EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 13.3.2019

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

(Text with EEA relevance)

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

EXPLANATORY MEMORANDUM

1. POLICY CONTEXT

The increasing volume of road transport in the European Union poses several challenges. Road transport is responsible for most emissions of greenhouse gases and air pollutants from the transport sector as a whole. While road safety has improved in the EU over the past few decades, this trend has slowed down recently and it is unlikely that the EU will achieve its objective of a 50 % reduction in fatalities between 2010 and 2020. In addition, congested roads incur huge costs to the EU economy. Coordinated action across a number of fronts is required to tackle these issues and prevent them from bringing serious harm to Europe's people, economy, environment and climate.

New technologies aimed at improving the efficiency, safety and environmental performance of road transport are playing a significant role in achieving the Commission's goals in this area. One emerging field is that of cooperative intelligent transport systems (C-ITS), which enable vehicles to interact directly with each other and the surrounding road infrastructure. In road transport, C-ITS typically involves vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and/or infrastructure-to-infrastructure (I2I) communication, and communication between vehicles and pedestrians or cyclists ('vehicle-to-everything', V2X). This enables a wide range of information and cooperation services.

C-ITS are a category of ITS services, based on an open network that enables a many-to-many or peer-to-peer relationship between C-ITS stations. This means all C-ITS stations, as defined by this Regulation, can securely exchange messages with each other, and are not limited to exchanging messages with (a single) pre-defined station(s). ITS services which provide similar information, for instance over digital broadcast, cellular networks, or FM radio, but without the characteristics of an open network that enables a many-to-many or peer-to-peer relationship between C-ITS stations, are outside the scope of this Regulation.

The benefits of C-ITS span a range of areas and include better road safety, less congestion, greater transport efficiency, mobility and service reliability, reduced energy use, fewer negative environmental impacts, and support for economic development. At the same time, care must be taken to avoid potential negative effects, e.g. increased traffic demand because of these improvements, drivers experiencing information overload, or the additional data sharing leading to greater cyber-security or privacy risks.

The past decade has seen remarkable new developments in technologies that facilitate C-ITS. Despite the potential benefits, however, these have not yet led to large-scale deployment. In 2011, EU vehicle manufacturers united in the CAR2CAR Communication Consortium issued a joint memorandum of understanding declaring their intention to start large-scale deployment by 2015, as the systems would be technologically ready by then. However, it became clear that this would not be possible unless the main stakeholders followed a common approach on both technical and non-technical aspects.

In 2014, the Commission responded by creating a platform for the deployment of cooperative intelligent transport systems in the EU (C-ITS platform), an expert group in which national authorities, C-ITS stakeholders and the Commission could work together on a shared vision and concrete implementation solutions for the interoperable deployment of C-ITS in the EU. The results of the extensive work of the platform and its working groups were summarised in the final reports[1] for phase I (2014-2016) and phase II (2016-2017).

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

Through the C-Roads platform[2], a joint initiative of European Member States and road operators for testing and implementing C-ITS services in light of cross-border harmonisation and interoperability, and significant investments at national and EU level (EUR 199 million, of which EUR 107 million was co-funded through the Connecting Europe Facility), 16 Member States have worked together with the industry to harmonise V2I C-ITS services and make them interoperable so that, for example, messages about roadworks can be understood consistently across different geographical environments and vehicle manufacturers. This has been the result of cooperation between the C-Roads platform and the CAR 2 CAR Communication Consortium, which has improved consistency in V2V and V2I messages and systems.

In 2016, automotive and telecommunication companies came together in the 5G Automotive Association on technology for connected and automated mobility including for C-ITS services. This has resulted in a situation where two technologies exist for short-range communication, at different levels of maturity and commercialisation, which are not interoperable at radio access level.

The work of the C-ITS platform was an essential input in the context of the European strategy on C-ITS[3], which aimed to facilitate the convergence of investments and regulatory frameworks across the EU so that deployment could start as quickly as possible and, in particular, mature safety-related C-ITS services could be deployed from 2019. The strategy identified the need to adopt an appropriate legal framework at EU level by 2018, possibly through delegated acts under Directive 2010/40/EU (the Intelligent Transport Systems (ITS) Directive)[4] or other legal instruments.

The purpose of this Delegated Regulation supplementing Directive 2010/40/EU of the European Parliament and of the Council is to create the minimal legal requirements for interoperability for C-ITS and to enable large-scale deployment of C-ITS systems and services from 2019. Directive 2010/40/EU (the ITS Directive) represents a policy and legal framework to accelerate the deployment of innovative transport solutions across Europe. The Directive focuses on intelligent transport systems for road and its interface with other modes of transport and empowers the Commission to adopt delegated acts in four priority areas. The definition of specifications for C-ITS is part of priority area IV of the Directive.

The focus of this Delegated Regulation is on ‘day 1’ services, i.e. C-ITS services to be deployed in the short term that will contribute particularly to road safety and traffic efficiency. Specifications and standards for interoperable priority ‘day 1’ services, and a common security solution are now available as a result of cooperation between a broad group of industry stakeholders and Member States’ authorities.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

2.1. Legal basis

This delegated act supplements Directive 2010/40/EU in compliance with its Article 7. A Regulation is the most appropriate legal instrument, as it does not call for national

[2] https://www.c-roads.eu

[3] Commission Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on *A European strategy on cooperative intelligent transport systems, a milestone towards cooperative, connected and automated mobility* (COM/2016/0766 final).

[4] 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 (OJ L 207, 6.8.2010, p. 1).

transposition measures and so ensures a greater degree of harmonisation, less administrative burden for the Member States, more legal certainty for public and private stakeholders and a swift entry into force.

2.2. Subsidiarity and proportionality

According to the principle of subsidiarity (Article 5(3) of the Treaty on European Union), EU-level action should be taken only where the envisaged aims cannot be achieved satisfactorily by Member States acting alone and can therefore, in view of the scale or effects of the proposed action, be better achieved by the EU.

While C-ITS services are already being deployed through projects across the EU and several Member States and many vehicle manufacturers have indicated that they intend to move to large-scale deployment, many have argued that a legal framework is needed at EU level. Industry-led standardisation through the European standardisation organisations (ESOs) contributes to interoperability, but it is voluntary and can allow for divergent, non-interoperable forms of implementation. With many different stakeholders and strong network effects, no stakeholder can introduce an interoperable solution on its own. Similarly, setting rules at national level would probably hinder the provision of continuous C-ITS services in the single European transport area.

Compatibility between infrastructure and vehicle solutions will need to be assured across the EU in order to reap the full benefits of C-ITS. In addition, a more harmonised approach at EU level is needed to ensure effective synergies with the deployment of new safety technologies and the roll-out of cooperative connected and automated mobility (CCAM) across the EU. Without an inclusive and future-proof EU-level framework, deployment would probably remain fragmented, uncoordinated and incapable of ensuring the geographical continuity of C-ITS services throughout the EU and at its external borders.

Compliance with this Delegated Regulation would be mandatory only where C-ITS services or stations were deployed. While binding EU specifications do require existing C-ITS stations and new technological solutions to adapt to these specifications, such specifications are essential to ensure the EU-wide interoperability of C-ITS services, and the planned review allows for flexibility in the development of technological solutions. A Regulation is more stringent than a guideline or a recommendation, but the expected direct and indirect benefits are also proportionally higher. In that sense, this delegated act is proportional.

Another important effect of this Delegated Regulation is to ensure the authenticity and integrity of messages exchanged between C-ITS stations. This should make it possible to assess the trustworthiness of such information. At the same time, the impact on the privacy of road users should be minimised. Accordingly, the C-ITS platform has developed a security architecture supported by a public key infrastructure (PKI) using frequently changing pseudonym certificates. The resulting common security and certificate policy has been the subject of broad consultation and been agreed upon by all stakeholders concerned.

2.3. Fundamental rights

The right to the protection of personal data is guaranteed under Article 8 of the Charter of Fundamental Rights of the European Union. Where the measures provided for in this Regulation entail the processing of personal data, they must be carried out in accordance with EU law on the protection of personal data, in particular the General Data Protection Regulation (GDPR)[5] and the e-Privacy Directive[6].

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of

On 10 July 2017, as part of its preparatory work, the Commission services consulted the technology subgroup of the Article 29 working party established under the Data Protection Directive[7]. The subgroup's opinion (October 2017) pointed to a number of actions required to support the lawful processing of personal data in the field of C-ITS. It was further clarified that, as this Regulation covers only the exchange of messages between C-ITS stations, it cannot by itself create a legal basis for the lawful processing of data. As a result, the obligations on data controllers and data processors remain fully applicable. However, this Regulation clarifies that without an appropriate, specific lawful basis, the personal data collected should not be (re)used, either for commercial purposes or as a new resource for law enforcement. Moreover, information relating to an identified or identifiable natural person should be processed in strict compliance with the principle of data minimisation and only for the purposes cited in this Regulation, and not stored longer than necessary. Finally, end-users should be informed clearly and in a comprehensive manner about the collection of data, and the arrangements for the periods during which it is kept.

3. RESULTS OF EX-POST EVALUATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

As there is no existing legislation in this area, no ex-post evaluation needed to be carried out.

- **Collection and use of expertise**

The Commission used the final reports of the C-ITS Platform Phases I and II. In addition, the Commission sought external expertise through a contract for an impact assessment support study with RICARDO Energy & Environment, supported by TRT and TEPR, which was launched in September 2017 and concluded in December 2018.

- **Impact Assessment**

The initiative is supported by an impact assessment which received a positive opinion with reservations after having been reviewed on 10 October 2018 by the Regulatory Scrutiny Board (RSB). The reservations of the RSB concerned two main aspects:

- The RSB was of the opinion that the report did not make sufficiently clear the need for a step-wise approach to reach the objectives of the initiative. As a result, the choice of the preferred option did not clearly flow from the analysis and presentation of the report.
- The RSB also considered that the report did not explain why it did not (yet) address stakeholder concerns on the safety of vulnerable road users and environmental impacts.

The following additions were made in the final impact assessment to address these reservations:

- The distinction between the different policy options and the considerations behind them have been reviewed and clarified throughout the Impact Assessment, in

such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) (OJ L281, 23.11.1995, p.31).

particular in sections 5.3, 7 and 8. The need for a separate impact assessment for potential follow-up legislative measures, including a V2V mandate, is explicitly discussed.

- The impact of C-ITS on vulnerable road users (VRUs) has been further clarified in section 6.1 and 6.5. It was underlined that VRU specific C-ITS services are not yet mature to be included in specifications and thus the policy options considered in this impact assessment. The stakeholder concerns have been described in more detail in Annex 2.
- Regarding the impacts, the sensitivity analysis in section 6.5 has been expanded to all policy options, and adjustments have been made throughout the report to better differentiate the policy options. Section 2 of Annex 4 has been updated to reflect that day 1 services have a strong focus on safety and to further clarify the limitations of the analysis.
- Section 6.4 has been added to discuss the data protection impacts of the different policy options. Annex 6 has also been updated in this regard.

The impact assessment examined three broad policy options:

PO1: Light intervention based on non-legislative measures, including non-binding guidelines on the interoperability of ‘day 1’ services, secure communication, data protection and compliance assessment;

PO2: Moderate intervention based on specifications under the ITS Directive. This would include elements similar to those in PO1, but make them legally binding through a Delegated Regulation. Nevertheless, Member States and industry remain free to decide whether or not to deploy C-ITS;

PO3: Strong intervention based on a vehicle-to-vehicle (V2V) mandate and the setting up of governance bodies. This option builds further on the legally binding specifications in a stepwise approach, by ensuring that all new vehicles are equipped with C-ITS stations, drastically increasing the uptake rate and thus meeting the threshold for effective service delivery (related to the network effect) much quicker. PO3 includes additional measures that support the deployment of C-ITS and cannot be introduced through a delegated act alone:

- a legislative measure can provide a legal basis for the lawful processing of personal data relating to C-ITS. This would increase legal certainty and probably result in the provision of more C-ITS services; and
- assigning governance roles to legal bodies will further ensure coordination and oversight on C-ITS deployment, thus ensuring that barriers to C-ITS uptake are reduced to a minimum.

The preferred approach is PO3 – a stepwise approach as provided for in the ITS Directive, where, after the adoption of specifications, a separate initiative for deployment will be considered, further analysing the efficiency and proportionality of a mandate based on the continued development of the C-ITS sector. This policy option is considered to most coherent and effective, delivering the highest reductions in accidents, congestion and CO_2 emissions.

The expected impacts are as follows:

- The main benefits are a reduction of accidents and fuel costs, and travel time savings. In addition, there is a slight reduction in the external costs of CO2 emissions and air pollutants. Total monetised benefits come to EUR 78.9 billion over the period 2020-

2035. This figure would rise to EUR 128.9 billion with the introduction of a V2V mandate.

- The main costs relate to C-ITS equipment in vehicles and in roadside infrastructure. Other compliance and administrative costs are assessed, but considered minor compared to the overall costs. Total monetised costs amount to EUR 19.1 billion relative over the period 2020-2035, or EUR 32.3 billion with the introduction of a V2V mandate. Thus the expected benefits strongly outweigh the expected costs.
- Although 90 % of the costs relate to equipping vehicle fleets, the cost of equipping infrastructure will largely be borne by the public sector. However, Member States remain free to decide whether or not to deploy.

4. RESULTS OF CONSULTATIONS

4.1. Meetings with experts nominated by Member States

Developing rules and requirements at EU level to support the deployment of C-ITS systems and services, and in particular the interoperability and continuity of EU-wide V2V and V2I services, required close cooperation between stakeholders (manufacturers, service providers and competent authorities). EU Member States and the EFTA countries were asked to nominate experts to attend a series of 13 meetings with the Commission services in Brussels between 23 May 2017 and 3 October 2018 to help produce the draft Regulation. Experts from the European Parliament were also invited to take part and the Commission held a number of bilateral meetings with Member States.

4.2. Stakeholder consultation

A public consultation was open on the Commission’s website from 10 October 2017 to 12 January 2018 (13 weeks) receiving 139 responses. The public consultation was based on a questionnaire exploring stakeholders’ opinions on the key components of the impact assessment: the main problem, its drivers, possible policy measures and their likely impacts, and the relevance of EU-level action.

A number of case studies were carried out as part of a support study:

- nine on EU C-ITS deployment projects; and
- three on C-ITS deployment in other countries (the United States, Australia and Japan); these involved interviews with senior representatives between October 2017 and February 2018.

All case studies focused on the following aspects of C-ITS deployment: objectives, progress, barriers, data collection and costs in the area concerned. In the EU case studies, respondents were also asked to provide feedback on the problem definition, policy measures and options, and the monitoring and evaluation of this policy initiative.

A stakeholder workshop was held on 9 February 2018 to gather specific information/data and experts’ and stakeholders’ views and suggestions. The workshop was well attended, with more than 140 participants.

On 6 September 2018 and 29 January 2019, the Commission presented the objective and scope of the Regulation to the members of the Transport and Tourism Committee.

The draft of the Regulation has been subject to a public consultation through the Better Regulation Portal from 11 January 2019 to 8 February 2019, receiving 100 responses.

4.3. C-ITS communication technologies

A particular important issue for C-ITS are the communication technologies that can be used for exchanging messages between C-ITS stations. This is directly linked to the need to ensure that everybody is able to talk to everybody (interoperability) and that everybody remains able to talk to everybody (compatibility).

Maximising benefits involves leveraging the distinct advantages of different, complementary technologies. The 'hybrid communication' approach combines two types of technologies:

- short-range communication technologies, which operate in a dedicated 5.9 GHz frequency band and are most relevant for time-critical services. ITS-G5 was developed specifically for this purpose and is now mature, tested and already deployed; and

- longer-range communication technologies, which leverage the coverage of existing networks and connect large areas, albeit for less time-critical V2I services. Cellular 3G/4G are mature technologies that already provide good coverage in large parts of the EU.

The practical implementation of the hybrid communication approach, combined with the need to ensure the interoperability and continuity of services, imposes certain technological choices. These are reflected in a minimum set of functional and technical requirements for the interoperable exchange of messages between C-ITS stations. As this should not hinder further innovation, this Regulation ensures that future technologies can be integrated in the 'hybrid communication' mix.

A review clause will facilitate the integration of several existing candidates, such as LTE-V2X (a cellular-based short-range communication technology) and 5G, the set of technologies for next-generation cellular networks. The Commission will discuss possible amendments to this Delegated Regulation with an expert group in an open and transparent way and inform it regularly about the progress and possible next steps. Stakeholders that have already put C-ITS stations in service should cooperate in this process in good faith, in line with both Union and national competition laws, to ensure a level playing field between different technologies, and without hindering the development of new ones. In the interest of allowing future developments in this area, these stakeholders should also prepare their products for the integration of future technologies.

5. BUDGETARY IMPLICATIONS

This Regulation has some implications for the EU budget.

To ensure that the C-ITS network functions smoothly, certain tasks need to be carried out by central entities before the full governance framework can be established. Pending the establishment of such entities, the Commission will perform some of the tasks – mainly those relating to the EU C-ITS security credential management system, the EU's C-ITS framework for the provision of trusted and secure communication on the basis of a PKI.

It is important to ensure that C-ITS stations can be enrolled in the security credential management system before being put in service and becoming operational. To this end, the tasks of the central point of contact, the trust list manager and the C-ITS certificate policy authority will be assumed by the Commission, as a shared task of JRC and DG MOVE.

This will have no impact in terms of human resources, as JRC and DG MOVE will use or redeploy staff as necessary. Also, JRC benefits from the 'Security architecture for connected infrastructure and vehicles in Europe' support action in the context of Commission

Implementing Decision C(2016) 1966[8], which assigns EUR 4 million for the implementation of phase I of the security credential management system (2018-2021). Should further support actions be needed, they could be financed under the Connecting Europe Facility.

[8] Commission Implementing Decision of 7 April 2016 amending Commission Implementing Decision C(2014) 1921 establishing a Multi-Annual Work Programme 2014-2020 for financial assistance in the field of Connecting Europe Facility (CEF) - Transport sector for the period 2014-2020.

COMMISSION DELEGATED REGULATION (EU) …/...

of 13.3.2019

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

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to 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[1], and in particular Article 6(3) in conjunction with Article 7 thereof,

Whereas:

(1) Article 2(1) of Directive 2010/40/EU identifies the linking of the vehicle with the transport infrastructure as priority area IV for the development and use of specifications and standards. This involves inter alia developing and implementing cooperative (vehicle-vehicle, vehicle-infrastructure, where messages can originate both in the vehicle and or in the infrastructure, and infrastructure-infrastructure) systems based on: the facilitation of the exchange of data or information between vehicles, between infrastructures and between vehicles and infrastructure; the use of a standardised message format for the exchange of data or information between vehicles and infrastructure; and the definition of a communication infrastructure for data or information exchange between vehicles, between infrastructures and between vehicles and infrastructure.

(2) Cooperative intelligent transport systems (C-ITS) use technologies that enable road vehicles to communicate with each other and with roadside infrastructure including traffic signals. C-ITS services are a category of ITS services based on an open network that enables a many-to-many or peer-to-peer relationship between C-ITS stations. This means all C-ITS stations, as defined by this Regulation, can securely exchange messages with each other, and are not limited to exchanging messages with (a single) pre-defined station(s). C-ITS stations do not need additional requirements such as: using the same software or having an account or contractual relationship with the same entity (e.g. the same vehicle manufacturer, road authority or service provider).

(3) The European C-ITS strategy[2] identified a risk of fragmentation of the internal market in the field of C-ITS and a need to lay down minimum requirements for C-ITS services to ensure their coordinated and coherent deployment. In this context, the

[1] OJ L 207, 6.8.2010, p. 1.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on *A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility* (COM(2016) 766 final).

Commission announced its intention, where appropriate, to make use of its mandate under Directive 2010/40/EU to adopt delegated act(s) by 2018 to ensure compatibility, interoperability and continuity of C-ITS services in the deployment and operational use of Union-wide C-ITS services based on trusted and secure communication.

(4) In order to foster and maximise all road safety and traffic efficiency benefits of C-ITS services, the specifications set out in this Regulation should apply to the entire road transport network. This includes its interfaces with other transport modes that are relevant to road safety or traffic efficiency, such as rail crossings, port areas, etc.

(5) The specifications laid down in this Regulation should apply to all C-ITS services without prejudice to particular specifications adopted in other acts under Directive 2010/40/EU, in particular Commission Delegated Regulations (EU) No 886/2013[3] and (EU) No 962/2015[4].

(6) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016[5] concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive") puts in place requirements concerning national capabilities in the area of cybersecurity, establishes mechanisms to enhance strategic and operational cooperation between Member States, and introduces obligations concerning security measures and incident notifications across sectors. As the NIS Directive listed operators of Intelligent Transport Systems as defined in paragraph 1 of Article 4 of Directive 2010/40/EU as potential operators of essential services, the application of the NIS Directive and of the requirements imposed pursuant to the present Regulation may be in certain cases complementary.

(7) Commission Decision 2008/671/EC[6] harmonises the conditions for the availability and efficient use of the 5 875-5 905 MHz frequency band for safety-related applications of ITS in the Union.

(8) In response to standardisation mandate M/453[7], the European standardisation organisations (ESOs) – the European Telecommunications Standards Institute (ETSI) and the European Committee for Standardisation (CEN) – have developed common standards for the deployment of C-ITS services, to which this Regulation refers. Those standards provide a basis for the effective provision of C-ITS priority services, enabling road traffic managers to take appropriate measures and preparing the ground for safer automation on EU roads. Standardisation work will continue, amongst others to integrate other technologies and further strengthen C-ITS. The relevant standardisation bodies and all stakeholders should therefore continue the work developed under standardisation mandate M/453 and jointly develop solutions that support interoperability and allow all technologies to play their role.

[3] Commission Delegated Regulation (EU) No 886/2013 of 15 May 2013 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to users (OJ L 247, 18.9.2013, p. 6).

[4] Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

[5] OJ L 194, 19.7.2016, p. 1.

[6] Commission Decision 2008/671/EC of 5 August 2008 on the harmonised use of radio spectrum in the 5 875-5 905 MHz frequency band for safety-related applications of Intelligent Transport Systems (ITS) (OJ L 220, 15.8.2008, p. 24).

[7] M/453: Standardisation mandate addressed to CEN, CENELEC and ETSI in the field of information and communication technologies to support the interoperability of co-operative systems for intelligent transport in the European Community

(9) To ensure interoperability, each C-ITS station requires a specific configuration of standards ('system profile') determining the implementation of various optional standards. The system profile describes external interfaces needed for communication between C-ITS stations. Each C-ITS station must comply with Directive 2014/53/EU of the European Parliament and of the Council[8]. Cooperation between industry and Member States' authorities has led to the development of harmonised system profiles for vehicle C-ITS stations and roadside C-ITS stations communicating in the 5 855-5 925 MHz frequency band. If all C-ITS services are to be received seamlessly across the Union, a 'hybrid communication' approach is needed, i.e. one that combines complementary communication technologies. In view of the pace of technological progress, industry and Member States are encouraged to develop – and harmonise across the Union – additional complementary and compatible system profiles for other types of C-ITS stations and technologies. Before using such new profiles or technologies, they should inform the Commission so that an update of this Regulation can be considered without delay. Such updates should be prepared in close cooperation with the Member States.

(10) The cooperative nature of C-ITS requires each C-ITS station to contribute information to the C-ITS network. C-ITS stations should not interfere with the provision of C-ITS priority services, European electronic toll services or the smart tachograph, nor with the functioning of other C-ITS stations.

(11) It is important that industry and Member States implement common technical solutions for the provision of C-ITS services. These should be developed in particular through the ESOs, in order to facilitate the introduction of C-ITS services, ensure the interoperability and continuity of the services throughout the Union, and reduce the costs of implementation. To ensure the compatibility, interoperability and continuity of Union-wide C-ITS services, the standards and system profiles referred to in this Regulation should be used where relevant as a reference for the development of future C-ITS technologies and services.

(12) As regards deployment, priority should be given to C-ITS services that contribute to road safety and traffic efficiency. Those that constitute road-safety-related minimum universal traffic information services, as defined in Delegated Regulation (EU) No 886/2013, should where possible be provided as a universal service free of charge to end-users at the point of use in accordance with that Regulation.

(13) To ensure interoperability, each C-ITS service requires a specific configuration of standards, called a service profile, defining the implementation of various options of standards. C-ITS services should not interfere with the provision of the C-ITS priority services. The current vehicle-vehicle service profiles have been developed primarily for passenger cars. To enable the deployment of these or similar services for other vehicle categories, the development of additional service profiles, or an update of the service profiles in this Regulation, might be required.

(14) Decision No 768/2008/EC of the European Parliament and of the Council[9] lays down common principles and reference provisions to apply across sectoral legislation. It

[8] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (OJ L 153, 22.5.2014, p. 62).

[9] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC (OJ L 218, 13.8.2008, p. 82).

therefore constitutes a general horizontal framework for any new legislation harmonising the conditions for the marketing of products. Its reference provisions provide definitions and general obligations for economic operators and a range of conformity assessment procedures from which the legislator can select as appropriate. In order to ensure the safety of the market place, it also lays down rules for CE marking and reference provisions on procedures for dealing with products presenting a risk. As this Regulation covers the placing on the market of C-ITS stations, it is appropriate to use reference provisions in Annex I to that Decision that make the manufacturer responsible for ensuring inter alia compliance with all applicable legislation; that an EU declaration of conformity is drawn up; that the conformity marking is affixed and that appropriate technical documentation is prepared. The roles and responsibilities of other entities, such as the authorised representative, the importer and the distributor, should also be regulated.

(15) In this Regulation, C-ITS stations installed on vehicles, handheld or alongside the road infrastructure are considered as products that can be placed on the market as stand-alone assemblies or as parts of larger assemblies. The extent to which C-ITS stations to be installed on vehicles comply with the applicable requirements can be tested before or after installation. In the case of roadside C-ITS stations, this can be tested before installation, so they can be placed on the market as stand-alone products. With central C-ITS stations, the situation may be different, because they will often be integrated in traffic control centres that are not standardised. As such traffic control centres are constructed gradually in line with the development of the traffic areas they manage, it may be that they cannot be fully tested before being placed on the market. In any case, the level of security and trust should be the same for all C-ITS stations, including central ones.

(16) Before any C-ITS station is put in service and becomes operational, it is necessary to identify the entity that will check that it is accompanied by an EU declaration of conformity and, where applicable, that conformity marking has been affixed. This entity should register the station in the EU C-ITS security credential management system and ensure that it continues to comply with the technical requirements throughout the period of its use. The entity will be the operator of the C-ITS station and be in charge of relations with the user.

(17) For many C-ITS services, it is essential to ensure the authenticity and integrity of C-ITS messages containing information, such as position, velocity and heading. Therefore, one common European C-ITS trust model should be established for all C-ITS stations (all mobile C-ITS stations, same requirements for vehicle and personal, and all fixed C-ITS stations, same requirements for central and roadside), regardless of communication technologies used. The rules and requirements of this trust model are laid down in the certificate and security policy. The highest level of the Public Key Infrastructure (PKI) is the European certificate trust list, which contains entries of all trusted root certification authorities in Europe.

(18) Some efforts have been made in the past in order to lead to a mutual recognition of security certificates of products in Europe. The most important example in this regard is the Senior Officials Group – Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA). While it represents the most important model for cooperation and mutual recognition in the field of security certification, SOG-IS includes only part of the Member States of the Union. As security certification of C-ITS stations is an important element of the C-ITS certificate and security policy, the

SOG-IS MRA is applied in the absence of other equivalent European cybersecurity certification schemes under the relevant European cybersecurity framework.

(19) Certain C-ITS stations placed on the market before the date of application of this Regulation, might not fully comply with C-ITS security related requirements of this Regulation, because technical deployment decisions might have already been taken at an earlier moment in time. To allow such C-ITS stations to become part of the C-ITS network after the date of application of this Regulation, a procedure should be provided to consider granting enrolment of such C-ITS stations in the C-ITS trust model.

(20) Article 6(6) of the Directive 2010/40/EU requires the Commission to adopt specifications complying with a set of principles, including the use of satellite-based infrastructures, or any technology providing equivalent levels of precision for the purposes of ITS applications and services that require global, continuous, accurate and guaranteed timing and positioning services. Therefore, it is appropriate to ensure the compatibility of C-ITS stations with the added value services provided by the Galileo and the European Geostationary Navigation Overlay Service ('EGNOS') programmes as set out in Regulation (EU) No 1285/2013 of the European Parliament and of the Council in order to improve the reliability of the C-ITS stations.

(21) The platform for the deployment of C-ITS in the Union (C-ITS platform), which was set up in November 2014 and chaired by Commission departments, developed a common security and certificate policy, endorsed by all interested stakeholders. As the common security and certificate policy should be updated in line with technical progress and the development of the governance framework, the Commission should be reviewing this Regulation on an ongoing basis in order to maintain coherence and consistency.

(22) To ensure the smooth functioning of the C-ITS network, certain tasks need to be carried out by central entities before the full governance framework can be established. Pending the establishment of central entities, the Commission should be in charge of those tasks, including those relating to the C-ITS certificate policy authority, the trust list manager, and the C-ITS point of contact.

(23) Where the measures provided for in this Regulation entail the processing of personal data, they should be carried out in accordance with Union law on the protection of personal data and privacy, in particular Regulation (EU) 2016/679[10], and, where applicable, Directive 2002/58/EC[11]. Such processing should have an appropriate legal basis, as listed in Article 6 of Regulation (EU) 2016/679, which is not provided for by this Delegated Regulation.

(24) Without an appropriate legal basis, the personal data collected should not be reused for any other purposes, such as commercial purposes or as a new resource for law enforcement, unless on the basis of a law.

(25) Information relating to an identified or identifiable natural person should be processed in strict compliance with the principle of data minimisation and only for the purposes

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[11] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

specified in this Regulation, and not stored longer than necessary. Security requirements on pseudonymisation that are provided for in this Regulation, contribute to reduce the risk of data misuse.

(26) End-users should be informed clearly and in a comprehensive manner on all relevant information on the processing of their personal data in accordance with Regulation (EU) 2016/679.

(27) As stated in the common security and certificate policy, developed within the context of the C-ITS platform, governance requires bodies in the form of common steering committees of stakeholders, including the Commission, Member States, road infrastructure operators, and C-ITS station manufacturers and operators. Pending the establishment of such bodies, the Commission, assisted by an expert group in which all relevant stakeholders are represented, should be in charge of the relevant tasks, including those relating to governance, supervision and the C-ITS certificate policy authority. This expert group should include in particular representatives of C-ITS station manufacturers and operators in the C-ITS network, as well as other concerned stakeholders and relevant authorities of the Member States.

(28) The broad and inclusive consultation process that led to the development of the security policy and governance framework and the certificate policy (with the support of all relevant public and private stakeholders) should also apply to the updating of this Regulation in line with technical progress and, where appropriate, with the development of the governance framework.

(29) Member States and root certification authorities should regularly provide the Commission with information enabling it to monitor the implementation of this Regulation.

(30) In order to take account of the rapid development of new markets, technologies and services, as already announced in the updated working programme of the ITS Directive, it is expected that this Regulation will be amended before the review of the implementation of this Regulation, which should be conducted three years following after its entry into force.

Prime candidate for such an amendment is the inclusion of existing 3G/4G networks to deliver the C-ITS priority services. In addition, specifications for LTE-V2X technologies have been finalised in 3GPP and prototype implementations are currently being validated. These technologies are currently being integrated into European norms and technical specifications, both for C-ITS priority services and for new emerging services. Finally, rapidly evolving new technologies such as 5G could also underpin C-ITS services.

Some of these developments could trigger one or more amendments of this Regulation, once a file with technically mature specifications is transmitted to the Commission. Such amendments should ensure an open and future-proof approach in standards and legislation. The Commission should consult an expert group on possible amendments to this Regulation in an open and transparent way and inform it regularly about the progress and possible next steps. To maintain the continuity of the C-ITS priority services, they should also ensure compatibility and interoperability with existing C-ITS stations, already put in service in accordance with this Regulation, or specify a suitable migration path taking into account also market and technology developments.

The Commission should analyse the file, and discuss it in the expert group without undue delay, in view of a possible amendment of this Regulation, examining whether a change to existing requirements is needed. Stakeholders that have already put C-ITS stations in service should cooperate in this process in good faith, in line with both Union and national competition laws, to ensure a level playing field between different technologies, and without hindering the development of new ones. In the interest of allowing future developments in this area, these stakeholders should also prepare their products for the integration of future technologies.

(31) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council[12] and delivered an opinion on … ,

HAS ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

1. This Regulation establishes specifications necessary to ensure compatibility, interoperability and continuity in the deployment and operational use of Union-wide C-ITS services based on trusted and secure communication.

   It lays down how vehicle-vehicle, vehicle-infrastructure and infrastructure-infrastructure communication is to be conducted by means of C-ITS stations and how C-ITS stations are to be placed on the market and put in service, to enable the provision of C-ITS services to ITS users.

2. This Regulation applies to all C-ITS stations in the field of road transport and to their interfaces with other modes of transport.

3. The deployment of C-ITS stations is carried out in accordance with Article 5 of Directive 2010/40/EU. Member States shall designate the part of their transport network infrastructure that is equipped with C-ITS stations.

Article 2

Definitions

For the purposes of this Regulation, the following definitions shall apply:

(1) ‘cooperative intelligent transport systems’ or ‘C-ITS’ means intelligent transport systems that enable ITS users to cooperate by exchanging secured and trusted messages using the EU C-ITS security credential management system;

(2) ‘C-ITS service’ means an ITS service provided through C-ITS;

[12] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1).

(3) ‘C-ITS station’ means the set of hardware and software components required to collect, store, process, receive and transmit secured and trusted messages in order to enable the provision of a C-ITS service. This includes personal, central, vehicle and roadside ITS stations as defined in EN 302 665 v 1.1.1;

(4) ‘mobile C-ITS station’ means a C-ITS station installed in a vehicle or in the form of a personal hand-held device;

(5) ‘fixed C-ITS station’ means a C-ITS station installed in a central system or roadside infrastructure;

(6) 'central C-ITS station' means a central server with integrated C-ITS station capabilities, such as in a traffic management centre;

(7) ‘making available on the market’ means the supply of a C-ITS station for distribution or use on the Union market in the context of a commercial activity, either in return for payment or free of charge;

(8) ‘placing on the market’ means the first making available of a C-ITS station on the Union market;

(9) the ‘putting in service’ of a C-ITS station means its first use in the Union for the purposes for which it was intended;

(10) ‘short-range communication’ means communication in the 5 855-5 925 MHz frequency band;

(11) ‘C-ITS priority service'’ means a C-ITS service that contributes to road safety or traffic efficiency and which is included in Annex I;

(12) ‘system profile’ means a minimum set of functional and technical requirements for the interoperable exchange of messages between C-ITS stations;

(13) ‘service profile’ means a set of functional specifications for interoperable messages to enable the provision of a C-ITS service;

(14) ‘Global Navigation Satellite System’ (‘GNSS’) means an infrastructure composed of a constellation of satellites and a network of ground stations, which provides accurate timing and geolocation information to users having an appropriate receiver.

(15) ‘manufacturer’ means any natural or legal person that designs and manufactures a C-ITS station or has a C-ITS station designed or manufactured, and markets that C-ITS station under its name or trademark;

(16) ‘C-ITS station operator’ means any natural or legal person who is responsible for the putting in service and the operation of C-ITS stations in accordance with this Regulation;

(17) ‘authorised representative’ means any natural or legal person established in the Union that has received a written mandate from a manufacturer to act on its behalf in relation to specified tasks;

(18) ‘importer’ means any natural or legal person established in the Union that places a C-ITS station from a third country on the Union market;

(19) ‘distributor’ means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a C-ITS station available on the market;

(20) ‘economic operator’ means the manufacturer, authorised representative, importer or distributor;

(21) ‘recall’ means any measure aimed at achieving the return of a C-ITS station that has already been made available to the end-user;

(22) ‘withdrawal’ means any measure aimed at preventing a C-ITS station in the supply chain from being made available on the market;

(23) 'CE marking' means a marking by which the manufacturer indicates that the product is in conformity with the applicable requirements set out in the Union legislation providing for its affixing;

(24) 'end-user' means a natural or legal person who ultimately uses or is intended to ultimately use a C-ITS station;

(25) ‘market surveillance authority’ means an authority of a Member State responsible for carrying out market surveillance on its territory;

(26) 'competent national authority' means any authority that is entitled to check the conformity of a C-ITS station with the applicable legislation;

(27) 'EU C-ITS security credential management system' means the European Union C-ITS framework for the provision of trusted and secure communication using a public key infrastructure (PKI);

(28) ‘enrolment authority’ means the legal and/or operational entity that authenticates a C-ITS station and grants it access to C-ITS.

(29) ‘C-ITS network’ means all operational C-ITS stations in the Union;

Article 3

Making available on the market and/or putting into service

A C-ITS station shall only be made available on the market and/or put into service if, where properly maintained and used for its intended purpose, it complies with this Regulation.

Article 4

Free movement

Member States shall not prohibit, restrict or impede, for the reasons covered by this Regulation, the making available on the market or the putting into service in their territory of C-ITS stations which comply with this Regulation.

CHAPTER II

TECHNICAL REQUIREMENTS

Article 5

Requirements for C-ITS stations

1. Vehicle C-ITS stations designed for short-range communication shall comply with the requirements laid down in the system profile in Section 2 of Annex II.

2. Roadside C-ITS stations designed for short-range communication shall comply with the requirements laid down in the system profile in Section 3 of Annex II.

3. C-ITS stations shall send messages that enable the provision of at least one of the C-ITS priority services listed in Annex I.

4. C-ITS stations shall be compatible with C-ITS stations that send messages for the C-ITS priority services listed in Annex I.

5. C-ITS stations shall not interfere with the operation of the European electronic toll service as referred to in Directive 2004/52/EC of the European Parliament and of the Council[13] and in Commission Decision 2009/750/EC[14] and the operation of the smart tachograph referred to in Regulation (EU) No 165/2014 of the European Parliament and of the Council[15].

6. C-ITS stations shall be compatible with C-ITS stations that comply with the system profiles set out in Annex II.

7. When C-ITS stations are enabled with GNSS, they shall be compatible with the positioning and timing services provided by the Galileo and EGNOS systems. In addition, C-ITS stations may be compatible with other satellite navigation systems.

Article 6

Requirements for C-ITS services

1. The C-ITS priority services listed in Annex I shall comply with the requirements of the corresponding C-ITS service profile.

2. Each C-ITS service shall work without modification with all service profiles as set out in Annex I.

CHAPTER III

PLACING C-ITS STATIONS ON THE MARKET

Article 7

Obligations of C-ITS station manufacturers

1. When placing C-ITS stations on the market, manufacturers shall ensure that they have been designed and manufactured in accordance with the requirements set out in Article 5.

2. Manufacturers shall draw up the technical documentation referred to in Part A of Annex V and carry out the conformity assessment procedure referred to in Part A of Annex V or have it carried out.

3. Where compliance of a C-ITS station with the applicable requirements has been demonstrated by the conformity assessment procedure referred to in Part A of Annex V, manufacturers shall draw up an EU declaration of conformity and affix the CE marking.

[13] Directive 2004/52/EC of the European Parliament and of the Council of 29 April 2004 on the interoperability of electronic road toll systems in the Community (OJ L 166, 30.4.2004, p. 124)

[14] Commission Decision 2009/750/EC of 6 October 2009 on the definition of the European Electronic Toll Service and its technical elements (OJ L 268, 13.10.2009, p. 11)

[15] Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport (OJ L 60, 28.2.2014, p. 1).

4. Manufacturers shall keep the technical documentation referred to in Part A of Annex V and the EU declaration of conformity for 10 years after the C-ITS station has been placed on the market.

5. Manufacturers shall ensure that procedures are in place for series production to remain in conformity with this Regulation.

6. To protect the health and safety of consumers, where deemed appropriate with regard to the risks presented by C-ITS stations, manufacturers shall:

   (a) carry out sample testing of marketed C-ITS stations;

   (b) investigate and, if necessary, keep a register of complaints, of non-conforming C-ITS stations and of C-ITS station recalls;

   (c) keep distributors informed of any such monitoring.

7. Manufacturers shall ensure that C-ITS stations that they have placed on the market bear a type, batch or serial number or other element allowing their identification.

8. On the C-ITS station or, where that is not possible, on its packaging or in a document accompanying the C-ITS station, manufacturers shall indicate their:

   (a) name;

   (b) registered trade name or registered trademark;

   (c) postal address, indicating a single point at which they can be contacted.

   The contact details shall be in a language easily understood by both end-users and market surveillance authorities.

9. Manufacturers shall ensure that the C-ITS station is accompanied by instructions and safety information in a language that can be easily understood by end-users, as determined by the Member State concerned. Such instructions and safety information, and any labelling, shall be clear, understandable and intelligible.

10. Manufacturers that consider that a C-ITS station that they have placed on the market is not in conformity with this Regulation shall immediately take the necessary corrective measures to bring it into conformity, or to withdraw or recall it, as appropriate. Where the C-ITS station presents a risk, manufacturers shall immediately inform the market surveillance authorities of the Member States in which they have made it available, giving details, in particular, with regard to the non-compliance and any corrective measures taken.

11. On reasoned request from a competent national authority, manufacturers shall provide it with all information and documentation in paper or electronic form necessary to demonstrate the conformity of the C-ITS station, in a language which can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action taken to eliminate the risks posed by C-ITS stations that they have placed on the market.

Article 8

Authorised representatives

1. A manufacturer may appoint an authorised representative by written mandate.

2. Authorised representatives shall perform the tasks specified in the mandate received from the manufacturer. The mandate shall allow the authorised representative to do at least the following:

(a) keep the EU declaration of conformity and the technical documentation at the disposal of national market surveillance authorities for 10 years after the C-ITS station has been placed on the market;

(b) on reasoned request from a competent national authority, provide it with all the information and documentation necessary to demonstrate the conformity of a C-ITS station;

(c) cooperate with the competent national authorities, at their request, on any action to eliminate the risks posed by C-ITS stations covered by their mandate.

The obligations laid down in Article 7(1) and the drawing up of technical documentation referred to in Article 7(2) shall not form part of the authorised representative's mandate.

Article 9

Obligations of importers

1. Importers shall place only compliant C-ITS stations on the Union market.

2. Before placing a C-ITS station on the market, importers shall ensure that:

(a) the manufacturer has carried out the conformity assessment procedure referred to in Article 7(2);

(b) the manufacturer has drawn up the technical documentation;

(c) the C-ITS station bears the required the CE marking ;

(d) the manufacturer has complied with the requirements set out in Article 7(7) and (8).

3. Where an importer considers that a C-ITS station is not in conformity with the requirements referred to in Article 5, it shall not place the product on the market until it has been brought into conformity. Where the C-ITS station presents a risk, the importer shall inform the manufacturer and the market surveillance authorities to that effect.

4. On the C-ITS station or, where that is not possible, on its packaging or in a document accompanying the C-ITS station, importers shall indicate:

(a) their name;

(b) their registered trade name or registered trademark;

(c) the address at which they can be contacted.

The contact details shall be in a language easily understood by end-users and competent national authorities.

5. Importers shall ensure that the C-ITS station is accompanied by instructions and safety information in a language that can be easily understood by end-users, as determined by the Member State concerned.

6. Importers shall ensure that, while a C-ITS station is under their responsibility, storage or transport conditions do not jeopardise its compliance with the requirements set out in Article 5.

7. To protect the health and safety of consumers, where deemed appropriate with regard to the risks presented by a C-ITS station, importers shall:

   (a) carry out sample testing of the marketed C-ITS station;

   (b) investigate and, if necessary, keep a register of complaints, of non-conforming C-ITS stations and of C-ITS station recalls;

   (c) keep distributors informed of such monitoring.

8. Importers who consider that a C-ITS station that they have placed on the market is not in conformity with this Regulation shall immediately take the corrective measures necessary to bring that C-ITS station into conformity, or to withdraw or recall it, as appropriate. Where the C-ITS station presents a risk, importers shall immediately inform the competent national authorities of the Member States in which they have made it available, giving details, in particular, of the non-compliance and any corrective measures taken.

9. For 10 years after the C-ITS station has been placed on the market, importers shall keep a copy of the EU declaration of conformity at the disposal of the market surveillance authorities and ensure that the technical documentation can be made available to those authorities on request.

10. On reasoned request from a competent national authority, importers shall provide it with all information and documentation in paper or electronic form necessary to demonstrate the conformity of a C-ITS station in a language that can be easily understood by that authority. They shall cooperate with that authority, at its request, on any action to eliminate the risks posed by C-ITS stations that they have placed on the market.

Article 10

Obligations of distributors

1. When making a C-ITS station available on the market, distributors shall act with due care in relation to the requirements of this Regulation.

2. Before making a C-ITS station available on the market, distributors shall verify that:

   (a) it bears the CE marking;

   (b) it is accompanied by the instructions and safety information referred to in Article 7(9) in a language that can be easily understood by end-users in the Member State in which it is to be made available on the market;

   (c) the manufacturer and the importer have complied with the requirements set out in Article 7(7) and (8) and Article 9(4).

3. Where a distributor considers that a C-ITS station is not in conformity with Article 5, it shall not make it available on the market until it has been brought into conformity. Where the C-ITS station presents a risk, the distributor shall inform the manufacturer or importer and the market surveillance authorities to that effect.

4. Distributors shall ensure that, while a C-ITS station is under their responsibility, storage or transport conditions do not jeopardise its compliance with the requirements in Article 5.

5. Distributors that consider that a C-ITS station which they have made available on the market is not in conformity with this Regulation or any other applicable Union legislation shall make sure that corrective measures are taken to bring it into conformity, or to withdraw it or recall it, as appropriate. Where the C-ITS station presents a risk, distributors shall immediately inform the market surveillance authorities of the Member States in which they made it available, giving details, in particular, of the non-compliance and of any corrective measures taken.

6. On reasoned request from a competent national authority, distributors shall provide it with all information and documentation necessary to demonstrate the conformity of a C-ITS station. They shall cooperate with that authority, at its request, on any action to eliminate the risks posed by C-ITS stations that they have made available on the market.

Article 11

Cases in which obligations of manufacturers apply to importers and distributors

Where an importer or distributor places a C-ITS station on the market under its name or trademark or modifies a C-ITS station already placed on the market in such a way that compliance with this Regulation may be affected, it shall be considered a manufacturer for the purposes of this Regulation and be subject to the obligations of the manufacturer under Article 7.

Article 12

Identification of economic operators

Economic operators shall, on request, identify the following to the market surveillance authorities;

(a) any economic operator who has supplied them with a C-ITS station;

(b) any economic operator to whom they have supplied a C-ITS station.

Economic operators shall be able to present the information referred to in the first paragraph for 15 years after they have been supplied with the C-ITS station and for 15 years after they have supplied with the C-ITS station.

Article 13

EU declaration of conformity

1. The EU declaration of conformity shall state that the fulfilment of requirements specified in Article 5 has been demonstrated.

2. The EU declaration of conformity shall be structured according to the model in Part B of Annex V, contain the elements specified in Part A of Annex V and be kept up to date. It shall be translated into the language or languages required by the Member State where the C-ITS station is made available on the market.

3. By drawing up the EU declaration of conformity, the manufacturer shall assume responsibility for the compliance of the C-ITS station with the requirements laid down in this Regulation.

4. Where a C-ITS station is subject to more than one Union act requiring an EU declaration of conformity, a single declaration shall be drawn up in respect of all such acts. That declaration shall identify the acts concerned, including their publication references.

Article 14

General principles of the CE marking

The CE marking shall be subject to the general principles set out in Article 30 of Regulation (EC) No 765/2008 of the European Parliament and of the Council[16].

Article 15

Rules and conditions for affixing the CE marking

1. The CE marking shall be affixed visibly, legibly and indelibly to the C-ITS station or to its data plate.

2. The CE marking shall be affixed before the C-ITS station is placed on the market. It may be followed by a pictogram or any other mark indicating a special risk or use.

Article 16

Union market surveillance and control of C-ITS stations entering the Union market

Article 15(3) and Articles 16 to 29 of Regulation (EC) No 765/2008 shall apply to C-ITS stations.

Article 17

Procedure for dealing with C-ITS stations presenting a risk at national level

1. Where the market surveillance authorities of one Member State have taken action pursuant to Article 20 of Regulation (EC) No 765/2008 or where they have reason to believe that a C-ITS station presents a risk to the health or safety of persons or road safety and traffic efficiency, they shall carry out an evaluation of the C-ITS station concerned covering all applicable requirements of this Regulation. The relevant economic operators shall cooperate with them as necessary.

   Where, in the course of the evaluation, the market surveillance authorities find that the C-ITS station does not comply with the requirements of this Regulation, they shall without delay require the relevant economic operator to take all appropriate corrective measures to bring it into compliance with those requirements, withdraw it

[16] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (OJ L 218, 13.8.2008, p. 30).

from the market or recall it within a reasonable period, commensurate with the nature of the risk.

Article 21 of Regulation (EC) No 765/2008 shall apply to the measures referred to in the second subparagraph of this paragraph.

2. Where the market surveillance authorities consider that non-compliance is not restricted to their national territory, they shall inform without delay the Commission and the other Member States of the results of the evaluation and of the measures that they have required the economic operator to take.

3. The economic operator shall ensure that all appropriate corrective measures are taken throughout the Union in respect of all C-ITS stations concerned that it has made available on the Union market.

4. Where the economic operator does not take adequate corrective measures within the period referred to in the second subparagraph of paragraph 1, the market surveillance authorities shall take all appropriate provisional measures to prohibit or restrict the making available of the C-ITS station on their national market, withdraw it from that market or recall it.

5. The market surveillance authorities shall inform the Commission and the other Member States of the provisional measures referred to in paragraph 4 without delay. That information shall include all available details, including:

(a) the data necessary to identify the non-compliant C-ITS station;

(b) the origin of the C-ITS station;

(c) the risk involved and the nature of the alleged non-compliance of the C-ITS with the requirements set out in this Regulation;

(d) the nature and duration of the provisional measures taken;

(e) the arguments put forward by the economic operator.

6. Member States other than the Member State initiating the procedure shall without delay inform the Commission and the other Member States of:

(a) any measures they have adopted;

(b) any additional information at their disposal relating to the non-compliance of the C-ITS station concerned;

(c) any objections they may have to the provisional measures taken by the Member State initiating the procedure.

7. Where, within three months of receiving the information referred to in paragraph 5, the other Member States or the Commission have raised no objection to a provisional measure taken by a Member State, that measure shall be deemed justified. Where the provisional measure is deemed justified, Member States shall ensure that appropriate restrictive measures are taken in respect of the C-ITS station concerned, such as its withdrawal from their market, without delay.

Article 18

Union safeguard procedure

1. Where, on completion of the procedure set out in Article 17(3) and (4), objections have been raised against a provisional measure taken by a Member State, or where the Commission considers a provisional measure to be contrary to Union legislation, the Commission shall without delay enter into consultation with the Member States and the relevant economic operators and evaluate the provisional measure. On the basis of the results of that evaluation, the Commission shall decide whether the national measure is justified or not.

   The Commission shall address its decision to all Member States and immediately communicate it to the relevant economic operators.

2. If the provisional measure is considered justified in a Commission decision, all Member States shall take the measures necessary to ensure that the non-compliant C-ITS station is withdrawn from their market and inform the Commission accordingly. If the provisional measure is considered unjustified, the Member State concerned shall withdraw it.

Article 19

Compliant C-ITS stations that present a risk to health and safety at national level

1. Where, after an evaluation pursuant to Article 17(1), the market surveillance authorities of a Member State find that, while in compliance with this Regulation, a C-ITS station presents a risk to the health or safety of persons or to other aspects of public interest protection, those authorities shall order the relevant economic operator to take one or more of the following corrective measures commensurate with the nature of the risk:

   (a) to take all appropriate measures to ensure that the C-ITS station, when placed on the market, no longer presents that risk;

   (b) to withdraw the C-ITS station from the market;

   (c) to recall the C-ITS station.

   The market surveillance authorities shall prescribe a reasonable period, commensurate with the nature of the risk, in which the economic operator is to take the measures referred to in the first subparagraph.

2. The economic operator shall ensure that the corrective measure is taken throughout the Union in respect of all such C-ITS stations that it has made available on the Union market.

3. The market surveillance authorities shall immediately inform the Commission and the other Member States of the corrective measures they have ordered pursuant to paragraph 1 and of all available details, including:

   (a) the data necessary to identify the C-ITS station concerned;

   (b) the origin and the supply chain of the C-ITS station;

   (c) the nature of the risk;

   (d) the nature and duration of the corrective measures.

4. The Commission shall without delay enter into consultation with the Member States and the relevant economic operators and evaluate the corrective measures ordered by the market surveillance authorities. On the basis of the results of the evaluation, it shall decide whether or not the measure is justified and, where necessary, propose appropriate measures.

5. The Commission shall address its decision to all Member States and immediately communicate it to the relevant economic operator or operators.

Article 20

Formal non-compliance

1. Without prejudice to Article 17, a Member State shall require the relevant economic operator to put an end to the non-compliance where it makes one of the following findings:

   (a) the CE marking has been affixed in violation of Article 14 or 15;

   (b) the CE marking has not been affixed;

   (c) the EU declaration of conformity has not been drawn up;

   (d) the EU declaration of conformity has not been drawn up correctly;

   (e) technical documentation is either not available or not complete;

   (f) the information referred to in Article 5(6) or Article 7(3) is absent, false or incomplete;

   (g) any other administrative requirement provided for in Article 5 or Article 7 is not fulfilled.

2. Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit the making available of the C-ITS station on the market or ensure that it is recalled or withdrawn from the market.

CHAPTER IV

PUTTING IN SERVICE AND OPERATION OF C-ITS STATIONS

Article 21

Putting in service of central C-ITS stations

1. Before putting central C-ITS stations in service, the C-ITS station operator shall ensure that they have been designed and manufactured in accordance with the requirements set out in Article 5. To this end, it shall take either of the following actions:

   (a) buy a central C-ITS station that was placed on the market in accordance with Chapter III. In that case, paragraphs 2 and 3 of this Article shall not apply;

   (b) integrate the C-ITS station capabilities in a traffic control centre or central server. In that case, paragraphs 2 and 3 of this Article shall apply and Articles 7 to 20 shall not apply to the central C-ITS station.

2. C-ITS station operators shall draw up the required technical documentation referred to in Part C of Annex V and carry out the conformity assessment procedure referred to in Part C of Annex V. Where compliance of a central C-ITS station with the requirements set out in Article 5 has been demonstrated by that procedure, C-ITS station operators shall draw up an EU declaration of conformity in accordance with Part D of Annex V.

3. C-ITS station operators shall keep the technical documentation and the EU declaration of conformity as long as the central C-ITS station is in operation.

Article 22

Obligations of C-ITS station operators

1. C-ITS station operators shall ensure that all their C-ITS stations are put in service and operated in accordance with this Regulation.

2. Before putting a C-ITS station in service, the C-ITS station operator shall check that:

   (a) it bears the CE marking

   (b) the technical documentation referred to in Article 7 is available;

   (c) the C-ITS station is certified in accordance with the requirements in Section 1.6.2 of Annex IV.

   The obligations provided for in points (a) and (b) of the first subparagraph of this paragraph shall not apply to central C-ITS stations put in service in accordance with point (b) of Article 21(1).

   Furthermore, before a C-ITS station is put in service, the C-ITS station operator shall enrol it in the EU C-ITS security credential management system in accordance with Article 23(3).

3. Before putting a C-ITS station in service, the C-ITS station operator shall agree with the owner of the C-ITS station on the rights and obligations with regard to the operation, maintenance and updating of the C-ITS station, including on how to inform the end-user.

4. Where a C-ITS station is enrolled in the EU C-ITS security credential management system, it shall be registered in a C-ITS station register of its enrolment authority together with the identification of its operator. The C-ITS point of contact shall maintain a list of C-ITS station registers.

5. The C-ITS station operator shall ensure that, while the C-ITS station is in use, it continues to comply with the requirements of Article 5, as applicable at the time of its putting in service.

6. Where a C-ITS station is to be upgraded either at the initiative of its operator or as required by an amendment to this Regulation, the operator shall ensure that the C-ITS station complies with the latest version of the relevant specifications referred to in Article 5.

7. Where a C-ITS station is to be upgraded at the initiative of the manufacturer or its authorised representative, the manufacturer or its authorised representative and the C-ITS station operators shall cooperate with a view to ensuring that the C-ITS station complies with the latest version of the relevant specifications referred to in Article 5.

CHAPTER V

SECURITY

Article 23

Enrolment of C-ITS stations in the EU C-ITS security credential management system

1. The EU C-ITS security credential management system is set up for the provision of trusted and secure communication between C-ITS stations.

2. The functioning of the EU C-ITS security credential management system shall comply with the requirements in:

   (a) Annex III (certificate policy), which sets out the requirements for the management of public key certificates for C-ITS services by issuing entities, and their usage by end-entities;

   (b) Annex IV (security policy), which sets out the requirements for the management of information security in C-ITS.

3. All C-ITS stations shall be enrolled in, and comply with the rules of, the EU C-ITS security credential management system, in accordance with the specifications laid down in Annexes III and IV.

Article 24

C-ITS certificate policy authority

1. The C-ITS certificate policy authority shall be responsible for managing the certificate policy and the PKI authorisation in accordance with the certificate policy set out in Annex III.

2. The Commission shall act as the C-ITS certificate policy authority until a dedicated entity is established.

Article 25

Trust list manager

1. The trust list manager shall be responsible for generating and updating the European Certificate Trust List (‘ECTL') in accordance with the certificate policy set out in Annex III and for regular activity reporting to the C-ITS certificate policy authority as regards the overall secure operation of C-ITS trust model.

2. The Commission shall act as the trust list manager until a dedicated entity is established.

Article 26

C-ITS point of contact

1. The C-ITS point of contact shall be responsible for handling all communication with root certification authority managers and publishing the public key certificate of the trust list manager and the ECTL in accordance with the certificate policy set out in Annex III.

2. The Commission shall act as the C-ITS point of contact until a dedicated entity is established.

Article 27

Information security management system

Each C-ITS station operator shall operate an information security management system in accordance with ISO/IEC 27001 and the additional requirements in Section 1.3.1 of Annex IV.

Article 28

Compliance with the security policy

C-ITS station operators shall periodically request and obtain certification in accordance with the requirements in Section 1.7 of Annex IV.

CHAPTER VI

IMPLEMENTATION

Article 29

Implementation of the C-ITS network

1. The Commission shall have the following tasks in the implementation of the C-ITS network:

   (a) governance tasks:

   (1) preparing updates to the C-ITS governance framework;

   (2) supporting the development of common principles for the lawful processing of personal data by data controllers and processors in the C-ITS network;

   (3) acting as contact point on the implementation of the C-ITS network for C-ITS station operators and manufacturers, ITS users groups and third country stakeholders;

   (4) reviewing the following:

   (a) C-ITS assessment criteria to be used by testing laboratories and other assessment organisations during the compliance assessment process;

(b) C-ITS reference specifications, including basic and test standards to be used during the various steps of the assessment process.

(b) supervision tasks: to supervise the management of large-scale and high-severity security incidents that impact the entire C-ITS network (including disaster recovery situations where the cryptographic algorithm is compromised).

(c) the C-ITS certificate policy authority tasks:

(1) certificate policy management;

(2) PKI authorisation management.

2. In carrying out the tasks referred to in paragraph 1 the Commission shall be assisted by an expert group with representatives from public and private stakeholders, in particular C-ITS station manufacturers and operators in the C-ITS network.

CHAPTER VII

FINAL PROVISIONS

Article 30

Interim measures

In the event of an emergency situation jeopardising the proper functioning of the C-ITS network and having a severe direct impact on road safety, cyber security or the availability and integrity of C-ITS services, the Commission may adopt a decision introducing interim measures in order to remedy that situation. That decision shall be strictly limited to addressing the causes and consequences of that situation. It shall apply until this Regulation is amended to remedy that situation.

Article 31

Reporting

1. Member States shall monitor the implementation of this Regulation on their territory and report on the progress made in its implementation in the regular reporting referred to in Article 17(3) of Directive 2010/40/EU. In particular, the reporting shall cover:

(a) a description of the relevant public and public-private initiatives for C-ITS deployment, including their objective, timescale, milestones, resources, lead stakeholder(s) and status;

(b) the coverage of the road network by road type for each vehicle-to-infrastructure C-ITS priority service listed in Annex I;

(c) the number of roadside and central C-ITS stations deployed on their territory.

The Member States shall report for the first time by 27 August 2020.

2. Root certification authorities listed in the European certificate trust list specified in Annex III shall notify to the Commission by 31 December 2020 and by 31 December

every year thereafter the number of enrolled and operational mobile and fixed C-ITS stations under their authority.

Article 32

C-ITS stations placed on the market before 31 December 2019

1. C-ITS stations placed on the market at the latest 31 December 2019, which do not fully comply with the C-ITS security related requirements of this Regulation, and C-ITS stations of the same type/model placed on the market at the latest 30 June 2021, may be granted enrolment in the C-ITS trust model by the C-ITS certificate policy authority on a case by case basis, provided that the conditions set out in paragraph 2 are fulfilled. C-ITS stations of the same type/model used for the replacement of defective or broken C-ITS stations referred to in the first sentence, may also be granted enrolment under the same conditions.

2. The C-ITS certificate policy authority may enrol the C-ITS stations referred to in paragraph 1 in the C-ITS trust model under the following conditions:

   (a) the same level of security and trust as required by this Regulation is established;

   (b) it is demonstrated that the respective C-ITS stations, and the envisaged enrolment procedure, pose no additional risks to the C-ITS network.

3. The C-ITS certificate policy authority shall take its decision on the basis of the report of an accredited PKI auditor and a security vulnerability assessment conducted by a conformity assessment body.

Article 33

Review

1. By [OP: Insert the date: 3 years after the entry into force of this Regulation], the Commission shall review the implementation of this Regulation and, if appropriate, adopt new common specifications within the scope of this Regulation.

2. Where stakeholders intend to deploy a new or updated communication method or service, or other innovative solutions, including technologies for which prototypes are currently being tested, in the C-ITS network, they shall first submit to the Commission a file containing the technical specifications and information on degree of maturity and compatibility of the innovative solution with this Regulation. Those technical specifications shall be developed in line with the principles of openness, consensus and transparency as defined in Annex II to Regulation (EU) No 1025/2012.

   The Commission shall then analyse the file without undue delay and start discussing the file with the expert group referred to in Article 29(2) within 2 months, in view of a possible amendment of this Regulation. The group of experts shall assess the need for common specifications integrating the new solutions into the C-ITS network and provide an opinion, at the latest 6 months after receiving the file. Where appropriate, the Commission's Joint Research Centre shall support the relevant discussions with an independent technical assessment.

The submission of innovative solutions to the Commission and, where appropriate, the subsequent amendment of this Regulation may intervene at any time following the entry into force of this Regulation.

3. To maintain the continuity of the C-ITS priority services listed in Annex I, any future amendments shall ensure compatibility and interoperability with existing C-ITS stations put in service in accordance with this Regulation, or specify a suitable migration path.

Article 34

Entry into force

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 31 December 2019.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 13.3.2019

For the Commission
The President
Jean-Claude JUNCKER

EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 1

ANNEX

to the

Commission Delegated Regulation

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

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

ANNEX I

1. INTRODUCTION

This Annex contains the service profiles for the C-ITS priority services. A service profile is a specific configuration of standards, defining the implementation of various options of standards.

1.1. References

The following references are used in this Annex:

TS 102 894-2 ETSI TS 102 894-2, *Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary*, V1.3.1 (2018-08)

EN 302 637-2 ETSI EN 302 637-2, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, V1.4.0 (2018-08); this reference shall be read as the reference to version 1.4.1 from the date of the publication of that version.

EN 302 637-3 ETSI EN 302 637-3, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, v1.3.0 (2018-08); this reference shall be read as the reference to version 1.3.1 from the date of the publication of that version.

ECE 13 Regulation No 13 of the Economic Commission for Europe of the United Nations (UN/ECE), *Uniform provisions concerning the approval of vehicles of categories M, N and O with regard to braking* [2016/194]

ECE 13H Regulation No 13H of the Economic Commission for Europe of the United Nations (UN/ECE), *Uniform provisions concerning the approval of passenger cars with regard to braking* [2015/2364]

ECE 48 Regulation No 48 of the Economic Commission for Europe of the United Nations (UN/ECE), *Uniform provisions concerning the approval of vehicles with regard to the installation of lighting and light-signalling devices* [2016/1723]

ECE 121 Regulation No 121 of the Economic Commission for Europe of the United Nations (UN/ECE), *Uniform provisions concerning the approval of vehicles with regard to the location and identification of hand controls, tell-tales and indicators* [2016/18]

ISO/TS 19321	ISO/TS 19321, *Intelligent transport systems — Cooperative ITS — Dictionary of in-vehicle information (IVI) data structures* (15 April 2015)
ISO 639-1	*Codes for the representation of names of languages — Part 1: Alpha-2 code*
ISO/TS 14823	ISO/TS 14823:2017. *Intelligent transport systems – Graphic data dictionary*

1.2. Notations and abbreviations

The following notations and abbreviated terms are used in this Annex:

ABS	Anti-lock Braking System
ASR	Anti-Slip Regulation
AT	Authorization Ticket
CAM	Cooperative Awareness Message
C-ITS	Cooperative Intelligent Transport Systems
DCC	Decentralized Congestion Control
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
GNSS	Global Navigation Satellite System
I2V	infrastructure-to-vehicle
IRC	Impact Reduction Container
IVI	Infrastructure to Vehicle Information
MAP	Topology information for the intersection
SPAT	Signal Phase and Timing
SREM	Signal Request Extended Message
SSEM	Signal Request Status Extended Message
TC	Traffic Class
TMS	Traffic Management system
TOC	traffic operations centre
TRCO	Triggering condition
TTC	Time to Collision
V2V	vehicle-to-vehicle

1.3. Definitions

The following definitions are used in this Annex:

(a) ‘stationary vehicle’ means a vehicle with an absolute speed <= 8 centimetres per second. This state shall be determined by internal vehicle sensors;

(b) ‘emergency vehicle’ means a vehicle that is designated and authorised to respond to an emergency. Emergency vehicles are often permitted by law to break conventional road rules in order to reach their destinations in the fastest possible time, such as (but not limited to) driving through an intersection when the traffic lights are red or exceeding the speed limit.

2. LIST OF PRIORITY SERVICES

Service category	Service	Service profile
Vehicle-to-vehicle services		
Traffic jam	Dangerous end of queue	Section 3
Traffic jam	Traffic jam ahead	Section 4
Stationary vehicle warning	Stopped vehicle	Section 5
Stationary vehicle warning	Broken-down vehicle	Section 6
Stationary vehicle warning	Post-crash	Section 7
Special vehicle warning	Emergency vehicle in operation	Section 8
Special vehicle warning	Stationary safeguarding emergency vehicle	Section 9
Special vehicle warning	Stationary recovery service warning	Section 10
Exchange of IRCs	Request IRC	Section 11
Exchange of IRCs	Response IRC	Section 12
Dangerous situation	Electronic emergency brake light	Section 13
Dangerous situation	Automatic brake intervention	Section 14
Dangerous situation	Reversible occupant restraint system intervention	Section 15
Adverse weather conditions	Fog	Section 16
Adverse weather conditions	Precipitation	Section 17
Adverse weather conditions	Traction loss	Section 18
Infrastructure-to-vehicle services		
In-vehicle signage	Dynamic speed limit information	Section 19
In-vehicle signage	Embedded VMS ‘free text’	Section 20
In-vehicle signage	Other signage information	Section 21
Hazardous locations notification	Accident zone	Section 22
Hazardous locations notification	Traffic jam ahead	Section 23
Hazardous locations notification	Stationary vehicle	Section 24
Hazardous locations notification	Weather condition warning	Section 25
Hazardous locations notification	Temporarily slippery road	Section 26

Hazardous locations notification	Animal or person on the road	Section 27
Hazardous locations notification	Obstacle on the road	Section 28
Road works warning	Lane closure (and other restrictions)	Section 29
Road works warning	Road closure	Section 30
Road works warning	Road works — mobile	Section 31
Signalised intersections	Green light optimal speed advisory	Section 32
Signalised intersections	Public transport prioritisation	Section 33

3. TRAFFIC JAM — DANGEROUS END OF QUEUE

3.1. Description of cooperative intelligent transport systems (C-ITS) service

This C-ITS service transmits vehicle-to-vehicle (V2V) information on a situation where an ego vehicle detects the end of a traffic jam (‘dangerous end of queue’). Such a situation exists when the traffic lane of the ego vehicle is blocked and the vehicle cannot proceed in its lane. Urban environment is not considered in this service.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘dangerous situations — electronic emergency brake light’.

3.2. Triggering conditions

3.2.1. Preconditions

(1) The following preconditions shall be satisfied every time before this C-ITS service is triggered:

(a) the ego vehicle is located in a non-urban environment, as determined in at least one of the following ways:

- the velocity is greater than 80 km/h for a time block of at least 30 s in the 60 s prior to each detection and the absolute value of the steering wheel angle is less than 90 ° for a time block of at least 30 s in the 60 s prior to each detection (‘dangerous end of queue’ should not be detected in a non-motorway environment);
- an on-board camera sensor indicates non-urban environment;
- an on-board digital map indicates non-urban environment.

(2) The vehicle velocity and deceleration shall be determined by the vehicle bus signal, not by a Global Navigation Satellite System (GNSS). The filtered vehicle velocity (with respect to sensor noise) shall be used. This requirement shall be applied for all subsequent occurrences of vehicle velocity and deceleration analysis.

(3) The velocity and angle values shall be measured continuously. The conditions shall be satisfied throughout the measurement duration. The process shall start over again if the conditions are not satisfied within measurement duration.

3.2.2. Service-specific conditions

(4) If the preconditions in point (1) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the

generation of a Decentralised Environmental Notification Message (DENM) shall be triggered:

- TRCO_0 AND (TRCO _2 OR TRCO _3 OR TRCO _4 OR TRCO _5 OR TRCO _6)
- TRCO_1 AND TRCO_2.

Table 1: 'Traffic jam — dangerous end of queue' service-specific conditions

Count	Triggering condition (TRCO)	Status
TRCO_0	The ego vehicle is driving with an initial velocity exceeding 80 km/h and the initial deceleration is equal to or below 0.1 m/s². The driver reacts to the dangerous end of queue by reducing the velocity from initial to target velocity of 30 km/h or less. The duration between initial and target velocity shall be 10 s or less. An instant deceleration between initial and target velocity exceeding 3.5 m/s² is detected.	driver reaction
TRCO_1	Passengers of the ego vehicle react to the traffic jam by enabling hazard lights for at least 3 s	driver reaction
TRCO_2	At least three other vehicles with a velocity of at least 7 km/h have hazard lights enabled for at least 3 s, as indicated by: • an on-board camera sensor; or • CAMs.	environment or on-board sensors
TRCO_3	At least one DENM corresponding to the '*Traffic jam - Dangerous end of queue*' C-ITS service has been received.	environment
TRCO_4	At least five different DENMs (i.e. with different *actionIDs*) corresponding to the '*traffic jam - traffic jam ahead*' C-ITS service have been received from the downstream traffic.	environment
TRCO_5	At least one DENM corresponding to the *'Special vehicle warning - Static safeguarding emergency vehicle*' C-ITS service has been received, with *linkedCause* equal to *Traffic Condition* or *Dangerous End of Queue*.	environment
TRCO_6	On-board sensors of the ego vehicle recognise that the vehicle is facing a dangerous end of queue.	on-board sensors

(5) A new DENM shall not be requested within the *Detection Blocking Time*. The *Detection Blocking Time* is launched after the event is detected and a DENM to that effect has been requested. In this way, a single event is not able to flood the transmission channel. The *Detection Blocking Time* shall be 60 s no matter how the event is detected. The detection period between two detected events shall be at least equal to the *Detection Blocking Time*. The detection algorithm may run during *Detection Blocking Time*.

Note: No period for the braking manoeuvres is presented, because the initial ego vehicle velocity has no upper restriction.

(6) A condition shall be valid as long as it is active and for an extra period of 5 s (the period increases the determinism of the detection algorithm). The validity shall decrease from the moment the condition is no longer satisfied, thus facilitating the combination of triggering conditions.

(7) CAMs and DENMs from remote vehicles used for evaluating service-specific conditions as described above shall be relevant for the ego vehicle. The relevance shall be determined in one of these ways:

(a) a digital map indicates that the event and the ego vehicle are separated by a distance of less than 500 m and share the same driving direction;

(b) a path history match indicates that the event and the ego vehicle are separated by a distance of less than 500 m and share the same driving direction;

(c) the Euclidean distance between the event and the ego vehicle is less than 500 m and the absolute value of the heading difference is less than 10 °. The traffic jam reference positions according to the DENMs are located in an area spanning from -45 ° to +45 ° starting at the ego vehicle's longitudinal axis.

Note: When counting vehicles or events, Authorization Ticket (AT) change should be considered in such a way that no vehicle or event is counted multiple times.

3.2.3. Information quality

(8) The value of the data element *informationQuality* in the DENM depends on how the situation is detected. TRCOs (see point (4)) are divided into groups: driver reaction, vehicle dynamics, environment and on-board sensors. The *informationQuality* value shall be set according to the following table. The highest possible value shall be used.

Table 2: Information quality of 'traffic jam — dangerous end of queue'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
At least one TRCO from the driver reaction AND environment group is fulfilled.	1
At least one TRCO from the driver reaction AND on-board sensors group is fulfilled.	2
At least one TRCO from the driver reaction AND environment AND on-board sensors group is fulfilled.	3

3.3. Termination conditions

(9) A termination of the C-ITS service shall not be considered.

3.3.1. Cancellation

(10) A cancellation DENM shall not be used for this C-ITS service.

3.3.2. Negation

(11) A negation DENM shall not be used for this C-ITS service.

3.4. Update

(12) An update DENM shall not be used for this C-ITS service.

3.5. Repetition duration and repetition interval

(13) New DENMs shall be repeated for a *repetitionDuration* of 20 s with a *repetitionInterval* of 0.5 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the Decentralised Environmental Notification (DEN) basic service shall be set according to the above values.

Note: Where two DENMs with the same *causeCode* originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

3.6. Traffic class

(14) New DENMs shall be set to *traffic class* 1.

3.7. Message parameters

3.7.1. DENM

(15) The following table specifies the data elements of the DENM that shall be set.

Table 3: DENM data elements of 'traffic jam — dangerous end of queue'

Data Field	**Value**
Management container	
actionID	Identifier of a DENM. Shall be set according to [TS 102 894-2].
detectionTime	*TimestampIts*-Timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
referenceTime	*TimestampIts*-Timestamp at which a new DENM is generated. Shall be set in accordance with [TS 102 894-2].
termination	Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.
eventPosition	*ReferencePosition*. Shall be set in accordance with [TS 102 894-2].
relevanceDistance	lessThan1000 m(4)
relevanceTrafficDirection	upstreamTraffic(1)
validityDuration	20s (it is expected that vehicles will be facing a different traffic situation 20 s after detection)
stationType	The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Situation container	
informationQuality	See point (8)
causeCode	dangerousEndOfQueue(27)
subCauseCode	unavailable(0)

<table>
<tr><th colspan="4">Location container</th></tr>
<tr><td><i>eventSpeed</i></td><td colspan="3">Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>eventPositionHeading</i></td><td colspan="3">Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>traces</i></td><td colspan="3"><i>PathHistory</i> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td rowspan="10"><i>roadType</i></td><td colspan="3"><i>RoadType</i> of the road on which the detecting C-ITS station is situated.</td></tr>
<tr><td colspan="3">Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td><b>Urban / non-urban</b></td><td><b>Structural separation</b></td><td><b>Data element</b></td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><th colspan="4">Alacarte container</th></tr>
<tr><td rowspan="2"><i>lanePosition</i></td><td colspan="3">If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition.</td></tr>
<tr><td colspan="3">If the lanePosition is unknown, the data element shall be omitted.</td></tr>
</table>

3.7.2. Cooperative Awareness Message (CAM)

(16) CAM adaption shall not be used for this C-ITS service.

3.8. Network and transport layer

(17) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

3.9. Security layer

(18) If the triggering conditions are fulfilled as described in point (4), an AT change shall be blocked for new DENMs as long as the *validityDuration* has not expired. Corresponding new DENMs shall be sent with the same AT.

4. TRAFFIC JAM — TRAFFIC JAM AHEAD

4.1. Description of C-ITS service

This C-ITS service transmits V2V information on a situation where an ego vehicle detects a traffic jam. Such a situation exists if the ego vehicle is surrounded by stationary traffic or a heavy volume of traffic. This service does not apply to urban environments.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- 'stationary vehicle warning — stopped vehicle';
- 'stationary vehicle warning — broken-down vehicle';
- 'stationary vehicle warning — post-crash';
- 'special vehicle warning — stationary recovery service warning'.

4.2. Triggering conditions

4.2.1. Preconditions

(19) The following preconditions shall be satisfied before this C-ITS service is initialised:

(a) no 'stationary vehicle warning' service (see sections 4 to 6) is detected;

(b) no 'special vehicle warning' service (see sections 7 to 9) is detected;

(c) the ego vehicle is located in a non-urban environment. The location shall be determined in at least one of these ways:

(a) the velocity is greater than 80 km/h for a time block of at least 30 s in the 180 s prior to each detection and the absolute value of the steering wheel angle is less than 90 ° for a time block of at least 30 s in the 60 s prior to each detection (traffic jams should not be detected on motorways);

(b) an on-board camera sensor indicates non-urban environment;

(c) an on-board digital map indicates non-urban environment.

(20) The vehicle velocity shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle velocity (with respect to sensor noise) shall be used. This requirement shall be applied for all subsequent occurrences of vehicle velocity analysis.

(21) The velocity and angle values shall be measured continuously. The conditions shall be satisfied throughout the measurement duration. The process shall start over again if the conditions are not satisfied within measurement duration.

4.2.2. *Service-specific conditions*

(22) If the preconditions in point (19) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

- TRCO_0;
- TRCO _1 AND (TRCO _2 OR TRCO _3 OR TRCO _4 OR TRCO _5)

Table 4: 'Traffic jam — traffic jam ahead' service-specific conditions

Count	Triggering condition	Status
TRCO_0	The ego vehicle is moving with an average velocity of 30 km/h or less and more than 0 km/h (this threshold is introduced to avoid overlap and to distinguish TRCO_0 and TRCO_1). The average velocity shall be calculated over a period of 120 s (the duration condition excludes frequently changing traffic states from triggering). Note: This TRCO covers the scenario where the ego vehicle is surrounded by stop-and-go traffic.	vehicle dynamics
TRCO_1	The ego vehicle velocity is equal to 0 km/h for at least 30 s. Note: This TRCO covers a scenario in which the ego vehicle is stationary and surrounded by other road users.	vehicle dynamics
TRCO_2	At least one DENM corresponding to the '*traffic jam - traffic jam ahead*' C-ITS service with the same driving direction has been received.	environment
TRCO_3	At least one traffic jam notification with the same driving direction has been received by means of mobile radio.	environment
TRCO_4	CAMs indicate a velocity of 30 km/h or less of at least five other vehicles within 100 m and with the same driving direction.	environment
TRCO_5	On-board sensors indicate a velocity 30 km/h or less of at least five other vehicles within 100 m and with the same driving direction.	on-board sensor

(23) A new DENM shall not be requested in the *Detection Blocking Time*. The *Detection Blocking Time* is launched after the event is detected and a DENM to that effect has been requested. In this way, a single event is not able to flood the transmission channel. The *Detection Blocking Time* shall be 180 s no matter how the event is detected. The detection period between two detected events shall be at least equal to the *Detection Blocking Time*. The detection algorithm may run during *Detection Blocking Time*.

(24) A condition shall be valid as long as it is active and for an extra period of 5 s (the period increases the determinism of the detection algorithm). The validity decreases from the moment the condition is no longer satisfied, thus facilitating the combination of triggering conditions.

(25) CAMs and DENMs from remote vehicles used to evaluate service-specific conditions as described above shall be relevant for the ego vehicle. The relevance shall be determined in one of these ways:

(a) a digital map indicates that the event and the ego vehicle are separated by a distance of less than 500 m and share the same driving direction;

(b) a path history match indicates that the event and the ego vehicle are separated by a distance of less than 500 m and share the same driving direction;

(c) the Euclidean distance between the event and the ego vehicle is less than 500 m and the absolute value of the heading difference is less than 10 °. The traffic jam reference positions according to the DENMs are located in an area spanning from -45 ° to +45 ° starting at the ego vehicle's longitudinal axis.

Note: When counting vehicles or events, AT change should be considered in such a way that no vehicle or event is counted multiple times.

4.2.3. Information quality

(26) The value of the data element *informationQuality* in the DENM depends on how the situation is detected. TRCOs (see point (22)) are divided into groups: driver reaction, vehicle dynamics, environment and on-board sensors. The *informationQuality* value shall be set in accordance with the following table. The highest possible value shall be used.

Table 5: Information quality of 'traffic jam — traffic jam ahead'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Al least one condition from the vehicle dynamics group is fulfilled, i.e. condition TRCO_0 is fulfilled.	1
At least one condition from the vehicle dynamics AND environment group is fulfilled.	2
At least one condition from the vehicle dynamics AND on-board sensor group is fulfilled.	3
At least one condition from the vehicle dynamics AND environment group AND on-board sensor group is fulfilled.	4

4.3. Termination conditions

(27) A termination of the C-ITS service shall not be considered.

4.3.1. Cancellation

(28) A cancellation DENM shall not be used for this C-ITS service.

4.3.2. Negation

(29) A negation DENM shall not be used for this C-ITS service.

4.4. Update

(30) An update DENM shall not be used for this C-ITS service.

4.5. Repetition duration and repetition interval

(31) New DENMs shall be repeated for a *repetitionDuration* of 60 s with a *repetitionInterval* of 1 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the values above.

Note: Where two DENMs with the same *causeCode* originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

4.6. Traffic class

(32) New DENMs shall be set to *traffic class* 1.

4.7. Message parameters

4.7.1. DENM

(33) The following table specifies the data elements of the DENM that shall be set.

Table 6: DENM data elements of 'traffic jam — traffic jam ahead'

Data field	**Value**
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].
detectionTime	*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
referenceTime	*TimestampIts*-timestamp at which a new DENM is generated. Shall be set in accordance with [TS 102 894-2].
termination	Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.
eventPosition	*ReferencePosition*. Shall be set in accordance with [TS 102 894-2].
relevanceDistance	lessThan1000m(4)
relevanceTrafficDirection	upstreamTraffic(1)
validityDuration	60 s (a traffic jam situation is expected to last at least 60 s)
stationType	The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Situation container	
informationQuality	See point (26).
causeCode	trafficCondition(1)

<table>
<tr><td><i>subCauseCode</i></td><td colspan="3">unavailable(0)</td></tr>
<tr><td colspan="4"><b>Location container</b></td></tr>
<tr><td><i>eventSpeed</i></td><td colspan="3">Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>eventPositionHeading</i></td><td colspan="3">Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>traces</i></td><td colspan="3"><i>PathHistory</i> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td rowspan="10"><i>roadType</i></td><td colspan="3"><i>RoadType</i> of the road on which the detecting C-ITS station is situated.</td></tr>
<tr><td colspan="3">Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td><b>Urban / non-urban</b></td><td><b>Structural separation</b></td><td><b>Data element</b></td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="4"><b>Alacarte container</b></td></tr>
<tr><td rowspan="2"><i>lanePosition</i></td><td colspan="3">If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition.</td></tr>
<tr><td colspan="3">If the lanePosition is unknown, the data element shall be omitted.</td></tr>
</table>

4.7.2. ***CAM***

(34) CAM adaption shall not be used for this C-ITS service.

4.8. Network and transport layer

(35) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

4.9. Security layer

(36) If the triggering conditions are fulfilled as described in point (22), an AT change shall be blocked for new DENMs as long as the *validityDuration* has not expired. Corresponding new DENMs shall be sent with the same AT.

5. STATIONARY VEHICLE WARNING - STOPPED VEHICLE

5.1. Description of C-ITS service

This C-ITS service transmits V2V information on a situation where a vehicle has stopped, without particular information about the reason.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘special vehicle warning — stationary recovery service warning’;
- ‘stationary vehicle warning — broken-down vehicle’;
- ‘stationary vehicle warning — post-crash’.

(37) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as being met. Such a signal prompts the stack to generate a new, update or cancellation DENM. If the triggering conditions are not fulfilled, a DENM signal shall not be generated.

5.2. Triggering conditions

5.2.1. Preconditions

(38) The following preconditions shall be satisfied before this C-ITS service is triggered:

(a) no breakdown warning message that prevents the driver from continuing driving (e.g. red warning symbols, in accordance with [ECE 121]) is shown on the instrument cluster.

Note: This service is not required to check ignition terminal 15 status for triggering (can be on or off). Operation of the service is optional when ignition terminal 15 is off.

(39) Parallel activation with the other related C-ITS services shall be avoided. Where the ‘*broken-down vehicle*’ and/or ‘*post-crash*’ C-ITS services are triggered simultaneously, the C-ITS services shall be prioritised as follows:

(a) ‘post-crash’ (highest priority);

(b) ‘broken-down vehicle’;

(c) ‘stopped vehicle’ (lowest priority).

5.2.2. *Service-specific conditions*

(40) If the preconditions in point (38) and all of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) the ego vehicle has enabled hazard lights;

(b) the vehicle is stationary;

(c) the *Triggering Timer* has expired.

(41) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used. This requirement shall be applied for all subsequent occurrences of vehicle speed analysis.

(42) If the vehicle has enabled hazard lights and is stationary, the *Triggering Timer* shall be set to 30 s and started. The *Triggering Timer* shall be reduced if the following situations arise:

(a) the timer shall be reduced by 10 s if the automatic transmission (AUT) is set to ‘park’ for at least 3 s;

(b) the timer shall be reduced by 10 s if the gear box is set to idle for at least 3 s;

(c) the timer shall be reduced by 10 s if the parking brake is enabled for at least 3 s;

(d) the timer shall be reduced by 10 s if an arbitrary number of seatbelt buckles change from ‘connected’ to ‘disconnected’ for at least 3 s;

(e) the timer shall be set to 0 if an arbitrary number of doors are open for at least 3 s;

(f) the timer shall be set to 0 if the ignition terminal is switched from on to off for at least 3 s;

(g) the timer shall be set to 0 if the boot is open for at least 3 s;

(h) the timer shall be set to 0 if the bonnet is open for at least 3 s.

(43) All above-listed procedures for the timer reduction shall be applied only once during initial detection. If the *Triggering Timer* has been counted down to 0, no further reduction is necessary in the current detection cycle.

(44) During the runtime of the *Triggering Timer*, the hazard lights shall be enabled and the vehicle shall be stationary. Otherwise, the detection shall be cancelled.

5.2.3. *Information quality*

(45) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (42)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 7: Information quality of ‘stationary vehicle — stopped vehicle’

Event detection	**Value of InformationQuality**

No TRCO-compliant implementation	unknown(0)
None of the conditions a) — h) are fulfilled.	1
At least one condition of a) — d) is fulfilled.	2
At least one condition of e) — h) is fulfilled.	3

(46) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated. In the update phase, only the conditions that would lead to a timer reduction shall be evaluated, but not the timer itself.

5.3. Termination conditions

(47) This C-ITS service is terminated by a cancellation of the originating C-ITS station. At the termination of the C-ITS service, update DENM request shall be terminated.

5.3.1. Cancellation

(48) If at least one of the following conditions is satisfied before the period set in the data element *validityDuration* has expired, the generation of a cancellation DENM shall be triggered:

(a) the vehicle is no longer stationary for a duration of 5 s;

(b) the hazard lights are disabled;

(c) the position of the vehicle has changed more than 500 m (e.g. because the vehicle has been towed away).

Note: The cancellation condition does not imply that the C-ITS station needs to be permanently operational or extend its operation during that cancellation condition.

5.3.2. Negation

(49) A negation DENM shall not be used for this C-ITS service.

5.4. Update

(50) If the previously triggered DENM for a detected *Stopped Vehicle* was not cancelled, the generation of an update DENM shall be triggered every 15 s.

(51) In the update phase, only the triggering conditions shall be checked (further evaluation of timers shall not be executed).

(52) New values shall be assigned to data fields or elements in the DENM according to the changed event (e.g. *detectionTime* or *informationQuality*).

Note: The update condition does not imply that the C-ITS station needs to be permanently operational or extend its operation during that update condition.

5.5. Repetition duration and repetition interval

(53) DENMs that are new, have been updated or have been cancelled shall be repeated for a *repetitionDuration* of 15 s with a *repetitionInterval* of 1 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval*

between the application and the DEN basic service shall be set in accordance with the above values.

Note: The *validityDuration* is set to 30 s. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: Where two DENMs with the same *causeCode* originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

5.6. Traffic class

(54) New, update and cancellation DENMs shall be set to *traffic class* 1.

5.7. Message parameters

5.7.1. DENM

(55) The following table specifies the data elements of the DENM that shall be set.

Table 8: DENM data elements of 'stationary vehicle warning — stopped vehicle'

<table>
<tr><th>Data field</th><th>Value</th></tr>
<tr><th colspan="2">Management container</th></tr>
<tr><td><i>actionID</i></td><td>Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>detectionTime</i></td><td><i>TimestampIts</i>-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].

Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>referenceTime</i></td><td><i>TimestampIts</i>-timestamp at which a new, update or cancellation DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>termination</i></td><td>Shall not be set in the case of new or update DENM. Shall be set to isCancellation(0) in the case of a cancellation DENM.</td></tr>
<tr><td><i>eventPosition</i></td><td><i>ReferencePosition</i>. Shall be set in accordance with [TS 102 894-2].

Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>relevanceDistance</i></td><td>lessThan1000m(4)</td></tr>
<tr><td><i>relevanceTrafficDirection</i></td><td>If the roadType is known, the value shall be set as follows:
<table>
<tr><th>RoadType</th><th>Direction</th></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
</table>
Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td><i>validityDuration</i></td><td>30 s</td></tr>
</table>

<table>
<tr><td><i>stationType</i></td><td>The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td colspan="2"><b>Situation container</b></td></tr>
<tr><td><i>informationQuality</i></td><td>See point (45). Shall be refreshed for every update DENM.</td></tr>
<tr><td><i>causeCode</i></td><td>stationaryVehicle(94)</td></tr>
<tr><td><i>subCauseCode</i></td><td>unavailable(0)</td></tr>
<tr><td colspan="2"><b>Location container</b></td></tr>
<tr><td><i>eventSpeed</i></td><td>Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>eventPositionHeading</i></td><td>Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>traces</i></td><td><i>PathHistory</i> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>roadType</i></td><td><i>RoadType</i> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.
Shall be set in accordance with [TS 102 894-2] in combination with the following rules:
<table>
<tr><th>Urban / non-urban</th><th>Structural separation</th><th>Data element</th></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
</table>
If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="2"><b>Alacarte container</b></td></tr>
</table>

lanePosition	If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition. If the lanePosition is unknown, the data element shall be omitted. Shall be refreshed for an update DENM.
Alacarte container: StationaryVehicleContainer	
stationarySince	Shall be set in accordance with the duration in minutes of the detecting C-ITS station being stationary. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM.

5.7.2. CAM

(56) CAM adaption shall not be used for this C-ITS service.

5.8. Network and transport layer

(57) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

5.9. Security layer

(58) If the triggering conditions as described in point (40) apply, an AT change shall be blocked for new, update and cancellation DENMs as long as the *validityDuration* has not expired. Corresponding new, update and cancellation DENMs shall be sent with the same AT.

6. STATIONARY VEHICLE WARNING — BROKEN-DOWN VEHICLE

6.1. Description of C-ITS service

This C-ITS service transmits V2V information on a broken-down vehicle. Though various reasons could cause a vehicle breakdown, such as bursting tires, lack of fuel or engine failure, this section focuses on reasons indicated by breakdown warning messages in the instrument cluster.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘special vehicle warning — stationary recovery service warning’;
- ‘stationary vehicle warning — stopped vehicle’;
- ‘stationary vehicle warning — post-crash’.

(59) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as valid. Such a signal prompts the stack to generate a new, update or cancellation DENM. If the triggering conditions are not fulfilled, a DENM signal shall not be generated.

6.2. Triggering conditions

6.2.1. Preconditions

(60) The following precondition shall be satisfied before this C-ITS service is triggered:

(a) a breakdown warning message that prevents the driver from continuing driving (e.g. red warning symbols, in accordance with [ECE 121]) is shown on the instrument cluster.

Note: This service is not required to check ignition terminal 15 status for triggering (can be on or off). Operation of the service is optional when ignition terminal 15 is off.

(61) Parallel activation with the other related C-ITS services shall be avoided. Where the '*stopped vehicle*' and/or '*post-crash*' C-ITS services are triggered simultaneously, the C-ITS services shall be prioritised as follows:

(a) 'post-crash' (highest priority);

(b) 'broken-down vehicle';

(c) 'stopped vehicle' (lowest priority).

6.2.2. Service-specific conditions

(62) If the precondition in point (60) and all of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) the ego vehicle has enabled hazard lights;

(b) the vehicle is stationary;

(c) the *Triggering Timer* has expired.

(63) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used. This requirement shall be applied for all subsequent occurrences of vehicle speed analysis.

(64) If the vehicle has enabled hazard lights and is stationary, the *Triggering Timer* shall be set to 30 s and started. The *Triggering Timer* shall be reduced if the following situations arise:

(a) the timer shall be reduced by 10 s if the automatic transmission (AUT) is set to 'park' for at least 3 s;

(b) the timer shall be reduced by 10 s if the gear box is set to idle for at least 3 s;

(c) the timer shall be reduced by 10 s if the parking brake is enabled for at least 3 s;

(d) the timer shall be reduced by 10 s if an arbitrary number of the seatbelt buckles change from 'connected' to 'disconnected' for at least 3 s;

(e) the timer shall be set to 0 if an arbitrary number of doors are open for at least 3 s;

(f) the timer shall be set to 0 if the ignition terminal is switched from on to off for at least 3 s;

(g) the timer shall be set to 0 if the boot is open for at least 3 s;

(h) the timer shall be set to 0 if the bonnet is open for at least 3 s.

(65) All above-listed procedures for the timer reduction shall be applied only once during initial detection. If the *Triggering Timer* has been counted down to 0, no further reduction is necessary in the current detection cycle.

(66) During the runtime of the *Triggering Timer*, the hazard lights shall be enabled and the vehicle shall be stationary all the time. Otherwise, the detection shall be cancelled.

6.2.3. Information quality

(67) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (64)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 9: Information quality of 'stationary vehicle — broken-down vehicle'

Event detection	Value of informationQuality
No TRCO-compliant implementation	unknown(0)
None of conditions a) — h) are fulfilled.	1
At least one condition of a) — d) is fulfilled.	2
At least one condition of e) — h) is fulfilled.	3

(68) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated. In the update phase, only the conditions that would lead to a timer reduction shall be evaluated, but not the timer itself.

6.3. Termination conditions

(69) This C-ITS service is terminated by a cancellation of the originating C-ITS station. At the termination of the C-ITS service, update DENM request shall be terminated.

6.3.1. Cancellation

(70) If at least one of the following conditions is satisfied before the period set in the data element *validityDuration* has expired, the generation of a cancellation DENM shall be triggered:

(a) the vehicle is no longer stationary for a duration of 5 s;

(b) the hazard lights are disabled;

(c) the position of the vehicle has changed more than 500 m (e.g. because the vehicle has been towed away).

Note: The cancellation condition does not imply that the C-ITS station needs to be permanently operational or extend its operation during that cancellation condition.

6.3.2. Negation

(71) A negation DENM shall not be used for this C-ITS service.

6.4. Update

(72) If the previously triggered DENM for a detected *Broken-down Vehicle* was not cancelled, the generation of an update DENM shall be triggered every 15 s.

(73) In the update phase, only the triggering conditions shall be checked (timers shall not be evaluated further).

(74) If the ignition terminal 15 is switched from on to off, an update DENM shall be triggered immediately.

(75) New values shall be assigned to data fields or elements in the DENM according to the changed event (e.g. *detectionTime* or *informationQuality*).

Note: The update condition does not imply that the C-ITS station needs to be permanently operational or extend its operation during that update condition.

6.5. Repetition duration and repetition interval

(76) DENMs that are new, have been updated or have been cancelled shall be repeated for a *repetitionDuration* of 15 s with a *repetitionInterval* of 1 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the above values.

