfaces have been developed for the so-called Intelligent Traffic Light Controller (iTLC, or iVRI in Dutch). Without going into details of that architecture, a relevant aspect is that the Roadside ITS Station (RIS) is functionally separated from the rest of the traffic light controller. The interface between the RIS and the rest of the TLC is based on IP communication, and is secured with TLS. The certificates used for this interface are provided from a dedicated “TLC” trust domain. Access to this trust domain is granted after an established compliance assessment process has been completed.

All RIS communicate with a central system called TLEX (Traffic Light Exchange), which is the central node. The interface between the RIS and TLEX contains both a management protocol, based on HTTPS/web services technology, and a streaming protocol for the exchange of actual ASN.1 encoded, standardized messages. The link is secured based on TLS with generic (internet) certificates and temporary authorization tokens. Access to TLEX is granted after successful completion of a compliance and interoperability test program.

Multiple data providers can obtain the data from TLEX, based on a similar interface and trust model as is in place between the RIS and TLEX, which includes: separate management and data flow protocols, security implemented based on generic certificates and authorization tokens. Also for this interface, access is granted based on the successful completion of a compliance and interoperability test program[6].

[6] As an extension to the Talking Traffic specifications and implementation, an implementation of IF2 has been added to provide the MAP and SPAT data for the realization of the InterCor GLOSA service.

Data providers can enrich the information with data from other sources, and can provide additional services to service providers, e.g. managing what information is relevant for what end-user. The (business) relation between data providers and service providers (that have the direct relation with end-users) is up to the data and service provider. Also the technical interface and method to establish the trust relation is not prescribed. This is also true for the message exchange between the service provider back-end and end-user device[7] (vehicle or personal system).

Via the same data path and trust relations, also information from the vehicles/personal systems is communicated to the RIS connected to the traffic light controllers. For the two interfaces to TLEX, CAM and SRM messages are exchanged towards the traffic light controllers.

In summary, the trust within this eco-system is based on agreed specifications, interoperability and compliance test specifications, and various ways of identification and authentication on link level for the various interfaces. The current specifications do not include signing of individual messages. It is currently under investigation whether there is an added value in (also) supporting the exchange of signed messages to increase the level of trust. This could be used, e.g. for the SRM messages containing priority request. If and how this would be realized is still under investigation as part of a possible future upgrade of the specifications.

[7] Strictly speaking, it is not even required that the service provider has a back office that is part of the real-time data flow; it is possible that the data provider delivers the data directly to the vehicle or personal system, without (technical) intervention of a back office system of the service provider.

7 Technical challenges

Several technical challenges still remain to realize end-to-end trust. For the application of the European C-ITS trust domain, complete technical specifications do not exist yet. The current specifications assume that messages are signed on the Geonet layer. The current and previous versions ETSI TS 103 097 specify how a message included in a Geonet layer should be signed, and how the required information to interpret the signatures can be exchanged. The Geonet protocol is designed to be used on ad-hoc broadcasting networks. Although it is technically possible to use other OSI layer 2 protocols than ITS-G5, the protocol has been developed based on (implicit) assumptions of ITS-G5, like a strong link between message reception and geographical distance, open broadcast (i.e. without encryption on lower layers), and limited reliability. Furthermore, the purpose of the protocol is to be able to handle the limitations of such ad-hoc broadcast networks. Therefore, it is unclear what the added value is for the inclusion of a Geonet layer on the cellular link of a hybrid communication solution, and what modifications to the Geonet standard are required to make it fully operational on cellular networks. So, although inclusion of the Geonet layer has the advantage that specifications exist on how to sign messages, the overall solution is not well defined, and it is not evident whether it would be technically the most appropriate solution. This solution has been implemented and tested in France.

The messages could also be signed at the facilities layer. The signing principles from TS 103 097 can also be applied to a payload that only contains the UPER encoded message, but the details need to be worked out and tested in pilots. Furthermore, as this solution is not yet standardized, it is not generally supported by existing systems implementing the European C-ITS trust domain. Signing messages at different layers will require every message to be signed twice in hybrid C-ITS stations, which might impact the performance.

A more practical technical choice is the version of the security standard to use. InterCor has decided to use TS 103 097 version 1.2.1 for the IF1 interface (ITS-G5), and the use of the same standard on IF2 would be a logical choice. Other European initiatives have already decided to use the newer version of the standard, version 1.3.1, which would be more future proof. The choice of the version is irrespective of whether the signing will be done on the facility or Geonet layer. Although this is “just” a technical choice related to the moment in time (also all InterCor Member States have expressed the intention to migrate to the new standards), the issue of (backward) compatibility will remain relevant also in the coming future. As the context of hybrid communication is more complex than for ITS-G5 stand alone, the issue of future upgrades will also become more complex. A clear approach supporting future upgrades needs to be developed, possibly before deployment.

8 Summary and Conclusions

Three models have been discussed for the implementation of IF2. These mainly differ on how data is aggregated and distributed amongst the Member States back offices: services providers can obtain the data from the country of origin (national node), a single point of contact per country can aggregate all data from other Member States and forward it to its local service providers, or a single central aggregation point can be established at European level, where all data from all Member States comes together and is redistributed to all services providers. These models are not mutually exclusive and mixed forms can also be implemented. Various advantages and disadvantages have been presented. Within InterCor, no decision has been taken on what model is the preferred implementation.

Two trust models have been presented and discussed that can be used to establish the required level of trust in cellular communication in the context of hybrid communication. Descriptions of these models are provided, including some of the identified strengths and weaknesses. Practical examples of two implementations have been described as well. Existing security and communication standards need to be further optimized in order to support an interoperable and harmonized solution over IF2 to deploy C-ITS services based on hybrid communication at European level. What ultimately is required is a solution that is optimised for hybrid communication, where C-ITS stations can either implement only ITS-G5 communication, only cellular communication, or a combination of both.

9 References

[1] InterCor, "Milestone 4 - Common set of upgraded specifications for Hybrid communication. Specifications for IF2 for hybrid communication version 1.0", 2018. *Note: superseded by [8]*

[2] InterCor, "InterCor_A2.1_a_002 Use Case Comparison", 2017.

[3] InterCor, "Milestone 6 Common set of upgraded specifications for Services v.2.0", 2019.

[4] Project Talking Traffic, "RFP Talking Traffic 1.1_Bijlage 9 Latency Tabel_Beter Benutten_2016.07.01.pdf", 2016.

[5] amqp.org, "AMQP Advanced Message Queuing Protocol, Protocol Specification, version 0.9.1", 2008.

[6] ISO, "EN ISO 17423:2017 Intelligent transport systems -- Cooperative systems -- Application requirements and objectives", 2017.

[7] InterCor, "Milestone 3 - Common set of upgraded specifications for ITS-G5 v1.1", 2017.

[8] InterCor, "Milestone 4 - Common set of upgraded specifications for Hybrid communication. Specifications for IF2 for hybrid communication version 2.1", 2019.

[9] Igor Passchier, "InterCor Deployment models for IF2", version 1.0, 5-4-2018.

[10] C-ITS Platform Phase I "Final report", Jan. 2016; C-ITS Platform Phase II "Final report", Sep. 2017, both available at https://ec.europa.eu/transport/themes/its/c-its/.

[11] ETSI "TS 102 940 v1.3.1 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management", 25-4-2018

[12] ETSI "TS 102 940 v1.3.1 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management", Feb. 2019

[13] C-ITS Platform Phase II, "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)", Release 1, June 2017, https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf

