Ecosystem for fully operational C-ITS service delivery

The infrastructure perspective

WG1 - C-ITS Organisation

V 0.91

14.03.2022

Co-financed by the European Union
Connecting Europe Facility

Index

Document history

Version	Date	Description, updates and changes	Status
0.1	13.11.2020	First draft	draft
0.1.1	10.12.2020	Feedback from WG1	draft
0.2	10.02.2021	First draft version for technical and organisational elements	draft
0.3	09.03.2021	Contribution to main chapters	draft
0.4	11.03.2021	Finalisation of part 1 for SCOM approval	draft
0.5	05.05.2021	Feedback of first part after SCOM meeting	draft
0.6	14.07.2021	Draft of the possible governance structures	draft
0.7	27.07.2021	Draft chapter 6	draft
0.8	25.10.2021	Updated draft version	draft
0.9	7.12.2021	Preparation of first final draft version	First final draft
0.91	14.03.2022	Final draft version	Final draft

Authors

Name	Affiliation
Alexander Frötscher	AustriaTech (Austria)
Dimitris Sermpis	Attikes Diadromes SA (Greece)
Eric Kenis	Departement Mobiliteit en Openbare Werken (Belgium/Flanders)
Fred Verweij	Rijkswaterstaat (The Netherlands)
Ilkka Kotilainen	Traficom (Finland)
Gary Crockford	DfT (UK)
Janez Čokl	DARS (Slovenia)
Johan Scholliers	VTT (Finland)
Marek Scerba	VSK (Czech Republic)
Martin Böhm (editor)	AustriaTech (Austria)
Martin Pichl	Ministry of Transport (Czech Republic)
Savin Gorup	Asist (Slovenia)
Stephanie Metzner	Die Autobahn GmbH (Germany)
Sophia Chirskaya	North Italy Communications (Italy)
Sukku Phull	DfT (UK)
Torsten Geissler	BASt (Germany)

List of abbreviations used

3G	3rd generation mobile network
4G	4th generation mobile network
5G	5th generation mobile network
AA	Authorisation Authority
ADAS	Advanced Driver Assistance System
ATIS	Advanced Traveller Information systems
C2C-CC	Car to Car Communication Consortium
CA	Certification Authority
CAM	cooperative awareness message
CAN	Controller Area Network
CCAM	Cooperative connected automated mobility
CCG	Collaborative C-ITS governance
C-ITS	Cooperative Intelligent Transport Systems
COM	Communication
CPA	Certificate Policy Authority
CPoC	C-ITS Point of Contact
CRL	Certificate Revocation List
CSO.Infra	C-ITS Station Operators - Infrastructure
CSO.OEM	C-ITS Station Operators - OEM
CSO.SO	C-ITS Station Operators - Service operator
DATEX II	Data exchange standard
DNS	Domain Name Server
EA	Enrolment Authority
EC	European Commission
ECTL	European Certificate Trust List
EN	European Norm
ERCA	European Root Certification Authority
ETSI	European Telecommunications Standards Institute
EU	European Union
FAQ	Frequently Asked Questions
ICT	Information communication technology
ID	Identity Identifier
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organisation for Standardisation
ITS	Intelligent Transport Systems
ITS-G5	European implementation of WLANp
KPI	Key Performance Indicator
LTE	long-term evolution
NAP	National Access Point
NRA	National Road Authority
OBU	On Board Unit
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
PKI.O	PKI Operator
ppp	Public private partnership
R&I	Research and Innovation
RCA	Root Certification Authority
RSU	Road Side Unit
RTTI	Real Time Traffic Information
RWW	Road works warning
SRTI	Safety Related Traffic Information
TEN	Trans European Network
TISP	Traveller Information Service Provider
TF	Task Force
TLM	Trust List Manager
TLS	Transport Layer Security
TMC	Traffic Management Centre
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
VMS	Variable Message Sign
WG	Working Group
WLANp	Wireless Long Area Network based on the IEEE 802.11p and IEEE 802.11bd standards

1 Scope of this document

This document presents the infrastructure owners' and road authorities' perspective on an ecosystem for fully operational C-ITS service delivery.

The focus is thereby set on a permanent operation of C-ITS services, where all C-ITS stakeholders will need to work in close cooperation to ensure sustainable and consistent C-ITS services acceptable to end-users. As the currently running C-Roads platform focuses first on the road-infrastructure side of C-ITS service delivery and secondly on a harmonisation of C-ITS pilot deployments, there is a risk that the current structure will not be sufficient for guaranteeing continuous fully operational C-ITS service delivery.

In this context, this document covers C-ITS operations in a situation where either the C-Roads platform pilot projects have ended or a parallel C-ITS organisational structure is fulfilling "full operational" tasks, which are not in scope of the current C-Roads Platform. For full operations and broader deployments, a specific technical and organisational management structure for harmonised and operational C-ITS services, including all stakeholders, is considered necessary. The basis of such new multi-stakeholder structure needs to be a commonly agreed vision, which needs to be reflected in a common C-ITS Strategy of the European C-ITS stakeholders.

The document results from the collaboration between the C-Roads platform road authorities and the C-ITS pilot members.

2 C-ITS as next generation ITS

Intelligent Transport Systems (ITS) are defined in the EU Directive 2010/40/EU as “systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport”. According to the White Paper for the European transport policy for 2010, the balance between different modes of transport must be shifted, bottlenecks must be eliminated and users should be placed at the heart of transport policy. The Commission’s proposal regarding the technological developments in the field of intelligent transport systems includes among its priority objectives those of perfecting new technologies to back up the development of safe and clean modes of transport and developing the European transport systems. Moreover, specific KPIs regarding traffic and road safety are defined.

The ITS Action plan and directive involved a number of key issues for the deployment of ITS services such as: eCall, cooperative systems, vulnerable road users, traffic and travel information, intelligent truck parking, open in-vehicle platform, public data for digital maps and availability and access to road data.

ITS involves the following axes: road safety improvement, congestion reduction, reduction of pollution, trip convenience and user integration. ITS may be classified in distinct categories. Examples include Advanced Driver Assistance systems (ADAS) i.e. systems that assist the driver considering the driving tasks, Advanced Traveller Information systems (ATIS) i.e. systems that provide information to the traveller (pedestrian, cyclist, driver, public transport user) and autonomous vehicles.

The direct interaction between users of the transportation system and the transport infrastructure is the domain of Cooperative Intelligent Transport Systems (C-ITS). More specifically, it will allow road users and traffic managers to share information and use it to coordinate their actions. This cooperative element – enabled by digital connectivity between vehicles and between vehicles and transport infrastructure – is expected to significantly improve road safety, traffic efficiency and comfort of driving, by helping the driver to take the right decisions and adapt to the traffic situation. Furthermore, communication between vehicles, infrastructure and other road users is also crucial to increase the safety of future automated vehicles and their full integration in the overall transport system. Cooperation, connectivity, and automation are not only complementary technologies; they reinforce each other and will over time merge completely.

While ITS focus on digital technologies providing intelligence placed at the roadside or in vehicles, C-ITS focuses on the communication, interaction and cooperation between those systems – whether it is a vehicle communicating with another vehicle, with the infrastructure, with other users (e.g. pedestrians) or in future with other C-ITS systems.

Intelligent Transport Systems embrace a wide variety of communications-related applications intended to improve road safety, minimize environmental impact, improve traffic management and maximize the benefits of transportation considering both commercial users and the general public. In C-ITS, users communicate with each other and/or with roadside infrastructure, greatly increasing the quality and reliability of information available about the vehicles, their location and the road environment. This will bring major social and economic benefits and lead to greater transport efficiency and increased safety.

However, the upcoming wide deployment of C-ITS services must smoothly match and build upon the ongoing use of ITS services. The C-ITS services must be supplementary to ITS services. To ensure that, C-ITS services ideally will be harmonised throughout Europe as well as ensure synergies with the already existing ITS services whenever needed. Hence, the benefits for all services such as traffic management, real-time traveller information, road safety, etc. will be further enhanced by the use of C-ITS services.

Most service providers, which include public and private sector, are on the whole trusted organisations. Most of the data originates from their respective infrastructure operators and information systems whilst some may be derived from infrastructure users. These systems normally have some kind of data filtering and validation policy in place. It is feasible that C-ITS systems take advantage of existing policies to provide the road users information which is consistent with other dissemination channels.

3 From pilots to continuous operations - including system maintenance

As a starting point the currently active actors and their roles within up and running C-ITS deployment pilot activities in the frame of the C-Roads platform will be described. This is especially useful in understanding the roles and contributions of different actors which in turn is helpful in identifying the required governance structures for continuous C-ITS service operations.

In a second step the different platforms relevant to C-ITS service operations will be described with a focus on their possible contribution to the C-ITS ecosystem.

Finally a short analysis of applicable business models for C-ITS service operation in a European ecosystem will be carried out, followed by a discussion on the needs for European harmonisation and collaboration.

3.1 Actors and roles within C-ITS pilots

3.1.1 Public Authorities

One of the main important actors for the successful deployment of C-ITS services are public authorities. Pubic authorities are defined as any government or other public administration, including advisory bodies at national, regional or local level (e.g. city level) or any natural or legal person performing public administrative functions under national law (including specific duties).

Public authorities have a primary role in the evolution and use of C-ITS services because they are responsible for setting future policies in the area of transport and deployment activities. The overall responsibility lies with them both in terms of policy decision and budget allocation/monitoring.

Furthermore, public authorities are responsible for establishing rules and regulations on safety, security and environmental provisions that may impact vital elements of the overall C-ITS system. Furthermore, pubic authorities may assume a role in the provision and maintenance of security infrastructure. Public authorities have a crucial role to play in the generic C-ITS value chain.

Public authorities need to be actively engaged in developing and implementing ambitious sustainable energy policies and plans. This will create awareness, understanding and support of the overall societal and macro-economic benefits of C-ITS services.

3.1.2 European Commission

The European Commission is primarily acting as the facilitator in both the research and the deployment in the field of C-ITS services. Therefore, it has adopted a European Strategy on Cooperative Intelligent Transport Systems (C-ITS) [1] a milestone initiative towards cooperative, connected and automated mobility. Towards this direction, the European Commission has taken steps in many directions such as convergence of investments, regulatory framework, international cooperation, coordination, harmonizing and providing security-certificates for C-ITS services in its Member States.

[1] A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility (COM(2016) 766)

One core element, which is currently set up by the European Commission, is the provision of security certificates for C-ITS services. In this domain recent EU initiatives include:

- C-ITS Point of Contact (CPOC) Protocol

  CPOC is fully hosted by the European Commission and is a set of definitions of secure protocols for exchange of root CA certificates, which are used to create the European Certificate Trust List (ECTL) to be distributed to the C-ITS stations in Europe.

- European Root Certification Authority (ERCA)

  The ERCA generates PKI root key pairs and respective certificates along with link certificates to create a chain of trust between different root certificates

- European Certificate Trust List (ECTL) and Trust List Manager (TLM)

  Member States have the obligation to establish, maintain and publish trusted lists of qualified trust service providers and the qualified trust services provided by them. Both are fully hosted by the European Commission.

Moreover, the 2018 EU strategy for mobility of the future set out a specific action to implement a pilot on common EU-wide cybersecurity infrastructures and processes needed for secure and trustful communication between vehicles and infrastructure. This sub-group on Cooperative Intelligent Transport Systems (C-ITS) shall assist the Commission in working on the implementation of the aforementioned pilot and to foster exchange of experience and good practice in the field of C-ITS.

3.1.3 Infrastructure operators

Infrastructure operators dealing with C-ITS services can be divided into road operators, rail operators and public transport operators. The role of infrastructure operators is to operate and maintain a road or rail network and in the case of public transport especially a bus and tram network. In specific circumstances infrastructure operation is carried out by third-parties as a concessionaire on behalf of a public authority under specific legal terms.

Hence, the main responsibility of the road operator is to contribute to policy goals along their road network, which are to sustain a high road safety levels and a high level of service. A similar responsibility is expected of rail and public transport infrastructure operators e.g. in the case of railway level crossings and tramway networks. At the same time, all of them need to ensure environmentally friendly transport operations.

The road operator has an important role in the ecosystem evolving around deployed C-ITS services. It can entail, but not limited to, provisioning data and consuming data, procuring, installing and maintaining physical ITS-infrastructure, all with the intent and purpose to benefit the road users. In order to ensure policy goals and the service to the road users, the road operator will evaluate, monitor and assess the deployed C-ITS services.

3.1.4 Component and equipment suppliers

Component and equipment suppliers are the actors in the C-ITS services chain who provide all the necessary components and equipment for these services. Their role is crucial in the commercial viability of these services on the market and other overall business opportunities that C-ITS services can bring.

Both the separate components and the respective equipment for the deployment of the C-ITS services need to guarantee and maintain high performance including security.

3.1.5 Automotive

Automotive actors include all kind of Original Equipment Manufacturers (OEMs) mainly referring to car manufacturers in the automotive industry. Their role in the deployment of C-ITS services is very significant as it has also been proven throughout the years in the field of Transport.

No matter whether research in the area of transport is initiated by the European Union and other research entities (e.g. universities), the automotive actors are the ones that need to be convinced for the importance of this research in order to move to mass production and adoption of these initiatives. Their financial power is also of vital importance for the enhancement of this research.

This is also the case with the deployment of C-ITS services. The automotive actors are the ones who will be responsible for the mass production of cars being equipped with all the necessary equipment (e.g. communication equipment, On-Board Units (OBUs) to participate in the chain of C-ITS services. The automotive actors are the ones who will contribute to the wide uptake of C-ITS services by the adoption of the necessary equipment in the cars and hence contributing to the uptake of services such as V2I or V2V.

3.1.6 Mobile Network Operators

Mobile network operators are crucial for the successful deployment of C-ITS services since they will provide the telecommunication system to efficiently set up the cellular network for the transmission of information between the infrastructure and the vehicles.

Mobile Network Operators are responsible for providing a communication network, which will be then used for the exchange of C-ITS information; this can be achieved either using short-range peer to peer communication (where today ETSI ITS-G5 is in deployment but might be extended to other short-range communication interfaces), or commercially available long-range cellular (3G, 4G LTE and 5G) or a combination of both.

The existing commercial cellular network and fast evolution in the field of telecommunication (e.g. introduction of 5G) must contribute to the fast and wide uptake of the C-ITS services, since it will provide new opportunities in the field of transport and telecommunications. Hence, Mobile Network Operators are the ones who will contribute with their knowledge and new forthcoming opportunities not so much to sustain the use of the C-ITS services, but to provide an initiative for further development and deployment.

3.1.7 Service providers

Service providers make available to C-ITS stakeholders services that provide access to data that is necessary for the delivery of C-ITS services. Often this data has its origin in road operators and OEMs. However, it is expected that also 3rd party service providers such as map makers, telecommunication companies, etc. are also providing services.. In addition, map makers provide the basis for the necessary accurate referencing of the C-ITS messages through the method of geo-messaging.

3.1.8 C-ITS service operators

C-ITS service operators are defined as the organisations supplying C-ITS service(s) to one or more customers (which can include both, end users and other organisations). They are the ones who provide the actual services to the end users or the ones who support and design the platforms on which these services are designed and operated. In both cases, C-ITS service operators are a key in the whole C-ITS service life cycle including the deployment of the C-ITS services and their wide uptake.

C-ITS service operators include road operators, OEMs, 3rd party service providers including map makers, telecommunication companies, etc. who are offering C-ITS services and provide data (such as RWW trailer), end-user applications and backend cloud solutions.

C-ITS service operators are important in the deployment of C-ITS services since they are important for the provision of accurate and reliable services to end users.

3.1.9 National Access Points and nominated bodies

The entire set of Delegated Regulations supplementing the ITS Directive 2010/40/EU, in the present context most notably the Delegated Regulations on Safety Related Traffic Information (SRTI) and Real Time Traffic Information (RTTI), require Member States and other third party countries to set up National Access Point(s) (NAP) and appoint an independent body for assessment of compliance (nominated body). Member States have embarked so far on different paths for NAPs (e.g. Metadata Directory, Data Marketplace, Data Warehouse) and are likely deploy different models to exchange ITS data/services over their interchange nodes in an interoperable way.

Even though C-ITS is not specifically mentioned in the existing Delegated Regulations so far, C-ITS services are supplementing existing and operational ITS services and as a minimum the underlying data might be used for several ITS service channels, including C-ITS services. Therefore, specific roles for supporting C-ITS operations can be seen with National Access Points (incl. some implementation considerations):

- Providing a **registry of C-ITS service providers**, both private and public (like road operators). Especially, when C-ITS services are provided by road operators, it might be important for C-ITS Service providers to integrate C-ITS services of different road operators into their end-user services. In addition, as in many countries road operation is not done by a single road authority, but several road authorities are operating their specific road network (which might be urban, interurban or nation-wide), such a registry will provide the link to the respective C-ITS service interface. Is it also vitally important that end-users do not receive conflicting messages from different service providers in particular for safety related applications based on missing alignments.

- Such a registry might also **link to service interfaces for in-vehicle data**. Under the revision of the ITS Directive and its Delegated Regulations access to in-vehicle generated data is one of the data elements considered. Here the same logic applies as before: getting knowledge about service interfaces up and running for a specific region might be crucial for C-ITS service delivery.

- A third element, which might be relevant for National Access Points and/or nominated bodies, is with a **monitoring of deployed services** in a hybrid C-ITS environment. Currently the TEN-TEC interactive map shows the location of deployed C-ITS short-range RSUs and services they support across Europe. In future such a deployment map for single Member States might be accessible via National Access Points covering services deployed, security mechanism in place, and communication channels used.

In addition, Member States should provide clarification about the role of their NAP and the associated value chain for the reliable delivery of ITS/C-ITS messages including the **assessment of compliance** using an independent assessment of compliance body for safety related use cases. This assessment of compliance of safety related C-ITS services and their underlying data might become an additional task in the responsibility of NAPs and/or nominated bodies in conjunction with the ITS Directive's Delegated Regulations.

3.2 Stakeholder platforms dealing with C-ITS service delivery

The list of identified stakeholder platforms is only an excerpt of the most important ones dealing with C-ITS operations. Here major platforms dealing with C-ITS research and development topics (e.g. POLIS, ERTICO) or industrial platforms (e.g. ACEA, FIA, CLEPA) are not listed.

3.2.1 C-Roads Platform

The C-Roads Platform (www.c-roads.eu) is a joint initiative of 18 European Member States and their road operators for piloting and deploying C-ITS services focusing at cross-border harmonisation and interoperability. Common technical specifications, including the common communication profiles, are developed, shared and published. Intensive cross-tests are performed to verify interoperability. In addition, system tests are undertaken based on the common communication profiles by focusing on hybrid communication mix, which is a combination of ETSI ITS-G5 and operational cellular networks.

3.2.2 CEDR

CEDR (www.cedr.eu) is the Road Directors' platform for cooperation and promotion of improvements to the road system and its infrastructure, as an integral part of a sustainable transport system in Europe. CEDR's Focus Area Digitalisation and Innovation encompasses activities related to Connected and Automated Driving, Future Transport and Innovation Activities. Specific objectives are providing the 'eyes and ears' of CEDR and NRAs with regard to European and global developments in a fast-moving domain of ITS and connected & automated transport.

3.2.3 Car 2 Car Communications Consortium

The CAR 2 CAR Communication Consortium (www.car-2-car.org) is a non-profit, industry driven organisation initiated by European vehicle manufacturers and supported by equipment suppliers, research organisations and other partners. The C2C-CC is dedicated to the objective of further increasing road traffic safety and efficiency and support automation by means of cooperative Intelligent Transport Systems (C-ITS) with Vehicle-to-Vehicle Communication (V2V) supported by Vehicle-to-Infrastructure Communication (V2I). The C2C-CC focuses on ad-hoc short-range communication and considers other means of communication like cellular where required. It supports the creation of European standards for communicating vehicles spanning all brands and cross border. As a key contributor, the C2C-CC works in close cooperation with the European and international standardisation organisations.

Within the C2C-CC a "**Special Working Group for Operations**" was formed. The objective of this working group is to offer a public and single point of contact for all questions and topics that are being raised while operating C-ITS Stations. This group complements the Deployment Working Group by focusing on all operational and procedural aspects related to operations and maintenance of C-ITS stations on the roads. The Special Working Group for Operations explicitly requires an equal status between vehicle manufacturers and C-ITS infrastructure operators and their suppliers with active operations to be able to address and resolve interoperability-related topics.

3.2.4 ASECAP

ASECAP's (www.asecap.com) mission is to promote toll as the most efficient tool to finance the construction, operation and maintenance of motorways and other major road infrastructures.

ASECAP and its members are committed to exchanging information and experience, participating in research programs and further developing and enhancing the direct “user/payer” toll system as an instrument of a sustainable, safe and environmentally friendly transport policy. Secondly ASECAP is strengthening the efficiency of their networks and permanently improving the level of services provided to the European citizens, by keeping up with the latest technology developments and the best operational practices.

3.2.5 5GAA

The 5G Automotive Association (www.5gaa.org) is a global, cross-industry organisation of more than 130 automotive, technology, and telecommunications (ICT) companies, working together to develop end-to-end connectivity solutions. 5GAA bridges the automotive and telecommunication industries in order to address society’s connected mobility and road safety needs with applications such as automated driving, ubiquitous access to services and integration into intelligent transportation and traffic management. The objectives of the association are to evolve, test and promote cellular technology-based communications solutions, to support their standardisation and to accelerate their commercial availability and global market penetration.