(77) In the case of an enabled ignition terminal 15, the *validityDuration* shall be set to 30 s. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: The *validityDuration* is set to a higher value in the case of a disabled ignition terminal 15 than in the case of an enabled ignition terminal 15. This is due to the fact that update DENM cannot be triggered and can no longer be sent. Therefore, the last DENM shall be kept alive longer.

Note: Where two DENMs with the same causeCode originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

6.6. Traffic class

(78) New, update and cancellation DENMs shall be set to *traffic class* 1.

6.7. Message parameters

*6.7.1. **DENM***

(79) The following table specifies the data elements of the DENM that shall be set.

Table 10: DENM data elements of 'stationary vehicle warning — broken-down vehicle'

Data field	**Value**
Management container	

<table>
<tr><td><em>actionID</em></td><td>Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><em>detectionTime</em></td><td><em>TimestampIts</em>-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].

Shall be refreshed for an update DENM.</td></tr>
<tr><td><em>referenceTime</em></td><td><em>TimestampIts</em>-timestamp at which a new, update or cancellation DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><em>termination</em></td><td>Shall not be set in the case of a new or update DENM. Shall be set to isCancellation(0) in the case of a cancellation DENM.</td></tr>
<tr><td><em>eventPosition</em></td><td><em>ReferencePosition</em>. Shall be set in accordance with [TS 102 894-2].

Shall be refreshed for an update DENM.</td></tr>
<tr><td><em>relevanceDistance</em></td><td>lessThan1000m(4)</td></tr>
<tr><td><em>relevanceTrafficDirection</em></td><td>If the roadType is known, the value shall be set as follows:
<table>
<tr><th>RoadType</th><th>Direction</th></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
</table>
Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td><em>validityDuration</em></td><td>• Ignition terminal 15 enabled: 30 s
• Ignition terminal 15 disabled: 900 s</td></tr>
<tr><td><em>stationType</em></td><td>The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td colspan="2"><strong>Situation container</strong></td></tr>
<tr><td><em>informationQuality</em></td><td>See point (67). Shall be refreshed for every update DENM.</td></tr>
<tr><td><em>causeCode</em></td><td>stationaryVehicle(94)</td></tr>
<tr><td><em>subCauseCode</em></td><td>vehicleBreakdown(2)</td></tr>
<tr><td colspan="2"><strong>Location container</strong></td></tr>
<tr><td><em>eventSpeed</em></td><td>Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].

Shall be refreshed for an update DENM.</td></tr>
<tr><td><em>eventPositionHeading</em></td><td>Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
</table>

<table>
<tr><td></td><td colspan="3">Shall be refreshed for an update DENM.</td></tr>
<tr><td><em>traces</em></td><td colspan="3"><em>PathHistory</em> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td rowspan="9"><em>roadType</em></td><td colspan="3"><em>RoadType</em> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.
Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td><strong>Urban / non-urban</strong></td><td><strong>Structural separation</strong></td><td><strong>Data element</strong></td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="4"><strong>Alacarte container</strong></td></tr>
<tr><td><em>lanePosition</em></td><td colspan="3">If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition.
If the lanePosition is unknown, the data element shall be omitted.
Shall be refreshed for an update DENM.</td></tr>
<tr><td colspan="4"><strong>Alacarte container: StationaryVehicleContainer</strong></td></tr>
<tr><td>stationarySince</td><td colspan="3">Shall be set according to the duration in minutes of the detecting C-ITS station being stationary. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
</table>

6.7.2. ***CAM***

(80) CAM adaption shall not be used for this C-ITS service.

6.8. Network and transport layer

(81) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

6.9. Security layer

(82) If the triggering conditions as described in point (62) apply, an AT change shall be blocked for new, update and cancellation DENMs as long as the *validityDuration* has not expired. Corresponding new, update and cancellation DENMs shall be sent with the same AT.

7. STATIONARY VEHICLE WARNING — POST-CRASH

7.1. Description of C-ITS service

This C-ITS service transmits V2V information on a vehicle that is stationary as the result of a traffic accident.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘stationary vehicle warning — stopped vehicle’;
- ‘stationary vehicle warning — broken-down vehicle’.

(83) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as valid. Such a signal prompts the stack to generate a new, update or cancellation DENM. If the triggering conditions are not fulfilled, a DENM signal shall not be generated.

7.2. Triggering conditions

7.2.1. Preconditions

(84) No specific preconditions apply for this C-ITS service.

(85) Parallel activation with the other related C-ITS services shall be avoided. Where the C-ITS services ‘*stopped vehicle*’ and/or ‘*broken-down vehicle*’ are triggered simultaneously, the C-ITS services shall be prioritised as follows:

(a) ‘post-crash’ (highest priority);

(b) ‘broken-down vehicle’;

(c) ‘stopped vehicle’ (lowest priority).

7.2.2. Service-specific conditions

(86) If the preconditions in point (84) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) an eCall has been triggered manually by an occupant of the vehicle by the eCall button and the vehicle becomes stationary within 15 s. If the vehicle is already stationary, the condition is fulfilled immediately;

(b) a low-severity crash is detected without the activation of an irreversible occupant restraint system (e.g. high-voltage battery cut-off, door unlock) and the vehicle becomes stationary within 15 s. If the vehicle is already stationary, the condition is fulfilled immediately;

(c) a pedestrian collision is detected with the activation of at least one irreversible pedestrian-protection system (e.g. pop-up bonnet, outside airbag) and the vehicle becomes stationary within 15 s. If the vehicle is already stationary, the condition is fulfilled immediately;

(d) a high-severity crash is detected with the activation of at least one irreversible occupant-restraint system (e.g. pyrotechnic belt-tightener, airbag).

(87) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used. This requirement shall be applied for all subsequent occurrences of vehicle speed analysis.

Note: The conditions need to be checked only if the necessary power supply is present. This means that crash-secure implementation of the system is not required.

7.2.3. Information Quality

(88) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (86)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 11: Information quality of 'stationary vehicle — post-crash'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Condition (a) is fulfilled.	1
Condition (b) or (c) is fulfilled.	2
Condition (d) is fulfilled.	3

(89) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

7.3. Termination conditions

(90) This C-ITS service is terminated by a cancellation of the originating C-ITS station. At the termination of the C-ITS service, update DENM request shall be terminated.

7.3.1. Cancellation

(91) Once at least one of the following conditions is satisfied before the period set in the data element *validityDuration* has expired, the generation of a cancellation DENM shall be triggered:

(a) the ego vehicle is not stationary for a duration of 15 s;

(b) the position of the vehicle has changed more than 500 m (e.g. because the vehicle has been towed away).

Note: The cancellation condition does not imply that the C-ITS station needs to be permanently operational or extend its operation during that cancellation condition.

7.3.2. Negation

(92) A negation DENM shall not be used for this C-ITS service.

7.4. Update

(93) An update DENM shall be triggered every 60 s if the C-ITS service has not been cancelled.

(94) If the ignition terminal 15 is switched from on to off, an update DENM shall be triggered immediately.

(95) New values shall be assigned to data fields or elements in the DENM according to the changed event (e.g. *detectionTime* or *informationQuality*).

Note: The update condition does not imply that the C-ITS station needs to be permanently operational or extend its operation during that update condition.

7.5. Repetition duration and repetition interval

(96) DENMs that are new, have been updated or have been cancelled shall be repeated for a *repetitionDuration* of 60 s with a *repetitionInterval* of 1 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the above values.

(97) In the case of an enabled ignition terminal 15, the *validityDuration* shall be set to 180 s. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: The *validityDuration* is set to a higher value in the case of a disabled ignition terminal 15 than in the case of an enabled ignition terminal 15. This is due to the fact that update DENM cannot be triggered and can no longer be sent. Therefore, the last DENM shall be kept alive longer.

Note: Where two DENMs with the same *causeCode* originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

7.6. Traffic class

(98) New, update and cancellation DENMs shall be set to *traffic class* 1.

7.7. Message parameters

7.7.1. DENM

(99) The following table specifies the data elements of the DENM that shall be set.

Table 12: DENM data elements of 'Stationary Vehicle Warning — Post-Crash'

Data field	Value
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].

<table>
<tr><td><i>detectionTime</i></td><td><i>TimestampIts</i>-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>referenceTime</i></td><td><i>TimestampIts</i>-timestamp at which a new, update or cancellation DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>termination</i></td><td>Shall not be set in the case of new or update DENM. Shall be set to isCancellation(0) in the case of a cancellation DENM.</td></tr>
<tr><td><i>eventPosition</i></td><td><i>ReferencePosition</i>. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>relevanceDistance</i></td><td>lessThan5km(5)</td></tr>
<tr><td><i>relevanceTrafficDirection</i></td><td>If the roadType is known, the value shall be set as follows:
<table>
<tr><th>RoadType</th><th>Direction</th></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
</table>
Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td><i>validityDuration</i></td><td>• Ignition terminal 15 enabled: 180 s
• Ignition terminal 15 disabled: 1 800 s</td></tr>
<tr><td><i>stationType</i></td><td>The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td colspan="2"><b>Situation container</b></td></tr>
<tr><td><i>informationQuality</i></td><td>See point (88). Shall be refreshed for every update DENM.</td></tr>
<tr><td><i>causeCode</i></td><td>stationaryVehicle(94)</td></tr>
<tr><td><i>subCauseCode</i></td><td>postCrash(3)</td></tr>
<tr><td colspan="2"><b>Location container</b></td></tr>
<tr><td><i>eventSpeed</i></td><td>Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>eventPositionHeading</i></td><td>Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
</table>

<table>
<tr><td>*traces*</td><td colspan="3">*PathHistory* of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td rowspan="9">*roadType*</td><td colspan="3">*RoadType* of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.
Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td>**Urban / non-urban**</td><td>**Structural separation**</td><td>**Data element**</td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="4">**Alacarte container**</td></tr>
<tr><td>*lanePosition*</td><td colspan="3">If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition.
If the lanePosition is unknown, the data element shall be omitted.
Shall be refreshed for an update DENM.</td></tr>
<tr><td colspan="4">**Alacarte container: StationaryVehicleContainer**</td></tr>
<tr><td>stationarySince</td><td colspan="3">Shall be set according to the duration in minutes of the detecting C-ITS station being stationary. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
</table>

7.7.2. CAM

(100) CAM adaption shall not be used for this C-ITS service.

7.8. Network and transport layer

(101) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

7.9. Security layer

(102) If the triggering conditions as described in point (86) apply, an AT change shall be blocked for new, update and cancellation DENMs as long as the *validityDuration* has not expired. Corresponding new, update and cancellation DENMs shall be sent with the same AT.

8. SPECIAL VEHICLE WARNING — EMERGENCY VEHICLE IN OPERATION

8.1. Description of C-ITS service

This C-ITS service transmits V2V information on an emergency vehicle moving to an operation scene, which is signalled by the use of the light bar.

(103) As soon as the C-ITS service is triggered, a DENM shall be transmitted by the emergency vehicle C-ITS station and parts of CAM data fields shall be set in accordance with section 8.7.2.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘special vehicle warning — stationary safeguarding emergency vehicle’;
- ‘special vehicle warning — stationary recovery service warning’.

(104) The default C-ITS service for an emergency vehicle C-ITS station is ‘*emergency vehicle in operation*’. A change to the ‘*stationary safeguarding emergency vehicle*’ C-ITS service shall be triggered only under the conditions set out in section9.

8.2. Triggering conditions

8.2.1. Preconditions

(105) The following preconditions shall be satisfied before this C-ITS service is triggered:

(a) the *stationType* is confirmed to be a special vehicle (*stationType* of CAM is set to *specialVehicles*(10)). The C-ITS service is restricted to emergency vehicles;

(b) the triggering conditions regarding ‘stationary safeguarding emergency vehicle’ shall not be satisfied (see section 9.2).

8.2.2. Service-specific conditions

(106) If the preconditions in point (105) and the following condition are satisfied, the generation of a DENM shall be triggered:

(a) the light bar is in use.

(107) The level of information quality can be improved by the following conditions:

(b) the siren is in use;

(c) the vehicle is not stationary.

(108) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used.

8.2.3. Information quality

(109) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see points (106) and (107)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 13: Information quality of 'emergency vehicle in operation'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Condition a) is fulfilled	1
Conditions a) and b) are fulfilled	2
Conditions a) and c) are fulfilled	3
Conditions a), b), and c) are fulfilled	4

(110) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

8.3. Termination conditions

(111) The C-ITS service shall be terminated when the light bar is no longer in use. At the termination of the C-ITS service, updating of DENMs shall be terminated. The *vehicleRole* shall be set to *default(0)* if the light bar is no longer in use.

8.3.1. Cancellation

(112) A cancellation DENM shall not be used for this C-ITS service.

8.3.2. Negation

(113) A negation DENM shall not be used for this C-ITS service.

8.4. Update

(114) The generated DENM shall be updated every 250 ms if the triggering conditions are still satisfied. The data fields that are assigned new values are defined in Table 14 below.

8.5. Repetition duration and repetition interval

(115) A repetition of the DENM shall not be used for this C-ITS service.

8.6. Traffic class

(116) New, update and cancellation DENMs shall be set to *traffic class* 1.

8.7. Message parameters

8.7.1. DENM

(117) The following table specifies the data elements of the DENM that shall be set.

Table 14: DENM data elements of ‘emergency vehicle in operation’

<table>
<tr><th>Data field</th><th>Value</th></tr>
<tr><td colspan="2"><b>Management container</b></td></tr>
<tr><td><i>actionID</i></td><td>Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>detectionTime</i></td><td><i>TimestampIts</i>-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>referenceTime</i></td><td><i>TimestampIts</i>-timestamp at which a new DENM or an update DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>termination</i></td><td>Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.</td></tr>
<tr><td><i>eventPosition</i></td><td><i>ReferencePosition</i>. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>relevanceDistance</i></td><td>lessThan1000m(4)</td></tr>
<tr><td><i>relevanceTrafficDirection</i></td><td>If the roadType is known, the value shall be set as follows:
<table>
<tr><th>RoadType</th><th>Direction</th></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
</table>
Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td><i>validityDuration</i></td><td>2 s</td></tr>
<tr><td><i>stationType</i></td><td>specialVehicles(10)</td></tr>
<tr><td colspan="2"><b>Situation container</b></td></tr>
<tr><td><i>informationQuality</i></td><td>See point (109). Shall be refreshed for every update DENM.</td></tr>
<tr><td><i>causeCode</i></td><td>emergencyVehicleApproaching(95)</td></tr>
<tr><td><i>subCauseCode</i></td><td>emergencyVehicleApproaching(1)</td></tr>
<tr><td colspan="2"><b>Location container</b></td></tr>
<tr><td><i>eventSpeed</i></td><td>Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
</table>

<table>
<tr><td><i>eventPositionHeading</i></td><td>Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>traces</i></td><td><i>PathHistory</i> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>roadType</i></td><td><i>RoadType</i> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.
Shall be set in accordance with [TS 102 894-2] in combination with the following rules:
<table>
<tr><th>Urban / non-urban</th><th>Structural separation</th><th>Data element</th></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
</table>
If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="2"><b>Alacarte container</b></td></tr>
<tr><td><i>lanePosition</i></td><td>If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition.
If the lanePosition is unknown, the data element shall be omitted.
Shall be refreshed for an update DENM.</td></tr>
<tr><td colspan="2"><b>Alacarte container: StationaryVehicleContainer</b></td></tr>
<tr><td><i>stationarySince</i></td><td>Shall be set according to the duration in minutes of the detecting C-ITS station being stationary. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
</table>

8.7.2. ***CAM***

(118) The *vehicleRole* shall be initialised at a 'default' setting (*vehicleRole* of CAM set to *default(0)*). If at least one of the triggering conditions in point (106) is satisfied, the *vehicleRole* shall be set to *emergency(6).*

(119) The following table specifies the data elements of the CAM that shall be set if the C-ITS service is triggered.

Table 15: CAM data elements of 'emergency vehicle in operation'

Data field	**Value**
CoopAwareness	
generationDeltaTime	Time corresponding to the time of the reference position in the CAM, considered as time of CAM generation. Shall be set in accordance with [EN 302 637-2].
BasicContainer	
stationType	specialVehicles(10)
referencePosition	Position and position accuracy measured at the reference point of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
HighFrequencyContainer shall be set to BasicVehicleContainerHighFrequency	
heading	Heading direction of the originating C-ITS station in relation to true north. Shall be set in accordance with [TS 102 894-2].
speed	Driving speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
driveDirection	Vehicle drive direction (forward or backward) of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
vehicleLength	Length of vehicle. Shall be set in accordance with [TS 102 894-2].
vehicleWidth	Width of vehicle. Shall be set in accordance with [TS 102 894-2].
longitudinalAcceleration	Vehicle longitudinal acceleration of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
curvature	Curvature of the vehicle trajectory and the accuracy. Shall be set in accordance with [TS 102 894-2].

curvatureCalcMode	Describes whether the yaw rate is used to calculate the curvature for a reported curvature value. Shall be set in accordance with [TS 102 894-2].
yawRate	Yaw rate of vehicle at a point in time. Shall be set in accordance with [TS 102 894-2].
LowFrequencyContainer shall be set to BasicVehicleContainerLowFrequency	
vehicleRole	emergency(6)
exteriorLights	Describes the status of the exterior light switches of a vehicle. Shall be set in accordance with [TS 102 894-2].
pathHistory	Represents the vehicle's movement over a recent period and/or distance. Shall be set in accordance with [TS 102 894-2].
SpecialVehicleContainer shall be set to EmergencyContainer	
lightBarSirenInUse	lightBarActivated bit shall be set to 1(onChange), if the usage of the light bar is detected; otherwise, it shall be set to 0. sirenActivated bit shall be set to 1, if usage of the siren is detected; otherwise, it shall be set to 0.
emergencyPriority	Is not required
causeCode	As specified in point (117)
subCauseCode	As specified in point (117)

8.8. Network and transport layer

(120) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

8.9. Security layer

(121) If the triggering conditions as described in point (106) apply, an AT change shall be blocked for new and update DENMs as long as the *validityDuration* has not expired. Corresponding new and update DENMs shall be sent with the same AT.

9. SPECIAL VEHICLE WARNING — STATIONARY SAFEGUARDING EMERGENCY VEHICLE

9.1. Description of C-ITS service

This C-ITS service transmits V2V information on a stationary emergency vehicle safeguarding a hazard area.

(122) As soon as the C-ITS service is triggered, a DENM shall be transmitted by the emergency vehicle C-ITS station and parts of CAM data fields shall be set in accordance with section 9.7.2.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘special vehicle warning — emergency vehicle in operation’;
- ‘special vehicle warning — stationary recovery service warning’.

9.2. Triggering conditions

9.2.1. Preconditions

(123) The following preconditions shall be satisfied before this C-ITS service is triggered:

- the *stationType* is confirmed to be an emergency vehicle (*stationType* of CAM is set to *specialVehicles*(10)). The C-ITS service is restricted to emergency vehicles;
- the *Standstill Timer* shall be initialised with zero.

(124) The default C-ITS service for an emergency vehicle C-ITS station is ‘*emergency vehicle in operation*’. A change to the C-ITS service ‘*stationary safeguarding emergency vehicle*’ shall be triggered only under the conditions defined in section 9.2.2.

9.2.2. Service-specific conditions

(125) If the vehicle is stationary and the light bar is in use, a *Standstill Timer* shall be initialised with zero and started. If the light bar is no longer in use or the vehicle is no longer stationary, the *Standstill Timer* shall be stopped and reset to zero.

(126) If the preconditions in point (123) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) the light bar is in use and engine relay is activated;

(b) the light bar is in use, the hazard lights are activated and the parking brake is activated or (in the case of automatic transmission) ‘park’ is selected;

(c) the light bar is in use, the hazard lights are activated and the *Standstill Timer* is 60 s or more.

(127) The level of information quality can be improved by the following conditions:

(d) the status of at least one door, or the boot, is ‘open’;

(e) the driver’s seat is detected, by one of the following techniques, as being ‘not occupied’:

(1) passenger compartment camera;

(2) state-of-the-art technique for seat occupation used in seatbelt reminder.

(128) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used. This requirement shall be applied for all subsequent occurrences of vehicle speed analysis.

(129) If the C-ITS service is triggered due to fulfilment of condition (a) or (b) in point (126), the *Standstill Timer* shall be stopped and set to 60 s. In the update phase, only the conditions shall be checked, but no timer shall be started.

9.2.3. Information quality

(130) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see points (126) and (127)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 16: Information quality of 'stationary safeguarding emergency vehicle'

Event detection	**Value of InformationQuality**
No TRCO-compliant implementation	unknown(0)
Condition (c) fulfilled	1
Condition (b) fulfilled	2
At least one of conditions (b) or (c) fulfilled and condition (d) fulfilled	3
At least one of conditions (b) or (c) fulfilled and condition (e) fulfilled	4
Condition (a) fulfilled	5

(131) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

9.3. Termination conditions

(132) This C-ITS service is terminated by a cancellation of the originating C-ITS station. At the termination of the C-ITS service, update DENM request shall be terminated.

9.3.1. Cancellation

(133) If the following condition is satisfied before the period set in the data element *validityDuration* has expired, the generation of a cancellation DENM shall be triggered:

(a) all the C-ITS service-specific conditions (a) to (c) in section 9.2.2 are no longer satisfied.

The *vehicleRole* shall be set to default(0) if the light bar is no longer in use.

9.3.2. Negation

(134) A negation DENM shall not be used for this C-ITS service.

9.4. Update

(135) The generated DENM shall be updated every 60 s if the triggering conditions are still satisfied. All data fields that are assigned new values are defined in Table 17 below.

9.5. Repetition duration and repetition interval

(136) DENMs that are new, have been updated or have been cancelled shall be repeated for a *repetitionDuration* of 60 s with a *repetitionInterval* of 1 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the above values.

Note: The *validityDuration* is set to 180 s. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: Where two DENMs with the same causeCode originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

9.6. Traffic class

(137) New, update and cancellation DENMs shall be set to *traffic class* 1.

9.7. Message parameters

9.7.1. DENM

(138) The following table specifies the data elements of the DENM that shall be set.

Table 17: DENM data elements of 'stationary safeguarding emergency vehicle'

<table>
<tr><th>Data field</th><th>Value</th></tr>
<tr><td colspan="2"><b>Management container</b></td></tr>
<tr><td><i>actionID</i></td><td>Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>detectionTime</i></td><td><i>TimestampIts</i>-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>referenceTime</i></td><td><i>TimestampIts</i>-timestamp at which a new, update or cancellation DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>termination</i></td><td>Shall not be set in the case of new or update DENM. Shall be set to isCancellation(0) in the case of fulfilment of cancellation conditions; see point (133).</td></tr>
<tr><td><i>eventPosition</i></td><td><i>ReferencePosition</i>. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>relevanceDistance</i></td><td>lessThan5km(5)</td></tr>
<tr><td><i>relevanceTrafficDirection</i></td><td>If the roadType is known, the value shall be set as follows:
<table>
<tr><th>RoadType</th><th>Direction</th></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td><table><tr><td>3</td><td>upstreamTraffic(1)</td></tr></table>Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td><em>validityDuration</em></td><td>180 s</td></tr>
<tr><td><em>stationType</em></td><td>specialVehicles(10)</td></tr>
<tr><td colspan="2"><strong>Situation container</strong></td></tr>
<tr><td><em>informationQuality</em></td><td>See point (130). Shall be refreshed for every update DENM.</td></tr>
<tr><td><em>causeCode</em></td><td>rescueAndRecoveryWorkInProgress(15)</td></tr>
<tr><td><em>subCauseCode</em></td><td>emergencyVehicles(1)</td></tr>
<tr><td colspan="2"><strong>Location container</strong></td></tr>
<tr><td><em>eventSpeed</em></td><td>Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><em>eventPositionHeading</em></td><td>Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><em>traces</em></td><td><em>PathHistory</em> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><em>roadType</em></td><td><em>RoadType</em> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.
Shall be set in accordance with [TS 102 894-2] in combination with the following rules:<table><tr><th>Urban / non-urban</th><th>Structural separation</th><th>Data element</th></tr><tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr><tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr></table></td></tr>
</table>

	Urban	Unknown	urban-NoStructuralSeparationToOppositeLanes(0)
	Non-urban	No	nonUrban-NoStructuralSeparationToOppositeLanes(2)
	Non-urban	Yes	nonUrban-WithStructuralSeparationToOppositeLanes(3)
	Non-urban	Unknown	nonUrban-NoStructuralSeparationToOppositeLanes(2)
	If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.		
Alacarte container			
lanePosition	If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition. If the lanePosition is unknown, the data element shall be omitted. Shall be refreshed for an update DENM.		
Alacarte container: StationaryVehicleContainer			
stationarySince	Shall be set according to the duration in minutes of the detecting C-ITS station being stationary. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM.		

9.7.2. CAM

(139) The *vehicleRole* shall be initialised at a 'default' setting (*vehicleRole* of CAM set to *default(0)*). If at least one of the triggering conditions defined in point (126) is satisfied, the *vehicleRole* shall be set to *emergency(6).*

(140) The following table specifies the data elements of the CAM that shall be set if the C-ITS service is triggered.

Table 18: CAM data elements of 'stationary safeguarding emergency vehicle'

Data field	**Value**
CoopAwareness	
generationDeltaTime	Time corresponding to the time of the reference position in the CAM, considered as time of CAM generation. Shall be set in accordance with [EN 302 637-2].
BasicContainer	
stationType	specialVehicles(10)

referencePosition	Position and position accuracy measured at the reference point of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
HighFrequencyContainer shall be set to BasicVehicleContainerHighFrequency	
heading	Heading direction of the originating C-ITS station in relation to true north. Shall be set in accordance with [TS 102 894-2].
speed	Driving speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
driveDirection	Vehicle drive direction (forward or backward) of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
vehicleLength	Length of vehicle. Shall be set in accordance with [TS 102 894-2].
vehicleWidth	Width of vehicle. Shall be set in accordance with [TS 102 894-2].
longitudinalAcceleration	Vehicle longitudinal acceleration of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
curvature	Curvature of the vehicle trajectory and the accuracy. Shall be set in accordance with [TS 102 894-2].
curvatureCalcMode	Describes whether the yaw rate is used to calculate the curvature for a reported curvature value. Shall be set in accordance with [TS 102 894-2].
yawRate	Yaw rate of vehicle at a point in time. Shall be set in accordance with [TS 102 894-2].
LowFrequencyContainer shall be set to BasicVehicleContainerLowFrequency	
vehicleRole	emergency(6)
exteriorLights	Describes the status of the exterior light switches of a vehicle. Shall be set in accordance with [TS 102 894-2].
pathHistory	Represents the vehicle’s movement over a recent period and/or distance. Shall be set in accordance with [TS 102 894-2].
SpecialVehicleContainer shall be set to EmergencyContainer	

lightBarSirenInUse	lightBarActivated bit shall be set to 1(onChange), if the usage of the light bar is detected, otherwise, it shall be set to 0. sirenActivated bit shall be set to 1, if usage of the siren is detected, otherwise, it shall be set to 0.
emergencyPriority	Is not required
causeCode	As specified in point (138)
subCauseCode	As specified in point (138)

9.8. Network and transport layer

(141) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

9.9. Security layer

(142) If the triggering conditions as described in point (126) apply, an AT change shall be blocked for new, update and cancellation DENMs as long as the *validityDuration* has not expired. Corresponding new, update and cancellation DENMs shall be sent with the same AT.

10. SPECIAL VEHICLE WARNING — STATIONARY RECOVERY SERVICE WARNING

10.1. Description of C-ITS service

This C-ITS service transmits V2V information on a recovery service vehicle supporting a broken-down vehicle. The C-ITS service of the moving recovery service, e.g. carrying a broken-down vehicle, is covered by the common CAM.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘special vehicle warning — emergency vehicle in operation’;
- ‘special vehicle warning — stationary safeguarding emergency vehicle’.

10.2. Triggering conditions

10.2.1. Preconditions

(143) The following preconditions shall be satisfied before this C-ITS service is triggered:

- the *stationType* is confirmed as an emergency vehicle (*stationType* of CAM is set to *specialVehicles*(10)). The C-ITS service is restricted to recovery service vehicles;
- the *Standstill Timer* shall be initialised with zero.

10.2.2. Service-specific conditions

(144) If the vehicle is stationary and the light bar is in use, a *Standstill Timer* shall be initialised with zero and started. If the light bar is no longer in use or the vehicle is no longer stationary, the *Standstill Timer* shall be stopped and reset to zero.

(145) If the preconditions in point (143) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) the light bar is in use, the hazard lights are activated and the parking brake is activated or (in the case of automatic transmission) ‘park’ is selected;

(b) the light bar is in use, the hazard lights are activated and the *Standstill Timer* is 60 s or more.

(146) The level of information quality can be improved by the following conditions:

(c) the status of driver door is ‘open’;

(d) the driver’s seat is detected, by one of the following techniques, as being ‘not occupied’:

(1) passenger compartment camera;

(2) state-of-the-art technique for seat occupation used in seatbelt reminder.

(147) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used. This requirement shall be applied for all subsequent occurrences of vehicle speed analysis.

(148) If the C-ITS service is triggered due to fulfilment of condition (a) in point (145), the *Standstill Timer* shall be stopped and set to 60 s. In the update phase, only the conditions shall be checked, but no timer shall be started.

10.2.3. *Information quality*

(149) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (145) and (146)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 19: Information quality of ‘stationary recovery service warning’

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Condition (b) fulfilled	1
Condition (a) fulfilled	2
At least one of conditions (a) or (b) fulfilled and condition (c) fulfilled	3
At least one of conditions (a) or (b) fulfilled and condition (d) fulfilled	4

(150) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

10.3. Termination conditions

(151) This C-ITS service is terminated by a cancellation of the originating C-ITS station. At the termination of the C-ITS service, update DENM request shall be terminated.

10.3.1. Cancellation

(152) If the following condition is satisfied before the period set in the data element *validityDuration* has expired, the generation of a cancellation DENM shall be triggered and the *vehicleRole* shall be set to *default*(0):

(a) C-ITS service-specific conditions (a) and (b) in point (145) are not satisfied.

10.3.2. Negation

(153) A negation DENM shall not be used for this C-ITS service.

10.4. Update

(154) The generated DENM shall be updated every 60 s if the triggering conditions are still satisfied. All data fields that are assigned new values are defined in Table 20 below.

10.5. Repetition duration and repetition interval

(155) DENMs that are new, have been updated or have been cancelled shall be repeated for a *repetitionDuration* of 60 s with a *repetitionInterval* of 1 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the above values.

Note: The *validityDuration* is set to 180 s. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: Where two DENMs with the same *causeCode* originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

10.6. Traffic class

(156) New, update and cancellation DENMs shall be set to *traffic class* 1.

10.7. Message parameters

*10.7.1. **DENM***

(157) The following table specifies the data elements of the DENM that shall be set.

Table 20: DENM data elements of 'stationary recovery service warning'

Data field	**Value**
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].
detectionTime	*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].

<table>
<tr><td></td><td>Shall be refreshed for an update DENM.</td></tr>
<tr><td>*referenceTime*</td><td>*TimestampIts*-timestamp at which a new, update or cancellation DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td>*termination*</td><td>Shall not be set in the case of new or update DENM. Shall be set to isCancellation(0) in the case of fulfilment of cancellation conditions, see point (152).</td></tr>
<tr><td>*eventPosition*</td><td>*ReferencePosition*. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td>*relevanceDistance*</td><td>lessThan5km(5)</td></tr>
<tr><td>*relevanceTrafficDirection*</td><td>If the roadType is known the value shall be set as follows:
<table>
<tr><th>RoadType</th><th>Direction</th></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
</table>
Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td>*validityDuration*</td><td>180 s</td></tr>
<tr><td>*stationType*</td><td>specialVehicles(10)</td></tr>
<tr><td colspan="2">**Situation container**</td></tr>
<tr><td>*informationQuality*</td><td>See point (149). Shall be refreshed for every update DENM.</td></tr>
<tr><td>*causeCode*</td><td>rescueAndRecoveryWorkInProgress(15)</td></tr>
<tr><td>*subCauseCode*</td><td>unavailable(0)</td></tr>
<tr><td colspan="2">**Location container**</td></tr>
<tr><td>*eventSpeed*</td><td>Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td>*eventPositionHeading*</td><td>Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td>*traces*</td><td>*PathHistory* of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
</table>

<table>
<tr><td></td><td></td></tr>
<tr><td><em>roadType</em></td><td><em>RoadType</em> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.
Shall be set in accordance with [TS 102 894-2] in combination with the following rules:
<table>
<tr><th>Urban / Non-urban</th><th>Structural separation</th><th>Data element</th></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
</table>
If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="2"><strong>Alacarte container</strong></td></tr>
<tr><td><em>lanePosition</em></td><td>If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition.
If the lanePosition is unknown, the data element shall be omitted.
Shall be refreshed for an update DENM.</td></tr>
<tr><td colspan="2"><strong>Alacarte Container: StationaryVehicleContainer</strong></td></tr>
<tr><td><em>stationarySince</em></td><td>Shall be set according to the duration in minutes of the detecting C-ITS station being stationary. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
</table>

10.7.2. ***CAM***

(158) The *vehicleRole* shall be initialised at a ‘default’ setting (*vehicleRole* of CAM set to *default(0)*). If at least one of the triggering conditions defined in point (145) is satisfied the *vehicleRole* shall be set to *rescue(5).*

(159) The following table specifies the data elements of the CAM that shall be set if the C-ITS service is triggered.

Table 21: CAM data elements of ‘stationary recovery service warning‘

Data field	**Value**
CoopAwareness	
generationDeltaTime	Time corresponding to the time of the reference position in the CAM, considered as time of the CAM generation. Shall be set in accordance with [EN 302 637-2].
BasicContainer	
stationType	specialVehicles(10)
referencePosition	Position and position accuracy measured at the reference point of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
HighFrequencyContainer shall be set to BasicVehicleContainerHighFrequency	
heading	Heading direction of the originating C-ITS station in relation to true north. Shall be set in accordance with [TS 102 894-2].
speed	Driving speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
driveDirection	Vehicle drive direction (forward or backward) of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
vehicleLength	Length of vehicle. Shall be set in accordance with [TS 102 894-2].
vehicleWidth	Width of vehicle. Shall be set in accordance with [TS 102 894-2].
longitudinalAcceleration	Vehicle longitudinal acceleration of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
curvature	Curvature of the vehicle trajectory and the accuracy. Shall be set in accordance with [TS 102 894-2].

curvatureCalcMode	Describes whether the yaw rate is used to calculate the curvature for a reported curvature value. Shall be set in accordance with [TS 102 894-2].
yawRate	Yaw rate of vehicle at a point in time. Shall be set in accordance with [TS 102 894-2].
LowFrequencyContainer shall be set to BasicVehicleContainerLowFrequency	
vehicleRole	rescue(5)
exteriorLights	Describes the status of the exterior light switches of a vehicle. Shall be set in accordance with [TS 102 894-2].
pathHistory	Represents the vehicle’s movement over a recent period and/or distance. Shall be set in accordance with [TS 102 894-2].
SpecialVehicleContainer shall be set to SafetyCarContainer	
lightBarSirenInUse	lightBarActivated bit shall be set to 1(onChange) if the usage of the light bar is detected; otherwise, it shall be set to 0. sirenActivated bit shall be set to 1 if usage of the siren is detected; otherwise, it shall be set to 0.
causeCode	As specified in point (157)
subCauseCode	As specified in point (157)

10.8. Network and transport layer

(160) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

10.9. Security layer

(161) If the triggering conditions as described in point (145) apply, an AT change shall be blocked for new, update and cancellation DENMs as long as the *validityDuration* has not expired. Corresponding new, update and cancellation DENMs shall be sent with the same AT.

11. EXCHANGE OF IRCS — REQUEST IRC

11.1. Description of C-ITS service

This C-ITS service transmits V2V information on a critical driving situation where a crash between two vehicles is highly likely or unavoidable. The ego vehicle recognises a potential collision and sends its own IRC to get the IRC of the collision opponent in response.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘exchange of IRCs — response IRC’;

(162) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as valid. Such a signal prompts the stack to generate a new DENM. If the triggering conditions are not met, a DENM signal shall not be generated.

11.2. Triggering conditions

11.2.1. Preconditions

(163) No specific preconditions apply to this C-ITS service.

11.2.2. Service-specific conditions

(164) If both the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) the ‘time to collision’ (TTC) calculated by an on-board measurement device algorithm is < 1.5 s. The acceptable tolerance for the calculated TTC value is 10 %;

(b) the relative speed between two potential collision opponents exceeds 20 km/h.

Note: Calculating the TTC on the basis of the GNSS position only, as delivered from state-of-the-art GNSS-receivers, is not reliable enough for this service.

11.2.3. Information quality

(165) The value of the data element *informationQuality* in the DENM depends on how the event is detected. The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 22: Information quality of ‘exchange of IRCs — request IRC’

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Otherwise	1

11.3. Termination conditions

(166) A termination of the C-ITS service shall not be considered.

11.3.1. Cancellation

(167) A cancellation DENM shall not be used for this C-ITS service.

11.3.2. Negation

(168) A negation DENM shall not be used for this C-ITS service.

11.4. Update

(169) An update DENM shall not be used for this C-ITS service.

11.5. Repetition duration and repetition interval

(170) New DENMs shall be repeated for a *repetitionDuration* of 300 ms (100 ms three times in a row) with a *repetitionInterval* of 100 ms. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the

application and the DEN basic service shall be set in accordance with the above values.

Note: As it is not guaranteed that a sent IRC will reach the receiver (e.g. because of channel load, temporarily out of range, etc.), the sender sends the IRC three times in a row. This is equivalent to a *repetitionDuration* of 300 ms.

Note: The estimated duration for transmitting (application to application) an IRC (repetition not included) over automotive WLAN is 200-300 ms. If only the third attempt is received (worst case), in both cases (request and response), the information will be available for both vehicles after 1 second (2 * (300 ms + 100 ms (@10 Hz) + 100 ms (@10 Hz))). Therefore, the trigger parameter TTC < 1.5 s is sufficient. Sending the IRC three times in a row is considered a good compromise between channel load and ensuring successful transmission.

Note: Only the first DENM will be sent without Decentralized Congestion Control (DCC) constraints. The second and third DENMs may be affected by DCC (based on current channel load).

Note: Where two DENMs with the same causeCode originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

11.6. Traffic class

(171) New DENMs shall be set to *traffic class* 0.

11.7. Message parameters

11.7.1. DENM

(172) The following table specifies the data elements of the DENM that shall be set.

Table 23: DENM data elements of 'exchange of IRCs — request IRC'

Data field	Value
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].
detectionTime	*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
referenceTime	*TimestampIts*-timestamp at which a new DENM is generated. Shall be set in accordance with [TS 102 894-2].
termination	Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.
eventPosition	*ReferencePosition*. Shall be set in accordance with [TS 102 894-2].
relevanceDistance	lessThan100m(1) Note: This shall also cover the worst-case scenario of driving at nearly 250 km/h towards a dangerous end of queue (s = v*t = 69.4 m/s * 1.5 s = 104.2 m).
relevanceTrafficDirection	allTrafficDirections(0)

validityDuration	2 s Note: Shall be larger than TTC.
stationType	The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Situation container	
informationQuality	See point (165)
causeCode	collisionRisk(97)
subCauseCode	unavailable(0)
Location container	
eventSpeed	Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
eventPositionHeading	Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
traces	*PathHistory* of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
roadType	Shall be set in accordance with [TS 102 894-2]. If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.
Alacarte container: ImpactReductionContainer	
heightLonCarrLeft	Height of left longitudinal carrier of the vehicle from base to top. Shall be set in accordance with [TS 102 894-2].
heightLonCarrRight	Height of right longitudinal carrier of the vehicle from base to top. Shall be set in accordance with [TS 102 894-2].
posLonCarrLeft	Longitudinal distance from the centre of vehicle front bumper to the front of the left longitudinal carrier of vehicle. Shall be set in accordance with [TS 102 894-2].
posLonCarrRight	Longitudinal distance from the centre of vehicle front bumper to the front of the right longitudinal carrier of vehicle. Shall be set in accordance with [TS 102 894-2].
positionOfPillars	Vehicle pillars refer to the vertical or near-vertical support of vehicle, designated respectively as A, B, C or D. Shall be set in accordance with [TS 102 894-2].
posCentMass	Perpendicular distance from the centre of mass of an empty load vehicle to the front line of the vehicle bounding box. Shall be set in accordance with [TS 102 894-2].
wheelBaseVehicle	Perpendicular distance between front and rear axle of the wheel base of vehicle. Shall be set in accordance with [TS 102 894-2].
turningRadius	The smallest circular turn (i.e. U-turn) that the vehicle is capable of making. Shall be set in accordance with [TS 102 894-2].

posFrontAx	Perpendicular distance between the vehicle front line of the bounding box and the front wheel axle. Shall be set in accordance with [TS 102 894-2].
positionOfOccupants	BitString that indicates whether a passenger seat is occupied or whether the occupation status is detectable. Shall be set in accordance with [TS 102 894-2].
vehicleMass	Mass of an empty load vehicle. Shall be set in accordance with [TS 102 894-2].
requestResponseIndication	request(0)

*11.7.2. **CAM***

(173) CAM adaption shall not be used for this C-ITS service.

11.8. Network and transport layer

(174) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

11.9. Security layer

(175) If the triggering conditions as described in point (164) apply, an AT change shall be blocked as long as the *validityDuration* has not expired.

12. EXCHANGE OF IRCS — RESPONSE IRC

12.1. Description of C-ITS service

This C-ITS service transmits V2V information on a critical driving situation where a crash between two vehicles is highly likely or unavoidable. The ego vehicle has received an IRC from another vehicle and sends its own IRC in response.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘exchange of IRCs — request IRC’.

(176) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as valid. Such a signal prompts the stack to generate a new DENM. If the triggering conditions are not met, a DENM signal shall not be generated.

12.2. Triggering conditions

12.2.1. Preconditions

(177) An IRC as described in Table 23 has been received.

12.2.2. Service-specific conditions

(178) If the precondition in point (177) and both the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) *requestResponseIndication* in the received IRC is set to request(0);

(b) the perpendicular distance between the requesting vehicle (event position in the IRC) and the ego vehicle (reference position as defined in CAM) is less than 100 m.

Note: When an IRC is received, the receiver has to check that it was actually requested before responding with its own IRC. This can be done on the basis of the requestResponseIndication. To avoid unnecessary load on the transmission channel from multiple transmitted IRCs, only vehicles in the immediate vicinity (within 100 m) respond to the request.

12.2.3. Information quality

(179) The value of the data element *informationQuality* in the DENM depends on how the event is detected. The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 24: Information quality of 'exchange of IRCs — response IRC'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Otherwise	1

12.3. Termination conditions

(180) A termination of the C-ITS service shall not be considered.

12.3.1. Cancellation

(181) A cancellation DENM shall not be used for this C-ITS service.

12.3.2. Negation

(182) A negation DENM shall not be used for this C-ITS service.

12.4. Update

(183) An update DENM shall not be used for this C-ITS service.

12.5. Repetition duration and repetition interval

(184) New DENMs shall be repeated for a *repetitionDuration* of 300 ms (100 ms three times in a row) with a *repetitionInterval* of 100 ms. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the above values.

Note: As it is not guaranteed that a sent IRC will reach the receiver (e.g. because of channel load, temporarily out of range, etc.), the sender sends the IRC three times in a row. This is equivalent to a *repetitionDuration* of 300 ms.

Note: The estimated duration for transmitting (application to application) an IRC (repetition not included) over automotive WLAN is 200-300 ms. If only the third attempt is received (worst case), in both cases (request and response), the information will be available for both vehicles after 1 second (2 * (300 ms + 100 ms (@10 Hz) + 100 ms (@10 Hz))). Therefore, the trigger parameter TTC < 1.5 s is sufficient. Sending the IRC three times in a row is considered a good compromise between channel load and ensuring successful transmission.

Note: Only the first DENM will be sent without DCC constraints. The second and third DENMs may be affected by DCC (based on current channel load).

Note: Where two DENMs with the same causeCode originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

12.6. Traffic class

(185) New DENMs shall be set to *traffic class* 0.

12.7. Message parameters

12.7.1. DENM

(186) The following table specifies the data elements of the DENM that shall be set.

Table 25: DENM data elements of 'exchange of IRCs — response IRC'

Data field	Value
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].
detectionTime	*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
referenceTime	*TimestampIts*-timestamp at which a new DENM is generated. Shall be set in accordance with [TS 102 894-2].
termination	Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.
eventPosition	*ReferencePosition*. Shall be set in accordance with [TS 102 894-2].
relevanceDistance	lessThan100m(1)
relevanceTrafficDirection	allTrafficDirections(0)
validityDuration	2 s
stationType	The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Situation container	
informationQuality	See point (179).
causeCode	collisionRisk(97)
subCauseCode	unavailable(0)
Location container	
eventSpeed	Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
eventPositionHeading	Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].

traces	*PathHistory* of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
roadType	Shall be set in accordance with [TS 102 894-2]. If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.
Alacarte container: ImpactReductionContainer	
heightLonCarrLeft	Height of left longitudinal carrier of the vehicle from base to top. Shall be set in accordance with [TS 102 894-2].
heightLonCarrRight	Height of right longitudinal carrier of the vehicle from base to top. Shall be set in accordance with [TS 102 894-2].
posLonCarrLeft	Longitudinal distance from the centre of vehicle front bumper to the front of the left longitudinal carrier of vehicle. Shall be set in accordance with [TS 102 894-2].
posLonCarrRight	Longitudinal distance from the centre of vehicle front bumper to the front of the right longitudinal carrier of vehicle. Shall be set in accordance with [TS 102 894-2].
positionOfPillars	Vehicle pillars refer to the vertical or near vertical support of vehicle, designated respectively as A, B, C or D. Shall be set in accordance with [TS 102 894-2].
posCentMass	Perpendicular distance from the centre of mass of an empty load vehicle to the front line of the vehicle bounding box. Shall be set in accordance with [TS 102 894-2].
wheelBaseVehicle	Perpendicular distance between front and rear axle of the wheel base of vehicle. Shall be set in accordance with [TS 102 894-2].
turningRadius	The smallest circular turn (i.e. U-turn) that the vehicle is capable of making. Shall be set in accordance with [TS 102 894-2].
posFrontAx	Perpendicular distance between the vehicle front line of the bounding box and the front wheel axle. Shall be set in accordance with [TS 102 894-2].
positionOfOccupants	BitString that indicates whether a passenger seat is occupied or whether the occupation status is detectable. Shall be set in accordance with [TS 102 894-2].
vehicleMass	Mass of an empty load vehicle. Shall be set in accordance with [TS 102 894-2].
requestResponseIndication	response(1)

12.7.2. CAM

(187) CAM adaption shall not be used for this C-ITS service.

12.8. Network and transport layer

(188) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

12.9. Security layer

(189) If the triggering conditions as described in point (178) apply, an AT change shall be blocked as long as the *validityDuration* has not expired. Corresponding new DENMs shall be sent with the same AT.

13. DANGEROUS SITUATION — ELECTRONIC EMERGENCY BRAKE LIGHT

13.1. Description of C-ITS service

This C-ITS service transmits V2V information on an emergency brake by the driver, e.g. as a reaction to a stationary or slower vehicle in front. The ego vehicle itself becomes a possible local danger zone.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘dangerous situations — automatic brake intervention’;
- ‘dangerous situations — reversible occupant restraint system intervention’.

13.2. Triggering conditions

13.2.1. Preconditions

(190) No specific preconditions apply for this C-ITS service.

(191) Parallel activation with the other related C-ITS services shall be avoided. Where the ‘*automatic brake intervention*’ and/or ‘*reversible occupant restraint system intervention*’ C-ITS services are triggered simultaneously, the C-ITS services shall be prioritised as follows:

(a) ‘electronic emergency brake light’ (highest priority);

(b) ‘automatic brake intervention’;

(c) ‘reversible occupant restraint system intervention’ (lowest priority).

(192) If a higher-priority C-ITS service is triggered, any related lower-priority C-ITS service transmission that has already been triggered and is still active regarding update, shall be aborted. In addition, the generation of a new DENM for the higher-priority C-ITS service shall be requested.

13.2.2. Service-specific conditions

(193) If the following condition is satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered.

(a) a signal representing the request for the electronic emergency brake light is detected. The conditions for such a request are set out in [ECE 48], [ECE 13] and [ECE 13H].

Vehicles may also use the following alternative triggering condition:

(b) the current vehicle speed is above 20 km/h and the current acceleration is below -7 m/s² for a minimum of 500 ms.

(194) The acceleration of the vehicle shall be determined by the vehicle bus signal, not by GNSS. The filtered acceleration with respect to sensor noise shall be used.

13.2.3. Information quality

(195) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (193)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 26: Information quality of 'electronic emergency brake light'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	0
Condition (a) fulfilled	1
Condition (a) fulfilled and current filtered longitudinal acceleration of the vehicle < -4 m/s^2	2
Condition (b) fulfilled	3

(196) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

13.3. Termination conditions

(197) The C-ITS service shall be terminated when condition (a) or (b) is no longer valid. At the termination of the C-ITS service, update DENM request shall be terminated.

13.3.1. Cancellation

(198) A cancellation DENM shall not be used for this C-ITS service.

13.3.2. Negation

(199) A negation DENM shall not be used for this C-ITS service.

13.4. Update

(200) The generated DENM shall be updated every 100 ms if the triggering conditions are still satisfied. All data fields that are assigned new values are defined in Table 27 below.

13.5. Repetition duration and repetition interval

(201) A repetition of the DENM shall not be used for this C-ITS service.

13.6. Traffic class

(202) New and update DENMs shall be set to *traffic class* 0.

13.7. Message parameters

13.7.1. ***DENM***

(203) The following table specifies the data elements of the DENM that shall be set.

Table 27: DENM data elements of 'electronic emergency brake light'

<table>
<tr><th>Data field</th><th colspan="2">Value</th></tr>
<tr><th colspan="3">Management container</th></tr>
<tr><td>*actionID*</td><td colspan="2">Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td>*detectionTime*</td><td colspan="2">*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td>*referenceTime*</td><td colspan="2">*TimestampIts*-timestamp at which a new DENM or an update DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td>*termination*</td><td colspan="2">Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.</td></tr>
<tr><td>*eventPosition*</td><td colspan="2">*ReferencePosition*. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for every update DENM.</td></tr>
<tr><td>*relevanceDistance*</td><td colspan="2">lessThan500m(3)</td></tr>
<tr><td rowspan="7">*relevanceTrafficDirection*</td><td colspan="2">If the roadType is known, the value shall be set as follows:</td></tr>
<tr><th>RoadType</th><th>Direction</th></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
<tr><td colspan="2">Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td>*validityDuration*</td><td colspan="2">2 s</td></tr>
<tr><td>*stationType*</td><td colspan="2">The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><th colspan="3">Situation container</th></tr>
<tr><td>*informationQuality*</td><td colspan="2">See point (195).</td></tr>
<tr><td>*causeCode*</td><td colspan="2">dangerousSituation(99)</td></tr>
<tr><td>*subCauseCode*</td><td colspan="2">emergencyElectronicBrakeEngaged(1)</td></tr>
<tr><th colspan="3">Location container</th></tr>
</table>

<table>
<tr><td><i>eventSpeed</i></td><td colspan="3">Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>eventPositionHeading</i></td><td colspan="3">Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>traces</i></td><td colspan="3"><i>PathHistory</i> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td rowspan="10"><i>roadType</i></td><td colspan="3"><i>RoadType</i> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.</td></tr>
<tr><td colspan="3">Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td><b>Urban / Non-urban</b></td><td><b>Structural separation</b></td><td><b>Data element</b></td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="4"><b>Alacarte container</b></td></tr>
<tr><td><i>lanePosition</i></td><td colspan="3">If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition.
If the lanePosition is unknown, the data element shall be omitted.
Shall be refreshed for an update DENM.</td></tr>
</table>

13.7.2. CAM

(204) CAM adaption shall not be used for this C-ITS service.

13.8. Network and transport layer

(205) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

13.9. Security layer

(206) If the triggering conditions as described in point (193) apply, an AT change shall be blocked for new and update DENMs as long as the *validityDuration* has not expired. Corresponding new and update DENMs shall be sent with the same AT.

14. DANGEROUS SITUATION — AUTOMATIC BRAKE INTERVENTION

14.1. Description of C-ITS service

This C-ITS service transmits V2V information on an autonomous emergency braking intervention by the vehicle. The ego vehicle itself becomes a possible local danger zone.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘dangerous situations — emergency electronic brake light’;
- ‘dangerous situations — reversible occupant restraint system intervention’.

14.2. Triggering conditions

14.2.1. Preconditions

(207) No specific preconditions apply for this C-ITS service.

(208) Parallel activation with the other related C-ITS services shall be avoided. Where the ‘*electronic emergency brake light*’ and/or ‘*reversible occupant restraint system intervention*’ C-ITS services are triggered simultaneously, the C-ITS services shall be prioritised as follows:

(a) ‘electronic emergency brake light’ (highest priority);

(b) ‘automatic brake intervention’;

(c) ‘reversible occupant restraint system intervention’ (lowest priority).

(209) If a higher-priority C-ITS service is triggered, any related lower-priority C-ITS service transmission that has already been triggered and is still active regarding update, shall be aborted. In addition, the generation of a new DENM for the higher priority C-ITS service shall be requested.

14.2.2. Service-specific conditions

(210) If the following condition is satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(a) a signal representing a request for the intervention of an autonomous emergency braking system is detected.

(211) The acceleration of the vehicle shall be determined by the vehicle bus signal, not by GNSS. The filtered acceleration with respect to sensor noise shall be used.

14.2.3. Information quality

(212) The value of the data element informationQuality in the DENM depends on how the event is detected (see point (210)). The informationQuality value shall be set in accordance with the following table (highest possible value shall be used):

Table 28: Information quality of 'automatic brake intervention'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	0
Condition (a) fulfilled	1
Condition (a) fulfilled and current filtered longitudinal acceleration of the vehicle < -4 m/s^2	2

(213) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

14.3. Termination conditions

(214) The C-ITS service shall be terminated when condition (a) is no longer valid. At the termination of the C-ITS service, update DENM request shall be terminated.

14.3.1. Cancellation

(215) A cancellation DENM shall not be used for this C-ITS service.

14.3.2. Negation

(216) A negation DENM shall not be used for this C-ITS service.

14.4. Update

(217) The generated DENM shall be updated every 100 ms if the triggering conditions are still satisfied. All data fields that are assigned new values are defined in Table 29.

14.5. Repetition duration and repetition interval

(218) A repetition of the DENM shall not be used for this C-ITS service.

14.6. Traffic class

(219) New and update DENMs shall be set to *traffic class* 0.

14.7. Message parameters

14.7.1. ***DENM***

(220) The following table specifies the data elements of the DENM that shall be set.

Table 29: DENM data elements of ‘automatic brake intervention’

<table>
<tr><th>Data field</th><th colspan="2">Value</th></tr>
<tr><td colspan="3"><b>Management container</b></td></tr>
<tr><td><i>actionID</i></td><td colspan="2">Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>detectionTime</i></td><td colspan="2"><i>TimestampIts</i>-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>referenceTime</i></td><td colspan="2"><i>TimestampIts</i>-timestamp at which a new DENM or an update DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>termination</i></td><td colspan="2">Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.</td></tr>
<tr><td rowspan="2"><i>eventPosition</i></td><td colspan="2"><i>ReferencePosition</i>. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td colspan="2">Shall be refreshed for every update DENM.</td></tr>
<tr><td><i>relevanceDistance</i></td><td colspan="2">lessThan500m(3)</td></tr>
<tr><td rowspan="7"><i>relevanceTrafficDirection</i></td><td colspan="2">If the roadType is known, the value shall be set as follows:</td></tr>
<tr><td><b>RoadType</b></td><td><b>Direction</b></td></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
<tr><td colspan="2">Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td><i>validityDuration</i></td><td colspan="2">2 s</td></tr>
<tr><td><i>stationType</i></td><td colspan="2">The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td colspan="3"><b>Situation container</b></td></tr>
<tr><td><i>informationQuality</i></td><td colspan="2">See point (212)</td></tr>
<tr><td><i>causeCode</i></td><td colspan="2">dangerousSituation(99)</td></tr>
<tr><td><i>subCauseCode</i></td><td colspan="2">aebEngaged(5)</td></tr>
<tr><td colspan="3"><b>Location container</b></td></tr>
</table>

<table>
<tr><td><i>eventSpeed</i></td><td colspan="3">Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>eventPositionHeading</i></td><td colspan="3">Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>traces</i></td><td colspan="3"><i>PathHistory</i> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td rowspan="10"><i>roadType</i></td><td colspan="3"><i>RoadType</i> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.</td></tr>
<tr><td colspan="3">Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td><b>Urban / Non-urban</b></td><td><b>Structural separation</b></td><td><b>Data element</b></td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparationToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparationToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparationToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparationToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparationToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparationToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="4"><b>Alacarte container</b></td></tr>
</table>

lanePosition	If the *lanePosition* is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate of the lane number is not legitimate for this version of the triggering condition. If the *lanePosition* is unknown, the data element shall be omitted. Shall be refreshed for an update DENM.

14.7.2. CAM

(221) CAM adaption shall not be used for this C-ITS service.

14.8. Network and transport layer

(222) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

14.9. Security layer

(223) If the triggering conditions as described in point (210) apply, an AT change shall be blocked for new and update DENMs as long as the *validityDuration* has not expired. Corresponding new and update DENMs shall be sent with the same AT.

15. DANGEROUS SITUATION — REVERSIBLE OCCUPANT RESTRAINT SYSTEM INTERVENTION

15.1. Description of C-ITS service

This C-ITS service transmits V2V information on an active intervention of a reversible occupant-restraint system (e.g. reversible belt-tightener) in the ego vehicle due to a critical driving situation.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘dangerous situations — electronic emergency brake light’;
- ‘dangerous situations — automatic brake intervention’.

15.2. Triggering conditions

15.2.1. Preconditions

(224) No specific preconditions apply for this C-ITS service.

(225) Parallel activation with the other related C-ITS services shall be avoided. Where the ‘*electronic emergency brake light*’ and/or ‘*automatic brake intervention*’ C-ITS services are triggered simultaneously, the C-ITS services shall be prioritised as follows:

(a) ‘electronic emergency brake light’ (highest priority);

(b) ‘automatic brake intervention’;

(c) ‘reversible occupant restraint system intervention’ (lowest priority).

(226) If a higher-priority C-ITS service is triggered, any related lower-priority C-ITS service transmission that has already been triggered and is still active regarding

update, shall be aborted. In addition, the generation of a new DENM for the higher priority C-ITS service shall be requested.

15.2.2. Service-specific conditions

(227) If the following condition is satisfied, the generation of a DENM shall be triggered:

(a) a signal representing a request for the active intervention of a reversible occupant-restraint system (e.g. reversible belt-tightener) is detected due to a critical driving situation.

15.2.3. Information quality

(228) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (227)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 30: Information quality of 'reversible occupant restraint system intervention'

Event detection	**Value of InformationQuality**
No TRCO-compliant implementation	0
Condition (a) fulfilled	1
Condition (a) fulfilled and current filtered longitudinal acceleration of the vehicle < -4 m/s^2	2

(229) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

15.3. Termination conditions

(230) The C-ITS service shall be terminated when condition (a) is no longer valid. At the termination of the C-ITS service, update DENM request shall be terminated.

15.3.1. Cancellation

(231) A cancellation DENM shall not be used for this C-ITS service.

15.3.2. Negation

(232) A negation DENM shall not be used for this C-ITS service.

15.4. Update

(233) The generated DENM shall be updated every 100 ms if the triggering conditions are still satisfied. All data fields that are assigned new values are defined in Table 31 below.

15.5. Repetition duration and repetition interval

(234) A repetition of the DENM shall not be used for this C-ITS service.

15.6. Traffic class

(235) New and update DENMs shall be set to *traffic class* 0.

15.7. Message parameters

15.7.1. DENM

(236) The following table specifies the data elements of the DENM that shall be set.

Table 31: DENM data elements of 'reversible occupant restraint system intervention'

<table>
<tr><th>Data field</th><th colspan="2">Value</th></tr>
<tr><td colspan="3"><b>Management container</b></td></tr>
<tr><td><i>actionID</i></td><td colspan="2">Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>detectionTime</i></td><td colspan="2"><i>TimestampIts</i>-timestamp at which the event is detected by the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>referenceTime</i></td><td colspan="2"><i>TimestampIts</i>-timestamp at which a new DENM or an update DENM is generated. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td><i>termination</i></td><td colspan="2">Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.</td></tr>
<tr><td><i>eventPosition</i></td><td colspan="2"><i>ReferencePosition</i>. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for every update DENM.</td></tr>
<tr><td><i>relevanceDistance</i></td><td colspan="2">lessThan500m(3)</td></tr>
<tr><td rowspan="7"><i>relevanceTrafficDirection</i></td><td colspan="2">If the roadType is known, the value shall be set as follows:</td></tr>
<tr><td><b>RoadType</b></td><td><b>Direction</b></td></tr>
<tr><td>0</td><td>allTrafficDirections(0)</td></tr>
<tr><td>1</td><td>upstreamTraffic(1)</td></tr>
<tr><td>2</td><td>allTrafficDirections(0)</td></tr>
<tr><td>3</td><td>upstreamTraffic(1)</td></tr>
<tr><td colspan="2">Otherwise, the value shall be set to allTrafficDirections(0)</td></tr>
<tr><td><i>validityDuration</i></td><td colspan="2">2 s</td></tr>
<tr><td><i>stationType</i></td><td colspan="2">The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td colspan="3"><b>Situation container</b></td></tr>
<tr><td><i>informationQuality</i></td><td colspan="2">See point (228).</td></tr>
</table>

<table>
<tr><td><i>causeCode</i></td><td colspan="3">dangerousSituation(99)</td></tr>
<tr><td><i>subCauseCode</i></td><td colspan="3">preCrashSystemEngaged(2)</td></tr>
<tr><td colspan="4"><b>Location container</b></td></tr>
<tr><td><i>eventSpeed</i></td><td colspan="3">Speed of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>eventPositionHeading</i></td><td colspan="3">Heading of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>traces</i></td><td colspan="3"><i>PathHistory</i> of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td rowspan="10"><i>roadType</i></td><td colspan="3"><i>RoadType</i> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM.</td></tr>
<tr><td colspan="3">Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td><b>Urban / Non-urban</b></td><td><b>Structural separation</b></td><td><b>Data element</b></td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
<tr><td colspan="4"><b>Alacarte container</b></td></tr>
</table>

lanePosition	If the lanePosition is provided by an on-board sensor (e.g. radar, camera), the value shall be set in accordance with [TS 102 894-2]. Use of GNSS and a digital map to estimate the lane number is not legitimate for this version of the triggering condition. If the lanePosition is unknown, the data element shall be omitted. Shall be refreshed for an update DENM.

15.7.2. CAM

(237) CAM adaption shall not be used for this C-ITS service.

15.8. Network and transport layer

(238) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

15.9. Security layer

(239) If the triggering conditions as described in point (227) apply, an AT change shall be blocked for new and update DENMs as long as the *validityDuration* has not expired. Corresponding new and update DENMs shall be sent with the same AT.

16. ADVERSE WEATHER CONDITIONS — FOG

16.1. Description of C-ITS service

This C-ITS service transmits V2V information on fog that may impede the driver’s vision.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- ‘adverse weather conditions — precipitation’.

(240) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as valid. Such a signal prompts the stack to generate a new or an update DENM. If the triggering conditions are not fulfilled, a DENM signal shall not be generated.

16.2. Triggering conditions

16.2.1. Preconditions

(241) The following preconditions shall be satisfied before this C-ITS service is triggered:

(a) the vehicle speed is greater than 7 km/h;

(b) the vehicle speed is less than 80 km/h.

(242) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used.

16.2.2. Service-specific conditions

(243) If the preconditions in point (241) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(1) driver reaction and light status:

(a) the driver enables the rear fog-light and the low-beam light is enabled. All these conditions must be valid for more than 20 s (to minimise risk of misuse by driver, conditions have to be valid for a longer period);

(b) the driver enables the rear fog-light, the low-beam light is enabled and the vehicle velocity is less than 60 km/h. All these conditions must be valid for a duration greater than 20 s;

(2) visibility range measurement device:

(a) the visibility due to fog is less than 80 m +/- 40 m tolerance for more than 5 s (the obscured view has to be detected for a reasonable period. The period is shorter than for conditions (a) and (b) due to more reliable information);

(b) the visibility due to fog is less than 80 m +/- 40 m tolerance and the vehicle velocity is less than 60 km/h (if the vehicle is in a non-urban area, this speed could be an indication of reduced visibility) for more than 5 s.

(244) A new or update DENM shall not be generated in the *Detection Blocking Time*. The *Detection Blocking Time* is launched after the event is detected and a DENM to that effect has been triggered. In this way, a single event cannot trigger a series of DENMs. For the visibility range measurement device (conditions (c) and (d)), the *Detection Blocking Time* shall be 15 s. For the other conditions there shall be no *Detection Blocking Time.*

(245) In order to ensure consistent functional behaviour for the different triggering conditions and the *Detection Blocking Time*, the *Minimum Detection Interval* between two detected events shall be 20 s.

16.2.3. Information quality

(246) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (243)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 32: Information quality of 'adverse weather condition — fog'

Event detection	**Value of InformationQuality**
No TRCO-compliant implementation	unknown(0)
Condition (a) is fulfilled	1
Condition (b) is fulfilled	2
Condition (c) is fulfilled	3
Condition (d) is fulfilled	4

(247) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed

conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

16.3. Termination conditions

(248) A termination of the C-ITS service shall not be considered.

16.3.1. Cancellation

(249) A cancellation DENM shall not be used for this C-ITS service.

16.3.2. Negation

(250) A negation DENM shall not be used for this C-ITS service.

16.4. Update

(251) The appropriate update procedure of the DENM shall be determined on the basis of the following conditions:

(a) at least one of the conditions in point (243) is fulfilled after the *Minimum Detection Interval* specified in section 16.2.2;

(b) the *validityDuration* of the former DENM has not expired;

(c) neither the value of the data element *DeltaLatitude* nor that of the data element *DeltaLongitude*, representing the distance between the current detected event and the former detected event, exceeds the threshold that can be covered by the data elements *DeltaLatitude* and *DeltaLongitude*.

(252) If conditions (a), (b) and (c) as specified in point (251) are fulfilled, an update DENM shall be generated. The information of the former DENM data elements (*eventPosition, eventDeltaTime, informationQuality*) shall be stored in the *eventHistory* as an additional *eventPoint*.

The event points shall be ordered in ascending order with respect to their lifetime, with the most recent *eventPoint* in first position. Event points in the eventHistory with lifetimes that exceed the validityDuration shall be deleted from the eventHistory for the update DENM. If the distance covered by the eventHistory exceeds the threshold allowed by the security, the oldest event points shall be deleted from the eventHistory.

The information of the current detected event shall be assigned to the DENM data fields of the updated DENM.

Note: It is up to the receiver to handle event points with lifetimes that exceed the validityDuration after the update DENM has been generated.

(253) If conditions (a) and (b) are fulfilled, but condition (c) is not fulfilled, no update DENM shall be generated. Instead, an additional new DENM shall be generated. The information of the current detected event shall be assigned to the DENM data fields of the additional new DENM. The former DENM shall continue to be transmitted as long as the *repetitionDuration* of the former DENM does not expire.

(254) If condition (a) is fulfilled, but condition (b) is not fulfilled, no update DENM shall be generated, but a new DENM according to the currently detected event shall be generated.

Note: In this case, the transmission of the former DENM has already been terminated, because the *repetitionDuration* of the former DENM has expired.

(255) If condition (a) is not fulfilled, the generation of an update DENM is not necessary.

16.5. Repetition duration and repetition interval

(256) DENMs that are new or have been updated shall be repeated for a *repetitionDuration* of 180 s with a *repetitionInterval* of 4 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the above values.

Note: The *validityDuration* is set to 300 s. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: Where two DENMs with the same causeCode originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

16.6. Traffic class

(257) New and update DENMs shall be set to *traffic class* 1.

16.7. Message parameters

16.7.1. DENM

(258) The following table specifies the data elements of the DENM that shall be set.

Table 33: DENM data elements of 'adverse weather condition — fog'

Data field	Value
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].
detectionTime	*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. The timestamp reflects the beginning of the detection of the current event. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM and set to the detection time of the current event.
referenceTime	*TimestampIts*-timestamp at which a new DENM or an update DENM is generated. Shall be set in accordance with [TS 102 894-2].
termination	Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.
eventPosition	*ReferencePosition*. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM.
relevanceDistance	• New DENM: lessThan1000m(4) • Update DENM: lessThan5km(5) (By using updates, the distance covered by the eventHistory becomes longer. To address all relevant ITS stations, the relevanceDistance is longer in this case.)
relevanceTrafficDirection	allTrafficDirections(0)

<table>
<tr><td><i>validityDuration</i></td><td>300 s</td></tr>
<tr><td><i>stationType</i></td><td>The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].</td></tr>
<tr><td colspan="2"><b>Situation container</b></td></tr>
<tr><td><i>informationQuality</i></td><td>See point (246). Shall be refreshed for every update DENM and set to the informationQuality of the current event point.</td></tr>
<tr><td><i>causeCode</i></td><td>adverseWeatherCondition-Visibility(18)</td></tr>
<tr><td><i>subCauseCode</i></td><td>unavailable(0) or fog(1)</td></tr>
<tr><td><i>eventHistory</i></td><td>This element shall be used for update DENMs only (see section 16.4).</td></tr>
<tr><td colspan="2"><b>Location container</b></td></tr>
<tr><td><i>traces</i></td><td><i>PathHistory</i> of the originating C-ITS station with reference to the current event point.
Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td><i>roadType</i></td><td><i>RoadType</i> of the road on which the detecting C-ITS station is situated.

Shall be refreshed for an update DENM.

Shall be set in accordance with [TS 102 894-2] in combination with the following rules:
<table>
<tr><th>Urban / Non-urban</th><th>Structural separation</th><th>Data element</th></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
</table>
If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
</table>

16.7.2. ***CAM***

(259) CAM adaption shall not be used for this C-ITS service.

16.8. Network and transport layer

(260) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

16.9. Security layer

(261) If the triggering conditions as described in point (243) apply, an AT change shall be blocked for new and update DENMs for 15 minutes (starting from the moment the new DENM was generated). Corresponding new and update DENMs shall be sent with the same AT.

(262) If the AT changes and there is an active DENM transmission (new or update DENM), the transmission shall be stopped. In addition, the *EventHistory* and the *PathHistory* shall be deleted. The regular DENM generation process shall then continue.

17. ADVERSE WEATHER CONDITIONS — PRECIPITATION

17.1. Description of C-ITS service

This C-ITS service transmits V2V information on precipitation that may impede the driver's vision.

The following C-ITS services are related to this service, because they share similar triggering conditions:

- 'adverse weather conditions — fog'.

(263) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as valid. Such a signal prompts the stack to generate a new or an update DENM. If the triggering conditions are not fulfilled, a DENM signal shall not be generated.

17.2. Triggering conditions

17.2.1. Preconditions

(264) The following preconditions shall be satisfied before this C-ITS service is triggered:

(a) the vehicle velocity is greater than 7 km/h;

(b) the vehicle velocity is less than 80 km/h;

(c) the windshield washer function is not active.

(265) The vehicle speed shall be determined by the vehicle bus signal, not by GNSS. The filtered vehicle speed (with respect to sensor noise) shall be used.

17.2.2. Service-specific conditions

(266) If the preconditions in point (264) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered.

(1) wiper level and light status:

(a) the wiper operates at its maximum speed level. The low-beam light is enabled. All these conditions must be valid for more than 20 s;

(b) the wiper operates at its maximum speed level and the vehicle velocity is less than 60 km/h. The low-beam light is enabled. All these conditions must be valid for more than 20 s;

(2) rain measurement device, wiper level and light status:

(a) the quantity of rainfall is at least 90 % of the maximum output of the measurement device and the wiper operates at its maximum speed level. The low-beam light is enabled. All these conditions must be valid for more than 20 s;

(b) the quantity of rainfall is at least 90 % of the maximum output of the measurement device and the wiper operates at its maximum speed level. The low-beam light is enabled and the vehicle velocity is less than 60 km/h. All these conditions must be valid for more than 20 s.

(267) The *Minimum Detection Interval* between two detected events shall be 20 s.

17.2.3. Information quality

(268) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (266)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 34: Information quality of 'adverse weather condition — precipitation'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Condition (a) is fulfilled	1
Condition (b) is fulfilled	2
Condition (c) is fulfilled	3
Condition (d) is fulfilled	4

(269) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

17.3. Termination conditions

(270) A termination of the C-ITS service shall not be considered.

17.3.1. Cancellation

(271) A cancellation DENM shall not be used for this C-ITS service.

17.3.2. Negation

(272) A negation DENM shall not be used for this C-ITS service.

17.4. Update

(273) The appropriate update procedure of the DENM shall be determined on the basis of the following conditions:

(a) at least one of the conditions in point (266) is fulfilled after the *Minimum Detection Interval* specified in section 17.2.2;

(b) the *validityDuration* of the former DENM has not expired;

(c) neither the value of the data element *DeltaLatitude* nor that of the data element *DeltaLongitude*, representing the distance between the current detected event and the former detected event, exceeds the threshold that can be covered by the data elements *DeltaLatitude* and *DeltaLongitude*.

(274) If conditions (a), (b) and (c) as specified in point (273) are fulfilled, an update DENM shall be generated. The information of the former DENM data elements (*eventPosition*, *eventDeltaTime*, *informationQuality*) must be stored in the *eventHistory* as an additional *eventPoint*.

The event points shall be ordered in ascending order with respect to their lifetime, with the most recent *eventPoint* in first position. Event points in the *eventHistory* with lifetimes that exceed the *validityDuration* shall be deleted from the *eventHistory* for the update DENM. If the distance covered by the *eventHistory* exceeds the threshold that is allowed by the security, the oldest event points shall be deleted from the *eventHistory*.

The information of the current detected event must be assigned to the DENM data fields of the updated DENM.

Note: It is up to the receiver to handle event points with lifetimes that exceed the *validityDuration* after the update DENM has been generated.

(275) If conditions (a) and (b) are fulfilled, but condition (c) is not fulfilled, no update DENM shall be generated. Instead, an additional new DENM shall be generated. The information of the current detected event must be assigned to the DENM data fields of the additional new DENM. The former DENM shall continue to be transmitted as long as the *repetitionDuration* of the former DENM does not expire.

(276) If condition (a) is fulfilled, but condition (b) is not fulfilled, no update DENM shall be generated, but a new DENM according to the currently detected event shall be generated.

Note: In this case, the transmission of the former DENM has already been terminated, because the *repetitionDuration* of the former DENM has expired.

(277) If condition (a) is not fulfilled, the generation of an update DENM is not necessary.

17.5. Repetition duration and repetition interval

(278) DENMs that are new or have been updated shall be repeated for a *repetitionDuration* of 180 s with a *repetitionInterval* of 4 s. Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set according to the above values.

Note: The *validityDuration* is set to 300 s. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: Where two DENMs with the same *causeCode* originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

17.6. Traffic class

(279) New and update DENMs shall be set to *traffic class* 1.

17.7. Message parameters

17.7.1. DENM

(280) The following table specifies the data elements of the DENM that shall be set.

Table 35: DENM data elements of 'adverse weather condition — precipitation'

Data field	Value
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].
detectionTime	*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. The timestamp reflects the beginning of the detection of the current event point. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM and set to the detection time of the current event point.
referenceTime	*TimestampIts*-timestamp at which a new DENM or an update DENM is generated. Shall be set in accordance with [TS 102 894-2].
termination	Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.
eventPosition	*ReferencePosition*. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM and set to the position of the current event point.
relevanceDistance	• New DENM: lessThan1000m(4) • Update DENM: lessThan5km(5) (By using updates, the distance covered by the *eventHistory* becomes longer. To address all relevant ITS stations, the *relevanceDistance* is longer in this case.)
relevanceTrafficDirection	allTrafficDirections(0)
validityDuration	300 s
stationType	The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Situation container	
informationQuality	See point (268). Shall be refreshed for every update DENM and set to the informationQuality of the current event point.
causeCode	adverseWeatherCondition-Precipitation(19)
subCauseCode	unavailable(0), heavyRain(1) or heavySnowfall(2)

<table>
<tr><td><i>eventHistory</i></td><td colspan="3">This element shall be used for update DENMs only (see section 17.4).</td></tr>
<tr><td colspan="4"><b>Location container</b></td></tr>
<tr><td><i>traces</i></td><td colspan="3"><i>PathHistory</i> of the originating C-ITS station with reference to the current event point.
Shall be set in accordance with [TS 102 894-2].
Shall be refreshed for an update DENM.</td></tr>
<tr><td rowspan="9"><i>roadType</i></td><td colspan="3"><i>RoadType</i> of the road on which the detecting C-ITS station is situated.
Shall be refreshed for an update DENM and set to the roadType of the current event point.
Shall be set in accordance with [TS 102 894-2] in combination with the following rules:</td></tr>
<tr><td><b>Urban / Non-urban</b></td><td><b>Structural separation</b></td><td><b>Data element</b></td></tr>
<tr><td>Urban</td><td>No</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Urban</td><td>Yes</td><td>urban-WithStructuralSeparation ToOppositeLanes(1)</td></tr>
<tr><td>Urban</td><td>Unknown</td><td>urban-NoStructuralSeparation ToOppositeLanes(0)</td></tr>
<tr><td>Non-urban</td><td>No</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td>Non-urban</td><td>Yes</td><td>nonUrban-WithStructuralSeparation ToOppositeLanes(3)</td></tr>
<tr><td>Non-urban</td><td>Unknown</td><td>nonUrban-NoStructuralSeparation ToOppositeLanes(2)</td></tr>
<tr><td colspan="3">If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.</td></tr>
</table>

17.7.2. ***CAM***

(281) CAM adaption shall not be used for this C-ITS service.

17.8. Network and transport layer

(282) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

17.9. Security layer

(283) If the triggering conditions as described in point (266) apply, an AT change shall be blocked for new and update DENMs for 15 minutes (starting from the moment the new DENM was generated). Corresponding new and update DENMs shall be sent with the same AT.

(284) If the AT changes and there is active transmission of a new or update DENM, the transmission shall be stopped. In addition, the *EventHistory* and the

PathHistory shall be deleted. The regular DENM generation process shall then continue.

18. ADVERSE WEATHER CONDITIONS — TRACTION LOSS

18.1. Description of C-ITS service

This C-ITS service transmits V2V information on slipperiness that may impact driving behaviour.

(285) A DENM signal shall be sent to the stack only if the triggering conditions described in this section are evaluated as valid. Such a signal prompts the stack to generate a new or an update DENM. If the triggering conditions are not fulfilled, a DENM signal shall not be generated.

18.2. Triggering conditions

18.2.1. Preconditions

(286) The following preconditions shall be satisfied before this C-ITS service is triggered:

(a) reverse gear is not enabled;

(b) no errors concerning engine, drive train and braking system are reported.

18.2.2. Service-specific conditions

(287) If the precondition in point (286) and at least one of the following conditions are satisfied, the triggering conditions for this C-ITS service are fulfilled and the generation of a DENM shall be triggered:

(1) on the basis of positive acceleration:

(a) on the basis of Anti-Slip Regulation (ASR), acceleration pedal, vehicle acceleration and vehicle velocity. An ASR request must be active for at least 200 ms (as for other safety functions depending on ASR). The acceleration pedal is pressed on average more than 30 % while ASR intervention is active. The acceleration of the vehicle (acceleration according to filtered vehicle bus signal) is less than 40 % of the vehicle acceleration on a surface with high friction coefficient (such as dry asphalt (typical μ = 0.85)) at the same start speed and driving manoeuvre. (In order to cover different drive configurations, e.g. two-wheel vs. four-wheel drive, no detailed values have been put here);

(b) on the basis of ASR, acceleration pedal, vehicle acceleration and vehicle velocity. An ASR request must be active for at least 200 ms. The acceleration pedal is pressed on average more than 30 % while ASR intervention is active. The acceleration of the vehicle (acceleration according to filtered vehicle bus signal) is less than 20 % of the vehicle acceleration on a surface with high friction coefficient (such as dry asphalt (typical μ = 0.85))at the same start speed and driving manoeuvre;

(c) on the basis of ASR, acceleration pedal, vehicle acceleration and vehicle velocity. An ASR request must be active for at least 200 ms. The acceleration pedal is pressed on average more than 30 % while ASR intervention is active. The acceleration of the vehicle (acceleration according to filtered vehicle bus signal) is less than 10 % of the vehicle acceleration on a surface with high friction coefficient (such as dry asphalt (typical μ = 0.85)) at the same start speed and driving manoeuvre;

(d) on the basis of ASR and acceleration pedal. An ASR request must be active for at least 200 ms. The acceleration pedal is pressed on average less than 30 % (so as not to cause an ASR intervention on ground with high friction value) while ASR intervention is active;

(2) on the basis of negative acceleration (deceleration):

(a) on the basis of Anti-lock Braking System (ABS), braking pressure and deceleration. ABS intervention is active for more than 200 ms (according to other safety functions depending on ABS). Braking pressure is more than 20 % of maximum capable braking pressure. The deceleration of the vehicle (deceleration according to filtered vehicle bus signal) is less than 50 % of the vehicle deceleration on a surface with high friction coefficient (such as dry asphalt (typical μ = 0.85)) at the same start speed and driving manoeuvre;

(b) on the basis of ABS, braking pressure and deceleration. ABS intervention is active for more than 200 ms. Braking pressure is more than 20 % of maximum capable braking pressure. The deceleration of the vehicle (deceleration according to filtered vehicle bus signal) is less than 25 % of the vehicle deceleration on a surface with high friction coefficient (such as dry asphalt (typical μ = 0.85)) at the same start speed and driving manoeuvre;

(c) on the basis of ABS, braking pressure and deceleration. ABS intervention is active for more than 200 ms. Braking pressure is more than 20 % (so as not to cause an ABS intervention on ground with high friction value) of maximum capable braking pressure. The deceleration of the vehicle (deceleration according to filtered vehicle bus signal) is less than 10 % of the vehicle deceleration on a surface with high friction coefficient (such as dry asphalt (typical μ = 0.85)) at the same start speed and driving manoeuvre;

(d) on the basis of ABS and braking pressure. ABS intervention is active for more than 200 ms. Braking pressure is less than 20 % of maximum capable braking pressure;

(3) on the basis of friction coefficient estimation:

(a) the friction coefficient is less than 0.3 for at least 5 s (the friction coefficient of ice is < 0.2; for snow and loose chippings, it is approx. 0.4. The friction coefficient needs to be detected for a certain period);

(b) the friction coefficient is less than 0.2 for at least 5 s.

(288) If conditions 1a-c or 2a-c are evaluated as valid, the vehicle acceleration/deceleration shall be determined by the vehicle bus signal, not by GNSS analysis.

(289) A new or update DENM shall not be generated in the *Detection Blocking Time*. The *Detection Blocking Time* is launched after the event is detected and a DENM to that effect has been triggered. This way, a single event is not able to trigger a series of DENMs. For friction coefficient estimation (conditions 3a

and 3b), the *Detection Blocking Time* shall be 15 s. For the other conditions the *Detection Blocking Time* shall be 20 s.

(290) In order to ensure consistent functional behaviour for triggering conditions (a)-(d) and the *Detection Blocking Time*, the *Minimum Detection Interval* between two detected events shall be 20 s.

18.2.3. Information quality

(291) The value of the data element *informationQuality* in the DENM depends on how the event is detected (see point (287)). The *informationQuality* value shall be set in accordance with the following table (highest possible value shall be used):

Table 36: Information quality of 'adverse weather condition — traction loss'

Event detection	Value of InformationQuality
No TRCO-compliant implementation	unknown(0)
Condition 1a or 2a is fulfilled	1
Condition 1b fulfilled	2
Condition 1c or 2b is fulfilled	3
Condition 2c fulfilled	4
Condition 1d or 2d fulfilled	5
Condition 3a is fulfilled	6
Condition 3b is fulfilled	7

(292) If the triggering conditions change between two updates, the *informationQuality* shall not be changed until the next update. If the changed conditions are still fulfilled while the DENM is updated, the *informationQuality* shall be updated.

18.3. Termination conditions

(293) A termination of the C-ITS service shall not be considered.

18.3.1. Cancellation

(294) A cancellation DENM shall not be used for this C-ITS service.

18.3.2. Negation

(295) A negation DENM shall not be used for this C-ITS service.

18.4. Update

(296) The appropriate update procedure of the DENM shall be determined on the basis of the following conditions:

(a) at least one of the conditions in point (287) is fulfilled after the *Minimum Detection Interval* specified in section 18.2.2;

(b) the *validityDuration* of the former DENM has not expired;

(c) neither the value of the data element *DeltaLatitude* nor that of the data element *DeltaLongitude*, representing the distance between the current detected event and the former detected event, exceeds the threshold that can be covered by the data elements *DeltaLatitude* and *DeltaLongitude*.

(297) If conditions (a), (b) and (c) as specified in point (296) are fulfilled, an update DENM shall be generated. The information of the former DENM data elements (*eventPosition*, *eventDeltaTime*, *informationQuality*) must be stored in the *eventHistory* as an additional *eventPoint*.

The event points shall be ordered in ascending order with respect to their lifetime, with the most recent *eventPoint* in first position. Event points in the *eventHistory* with lifetimes that exceed the *validityDuration* (see point (303)) shall be deleted from the *eventHistory* for the update DENM. If the distance covered by the *eventHistory* exceeds the threshold that is allowed by the security, the oldest event points shall be deleted from the *eventHistory*.

The information of the current detected event must be assigned to the DENM data fields of the updated DENM.

Note: It is up to the receiver to handle event points with lifetimes that exceed the *validityDuration* after the update DENM has been generated.

(298) If conditions (a) and (b) are fulfilled, but condition (c) is not fulfilled, no update DENM shall be generated. Instead, an additional new DENM shall be generated. The information of the current detected event shall be assigned to the DENM data fields of the additional new DENM. The former DENM shall continue to be transmitted as long as the *repetitionDuration* of the former DENM does not expire.

(299) If condition (a) is fulfilled, but condition (b) is not fulfilled, no update DENM shall be generated, but a new DENM according to the currently detected event shall be generated.

Note: In this case, the transmission of the former DENM has already been terminated, because the *repetitionDuration* of the former DENM has expired.

(300) If condition (a) is not fulfilled, the generation of an update DENM is not necessary.

18.5. Repetition duration and repetition interval

(301) By default, DENMs that are new or have been updated shall be repeated for a *repetitionDuration* of 300 s with a *repetitionInterval* of 1 s.

However, if the DENM is triggered in an urban area, as determined by a digital map or an on-board sensor algorithm, it shall be repeated for a *repetitionDuration* of 180 s with a *repetitionInterval* of 4 s.

Therefore, the interface parameters *Repetition duration* and *Repetition interval* between the application and the DEN basic service shall be set in accordance with the above values.

Note: The *validityDuration* is set to 600 s or 300 s respectively. Therefore, one can prevent a gap of DENMs if the *repetitionDuration* of the original DENM has expired and the update has not yet been received.

Note: Where two DENMs with the same causeCode originate from the same C-ITS station, the case shall be managed by the receiving C-ITS station.

18.6. Traffic class

(302) New and update DENMs shall be set to *traffic class* 1.

18.7. Message parameters

18.7.1. DENM

(303) The following table specifies the data elements of the DENM that shall be set.

Table 37: DENM data elements of 'adverse weather condition — traction loss'

Data field	Value
Management container	
actionID	Identifier of a DENM. Shall be set in accordance with [TS 102 894-2].
detectionTime	*TimestampIts*-timestamp at which the event is detected by the originating C-ITS station. The timestamp reflects the beginning of the detection of the current event point. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM and set to the detection time of the current event point.
referenceTime	*TimestampIts*-timestamp at which a new DENM or an update DENM is generated. Shall be set in accordance with [TS 102 894-2].
termination	Shall not be set, because neither negation nor cancellation are to be used in this C-ITS service.
eventPosition	*ReferencePosition*. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM and set to the position of the current event point.
relevanceDistance	• New DENM: lessThan1000m(4) • Update DENM: lessThan5km(5) (By using updates, the distance covered by the *eventHistory* becomes longer. To address all relevant ITS stations, the *relevanceDistance* is longer in this case.)
relevanceTrafficDirection	allTrafficDirections(0)
validityDuration	Default: 600 s In urban areas, as determined by digital map or on-board sensor algorithm: 300 s (If the vehicle has no information about the urban/non-urban status, the default value shall be used.)
stationType	The type of the originating C-ITS station. Shall be set in accordance with [TS 102 894-2].
Situation container	
informationQuality	See point (291). Shall be refreshed for every update DENM and set to the informationQuality of the current event point.
causeCode	adverseWeatherCondition-Adhesion(6)

subCauseCode	unavailable(0)		
eventHistory	This element shall be used for update DENMs only (see section 18.4).		
Location container			
traces	*PathHistory* of the originating C-ITS station with reference to the current event point. Shall be set in accordance with [TS 102 894-2]. Shall be refreshed for an update DENM.		
roadType	*RoadType* of the road on which the detecting C-ITS station is situated. Shall be refreshed for an update DENM and set to the *roadType* of the current event point.		
	Shall be set in accordance with [TS 102 894-2] in combination with the following rules:		
	Urban / non-urban	**Structural separation**	**Data element**
	Urban	No	urban-NoStructuralSeparationToOppositeLanes(0)
	Urban	Yes	urban-WithStructuralSeparationToOppositeLanes(1)
	Urban	Unknown	urban-NoStructuralSeparationToOppositeLanes(0)
	Non-urban	No	nonUrban-NoStructuralSeparationToOppositeLanes(2)
	Non-urban	Yes	nonUrban-WithStructuralSeparationToOppositeLanes(3)
	Non-urban	Unknown	nonUrban-NoStructuralSeparationToOppositeLanes(2)
	If the information about the urban/non-urban status cannot be determined, the data element shall be omitted.		

18.7.2. ***CAM***

(304) CAM adaption shall not be used for this C-ITS service.

18.8. Network and transport layer

(305) The interface parameter *DENM destination area* between the DEN basic service and the networking and transport layer shall be equal to a circular shape with radius equal to *relevanceDistance.*

18.9. Security layer

(306) If the triggering conditions as described in point (287) apply, an AT change shall be blocked for new and update DENMs for 15 minutes (starting from the moment the new DENM was generated). Corresponding new and update DENMs shall be sent with the same AT.

(307) If the AT changes and there is active transmission of a new or update DENM, the transmission shall be stopped. In addition, the *EventHistory* and the *PathHistory* shall be deleted. The regular DENM generation process shall then continue.

19. IN-VEHICLE SIGNAGE — DYNAMIC SPEED LIMIT INFORMATION

This C-ITS service transmits I2V information (using IVI) on the currently valid speed limit, by segment, lane or vehicle category, continuously, as set and distributed by the road operator.

(308) The information shall be consistent with the currently valid dynamic traffic signs.

(309) [ISO/TS 14823] Data Field shall be set with serviceCategoryCode = regulatory, nature = 5, serialnumber = 57, attributes/spe/spm = the value of the speed limit in km/h and unit = 0 (i.e. kmperh) or the equivalent for other countries (e.g. 1 for milesperh).

(310) With regard to the end of the speed limit, the following may be used: [ISO/TS 14823] Data Field with serviceCategoryCode = regulatory (12), nature = 6, serialnumber = 14 (notice of end of speed limit) or serviceCategoryCode = informative (13), nature = 6, serial number = 63 (notice of end of all restrictions by electronic signs) if this sign is shown on the road. Ending messages might be redundant, as the end point of the relevance zone of the initial IVI message already terminates the speed limit.

20. IN-VEHICLE SIGNAGE — EMBEDDED VMS 'FREE TEXT'

This C-ITS service transmits infrastructure-to-vehicle (I2V) information (using Infrastructure to Vehicle Information (IVI)) in 'free text', as set and distributed by the road operator. The priority of the IVS messages sent is defined by the road operator.

(311) The information shall be consistent with the currently valid dynamic traffic signs.

21. IN-VEHICLE SIGNAGE — OTHER SIGNAGE INFORMATION

This C-ITS service transmits I2V signage information (using IVI) other than dynamic speed limit and free text information, e.g. bans on overtaking or lane advice, as set and distributed by the road operator.

(312) The information shall be consistent with the currently valid dynamic traffic signs.

(313) [ISO/TS 14 823] Data Field is set with serviceCategoryCode = informative; nature = 6; serialnumber = 59 (for lane closed), 60 (for lane free), 61 (for clear lane to left) or 62 (for clear lane to right).

(314) As regards 'end of the restriction': serviceCategoryCode = informative (13), nature = 6, serial number = 63 for 'end of all restrictions by electronic signs' may be used if this electronic sign is shown. Ending messages might be redundant, as the end point of the relevance zone of the initial IVI message already terminates the signage information.

22. HAZARDOUS LOCATIONS NOTIFICATION — ACCIDENT ZONE

This C-ITS service transmits I2V information (using DEN) about an accident zone using a single warning message ID, as set and distributed by the road operator.

(315) CauseCode shall be set to 2 (accident) and subCauseCode shall be set between 0 and 7 (except 6).

23. HAZARDOUS LOCATIONS NOTIFICATION — TRAFFIC JAM AHEAD

This C-ITS service transmits I2V information (using DEN) about a traffic jam ahead, by segment or lane, using a single warning message ID, as set and distributed by the road operator (mentioning the positions, the length of the traffic jam and the section/lanes concerned, if this information is available).

(316) CauseCode shall be set to 27 (dangerous end of queue) and subCauseCode shall be set to 0 (unavailable) to signal a dangerous end of queue. To convey information about the whole length of the queue, causeCode shall be set to 1 (traffic congestion) and subCauseCode shall be set to 0.

24. HAZARDOUS LOCATIONS NOTIFICATION — STATIONARY VEHICLE

This C-ITS service transmits I2V information (using DEN) about a stationary vehicle using a single warning message ID, as set and distributed by the road operator.

(317) CauseCode shall be set to 94 (stationary vehicle) and subCauseCode shall be set to 0 (unavailable) or 2 (breakdown vehicle).

25. HAZARDOUS LOCATIONS NOTIFICATION — WEATHER CONDITION WARNING

This C-ITS service transmits I2V information (using DEN) about current and/or expected precipitation or extreme weather conditions (scenario 1) or low visibility ranges (scenario 3), using a single warning message ID, as set and distributed by the road operator.

(318) CauseCode shall be set to 17 (extreme weather condition) or 19 (precipitation).

26. HAZARDOUS LOCATIONS NOTIFICATION — TEMPORARY SLIPPERY ROAD

This C-ITS service transmits I2V information (using DEN) on slippery sections of road using a single warning message ID, as set and distributed by the road operator.

(319) CauseCode shall be set to 6 (adhesion) and subCauseCode shall be set between 0 and 9.

27. HAZARDOUS LOCATIONS NOTIFICATION — ANIMAL OR PERSON ON THE ROAD

This C-ITS service transmits I2V information (using DEN) on animals or persons on the road, using a single warning message ID, as set and distributed by the road operator.

(320) CauseCode shall be set to 11 (animal on the road) or 12 (human presence on the road).

28. HAZARDOUS LOCATIONS NOTIFICATION — OBSTACLE ON THE ROAD

This C-ITS service transmits I2V information (using DEN) on one or more obstacles in one or more lanes. However, traffic can still go through (not a blockage). It uses a single warning message ID, as set and distributed by the road operator.

(321) CauseCode shall be set to 10 (obstacle on the road) and subCauseCode shall be set between 0 and 5 (6 and 7 are not used).

29. ROAD WORKS WARNING — LANE CLOSURE (AND OTHER RESTRICTIONS)

This C-ITS service transmits I2V information (using DEN) on the closure of part of a lane, a whole lane or several lanes (including hard shoulder), but without full road closure. It uses a single warning message ID, as set and distributed by the road operator.

It can be provided in one the following ways:

- static planned roadworks (Traffic Operation Centre (TOC) triggered) – the road operator programmes static and planned (or *ad hoc*) road works in its Traffic Management System (TMS);
- stand-alone mode – a trailer is used for a short-term or long-term roadwork, but without a connection to the TOC (no connection available);
- augmented (stand-alone followed by TOC triggered) – the message is first sent from a trailer and can be updated later, including with additional details from the TOC.

(322) CauseCode shall be set to 3 (roadworks) and subCauseCode shall be set to 0 or 4.

30. ROAD WORKS WARNING — ROAD CLOSURE

This C-ITS service transmits I2V information (using DEN) on a road closure due to a set of static roadworks. The closure is temporary. It uses a single warning message ID, as set and distributed by the road operator.