3.2.6 EATA

EATA (www.eata.be) is a unique forum for cooperation between Europe's automotive and telecoms sectors: the main aim is to jointly explore how to best accelerate the deployment of connected and automated mobility (CAM) in Europe.

3.2.7 C-ITS Deployment Group

The C-ITS Deployment Group (www.c-its-deployment-group.eu) is a promotional association of vehicle manufacturers, road infrastructure providers, authorities and federal states, as well as industry, and research partners, which aims to increase road safety and decrease congestions on Europe´s motor- and expressways by deploying C-ITS. It brings together the most prominent automotive manufacturing companies and interest groups in the traffic and transportation sector. The C-ITS Deployment Group is mainly a marketing platform for C-ITS deployments.

3.2.8 EC sub-group on Cooperative Intelligent Transport systems

The EC sub-group on C-ITS was set up under the Commission Expert Group on Intelligent Transport Systems. It supports the European Commission in the implementation of the pilot on common EU-wide cybersecurity infrastructures and processes needed for secure and trustful communication between vehicles and infrastructure for road safety and traffic management related messages and fosters exchange of experience and good practice in the field of C-ITS.

3.2.9 CCAM partnership

The CCAM Partnership aims at prioritizing and aligning European research and innovation (R&I) efforts to accelerate the implementation of innovative cooperative connected automated mobility (CCAM) technologies and services. As such it will foster chances for grasping the full systemic benefits of new mobility solutions enabled by CCAM: increased safety, reduced environmental impacts, and inclusiveness. By bringing together the actors of the complex cross-sectoral value chain, the partnership will execute the agreed shared, coherent and long-term R&I agenda. The Vision of the Partnership is: “European leadership in safe and sustainable road transport through automation”.

3.2.10 Data for Road Safety Initiative

The mission of the European Data for Road Safety Initiative (previously Data Task Force; www.dataforroadsafety.eu) is to improve road safety by maximizing the reach of safety-related traffic information powered by safety data generated by vehicles and infrastructure. The Data Task Force was structured around 3 core principles:

- Working together to make driving safer: Safer driving is a shared vision amongst government and industry stakeholders and is a key founding for this public-private partnership.
- Safety without compromise: Vehicle data has the potential to save lives. By making safety data a priority and share data across brands and across borders, we can maximize the benefit it brings and enhance road safety.
- A fair and trusted partnership: The Data Task Force is a trusted partnership of government and industry stakeholders that enables fair competition.

3.2.11 EU-EIP

The EU ITS Platform (https://eip.its-platform.eu) is the place where National Ministries, Road Authorities, Road Operators and partners from the private and public sectors of almost all EU Member States and neighboring countries, cooperate in order to foster, accelerate and optimize current and future ITS deployments in Europe in a harmonized way. Sub-Activity 4.4 - Cooperative ITS Services Deployment Support - aims at developing and providing deployment guidance to road authorities and operators on Cooperative ITS (C-ITS). Following objectives of the sub-activity are set:

- Ensuring functional interoperability of infrastructure-vehicle (and vice versa) applications across the EU,
- Providing deployment guidance to road authorities and operators implementing C-ITS services with infrastructure involvement and consolidating lessons learned from pilot/continuous operation deployments in order to improve guidance,
- Preparing for C-ITS based services as part of regular operation,
- Making reference to previous important work quality criteria and assessment methodology for C-ITS use cases.

3.2.12 NAPCORE

NAPCORE (National Access Point Coordination Organisation for Europe) consists of representatives of National Access Points (NAP) and National Bodies (NB) for traffic and mobility data. The goals of this group which are relevant to C-ITS are primarily to strengthen the position and role of NAPs as backbone of European ITS, transport and mobility data/digital infrastructure; to work towards harmonisation and NAP interoperability; and to exchange best practices and experiences.

3.2.13 UITP

UITP is the International Association of Public Transport (www.uitp.org). When it comes to C-ITS services UITP contributes to traffic management and intelligent transport systems, including C-ITS in urban and public transport. This is especially important for operating urban use-cases as well as on-level railway crossings.

3.2.14 Platforms for harmonising data exchange

There are several platforms and associations existing that are relevant for C-ITS operations, as they mainly look on the harmonisation of data exchange. This is done primarily by making standard-based specifications for data- and service-exchange which are relevant for C-ITS service operation. These platforms include as example following associations: DATEX II, TN-ITS, TISA, etc.

3.3 C-ITS operations and business models in the ecosystem

‘C-ITS operations’ in the C-Roads platform is led by a consortium of infrastructure owners, road authorities and covers for collaboration with a variety of many other private partners and organisations. Many C-ITS actors and stakeholder platforms, as explained in the previous chapter, collaborate in many ways and agreements to deploy C-ITS services in specific pilot environments. Applicable business models, roles and organisational aspects have been studied in the C-Roads WG1 “Report on Legal and Organisational Structures for C-ITS Operation” and the “C-ITS Lessons learned and Legal structures”, reports which both can be found on the C-Roads webpage (www.c-roads.eu). The WG1 report also elaborates on business model results as reported by the WG3 Evaluation on basis of the pilot C-ITS implementations in Europe assessed. In addition, the C-Roads WG2 TF4 Hybrid communication has presented a variety of deployment models for hybrid communication backend communication in its specifications.

Both deployment and business models impact the operational management and financial liabilities as well as the roles and responsibilities assumed by ecosystem members. For example, public authorities, road operators and cities may take up a different role depending on their infrastructure ownership and service delivery. Similarly, OEMs, service providers and data aggregators may apply specific business models depending on the vehicles and services provided. Collaboration among C-ITS public and private stakeholders is required to foster harmonisation, scalability of services, reliability, innovations and higher quality of information for road users and road operators.

Therefore, a future governance structure for C-ITS service operation needs to take into consideration business models and piloted deployment models.

3.3.1 Public investments in C-ITS

Public investments in C-ITS should be oriented towards projects „in public interests“, i.e. projects that will contribute to improve traffic control and the flow of traffic, contribute to better road safety, to improve incidents management and further to improve public transport safety and its accessibility as well as to improve logistic processes for consignments required special supervision (e.g. transport of heavy and oversized loads). In these cases transport infrastructure operators and/or public transport operators will act as investors. Concerning C-ITS it is expected that investments, maintenance and operation costs from public budgets will be related to equipment for transport infrastructure as well as for the provision of C-ITS services (mainly transport information-related and road safety-related) on this transport network. Private sector can provide market driven C-ITS solutions. What private sector C-ITS value added services will be offered need to be decided by the private companies.

It is important to consider those cases in which data is handed over to third parties (subcontractors). It is necessary for this subcontractor to submit a proof of its registered office (in order to enforce requirements of EU legislation) and to inform where the data processing infrastructure is really based, who controls it and how the technical data protection system is implemented. When handing over the data to third parties, the contract represents the main tool to ensure the quality of service and to protect the data. This is why contracts governing data processing ought to include stipulations regulating mainly the following:

- Scope of authorization to use the provided data: this is important for re-using public sector information
- Protection of privacy and business confidentiality
- Definition of principles governing the transmission of data to third parties:
    - Definition of liabilities when obligations are not met by the third party

- Setting guarantees for the provision of services (responsibilities for defects) and Setting responsibilities for damages
- Definition of the procedure to be followed to terminate the contract.

3.4 The need for European cooperation to ensure C-ITS operation

C-ITS services have been demonstrated in several pilot deployment activities at European and national levels which has led to a number of member states and road operators within them to invest in large scale deployments. This has incentives OEMs to roll out C-ITS connected vehicles on the market. In addition, infrastructure operators (including public transport operators and road operators) and emergency organisations have started to provide C-ITS capabilities their fleets. The starting point for large scale deployments of C-ITS services has been reached. However, to ensure further investments by additional stakeholders and that further developments are successfully integrated in up and running C-ITS services, a common approach for upgrading and updating existing and new C-ITS infrastructures, equipment and services is necessary. Cooperation is therefore necessary to avoid fragmentation, to ensure interoperability and an efficient large-scale technology neutral deployment of C-ITS services.

Collaborative action at European level is necessary to provide sustainable deployments and encourage innovations and investments C-ITS.. Close coordination between all stakeholders such as mobile network operators, vehicle manufacturers, road operators and the exploitation of possible synergies will be instrumental in achieving the full benefits offered by C-ITS services.

Some of the existing platforms e.g. C-Roads, Car 2 Car Communications Consortium, are able to undertake pilot testing and further developments, but their existing governance structures are not able to ensure national roll-outs and continuous EU-wide C-ITS operations. This is because platforms are usually set up for developments and promotion, but as soon as it comes to real-life deployments and continuous operation, it is important to get a buy-in from the relevant stakeholders   in terms of technical and business commitments. A governance structure needs to be identified, where all stakeholders can contribute directly and commit themselves for investments on C-ITS services based on commonly agreed and committed technical specifications.

The following chapters will detail the elements that need to be taken into consideration when setting up such a European-wide Governance Structure for C-ITS service operation including all relevant stakeholders.

4 Organisational elements to be coordinated at a cross-national scale during C-ITS operations

Technical elements under consideration for continuous C-ITS operation require direct cooperation between infrastructure operators and other stakeholders at organisational level.

4.1 Vision and Strategy

C-ITS deployments strategies are becoming common amongst C-ITS stakeholders, including C-ITS strategies at the European level (the European C-ITS Strategy COM(2016) 766[2]), at national level (e.g. the Austrian C-ITS strategy[3]) and as well with several other platforms and single stakeholders.

Most strategies are aiming at the implementation of C-ITS services including the visions and perspectives of C-ITS service impact on road safety; a common harmonised strategy driven by all stakeholders is therefore needed.

However, hardly any strategy is dealing with C-ITS service operation. In this respect a commonly agreed high level European view is needed, to ensure sustainable operation and maintenance of C-ITS services. The most important element of such a European C-ITS Strategy is the agreement of a **common C-ITS Vision**.

Within the governance of C-ITS operation this vision will form the basis for cooperation and needs to be reflected and, if needed, validated on a regular basis, to ensure that the current vision is valid and still accepted by all C-ITS operation stakeholders.

This vision might again form the basis for individual C-ITS operation strategies of the single stakeholders including missions and action to be undertaken.

4.2 Regulatory aspects

The legal framework related to C-ITS operation is under permanent transformation. Besides transport related elements elements with regard to digitisation (including data), privacy, telecom, etc. need to be **monitored and evaluated to assess the impact on C-ITS operation**. Where applicable, needs for adoptions on the C-ITS operating system need to be identified in the multi-stakeholder environment.

Here a specific focus needs to be given to the **privacy aspects**, especially in relation with in-vehicle generated data (e.g. for the probe-vehicle-data use-case), which are currently seen as personal data. Legal certainty for all C-ITS stakeholders needs to be ensured for both, public as well as private driven organisational environments. Especially in this regard, a continuous monitoring of the legal framework evolution needs to be ensured.