(323) CauseCode shall be set to 3 (roadworks) and subCauseCode shall be set to 1.

31. ROAD WORKS WARNING — ROAD WORKS (MOBILE)

This C-ITS service transmits I2V information (using DEN) on a zone on the road in which, at some point, a lane is narrowed or closed (but without road closure), due to a planned mobile work site. It uses a single warning message ID, as set and distributed by the road operator.

This C-ITS service can be provided in one the following ways:

- TOC triggered – the road operator programmes mobile and planned (or *ad hoc*) road works in its TMS. The information contains all elements that can be used to identify the work zone (start/end position, duration). The operating agents will not use the entire zone, but mark the actual work site within it. More information can be added, such as the speed limit in each narrowed portion;
- stand-alone mode – a trailer is used for a short-term or long-term roadworks, but without a connection to the TOC (no connection available).

(324) CauseCode shall be set to 3 (roadworks) and subCauseCode shall be set to 3.

32. SIGNALISED INTERSECTIONS — GREEN LIGHT OPTIMAL SPEED ADVISORY

This C-ITS service transmits I2V information, using Signal Phase and Timing (SPAT) and Topolgy Information for the Intersection (MAP), on speed advice to road users approaching and passing traffic-light-controlled intersections, based on the current phase state and predicted timing of the traffic lights, and road topology for the intersection(s) ahead.

It can be provided in one of the following ways:

- vehicle calculates speed advice – the signalised intersection transmits periodically and in real time the current phase state of the traffic lights and the timing of upcoming phase changes. The approaching vehicle, aware of its own location and velocity, receives the messages and calculates the optimal speed for approaching the intersection;
- infrastructure calculates speed advice – the signalised intersection calculates and transmits periodically and in real time advisory speed information for multiple road segments of the approach to the intersection. The approaching vehicle, aware of its own location and velocity, receives the messages and extracts the optimal speed for approaching the intersection;
- green-wave speed advice – a sequence of traffic-light-controlled, synchronised intersections transmit pre-defined/planned green-wave speed advice. The approaching vehicle, aware of its own location and velocity, receives the messages and extracts the green-wave speed for passing the intersections.

(325) Information on the current phase state and timing of upcoming phase changes from the signalised intersection shall be sufficiently accurate and reliable to ensure high-quality speed advice.

(326) The information shall be consistent with the physical signal heads of the intersection.

(327) Traffic conditions, such as queues or traffic jams, affect the validity of speed advice and shall therefore be taken into account.

(328) Advised speeds shall never exceed the legal speed limit.

33. SIGNALISED INTERSECTIONS — PUBLIC TRANSPORT PRIORITISATION

This C-ITS service gives priority to public transport vehicles over private vehicles at signalised intersections using Signal Request Extended Message (SREM) and Signal Request Status Extended Message (SSEM). The public transport vehicle transmits a prioritisation request using V2I. The public transport prioritisation system processes the request, accepts or rejects it, and sends feedback to the public transport vehicle using I2V. If the request is accepted, e.g. ‘red phases’ may be shortened and ‘green phases’ extended, the public transport vehicle gets a ‘green light’ with minimum delay at the stop line. After it has successfully driven through the intersection, the traffic-light controller switches back to normal operation.

(329) The stationID of the vehicle shall not change during processing of a prioritisation request.

(330) Authentication and authorisation of public transport vehicles shall be ensured.

(331) The priority request shall be provided in time to allow the public transport prioritisation system to react.

EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 2

ANNEX

to the

Commission Delegated Regulation

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

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

ANNEX II

1. INTRODUCTION

1.1. References

The following references are used in this Annex:

EN 302 636-4-1 — ETSI EN 302 636-4-1, *Intelligent Transport Systems (ITS); Vehicular Communication; Geonetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality*. V1.3.1 (2017-08)

TS 102 894-2 — ETSI TS 102 894-2, *Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary*, V1.3.1 (2018-08)

ISO/TS 19091 — ISO/TS 19091, *Intelligent transport systems – Cooperative ITS – Using V2I and I2V communications for applications related to signalized intersections*, (2017-03)

EN 302 663 — ETSI EN 302 663, *Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band*, V1.2.1 (2013-07)

TS 102 687 — ETSI TS 102 687, *Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part*, V1.2.1 (2018-04)

TS 102 792 — ETSI TS 102 792, *Intelligent Transport Systems (ITS); Mitigation techniques to avoid interference between European CEN Dedicated Short Range Communication (CEN DSRC) equipment and Intelligent Transport Systems (ITS) operating in the 5 GHz frequency range*, V1.2.1 (2015-06)

EN 302 637-2 — ETSI EN 302 637-2, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*, V1.4.0 (2018-08); this reference shall be read as the reference to version 1.4.1 from the date of the publication of that version.

TS 102 724 — ETSI TS 102 724, Intelligent Transport Systems (ITS); Harmonized *Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band*, V1.1.1 (2012-10)

EN 302 636-5-1 — ETSI EN 302 636-5-1, *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking;*

	Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol, V2.1.1 (2017-08)
TS 103 248	ETSI TS 103 248, *Intelligent Transport Systems (ITS); GeoNetworking; Port Numbers for the Basic Transport Protocol (BTP)*, V1.2.1 (2018-08)
EN 302 931	ETSI EN 302 931, *Vehicular Communications; Geographical Area Definition*, V1.1.1 (2011-7)
EN 302 637-3	ETSI EN 302 637-3, *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*, V1.3.0 (2018-08); this reference shall be read as the reference to version 1.3.1 from the date of the publication of that version.
TS 102 636-4-2	ETSI TS 102 636-4-2, *Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 2: Media-dependent functionalities for ITS-G5*, V1.1.1 (2013-10)
SAE J2945/1	SAE J2945/1, *On-board System Requirements for V2V Safety Communications*, (2016-03)
TS 103 097	ETSI TS 103 097, *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*, V1.3.1 (2017-10)
ISO 8855	ISO 8855, *Road vehicles — Vehicle dynamics and road-holding ability — Vocabulary*, (2011-12)
TS 103 301	ETSI TS 103 301, *Intelligent Transport Systems (ITS)*; *Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services*, V1.2.1 (2018-08)
TS 103 175	ETSI TS 103 175, *Intelligent Transport Systems (ITS); Cross Layer DCC Management Entity for operation in the ITS G5A and ITS G5B medium*, V1.1.1 (2015-06)
ISO/TS 19321	ISO/TS 19321, *Intelligent transport systems — Cooperative ITS — Dictionary of in-vehicle information (IVI) data structures*, (2015-04-15)
ISO 3166-1	ISO 3166-1:2013, *Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes*
ISO 14816	ISO 14816:2005, *Road transport and traffic telematics; Automatic vehicle and equipment identification; Numbering and data structure*

ISO/TS 14823	ISO/TS 14823:2017, *Intelligent transport systems – Graphic data dictionary*
IEEE 802.11	IEEE 802.11-2016, IEEE Standard for Information technology — Telecommunications and information exchange between systems, local and metropolitan area networks — Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, (2016-12-14)

1.2. Notations and abbreviations

The following notations and abbreviated terms are used in this Annex.

AT	Authorization Ticket
BTP	Basic Transport Protocol
CA	Cooperative Awareness
CAM	Cooperative Awareness Message
CBR	Channel Busy Ratio
CCH	Control Channel
CDD	Common Data Dictionary
CEN-DSRC	European Committee for Standardisation (CEN)-Dedicated Short Range Communication
C-ITS	Cooperative Intelligent Transport Systems
DCC	Decentralized Congestion Control
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
DP	Decentralized Congestion Control Profile
ETSI	European Telecommunications Standards Institute
GBC	GeoBroadcast
GN	GeoNetworking
GNSS	Global Navigation Satellite System
IEEE	Institute of Electrical and Electronics Engineers
IVI	Infrastructure to Vehicle Information
IVIM	Infrastructure to Vehicle Information Message
MAP	Topology information for the intersection
MAPEM	MAP Extended Message
NH	Next Header
NTP	Network Time Protocol
PAI	Position Accuracy Indicator
PoTi	Position and Time

QPSK	Quadrature Phase-Shift Keying
RLT	Road Lane Topology
RSU	Road-side Unit
SCF	Store Carry Forward
SHB	Single Hop Broadcast
SPATEM	Signal Phase and Timing Extended Message
SREM	Signal Request Extended Message
SSEM	Signal Request Status Extended Message
TAI	International Atomic Time
TAL	Trust Assurance Level
TLM	Traffic Light Manoeuvre
TC	Traffic Class
UTC	Coordinated Universal Time
WGS84	World Geodetic System 84

1.3. Definitions

The following definitions are used in this Annex:

(a) ‘C-ITS time’ or ‘time base’ means the number of elapsed International Atomic Time (TAI) milliseconds since 2004-01-01 00:00:00.000 Coordinated Universal Time (UTC)+0 as defined in [ETSI EN 302 636-4-1]. Timestamps as defined in [ETSI TS 102 894-2] follow this time format.

Note: ‘TAI milliseconds’ denote the true number of milliseconds counted and not altered by leap seconds after 1 January 2004.

(b) ‘station clock’ means a clock representing Cooperative Intelligent Transport Systems (C-ITS) time in a C-ITS station.

2. REQUIREMENTS FOR VEHICLE C-ITS STATIONS DESIGNED FOR SHORT-RANGE COMMUNICATION

This system profile specifies a minimum set of standards and fills the missing gaps as necessary for the realisation of an interoperable vehicle C-ITS station on the transmitting side. The profile includes interoperability requirements only, leaving open any additional requirements. It therefore does not describe the full functionality of the vehicle C-ITS station.

This system profile enables the deployment of the priority (in particular, V2V) services. It may support other services, but these may require additional system specifications.

The profile provides descriptions, definitions and rules for the layers (Applications, Facilities, Networking & Transport and Access) of the ETSI ITS station reference architecture/ITS-S host.

2.1. Definitions

The following definitions are used in this part of the Annex:

(a) ‘vehicle states’ comprise absolute position, heading and velocity at a certain point in time;

(b) information provided with a ‘confidence level’ of 95 % means that the true value is inside the range specified by the estimated value plus/minus the confidence interval in 95 % of the data points in a given statistical base;

(c) ‘sky obstruction’ means the fraction of half-hemisphere values that are obstructed for Galileo or other Global Navigation Satellite Systems (GNSS) satellites due to mountains, buildings, trees, etc.

(d) ‘CEN-DSRC’ (Comité Européen de Normalisation - Dedicated Short Range Communication) is a microwave technology used for electronic toll systems to finance road infrastructure costs or to collect road usage fees. For the purpose of this Annex, ‘CEN-DSRC’ covers all 5.8 GHZ microwave technologies as referred to in Directive 2004/52/EC of the European parliament and of the Council and in Commission Decision 2009/750/EC.

2.2. Parameter settings

The parameter settings in Table 1 are used in this part of the Annex.

Table 1: Parameter settings

Parameter	**Value**	**Unit**	**Description**
pAlDataRateCch	6	Mbit/s	Default data rate for Control Channel (CCH)
pAlDataRateCchHigh	12	Mbit/s	Optional higher data rate for CCH than the default one
pAlDataRateCchLow	3	Mbit/s	Optional lower data rate for CCH than the default one
pBtpCamPort	2001	n/a	Well-known destination port for CAMs
pBtpDenmPort	2002	n/a	Well-known destination port for DENMs
pBtpDestPortInfo	0	n/a	Value for the destination port information
pCamGenNumber	3	n/a	Number of consecutive generated CAMs without time restrictions
pCamTraceMaxLength	500	m	Maximal length of a trace in CAMs
pCamTraceMinLength	200	m	Minimal length of a trace in CAMs
pCamTrafficClass	2	n/a	Traffic class (TC) value with which CAMs are sent
pDccCcaThresh	-85	dBm	Minimum sensitivity of the channel
pDccMeasuringInterval	100	ms	Value for the interval in which the channel load is provided
pDccMinSensitivity	-88	dBm	Value for minimum receiver sensitivity

pDccProbingDuration	8	µs	Value for the probing sample duration
pDccPToll	10	dBm	Value for transmission power inside protected zones
pDCCSensitivityMargin	3	dB	Value for margin of parameter pDccMinSensitivity
pDenmTraceMaxLength	1000	m	Maximum length of a trace in DENMs
pDenmTraceMinLength	600	m	Minimum length of a trace in DENMs
pGnAddrConfMode	ANONYMOUS (2)	n/a	Configuration method for GeoNetworking (GN) address
pGnBtpNh	2	n/a	Value for the Next Header (NH) field of GN common header
pGnChannelOffLoad	0	n/a	Value for the channel offload field
pGnEtherType	0x8947	--	Value for the EtherType to use
pGnGbcHtField	4	n/a	Value for the HeaderType field in cases of GeoBroadcast (GBC)
pGnGbcScf	1	n/a	Value for the store-carry-forward field in cases of GBC
pGnInterfaceType	ITS-G5 (1)	n/a	Interface type to be used by GN
pGnIsMobile	1	n/a	Defines whether C-ITS station is mobile or not
pGnMaxAreaSize	80	km²	Supported area to cover
pGnSecurity	ENABLED (1)	n/a	Defines use of GN security headers
pGnShbHstField	0	n/a	Value for the HeaderSubType field in cases of Single Hop Broadcast (SHB)
pGnShbHtField	5	n/a	Value for the HeaderType field in cases of SHB
pGnShbLifeTimeBase	1	n/a	Value for the LifeTimeBase field in case of SHB.
pGnShbLifeTimeMultiplier	1	n/a	Value for the LifeTimeMultiplier field in cases of SHB
pPotiMaxTimeDiff	20	ms	Maximum time difference between station clock and time base
pPotiWindowTime	120	s	Size of Position and Time (PoTi) sliding window in seconds

pPotiUpdateRate	10	Hz	Update rate for position and time information
pSecCamToleranceTime	2	s	Maximum time deviation between time in the security header of the Cooperative Awareness Message (CAM) and station clock to accept the CAM
pSecGnScc	0	n/a	Value for the SCC field of the GN address
pSecGnSourceAddressType	0	n/a	Value for the M field of the GN address (configuration type of the address)
pSecMaxAcceptDistance	6	km	Maximum distance between sender and receiver to accept messages
pSecMessageToleranceTime	10	min	Maximum time deviation between time in security header of message (other than CAM) and station clock to accept the message
pSecRestartDelay	1	min	Grace period for AT change after turning on ignition terminal
pTraceAllowableError	0.47	m	Parameter for calculation of path history; see Appendix A.5 of [SAE J2945/1] for further details.
pTraceDeltaPhi	1	°	Parameter for calculation of path history; see Appendix A.5 of [SAE J2945/1] for further details.
pTraceEarthMeridian	6,378.137	km	Earth mean radius (according to International Union of Geodesy and Geophysics (IUGG). Used for calculation of traces; see Appendix A.5 of [SAE J2945/1] for further details.
pTraceMaxDeltaDistance	22.5	m	Parameter for calculation of traces; see Appendix A.5 of [SAE J2945/1] for further details.

2.3. Security

(1) A vehicle C-ITS station shall be securely linked to one specific vehicle. Where the vehicle C-ITS station is powered, it shall verify that it is operating in the vehicle with which it has been securely linked. If such correct functioning condition cannot be verified, the C-ITS station shall be deactivated, preventing it from sending messages (i.e. deactivate at least the radio transmission level of the C-ITS station).

(2) The vehicle C-ITS station shall check the timestamp in the security header against the reception time and accept only CAMs in the last time of *pSecCamToleranceTime* and other messages within the last time of *pSecMessageToleranceTime*.

(3) The vehicle C-ITS station shall check the distance from the sender position — in the security header, if available — and forward only messages with a distance from the sender of *pSecMaxAcceptDistance* or less.

(4) The verification of a message shall comprise at least cryptographic verification of the message's signature.

(5) The vehicle C-ITS station shall forward only verified messages.

(6) The vehicle C-ITS station shall use one end-to-end security header and signature per message in accordance with [TS 103 097] and [EN 302 636-4-1].

(7) The signature shall be generated using a private key corresponding to a valid AT in accordance with clause 7.2.1 in [TS 103 097].

(8) All addresses and identifiers transmitted through short-range communication shall be changed when the AT is changed.

2.4. Positioning and timing

(9) The vehicle states shall be consistent. Therefore, heading and velocity shall refer to the same time as the absolute position (e.g. GenerationDeltaTime in CAMs).

Note: Any inaccuracies that might result from time-related effects should be taken into account in the accuracies of the state variables.

(10) The vehicle C-ITS station shall use World Geodetic System 84 (WGS84) as its reference coordinate system, as specified in [TS 102 894-2].

Note: Based on the drift of the European Terrestrial Reference System (ETRS89), which is fixed to the continental plate of Europe, of 2.5 cm/year in WGS84 it needs to be noted that Vehicle C-ITS stations need to be aware what referencing system is used. When an enhanced referencing system such as a Real-time Kinematics enhanced system is used for high-precision location referencing, this shift may need to be compensated.

(11) Altitude information shall be interpreted as height above WGS84 Ellipsoid.

Note: Alternative altitude interpretations using Geoid definitions (e.g. relative to mean sea level) shall not be used.

(12) For horizontal position, a confidence area is used instead of a single confidence interval. The confidence area is described as ellipse specified via a major axis, minor axis and orientation of the major axis relative to the north direction, as defined in point (10).

(13) The vehicle C-ITS station shall interpret 'heading' as the direction of the horizontal velocity vector. The starting point of the velocity vector shall be the ITS vehicle reference point, as defined in B.19 'referencePosition' in [EN 302 637-2].

Note: Alternative heading interpretations referring to the vehicle body orientation shall not be used.

Note: This definition implies that straight backward driving results in 180 ° difference between heading and vehicle body orientation.

(14) C-ITS time shall be the basis for all timestamps in all messages transmitted by the vehicle C-ITS station in all EU Member States.

(15) When active, C-ITS stations shall update the vehicle states with a frequency of at least the *pPotiUpdateRate*.

(16) Timestamps in messages shall be based on the station clock.

(17) The difference between the station clock and C-ITS time shall be estimated. If the absolute difference |Station clock time - C-ITS time | >= *pPotiMaxTimeDiff*, the vehicle C-ITS station shall not be active.

Note: A precise timestamp is not only needed for time synchronisation, but also implies that system states are valid at precisely that point in time, i.e. that the vehicle states stay consistent.

(18) When coming to a standstill, the system shall report the last known heading value (vehicle direction of motion). The value shall be unlatched when returning to motion.

2.5. System behaviour

(19) The vehicle C-ITS station shall operate the Cooperative Awareness Basic Service when it is on public roads and under regular driving dynamics.

Note: Operation of the cooperative awareness basic service includes the transmission of CAMs if all conditions for CAM generation are fulfilled.

(20) Traces and path history data shall be generated only when position confidence information is available and the station clock adheres to point (90)(91).

(21) A vehicle occupant shall be enabled to deactivate the vehicle C-ITS station easily at any time.

(22) The vehicle C-ITS station shall handle CAM transmissions so that no outdated messages are transmitted even if congestion control is applied.

2.6. Access layer

(23) The vehicle C-ITS station shall use the control channel G5-CCH as specified in Table 3 in [EN 302 663] to send messages to support the Cooperative Awareness Basic Service and the priority C-ITS services specified in Annex I of this Regulation.

(24) The vehicle C-ITS station's access layer shall be compliant with [EN 302 663], with the exception of emission limits and with the exception of clauses 4.2.1, 4.5 and 6.

(25) The vehicle C-ITS station shall use a default transfer rate of *pAlDataRateCch* on the control channel.

(26) The vehicle C-ITS station shall also support *pAlDataRateCchLow* and *pAlDataRateCchHigh* transfer rates on the control channel.

(27) The vehicle C-ITS station's access layer shall be compliant with [TS 102 724].

(28) The vehicle C-ITS station shall support the following Decentralised Congestion Control profiles (DPs) defined in [TS 102 724]: DP0, DP1, DP2 and DP3.

These DCC profiles shall use the following DCC-profile identification values:

- DP0, used only for DENMs with TC = 0;
- DP1, used for DENMs with TC = 1;

- DP2, used for CAMs with TC = *pCamTrafficClass*;
- DP3, used for forwarded DENMs and other low priority messages.

(29) The vehicle C-ITS station's DCC mechanism shall comply with [TS 102 687].

(30) The settings of Table A.2 in [TS 102 687] shall be used if the reactive DCC algorithm outlined in clause 5.3 of [TS 102 687] is implemented.

Note: Table A.2 in [TS 102 687] is based on CAM and Decentralised Environmental Notification Message (DENM) dissemination for priority C-ITS services with an average T_{on} of 500 µs.

(31) The following smoothing function of Channel Busy Ratio (CBR) values shall be performed if the vehicle C-ITS station uses the reactive DCC algorithm outlined in clause 5.3 of [TS 102 687]: CBR_now = (CBR(n)+CBR(n-1))/2 (

Note: Where 'n' and 'n-1' are the current and previous CBR sampling periods respectively).

(32) The vehicle C-ITS station shall, at a minimum, be able to generate and transmit the number of messages determined by the value of the highest CAM generation rate (i.e. 10 Hz) and, if detection algorithms are used, it shall be increased by the minimum required DENM generation rate derived from those triggering conditions.

(33) The vehicle C-ITS station shall abide by the following maximum message rates if it uses the reactive DCC algorithm outlined in clause 5.3 of [TS 102 687]:

- for the relaxed state: the sum of all messages sent on DP1, DP2 and DP3 shall not surpass $R_{max\_relaxed}$ = 16.7 messages per second. Message bursts are allowed for DP0 with R_{Burst} = 20 messages per second, with a maximum duration of T_{Burst} = 1 second, and may take place only every $T_{BurstPeriod}$ = 10 seconds. Thus, adding DP0 messages, the maximum message rate amounts to $R_{max\_relaxed}$ = 36.7 messages per second;
- for active states: the maximum message rate for each state is given in Table A.2 in [TS 102 687];
- for the restrictive state: the maximum message rate per vehicle C-ITS station is set to 2.2 messages per second, i.e. the inverse of T_{TX_MAX} = 460 ms.

(34) The vehicle C-ITS station shall support per-packet transmission power control.

Note: P_{Tx} may depend on the current DCC state (i.e. relaxed, active or restrictive) and on the DCC profile (i.e. DP0, DP1, etc.).

(35) The vehicle C-ITS station shall reduce its transmission power to P_{Toll} = *pDccPToll* as soon as the protected zone is entered and without changing any other DCC transmission parameters as per Table A.2 in [TS 102 687]. DP0 messages are excluded from this restriction.

(36) Where the vehicle C-ITS station is not equipped with a CEN-DSRC radio detector as described in clause 5.2.5 of [TS 102 792], it shall maintain a list of protected zone positions as described in clause 5.5.1 of [TS 102 792]. This list shall be composed of:

- a set of protection zones as listed in the 'latest version' (available when the vehicle is developed) of the protected zone database. The vehicle C-ITS station may include update mechanisms of the database;
- a set of protected zones as identified by the reception of CEN-DSRC mitigation CAMs as described in clauses 5.2.5 and 5.2.2.3 of [TS 102 792];
- a temporarily protected zone as identified by the reception of CEN-DSRC mitigation CAMs as described in clause 5.2.2.2 of [TS 102 792].

(37) Where the vehicle C-ITS station is equipped with a CEN-DSRC radio detector, mitigation shall be applied as described in clause 5.2.5 of [TS 102 792] and the vehicle C-ITS station shall generate CAMs in accordance with clause 5.5.1 of [TS 102 792].

(38) Where the vehicle C-ITS station is not equipped with a CEN-DSRC radio detector, mitigation shall be applied in accordance with [TS 102 792] on the basis of the list defined in point (36) and received CAMs from other road users which have implemented point (37).

Note: Clarification of clause 5.2.5 of [TS 102 792]: A mobile ITS station should mitigate each time to the nearest tolling station centre position. Where several positions are given in the same area, the mobile ITS station should respond to each centre position, possibly in a sequence. Protected zones with identical protectedZone ID may be seen as a single station. Where the protected zone database and the CEN-DSRC mitigation CAMs contain a valid protected zone with the identical protectedZone ID, mitigation shall be based only on the CEN-DSRC mitigation CAM content.

2.7. Networking and transport layer

(39) The vehicle C-ITS station's media-independent part of GeoNetworking (GN) shall be compliant with [EN 302 636-4-1].

(40) All default constants and parameters of the vehicle C-ITS station profile not defined or overwritten in this Regulation shall be set as specified in Annex H to [EN 302 636-4-1].

(41) GN shall be used with itsGnSecurity set to *pGnSecurity*.

(42) GN shall be used with itsGnLocalAddrConfMethod set to *pGnAddrConfMode*.

(43) GN parameter itsGnMaxGeoAreaSize shall be set to *pGnMaxAreaSize*.

(44) Packet repetition shall not be performed by GN in a vehicle C-ITS station and the corresponding steps for repetition in the packet-handling procedures described in clause 10.3 of [EN 302 636-4-1] shall not be executed.

The 'maximum repetition time' parameter of the service primitive GN-DATA.request and the GN protocol constant itsGnMinPacketRepetitionInterval do not apply to a vehicle C-ITS station.

(45) GN shall be used with its GnIfType set to *pGnInterfaceType.*

(46) The Vehicle C-ITS station shall use Single Hop Broadcast (SHB) headers as defined in [EN 302 636-4-1] on all CAM packets it sends.

Consequently, the GN common header shall use a value of *pGnShbHtField* for the HT field and a value of *pGnShbHstField* for the HST field when transmitting SHB packets.

The vehicle C-ITS station shall use GBC headers as defined in [EN 302 636-4-1] on all DENM packets it sends.

Consequently, the GN common header shall use a value of *pGnGbcHtField* for the HT field when transmitting DENM packets.

For the HST field one of the following values shall be used:

- 0 for circular areas;
- 1 for rectangular areas;
- 2 for ellipsoidal areas.

Note: This profile covers the handling of SHB and GBC packets. As it does not cover the handling of other GN packet types defined in [EN 302 636-4-1], it does not prevent their implementation.

(47) The vehicle C-ITS station shall set the LifeTime field of all SHB packets in the following manner:

- set the sub-field multiplier to *pGnShbLifeTimeMultiplier* and the sub-field base to *pGnShbLifeTimeBase*.

(48) The vehicle C-ITS station shall set the LifeTime field of all GBC packets to the minimum value of ValidityDuration and RepetitionInterval, where ValidityDuration and RepetitionInterval are defined in the relevant service profile. The value of the LifeTime field shall not exceed the itsGnMaxPacketLifetime, as specified in Annex H to [EN 302 636-4-1].

(49) The vehicle C-ITS station shall buffer GBC packets where no neighbours are available (store-carry-forward). Consequently, the Store Carry Forward (SCF) bit of the TC field of GBC packets shall be set to *pGnGbcScf*.

(50) The vehicle C-ITS station is not required to offload packets to another channel. Consequently, the channel offload bit of the TC field should be set to *pGnChannelOffLoad*.

(51) The vehicle C-ITS station shall use the DCC profiles specified in point (28). Consequently, the DCC Profile ID bits of the TC field shall use the DCC-profile identification values defined in point (28).

(52) The vehicle C-ITS station shall set the itsGnIsMobile bit of the Flags field to *pGnIsMobile*.

(53) The vehicle C-ITS station shall support multi-hop operation mode. It shall implement the forwarding algorithm specified in Annexes D, E.3 and F.3 to [EN 302 636-4-1].

(54) When forwarding packets, the vehicle C-ITS station shall use the DCC profile DP3 as defined in [TS 102 724] and referred to in point (28).

(55) The vehicle C-ITS station shall use duplicate packet detection on the networking and transport layer. Consequently, the algorithm specified in Annex A.2 to [EN 302 636-4-1] shall be used for detecting duplicate packets.

(56) All GN frames sent by the vehicle C-ITS station shall use the EtherType value *pGnEtherType* as listed by the Institute of Electrical and Electronics Engineers (IEEE) Registration Authority at http://standards.ieee.org/develop/regauth/ethertype/eth.txt.

(57) The vehicle C-ITS station's Basic Transport Protocol (BTP) shall be compliant with [EN 302 636-5-1].

(58) The vehicle C-ITS station shall employ BTP-B headers. Consequently, the GN common header shall use a value of *pGnBtpNh* for the NH field.

(59) The vehicle C-ITS station shall set the destination port info field to the value *pBtpDestPortInfo*.

(60) In the BTP-B header, the vehicle C-ITS station shall set the destination port to the value *pBtpCamPort* for CAMs.

(61) In the BTP-B header, the vehicle C-ITS station shall set the destination port to the value *pBtpDenmPort* for DENMs.

(62) The vehicle C-ITS station shall support circular, rectangular and ellipsoidal geographical areas as defined in [EN 302 931]. Each use case defined in the relevant service profile must specify one of the above geographical area types indicated through the GN header as specified in [EN 302 636-4-1].

(63) Where a vehicle C-ITS station calculates the distance between two positions using Galileo or other GNSS coordinates (e.g. for PathDeltaPoints or in cases of circular relevance area), the great circle or a more accurately performing method shall be used.

2.8. Facility layer

(64) The vehicle C-ITS station's Cooperative Awareness (CA) basic service shall be compliant with [EN 302 637-2].

(65) The path history field in the CAM low-frequency container shall be generated according to the method specified in point (86) and shall contain a PathHistory data element covering a minimum distance of *pCamTraceMinLength* (K_PHDISTANCE_M parameter, as defined in Appendix A.5 to [SAE J2945/1]).

An exception to the minimum covered distance by PathHistory shall be made only if:

- the vehicle has not yet physically covered the distance with its current AT (e.g. after vehicle startup or right after AT change when driving); or
- the maximum number of PathPoints is used, but the overall length covered by the PathHistory still does not reach *pCamTraceMinLength.*

  Note: This may happen if the road topology contains tight curves and the distance between consecutive PathPoints is reduced.

Only in the above cases may the vehicle send PathHistory information covering a distance below *pCamTraceMinLength*.

(66) The PathHistory in CAMs shall cover at most *pCamTraceMaxLength.*

(67) The PathHistory in CAMs shall include PathDeltaTime in every PathPoint. It shall describe a list of actually travelled geographical locations leading to the

current vehicle position, sorted by the time the positions were reached by the vehicle, with the first point being the closest in time to the current time.

(68) Where the vehicle C-ITS station does not move, i.e. PathPoint position information does not change, the PathDeltaTime of the first PathPoint shall still be updated with every CAM.

(69) Where the vehicle C-ITS station does not move, i.e. PathPoint position information does not change, for a duration longer than the maximum value of PathDeltaTime (specified in [TS 102 894-2]) the PathDeltaTime of the first PathPoint in the CAM shall be fixed to the maximum value.

(70) The CA basic service shall be active as long as the vehicle is on public roads and under regular driving dynamics. As long as the CA basic service is active, CAMs shall be generated in accordance with the generation rules in [EN 302 637-2].

(71) A vehicle C-ITS station shall transmit CAM messages where position confidence information is available and the station clock adheres to point (91).

(72) The TC value for CAM messages shall be set to *pCamTrafficClass.*

(73) The parameter T_GenCam_Dcc (see [EN 302 637-2]) shall be set to the value of the minimum time between two transmissions, T_{off}, as given by Table A.2 (DCC mechanisms) in [TS 102 687].

(74) The adjustable N_GenCam parameter (see [EN 302 637-2]) specified in the CAM generation frequency management shall be set to *pCamGenNumber* for the vehicle C-ITS station.

(75) The vehicle C-ITS station’s Decentralised Environmental Notification (DEN) basic service shall be compliant with [EN 302 637-3].

(76) The DENM repetition shall be done by the DEN basic service as specified in [EN 302 637-3].

(77) The path history field in the DEN messages shall be generated according to the method specified in point (86) and shall contain trace-data elements covering a minimum distance of *pDenmTraceMinLength* (K_PHDISTANCE_M parameter defined in Appendix A.5 to [SAE J2945/1]).

An exception to the minimum covered distance by traces shall be made only if:

- the vehicle has not yet physically covered the distance with its current AT. (e.g. after vehicle startup or right after AT change when driving); or
- the maximum number of PathPoints is used, but the overall length covered by the PathHistory still does not reach *pDenmTraceMinLength*.

  Note: This may happen if the road topology contains tight curves and the distance between consecutive PathPoints is reduced.

Only in the above two cases may the vehicle send trace information covering a distance below *pDenmTraceMinLength*.

(78) The traces in the DENMs shall cover at most *pDenmTraceMaxLength*.

(79) A vehicle C-ITS station shall use the DENM traces as follows:

- the first trace element shall describe a time-ordered list of actually travelled geographical locations leading to the event position, as specified in point (67).

(80) The PathDeltaTime data elements of the PathPoints in the first DENM traces element shall be updated only if the DENM is updated.

(81) Where the event-detecting vehicle does not move, i.e. PathPoint position information does not change, the PathDeltaTime of the first PathPoint of the first DENM traces element shall still be updated with every DEN_Update.

Note: This is only the case for stationary events where the detecting vehicle is identical to the event, e.g. a stationary vehicle warning. For dynamic events, e.g. dangerous situations or events that are not identical to the vehicle (adverse weather warnings, etc.), this is not the case.

(82) Where the vehicle C-ITS station does not move, i.e. PathPoint position information does not change, for a duration longer than the maximum value of PathDeltaTime (specified in [TS 102 894-2]), the PathDeltaTime of the first PathPoint in the first DENM trace element shall be fixed to the maximum value.

(83) Additional PathHistory elements may be present in the DENM traces. However, unlike the first element, these shall describe alternative routes to the event location. These routes may or may not be available at the time of detecting the event. In the alternative routes, the PathPoints shall be position-ordered (i.e. shortest-path routes) and shall not include the PathDeltaTime.

(84) For the priority services, the vehicle C-ITS station shall generate only DENMs as described in the relevant service profile.

(85) The data elements that constitute the content of the CAM and DENM shall be compliant with [TS 102 894-2] and use the coordinate system specified in points (87), (10) and (11).

(86) The traces and path histories used by the vehicle C-ITS station shall be generated using Design Method One, as specified in Appendix A.5 to [SAE J2945/1]. The vehicle C-ITS Station shall use this generation method with the following settings:

- K_PHALLOWABLEERROR_M = *pTraceAllowableError*, where PH_ActualError < K_PHALLOWABLEERROR_M;
- maximum distance between concise path points, K_PH_CHORDLENGTHTHRESHOLD = *pTraceMaxDeltaDistance*;
- K_PH_MAXESTIMATEDRADIUS = REarthMeridian;
- K_PHSMALLDELTAPHI_R = *pTraceDeltaPhi*;
- REarthMeridian = *pTraceEarthMeridian* (according to the IUGG), used for great-circle or orthodromic distance calculation:

$$\text{PH\_ActualChordLength} = \text{REarthMeridian}*\cos^{-1}[\cos(lat_1)\cos(lat_2)\cos(long_1-long_2)+\sin(lat_1)\sin(lat_2)]$$

(87) The vehicle C-ITS station shall use a coordinate system compliant with section 2.13 of [ISO 8855].

Note: This means that the X and Y axes are parallel to the ground plane, the Z axis is aligned vertically upwards, the Y axis points to the left of the vehicle's forward direction and the X axis points towards the vehicle's forward driving direction.

2.9. Hardware-related requirements

(88) The 95 % confidence value (see points 2.1 (b) and (12)) shall be valid in each scenario listed in point (92). This implies that in a confidence value assessment test (which can be offline) a statistic averaging over all states and scenarios is not appropriate.

Instead, a sliding window containing the vehicle states (see point 2.1 (a)) of the last *pPotiWindowTime* seconds shall be used as the statistical base.

Note: The proposed confidence validation mechanism using the sliding window is typically performed offline, as post-processing of collected test data. It is not required that the vehicle C-ITS station performs confidence validation online, i.e. while in public roads and under regular driving dynamics.

Note: The sliding window approach has the following advantages over separate statistics for each scenario:

- transitions between scenarios are included;
- confidence is valid 'now' instead of 'over lifetime'. 'Error bursts' (many invalid confidence values in a short timeframe) are not allowed, thus:
  - enhancing the usefulness of the confidence value for applications;
  - requiring fast detection of accuracy degradation inside POTI;
- the precise definition of test data has no effect on confidence validation parameters. However, the test data shall contain all scenarios listed in point (92);
- no further statistical calculations are needed; the scenarios cover all relevant states;
- the interval length is similar to typical (environment and driving condition) scenario lengths (e.g. city tunnel, standing at traffic light, driving manoeuvres);
- 5 % of the interval is similar to typical short-term effects (e.g. driving under a bridge).

(89) A vehicle is considered to be under regular driving dynamics when:

- it has passed its initial startup phase;
- it is being used as envisaged by the manufacturer;
- normal control of the vehicle is possible (e.g. it is not directly involved in an accident, road surface allows normal tyre grip);
- all the following conditions (values) apply for passenger cars:
  - vehicle lateral acceleration is < 1.9 m/s^2;
  - vehicle longitudinal acceleration is > -2.4 m/s^2 (deceleration);
  - vehicle longitudinal acceleration is < 2.5 m/s^2;

- vehicle speed is ≤ minimum of (130 km/h, Vmax).

(90) Under optimal GNSS conditions and regular driving dynamics, as defined in point (89), the confidence values shall be equal to or lower than the following values in at least 95 % of 3D position data points in a dataset:

- horizontal position confidence of 5 m;
- vertical position confidence of 20 m.

In other scenarios, the requirement degradations in point (92) apply. This requirement ensures the usefulness of information sent in all C-ITS messages.

(91) The station clock shall be within *pPotiMaxTimeDiff* of C-ITS time, i.e. Delta t = |station clock time - C-ITS time| < *pPotiMaxTimeDiff*.

(92) A vehicle C-ITS station shall be able to provide useful vehicle state estimates even in challenging scenarios. To account for inevitable degradations, required confidence values are defined for different scenarios in Table 2.

‘C’ is the maximum of semiMajorConfidence and semiMinorConfidence. The condition for ‘C’ shall be fulfilled in 95 % of data points in the dataset of the given scenario.

Note: The criteria shall be met under the following slope dynamics for the analysed trace fraction: average slope <= 4 % and maximum slope <= 15 %

Note: As a precondition, each scenario shall be started with one minute of driving under open sky and regular driving dynamics.

Note: No C values indicate that the scenario shall be tested to ensure that the reported confidence interval is valid, but no limit is given.

Table 2: Scenarios

ID	Scenario	Definition	Acceptance
Environment under regular driving dynamics			
S1	Open sky	Sky is less than 20 % obstructed, with vehicle moving with normal driving dynamics, normal road conditions	C <= 5 m
S2	Tunnel	No GNSS satellite is visible for at least 30 s and 250 m (v_{min}=30 km/h); GNSS signal reflection at entrance and end of tunnel	C < 15 m
S3	Parking Structure	No direct visible GNSS satellites, but connection by reflections, T > 60 s, v_{max} < 20 km/h, minimum two 90 ° curves and s > 100 m, two ramps in the entrance and exit area	any value is allowed
S4	Half open sky	Sky is 30-50 % obstructed (obstruction concentrated on one side of the car) for more than 30 s; driving conditions as S1	C < 7 m
S5	Forest	Sky is 30-50 % obstructed by objects, including trees higher than the antenna, for more than 30 s.	C < 10 m
S6	Mountains (valley)	Sky is 40-60 % obstructed by high mountain(s); driving conditions as S1	C < 10 m

S7	City	In a 300 s drive, the sky was 30-50 % obstructed (short periods of less than 30-50 % obstructions allowed), frequent GNSS signal reflection off buildings, including short losses of GNSS signal (i.e. fewer than four satellites); driving conditions as S1	C < 14 m
S8	Mild urban	Sky is 20-40 % obstructed, t > 60 s, s > 400 m. Driving conditions as S1, with stops, trees and/or buildings, as well as alleys	C < 10 m
Driving conditions under open sky			
S9	Dynamic driving	Test drive with longitudinal accelerations of more than -6 m/s² and lateral accelerations of > (±) 5 m/s²	C < 7 m
S10	Static	Vehicle standing still for 30 min	C < 5 m
S11	Rough road	Test drive on dirt road with pot holes, v= 20-50 km/h	C < 10 m
S12	Icy road	Test drive with longitudinal accelerations of more than -0.5 m/s² and lateral accelerations of > (±) 0.5 m/s², µ < 0.15	C < 7 m
S13	High speed	V= minimum of (130 km/h, Vmax) on dry road for 30 s	C < 5 m

(93) Under optimal GNSS conditions and regular driving dynamics as defined in point (89), the speed confidence values shall be equal to or lower than the following values in at least 95 % of data points in a dataset:

- 0.6 m/s for speeds between 1.4 m/s and 12.5 m/s;
- 0.3 m/s for speeds greater than 12.5 m/s.

(94) Under optimal GNSS conditions and regular driving dynamics as defined in point (89), the heading confidence values shall be equal to or lower than the following values in at least 95 % of data points in a dataset:

- 3° for speeds between 1.4 m/s and 12.5 m/s;
- 2° for speeds greater than 12.5 m/s.

3. REQUIREMENTS FOR ROADSIDE C-ITS STATIONS DESIGNED FOR SHORT-RANGE COMMUNICATION

This system profile specifies a minimum set of standards and fills the missing gaps as necessary for the realisation of an interoperable roadside C-ITS station on the transmitting side. The profile includes interoperability requirements only, leaving open any additional requirements. It therefore does not describe the full functionality of the roadside C-ITS station.

This system profile enables the deployment of the priority (in particular, I2V) services. It may support other services, but these may require additional system specifications.

The profile provides descriptions, definitions and rules for the layers (Applications, Facilities, Networking & Transport and Access) and management of the ETSI ITS station reference architecture/ITS-S host.

3.1. Positioning and timing

(95) The C-ITS time of a static roadside C-ITS station shall be the basis for all timestamps in all transmitted messages and GN beacons.

Note: This means that timestamps in GN header must use the same clock and time base as timestamps in CAM/DENM/IVIM payloads. For SPATEM and MAPEM, the timestamp used should be as specified in [ISO TS 19091].

(96) The position of static roadside C-ITS stations shall be accurately measured and set permanently.

The confidence values shall be equal to or lower than the following values in at least 95 % of datasets:

- horizontal (latitude, longitude) position confidence of 5 m;
- altitude position confidence of 20 m.

Note: This avoids GNSS jitter in position accuracy and raises confidence to nearly 100 %.

(97) The difference between station clock and time base shall be estimated. The absolute difference |station clock time — time base| should not exceed 20 ms, but must in any case be less than 200 ms. The roadside C-ITS station shall not transmit messages if the station clock time differs by more than 200 ms.

Note: A precise timestamp is not only needed for time synchronisation, but also means that system states are valid at precisely that point in time, i.e. that the system states stay consistent.

Note: The information for time synchronisation can be obtained from a Galileo or other GNSS receiver or from a Network Time Protocol (NTP) service.

3.2. System behaviour

(98) All roadside C-ITS stations shall be able to transmit the infrastructure messages (e.g. DENM, CAM, Infrastructure to Vehicle Information Message (IVIM), Signal Phase and Timing Extended Message (SPATEM), MAP Extended Message (MAPEM) and Signal Request Status Extended Message (SSEM).

(99) Roadside C-ITS stations shall be able to receive DENM, CAM and Signal Request Extended Message (SREM) messages as defined in section 3.6.

3.3. Access layer

The access layer comprises the two lowest layers in the protocol stack, i.e. physical (PHY) and data-link layers, where the latter is further subdivided into medium-access control (MAC) and logical-link control (LLC).

(100) Roadside C-ITS stations shall use the optional enhanced receiver performance requirements as defined in Tables 17-19 in IEEE 802.11.

(101) Roadside C-ITS stations shall use the control channel G5-CCH as specified in Table 3 in [EN 302 663] to send messages to support the priority C-ITS services specified in Annex 3, using a default transfer rate of 6 Mbit/s (Quadrature Phase-Shift Keying (QPSK) 1/2).

(102) Roadside C-ITS stations' access layer shall be compliant with [EN 302 663], with the exception of emission limits and with the exception of clauses 4.2.1, 4.5 and 6.

(103) Roadside C-ITS stations shall be compliant with [TS 102 687].

(104) Roadside C-ITS stations should manage the limited hardware and software resources at their disposal and may perform traffic shaping or selective forwarding in line with the 'best effort' principle.

Note: Traffic shaping is especially relevant for relayed DENM messages, as it is anticipated that in some situations (such as severe traffic congestion or other extreme vehicular network scenarios) the DENM load might increase abruptly. In such cases, roadside C-ITS stations are explicitly allowed to forego the forwarding of foreign DENM messages.

(105) A roadside C-ITS station shall, at a minimum, be able to generate and transmit the number of messages as determined by the value of the highest CAM generation rate (i.e. 10 Hz) and, if detection algorithms are used, increased by the minimum required DENM generation rate derived from those triggering conditions.

(106) A roadside C-ITS station shall support the broadcast mode defined in [EN 302 663].

(107) A protected zone shall be defined as follows:

- where a tolling location consists of a single CEN-DSRC Road-side Unit (RSU), a protected zone with a default radius of 55 m shall be defined, with the location of the CEN-DSRC RSU as centre position;
- where there are multiple CEN-DSRC RSUs nearby, overlaps of protected zones should be avoided as far as possible through a combined protected zone. A combined Protected Zone shall use the geographical centre (circumcentre) of all DSRC RSUs concerned as a centre position; the radius shall be given by the circumradius + 55 m. In any case, a maximum radius of 255 m shall not be exceeded.

Note: Due to the maximum radius of 255 m, overlaps cannot always be avoided.

(108) Where a roadside C-ITS station is located close to CEN-DSRC-based tolling equipment (at least inside the protected zone), it shall apply mitigation techniques as defined in [TS 102 792].

(109) Mobile roadside C-ITS stations shall apply mitigation methods on the basis of tolling zone announcement messages.

(110) Where the roadside C-ITS station is used to indicate the presence of a tolling station, it shall transmit CAMs including protected zones in line with the technique defined in [TS 102 792] and with the CA message format as specified in [EN 302 637-2]. It shall transmit these CAMs on the control channel, before a vehicle C-ITS station enters the protected zone.

(111) Roadside C-ITS stations' access layer shall be compliant with [TS 102 724].

(112) Roadside C-ITS stations shall apply DCC techniques in accordance with [TS 102 687].

3.4. Network and transport layer

(113) Roadside C-ITS stations shall apply GN as networking protocol in accordance with [EN 302 636-4-1].

(114) All default constants and parameters of the infrastructure roadside profile not specified in this Annex shall be set as specified in Annex H to [EN 302 636-4-1].

(115) Packet repetition shall not be performed by GN and the corresponding steps in the packet-handling procedures defined in clause 10.3 of [EN 302 636-4-1] shall not be executed. The ‘maximum repetition time’ parameter of the service primitive GN-DATA.request and the GN protocol constant itsGnMinPacketRepetitionInterval do not apply.

(116) Roadside C-ITS stations may choose ‘anonymous address’ for GN address configuration (itsGnLocalAddrConfMethod set to ANONYMOUS(2)).

(117) Roadside C-ITS stations shall use GN with itsGnIfType set to ITS-G5(1).

(118) Where GN packet repetition is disabled, itsGnMinPacketRepetitionInterval is not applicable.

(119) The LifeTime field of all SHB packets shall be set to one second.

(120) The LifeTime field of all GBC packets shall be set to the minimum of ValidityDuration and RepetitionInterval, but shall not exceed the itsGnMaxPacketLifetime parameter, specified in Annex H to [EN 302 636-4-1].

(121) Where ‘store-carry-forward’ is enabled, the SCF bit in the TC field shall be set to one.

Note: As a result, packets can be buffered if no neighbours are available.

(122) A roadside C-ITS station is not required to offload packets to another channel. Consequently, the channel offload bit of the TC field should be set to 0 for all message types.

(123) A stationary roadside C-ITS station shall set the itsGnIsMobile bit of the Flags field to 0. A mobile roadside C-ITS station shall set the itsGnIsMobile bit of the Flags field to 1.

(124) Roadside C-ITS stations shall support the multi-hop operation mode by using the algorithms specified in Annexes E.3 and F.3, based on the selection principles outlined in Annex D, to [EN 302 636-4-1].

(125) Roadside C-ITS stations shall use duplicate packet detection on the networking and transport layer. For the detection of duplicated packets, the algorithm specified in Annex A.2 to [EN 302 636-4-1] shall be used.