A specific task within the legal framework is with data and service ownership and related responsibilities (**Data and Service Access Information System**). As within C-ITS service operation cooperation is key, it is important to come to agreements on data/service-ownerships, responsibilities, and licences, if applicable. In the current C-ITS deployment status that is not the central element, as usually one service provider (which might be a road operator) provides services to end-users. But by preparing for future C-ITS operation, C-ITS service providers will provide services coming not only from own sources, but from multiple sources. Here several compositions are seen as possible, e.g. a national road authority might provide C-ITS services as well on behalf of regional and/or city-authorities; or: a private C-ITS service provider provides services based on

[2] https://ec.europa.eu/transport/themes/its/c-its_en

[3] https://www.bmk.gv.at/en/topics/mobility/alternative_transport/its.html

data/services of several road operators as well as OEMs. In such cases, Service (Level) Agreements need to be considered, describing aside responsibilities and authorisations as well as service descriptions covering quality of data/service and area/roads covered by the services. Such Service (Level) Agreements might as well be useful in a multi-stakeholder service chain, e.g. using long-range communication channels where aside road operators and end-users (represented by OEMs) the carrier of the information (Telecom-providers) need to be included.

Even the setup of such Service (Level) Agreements is out of scope for the governance of C-ITS operation, the knowledge about responsibilities in case of failures is needed. Therefore, a **central C-ITS information system**, where e.g. services operative, areas covered, and entities responsible for operation are listed. The central information system is seen crucial especially for pan-European service provision in a real multi-stakeholder environment. Current activities like the visualisation of infrastructure based C-ITS stations and the promoted services done on the TENtec interactive map viewer (https://ec.europa.eu/transport/infrastructure/tentec/tentec-portal/map/maps.html) could be seen as starting point for such a central C-ITS information system.

4.3 Monitoring of operations

Such a **central C-ITS information system** described under legal aspects will be needed for the **monitoring of operations**, it describes the accessibility of services for end-users. Ideally following information form the basis for such a central C-ITS information system:

- Service provider and responsibilities along a service chain
- Services operative
- Area covered
- C-ITS communication channels supported by the operative services in a hybrid communication environment

Apart from the monitoring of operative services, **planned future service-provision** (with a clear time-line) shall be included in the central C-ITS information system. This helps all stakeholders to setup road-maps and roll-out plans for extension of current active services including marketing and dissemination strategies.

Within the monitoring task, also all stakeholders might bring in an indication of **needs for future service provisions**. This helps all stakeholders to ensure sustainable investments into the necessary C-ITS infrastructure by ensuring, that provided services will also be used by end-users. It should be noted that identification of future service provision may not necessarily attract investment. Therefore priorities and bottlenecks need to be identified based on a cooperative stakeholder approach. Such needs for service provision might be identified for all stakeholders in the C-ITS service chain, e.g.:

- Road operators to invest into new C-ITS infrastructure for service provision
- OEMs to invest into new services being accepted and implemented in-vehicle
- Telecom providers to invest in telecom-infrastructure in specific areas

4.4 Performance Monitoring

The use of C-TS services will not meet its purpose unless their impact is evaluated and assessed to quantify the effect of the C-ITS services on different impact areas. Data should be collected during the use of the C-ITS services to formulate links between data and critical research questions with relevance to contribute to policy goals. Hence, the observed pattern of behaviour to some “counterfactual” for what would have happened without the C-ITS intervention must be explored, i.e. the impacts of C-ITS services are the result of a comparison between a framework with C-ITS services that are working or activated on the equipped vehicles/devices and other vehicles that are not equipped with C-ITS services or have them switched off.

The three main impact areas to be included in the evaluation and assessment approach are:

- User acceptance
- Impact assessment
- Key Performance Indicators

All these elements should continuously be monitored to ensure a broad uptake by end-users as well as support by policy and decision makers.

User acceptance

User acceptance could be classified as follows:

- A priori acceptability: studied before use
- Acceptance: studied in first use
- Appropriation: studied after several weeks or months of use

The user acceptance should focus on the respondents' attitudes, including their behavioural responses when the users have had experiences with the use of C-ITS.

Typically, user acceptance is measured through questionnaires which are answered by end users. Characteristic topics to be covered are general (social) information, social/ID information, information in relation to driving behaviour, information on knowledge/experience about technology and C-ITS, general service information and expectations and use case service information.

Impact assessment

In the coming years, C-ITS services will significantly increase as will the number of vehicles equipped to receive C-ITS messages (increasing market penetration) The C-Roads field tests are mainly based on test vehicles, very often equipped with ad-hoc C-ITS stations and interfaces. The impact is measured starting from the driver behaviour changes of few vehicles. The evaluation studies provided the best effort to estimate possible impact on mobility. However, impact on the entire traffic flow at this stage are estimates which are not fully measurable. User acceptance has been widely investigated; in some cases with few drivers (including professional drivers), in others with a consistent number of interviews. In any case the questions were based on prototype services or on future services availability.

An improved number of vehicles regularly receiving C-ITS services, an xtended part of road network where these services will be available and a greater awareness and knowledge of the C-ITS services by the users will increase significantly the quality and level of detail of the next impact assessment studies providing more reliable estimation also of the socio-economic benefit on large scale.

Also, the analysis of cross-border services and of service continuity and interoperability will improve because travel limitations will, hopefully, be reduced. The Covid-19 Pandemic has significantly limited the freedom to investigate such issues, especially through in situ observations.

A stricter collaboration with the car manufactures, already started in this phase of C-Roads, can significantly improve the analysis of the impacts. For example, data collected from the CAN Buses, information from the vehicles that receive C-ITS messages, information that can be collected by the RSUs when C-ITS receiving vehicles transit nearby them will enrich the dataset at disposal for evaluation analysis.

The ability of the RSUs to collect data from the vehicles is opening new possibilities of dynamic traffic management and long-distance services. For example, re-routing services can be more effective, continuous and able to provide long-distance solution. Traffic flows can be monitored in a continuous way, having also the possibility to assess the percentage of vehicles that are following some specific indications.

The field tests of the first phase of C-Roads provided a first set of impacts analysis but they also highlighted the need for further investigation of different aspects that are influencing drivers' behaviours, such as:

- HMI interfaces: how to provide the information (Not just a graphic issue but also a content decision).
- The distance from the event point where the C-ITS information should be provided to the drivers.
- The frequency of the message provision.
- The precision of the event location.
- The choice to which vehicles the information should be provided; all users, certain categories, certain types of vehicles, etc.
- Other lessons learned still under investigation.

In general, there is a need to move from an approach that is more focused on the technical analysis to an impacts-based approach: move from “Does C-ITS work?” to “Are C-ITS services useful and effective?”

During the investigation of the impact some additional areas of implementation were highlighted:

- C-Roads is focused on V2I communication, but also V2V data exchange should be investigated (for example the platooning and highway chauffeur field tests in C-Roads Italy).
- Vulnerable Road Users and all road users that are not equipped with C-ITS stations should be considered, especially in urban areas.
- New services definition in urban areas that are involving also Public Transport or facing some issues that are relevant in the cities (traffic re-routing or distribution on the road network, parking issues, pricing policies, reserved or dedicated lanes, etc.).
- The definition and analysis of C-ITS services bundles that are more complex to be analyzed. The studies fulfilled within the first phase of C-Roads are an important starting point.
- The analysis of the biometric status of the drivers that is an important element to understand the perception, the reaction and the compliance to the received information by the users.
- The definition of large-scale services (both at extra-urban and urban level) able to manage the traffic with wide range traffic management policies for which the C-ITS are a very powerful tool.
- The definition of C-ITS services that are based on forecasting models that are especially useful to predict traffic and provide messages that can last in time.
- The investigation of how much and how C-ITS can support autonomous driving and the definition of new use cases and specialize some existing ones.

KPI monitoring

The Key Performance Indicators (KPIs) are specified in detail in the Evaluation and Assessment Plan provided by WG3 - Evaluation and Assessment. Further and more specific KPIs are defined within the different Evaluation studies. The continuation of evaluation studies that will be based on the same guidelines will provide a continuous observing of the KPIs and monitor the trend of the measured impacts.

In general, several Key Performance Indicators (KPIs) are defined to measure the effect of C-ITS services on safety, traffic efficiency and the environment. KPIs are defined as the comparison between revealed measures with C-ITS and the baseline that is the current framework without C-ITS services. This can take place either ex-ante (simulated events) or ex-post (real-life demonstration).

Characteristic KPIs include:

- Speed adaptation
- Travel time
- Lane change
- Change in the number of accidents
- Change in time spent in queue
- Fuel consumption
- Noise level
- Change in pollution level

The main sources of data would be, together with the in-vehicle C-ITS-Station, the vehicles (CAN Bus data) and/or the traffic monitoring systems on the road. Characteristic data/parameters that should be collected to measure/calculate the changes in driver behaviour are: time, dynamic parameters of the vehicle (speed, position, steering angle, etc.) and information concerning messages (typology, time and position). Based on the measurement or calculation of the aforementioned parameters the performance indicators are defined (e.g. speed adaptation, change in acceleration, average speed change). Finally, the future estimated impact KPIs (when penetration rate will be higher) could be estimated by using the aforementioned measured or calculated KPIs for a higher C-ITS penetration rate. This estimation could be based on algorithms, traffic modelling, and even through qualitative estimation.

5 Technical elements to be coordinated during C-ITS operations

First and foremost, the technical requirements are governed by harmonized EU legislation. In absence of C-ITS specific legislation[4], the EU ITS Directive[5] is a core legal framework followed by technical standards and EU-wide technical specifications (C-Roads, C2C CC etc.). In C-Roads, the WG2 and its assigned Task Forces have issued a number of valuable documents, which complement technical standards[6].

When moving from pilot phase to continuous operation of C-ITS services, some important decisions on technology selection, installed equipment and standards compliance have been already made, and may have irreversible impact on site operation. For this reason, the harmonization and coordination of specifications between the automotive industry and infrastructure operators is an important process for the future. Standards can be misinterpreted in some cases, this is why it is important to create a common understanding of commonly agreed specifications and profiles. However, C-ITS operation is not possible without adhering to governance arrangements resulting in legal certainty. This is one important drive of changes to existing pilot deployment projects. The second is emergence of new technologies and new standards versions.

The C-ITS sites have thus needed to adapt to these changes during the operational phase. **Change management** refers to process of operating and maintaining the site, managing upgrades of hardware and software components, maintaining compatibility between components and units, adjusting to legislation changes and requirements as well as new standards versions and enabling new technologies.