(126) Roadside C-ITS stations may send only GN beacons with the Position Accuracy Indicator (PAI) set to 1.

(127) GN frames sent by the roadside C-ITS station shall use the EtherType value 0x8947 as listed by the IEEE Registration Authority at http://standards.ieee.org/develop/regauth/ethertype/eth.txt.

(128) Roadside C-ITS stations shall implement the BTP in accordance with [EN 302 636-5-1].

(129) Roadside C-ITS stations shall use BTP-B headers. Consequently, the GN common header shall use a value of 2 for the NH field.

(130) Roadside C-ITS stations shall set the destination port info field to the value 0.

(131) Roadside C-ITS stations shall set the destination port depending on the message set as specified in [TS 103 248].

(132) Geographical areas shall be applied in accordance with [EN 302 931].

(133) Roadside C-ITS stations shall support at least circular, rectangular and ellipsoidal geographical areas as defined in [EN 302 931]. Each C-ITS service shall specify one of the above geographical area types, indicated through the GN header as specified in [EN 302 636-4-1].

(134) Where the roadside C-ITS station calculates the distance between two positions using Galileo or other GNSS coordinates (e.g. for PathDeltaPoints or in cases of circular relevance area), it is recommended that the great circle or a more accurately performing method shall be used. Care shall be taken (e.g. by using the haversine formula) to avoid large rounding errors on low-precision floating point systems.

Where the relevance area is an ellipse or a rectangle, the Cartesian coordinates of the area centre and of the current position must be calculated as specified in [EN 302 931], for assessing whether to hop the packet. For this purpose, the ‘local tangent plane’ method is recommended, or another method delivering the same accuracy.

3.5. Facility layer

(135) Roadside C-ITS stations’ DEN basic service shall be compliant with [EN 302 637-3].

(136) Roadside C-ITS station shall implement the DENM repetition as specified in [EN 302 637-3].

(137) The cases in which DENM updates are triggered are specified in the relevant service profile in Annex I.

(138) Where a roadside C-ITS station sends a DENM, the traces shall be described as a list of geographical locations leading from the event position back to the first path point.

(139) Where a mobile roadside C-ITS station becomes stationary, the PathDeltaTime of the first PathPoint of the first DENM traces element shall be fixed to the maximum value specified in [EN 302 637-3]. Therefore, PathPoints do not ‘fall out’ of the first DENM traces element. This applies only to trailer-based C-ITS services.

(140) Additional PathHistory elements may be present in the DENM traces. However, unlike the first element, these shall describe alternative routes to the event location. These routes may or may not be available at the time of detecting the event.

(141) For roadside C-ITS stations, the TC value of a message is specific to the based service of the message format or the C-ITS service itself and is therefore specified in the relevant service profile in Annex I. The selected TC value shall comply with the message classifications as specified in [TS 102 636-4-2] and [TS 103 301], except that Infrastructure to Vehicle Information (IVI) messages

related to variable speed limits are low-priority DENM equivalents and therefore may have the same TC value.

(142) The roadside system shall use a coordinate system compliant with section 2.13 of [ISO 8855].

Note: This means that the X and Y axes are parallel to the ground plane, the Z axis is aligned vertically upwards, the Y axis points to the left of the vehicle’s forward direction and the X axis points towards the vehicle’s forward driving direction.

(143) For the transmission of messages by roadside systems, the facilities layer protocol and communication profile setting CPS_001 shall be used as specified in [TS 103 301].

(144) The protected zone data provided in a CAM sent by a roadside C-ITS station shall not conflict with the protected zone information provided in the protected zone database or an equivalent database. If the same zone is defined in the protected zone database, the same ID shall be used as protectedZoneID. Otherwise, an ID greater than 67108863 that is not used in the database shall be used.

(145) Roadside C-ITS stations intended to disseminate protected zone data shall transmit CAMs on a regular basis containing protected zone data using the message format specified by [EN 302 637-2]. CAM termination is not used.

Note: The specific data elements for the coexistence C-ITS service are located in the highFrequencyContainer and the rsuContainerHighFrequency data frame.

Note: A CAM may contain other data elements not related to the coexistence C-ITS service.

(146) The antenna of a roadside C-ITS station intended to disseminate protected zone data shall be placed so that protection zone CAMs can be received in time before entry into the protected zone.

Note: Arrangements for complying with this requirement must take account of the processing time the road-user’s equipment needs to process the information received. A time of 300 ms should be used as a reference.

(147) A roadside C-ITS station intended to disseminate protected zone data shall transmit CAMs containing protected zone data with a transmission frequency that ensures that mobile C-ITS stations are able to identify the presence of protected zones in time.

(148) A roadside C-ITS station intended to disseminate protected zone data shall be installed outside protected zones or configured in accordance with [TS 102 792].

(149) A CAM shall not contain more than one temporary protected zone (i.e. ProtectedCommunicationZone with ProtectedZoneType=1).

Note: This is specific to temporary tolling and enforcement vehicles. Mobile C-ITS stations are required to store only one temporary protected zone in accordance with clause 5.2.2.2 of [TS 102 792], in order to avoid ambiguity.

(150) Where the coexistence (ITS-G5 — CEN-DSRC) Facilities Layer Service is used, it shall be applied in accordance with [EN 302 637-2] and as specified in [TS 102 792].

(151) [ISO/TS 19321] refers to an older version (1.2.1) of the [TS 102 894-2] common data dictionary (CDD) for payload data. All [ISO/TS 19 321] based IVI C-ITS services shall therefore be based on the updated version (1.3.1), until [ISO/TS 19321] is updated accordingly.

(152) The CA basic service shall be active as long as the mobile roadside C-ITS station is participating on public roads under regular driving dynamics. As long as the CA basic service is active, CAMs shall be generated in accordance with the generation rules in [EN 302 637-2].

(153) Roadside C-ITS stations shall transmit CAM messages where position confidence information is available and the station clock adheres to point (97).

(154) The parameter T_GenCam_Dcc shall be set to the value of the minimum time between two transmissions T_{off} as provided by the DCC mechanism specified in point (103).

(155) The adjustable N_GenCam parameter specified in the CAM generation frequency management shall be set to 0 for the roadside C-ITS station, unless it is intended to disseminate protected zone data as defined in point (145).

3.6. Management

Not all specified security services have to be implemented. In addition, for some services, implementation is defined internally by the C-ITS station operator.

(156) Roadside C-ITS stations implementing ITS-G5 functionalities shall implement a management layer including a DCC_CROSS entity as specified in [TS 103 175].

3.7. Service Elements

3.7.1. DEN basic service

The DEN basic service uses the services provided by the protocol entities of the ITS networking and transport layer to disseminate DENMs.

A DENM contains information relating to an event that has a potential impact on road safety or traffic conditions. An event is characterised by an event type, an event position, a detection time and a time duration. These attributes may change over space and over time. DENM transmission may be independent from the originating C-ITS station in some situations.

Four types of DENM are generated by the DEN basic service:

- new DENMs;
- update DENMs;
- cancellation DENMs;
- negation DENM.

(157) The DENM header shall be as specified in the data dictionary [TS 102 894-2].

(158) DENM data elements, data frames and service parameters shall be set in accordance with Table 3. In addition, for C-ITS services on roadworks warnings, DENM data frames and service parameters shall be set in accordance with Table 4.

Table 3: DENM elements in general

Name	Use	Usage
Management container	Mandatory	
actionID	Mandatory	**Content**: The actionID is the unique identifier of a DENM and consists of the data elements originatingStationID and sequenceNumber. originatingStationID is the unique identifier of the C-ITS station whose facility layer created the message, which may be either the central or the roadside C-ITS station. If not set by the central C-ITS station, messages of which the content is generated centrally but which are broadcast from different roadside C-ITS stations will have different originatingStationIDs, resulting in different actionIDs If the originatingStationID and sequenceNumber are given by the central C-ITS station where centrally generated content is (potentially) sent out via multiple roadside C-ITS stations, the system provides the same actionID for all messages relating to the same event, regardless of which roadside C-ITS station is sending the message. Once the actionID is set, it will not change for messages relating to the same event, even if they are frequently updated. **Value**: not pre-defined, set by system
detectionTime	Mandatory	Initially, this DE shall be set to the time the event was detected. The time shall come from a local time source in the roadside C-ITS station in stand-alone use-case scenarios. In use-case scenarios with connection to the central C-ITS station, the detectionTime shall initially be set to the time that the application that creates the DENM receives the relevant information, i.e. the moment a roadwork or a hazardous location starts / is detected at a functional level. **Value:** detectionTime is initially set to the start time of the event (new DENM) then reset for each DENM update. For DENM termination, this DE shall be the time at which the termination of the event is detected.
referenceTime	Mandatory	**Content:** The referenceTime shall be set to the time the DENM message is generated or updated. **Value:** Set automatically
termination	Optional	C-ITS service specific
eventPosition	Mandatory	In the I2V use-case scenario, the DF eventPosition is used to locate lane or carriageway blockings or hazardous locations. It represents the position where the physical blockage on the lane (including hard shoulder) or the carriageway or the hazardous location starts. The accuracy should be at lane level, but must be at least at carriageway level. Altitude and confidence DEs can be used or set to the values

Name	Use	Usage
		corresponding with 'unavailable'.
relevanceDistance	Optional	Optional
relevanceTrafficDirection	Mandatory	**Content:** Fixed value. For highways this value is set to 1 (upstream traffic). This DF indicates for which traffic direction the message is relevant (from the perspective of the eventPosition).
validityDuration	Mandatory	Events are represented by DEN messages. The duration of a singular DENM is based on the (configurable) value of 'validityDuration'. As long as an event is valid for the road operator, it will be continuously sent (using DENM repetition) and updated (using DENM update, renewing 'validityDuration', 'detectionTime' and 'referenceTime' in the process). A message update will be triggered by 'validityDuration' falling below a certain (also configurable) threshold. If the event is no longer valid, it is either timed out or actively cancelled (DENM cancellation). **Content:** The DE validityDuration is set to a fixed value. **Value:** C-ITS service specific.
TransmissionInterval	Not used	Not used
stationType	Mandatory	**Content:** Fixed value, set to 15 (roadSideUnit). This is true for fixed and mobile roadside C-ITS stations. The value can be 9 (trailer) or 10 (specialVehicles) in the case of road operator vehicles. **Value:** Set to 9, 10 or 15.
Situation container	Mandatory	
informationQuality	Mandatory	Information quality is the likelihood of occurrence, in a range of 0 to 7. Values: risk (2), probable (4), certain (6) If (0) is received, it should be rejected; if (7) is received, it should be considered as certain.
eventType	Mandatory	Combination of DE causeCode and DE subCauseCode. C-ITS service specific.
linkedCause	Optional	Possibility of linking the current message to a set of causeCode / subCauseCode (similar to eventType) to provide further information.
eventHistory	Optional	**Content:** This profile optionally uses this DE when the endpoint of the physical blockage can be determined. If so, it describes the start of a blockage to the end of the blockage, or to the start of a new

Name	Use	Usage
		blockage (another DENM). In this context, the eventPoint values are provided without corresponding eventDeltaTime, since the points describe a geospatial extent and not a trajectory. The DE informationQuality in the eventHistory will be set to the same value as the above-specified informationQuality of the whole DENM. Where map projections are used, these shall refer to points at the middle of the lane or carriageway. Maximum deviation between reality and map projections shall not exceed a quarter of the width of the carriageway.
Location container	Optional	
eventSpeed	Optional	This DF shall only be provided in case of a moving event, if available. In case of static events it shall not be provided.
eventPositionHeading	Optional	Heading information will be provided only for moving events via eventPositionHeading. Stationary DENM-based events will not use this DF.
traces	Mandatory	The first trace point in the message is the point closest to the event position. This point is in the middle of the lane or carriageway upstream from the event position, considering the curvature of the road. It is coded as an offset or delta position about the event position. Additional trace points are defined as offsets or delta positions with respect to their previous trace points. The trace points will be listed in upstream order, thus also defining the event heading. Up to seven traces can be present. When map projections are used, these shall refer to points in the middle of the lane or carriageway. Maximum deviation between reality and map projections shall not exceed a quarter of the width of the carriageway.
roadType	Optional	Optional
Alacarte container	Optional	
lanePosition	Optional	C-ITS service specific.
impactReduction	Not used	Not used
externalTemperature	Not used	Not used
lightBarSirenInUse	Not used	Not used

Table 4: DENM elements specific to roadworks warnings

Name	Use	Usage
Alacarte container	Optional	
lanePosition	Optional	optional
closedLanes	Optional	The lanes are counted from the inside border of the road, excluding the hard shoulder. This DF consists of drivingLaneStatus and hardShoulderStatus.
speedLimit	Optional	optional
recommendedPath	Optional	optional
startingPointSpeedLimit	Optional	optional
trafficFlowRule	Optional	optional passToRight(2) or passToLeft(3) are generally supported in all C-ITS service scenarios.
referenceDenms	Optional	Road works warning DENMs belonging to the same roadwork situation will be linked in the central C-ITS station by listing all actionIDs belonging together in the referenceDenms data element of each message.

3.7.2. *IVI Service*

The IVI service uses the services provided by the protocol entities of the ITS networking and transport layer to disseminate IVIM.

An IVIM supports mandatory and advisory road signage such as contextual speeds and roadworks warnings. IVIM provides information of physical road signs such as static or variable road signs, virtual signs or roadworks.

The IVI service instantiated in a C-ITS station shall provide either the transmission or the reception service.

The IVI service generates four types of IVIM:

- new IVIMs;
- update IVIMs;
- cancellation IVIMs;
- negation IVIMs.

(159) The IVIM header shall be as specified in [TS 102 894-2].

(160) The data elements of the IVIM message payload are defined in [ISO/TS 19321].

(161) IVIM data elements, IVIM data frames and service parameters shall be set in accordance with Table 5.

Table 5

Name	Use	Usage

Name	Use	Usage
IVI management container	Mandatory	
serviceProviderId	Mandatory	serviceProviderID consists of data elements ‘countryCode’ and ‘providerIdentifier’. countryCode is a bitstring in line with [ISO 3166-1]. For Austria, for example, the bitstring stands for ‘AT’ (bitstring code: A (11000) and T (00001) 1100000001 in line with [ISO 14 816]). Together with iviIdentificationNumber, this is the unique identifier for messages for the receiving vehicle C-ITS station.
iviIdentificationNumber	Mandatory	This DE is the identifier of the IVI structure, as assigned by the service provider. This component serves as the ID of the message per serviceProvider and can be used by other related messages as a reference.
timestamp	Mandatory	This DE is the timestamp representing the time at which the IVI message is generated or when the content of the messages was last changed.
validFrom	Mandatory	This component may hold the start time of the validity period of the message. If start time is not relevant or unknown to the system, validFrom is not present or is equal to timestamp.
validTo	Mandatory	This DE shall always be used to determine the validity. An update shall be sent before the message times out. Value: set by application Default validity period is defined by the road operator.
connectedIviStructures (1..8)	Not used	Not used.
iviStatus	Mandatory	This component holds the status of the IVI structure. This can be set to new(0), update(1), cancellation(2) or negation(3). It is used for message handling.
Geographical location container (GLC)	Mandatory	
referencePosition	Mandatory	This DE is used as a reference point for all zones in the GLC. The reference point for IVI is the middle of the carriageway, at a gantry, and is the first point of zone definitions for relevance zones and detection zones. The altitude may be set to unavailable if unknown. If the altitude is provided, it is the altitude of the road. Value: set by application
referencePositionTime	Not used	Not used.
referencePositionHeading	Not used	Not used
referencePositionSpeed	Not used	Not used.

Name	Use	Usage
GlcPart	**Mandatory**	parts (1..16). Up to 16 parts can be defined in each GLC. The GLC contains at least two zones: one for relevance and one for detection. Value: set by application
zoneId	Mandatory	At least one detection zone and one relevance zone shall be provided for each message.
laneNumber	Optional	Mandatory if single lanes are described in this location container. Default is absent (no lane information).
zoneExtension	Not used	Not used.
zoneHeading	Mandatory	Mandatory
zone	Mandatory	Definition of a zone using the DF zone consisting of either a chosen DF segment, DF polygonalLine or DF computedSegment. The segment option shall be used with polygonalLine as a line (constructed with deltaPosition as for DENM traces) and with laneWidth optionally (used only where a single lane is referenced within the zone).
IVI application container	Mandatory	
detectionZoneIds	Mandatory	List of identifier(s) of the definition(s) of the detection zone(s), using the DE Zid (1..8)
its-Rrid	Not used	Not used.
relevanceZoneIds	Mandatory	List of identifier(s) of the definition(s) of the relevance zone(s) to which the IVI container applies, using the DE Zid (1..8)
direction	Mandatory	Direction of relevance in relation to the direction (implicitly) defined by the zone using the DE direction. Always set to sameDirection(0).
driverAwarnessZoneIds	Not used	Not used.
minimumAwarenessTime	Not used	Not used.
applicableLanes (1..8)	Optional	List of identifiers of the lane(s) to which the IVS container applies using the DE LanePosition (1..8).
iviType	Mandatory	Provides the type of IVI (e.g. immediate danger message, regulatory message, traffic information message) to allow for classification and prioritisation of IVI at the receiving C-ITS station.
iviPurpose	Not used	Not used.
laneStatus	Optional	Indicates the lane status (e.g. open, closed, mergeL, mergeR) of the applicableLanes.
completeVehicleCharacteristics	Optional	completeVehicleCharacteristics shall contain the definition of the characteristics of the vehicles to which an application container is applicable. The component ‘train’ (if present)

Name	Use	Usage
		shall contain the characteristics applicable to the entire vehicle train.
driverVehicleCharacteristics	Not used	Not used.
layoutId	Not used	Not used.
preStoredLayoutId	Not used	Not used.
roadSignCodes	Mandatory	It shall contain the definition of the road sign code. It allows different options pointing to different pictogram catalogues. This component specifies which road signs are applicable for a relevance zone. Road sign codes are dependent on the referenced classification scheme. Additional attributes to the road sign code can be added as provided by the options. List of 1..4 of RSCode
RSCode	**Mandatory**	It contains layoutComponentId and a code.
layoutComponentId	Not used	This data frame can be used to associate RSCode to the layout component of referenced layout.
code	Mandatory	For signcoding [ISO/TS 14 823] shall be used.
ISO 14823Code	Mandatory	For signcoding, [ISO/TS 14 823] shall be used. This data frame includes several DFs and DEs. It includes pictogramCode (countryCode, serviceCategorycode and pictogramCategoryCode). The attributes SET (section) and NOL (number of lane) are not supported, because they duplicate information that is already supported in the application container.
extraText ((1..4),...)	Optional	List of text lines associated with the ordered list of road sign codes. Each piece contains language code plus extra, limited-size text in the selected language using the DF text. Note: This DF can be safely overloaded to include more lines of text.

3.7.3. Road Lane Topology (RLT) service

The RLT service uses the services provided by the protocol entities of the ITS networking & transport layer to disseminate RLT.

It includes the lane topology for vehicles, bicycles, parking, public transport and the paths for pedestrian crossings, for example, and the permissible manoeuvres within an intersection area or a road segment. In future enhancements, the digital map will include additional topology descriptions such as traffic roundabouts.

(162) MAPEM headers shall be as specified in [ETSI TS 102 894-2].

(163) MAPEM data elements, MAPEM data frames and service parameters shall be set in accordance with Table 6.

Table 6: MAPEM data elements

Level	Name	Type	Use	Usage
*	mapData	DF	Mandatory	
**	timeStamp	DE	Not used	Not used.
**	msgIssue Revision	DE	Mandatory	Mandatory and set to 0. As defined in [ISO TS 19091].
**	layerType	DE	Not used	Not used.
**	layerID	DE	Optional	Optional. As defined in [ISO TS 19091].
**	intersections (1..32)	DF	Mandatory	IntersectionGeometryList::= SEQUENCE (SIZE(1..32)) OF IntersectionGeometry (see Table 6.1) Mandatory for Traffic Light Manouvre (TLM)/RLT C-ITS services.
**	roadSegments (1..32)	DF	Not used	Not used. Data elements are not further profiled.
**	dataParameters	DF	Optional	Optional.
***	processMethod	DE	Not used	Not used.
***	processAgency	DE	Optional	Optional.
***	lastCheckedDate	DE	Optional	Optional, as yyyy-mm-dd
***	geoidUsed	DE	Not used	Not used.
**	restriction List (1..32)	DF	Optional	RestrictionClassList::= SEQUENCE (SIZE(1..254)) OF RestrictionClassAssignment (see Table 6.3). Optional.
**	regional	DE	Not used	REGION.Reg-MapData. Not used.

Table 6.1: IntersectionGeometryList -> Intersection Geometry

Level	Name	Type	Use	Usage
*	intersectionGeometry	DF	Mandatory	Mandatory if ’intersections‘ is used.
**	name	DE	Optional	Optional. Typically human-readable and recognisable by road authority.
**	id	DF	Mandatory	(IntersectionReferenceID) Mandatory. Must be the same as in the SPATEM. The combination of region and id must be unique within a country.

***	region	DE	Optional	Optional.
***	id	DE	Mandatory	Mandatory.
**	revision	DE	Mandatory	Mandatory. The revision number must be increased by one each time the MapData of this intersection changes. The revision numbers of SPATEM and MAPEM must be the same, to indicate that the right MAPEM revision is used. As defined in [ISO TS 19091].
**	refPoint	DF	Mandatory	Mandatory.
***	lat	DE	Mandatory	Mandatory.
***	long	DE	Mandatory	Mandatory.
***	elevation	DE	Not used	Not used. Replaced by regional Reg-Position3D.
***	regional	DF	Optional	REGION.Reg-Position3D. Optional. When given, provides altitude.
****	altitude	DF	Mandatory	Mandatory. Consists of altitudeValue and altitudeConfidence
*****	altitudeValue	DE	Mandatory	Mandatory.
*****	altitudeConfidence	DE	Optional	Mandatory; when not available set to (15) = unavailable.
**	laneWidth	DE	Optional	Optional.
**	speedLimits (1..9)	DF	Optional	SpeedLimitList::= SEQUENCE (SIZE(1..9)) OF RegulatorySpeedLimit (see Table 6.2). Optional.
**	laneSet (1..255)	DF	Mandatory	LaneList::= SEQUENCE (SIZE(1..255)) OF GenericLane (see Table 6.4). Mandatory.
**	preemptPriorityData (1..32)	DF	Not used	Not used. Data elements are not further profiled.
**	Regional	DF	Not used	REGION.Reg- IntersectionGeometry). Not used.

Table 6.2: SpeedLimitList -> RegulatorySpeedLimit

Level	Name	Type	Use	Usage
*	regulatory SpeedLimit	DF	Mandatory	Mandatory if ‘speedLimits’ is used.
**	type	DE	Mandatory	Mandatory.

**	speed	DE	Mandatory	Mandatory.

Table 6.3: RestrictionClassList -> RestrictionClassAssignment

Level	Name	Type	Use	Usage
*	restriction ClassAssignment	DF	Mandatory	Mandatory if restrictionList is used.
**	id	DE	Mandatory	Mandatory.
**	users	DF	Mandatory	RestrictionUserTypeList::= SEQUENCE (SIZE(1..16)) OF RestrictionUserType Mandatory.
***	restrictionUserType	DF	Mandatory	
****	basicType	DE	Optional	Used.
****	regional (1..4)	DF	Optional	REGION.Reg-RestrictionUserType-addGrpC. Optional to provide emission restrictions.
*****	emission	DE	Optional	Optional.

Table 6.4: LaneList -> GenericLane

Level	Name	Type	Use	Usage
*	genericLane	DF	Mandatory	Mandatory if 'laneSet' is used.
**	laneID	DE	Mandatory	Mandatory.
**	name	DE	Optional	Optional.
**	ingressApproach	DE	Optional	Optional. If used, ingress and egress approaches of the same arm have the same ApproachID.
**	egressApproach	DE	Optional	Optional. If used, ingress and egress approaches of the same arm have the same ApproachID.
**	laneAttributes	DF	Mandatory	Mandatory.
***	directional Use	DE	Mandatory	Mandatory.
***	sharedWith	DE	Mandatory	Mandatory. With bits as defined: overlappingLaneDescriptionProvided(0) multipleLanesTreatedAsOneLane(1) -- not permitted in profile, as all lanes must be described. otherNonMotorizedTrafficTypes(2) -- e.g. horse-drawn individualMotorizedVehicleTraffic(3) -- passenger cars busVehicleTraffic(4)

				taxiVehicleTraffic(5)
				pedestriansTraffic(6)
				cyclistVehicleTraffic(7)
				trackedVehicleTraffic(8) pedestrianTraffic(9) -- use 6 instead (error)

***	laneType	DF	Mandatory	Mandatory. Used in this profile: vehicle crosswalk bikeLane trackedVehicle -- see [ISO TS 19091] for pedestrian crossing examples.
****	Vehicle	DE	Optional	Optional (choice).
****	crosswalk	DE	Optional	Optional (choice).
****	bikeLane	DE	Optional	Optional (choice).
****	sidewalk	DE	Not used	Not used.
****	median	DE	Not used	Not used.
****	striping	DE	Not used	Not used.
****	trackedVehicle	DE	Optional	Optional (choice).
****	parking	DE	Not used	Not used.
***	regional	DF	Not used	Reg-laneAttributes. Not used.
**	maneuvers	DE	Not used	Not used.
**	nodeList	DF	Mandatory	Mandatory.
***	nodes (2..63)	DF	Mandatory	NodeSetXY::= SEQUENCE (SIZE(2..63)) OF NodeXY (see Table 6.5) Mandatory if ‘nodeList’ is used. Recommended use for curved lanes is to add an additional node when the centre line of the GenericLane deviates more than 0.5 m from the actual centre line.
***	computed	DF	Not used	Not used.
**	connectsTo (1..16)	DF	Optional	ConnectsToList::= SEQUENCE (SIZE(1..16)) OF Connection (see Table 6.6). Optional. For example for egress lane(s) not managed by a traffic light.
**	overlays	DF	Not used	Not used.
**	regional	DF	Not used	REGION-Reg-GenericLane. Not used (until upcoming release of [ISO TS 19091]). To provide ConnectionTrajectory-

				addGrpC. Relevant for use-case scenario safe intersection manoeuvre.

Table 6.5: NodeSetXY -> NodeXY

Level	Name	Type	Use	Usage
*	nodeXY	DF	Mandatory	Mandatory if ‘nodes’ is used.
**	delta	DF	Mandatory	Mandatory.
***	node-XY1	DF	Optional	Optional (choice). DF composed with X and Y, both mandatory.
***	node-XY2	DF	Optional	Optional (choice). DF composed with X and Y, both mandatory.
***	node-XY3	DF	Optional	Optional (choice). DF composed with X and Y, both mandatory.
***	node-XY4	DF	Optional	Optional (choice). DF composed with X and Y, both mandatory.
***	node-XY5	DF	Optional	Optional (choice). DF composed with X and Y, both mandatory.
***	node-XY6	DF	Optional	Optional (choice). DF composed with X and Y, both mandatory.
***	node-LatLon	DF	Not used	Not used for intersections. Use for motorways, for example, is acceptable.
***	regional	DF	Not used	REGION.Reg-NodeOffsetPointXY. Not used.
**	attributes	DF	Optional	This DE provides any optional attributes that are needed. This includes changes to the current lane width and elevation. All attributes are provided in the order of the nodes (as opposed to the driving direction). Also left/right indications by attributes must be interpreted on the basis of the order of the nodes.
***	localNode	DF	Optional	NodeAttributeXYList::=

	(1..8)			SEQUENCE (SIZE(1..8)) OF NodeAttributeXY Optional. Subject to case. Stopline is mandatory when present in the field.
****	nodeAttributeXY	DE	Mandatory	Mandatory if localNode is used.
***	disabled (1..8)	DF	Optional	SegmentAttributeXYList::= SEQUENCE (SIZE(1..8)) OF SegmentAttributeXY Optional. Subject to case.
****	segmentAttributeXY	DE	Mandatory	Mandatory if disabled is used.
***	enabled (1..8)	DF	Optional	SegmentAttributeXYList::= SEQUENCE (SIZE(1..8)) OF SegmentAttributeXY Optional. Subject to case.
****	segmentAttributeXY	DE	Mandatory	Mandatory if enabled is used.
***	data	DF	Optional	Optional.
****	pathEndPointAngle	DE	Not used	Not used.
****	pathEndPointAngle	DE	Not used	Not used.
****	laneCrownPointCenter	DE	Not used	Not used.
****	laneCrownPointLeft	DE	Not used	Not used.
****	laneCrownPointRight	DE	Not used	Not used.
****	laneAngle	DE	Not used	Not used.
****	speedLimits (1..9)	DE	Optional	SpeedLimitList::= SEQUENCE (SIZE(1..9)) OF RegulatorySpeedLimit (see Table 6.2). Optional (choice).
****	regional	DF	Not used	REGION.Reg-LaneDataAttribute. Not used.
***	dWidth	DE	Optional	Optional.
***	dElevation	DE	Optional	Optional.
***	regional	DF	Not used	REGION.Reg-NodeAttributeSetXY.

				Not used.

Table 6.6: ConnectsToList -> Connection

Level	Name	Type	Use	Usage
*	connection	DF	Optional	Mandatory if ‘connectsTo’ is used.
**	connectingLane	DF	Mandatory	Mandatory.
***	lane	DE	Mandatory	Mandatory.
***	maneuver	DE	Optional	Optional.
**	remoteIntersection	DF	Optional	Optional. Only used if the referenced intersection is part of the same MAPEM.
***	Region	DE	Optional	Optional.
***	Id	DE	Mandatory	Mandatory.
**	signalGroup	DE	Optional	Optional, as not all connections may have related signalgroups. However, for connections controlled by a traffic light, the signalgroup must be set.
**	userClass	DE	Optional	Optional.
**	connectionID	DE	Mandatory	Mandatory.

3.7.4. TLM service

The TLM service uses the services provided by the protocol entities of the ITS networking & transport layer to disseminate TLM.

It includes safety-related information to help traffic participants (vehicles, pedestrians, etc.) to execute safe manoeuvres in an intersection area. The goal is to enter and exit an intersection ‘conflict area’ in a controlled way. The TLM service provides real-time information about the operational states of the traffic light controller, the current signal state, the residual time of the state before changing to the next state, and permissible manoeuvres, and helps with crossing.

(164) SPATEM headers shall be as specified in [TS 102 894-2].

(165) SPATEM data elements, data frames and service parameters shall be set in accordance with Table 7.

Table 7: SPATEM data elements

Level	Name	Type	Use	Usage
*	Spat	DF	Mandatory	
**	timeStamp	DE	Optional	Not used, but kept optional.
**	name	DE	Optional	Not used, but kept optional.

**	Intersections (1..32)	DF	Mandatory	IntersectionStateList::= SEQUENCE (SIZE(1..32)) OF IntersectionState (see Table 7.1). Mandatory
**	regional (1..4)	DF	Not used	REGION.Reg-SPAT. Not used.

Table 7.1: IntersectionStateList -> IntersectionState

Level	Name	Type	Use	Usage
*	intersectionState	DF	Mandatory	
**	name	DE	Optional	Used, but kept optional. Based on a numbering scheme used by the road authority.
**	id	DF	Mandatory	(IntersectionReferenceID) Mandatory. Must be the same as in the MAPEM. The combination of region and ID must be unique within a country.
***	region	DE	Optional	Optional.
***	id	DE	Mandatory	Mandatory.
**	revision	DE	Mandatory	Mandatory. The revision number must be increased by one each time the MapData of this intersection changes. The revision numbers of SPATEM and MAPEM must be the same, to indicate that the right MAPEM revision is used. As defined in [ISO TS 19091].
**	status	DE	Mandatory	Mandatory. Typically used, on the basis of EN 12675, are: • manualControlIsEnabled(0); • fixedTimeOperation(5); • trafficDependentOperation(6); • standbyOperation(7); • failureMode(8).
**	moy	DE	Mandatory	Mandatory. Also used to validate the reference time of the TimeMarks.
**	timeStamp	DE	Mandatory	Mandatory.
**	enabledLanes	DF	Optional	Mandatory if the revocableLane bit is used in any of the lane descriptions; otherwise not used.
**	states	DF	Mandatory	MovementList::= SEQUENCE (SIZE(1..255)) OF

	(1..16)			MovementState (see Table 7.2). Mandatory.
**	maneuverAssistList (1..16)	DF	Not used	ManeuverAssistList::= SEQUENCE (SIZE(1..16)) OF ConnectionManeuverAssist (see Table 7.5). Not used, therefore not further profiled on this level.
**	Regional (1..4)	DF	Optional	REGION.Reg-IntersectionState. Optional, to ensure interoperability with existing public transport prioritisation systems.

Table 7.2: MovementList -> MovementState

Level	Name	Type	Use	Usage
*	movementState	DF	Mandatory	Mandatory if 'states' is used.
**	movementName	DE	Optional	Optional.
**	signalGroup	DE	Mandatory	Mandatory.
**	state-time- speed	DF	Mandatory	MovementEventList::= SEQUENCE (SIZE(1..16)) OF MovementEvent. Mandatory (1-16). (see Table 7.3).
**	maneuverAssistList (1..16)	DF	Optional	ManeuverAssistList::= SEQUENCE (SIZE(1..16)) OF ConnectionManeuverAssist (see Table 7.5). Optional.
**	regional (1..4)	DF	Not used	REGION.Reg-MovementState. Not used.

Table 7.3: MovementEventList -> MovementEvent

Level	Name	Type	Use	Usage
*	movementEvent	DF	Mandatory	Mandatory if 'state-time-speed' is used.

**	eventState	DE	Mandatory	Mandatory and defined as follows:
				(0) unavailable (unknown or error);
				(1) dark (not used in EU);
				(2) stop-then-Proceed (e.g. red light combined with road sign with green arrow for turn movement);
				(3) stop-and-remain (e.g. red light);
				(4) pre-Movement (e.g. red/amber as used in some EU countries before green signal);

				(5) permissive-Movement-Allowed (e.g. green ‘full ball’ light, with potential conflicting traffic, especially when turning); (6) protected-Movement-Allowed (e.g. green ‘arrow’ light, with no conflicting traffic or pedestrians while crossing the conflict area); (7) permissive clearance (e.g. amber ‘full ball’ light, prepare to stop. Used after a ‘green’ signal state); (8) protected clearance (e.g. amber ‘arrow’ light, directional prepare to stop. Used after a ‘green arrow’ signal state); (9) caution-Conflicting-Traffic (e.g. amber light blinking; proceed with caution, conflicting traffic may be present in the intersection conflict area).
**	timing	DF	Optional	Optional. For example, timing data may not be available when ‘status’ is 0, 1 or 9. All TimeMarks are defined as an offset to the UTC full hour (see [ISO TS 19091]) and not for functional safety, but informative related to signal timing. likelyTime with confidence or minEndTime with maxEndTime are both measures for probability and can be used interchangeably subject to availability.
***	startTime	DE	Not used	Not used.
***	minEndTime	DE	Mandatory	Mandatory. Pre-configured or calculated value with high probability, but sometimes not available (36001). In cases of fixed time control, for example, identical to maxEndTime, which indicates high probability.
***	maxEndTime	DE	Mandatory	Mandatory. Pre-configured or calculated value with high probability, but sometimes not available (36001). In cases of fixed time control, for example, identical to minEndTime, which indicates high probability.
***	likelyTime	DE	Optional	Optional.
***	confidence	DE	Optional	Mandatory if likelyTime is provided. The definition of ‘confidence’ in the base standard is not useable. Instead, confidence is defined by the standard deviation (sigma) of the likelyTime in seconds. The value provided by this data element, between 0 and 15, represents 1 sigma (rounded). 15 = unknown. Hence, the conversion table with probabilities as provided in SAE J2735 is

				not used. Assuming normal distribution and a standard deviation of 3.6 seconds, likelyTime is: • within 26 and 34 seconds (1 sigma), with 68.27 % probability; • within 22 and 38 seconds (2 sigma), with 95.44 % probability; • within 18 and 42 seconds (3 sigma), with 99.73 % probability.
***	nextTime	DE	Optional	Optional.
**	speeds (1..16)	DF	Optional	AdvisorySpeedList::= SEQUENCE (SIZE(1..16)) OF AdvisorySpeed (see Table 7.4). Optional.
**	regional (1..4)	DF	Optional	REGION.Reg-MovementEvent, Optional.

Table 7.4: AdvisorySpeedList -> AdvisorySpeed

Level	Name	Type	Use	Usage
*	advisorySpeed	DF	Mandatory	Mandatory if ‘speeds’ is used.
**	type	DE	Mandatory	Mandatory. greenwave(1) = speed for a sequence of coordinated intersections (repeated at each intersection). ecoDrive(2) = speed for current intersection. transit(3) = restricted to specific vehicle type.
**	speed	DE	Optional	Optional.
**	confidence	DE	Not used	Not used.
**	distance	DE	Optional	Optional. Not used for greenwave(1). In other cases, distance is specified upstream from the stop bar along the ingressing lane.
**	class	DE	Optional	Optional.
**	regional (1..4)	DF	Not used	REGION.Reg-AdvisorySpeed. Not used.

Table 7.5: ManeuverAssistList -> ConnectionManeuverAssist

Level	Name	Type	Use	Usage

*	connection ManeuverAssist	DF	Mandatory	Mandatory if ‘maneuverAssistList’ is used.
**	connectionID	DE	Mandatory	Mandatory.
**	queueLength	DE	Optional	Optional.
**	availableStorageLength	DE	Not used	Not used.
**	waitOnStop	DE	Not used	Not used.
**	pedBicycleDetect	DE	Not used	Not used.
**	regional (1..4)	DF	Not used	REGION.Reg-ConnectionManeuverAssist. Not used.

EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 3

ANNEX

to the

Commission Delegated Regulation

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

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

TABLE OF CONTENTS

1. Introduction ... 9

1.1. Overview and scope of this policy ... 9

1.2. Definitions and acronyms ... 11

1.3. PKI participants ... 13

1.3.1. Introduction ... 13

1.3.2. C-ITS certificate policy authority ... 16

1.3.3. Trust list manager ... 17

1.3.4. Accredited PKI auditor ... 17

1.3.5. C-ITS point of contact (CPOC) ... 17

1.3.6. Operational roles ... 18

1.4. Certificate usage ... 18

1.4.1. Applicable domains of use ... 18

1.4.2. Limits of responsibility ... 19

1.5. Certificate policy administration ... 19

1.5.1. Updating of CPSs of CAs listed in the ECTL ... 19

1.5.2. CPS approval procedures ... 20

2. Publication and repository responsibilities ... 20

2.1. Methods for the publication of certificates information ... 20

2.2. Time or frequency of publication ... 21

2.3. Repositories ... 21

2.4. Access controls on repositories ... 21

2.5. Publication of certificate information ... 22

2.5.1. Publication of certificate information by the TLM ... 22

2.5.2. Publication of certificate information by CAs ... 22

3. Identification and authentication ... 23

3.1. Naming ... 23

3.1.1. Types of name ... 23

3.1.1.1. Names for TLM, root CAs, EAs, AAs ... 23

3.1.1.2. Names for end-entities ... 23

3.1.1.3. Identification of certificates ... 23

3.1.2. Need for names to be meaningful ... 23

3.1.3. Anonymity and pseudonymity of end-entities ... 23

3.1.4. Rules for interpreting various name forms ... 23

3.1.5. Uniqueness of names ... 24

3.2. Initial identity validation 24
3.2.1. Method to prove possession of private key 24
3.2.2. Authentication of organisation identity 24
3.2.2.1. Authentication of root CAs' organisation identity 24
3.2.2.2. Authentication of TLM organisation identity 25
3.2.2.3. Authentication of sub-CAs organisation identity 25
3.2.2.4. Authentication of end-entities' subscriber organisation 26
3.2.3. Authentication of individual entity 26
3.2.3.1. Authentication of TLM/CA individual entity 26
3.2.3.2. Authentication of C-ITS stations' subscriber identity 27
3.2.3.3. Authentication of C-ITS stations' identity 27
3.2.4. Non-verified subscriber information 27
3.2.5. Validation of authority 27
3.2.5.1. Validation of TLM, root CA, EA, AA 27
3.2.5.2. Validation of C-ITS station subscribers 28
3.2.5.3. Validation of C-ITS stations 28
3.2.6. Criteria for interoperation 28
3.3. Identification and authentication for re-key requests 28
3.3.1. Identification and authentication for routine re-key requests 28
3.3.1.1. TLM certificates 28
3.3.1.2. Root CA certificates 28
3.3.1.3. EA/AA certificate renewal or re-keying 28
3.3.1.4. End-entities' enrolment credentials 29
3.3.1.5. End-entities' authorisation tickets 29
3.3.2. Identification and authentication for re-key requests after revocation 29
3.3.2.1. CA certificates 29
3.3.2.2. End-entities' enrolment credentials 29
3.3.2.3. End-entities' authorisation requests 29
3.4. Identification and authentication for revocation request 29
3.4.1. Root CA/EA/AA certificates 29
3.4.2. C-ITS station enrolment credentials 30
3.4.3. C-ITS station authorisation tickets 30
4. Certificate Life-cycle operational requirements 30
4.1. Certificate application 30
4.1.1. Who can submit a certificate application 30

4.1.1.1. Root CAs 30
4.1.1.2. TLM 31
4.1.1.3. EA and AA 31
4.1.1.4. C-ITS station 31
4.1.2. Enrolment process and responsibilities 31
4.1.2.1. Root CAs 31
4.1.2.2. TLM 32
4.1.2.3. EA and AA 32
4.1.2.4. C-ITS station 32
4.2. Certificate application processing 33
4.2.1. Performing identification and authentication functions 33
4.2.1.1. Identification and authentication of root CAs 33
4.2.1.2. Identification and authentication of the TLM 33
4.2.1.3. Identification and authentication of EA and AA 33
4.2.1.4. Identification and authentication of EE subscriber 34
4.2.1.5. Authorisation tickets 34
4.2.2. Approval or rejection of certificate applications 34
4.2.2.1. Approval or rejection of root CA certificates 34
4.2.2.2. Approval or rejection of TLM certificate 34
4.2.2.3. Approval or rejection of EA and AA certificates 34
4.2.2.4. Approval or rejection of EC 34
4.2.2.5. Approval or rejection of AT 35
4.2.3. Time to process the certificate application 35
4.2.3.1. Root CA certificate application 35
4.2.3.2. TLM certificate application 35
4.2.3.3. EA and AA certificate application 35
4.2.3.4. EC application 35
4.2.3.5. AT application 35
4.3. Certificate issuance 35
4.3.1. CA actions during certificate issuance 35
4.3.1.1. Root CA certificate issuance 35
4.3.1.2. TLM certificate issuance 36
4.3.1.3. EA and AA certificate issuance 36
4.3.1.4. EC issuance 36
4.3.1.5. AT issuance 36

4.3.2. CA’s notification to subscriber of issuance of certificates.. 36
4.4. Certificate acceptance 37
4.4.1. Conducting certificate acceptance.. 37
4.4.1.1. Root CA 37
4.4.1.2. TLM 37
4.4.1.3. EA and AA.. 37
4.4.1.4. C-ITS station 37
4.4.2. Publication of the certificate 37
4.4.3. Notification of certificate issuance.. 37
4.5. Key pair and certificate usage 37
4.5.1. Private key and certificate usage.. 37
4.5.1.1. Private key and certificate usage for TLM.. 37
4.5.1.2. Private key and certificates usage for root CAs 37
4.5.1.3. Private key and certificate usage for EAs and AAs 37
4.5.1.4. Private key and certificate usage for end-entity.. 38
4.5.2. Relying party public key and certificate usage 38
4.6. Certificate renewal 38
4.7. Certificate re-key.. 38
4.7.1. Circumstances for certificate re-key 38
4.7.2. Who may request re-key 38
4.7.2.1. Root CA 38
4.7.2.2. TLM 38
4.7.2.3. EA and AA.. 38
4.7.2.4. C-ITS station 39
4.7.3. Re-keying process 39
4.7.3.1. TLM certificate 39
4.7.3.2. Root CA certificate 39
4.7.3.3. EA and AA certificates 39
4.7.3.4. C-ITS station certificates.. 40
4.8. Certificate modification 40
4.9. Certificate revocation and suspension... 40
4.10. Certificate status services... 40
4.10.1. Operational characteristics.. 40
4.10.2. Service availability.. 40
4.10.3. Optional features 40

4.11. End of subscription 40
4.12. Key escrow and recovery 40
4.12.1. Subscriber 40
4.12.1.1. Which key pair can be escrowed 40
4.12.1.2. Who can submit a recovery application 40
4.12.1.3. Recovery process and responsibilities 40
4.12.1.4. Identification and authentication 40
4.12.1.5. Approval or rejection of recovery applications 40
4.12.1.6. KEA and KRA actions during key pair recovery 41
4.12.1.7. KEA and KRA availability 41
4.12.2. Session key encapsulation and recovery policy and practices 41
5. Facility, management and operational controls 41
5.1. Physical controls 41
5.1.1. Site location and construction 41
5.1.1.1. Root CA, CPOC, TLM 41
5.1.1.2. EA/AA 42
5.1.2. Physical access 42
5.1.2.1. Root CA, CPOC, TLM 42
5.1.2.2. EA/AA 43
5.1.3. Power and air conditioning 43
5.1.4. Water exposures 43
5.1.5. Fire prevention and protection 44
5.1.6. Media management 44
5.1.7. Waste disposal 44
5.1.8. Off-site backup 44
5.1.8.1. Root CA, CPOC and TLM 44
5.1.8.2. EA/AA 45
5.2. Procedural controls 45
5.2.1. Trusted roles 45
5.2.2. Number of persons required per task 45
5.2.3. Identification and authentication for each role 46
5.2.4. Roles requiring separation of duties 46
5.3. Personnel controls 47
5.3.1. Qualifications, experience and clearance requirements 47
5.3.2. Background check procedures 47

5.3.3. Training requirements 48
5.3.4. Retraining frequency and requirements 48
5.3.5. Job rotation frequency and sequence 48
5.3.6. Sanctions for unauthorised actions 48
5.3.7. Independent contractor requirements 49
5.3.8. Documentation supplied to personnel 49
5.4. Audit logging procedures 49
5.4.1. Types of event to be recorded and reported by each CA 49
5.4.2. Frequency of processing log 50
5.4.3. Retention period for audit log 50
5.4.4. Protection of audit log 51
5.4.5. Audit log backup procedures 51
5.4.6. Audit collection system (internal or external) 51
5.4.7. Notification to event-causing subject 51
5.4.8. Vulnerability assessment 51
5.5. Record archiving 52
5.5.1. Types of record archived 52
5.5.2. Retention period for archive 53
5.5.3. Protection of archive 53
5.5.4. System archive and storage 53
5.5.5. Requirements for time-stamping of records 54
5.5.6. Archive collection system (internal or external) 54
5.5.7. Procedures to obtain and verify archive information 54
5.6. Key changeover for C-ITS trust model elements 54
5.6.1. TLM 54
5.6.2. Root CA 54
5.6.3. EA/AA certificate 54
5.6.4. Auditor 55
5.7. Compromise and disaster recovery 55
5.7.1. Incident and compromise handling 55
5.7.2. Corruption of computing resources, software and/or data 56
5.7.3. Entity private key compromise procedures 56
5.7.4. Business continuity capabilities after a disaster 56
5.8. Termination and transfer 57
5.8.1. TLM 57

5.8.2. Root CA ... 57
5.8.3. EA/AA ... 58
6. Technical security controls ... 58
6.1. Key-pair generation and installation ... 58
6.1.1. TLM, root CA, EA, AA ... 58
6.1.2. EE — mobile C-ITS station ... 58
6.1.3. EE — fixed C-ITS station ... 59
6.1.4. Cryptographic requirements ... 59
6.1.4.1. Algorithm and key length - signature algorithms ... 59
6.1.4.2. Algorithm and key length - encryption algorithms for enrolment and authorisation 60
6.1.4.3. Crypto-agility ... 61
6.1.5. Secure storing of private keys ... 61
6.1.5.1. Root CA, sub-CA and TLM level ... 61
6.1.5.2. End-entity ... 62
6.1.6. Backup of private keys ... 63
6.1.7. Destruction of private keys ... 63
6.2. Activation data ... 63
6.3. Computer security controls ... 63
6.4. Life-cycle technical controls ... 63
6.5. Network security controls ... 63
7. Certificate profiles, CRL and CTL ... 63
7.1. Certificate profile ... 63
7.2. Certificate validity ... 64
7.2.1. Pseudonym certificates ... 65
7.2.2. Authorisation tickets for fixed C-ITS stations ... 65
7.3. Revocation of certificates ... 65
7.3.1. Revocation of CA, EA and AA certificates ... 65
7.3.2. Revocation of enrolment credentials ... 66
7.3.3. Revocation of authorisation tickets ... 66
7.4. Certificate revocation list ... 66
7.5. European certificate trust list ... 66
8. Compliance audit and other assessments ... 66
8.1. Topics covered by audit and audit basis ... 66
8.2. Frequency of the audits ... 67
8.3. Identity/qualifications of auditor ... 67

8.4. Auditor’s relationship to audited entity 67
8.5. Action taken as a result of deficiency 68
8.6. Communication of results 68
9. Other provisions 68
9.1. Fees 68
9.2. Financial responsibility 69
9.3. Confidentiality of business information 69
9.4. Privacy plan 69
10. References 69

ANNEX III

1. INTRODUCTION

1.1. Overview and scope of this policy

This certificate policy defines the European C-ITS trust model based on public key infrastructure (PKI) within the scope of the overall EU C-ITS security credential management system (EU CCMS). It defines requirements for the management of public key certificates for C-ITS applications by issuing entities and their usage by end-entities in Europe. At its highest level, the PKI is composed of a set of root CAs 'enabled' as a result of the trust list manager (TLM) inserting their certificates in a European certificate trust list (ECTL), which is issued and published by the central entity TLM (see sections 1.2 and 1.3).