The central subject, from infrastructure point of view, is how the end-user interacts with this infrastructure and the C-ITS services provided to improve safety and comfort. **Information management** comprises all necessary data related actions including classification, entry, distribution, filtering and dissemination, information quality assessment, information sources evaluation and management. Pilot sites may be oriented to technology (testing, standards compliance, new features…), but in a fully operational C-ITS system road users expect accurate, timely and relevant network information in the locality.

For data exchange direct cooperation between infrastructure operators is envisaged (domestic and cross-border). It is not feasible that the data exchange for C-ITS systems would be separated from normal centre - to - centre data exchange. Therefore, C-ITS should leverage existing efforts in this area, most notably DATEX II data exchange standard and its published profiles. Existing DATEX II data transfer paths, which are already operational, shall be utilized to convey the data between infrastructure operators and other stakeholders (most notably, national access points). In future C-ITS will lead to large volumes of messages making other standards more feasible.

[4] Supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems was not accepted by Council of the European Union.

[5] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.

[6] Deliverables of Workgroup 2 (Technical aspects) and task forces TF1 (Security aspects), TF2 (Service harmonization), TF3 (Infrastructure communication), TF4 (Hybrid Communication), TF5 (Cross-testing and validation)

5.1 Change management

Changes in legislation, standard support, unit types or services offered may result in hardware and/or software upgrades on various levels of the whole operational C-ITS system. Following each significant system upgrade, the testing of a site according to TF5 C-ITS Cross-Border Testing and Validation Concept is recommended. In case of ITS-G5 roadside units, all RSUs shall be equipped with the same firmware version (except for testing environment) ideally within a specific and defined timeframe. In parallel in-vehicle C-ITS stations need to perform the software upgrades to ensure interoperability of C-ITS services.

It is recommended that each C-ITS site maintains testing and operation environments. Both environments are inside the same information path, with the difference that the staging environment only influences a small portion of C-ITS users.

As a C-ITS site is always seen as part of the overall C-ITS system, the cooperation of sites on national and international level as well as cooperation with all stakeholders involved is mandatory. This includes notification of changes (with detailed description of changes) e.g. to NAPs, which then distribute this information to all interested parties. Currently this task is taking place within the C2C CC “Special Working Group for Operations”.

5.2 Information management

Users receive data from multiple information providers using various dissemination channels (C-ITS, variable message signs (VMS), internet sites, mobile apps, radio, navigation services…). It is important, that these information channels provide consistent and relevant information to road users. The following are recommendations for achieving this goal in C-ITS site:

1. The information path shall be automatic and secure. In order to minimize human error factor, the information shall be transferred to receivers without human intervention.
2. The information source shall be same for the same type of information. For example, generation of IVI messages shall use the same source as generation of VMS messages.
3. Only most important information shall be provided to users. For example, temperatures below zero are not important, but ice on the road surface is. This includes the prioritisation of messages in case several messages need to be exchanged in a specific area.
4. The information providers should be continuously assessed the quality of particular use cases. Incorrect, incomplete or delayed information shall be logged.

Information providers are usually trusted institutions. Most data originates from the road operator and their information systems. Some data, may come from infrastructure users. Usually, such systems have already some data filtering and validation policy in place. It is feasible that C-ITS systems take advantage of existing policies to provide the road users information, consistent with other dissemination channels.

However, one important aspect of C-ITS information system is the amount of data presented to the road user. It is evident that messages may distract the driver from their primary task. It is therefore vitally important that the messages transmitted by the C-ITS system are prioritized according to vehicle location, direction and importance of the message. Within a short-range communication system, the filtering of important messages may take place at RSU level, while IP-based services may allow for even finer granularity of personalised message filtering.

Connected vehicles are likely to generate terabytes of data per day based on CAM messages alone. However, this data needs to be filtered and aggregated at the C-ITS station level of the infrastructure operator. There is no need to store raw data during normal C-ITS operations (as opposed to pilots). This is also consistent with privacy policy, which recommends anonymization at the lowest possible level. With CAM messages, the most important data shall be extracted at C-ITS station level (e.g. low speed or stopped vehicle on motorway, airbag deployment, instant breaking, emergency vehicle with lights on etc.), all other data can be used for statistical analysis (number of vehicles, speed, etc.).

5.3 Quality measures and assurance

The architecture of C-ITS service operation is heterogeneous in Europe and has a fundamental international overlap, so it is necessary to ensure comprehensive interoperability of C-ITS services so that underlying C-ITS systems are not dependent on component manufacturers, suppliers, implementing software tools or geographical areas. The main goal of implementing C-ITS systems is to make them fully operational across Europe, regardless of single suppliers of vehicles or equipment used. The operative C-ITS system needs to ensure that it is certified by independent providers in terms of security and compliance with defined requirements and standards.

The overall system should consist of several parts, especially the following:

- Data quality and data formats
- Verification of conformity of components and services

Data quality and data formats need to be agreed and followed including criteria and procedures to evaluate quality of service, documentation, structure, distribution and the content of data. Hereby each use case may have unique requirements in terms of quality criteria and assessment methodology. Besides of the definition of data quality within the system, the definition of and commitment to specific interfaces where data/service quality can be verified is essential.

For the quality assessment knowledge of data acquisition might be helpful. For the proper functioning of the system it is necessary to obtain data from external sources and it is important to be prepared to know more about this data. In the process of data collection, it is important to test its frequency, content, size (in bytes and number of records) and conformance to a schema.

When data is collected internally, a proper quality management needs to be in place before being used for creating a service. The tool for evaluation initial data quality in daily operation should be able to alert, when things go wrong. In a case of complaining about data, it could be possible quickly and easily to find how things were working and resolve the root of the problem soon. This task could be e.g. be undertaken by an independent assessment of compliance body.

In some cases, it may even be necessary to archive data, especially when it comes to malfunctioning C-ITS services based on corrupted data.

In general, some form of declaration on quality criteria and procedures of measurement of all C-ITS stakeholders would be beneficial to ensure accurate and high-quality end-user services. Such a declaration is needed alongside procedures for regular evaluation of the quality of data and services provided.

In addition to data quality the **verification of conformity of products and services** is seen as essential. Ensuring the international interoperability of C-ITS services presupposes the compliance of central components and individual stations with defined normative and legislative documents. In order to be able to provide C-ITS services continuously and eliminate the risks associated with incorrectly implemented functionalities or developed products, it would be appropriate to introduce a form of certification or conformity assessment process in this area.

The system for ensuring the deployment of quality components and conformity assessment can be set up in four levels:

- **Self-certification**: Conformity assessment by the first party is a technical term for the case where the conformity assessment is performed directly by the manufacturer. It is sometimes called self-assessment, in the worst-case self-certification and is solved within the Methodology of Conformity Assessment, the so-called declaration of conformity.
- **Conformity assessment by the other party** is a technical term for the case where the conformity assessment is performed by the manufacturer's customer. E.g. the manufacturer invites the potential customer to verify that the products comply with the relevant standard.
- **Third party conformity assessment** is a technical term for the case where conformity assessment is performed by a third party, independent of products and customers. Only in this case is it a certification. Specifically, the third party is represented by testing laboratories and certification bodies.
- **Third party conformity assessment with recertification** is an extended option of the previous variant, where certification is not performed only once, but repeatedly (in defined periods, or in case of significant changes.

According to EN 17000, certification is the process by which a third party provides written assurance that a product, process, or service follows specified requirements. A certificate of conformity is then a document issued under the rules of a certification system, expressing the provision of reasonable confidence that a properly identified product, process or service is in conformity with a particular standard or other normative document. The certification process primarily serves to demonstrate that the relevant product, process or service is in compliance with the specified requirements that it meets and is of sufficient quality and safety for the purposes for which it was designed and manufactured. As the rules of international and national certification and certification procedures for the connection of C-ITS systems and equipment to central elements are not yet defined, although this is being discussed at European level, it will be necessary to build a comprehensive certification system that might require an accreditation body and testing laboratory, according to the relevant standards EN ISO / IEC 17065, respective EN ISO / IEC 17025: 2018 and in accordance with the specific laws of the single Member States.

Such a certificate will guarantee quality services with parameters such as delays, relevance of information, number of customers, and customer evaluation. At message level at a minimum following elements based on commonly agreed quality parameters, need to become part of such a certification process:

- measurement of latency
- clock synchronisation
- message conformity

There is also a need to be ensured that there will be non-conflicting messages, without duplication, via different communication channels. The scheme of technical conformity assessment of C-ITS / ITS equipment and systems currently doesn’t exist in Europe, if we do not consider the assessment of conformity with the requirements for common electronic equipment. Therefore, it is necessary to discuss such a certification system and in particular to set the legal requirements for conformity assessment of C-ITS / ITS components. At the same time, it is necessary to determine which technical issues (component parameters) can be certified by self-certification, or by a declaration of conformity of the equipment manufacturer, and which technical issues must already be assessed by an independent third party. In addition, re-certification in case of product-changes must be considered.

5.4 Security

Security has been extensively studied, specified and analysed within WG 2 / TF 1[7]. Security is one of the key components of C-ITS service operation. The goal is to create a unified trusted environment ensuring mutual trust of individual components that communicate with each other and use certificates from different Certification Authorities (CA). The distributed architecture of C-ITS systems, and in particular their international interoperability, laid the foundation for an architecture that creates a credible ecosystem across all EU Member States involved in the C-ITS architecture. The system architecture is divided into two basic levels:

- National level
- International level

At the national level, there are individual Public Key Infrastructure (PKI) systems that manage digital certificates of individual system participants (ensure their registration in the system, assign appropriate rights, revoke certificates, etc.), trust is ensured by the root certification authority, which is the highest trusted third party in the given system (which is usually local) and two subordinate certification authorities to which some functionalities are delegated (registration authority, authorization authority).

The international level is interconnected with the national level and ensures credibility between individual local PKI systems. In the C-ITS security architecture, a superior layer is thus introduced, ensuring the mutual trustworthiness of individual PKI solutions, which is ensured by central European components, currently operated by the European Commission within the Joint Research Centre (JRC) as an independent entity and a guarantor of equal access.

The overall C-ITS security system is defined in the European C-ITS Certificate policy, where the rules are clearly given - PKI audits, key issue / revocation, key revocation. For a sustainable operation of the security system following points need to be taken into consideration:

- Ensured sustainable operation of Trust List Management (TLM), European Certificate Trust List (ECTL) and C-ITS Point of Contact (CPoC). If these elements will be continuously operated by the European Commission, a long-term commitment is needed.
- Continuous monitoring of the security system in place
- Having day-to-day processes for efficient trouble shooting in place
- reporting and information sharing to identify and mitigate risks
- Cooperation for the implementation of new security solutions, e.g. cross-certification

In addition, for the security of data transmissions based on IP communications in hybrid systems, a TLS Root CA and DNS are required, as specified in the WG2 TF4 document “C-ITS IP Based Interface Profile, Version 2.0.2”, as illustrated in the figure below.