This policy is binding on all entities participating in the trusted C-ITS system in Europe. It helps in the assessment of the level of trust that can be established in the received information by any receiver of a message authenticated by an end-entity certificate of the PKI. To allow assessment of trust in the certificates provided by the EU CCMS, it sets out a binding set of requirements for the operation of the central entity TLM and the compilation and management of the ECTL. Consequently, this document governs the following aspects relating to the ECTL:

- identification and authentication of principals obtaining PKI roles for the TLM, including statements of the privileges allocated to each role;
- minimum requirements for local security practices for the TLM, including physical, personnel and procedural controls;
- minimum requirements for technical security practices for the TLM, including computer security, network security and cryptographic module engineering controls;
- minimum requirements for operational practices for the TLM, including registration of new root CA certificates, the temporary or permanent deregistration of existing included root CAs, and the publication and distribution of ECTL updates;
- an ECTL profile, including all mandatory and optional data fields in the ECTL, cryptographic algorithms to be used, the exact ECTL format and recommendations for processing the ECTL;
- ECTL certificate lifecycle management, including distribution of ECTL certificates, activation, expiration and revocation;
- management of the revocation of trust of root CAs where necessary.

Since the trustworthiness of the ECTL does not depend solely on the ECTL itself, but to a large extent also on the root CAs that compose the PKI and their sub-CAs, this policy also sets out minimum requirements, which are mandatory for all participating CA's (root CAs and sub-CAs). The requirement areas are the following:

- identification and authentication of principals obtaining PKI roles (e.g. security officer, privacy officer, security administrator, directory administrator and end-user), including a statement of duties, responsibilities, liabilities and privileges associated with each role;

- key management, including acceptable and mandatory certificate-signing and data-signing algorithms, and certificate validity periods;
- minimum requirements for local security practices, including physical, personnel and procedural controls;
- minimum requirements for technical security practices such as computer security, network security and cryptographic module engineering controls;
- minimum requirements for operational practices of the CA, EA, AA and end-entities, including aspects of registration, de-registration (i.e. de-listing), revocation, key-compromise, dismissal for cause, certificate update, audit practices and non-disclosure of privacy-related information;
- certificate and CRL profile, including formats, acceptable algorithms, mandatory and optional data fields and their valid value ranges, and how verifiers are expected to process certificates;
- regular monitoring, reporting, alerting and restoring duties of the C-ITS trust model entities in order to establish secure operation, including in cases of misbehaviour.

In addition to these minimum requirements, the entities running the root CAs and sub-CAs may decide their own additional requirements and set them out in the relevant certificate practice statements (CPSs), provided they do not contradict the requirements set out in the certificate policy. See section 1.5 for details on how CPSs are audited and published.

The CP also states the purposes for which the root CAs, sub-CAs and their issued certificates may be used. It sets out the liabilities assumed by:

- the TLM;
- each root CA whose certificates are listed in the ECTL;
- the root CA’s sub-CAs (EA and AA);
- each member or organisation responsible for, or operating, one of the C-ITS trust model entities.

The CP also defines mandatory obligations applying to:

- the TLM;
- each root CA whose certificates are listed in the ECTL;
- each sub-CA certified by a root CA;
- all end-entities;
- each member organisation responsible for, or operating, one of the C-ITS trust model entities.

Finally, the CP sets out requirements as regards the documentation of limitations to liabilities and obligations in the CPS of each root CA whose certificates are listed in the ECTL.

This CP is in line with the certificate policy and certification practices framework adopted by the Internet Engineering Task Force (IETF) [3].

1.2. Definitions and acronyms

The definitions in [2], [3] and [4] apply.

AA	authorisation authority
AT	authorisation ticket
CA	certification authority
CP	certificate policy
CPA	C-ITS certificate policy authority
CPOC	C-ITS point of contact
CPS	certificate practice statement
CRL	certificate revocation list
EA	enrolment authority
EC	enrolment credential
ECIES	elliptic curve integrated encryption scheme
EE	end-entity (i.e. C-ITS station)
ECTL	European certificate trust list
EU CCMS	EU C-ITS security credential management system
GDPR	General Data Protection Regulation
HSM	Hardware security module
PKI	public key infrastructure
RA	registration authority
sub-CA	EA and AA
TLM	trust list manager

Glossary

applicant	The natural person or legal entity that applies for (or seeks renewal of) a certificate. Once the initial certificate is created (initialisation), the applicant is referred to as the subscriber. For certificates issued to end-entities, the subscriber (certificate applicant) is the entity that controls or operates/maintains the end-entity to which the certificate is issued, even if the end-entity is sending the actual certificate request.
authorisation authority	In this document, the term 'authorisation authority' (AA) refers not only to the specific function of the AA, but also to the legal and/or operational entity managing it.
certification authority	The root certification authority, enrolment authority and authorisation authority are cumulatively referred to as the certification authority (CA).
C-ITS trust model	The C-ITS trust model is responsible for establishing a relationship of trust between C-ITS stations. It is implemented through the use of a PKI composed of root CAs, the CPOC, TLM, EAs, AAs and a secure network.
crypto-agility	The capability of the C-ITS trust model entities to adapt the CP to changing environments or to new future requirements, e.g. by a change of cryptographic algorithms and key length over time
cryptographic module	A secure hardware-based element within which keys are generated and/or stored, random numbers are generated and data are signed or encrypted.
enrolment authority	In this document, the term 'enrolment authority' (EA) refers not only to the specific function of the EA, but also to the legal and/or operational entity managing it.
PKI participants	Entities of the C-ITS trust model, i.e. the TLM, root CAs, EAs, AAs and C-ITS stations.
re-keying	This subcomponent is used to describe certain elements relating to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key as described in [3].
repository	The repository used for storing the certificates and information on certificates provided by the entities of the C-ITS trust model, as defined in section 2.3.
root certification authority	In this document, the term 'root certification authority' (CA) refers not only to the specific function of the CA, but also to the legal and/or operational entity managing it.
subject	The natural person, device, system, unit or legal entity identified in a certificate as the subject, i.e. either the subscriber or a device under the control and operation of the subscriber.
subscriber	A natural person or legal entity to which a certificate is issued and which is legally bound by a subscriber or terms of use agreement.
subscriber agreement	An agreement between the CA and the applicant/subscriber that specifies the rights and responsibilities of the parties.

1.3. PKI participants

1.3.1. Introduction

PKI participants play a role in the PKI defined by the present policy. Unless explicitly it is prohibited, a participant can assume multiple roles at the same time. It may be prohibited from assuming specific roles at the same time in order to avoid conflicts of interest or to ensure a segregation of duties.

Participants may also delegate parts of their role to other entities as part of a service contract. For example, when revocation status information is provided using CRLs, the CA is also the CRL issuer, but it may delegate the responsibility for issuing CRLs to a different entity.

PKI roles consist of:

- authoritative roles, i.e. each role is uniquely instantiated;
- operational roles, i.e. roles that can be instantiated in one or more entities.

For example, a root CA can be implemented by a commercial entity, a common interest group, a national organisation and/or a European organisation.

Figure 1 shows the C-ITS trust model architecture based on [2]. The architecture is described briefly here, but the main elements are described in more detail in sections 1.3.2 to 1.3.6.

The CPA appoints the TLM, which is therefore a trusted entity for all PKI participants. The CPA approves the root CA operation and confirms that the TLM can trust the root CA(s). The TLM issues the ECTL that provides all PKI participants with trust in the approved root CAs. The root CA issues certificates to the EA and AA, thus providing trust in their operation. The EA issues enrolment certificates to the sending and relaying C-ITS stations (as end-entities), thus providing trust in their operation. The AA issues ATs to the C-ITS stations on the basis of trust in the EA.

The receiving and relaying C-ITS station (as relaying party) can trust other C-ITS stations, since the ATs are issued by an AA that is trusted by a root CA, which is trusted by the TLM and the CPA.

Note that Figure 1 describes only the root CA level of the C-ITS trust model. Details of the lower layers are provided in the subsequent sections of this CP or the CPS of the specific root CAs.

Figure 2 provides an overview of the information flows between PKI participants. The green dots indicate flows that require machine-to-machine communications. The information flows in red have defined security requirements.

The C-ITS trust model is based on a multiple root CA architecture, where the root CA certificates are transmitted periodically (as set out below) to the central point of contact (CPOC) through a secure protocol (e.g. link certificates) defined by the CPOC.

A root CA can be operated by a governmental or a private organisation. The C-ITS trust model architecture contains at least one root CA (the EU root CA with the same level as the other root CAs). The EU root CA is delegated by all entities participating in the C-ITS trust model that do not want to set up their own root CA. The CPOC transmits the received root CA certificates to the TLM, which is responsible for collecting and signing the list of root CA certificates and sending them back to the CPOC, which makes them publicly available to everybody (see below).

The trust relationships between the entities in the C-ITS trust model are described in the following figures, tables and sections.

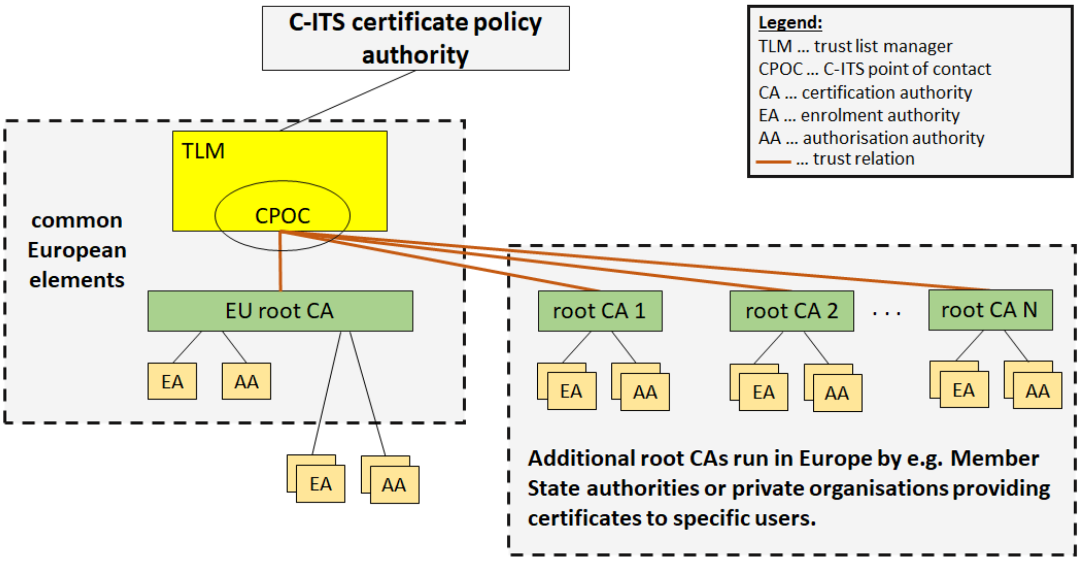
C-ITS certificate policy authority
Legend:
TLM ... trust list manager
CPOC ... C-ITS point of contact
CA ... certification authority
EA ... enrolment authority
AA ... authorisation authority
... trust relation
TLM
CPOC
common European elements
EU root CA
EA
AA
EA
AA
root CA 1
root CA 2
. . .
root CA N
EA
AA
EA
AA
EA
AA
Additional root CAs run in Europe by e.g. Member State authorities or private organisations providing certificates to specific users.

Figure 1: C-ITS trust model architecture

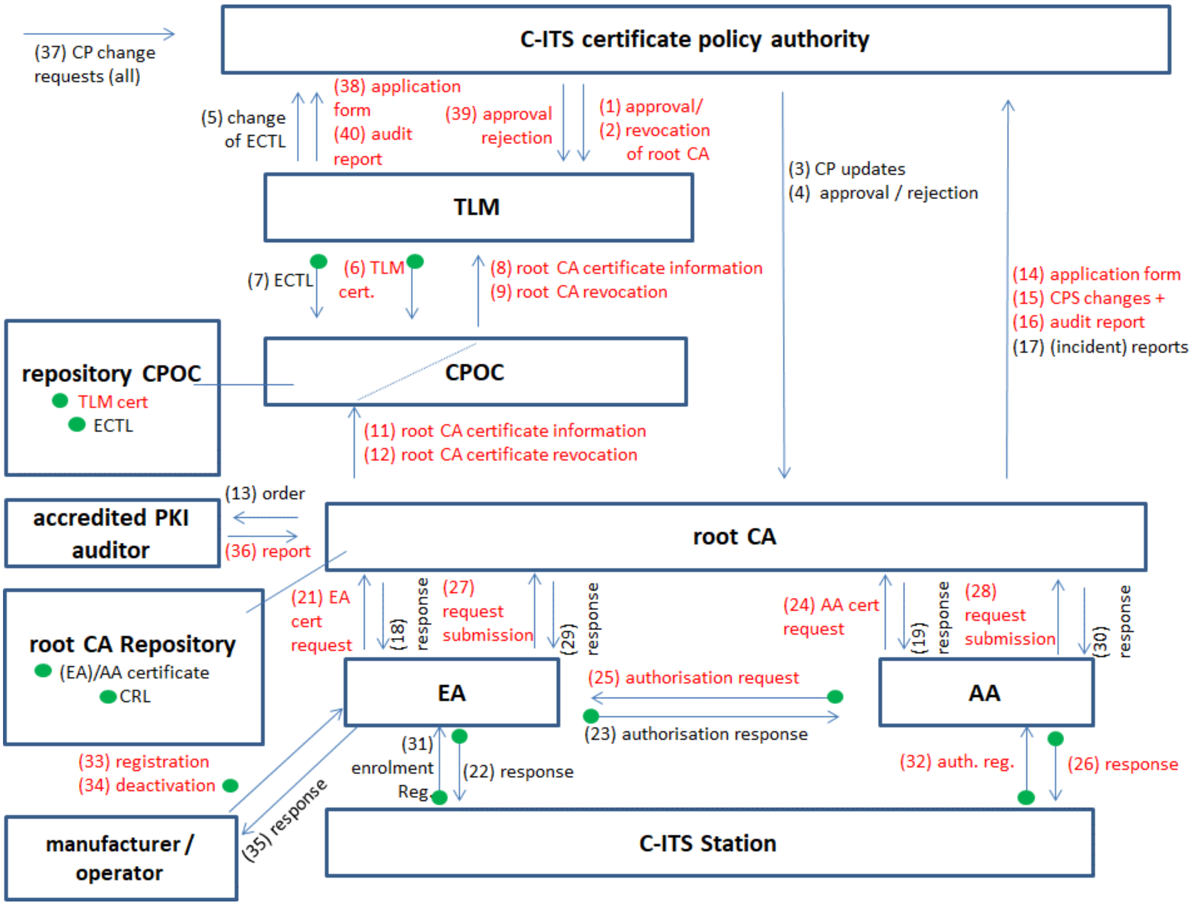

Figure 2: C-ITS Trust model information flows

Flow ID	From	To	Content	Reference
(1).	CPA	TLM	approval of root CA application	8
(2).	CPA	TLM	information on revocation of root CA	8.5
(3).	CPA	root CA	CP updates	1.5
(4).	CPA	root CA	approval/rejection of root CA application form or the CPS request changes or the audit process.	8.5, 8.6
(5).	TLM	CPA	notification of change of ECTL	4, 5.8.1
(6).	TLM	CPOC	TLM certificate	4.4.2
(7).	TLM	CPOC	ECTL	4.4.2
(8).	CPOC	TLM	root CA certificate information	4.3.1.1
(9).	CPOC	TLM	root CA certificate revocation	7.3
(10).	CPOC	all end-entities	TLM certificate	4.4.2
(11).	root CA	CPOC	root CA certificate information	4.3.1.1
(12).	root CA	CPOC	root CA certificate revocation	7.3
(13).	root CA	auditor	audit order	8
(14).	root CA	CPA	root CA application form — initial request	4.1.2.1
(15).	root CA	CPA	root CA application form — CPS changes	1.5.1
(16).	root CA	CPA	root CA application form — audit report	8.6
(17).	root CA	CPA	root CA incident reports, including revocation of a sub-CA (EA, AA)	Annex III, 7.3.1
(18).	root CA	EA	EA certificate response	4.2.2.3
(19).	root CA	AA	AA certificate response	4.2.2.3
(20).	root CA	All	EA/AA certificate, CRL	4.4.2
(21).	EA	root CA	EA certificate request	4.2.2.3
(22).	EA	C-ITS station	enrolment credential response	4.3.1.4
(23).	EA	AA	authorisation response	4.2.2.5
(24).	AA	root CA	AA certificate request	4.2.2.3
(25).	AA	EA	authorisation request	4.2.2.5
(26).	AA	C-ITS station	authorisation ticket response	4.3.1.5
(27).	EA	root CA	request submission	4.1.2.3
(28).	AA	root CA	request submission	4.1.2.3
(29).	root CA	EA	response	4.12 and 4.2.1

(30).	root CA	AA	response	4.12 and 4.2.1
(31).	C-ITS station	EA	enrolment credential request	4.2.2.4
(32).	C-ITS station	AA	authorisation ticket request	4.2.2.5
(33).	manufacturer / operator	EA	registration	4.2.1.4
(34).	manufacturer / operator	EA	deactivation	7.3
(35).	EA	manufacturer / operator	response	4.2.1.4
(36).	auditor	root CA	report	8.1
(37).	all	CPA	CP change requests	1.5
(38).	TLM	CPA	application form	4.1.2.2
(39).	CPA	TLM	approval/rejection	4.1.2.2
(40).	TLM	CPA	audit report	4.1.2.2

Table 1: Detailed description of information flows in the C-ITS trust model

1.3.2. C-ITS certificate policy authority

(1) The C-ITS certificate policy authority (CPA) is composed of the representatives of public and private stakeholders (e.g. Member States, vehicle manufacturers, etc.) participating in the C-ITS trust model. It is responsible for two sub-roles:

(1) certificate policy management, including:

- approval of the present CP and future CP change requests;
- deciding on the review of CP change requests and recommendations submitted by other PKI participants or entities;
- deciding on the release of new CP versions;

(2) PKI authorisation management, including:

- defining, deciding and publishing the CPS approval and CA audit procedures (collectively referred to as ‘CA approval procedures’);
- authorising the CPOC to operate and report regularly;
- authorising the TLM to operate and report regularly;
- approval of the root CA’s CPS, if it is in line with the common and valid CP;
- scrutiny of the audit reports from the accredited PKI auditor for all root CAs;
- notifying the TLM about the list of approved or non-approved root CAs and their certificates on the basis of received approval reports of the root CAs and regular operations reports.

(2) The CPA's authorised representative is responsible for authenticating the TLM's authorised representative and approving the TLM's enrolment process application form. The CPA is responsible for authorising the TLM to operate as mentioned in this section.

1.3.3. Trust list manager

(3) The TLM is a single entity appointed by the CPA.

(4) The TLM is responsible for:

- the operation of the ECTL in accordance with the common valid CP and regular activity reporting to the CPA for the overall secure operation of the C-ITS trust model;
- receiving root CA certificates from the CPOC;
- including/excluding root CA certificates in the ECTL upon notification by the CPA;
- signing the ECTL;
- the regular and timely transmission of the ECTL to the CPOC.

1.3.4. Accredited PKI auditor

(5) The accredited PKI auditor is responsible for:

- performing or organising audits of root CAs, TLM and sub-CAs;
- distributing the audit report (from an initial or periodic audit) to the CPA in line with the requirements in section 8 below. The audit report is to include recommendations from the accredited PKI auditor;
- notifying the entity managing the root CA of the successful or unsuccessful execution of an initial or periodic audit of the sub-CAs;
- assessing CPSs' compliance with this CP.

1.3.5. C-ITS point of contact (CPOC)

(6) The CPOC is a single entity appointed by the CPA. The CPA's authorised representative is responsible for authenticating the CPOC's authorised representative and approving the CPOC enrolment process application form. The CPA is responsible for authorising the CPOC to operate as set out in this section.

(7) The CPOC is responsible for:

- establishing and contributing to the secure communication exchange between all entities of the C-ITS trust model in an efficient and fast way;
- reviewing procedural change requests and recommendations submitted by other trust model participants (e.g. root CAs);
- transmitting root CA certificates to the TLM;
- publication of the common trust anchor (current public key and link certificate of the TLM);
- publication of the ECTL.

Complete details of the ECTL can be found in section 7.

1.3.6. *Operational roles*

(8) The following entities defined in [2] play an operational role, as defined in RFC 3647:

Functional element	PKI role ([3] and [4])	Detailed role ([2])
root certification authority	CA/RA (registration authority)	Provides EA and AA with proof that it may issue ECs or ATs
enrolment authority	subscriber to root CA / subject of EA certificate CA/RA	Authenticates a C-ITS station and grants it access to ITS communications
authorisation authority	subscriber to root CA / subject of AA certificate CA/RA	Provides a C-ITS station with authoritative proof that it may use specific ITS services
sending C-ITS station	subject of end-entity (EE) certificate (EC)	Acquires rights from EA to access ITS communications Negotiates rights from AA to invoke ITS services Sends single-hop and relayed broadcast messages
relaying (forwarding) C-ITS station	relaying party / subject of EE certificate	Receives broadcast message from sending C-ITS station and forwards them to receiving C-ITS station if required
receiving C-ITS station	relaying party	Receives broadcast messages from sending or relaying C-ITS station
manufacturer	subscriber to EA	Installs necessary information for security management in C-ITS station at production
operator	subscriber to EA / AA	Installs and updates necessary information for security management in C-ITS station during operation

Table 2: Operational roles

Note: in accordance with [4], different terms are used in this CP for the ‘subscriber’ which contracts with the CA for the issuance of certificates and the ‘subject’ to which the certificate applies. Subscribers are all entities that have a contractual relationship with a CA. Subjects are entities to which the certificate applies. EA/AAs are subscribers and subjects of the root CA and can request EA/AA certificates. C-ITS stations are subjects and can request end-entity certificates.

(9) Registration authorities:

The EA is to perform the role of a registration authority for end-entities. Only an authenticated and authorised subscriber can register new end-entities (C-ITS stations) in an EA. The relevant root CAs are to perform the role of registration authorities for EAs and AAs.

1.4. Certificate usage

1.4.1. *Applicable domains of use*

(10) Certificates issued under the present CP are intended to be used to validate digital signatures in the cooperative ITS communication context in accordance with the reference architecture of [2].

(11) The certificate profiles in [5] determine certificate uses for the TLM, root CAs, EAs, AAs and end-entities.

1.4.2. Limits of responsibility

(12) Certificates are not intended, nor authorised, for use in:

- circumstances that offend, breach or contravene any applicable law, regulation (e.g. GDPR), decree or government order;
- circumstances that breach, contravene or infringe the rights of others;
- breach of this CP or the relevant subscriber agreement;
- any circumstances where their use could lead directly to death, personal injury or severe environmental damage (e.g. through failure in the operation of nuclear facilities, aircraft navigation or communication, or weapons control systems);
- circumstances that contravene the overall objectives of greater road safety and more efficient road transport in Europe.

1.5. Certificate policy administration

1.5.1. Updating of CPSs of CAs listed in the ECTL

(13) Each root CA listed in the ECTL shall publish its own CPS, which must be in compliance with this policy. A root CA may add additional requirements, but shall ensure that all requirements of this CP are met at all times.

(14) Each root CA listed in the ECTL shall implement an appropriate change process for its CPS document. The key properties of the change process shall be documented in the public part of the CPS.

(15) The change process shall ensure that all changes to this CP are carefully analysed and, if necessary for compliance with the CP as amended, the CPS is updated within the timeframe laid down in the implementation step of the change process for the CP. In particular, the change process shall involve emergency change procedures that ensure timely implementation of security-relevant changes to the CP.

(16) The change process shall include appropriate measures to verify CP compliance for all changes to the CPS. Any changes to the CPS shall be clearly documented. Before a new version of a CPS is implemented, its compliance with the CP must be confirmed by an accredited PKI auditor.

(17) The root CA shall notify the CPA of any change made to the CPS with at least the following information:

- an exact description of the change;
- the rationale for the change;
- a report from the accredited PKI auditor confirming compliance with the CP;
- contact details of the person responsible for the CPS;
- planned timescale for implementation.

1.5.2. CPS approval procedures

(18) Before starting its operations, a prospective root CA shall present its CPS to an accredited PKI auditor as part of an order for compliance audit (flow 13) and to the CPA for approval (flow 15).

(19) A root CA shall present changes to its CPS to an accredited PKI auditor as part of an order for compliance audit (flow 13) and to the CPA for approval (flow 15) before those changes become effective.

(20) An EA/AA shall present its CPS or changes to its CPS to the root CA. The root CA may order a certificate of conformity from the national body or private entity responsible for approval of the EA/AA, as defined in sections 4.1.2 and 8.

(21) The accredited PKI auditor shall assess the CPS in accordance with section 8.

(22) The accredited PKI auditor shall communicate the results of the CPS assessment as part of the audit report, as set out in section 8.1. The CPS shall be accepted or rejected as part of the audit report acceptance referred to in sections 8.5 and 8.6.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Methods for the publication of certificates information

(23) Certificate information may be published pursuant to section 2.5:

- in a regular or periodic way; or
- in response to a request from one of the participating entities.

In each case, different degrees of urgency for publication and therefore time schedules apply, but entities must be ready for both types of arrangement.

(24) The regular publication of the certificate information makes it possible to determine a maximum deadline by which certificate information is updated for all nodes of the C-ITS network. The frequency of the publication of all certificate information is laid down in section 2.2.

(25) At the request of entities participating in the C-ITS network, any of the participants may start to publish certificate information at any time and, depending on its status, request a current set of certificate information so as to become a fully trusted node of the C-ITS network. The purpose of such publication is mainly to update entities on the overall current status of certificate information in the network and enable them to communicate on a trusted basis until the next regular publication of the information.

(26) A single root CA may also initiate the publication of certificate information at any point in time by sending an updated set of certificates to all ‘subscribed members’ of the C-ITS network that are regular recipients of such information. This supports the operation of the CAs and enables them to address members between the regular and scheduled dates for publishing the certificates.

(27) Section 2.5 sets out the mechanism and all procedures for publishing root CA certificates and the ECTL.

(28) The CPOC shall publish the root CA certificates (as included in the ECTL and intended for public consumption), the TLM certificate and the ECTL that it issues.

(29) Root CAs shall publish their EA/AA certificates and CRLs, and be able to support all three mechanisms referred to here for publishing them to their subscribed members and relying parties, taking all necessary steps to ensure secure transmission, as referred to in section 4.

2.2. Time or frequency of publication

(30) The requirements as to the publication schedule for certificates and CRLs must be determined in the light of the various limiting factors of the single C-ITS nodes, with the overall goal of operating a 'trusted network' and publishing updates as quickly as possible to all C-ITS stations involved.

- For the regular publication of updated certificate information (e.g. changes in the ECTL or CRL composition), a maximum period of three months is required for the safe operation of the C-ITS network.
- Root CAs shall publish their CA certificates and CRLs as soon as possible after issuance.
- For the publication of the CRL, the root CA repository shall be used.

In addition, the CPS for each CA shall specify the period of time within which a certificate will be published after the CA issues the certificate.

This section specifies only the time or frequency of the regular publication. Means of connectivity to update C-ITS stations with the ECTL and CRLs within a week of their publication (under normal operation conditions, e.g. with cellular coverage, vehicle in actual operation, etc.) shall be implemented in accordance with the requirements in this document.

2.3. Repositories

(31) The requirements regarding the structure of the repository for storing the certificates and what information is provided by the entities of the C-ITS network are as follows for the single entities:

- in general, each root CA should use a repository of its own currently active EA/AA certificate information and CRL to publish certificates for the other PKI participants (e.g. an LDAP-based directory service). The repository of each root CA shall support all required access controls (section 2.4) and transmission times (section 2.2) for every method of distribution of C-ITS-related information;
- the TLM's repository (which stores the ECTL and TLM certificates published by the CPOC, for example) should be based on a publication mechanism able to ensure the transmission times set out in section 2.2 for every method of distribution.

Requirements of AAs are not defined, but they must support the same security levels as the other entities and these must be declared in their CPS.

2.4. Access controls on repositories

(32) The requirements on access control to repositories of certificate information shall at least comply with the general standards of secure information handling

outlined in ISO/IEC 27001 and with the requirements in section 4. In addition, they shall reflect the process security needs to be established for the single process steps in the publication of certificate information.

- This includes the implementation of the repository for TLM certificates and the ECTL in the TLM/CPOC. Each CA or repository operator shall implement access controls in relation to all of the C-ITS entities and external parties for at least three different levels (e.g. public, restricted to C-ITS entities, root CA level) in order to prevent unauthorised entities from adding to, amending or deleting repository entries.
- The exact access control mechanisms of the single entity should be part of the respective CPS.
- For each root CA, the EA and AA repositories shall comply with the same requirements for access control procedures regardless of the place or contractual link to the service provider operating the repository.

As a starting point for the levels of access control, each root CA or repository operator should provide at least three different levels (e.g. public, restricted to C-ITS entities, root CA level).

2.5. Publication of certificate information

2.5.1. Publication of certificate information by the TLM

(33) The TLM in the European common C-ITS trust domain shall publish the following information via the CPOC:

- all currently valid TLM certificates for the next period of operation (current and link certificate if available);
- access point information for the CPOC repository to provide the signed list of root CA´s (ECTL);
- general information point for the ECTL and C-ITS deployment.

2.5.2. Publication of certificate information by CAs

(34) Root CAs in the European common C-ITS trust domain shall publish the following information:

- issued (currently valid) root CA certificates (current and correctly re-keyed certificates, including a link certificate) in the repository referred to in section 2.3;
- all valid EA, AA entities, with their operator ID and planned period of operation;
- issued CA certificates in the repositories referred to in section 2.3;
- the CRLs for all revoked CA certificates covering their subordinate EAs and AAs;
- information regarding the root CA’s point of access to the CRL and CA information.

All certificate information shall be categorised in accordance with three levels of confidentiality and documents for the general public must be publicly available without restrictions.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of name

3.1.1.1. Names for TLM, root CAs, EAs, AAs

(35) The name in the TLM certificate shall consist of a single subject_name attribute with the reserved value 'EU_TLM'.

(36) The name for root CAs shall consist of a single subject_name attribute with a value allocated by the CPA. The uniqueness of names is the sole responsibility of the CPA and the TLM shall maintain the registry of root CA names upon notification by the CPA (approval, revocation/removal of a root CA). Subject names in certificates are limited to 32 bytes. Each root CA proposes its name to the CPA in the application form (flow 14). The CPA is responsible for checking name uniqueness. If the name is not unique, the application form is rejected (flow 4).

(37) The name in each EA/AA certificate may consist of a single subject_name attribute with a value generated by the issuer of the certificate. The uniqueness of names is the sole responsibility of the issuing root CA.

(38) The EA and AA certificates shall not use a name greater than 32 bytes, because subject_name in certificates are limited to 32 bytes.

(39) ATs shall not contain a name.

3.1.1.2. Names for end-entities

(40) Each C-ITS station shall be assigned two kinds of unique identifier:

- a canonical ID that is stored at the initial registration of the C-ITS station under the responsibility of the manufacturer. This shall contain a substring identifying the manufacturer or operator so that this identifier can be unique;
- a subject_name, which may be part of the C-ITS station's EC, under the responsibility of the EA.

3.1.1.3. Identification of certificates

(41) Certificates following the format of [5] shall be identified by computing a HashedId8 value as defined in [5].

3.1.2. Need for names to be meaningful

No stipulation.

3.1.3. Anonymity and pseudonymity of end-entities

(42) The AA shall ensure that the pseudonymity of a C-ITS station is established by providing the C-ITS station with ATs that do not contain any names or information that may link the subject to its real identity.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of names

(43) Names for the TLM, root CAs, EAs, AAs and canonical IDs for C-ITS stations shall be unique.

(44) The TLM shall ensure in the registration process of a given root CA in the ECTL that its certificate identifier (HashedId8) is unique. The root CA shall ensure in the issuance process that the certificate identifier (HashedId8) of each subordinate CA is unique.

(45) The HashedId8 of an EC shall be unique within the issuing CA. The HashedId8 of an AT does not have to be unique.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

(46) The root CA shall prove that it rightfully holds the private key corresponding to the public key in the self-signed certificate. The CPOC shall check this proof.

(47) The EA/AA shall prove that it rightfully holds the private key corresponding to the public key to be listed in the certificate. The root CA shall check this proof.

(48) Possession of a new private key (for re-keying) shall be proven by the signing of the request with the new private key (inner signature) followed by the generation of an outer signature over the signed request with the current valid private key (to guarantee the authenticity of the request). The applicant shall submit the signed certificate request to the issuing CA via a secure communication. The issuing CA shall verify that the applicant's digital signature on the request message was created using the private key corresponding to the public key attached to the certificate request. The root CA shall specify which certificate request and responses it supports in its CPS.

3.2.2. Authentication of organisation identity

3.2.2.1. Authentication of root CAs' organisation identity

(49) In an application form to the CPA (i.e. flow 14), the root CA shall provide the identity of the organisation and registration information, composed of:

- organisation name;
- postal address;
- e-mail address;
- the name of a physical contact person in the organisation;
- telephone number;
- digital fingerprint (i.e. SHA 256 hashvalue) of the root CA's certificate in printed form;
- cryptographic information (i.e. cryptographic algorithms, key lengths) in the root CA certificate;
- all permissions that the root CA is allowed to use and to pass to the sub-CAs.

(50) The CPA shall check the identity of the organisation and other registration information provided by the certificate applicant for the insertion of a root CA certificate in the ECTL.

(51) The CPA shall collect either direct evidence, or an attestation from an appropriate and authorised source, of the identity (e.g. name) and, if applicable, any specific attributes of subjects to which a certificate is issued. Submitted evidence may be in the form of paper or electronic documentation.

(52) The subject's identity shall be verified at the time of registration by appropriate means and in accordance with the present certificate policy.

(53) At each certificate application, evidence shall be provided of:

- the full name of the organisational entity (private organisation, government entity or non-commercial entity);
- nationally recognised registration or other attributes that may be used, as far as possible, to distinguish the organisational entity from others with the same name.

The rules above are based on TS 102 042 [4]: *The CA shall ensure that evidence of the subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestations from appropriate and authorised sources, and that certificate requests are accurate, authorised and complete in accordance with the collected evidence or attestation.*

3.2.2.2. Authentication of TLM organisation identity

(54) The organisation operating the TLM shall provide evidence of the identification and accuracy of the name and associated data in order to enable appropriate verification at initial creation and re-keying of the TLM certificate.

(55) The subject's identity shall be verified at the time of certificate creation or re-keying by appropriate means and in accordance with the present CP.

(56) Organisation evidence shall be provided as specified in section 3.2.2.1.

3.2.2.3. Authentication of sub-CAs organisation identity

(57) The root CA shall check the identity of the organisation and other registration information provided by certificate applicants for sub-CA (EA/AA) certificates.

(58) At a minimum, the root CA shall:

- determine that the organisation exists by using at least one third-party identity proofing service or database, or, alternatively, organisational documentation issued by or filed with the relevant government agency or recognised authority that confirms the existence of the organisation;
- use postal mail or a comparable procedure requiring the certificate applicant to confirm certain information about the organisation, that it has authorised the certificate application and that the person submitting the application on behalf of the applicant is authorised to do so. Where a certificate includes the name of an individual as an authorised representative of the organisation, it shall also confirm that it employs that individual and has authorised him/her to act on its behalf.

(59) Validation procedures for issuing CA certificates shall be documented in a CPS of the root CA.

3.2.2.4. Authentication of end-entities' subscriber organisation

(60) Before the subscriber of end-entities (manufacturer/operator) can register with a trusted EA to enable its end-entities for sending EC certificate requests, the EA shall:

- check the identity of the subscriber organisation and other registration information provided by the certificate applicant;
- check that the C-ITS station type (i.e. the concrete product based on brand, model and version of the C-ITS station) meets all compliance assessment criteria.

(61) At a minimum, the EA shall:

- determine that the organisation exists by using at least one third-party identity proofing service or database, or, alternatively, organisational documentation issued by or filed with the relevant government agency or recognised authority that confirms the existence of the organisation;
- use postal mail or a comparable procedure to require the certificate applicant to confirm certain information about the organisation, that it has authorised the certificate application and that the person submitting the application on its behalf is authorised to do so. Where a certificate includes the name of an individual as an authorised representative of the organisation, it shall also confirm that it employs that individual and has authorised him/her to act on its behalf.

(62) Validation procedures for the registration of a C-ITS station by its subscriber shall be documented in a CPS of the EA.

3.2.3. Authentication of individual entity

3.2.3.1. Authentication of TLM/CA individual entity

(63) For the authentication of an individual entity (physical person) identified in association with a legal person or organisational entity (e.g. the subscriber), evidence shall be provided of:

- full name of the subject (including surname and given names, in line with the applicable law and national identification practices);
- date and place of birth, reference to a nationally recognised identity document or other attributes of the subscriber that may be used, as far as possible, to distinguish the person from others with the same name;
- full name and legal status of the associated legal person or other organisational entity (e.g. the subscriber);
- any relevant registration information (e.g. company registration) of the associated legal person or other organisational entity;
- evidence that the subject is associated with the legal person or other organisational entity.

Submitted evidence may be in the form of paper or electronic documentation.

(64) To verify his/her identity, the authorised representative of a root CA, EA, AA or subscriber shall provide documentation proving that he/she works for the organisation (certificate of authorisation). He/she shall also show an official ID.

(65) For the initial enrolment process (flow 31/32), a representative of the EA/AA shall provide the corresponding root CA with all necessary information (see section 4.1.2).

(66) The personnel at the root CA shall verify the identity of the certificate applicant representative and all associated documents, applying the requirements of 'trusted personnel' as set out in section 5.2.1. (The process of validating application information and generating the certificate by the root CA shall be carried out by 'trusted persons' at the root CA, under at least dual supervision, as they are sensitive operations within the meaning of section 5.2.2).

3.2.3.2. Authentication of C-ITS stations' subscriber identity

(67) Subscribers are represented by authorised end-users in the organisation who are registered at the issuing EA and AA. These end-users designated by organisations (manufacturers or operators) shall prove their identity and authenticity before:

- registering the EE at its corresponding EA, including its canonical public key, canonical ID (unique identifier) and the permissions in accordance with the EE;
- registering at the AA and securing proof of a subscriber agreement that can be sent to the EA.

3.2.3.3. Authentication of C-ITS stations' identity

(68) EE subjects of ECs shall authenticate themselves when requesting ECs (flow 31) by using their canonical private key for the initial authentication. The EA shall check the authentication using the canonical public key corresponding to the EE. The canonical public keys of the EEs are brought to the EA before the initial request is executed, by a secure channel between the C-ITS station manufacturer or operator and the EA (flow 33).

(69) EE subjects of ATs shall authenticate themselves when requesting ATs (flow 32) by using their unique enrolment private key. The AA shall forward the signature to the EA (flow 25) for validation; the EA shall validate it and confirm the result to the AA (flow 23).

3.2.4. Non-verified subscriber information

No stipulation.

3.2.5. Validation of authority

3.2.5.1. Validation of TLM, root CA, EA, AA

(70) Every organisation shall identify in the CPS at least one representative (e.g. a security officer) responsible for requesting new certificates and renewals. The naming rules in section 3.2.3 shall apply.

3.2.5.2. Validation of C-ITS station subscribers

(71) At least one physical person responsible for registering C-ITS stations at an EA (e.g. security officer) shall be known to and approved by the EA (see section 3.2.3).

3.2.5.3. Validation of C-ITS stations

(72) A C-ITS station's subscriber may register C-ITS stations at a specific EA (flow 33) as long as it is authenticated at that EA.

Where the C-ITS station is registered at an EA with a unique canonical ID and a canonical public key, it may request an EC using a request signed with the canonical private key related to the previously registered canonical public key.

3.2.6. Criteria for interoperation

(73) For communication between C-ITS stations and EAs (or AAs), the C-ITS station shall be able to establish secure communication with EAs (or AAs), i.e. to implement authentication, confidentiality and integrity functions, as specified in [1]. Other protocols may be used, provided that [1] is implemented. The EA and AA shall support this secure communication.

(74) The EA and AA shall support certificate requests and responses that comply with [1], which provides for a secure AT request/response protocol supporting the anonymity of the requester *vis-à-vis* the AA and separation of duties between the AA and the EA. Other protocols may be used, provided that [1] is implemented. To prevent disclosure of C-ITS stations' long-term identity, communication between a mobile C-ITS station and an EA shall be confidential (e.g. communication data shall be encrypted end-to-end).

(75) The AA shall submit an authorisation validation request (flow 25) for each authorisation request it receives from an EE certificate subject. The EA shall validate this request with respect to:

- the status of the EE at the EA;
- the validity of the signature;
- the requested ITS Application IDs (ITS-AID) and permissions;
- the status of service provision of the AA to the subscriber.

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for routine re-key requests

3.3.1.1. TLM certificates

(76) The TLM generates a key pair and two certificates: one self-signed and one link certificate as referred to in section 7.

3.3.1.2. Root CA certificates

Not applicable.

3.3.1.3. EA/AA certificate renewal or re-keying

(77) Prior to the expiry of an EA/AA certificate, the EA/AA shall request a new certificate (flow 21/flow 24) to maintain continuity of certificate usage. The EA/AA shall generate a new key pair to replace the expiring key pair and sign the re-key request containing the new public key with the current valid private

key ('re-keying'). The EA or AA generates a new key pair and signs the request with the new private key (inner signature) to prove possession of the new private key. The whole request is signed (oversigned) with the current valid private key (outer signature) to ensure the integrity and authenticity of the request. If an encryption and decryption key pair is used, possession of private decryption keys shall be proven (for detailed description of re-keying, see section 4.7.3.3).

(78) The identification and authentication method for routine re-keying is the same as that for the initial issuance of an initial root CA certificate validation, as set out in section 3.2.2.

3.3.1.4. End-entities' enrolment credentials

(79) Prior to the expiry of an existing EC, the EE shall request a new certificate (flow 31) to maintain continuity of certificate usage. The EE shall generate a new key pair to replace the expiring key pair and request a new certificate containing the new public key; the request shall be signed with the current valid EC private key.

(80) The EE may sign the request with the newly created private key (inner signature) to prove possession of the new private key. The whole request is then signed (oversigned) with the current valid private key (outer signature) and encrypted to the receiving EA as specified in [1], to ensure the confidentiality, integrity and authenticity of the request. Other protocols may be used, provided that [1] is implemented.

3.3.1.5. End-entities' authorisation tickets

(81) The certificate re-key for ATs is based on the same process as the initial authorisation, as defined in [1]. Other protocols may be used, provided that [1] is implemented.

3.3.2. Identification and authentication for re-key requests after revocation

3.3.2.1. CA certificates

(82) The authentication of a CA organisation for root CA, EA and AA certificate re-keying after revocation is handled in the same way as the initial issuance of a CA certificate, as set out in section 3.2.2.

3.3.2.2. End-entities' enrolment credentials

(83) The authentication of an EE for EC certificate re-keying after revocation is handled in the same way as the initial issuance of an EE certificate, as set out in section 3.2.2.

3.3.2.3. End-entities' authorisation requests

Not applicable, since ATs are not revoked.

3.4. Identification and authentication for revocation request

3.4.1. Root CA/EA/AA certificates

(84) Requests to delete a root CA certificate from the ECTL shall be authenticated by the root CA to the TLM (flows 12 and 9). Requests to revoke an EA/AA certificate shall be authenticated by the relevant root CA and sub-CA itself.

(85) Acceptable procedures for authenticating a subscriber's revocation requests include:

- a written and signed message on corporate letter paper from the subscriber requesting revocation, with reference to the certificate to be revoked;
- communication with the subscriber providing reasonable assurances that the person or organisation requesting revocation is in fact the subscriber. Depending on the circumstances, such communication may include one or more of the following: e-mail, postal mail or courier service.

3.4.2. C-ITS station enrolment credentials

(86) The C-ITS station subscriber may revoke the EC of a previously registered C-ITS station at an EA (flow 34). The requesting subscriber shall create a request for revocation of a given C-ITS station or list of C-ITS stations. The EA shall authenticate the revocation request before processing it and confirm the revocation of the C-ITS stations and their ECs.

(87) The EA may revoke the EC of a C-ITS station in accordance with section 7.3.

3.4.3. C-ITS station authorisation tickets

(88) As ATs are not revoked, their validity shall be limited to a specific period. The range of acceptable validity periods in this certificate policy is specified in section 7.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate application

(89) This section sets out the requirements for an initial application for certificate issuance.

(90) The term 'certificate application' refers to the following processes:

- registration and setup of a trust relation between the TLM and the CPA;
- registration and setup of a trust relation between the root CA and the CPA and TLM, including the insertion of the first root CA certificate in the ECTL;
- registration and setup of a trust relation between the EA/AA and the root CA, including the issuance of a new EA/AA certificate;
- registration of the C-ITS station at the EA by the manufacturer/operator;
- C-ITS station's request for EC/AT.

4.1.1. Who can submit a certificate application

4.1.1.1. Root CAs

(91) Root CAs generate their own key pairs and issue their root certificate by themselves. A root CA can submit a certificate application through its designated representative (flow 14).

4.1.1.2. *TLM*

(92) The TLM generates its own key pairs and issues its certificate by itself. The initial creation of the TLM certificate shall be processed by a TLM organisation representative under the control of the CPA.

4.1.1.3. EA and AA

(93) An authorised representative of the EA or AA may submit the sub-CA (EA and/or AA) certificate request application to the authorised representative of the relevant root CA (flow 27/28).

4.1.1.4. C-ITS station

(94) Subscribers shall register each C-ITS station at the EA in accordance with section 3.2.5.3.

(95) Each C-ITS station registered at the EA may send EC requests (flow 31).

(96) Each C-ITS station may send AT requests (flow 32) without requesting any subscriber interaction. Before requesting an AT, a C-ITS station shall have an EC.

4.1.2. Enrolment process and responsibilities

(97) Permissions for root-CAs and sub-CAs issuing certificates for special (governmental) purposes (i.e.special mobile and fixed C-ITS stations) may be granted only by the Member States in which the organisations are located.

4.1.2.1. Root CAs

(98) After being audited (flow 13 and 36, section 8), root CAs may apply for insertion of their certificate(s) in the ECTL at the CPA (flow 14). The enrolment process is based on a signed manual application form that shall be physically delivered to the CPA by the root CA's authorised representative and that contains at least the information referred to in sections 3.2.2.1, 3.2.3 and 3.2.5.1.

(99) The root CA's application form shall be signed by its authorised representative.

(100) In addition to the application form, the root CA's authorised representative shall provide a copy of the root CA's CPS (flow 15) and its audit report to the CPA for approval (flow 16). In cases of positive approval, the CPA generates and sends a certificate of conformity to the CPOC/TLM and the corresponding root CA.

(101) The root CAs authorised representative shall then bring its application form (containing the fingerprint of the self-signed certificate), the official ID and a proof of authorisation to the CPOC/TLM. The self-signed certificate shall be delivered electronically to the CPOC/TLM. The CPOC/TLM shall verify all documents and the self-signed certificate.