[7] TF1 Security Report v 1.5, 2019

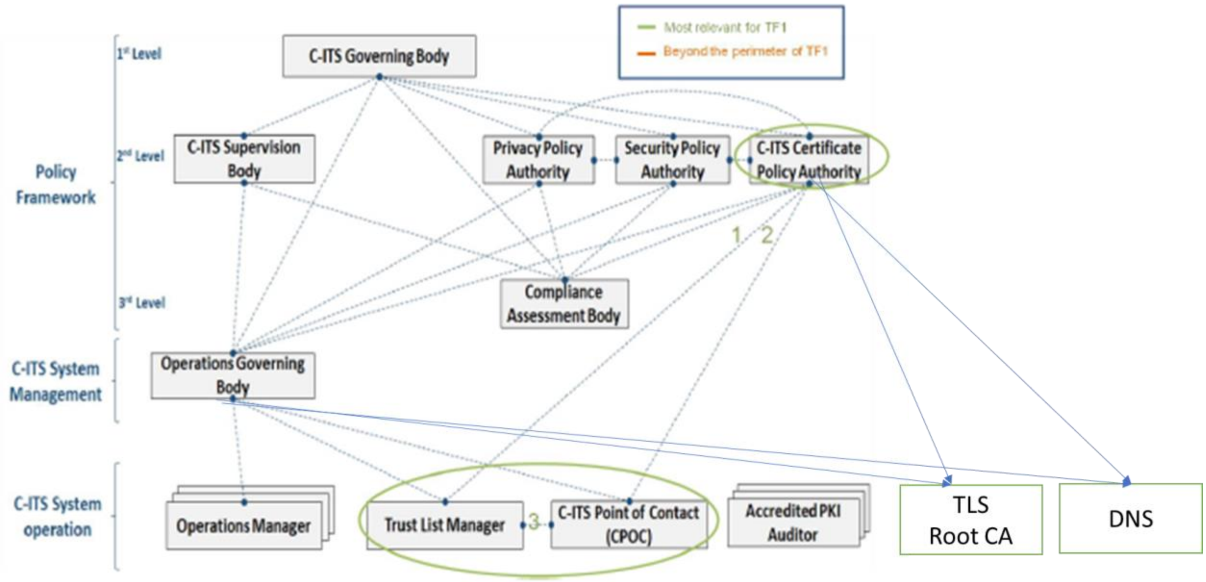

Figure 1: C-ITS IP Based Interface Profile, Version 2.0.2

However, for continuous operation of the C-ITS infrastructure, some other aspects shall also be taken into account.

Consistency: all information units (for example, RSUs) shall implement the same security standards at all times. This is important while partial upgrades may leave security holes in the system which can be easily forgotten.

Chain of trust: security of the whole information path shall be documented and maintained at all times. The focus of security is normally on user - (RSU) - local centre data path, but the information chain does not stop there. It is important to document security measures, used in every step of data path, including physical access, network topology, firewalls, etc.

Breach mitigation plan: The procedure shall be developed in case of security breach on each level of information chain. If there is a physical security breach on RSU level, the procedure shall be developed, how to isolate the network to prevent the harm to spread to wide area level. This may include shutting down parts of the C-ITS site or the whole site, certificate revocation procedures etc.

Reporting: Security breaches or problems shall be reported to all stakeholders, which are in the chain of trust, along with expected mitigation procedure and expected impact. Aside the breach mitigation plan also a process for coordination and resolving identified problems needs to be set up.

Continuous monitoring: security breaches are hard to detect. However, automatic data consistency checks and monitoring of outages are of great help there. Serious security breaches in many cases include bypassing, modification, or insertion of equipment, which results in a (sometimes) minimal downtimes. Each such event shall be investigated according to security protocol.

5.5 Technical upgrades based on improved and new standards

Technical bodies are issuing new versions of standards continuously. It is important to ensure coherent operation of C-ITS site regarding supported versions of standards. For each C-ITS stakeholder, a list of supported standards shall be maintained. The monitoring of the evolution of standards used needs to be in place to ensure the integration of the latest standard-releases for the service-interface specifications.

Aside the monitoring of standards a process for coordinating the deployment of common standard-related changes needs to be continued, as it currently happens within the C2C CC “Special Working Group for Operations”.

Issues discovered during C-ITS site operation shall be reported back to the standards organisations in order to improve standards referred to in C-ITS deployment specifications.

6 Stakeholder management for harmonised C-ITS operations

Aside cooperation on organisational and technical issues, which are both mainly necessary for internal organisation for the overall C-ITS service provision, a key element deals with collaboration based on external requests. As the end-user is key for achieving acceptance of C-ITS services and by that contributing to policy and business goals, proper engagement with end-users, as well as other new stakeholders, is seen as highly important.

6.1 End-user support

C-ITS services will only be operated sustainably, if they are accepted and used by end-users. Therefore, a proper end-user support by all stakeholders needs to be in place.

As C-ITS service delivery is based on a multi-stakeholder environment, all elements need to work together in an integrated manner. The end-user is not interested in single stakeholders, but in the service itself. And what happens if a service fails (for whatever reason). As an example: A Belgian driver is driving with his German branded car on a French Road using a C-ITS service where he subscribed at a Dutch C-ITS Service Provider. And now the driver notices a C-ITS service failure. Whom will he contact? There are several options: the road operator, the OEM, or the C-ITS Service Operator? And if one of these stakeholders is contacted, how to ensure, that the C-ITS service will be prepared?

At the end, it needs to be ensured to make no difference, who is contacted by the end-user. But the problem with the malfunctioning C-ITS service needs to be resolved to ensure satisfied end-users. For that reason, a kind of **clearing house for end-user feedback** needs to be created, especially when the end-user request cannot be solved by the stakeholder contacted by the end-user.

Such a clearing-house needs to have access to the technical monitoring of the overall system giving the possibility to identify and verify malfunctions. Here all C-ITS stakeholders need to work together for ensuring satisfied end-users. In general, a clearing house process needs to be established, by agreeing and following specific process-steps in resolving issues and providing a proper response to end-users.

6.2 Stakeholder support

Even today several C-ITS stakeholders are committed and are contributing to the deployment and operation of C-ITS services, there are many more stakeholders that will contribute to the C-ITS ecosystem in future. E.g. currently mainly national road operators are contributing to C-ITS pilots and are committed to start large-scale C-ITS deployments. In future urban road operators as well as regional road operators might be willing to support their road-users as well via C-ITS services.

For a proper functioning C-ITS ecosystem support for such new stakeholders need to be ensured, to be properly prepared to support their customers with a satisfying service. Therefore, a kind of alignment with newcomers needs to be established. This should include a basic support on duties and responsibilities of specific stakeholders within the C-ITS service chain. Ideally a kind of FAQ section on technical as well as organisational elements needs to be prepared and maintained to support newcomers to become active C-ITS stakeholders.

The national access points (NAP) established by single European countries can play an important role. NAPs might list and route to active and running C-ITS services, and data used for these services. This might be of help for another stakeholder group, e.g. C-ITS service operators.

7 Possible governance structures for C-ITS operations

7.1 Tasks to be considered in a collaborative C-ITS governance (CCG)

Chapters 4, 5 and 6 are detailing the technical and organisational elements as well as the stakeholder management to be considered to enable a sustainable operation of pan-European C-ITS services, including maintenance and upgrade of operative services as well as underlying infrastructures. As a summary of these chapters, following activities and tasks are currently seen to be covered by a collaborative governance enabling continuous C-ITS service operations, in short CCG (collaborative C-ITS governance).

In addition, if a pan-European cooperative governance structure for C-ITS operations is set up, the first element to consider is to setup the framework which enables the partnership of different stakeholders. Therefore as pre-conditions for the CCG following tasks have to be finalised:

- An **agreement on a common C-ITS vision for the CCG**. This vision, of course, will go beyond the C-ITS visions of the single stakeholders, it serves as a basis for all activities taken up by the CCG. A commitment of all initiating stakeholders forms the basis for setting up the CCG. Such an agreement needs to be based on political support. So, this common C-ITS vision should work in two ways: “downwards”, to give a base for further detailing the agreements among stakeholders and “upwards” to the political level to provide support and regulation for C-ITS.
- Based on the commonly agreed C-ITS vision, a **common mission** for the CCG needs to be elaborated to ensure concerted actions of all stakeholders involved.
- Based on this mission **cooperation agreements**, which include a description of tasks, responsibilities and commitments of single stakeholders, need to be agreed upon by the CCG. Here as well decision making rules and procedures need to be agreed upon. These agreements need to be signed by all initiating stakeholders as well as by all stakeholders willing to join the CCG later on.

7.1.1 Organisational elements

Chapter 5 focuses on the organisational elements. Hereby following elements for the cooperation in the CCG can be summarised, all based on commonly agreed decision making processes that include “endorsement and adoption”:

- **Monitoring** focuses on the supervision of the overall C-ITS service performance and the further development:
  - Security System in place (here a regular information needs to be provided by the CCG members in accordance to general agreed reporting rules).
  - Information on active C-ITS services (ideally displayed in an information system operated by the “central service”. Also here a regular information needs to be provided by the CCG members in accordance to general agreed reporting rules).
  - Information on data and services available (ideally registry service is set up by the “central service” based on the inputs received from CCG members. Also here a regular information needs to be provided by the CCG members in accordance to general agreed reporting rules).

  - Regulatory aspects are considered (even legal aspects are taken into account by the single stakeholders potential legal findings can be shared, discussed, and ideally solutions to overcome problems can be discussed).

7.1.2 Technical elements

The need for cooperation on technical elements is described in detail in chapter 4. Hereby following activities for collaboration of all stakeholders are identified:

- **Change Management** describes elements, where changes need to be undertaken by several (or even all) CCG stakeholders. This includes:
  - Update and authorisation of specifications and systems (while the acceptance of the update of specifications is done by the CCG, the systems-update needs to be done by the single stakeholders for the system-components in their responsibility. Also re-certification issues for system components need to be discussed and agreed upon).
  - Agreement on implementation plans for new releases (aside the agreement on new releases also implementation plans – from what date on the new release will form the basis for C-ITS service provision – need to agree on. Those form the basis for the update of the operative systems).
  - Setup and performing cross-tests, including validation (even cross-tests are organised by single stakeholders, invitations to other stakeholders should be spread. Such cross-tests might include the check of data quality and data formats compared to specifications and/or verification of conformity on security issues).
  - Roll-out of new versions/generation of PKI certificates (similar to the agreement on the implementation plans for new releases updates and/or upgrades of the PKI infrastructure need to be rolled out based on a commonly agreed roll-out plan).
- **Information Management** focuses on elements where single stakeholders inform other CCG members on C-ITS related issues:
  - Data sources used for generating C-ITS service provision might be reported in accordance to general reporting rules set-up in the cooperation agreements.
  - The consistency of the C-ITS service chain comprises two elements – the consistency of the service chain from service generation to end-user service delivery and consistency of the C-ITS service itself in comparison to other ITS services. For both elements a kind of ticketing-system needs to be set-up by a “central service” to enable a validation of identified inconsistencies.
- **Security Management** needs to be in place. This includes
  - the operation of a central PKI infrastructure
  - TLS session level security
  - Handling of security issues

7.1.3 Elements fostering sustainable stakeholder engagement

In accordance to chapter 6 following elements need to be considered when focusing at the stakeholder management:

- **Stakeholder Support** to newcomers should be provided by a “central service”
- **End-user support** will be usually managed by the single stakeholder for their customers. But there will be cases, where a hand-over to the “central service” id needed for further spread out to other stakeholders.

7.2 Stakeholders involved in collaborative C-ITS operations

Chapter 3.1 deals with several actors currently identified in the C-ITS environment. While several stakeholders are uniting different roles in the C-ITS environment - e.g. road operators are operating the digital road infrastructure as well as providing end-user services – the easiest way to deal with the single groups needed for setting up a proper governance structure for C-ITS operations. However, C-ITS is still very much developing. Therefore, for a long time there will still be a lot of interaction necessary with the authorities setting the (legal) framework.

- **C-ITS station operators - Infrastructure** (CSO.Infra) unites road operators as well as public transport operators and operators of emergency services. In total the number of stakeholders might exceed 100.000 single stakeholder organisations, taking road operators of municipality level into consideration. This is for sure the biggest group of stakeholders to be addressed by the collaborative C-ITS Governance (CCG) structure,
- **C-ITS station operators - OEM** (CSO.OEM) brings together the automotive sector responsible for delivering the C-ITS service to the end-user. In mass penetration, it outnumbers the stations operated by the infrastructure by far. However, there is only a lower two-digit number of station operators on OEM side.
- **C-ITS station operators – service operator** (CSO.SO) is hardy visible today, but it can be expected that in future C-ITS service operators outside the OEM and road-operator stakeholder groups will arise providing specific C-ITS services for specific end-user groups.
- **PKI operator** (PKI.O) is operating the security system needed for providing trusted C-ITS services.
- **End-users** are the core stakeholders to be considered and served by the CCG. Even they are not directly reflected in the CCG structure all activities undertaken need to serve end-users to ensure end-user acceptance or even end-user satisfaction.

7.3 Governance schemes for C-ITS operations

Based on the elements to be considered and the stakeholders involved in the collaborative C-ITS governance (CCG) a governance scheme needs to be set up. Here currently three different approaches can be seen in the C-ITS landscape:

7.3.1 European Body

Reading through the “Sustainable and Smart Mobility Strategy – putting European transport on track for the future” of the European Commission (COM(2020) 789) there is the idea to delegate new tasks to an existing agency or set up another body to support the deployment and management of ITS and sustainable connected and automated mobility across Europe. Such a body could facilitate the preparation of relevant technical rules, which might include as well C-ITS-operations. Such rules would in turn create synergies across Member States.

	Pro	Con
Set-up	Legitimation to “go in” on the basis of the ITS Directive generate new energy to realise C-ITS	Would be a new Group, which might need time.
commitment	An active role of the EC might stimulate certain stakeholders to commit themselves. It might give them more certainty that it is worth to invest in C-ITS.	A stronger commitment is anyhow expected, if stakeholders need to provide their own resources
Inclusion of Member States	Member States would be directly addressed by activities driven by the European Commission	How a balanced participation of public and private C-ITS station operators is ensured is quite uncertain.
Timeframe for implementation		Establishing a new organizational structure takes time because a legally binding framework must be created. The operation of C-ITS has already been launched in 2021
financing	At least co-financing by the European Commission would be ensured even for the In-kind resources to be provided.	In the end a market driven way of financing will be necessary to make C-ITS successful (at least partly). Will this be reached, if the EC is financing a big part of the activities?
Scalability	Keystone approach, “neutral” place for all current and forthcoming custodians of C-ITS profiles	Assuming in total more than 10.000 stakeholders, EC driven processes need to be set up to ensure participation of all stakeholders resulting in proper decision making processes
Decision procedures	Striving for consensus advise feeding the decisions on EU agency level	Having the European Commission in the driving seat might hinder stakeholder driven bottom-up initiatives

Table 1: Pro’s and Con’s for a collaborative C-ITS governance set-up by a European Body

7.3.2 Industry driven platform

An industry driven platform, similar to the current operative “Working Group for Operations” of the Car-to-Car Communication Consortium, could be followed. Even currently only few motorway operators and a few OEMs are participating, this governance structure could be enlarged.

	Pro	Con
Set-up	Built upon an existing Working Group. The group is already active and is composed of frontrunners already in operation. Infrastructure elements already exist and can be used by the group.	Rules are already in place which might hinder newcomers.
commitment	Strong commitment of the participating stakeholders, as own resources are provided.	(New) organisations outside an industry driven platform will not easily commit themselves
Inclusion of Member States		Member States are hardly involved in activities of an industry driven platform
Timeframe for implementation	Already existing	
financing	Market driven approach, which is focused at business cases. Financing needs to be provided via the partnership in an industry driven platform	Financing needs to be provided via the partnership in an industry driven platform.
Scalability	Scalability already in progress but limited	As all participating members of in the “Working Group for Operations” are as well need to become partner of the Car-to-Car Communication Consortium scalability is questionable. In addition, current discussions show, that this Working Group is currently not prepared to coordinate a wider stakeholder community
Decision procedures	There is a clear decision procedure of the stakeholders currently involved in the discussions of the “Working Group for Operations” ensuring an equal treatment of infrastructure operators and OEMs.	Unsure, if decision procedures will work as well for a platform involving all relevant stakeholders

Table 2: Pro’s and Con’s for a collaborative C-ITS governance set-up by an Industrial Platform

7.3.3 Public private partnership

C-ITS operations show, that all stakeholders involved need to be committed to have their say and to follow decisions in accordance to general rules. A set-up with clear commitments of all involved stakeholders in a public private partnership (ppp), similar to 3GPP (3rd Generation Partnership Project) dealing with the Mobile Broadband Standard, could be followed. All stakeholders are grouped to core groups (similar to the group settings undertaken in chapter 6.2) and the group as core has a quorum. Such a logic would ensure that neither OEMs could overrule infrastructure operators nor vice versa.

From the current logic, this would be the proposed way forward to establish a proper decision making within the collaborative C-ITS governance.

	Pro	Con
Set-up	A new group can be set up, especially focusing at necessary tasks and using the experience from earlier coordinating attempts.	Would be a new Group, which might need time.
commitment	Strong commitment of the participating stakeholders, as own resources are provided.	
Inclusion of Member States		
Timeframe for implementation		Establishing a new organizational structure takes time because a legally binding framework must be created. The operation of C-ITS has already been launched in 2021.
financing	ppp allows to access alternative private sources of capital, enabling important and urgent tasks and projects to be performed even when otherwise financing may be difficult	Financing needs to be set-up. An EC-driven initiative may be needed for the setup.
Scalability	The learnings from 3GPP show, that scalability is ensured. There are no limits for stakeholder representation.	When the number of participants grows it may become more difficult to reach consensus within the stakeholder group.
Decision procedures	Proven decision procedure could be taken over ensuring proper representation of all stakeholders involved.	This decision procedure probably functions well, if the set-up enables infrastructure operators to talk with one voice. Because of the differences among the road operators (national, regional, local) this may be difficult, resulting in blocking certain developments of the “front-runners”.

Table 3: Pro’s and Con’s for a collaborative C-ITS governance set-up as public private partnership (ppp)

7.4 Analyses of the discussed Governance schemes for C-ITS operations

The strengths and weaknesses of the collaborative C-ITS governance are discussed in the previous chapters in detail. Comparing the pro's and con's, the following situation becomes evident:

	European Body	Industry driven platform	Public private partnership
Set-up	++	+	+
commitment	+	+	++
Inclusion of Member States	++	-	+
Timeframe for implementation	~	++	~
financing	+	~	++
Scalability	~	~	++

Table 4: Summarizing the discussed Pro's and Con's for a collaborative C-ITS governance

For the set-up there is currently only discussed model existing, which is the industrial driven platform. But it is uncertain, if this approach is scalable and ensure a proper integration and commitment of all stakeholders necessary. This strong commitment goes in line with ensuring a one level playing field for all stakeholders. This would be one major factor when using a public private partnership model – ensuring the one level playing field. Anyhow, the strongest boost for C-ITS deployment would be with the European Body which would legitimate the cooperation in the field of C-ITS operations.

Concerning the commitment such a European Body will for sure activate several stakeholders. Anyhow, it can be expected that the contribution of stakeholders' own resources brings an ever stronger commitment. That would be the case for the other two schemes where anyhow, a new set-up organisation might have a slight benefit compared to an existing organisation.

From the C-Roads partnership perspective the inclusion of member States is a critical factor. Here it is unlikely that Member States are becoming partner in an industrial driven platform. Here a cooperation in a public private partnership seems to be much more realistic. Anyhow, in a European Commission driven approach Member States would be directly addresses, even the balanced participation of the private sector is quite uncertain.

Looking at the timeframe for implementation of course, an existing partnership has a huge benefit, which is a pro for the industrial driven approach. For the other two schemes the set-up of a new sustainable and legally well-established organisational structure takes time. This is insofar critical, as deployment has started already in 2020.

Having a deeper look at the financing of the different collaborative C-ITS governance schemes it becomes evident that an industrial driven approach is primarily focused at business cases, which sometimes might become difficult for participation of the public sector. On the other hand co-financing by the European Commission would helpful for the public sector at least for starting a collaborative C-ITS governance model. Here a good balance between EC funding and market driven way of financing needs to be identified. Such a balanced approach would be seen most likely in a public private partnership which even allows to access alternative private capitals, enabling urgent tasks.

One main criteria for a collaborative C-ITS governance model is with the scalability. As discussed in chapter 7.2 we estimate more than 100.000 single stakeholder organisations operating C-ITS stations from the infrastructure side. In parallel we assume only a lower two-digit number of OEM C-ITS station operators who will be responsible to operate far more C-ITS stations than the infrastructure operators. In addition, there will be additional C-ITS stakeholders, including the PKI operators that need to be integrated in the governance scheme ensuring scalability to larger stakeholder numbers. Having a look at the discussed collaborative C-ITS governance models, it seems that only the public private partnership model might be prepared to setup decision making processes covering the needs and expectations of the C-ITS stakeholders.

Having a look at the stakeholders involved there are doubts, if a proper coordination of activities and tasks should be facilitated by a European body or an industry driven governance scheme, or if a direct partnership of involved stakeholders would turn out with better results. In view of the C-Roads actors **the public private partnership model seems to be best model to focus at for a collaborative C-ITS governance**. Of course there are some evident risks of such a public private partnership model, that need to be taken in consideration when setting up such a collaborative C-ITS governance model.

- First the public private partnership model might become, especially in the set-up phase, too much private and business driven which in return might risk the delivery of essential services to the general public.
- The set-up of a public private partnership is tricky and might take time. A legal framework needs to be developed, processes and procedures need to defined and agreed upon. Here a proposal for such processes and procedures for decision making are discussed in chapter 7.4.
- And even when processes and procedures are set-up the further development for effective procedures is tricky. Hereby ‘Institutional certainty’ is critically important in success, as private investors will readily shy away from an opportunity where they are asked to take on a project that contains unforeseen risks. This ‘institutional certainty’ consist of two types: the ‘formal’, meaning the legal and regulatory frameworks and policy coherence; and the ‘informal’, such as the ‘forums’ where public and private sectors meet to smooth over the misunderstandings and frictions that can arise on specific projects.
- The lack of well performing institutions could delay processes such as the protracted length of negotiations between public and private partners, the slowness of reaching closure and the lack of flexibility in risk-sharing.

While public private partnerships present challenges, they also hold benefits. A public private partnerships approach will deliver value to the public.

- It can be expected that the close cooperation in a public private partnership model ensures the focused use of resources, which lowers costs.
- In addition, higher levels of service can be reached as a strong focus will be given to change management and end-user support
- A strong cooperation where all parties contribute with own resources reduces as well the risk for a single party. As consent driven decisions are made single stakeholders have evidence on the way forward and receive a kind of certainty for own investments in the C-ITS landscape.

- This certainty of outcomes is for sure one of the major benefits. The certainty of outcomes are increased both in terms of ‘on time’ delivery of projects (the private partner is strongly motivated to complete the project as early as possible to control its costs and so that the payment stream can commence) and in terms of ‘on-budget’ delivery of projects (the payment scheduled is fixed before construction commences, protecting the public from exposure to cost overruns).
- Such a public private partnership helps as well in the area of innovation. By combining the unique motivations and skills of both the public and private sectors and through a competitive process for contract award, there is a high potential for innovative approaches to public infrastructure delivery with public private partnerships.

7.5 Overview of tasks and stakeholders involved in a collaborative C-ITS governance following the public private partnership Governance model

The biggest risk within a public private partnership model is seen with the set-up including the definition of processes and procedures. Therefore this chapter is a first try to look on a possible decision procedure taking the identified activities into account. Hereby the different stakeholder groups, as described in chapter 7.2, are grouped together:

- C-ITS station operators - Infrastructure (CSO.Infra)
- C-ITS station operators - OEM (CSO.OEM)
- C-ITS station operators – service operator (CSO.SO)
- PKI operator (PKI.O)

Within the single stakeholder groups decisions on single tasks are done. And for the execution of single tasks all four groups need to provide their “group”-decision as basis for a final collaborative C-ITS governance decision. This ensures that no single stakeholder group has the possibility to overrule another group, e.g. 100.000 infrastructure operators are not able to overrule a lower two-digit number of OEMs. An overall decision is only valid, if all groups individually have decided in accordance to given voting-rules.

As example, such a decision scheme could look like the following:

Main Activity	Core tasks	Decision procedure following the ppp model
Precondition for becoming a partner	Agreement on a common C-ITS vision	
	Setup of a cooperation agreement (tasks, responsibilities, commitments)	
Change Management	Update and authorization of Specifications and systems	- CSO.Infra (acceptance by a simple majority) - CSO.OEM (acceptance by at least one OEM for new use-cases; acceptance by a simple majority of operators active in the use-case for updates) - CSO.SO (acceptance by at least one OEM for new use-cases; acceptance

Co-financed by the European Union
Connecting Europe Facility

		by a simple majority of operators active in the use-case for updates) - PKI.O (observer)
	Agreement on Implementation plans for new releases	- CSO.Infra (acceptance by an absolute majority) - CSO.OEM (acceptance by an absolute majority) - CSO.SO (acceptance by an absolute majority) PKI.O (observer)
	Setup and performing cross-tests (test and validation) – this includes: - check of data quality and data formats compared to specification - verification of conformity on security issues	No decision needed, invitation by single stakeholders and participation of other stakeholders
	Roll-out of new versions/generation of PKI certificates	- CSO.Infra (acceptance by an absolute majority) - CSO.OEM (acceptance by an absolute majority) - CSO.SO (acceptance by an absolute majority) - PKI.O (acceptance of full majority)
Information Management	Data sources for C-ITS services	No decision needed, information needs to be provided in accordance to general agreed reporting rules.
	Consistency of - service chain (end-user service) - C-ITS service itself (compared to other ITS channels and reality)	Operation of a central ticketing system by a “central service”
Security Management	- Operation of a PKI central infrastructure - Handling of security issues - TLS session level security	Operated and driven by PKI.O
Monitoring	Security system in place	No decision needed, regular information needs to be provided in accordance to general reporting rules
	Information system on active C-ITS services	No decision needed, regular information needs to be provided in accordance to general reporting rules
	Registry of data and services available	Needs to be provided by a “central service” based on inputs received
	Regulatory aspects are considered	No decision needed, a “central service” ensures regular communication and discussion of solutions
Stakeholder support to newcomers		To be provided by a “central service”

End-user support	Based on monitoring	Members of the single CSOs for their customers, if applicable. Handover to central service for spreading out to other CSOs (ticketing system)

Table 5: Overview of tasks, stakeholders involved, and decision procedures in in a collaborative C-ITS governance following the public private partnership Governance model

8 The way forward – next steps

This report on the “Ecosystem for fully operational C-ITS service delivery” discussed a framework for operation and maintenance of the C-ITS ecosystem, including updates and upgrades, from an infrastructure perspective. So far no discussions with other C-ITS stakeholders took place, neither with industrial C-ITS stakeholders nor with the European Commission. Therefore this report aims to form one **basis for discussion** with other stakeholders, including the European Commission followed by a phased approach to implementation.

It is evident, that similar discussions are ongoing between the actors in the CCAM ecosystem, bringing cooperation and competition together under the term “coopetition”. They collaborate on the essential parts of the system whereas they compete in other elements of the value network. This brings along a duality in responsibilities. Individual actors fill a role in the value network by performing their own responsibility (this can be both directions, e.g. serving brand customers in different industries as well as providing cross-cutting essential facilities such as a Security Credential Management System). At a system level, all actors contribute to functioning CCAM services which represent a joint responsibility for the system.To do so, a common understanding for end-to-end consideration and responsibility must be created among all stakeholders involved.

Here the C-ITS stakeholders might become the frontrunners in making such “coopetition” reality. It is evident, that a suitable governance scheme is not available off the shelf. But there is the need to identify as quickly as possible a way forward to ensure sustainability for completed deployments and evidence for end-users on continuous C-ITS service delivery in high quality. This includes a deep mutual understanding of business processes (e.g. innovation cycles, planning routines) with the different stakeholder groups, including public and private entities. This is especially important to safeguard C-ITS related investments as well as future investments in terms of services, infrastructure locations and time schedules. Hereby the sustainability of the ecosystem is directly linked to the principle of fairness when sharing costs and benefits.

Therefore the next steps need to be divided in two dimensions, a European one and a national one.

8.1 Next steps on pan-European level

First of all it is highly important to understand the difference between the currently highly active C-Roads Platform and the discussed collaborative C-ITS governance model.

The C-Roads Platform is highly important to develop harmonised C-ITS specifications including security, use-cases, technical specifications, the hybrid communication mix and cross-testing. This work for sure needs to be continued and includes the further development of existing specifications as well as the definition and specification of upcoming new use-cases. This work as well forms the basis for discussions and agreements with the Car industry, represented by the Car-2-Car Communication Consortium. But the focus is here on (further) development of specifications.

But operation of the C-ITS network, as discussed in the collaborative C-ITS governance model, has a slightly different focus. Here the key element is not so much with new specifications, but with the maintenance and operation of the active running C-ITS eco-system based on common interfaces and key factors such as launch dates for new services, so that all stakeholders can synchronize their processes to this end. Further developments might be triggered, based on needs identified, but the core focus is on guaranteeing a highly performing C-ITS operation on a high quality level. The focus needs to be with the end-user and fulfilling the end-user expectations (and satisfaction) of active running services. Only if a long-term operation and maintenance in such a multi-stakeholder-ecosystem can be ensured, next steps towards supporting automated in-vehicle functions with C-ITS services can be reached.

Therefore following next steps on European level are seen:

1. Start discussion with other C-ITS stakeholders (including OEMs and European Commission) on the needs for a closer cooperation, as discussed in the collaborative C-ITS governance model. Here a common understanding on the cooperation areas needs to be agreed on.
2. Work together with all stakeholders on a “common C-ITS vision for Europe”
3. Start discussions with the European Commission on their expectations on the way forward for C-ITS deployment and operation. C-Roads needs to make it evident, that there is a need for two C-ITS platform elements from the infrastructure perspective:
    a. One element, today covered by the C-Roads Platform, dealing with the further development of C-ITS use cases including the setup of technical specifications. In addition, here a monitoring of deployments and evaluation of the overall benefits as input for policy decisions needs to be done.
    b. The second element goes with the close collaboration between infrastructure operators and other C-ITS stakeholders to enable the permanent operation and maintenance of the overall C-ITS system with a high quality level. This will include a kind of prioritised implementation plan, where all stakeholders agree together on the next steps based on the agreed common C-ITS vision for Europe.
4. Based on these discussions the agreements between the single active C-ITS stakeholders for the next steps need to be done. For the time being, operational tasks can be fulfilled by the Car-2-Car Communication Consortium’s Working Group for Operations. But on a medium-term perspective a more sustainable approach needs to be agreed on between all active C-ITS Stakeholders.

8.2 Next steps on national level

In parallel to the activities on European level it is as important to continue discussions on national level. Still most national infrastructure operators are either in a piloting phase or are still not convinced on the benefits of C-ITS. Especially in rural areas hardly infrastructure based C-ITS services are piloted or even deployed.

Here discussions need to start especially on two levels:

- First, operators that are running C-ITS pilots need to receive support for the transition from pilots to continuous operations. This for sure needs to go beyond national level and needs to include sub-national level. This support might be given by the C-Roads Platform partners, especially as they have experience with the implementation of the services.
- In addition, based on evaluation results of up and running C-ITS pilot initiatives, a discussion with national infrastructure operators not testing or piloting C-ITS services up to now needs to start. This especially to support them in decision and deployment procedures. Technical specifications for deployment procedures are available, but successful procurements include aside technical elements a clear understanding of responsibilities of single actors and a knowledge of interactions necessary between all C-ITS stakeholders.

For both elements clarity can be achieved by starting discussions on the collaborative C-ITS governance between all active C-ITS stakeholders. Here the framework needs to be prepared on European level followed by discussions on national level.