(102) In cases of positive verifications, the TLM shall add the root CA's certificate to the ECTL based on the notification from the CPA (flows 1 and 2). The detailed process is described in the CPS of the TLM.

(103) An additional procedure to get an approval of the CPS and audit report of a root CA at a national body of specific countries should be possible.

4.1.2.2. *TLM*

(104) After being audited, the TLM may enrol with the CPA. The enrolment process is based on a signed manual application form that shall be physically delivered to the CPA (flow 38) by the TLM's authorised representative and contains at least the information referred to in sections 3.2.2.2 and 3.2.3.

(105) The TLM's application form shall be signed by its authorised representative.

(106) First, the TLM generates its self-signed certificate and transmits it securely to the CPA. The TLM then brings its application form (containing the fingerprint of the self-signed certificate), a copy of its CPS, an official ID, a proof of authorisation and its audit report to the CPA (flow 40). The CPA shall check all the documents and the self-signed certificate. In cases of positive verification of all documents, the self-signed certificate and the fingerprint, the CPA shall confirm the enrolment process by sending its approval to the TLM and the CPOC (flow 39). The CPA shall store the application information sent by the TLM. The TLM certificate is then issued via the CPOC.

4.1.2.3. EA and AA

(107) During the enrolment process, the EA/AA shall bring the relevant documents (e.g. the CPS and the audit report) to the corresponding root CA for approval (flow 27/28). In cases of positive checks of the documents, the root CA sends an approval to the corresponding root sub-CAs (flow 29/30). The sub-CA (EA or AA) shall then transmit its signed request electronically, and physically deliver its application form (in accordance with section 3.2.2.1), proof of authorisation and ID document to the corresponding root CA. The root CA verifies the request and the received documents (application form containing the fingerprint, which is the SHA 256 hashvalue of the sub-CA request, proof of authorisation and ID Document). If all checks lead to a positive result, the root CA issues the corresponding sub-CA certificate. Detailed information how an initial request is done is described in its specific CPS.

(108) In addition to the sub-CA application form, the sub-CA's authorised representative shall attach a copy of the CPS to the root CA.

(109) Information shall be given to an accredited PKI auditor for auditing in accordance with section 8.

(110) If a sub-CA is owned by an entity different than the entity that owns a root CA, before issuing a sub-CA certificate request, the sub-CA's entity shall sign a contract regarding the root CA service.

4.1.2.4. C-ITS station

(111) The initial registration of end-entities subjects (C-ITS stations) shall be carried out by the responsible subscriber (manufacturer /operator) with the EA (flows 33 and 35) after successful authentication of the subscriber organisation and one of its representatives in line with sections 3.2.2.4 and 3.2.5.2.

(112) A C-ITS station may generate an EC key pair (see section 6.1) and create a signed EC request in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(113) During the registration of a normal C-ITS station (as opposed to a special mobile or fixed C-ITS station), the EA must verify that the permissions in the

initial request are not for governmental use. Permissions for governmental use are defined by the corresponding Member States. The detailed procedure for the registration and response of the EA to the manufacturer/operator (flows 33 and 35) shall be set out in the corresponding CPS of the EA.

(114) A C-ITS station shall be enrolled at an EA (section 3.2.5.3) by sending its initial EC request in accordance with [1].

(115) Upon initial registration by an authenticated subscriber representative, the EA approves which ATs the end-entity subject (i.e. the C-ITS station) may obtain. Furthermore, each end-entity is assigned a trust assurance level, which is related to the certification of the end-entity in accordance with one of the protection profiles listed in section 6.1.5.2.

(116) Regular vehicles shall have only one C-ITS station that is registered at one EA. Special-purpose vehicles (such as police cars and other special-purpose vehicles with specific rights) may be registered at an additional EA or have one additional C-ITS station for authorisations within the scope of the special purpose. Vehicles to which such an exemption applies shall be defined by the Member States responsible. Permissions for special mobile and fixed C-ITS stations shall be granted only by the Member States responsible. The CPS of root CAs or sub-CAs issuing certificates for such vehicles in those Member States shall determine how the certificate process applies to such vehicles.

(117) Where the subscriber is in the process of migrating a C-ITS station from one EA to another EA, the C-ITS station may be registered at two (similar) EAs.

(118) A C-ITS station generates an AT key pair (see section 6.1) and creates an AT request in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(119) C-ITS stations send an authorisation request to the AA's URL (flows 32 and 26) by sending at least the required information referred to in section 3.2.3.3). The AA and EA validate the authorisation for each request in accordance with sections 3.2.6 and 4.2.2.5.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

4.2.1.1. Identification and authentication of root CAs

(120) The CPA's authorised representative is responsible for authenticating the root CA's authorised representative and approving its enrolment process in accordance with section 3.

4.2.1.2. Identification and authentication of the TLM

(121) The CPA's authorised representative is responsible for authenticating the TLM's authorised representative and approving its enrolment process application form in accordance with section 3.

4.2.1.3. Identification and authentication of EA and AA

(122) The corresponding root CA is responsible for authenticating the EA/AA's authorised representative and approving its enrolment process application form in accordance with section 3.

(123) The root CA shall confirm its positive validation of the application form to the EA/AA. The EA/AA may then send a certificate request to the root CA (flow 21/24), which shall issue certificates to the corresponding EA/AA (flow 18/19).

4.2.1.4. Identification and authentication of EE subscriber

(124) Before a C-ITS station can request an EC certificate, the EE subscriber shall securely transmit the C-ITS station identifier information to the EA (flow 33). The EA shall verify the request and in cases of positive verification register the C-ITS station information in its database and confirm this to the EE subscriber (flow 35). This operation is done only once by the manufacturer or operator for each C-ITS station. Once a C-ITS station is registered by an EA, it may request a single EC certificate it needs (flow 31) at a time. The EA authenticates and verifies that the information in the EC certificate request is valid for a C-ITS station.

4.2.1.5. Authorisation tickets

(125) During authorisation requests (flow 32), in accordance with [1], the AA must authenticate the EA from which the C-ITS station received its EC. Other protocols may be used, provided that [1] is implemented. If the AA is not able to authenticate the EA, the request is rejected (flow 26). As a requirement, AA shall possess the EA certificate to authenticate the EA and verify its response (flows 25 and 23, section 3.2.5.3).

(126) The EA authenticates the C-ITS station requesting an AT by verifying its EC (flows 25 and 23).

4.2.2. Approval or rejection of certificate applications

4.2.2.1. Approval or rejection of root CA certificates

(127) The TLM inserts/deletes the root CA certificates into the ECTL in accordance with the approval of the CPA (flow 1/2).

(128) The TLM should verify the signature, information and encoding of root CA certificates after receiving an approval by the CPA (flow 1). After positive validation and the CPA’s approval, the TLM shall put the corresponding root certificate on the ECTL and notify the CPA (flow 5).

4.2.2.2. *Approval or rejection of TLM certificate*

(129) The CPA is responsible for approving or rejecting TLM certificates.

4.2.2.3. *Approval or rejection of EA and AA certificates*

(130) The root CA verifies sub-CA certificate requests (flow 21/24) and the relevant reports (issued by the accredited PKI auditor) on receiving them (flow 36, section 8) from the corresponding sub-CA of the root CA. If the check of the request leads to a positive result, the corresponding root CA issues a certificate to the requesting EA/AA (flow 18/19); otherwise, the request is rejected and no certificate shall be issued to the EA/AA.

4.2.2.4. Approval or rejection of EC

(131) The EA shall verify and validate EC requests in accordance with sections 3.2.3.2 and 3.2.5.3.

(132) If the certificate request in accordance with [1] is correct and valid, the EA shall generate the requested certificate.

(133) Where the certificate request is invalid, the EA refuses it and sends a response setting out the reason for refusal in accordance with [1]. If a C-ITS station still wants an EC, it shall make a new certificate request. Other protocols may be used, provided that [1] is implemented.

4.2.2.5. Approval or rejection of AT

(134) The certificate request is checked by the EA. The AA shall establish communication with EA to validate the request (flow 25). The EA shall authenticate the requesting C-ITS station and validate whether it is entitled to receive the requested AT following the CP (e.g. by checking the revocation status and validate certificate time/region validity, permissions, assurance level, etc.). The EA shall return a validation response (flow 23) and, if the response is positive, the AA shall generate the requested certificate and transmit it to the C-ITS station. If the AT request is not correct or the EA validation response is negative, the AA refuses the request. If a C-ITS station still requires an AT, it shall make a new authorisation request.

4.2.3. Time to process the certificate application

4.2.3.1. Root CA certificate application

(135) The time to process the identification and authentication process of a certificate application is during working day and shall be subject to a maximum time limit laid down in the root CA's CPS.

4.2.3.2. *TLM certificate application*

(136) The processing of the TLM certificate application shall be subject to a maximum time limit laid down in the TLM's CPS.

4.2.3.3. *EA and AA certificate application*

(137) The time to process the identification and authentication process of a certificate application is during working day in accordance with the agreement and contract between the Member State/private organisation root CA and the sub-CA. The time to process sub-CA certificate applications shall be subject to a maximum time limit laid down in the sub-CA's CPS.

4.2.3.4. *EC application*

(138) The processing of EC applications shall be subject to a maximum time limit laid down in the EA's CPS.

4.2.3.5. *AT application*

(139) The processing of AT applications shall be subject to a maximum time limit laid down in the AA's CPS.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

4.3.1.1. Root CA certificate issuance

(140) Root CAs issue their own self-signed root CA certificates, link certificates, sub-CA certificates and CRLs.

(141) After CPA approval (flow 4), the root CA sends its certificate to the TLM through the CPOC to be added to the ECTL (flows 11 and 8) (see

section 4.1.2.1). The TLM checks whether the CPA has approved the certificate (flow 1).

4.3.1.2. *TLM certificate issuance*

(142) The TLM issues its own self-signed TLM and link certificate and sends it to the CPOC (flow 6).

4.3.1.3. EA and AA certificate issuance

(143) The sub-CAs generate a signed certificate request and transmit it to the corresponding root CA (flows 21 and 24). The root CA verifies the request and issues a certificate to the requesting sub-CA in accordance with [5] as soon as possible, as laid down in the CPS for usual operational practices, but not later than five working days after the request has been received.

(144) The root CA shall update the repository containing the certificates of the sub-CAs.

4.3.1.4. EC issuance

(145) The C-ITS station shall send an EC request to the EA in accordance with [1]. The EA shall authenticate and verify that the information in the certificate request is valid for a C-ITS station. Other protocols may be used, provided that [1] is implemented.

(146) In cases of positive validation, the EA shall issue a certificate in accordance with the C-ITS station registration (see 4.2.1.4) and send it to the C-ITS station using an EC response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(147) If there is no registration, the EA shall generate an error code and send it to the C-ITS station using an EC response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(148) EC requests and EC responses shall be encrypted to ensure confidentiality and signed to ensure authentication and integrity.

4.3.1.5. AT issuance

(149) The C-ITS station shall send an AT request message to the AA, in accordance with [1]. The AA shall send an AT validation request in accordance with [1] to the EA. The EA shall send an AT validation response to the AA. In cases of a positive response, the AA shall generate an AT and send it to the C-ITS station using an AT response message in accordance with [1]. In cases of a negative response, the AA shall generate an error code and send it to the C-ITS station using an AT response message in accordance with [1]. Other protocols may be used, provided that [1] is implemented.

(150) AT requests and AT responses shall be encrypted (only needed for mobile C-ITS stations) to ensure confidentiality and signed to ensure authentication and integrity.

4.3.2. *CA's notification to subscriber of issuance of certificates.*

Not applicable.

4.4. Certificate acceptance

4.4.1. Conducting certificate acceptance

4.4.1.1. *Root CA*

Not applicable.

4.4.1.2. *TLM*

Not applicable.

4.4.1.3. EA and AA

(151) The EA/AA shall verify the certificate type, the signature and the information in the received certificate. The EA/AA shall discard all EA/AA certificates that are not correctly verified and issue a new request.

4.4.1.4. C-ITS station

(152) The C-ITS station shall verify the EC/AT response received from the EA/AA against its original request, including the signature and the certificate chain. It shall discard all EC/AT responses that are not correctly verified. In such cases, it should send a new EC/AT request.

4.4.2. Publication of the certificate

(153) TLM certificates and their link certificates shall be made available to all participants through the CPOC.

(154) Root CA certificates are published by the CPOC via the ECTL, which is signed by the TLM.

(155) Sub-CAs' (EAs' and AAs') certificates are published by the root CA.

(156) ECs and ATs are not published.

4.4.3. Notification of certificate issuance

There are no notifications of issuance.

4.5. Key pair and certificate usage

*4.5.1. **Private key and certificate usage***

4.5.1.1. Private key and certificate usage for TLM

(157) The TLM shall use its private keys to sign its own (TLM and link) certificates and the ECTL.

(158) The TLM certificate shall be used by PKI participants to verify the ECTL and authenticate the TLM.

4.5.1.2. Private key and certificates usage for root CAs

(159) Root CAs shall use their private keys to sign their own certificates, CRL, link certificates and the EA/AA certificates.

(160) Root CA certificates shall be used by PKI participants to verify the associated AA and EA certificates, link certificates and the CRLs.

4.5.1.3. Private key and certificate usage for EAs and AAs

(161) EAs shall use their private keys to sign ECs and for enrolment request decryption.

(162) EA certificates shall be used to verify the signature of the associated ECs and for EC and AT request encryption by EEs as defined in [1].

(163) AAs shall use their private keys to sign ATs and for AT request decryption.

(164) AA certificates shall be used by EEs to verify associated ATs and for AT request encryption as defined in [1].

4.5.1.4. Private key and certificate usage for end-entity

(165) EEs shall use the private key corresponding to a valid EC to sign a new enrolment request as defined in [1]. The new private key shall be used to build the inner signature in the request to prove possession of the private key corresponding to the new EC public key.

(166) EEs shall use the private key corresponding to a valid EC to sign an authorisation request as defined in [1]. The private key corresponding to the new AT should be used to build the inner signature in the request to prove possession of the private key corresponding to the new AT public key.

(167) EE shall use the private key corresponding to an appropriate AT to sign C-ITS messages as defined in [5].

4.5.2. Relying party public key and certificate usage

(168) Relying parties use the trusted certification path and associated public keys for the purposes referred to in the certificates and to authenticate the trusted common identity of ECs and ATs.

(169) Root CA, EA and AA certificates, ECs and ATs shall not be used without a preliminary check by a relying party.

4.6. Certificate renewal

Not allowed.

4.7. Certificate re-key

4.7.1. Circumstances for certificate re-key

(170) Certificate re-key shall be processed when a certificate reaches the end of its lifetime or a private key reaches the end of operational use, but the trust relation with the CA still exists. A new key pair and the corresponding certificate shall be generated and issued in all cases.

4.7.2. Who may request re-key

4.7.2.1. *Root CA*

(171) The root CA does not request re-key. The re-keying process is an internal process for the root CA, because its certificate is self-signed. The root CA shall re-key either with link certificates or new issuance (see section 4.3.1.1).

4.7.2.2. *TLM*

(172) The TLM does not request re-key. The re-keying process is internal for the TLM, because the TLM certificate is self-signed.

4.7.2.3. EA and AA

(173) The sub-CA's certificate request has to be submitted in due time in order to be sure to have a new sub-CA certificate and operational sub-CA key pair before

expiry of the current private sub-CA key. The date of submission must also take account of the time required for approval.

4.7.2.4. C-ITS station

Not applicable.

4.7.3. Re-keying process

4.7.3.1. TLM certificate

(174) The TLM decides to re-key on the basis of the requirements in sections 6.1 and 7.2. The detailed process is set out in its CPS.

(175) The TLM shall execute the re-keying process in due time in order to allow for the distribution of the new TLM certificate and link certificate to all participants before the current TLM certificate expires.

(176) The TLM shall use link certificates for re-keying and to guarantee the trust relation of the new self-signed certificate. The newly generated TLM and link certificate is transferred to the CPOC.

4.7.3.2. Root CA certificate

(177) The root CA decides to re-key on the basis of the requirements of sections 6.1.5 and 7.2. The detailed process should be defined in its CPS.

(178) The root CA shall execute the re-keying process in due time (before the root CA certificate expires) in order to allow for insertion of the new certificate in the ECTL before the root CA certificate becomes valid (see section 5.6.2). The re-keying process shall be carried out either via link certificates or like an initial request.

4.7.3.3. EA and AA certificates

(179) The EA or AA shall request a new certificate as follows:

Step	**Indication**	**Re-keying request**
1	**Key-pair generation**	The sub-CAs (EAs and AAs) shall generate new key pairs in accordance with section 6.1.
2	**Generation of certificate request and inner signature**	The sub-CA generates a certificate request out of the newly generated public key considering the naming scheme (subject_info) of section 3, the signature algorithm, the Service Specific Permissions (SSP) and optional additional parameter, and generates the inner signature with the corresponding new private key. If an encryption key is required, the sub-CA must also prove possession of the corresponding private decryption key.
3	**Generate outer signature**	The whole request shall be signed with the current valid private key to guarantee the authenticity of the signed request.
4	**Send request to root CA**	The signed request shall be submitted to the corresponding root CA.
5	**Verification of request**	The corresponding root CA shall verify the integrity and authenticity of the request. First, it shall check the outer signature. If the verification is positive, it shall check the inner signature. Where there is proof of possession of the private decryption key, it shall also check this proof.
6	**Accept or reject request**	If all checks lead to a positive result, the root CA accepts the request; otherwise, it rejects it.

7	**Generate and issue certificate**	The root CA generates a new certificate and distributes it to the requesting sub-CA.
8	**Send response**	The sub-CA shall send a status message (as to whether or not the certificate was received) to the root CA.

Table 3: Re-keying process for EAs and AAs

(180) During automatic re-keying for sub-CAs, the root CA shall ensure that the requestor is indeed in possession of its private key. Appropriate protocols for proof of possession of private decryption keys shall be applied, for instance as defined in RFC 4210 and 4211. For private signature keys, the inner signature should be used.

4.7.3.4. C-ITS station certificates

Not applicable for AT.

4.8. Certificate modification

Not allowed.

4.9. Certificate revocation and suspension

See section 7

4.10. Certificate status services

4.10.1. Operational characteristics

Not applicable

4.10.2. Service availability

Not applicable

4.10.3. Optional features

Not applicable

4.11. End of subscription

Not applicable

4.12. Key escrow and recovery

4.12.1. Subscriber

4.12.1.1. Which key pair can be escrowed

Not applicable.

4.12.1.2. Who can submit a recovery application

Not applicable.

4.12.1.3. Recovery process and responsibilities

Not applicable.

4.12.1.4. Identification and authentication

Not applicable.

4.12.1.5. Approval or rejection of recovery applications

Not applicable.

4.12.1.6.KEA and KRA actions during key pair recovery

Not applicable.

4.12.1.7.KEA and KRA availability

Not applicable.

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

(181) The PKI is composed of the root CA, the EA/AA, the CPOC and the TLM, including their ICT components (e.g. networks and servers).

(182) In this section, the entity responsible for an element of the PKI is identified by the element itself. In other words, the sentence ‘the CA is responsible for executing the audit’ is equivalent to ‘the entity or personnel managing the CA is responsible for executing …’.

(183) The term ‘C-ITS trust model elements’ includes the root CA, the TLM, the EA/AA, the CPOC and the secure network.

5.1. Physical controls

(184) All C-ITS trust model operations shall be conducted in a physically protected environment that deters, prevents and detects unauthorised use of, access to or disclosure of sensitive information and systems. C-ITS trust model elements shall use physical security controls in compliance with ISO 27001 and ISO 27005.

(185) The entities managing the C-ITS trust model elements shall describe the physical, procedural and personnel security controls in their CPS. In particular, the CPS shall cover information about the site location and construction of the buildings and their physical security controls guaranteeing controlled access to all rooms used in the facility of the C-ITS trust model entities.

5.1.1. Site location and construction

5.1.1.1. Root CA, CPOC, TLM

(186) The location and construction of the facility housing the root CA, CPOC and TLM equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall be consistent with facilities used to house high-value and sensitive information. Root CA shall be operated in a dedicated physical area separated from other PKI components’ physical areas.

(187) The root CA, CPOC and TLM shall implement policies and procedures to ensure that a high level of security is maintained in the physical environment in which the root CA equipment is installed, so as to guarantee that:

- it is isolated from networks outside the trust model;
- it is separated into a series of (at least two) progressively more secure physical perimeters;
- sensitive data (HSM, key pair backup, activation data, etc.) are stored in a dedicated safe located in a dedicated physical area under multiple access control.

(188) The security techniques employed shall be designed to resist a large number and combination of different forms of attack. The mechanisms used shall include at least:

- perimeter alarms, closed-circuit television, reinforced walls and motion detectors;
- two-factor authentication (e.g. smartcard and PIN) for every person and badge to enter and leave the root CA facilities and safe physical secured area.

(189) The root CA, CPOC and TLM use authorised personnel to continually monitor the facility housing equipment on a 7x24x365 basis. The operational environment (e.g. physical facility) shall never be left unattended. The personnel of the operational environment shall never have access to the secure areas of root CAs or sub-CAs unless authorised.

5.1.1.2. *EA/AA*

(190) The same provisions of section 5.1.1.1 apply.

5.1.2. Physical access

5.1.2.1. Root CA, CPOC, TLM

(191) Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall always be protected from unauthorised access. The physical security mechanisms for equipment shall at least:

- monitor, either manually or electronically, for unauthorised intrusion at all times;
- ensure that no unauthorised access to the hardware and activation data is permitted;
- ensure that all removable media and paper containing sensitive plain-text information are stored in a secure container;
- ensure that any individual entering secure areas who is non-authorised on a permanent basis shall not be left without supervision by an authorised employee of the root CA, CPOC and TLM facilities;
- ensure that an access log is maintained and inspected periodically;
- provide at least two layers of progressively increasing security, e.g. at perimeter, building and operational room level;

- require two trusted-role physical access controls for the cryptographic HSM and activation data.

(192) A security check of the facility housing equipment shall be carried out if it is to be left unattended. At a minimum, the check shall verify that:

- the equipment is in a state that is appropriate for the current mode of operation;
- for off-line components, all equipment is shut down;
- any security containers (tamper-proof envelope, safe, etc.) are properly secured;
- physical security systems (e.g. door locks, vent covers, electricity) are functioning properly;
- the area is secured against unauthorised access.

(193) Removable cryptographic modules shall be deactivated prior to storage. When not in use, such modules and the activation data used to access or enable them shall be placed in a safe. Activation data shall either be memorised or recorded and stored in a manner commensurate with the security afforded to the cryptographic module. They shall not be stored with the cryptographic module, so as to avoid only one person having access to the private key.

(194) A person or group of trusted roles shall be made explicitly responsible for making such checks. Where a group of people is responsible, a log shall be maintained that identifies the person performing each check. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and confirms that all necessary physical protection mechanisms are in place and activated.

5.1.2.2. *EA/AA*

(195) The same provisions of section 5.1.2.1 apply.

5.1.3. Power and air conditioning

(196) Secure facilities of C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall be equipped with reliable access to electric power to ensure operation with no or minor failures. Primary and back-up installations are required in the event of external power failure and smooth shutdown of the C-ITS trust model equipment in the event of a lack of power. C-ITS trust model facilities shall be equipped with heating/ventilation/air-conditioning systems to maintain the temperature and relative humidity of the C-ITS trust model equipment within operational range. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.4. Water exposures

(197) Secure facilities of C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) should be protected in a way that minimises impact from water exposure. For this reason, water and soil pipes shall be avoided. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.5. Fire prevention and protection

(198) To prevent damaging exposure to flame or smoke, the secure facilities of C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall be constructed and equipped accordingly and procedures shall be implemented to address fire-related threats. Media storage should be protected against fire in appropriate containers.

(199) C-ITS trust model elements shall protect physical media holding backups of critical system data or any other sensitive information from environmental hazards and unauthorised use of, access to or disclosure of such media. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.6. Media management

(200) Media used in the C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) are securely handled to protect them from damage, theft and unauthorised access. Media management procedures are implemented to protect against obsolescence and deterioration of media in the period for which records have to be retained.

(201) Sensitive data shall be protected against being accessed as a result of re-used storage objects (e.g. deleted files), which may make the sensitive data accessible to unauthorised users.

(202) An inventory of all information assets shall be maintained and requirements set out for the protection of those assets that are consistent with the risk analysis. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.7. Waste disposal

(203) C-ITS trust model elements (root CA, CPOC, TLM, EA and AA) shall implement procedures for the secure and irreversible disposal of waste (paper, media or any other waste) to prevent the unauthorised use of, access to or disclosure of waste containing confidential/private information. All media used for the storage of sensitive information, such as keys, activation data or files, shall be destroyed before being released for disposal. The CPS of the C-ITS trust model element will describe in detail the plan and processes to implement such requirements.

5.1.8. Off-site backup

5.1.8.1. Root CA, CPOC and TLM

(204) Full back-ups of root CA, CPOC and TLM components, sufficient to recover from system failure, are made offline after root CA, CPOC and TLM deployment and after each new key-pair generation. Back-up copies of essential business information (key pair and CRL) and software are made regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems are regularly tested to ensure that they meet the requirements of the business continuity plan. At least one full backup copy is stored at an offsite location (disaster recovery). The back-up copy is stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

(205) Backup data are subject to the same access requirements as the operational data. Backup data shall be encrypted and stored offsite. In the event of complete loss of data, the information required for putting the root CA, CPOC and TLM back into operation shall be completely recovered from the backup data.

(206) Private root CA, CPOC and TLM key material shall not be backed up using standard backup mechanisms, but using the backup function of the cryptographic module.

5.1.8.2. *EA/AA*

(207) The processes described in the section 5.1.8.1 apply to this section.

5.2. Procedural controls

This section describes requirements for roles, duties and identification of personnel.

5.2.1. Trusted roles

(208) Employees, contractors and consultants who are assigned to trusted roles shall be considered ‘trusted persons’. Persons seeking to become trusted persons for obtaining a trusted position shall meet the screening requirements of this certificate policy.

(209) Trusted persons have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in certificate applications;
- the acceptance, rejection or other processing of certificate applications, revocation requests or renewal requests;
- the issuance or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

(210) Trusted roles include, but are not limited to:

- customer service;
- system administration;
- designated engineering;
- executives charged with the management of infrastructural trustworthiness.

(211) The CA shall provide clear descriptions of all trusted roles in its CPS.

5.2.2. Number of persons required per task

(212) C-ITS trust model elements shall establish, maintain and enforce rigorous control procedures to ensure the separation of duties based on trusted roles and to ensure that multiple trusted persons are required to perform sensitive tasks. The C-ITS trust model elements (TLM, CPOC, root CA, EA and AA) should comply with [4] and with the requirements in the following paragraphs.

(213) Policy and control procedures are in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as access to and the

management of CA cryptographic hardware (HSM) and its associated key material, must require the authorisation of multiple trusted persons.

(214) These internal control procedures shall be designed to ensure that at least two trusted persons are required to have physical or logical access to the device. Restrictions on access to CA cryptographic hardware must be strictly enforced by multiple trusted persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

5.2.3. *Identification and authentication for each role*

(215) All persons assigned a role, as described in this CP, are identified and authenticated so as to guarantee that the role enables them to perform their PKI duties.

(216) C-ITS trust model elements shall verify and confirm the identity and authorisation of all personnel seeking to become trusted persons before they are:

- issued with their access devices and granted access to the required facilities;
- given electronic credentials to access and perform specific functions on CA systems.

(217) The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4. *Roles requiring separation of duties*

(218) Roles requiring separation of duties include (but are not limited to):

- the acceptance, rejection and revocation of requests, and other processing of CA certificate applications;
- the generation, issuing and destruction of a CA certificate.

(219) Segregation of duties may be enforced using PKI equipment, procedures or both. No individual shall be assigned more than one identity unless approved by the root CA.

(220) The part of the root CA and CA concerned with certificate generation and revocation management shall be independent of other organisations for its decisions relating to the establishing, provisioning, maintaining and suspending of services in line with the applicable certificate policies. In particular, its senior executive, senior staff and staff in trusted roles shall be free from any commercial, financial and other pressures that might adversely influence trust in the services it provides.

(221) The EA and AA that serve mobile C-ITS stations shall be separate operational entities, with separate IT infrastructure and IT management teams. In accordance with the GDPR, the EA and AA shall not exchange any personal data, except for the authorisation of AT requests. They shall transfer data relating to the approval of AT requests only using the authorisation validation protocol of [1] over a dedicated secure interface. Other protocols may be used, provided that [1] is implemented.

(222) The logfiles stored by the EA and AA may be used solely for the purpose of revoking misbehaving ECs based on ATs in intercepted malicious CAM/DENM messages. After a CAM/DENM message has been identified as malicious, the AA will look up the AT's verification key in its issuance logs and submit a revocation request to the EA containing the encrypted signature under the EC private key that was used during the issuance of the AT. All logfiles must be adequately protected against access by unauthorised parties and may not be shared with other entities or authorities.

Note: At the time of drafting this version of the CP, the design of the misbehaving function is not defined. It is planned to potentially design the misbehaving function in future revisions of the policy.

5.3. Personnel controls

5.3.1. Qualifications, experience and clearance requirements

(223) C-ITS trust model elements employ a sufficient number of personnel with the expert knowledge, experience and qualifications necessary for the job functions and services offered. PKI personnel fulfil those requirements through formal training and credentials, actual experience or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel sub-contractors have job descriptions defined to ensure separation of duties and privileges, and position sensitivity is determined on the basis of duties and access levels, background screening, and employee training and awareness.

5.3.2. Background check procedures

(224) C-ITS trust model elements shall conduct background checks on personnel seeking to become trusted persons. Background checks shall be repeated for personnel holding trusted positions at least every five years.

(225) The factors revealed in a background check that may be considered grounds for rejecting candidates for trusted positions or for taking action against an existing trusted person include (but are not limited to) the following:

- misrepresentations made by the candidate or trusted person;
- highly unfavourable or unreliable professional references;
- certain criminal convictions;
- indications of a lack of financial responsibility.

(226) Reports containing such information shall be evaluated by human resources personnel, who shall take reasonable action in the light of the type, magnitude and frequency of the behaviour uncovered by the background check. Such action may include measures up to and including cancelling offers of employment made to candidates for trusted positions or terminating the employment of existing trusted persons. The use of information revealed in a background check as a basis for such action shall be subject to applicable law.

(227) Background investigation of persons seeking to become a trusted person includes but is not limited to:

- confirmation of previous employment;

- a check of professional references covering their employment over a period of at least five years;
- a confirmation of the highest or most relevant educational degree obtained;
- a search of criminal records.

5.3.3. *Training requirements*

(228) C-ITS trust model elements shall provide their personnel with the requisite training to fulfil their responsibilities relating to CA operations competently and satisfactorily.

(229) Training programmes shall be reviewed periodically and their training shall address matters that are relevant to functions performed by their personnel.

(230) Training programmes shall address matters that are relevant to the particular environment of the trainee, including:

- security principles and mechanisms of the C-ITS trust model elements;
- hardware and software versions in use
- all duties the person is expected to perform, and internal and external reporting processes and sequences;
- PKI business processes and workflows;
- incident and compromise reporting and handling;
- disaster recovery and business continuity procedures;
- sufficient IT knowledge.

5.3.4. *Retraining frequency and requirements*

(231) The persons assigned to trusted roles are required to refresh the knowledge they have gained from training on an ongoing basis using a training environment. Training must be repeated whenever deemed necessary and at least every two years.

(232) C-ITS trust model elements shall provide their staff with refresher training and updates to the extent and with the frequency required to ensure that they maintain the required level of proficiency to fulfil their job responsibilities competently and satisfactorily.

(233) Individuals in trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan and the execution of that plan shall be documented.

5.3.5. *Job rotation frequency and sequence*

(234) No stipulation as long as the technical skills, experience and access rights are ensured. The administrators of the C-ITS trust model elements shall ensure that changes in staff do not affect the security of the system.

5.3.6. *Sanctions for unauthorised actions*

(235) Each C-ITS trust model elements must develop a formal disciplinary process to ensure that unauthorised actions are appropriately sanctioned. In severe cases, the role assignments and corresponding privileges must be withdrawn.

5.3.7. Independent contractor requirements

(236) C-ITS trust model elements may permit independent contractors or consultants to become trusted persons only to the extent necessary to accommodate clearly defined outsourcing relationships and on condition that the entity trusts the contractors or consultants to the same extent as if they were employees and that they fulfil the requirements applicable to employees.

(237) Otherwise, independent contractors and consultants shall have access to C-ITS PKI secure facilities only if escorted and directly supervised by trusted persons.

5.3.8. Documentation supplied to personnel

(238) C-ITS trust model elements shall provide their personnel with requisite training and access to the documentation they need to fulfil their job responsibilities competently and satisfactorily.

5.4. Audit logging procedures

(239) This section sets out requirements as regards the types of event to be recorded and the management of audit logs.

5.4.1. Types of event to be recorded and reported by each CA

(240) A CA representative shall regularly review the CA logs, events and procedures.

(241) C-ITS trust model elements shall record the following types of audit event (if applicable):

- physical facility access – access by physical persons to the facilities will be recorded by storing the access requests through smartcards. An event will be created every time a record is created;
- trusted roles management – any change in the definition and level of access of the different roles will be recorded, including modification of the attributes of the roles. An event will be created every time a record is created;
- logical access – an event will be generated when an entity (e.g. a program) has access to sensitive areas (i.e. networks and servers);
- backup management – an event is created every time a backup is completed, either successfully or unsuccessfully;
- log management – logs will be stored. An event is created when the log size exceeds a specific size;
- data from the authentication process for subscribers and C-ITS trust model elements – events will be generated for every authentication request by subscribers and C-ITS trust model elements;
- acceptance and rejection of certificate requests, including certificate creation and renewal – an event will be generated periodically with a list of accepted and rejected certificate requests in the previous seven days;
- manufacturer registration – an event will be created when a manufacturer is registered;
- C-ITS station registration – an event will be created when a C-ITS station is registered;

- HSM management – an event will be created when an HSM security breach is recorded;
- IT and network management, as they pertain to the PKI systems – an event will be created when a PKI server is shut down or restarted;
- security management (successful and unsuccessful PKI system access attempts, PKI and security system actions performed, security profile changes, system crashes, hardware failures and other anomalies, firewall and router activities; and entries to and exits from the PKI facilities);
- event-related data will be stored for at least five years unless additional national rules apply.

(242) In accordance with the GDPR, the audit logs shall not permit access to privacy-related data concerning C-ITS station private vehicles.

(243) Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

(244) Each event related to certificate life-cycle is logged in such a way that it can be attributed to the person that performed it. All data relating to a personal identity are encrypted and protected against non-authorised access.

(245) At a minimum, each audit record includes the following (recorded automatically or manually for each auditable event):

- type of event (as from the list above);
- trusted date and time the event occurred;
- result of the event – success or failure where appropriate;
- identity of the entity and/or operator that caused the event if applicable;
- identity of the entity for which the event is addressed.

5.4.2. *Frequency of processing log*

(246) Audit logs shall be reviewed in response to alerts based on irregularities and incidents within the CA systems and in addition periodically every year.

(247) Audit-log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit-log summary. Audit-log reviews shall include a verification that the log has not been tampered with, an inspection of all log entries and an investigation of any alerts or irregularities in the logs. Action taken on the basis of audit-log reviews shall be documented.

(248) The audit log is archived at least weekly. An administrator shall archive it manually if the free disk space for audit log is below the expected amount of audit-log data produced that week.

5.4.3. *Retention period for audit log*

(249) Log records relating to certificate life-cycles are kept for at least five years after the corresponding certificate expires.

5.4.4. *Protection of audit log*

(250) The integrity and confidentiality of the audit log is guaranteed by a role-based access control mechanism. Internal audit logs may be accessed only by administrators; certificate life-cycle related audit logs may also be accessed by users with the appropriate authorisation via a web page with user login. Access has to be granted with multi-user (at least two-user) and at least two-level authentication. It must be technically ensured that users cannot access their own log files.

(251) Each log entries shall be signed using key material from HSM.

(252) Event logs containing information that can lead to personal identification, such as a private vehicle, are encrypted in such a way that only authorised persons can read them.

(253) Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long-term media) within the period for which the logs have to be held.

(254) Event logs are protected in such a way as to remain readable for the duration of their storage period.

5.4.5. *Audit log backup procedures*

(255) Audit logs and summaries are backed up via enterprise backup mechanisms, under the control of authorised trusted roles, separated from their component source generation. Audit-log backups are protected with the same level of trust that applies to the original logs.

5.4.6. *Audit collection system (internal or external)*

(256) The equipment of the C-ITS trust model elements shall activate the audit processes at system startup and deactivate them only at system shutdown. If audit processes are not available, the C-ITS trust model element shall suspend its operation.

(257) At the end of each operating period and at the re-keying of certificates, the collective status of equipment should be reported to the operations manager and operation governing body of the respective PKI element.

5.4.7. *Notification to event-causing subject*

(258) Where an event is logged by the audit collection system, it guarantees that the event is linked to a trusted role.

5.4.8. *Vulnerability assessment*

(259) The role in charge of conducting audit and roles in charge of realising PKI system operation in the C-ITS trust model elements explain all significant events in an audit-log summary. Such reviews involve verifying that the log has not been tampered with and that there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken as a result of these reviews is documented.

(260) C-ITS trust model elements shall:

- implement organisational and/or technical detection and prevention controls under the control of the C-ITS trust model elements to protect PKI systems against viruses and malicious software;
- document and follow a vulnerability correction process that addresses the identification, review, response and remediation of vulnerabilities;
- undergo or perform a vulnerability scan:
    - after any system or network changes determined by the C-ITS trust model elements as significant for PKI components; and
    - at least once a month, on public and private IP addresses identified by the CA, CPOC as the PKI's systems,
- undergo a penetration test on the PKI's systems on at least an annual basis and after infrastructure or application upgrades or modifications determined by the C-ITS trust model elements as significant for CA's PKI component;
- for online systems, record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics and independence necessary to provide a reliable vulnerability or penetration test;
- track and remediate vulnerabilities in line with enterprise cybersecurity policies and risk mitigation methodology.

5.5. Record archiving

5.5.1. Types of record archived

(261) C-ITS trust model elements shall archive records detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following PKI events records shall be archived (if applicable):

- physical facility access log of C-ITS trust model elements (minimum one year);
- trusted roles management log for C-ITS trust model elements (minimum 10 years);
- IT access log for C-ITS trust model elements (minimum five years);
- CA key creation, use and destruction log (minimum five years) (not for TLM and CPOC);
- certificate creation, use and destruction log (minimum two years);
- CPA request log (minimum two years);
- activation data management log for C-ITS trust model elements (minimum five years);
- IT and network log for C-ITS trust model elements (minimum five years);

- PKI documentation for C-ITS trust model elements (minimum five years);
- security incident and audit report for C-ITS trust model elements (minimum 10 years);
- system equipment, software and configuration (minimum five years).

(262) The C-ITS trust model elements shall retain the following documentation relating to certificate requests and the verification thereof, and all TLM, root CAs and CA certificates and CRL thereof, for at least seven years after any certificate based on that documentation ceases to be valid:

- PKI audit documentation kept by C-ITS trust model elements;
- CPS documents kept by C-ITS trust model elements;
- contract between CPA and other entities kept by C-ITS trust model elements;
- certificates (or other revocation information) kept by CA and TLM;
- certificate request records in root CA system (not applicable to the TLM);
- other data or applications sufficient to verify archive contents;
- all work related to or from the C-ITS trust model elements and compliance auditors.

(263) The CA entity shall retain all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven years after any certificate based on that documentation ceases to be valid.

5.5.2. *Retention period for archive*

(264) Without prejudice to regulations requiring a longer archival period, C-ITS trust model elements shall keep all records for at least five years after the corresponding certificate has expired.

5.5.3. *Protection of archive*

(265) C-ITS trust model elements shall store the archive of records in a safe, secure storage facility separate from the CA equipment, with physical and procedural security controls equivalent to or better than those of the PKI.

(266) The archive shall be protected against unauthorised viewing, modification, deletion or other tampering by storage in a trustworthy system.

(267) The media holding the archive data and the applications required to process them shall be maintained to ensure that they can be accessed for the period set in this CP.

5.5.4. *System archive and storage*

(268) C-ITS trust model elements shall incrementally back up system archives of such information on a daily basis and perform full backups on a weekly basis. Copies of paper-based records shall be maintained in an offsite secure facility.

5.5.5. Requirements for time-stamping of records

(269) C-ITS trust model elements managing a revocation database shall ensure that the records contain information as to the time and date when revocation records are created. The integrity of such information will be implemented with cryptographic-based solutions.

5.5.6. Archive collection system (internal or external)

(270) The archive collection system is internal.

5.5.7. Procedures to obtain and verify archive information

(271) All C-ITS trust model elements shall allow only authorised trusted persons to access the archive. Root CAs and CAs shall describe the procedures for creating, verifying, packaging, transmitting and storing archive information in the CPS.

(272) Root CA and CA equipment shall verify the integrity of the information before it is restored.

5.6. Key changeover for C-ITS trust model elements

(273) The following elements of the C-ITS trust model have specific requirements for their key changeover: TLM, root CA and EA/AA certificates.

*5.6.1. **TLM***

(274) The TLM shall delete its private key on expiry of the corresponding certificate. It shall generate a new key pair and corresponding TLM certificate before deactivation of the current valid private key. It shall take care that the new (link) certificate is inserted in the ECTL in time to be distributed to all C-ITS stations before it becomes valid. The link certificate and the new self-signed certificate are transferred to the CPOC.

5.6.2. Root CA

(275) The root CA shall deactivate and delete the current private key (including backup keys), so that it will not issue EA/AA certificates with a validity that extends beyond the validity of the root CA certificate.

(276) The root CA shall generate a new key pair and corresponding root CA and link certificate before deactivation of the current private key (including backup keys) and send it to the TLM for insertion into the ECTL. The validity period of the new root CA certificate shall start at the planned deactivation of the current private key. The root CA shall take care that the new certificate is inserted in the ECTL in time to be distributed to all C-ITS stations before it becomes valid.

(277) The root CA shall activate the new private key when the corresponding root CA certificate becomes valid.

5.6.3. EA/AA certificate

(278) The EA/AA shall deactivate the current private key so that it will not issue ECs/ATs with a validity that extends beyond the validity of the EA/AA certificate.

(279) The EA/AA shall generate a new key pair and request a corresponding EA/AA certificate before deactivation of the current private key. The validity period of

the new EA/AA certificate shall start at the planned deactivation of the current private key. The EA/AA shall take care that the new certificate can be published in time to be distributed to all C-ITS stations before it becomes valid.

(280) The EA/AA shall activate the new private key when the corresponding EA/AA certificate becomes valid.

5.6.4. Auditor

No provisions.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling

(281) C-ITS trust model elements shall monitor their equipment on an ongoing basis, so as to detect potential hacking attempts or other forms of compromise. In such an event, they shall investigate in order to determine nature and degree of damage.

(282) If the personnel responsible for the management of the root CA or TLM detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and the degree of damage. In the event of the private key being compromised, the root CA certificate shall be revoked. The IT security experts of the CPA shall assess the scope of potential damage in order to determine whether the PKI needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI has been compromised. In addition, the CPA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the CPA business continuity plan.

(283) Incident, compromise and business continuity are covered in the CPS, which may also rely on other enterprise resources and plans for its implementation.

(284) If the personnel responsible for the management of the EA/AA/CPOC detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and degree of damage. The personnel responsible for the management of the CA or the CPOC entity shall assess the scope of potential damage in order to determine whether the PKI component needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI component has been compromised. In addition, the sub-CA entity determines which services are to be maintained and how, in accordance with the sub-CA entity business continuity plan. In the event of a PKI component being compromised, the CA entity shall alert its own root CA and the TLM through the CPOC.

(285) Incident, compromise and business continuity are covered in the CPS of the root CA or the TLM or other relevant documents in the case of the CPOC, which may also rely on other enterprise resources and plans for their implementation.

(286) The root CA and CA shall alert, with precise information on the consequences of the incident, each Member State representative and root CA with which they have an agreement in the C-ITS context, in order to allow them to activate their own incident management plan.

5.7.2. Corruption of computing resources, software and/or data

(287) If a disaster is discovered that prevents the proper operation of a C-ITS trust model element, that element shall suspend its operation and investigate whether the private key has been compromised (except CPOC). Defective hardware shall be replaced as quickly as possible and the procedures described in sections 5.7.3 and 5.7.4 shall apply.

(288) The corruption of computing resources, software and/or data shall be reported to the root CA within 24 hours for the highest levels of risk. All other events must be included in the periodic report of the root CA, EAs and AAs.

5.7.3. Entity private key compromise procedures

(289) If the private key of a root CA is compromised, lost, destroyed or suspected of being compromised, the root CA shall:

- suspend its operation;
- start the disaster recovery and migration plan;
- revoke its root CA certificate;
- investigate the ‘key issue’ that generated the compromise and notify the CPA, which will revoke the root-CA certificate through the TLM (see section 7);
- alert all subscribers with which it has an agreement.

(290) If an EA/AA’s key is compromised, lost, destroyed or suspected of being compromised, the EA/AA shall:

- suspend its operation;
- revoke its own certificate;
- investigate the ‘key issue’ and notify the root CA;
- alert subscribers with which an agreement exists.

(291) If a C-ITS station EC or AT key is compromised, lost, destroyed or suspected of being compromised, the EA/AA to which the C-ITS station is subscribed shall:

- revoke the EC of the affected ITS;
- investigate the ‘key issue’ and notify the root CA;
- alert subscribers with which it has an agreement.

(292) Where any of the algorithms or associated parameters used by the root CA and/or CA or C-ITS stations becomes insufficient for its remaining intended usage, the CPA (with a recommendation from cryptographic experts) shall inform the root CA entity with which it has an agreement and change the algorithms used. (For details, see section 6 and the CPSs of the root CA and sub-CA).

5.7.4. Business continuity capabilities after a disaster

(293) The C-ITS trust model elements operating secure facilities for CA operations shall develop, test, maintain and implement a disaster recovery plan designed

to mitigate the effects of any natural or man-made disaster. Such plans address the restoration of information systems services and key business functions.

(294) After an incident of a certain risk level, the compromised CA must be re-audited by an accredited PKI auditor (see section 8).

(295) Where the compromised CA is unable to operate any longer (e.g. following a severe incident), a migration plan must be drawn up for the transfer of its functions to another root CA. At least the EU root CA shall be available to support the migration plan. The compromised CA shall cease its functions.

(296) The root CAs shall include the disaster recovery plan and the migration plan in the CPS.

5.8. Termination and transfer

5.8.1. TLM

(297) The TLM shall not terminate its operation, but an entity managing the TLM may take over another entity.

(298) In the event of the managing entity changing:

- it shall request the CPA's approval for a change of TLM management from the old entity to the new entity;
- the CPA shall approve the change of TLM management;
- all audit logs and archived records shall be transferred from the old management entity to the new entity.

5.8.2. Root CA

(299) The root CA shall not terminate/start its operation without establishing a migration plan (set out in the relevant CPS) that guarantees ongoing operation for all subscribers.

(300) In the event of the termination of the root CA service, the root CA shall:

- notify the CPA;
- notify the TLM so that it can delete the root CA certificate from the ECTL;
- revoke the corresponding root CA by issuing a CRL containing itself;
- alert root CAs with which it has an agreement for the renewal of EA/AA certificates;
- destroy the root CA private key;
- communicate last revocation status information (CRL signed by root CA) to the relying party, indicating clearly that it is the latest revocation information;
- archive all audit logs and other records prior to termination of the PKI;
- transfer archived records to an appropriate authority.

(301) The TLM shall delete the corresponding root CA certificate from the ECTL.

5.8.3. ***EA/AA***

(302) In the event of the termination of the EA/AA service, the EA/AA entity provides notice prior to the termination. An EA or AA shall not terminate/start its operation without establishing a migration plan (set out in the relevant CPS) that guarantees ongoing operation for all subscribers. The EA/AA shall:

- inform the root CA by registered letter;
- destroy the CA private key;
- transfer its database to the entity appointed by the root CA;
- stop issuing certificates;
- during the transfer of its database and until the database is fully operational in a new entity, maintain capability to authorise requests from the responsible privacy authority;
- where a sub-CA has been compromised, the root CA shall revoke the sub-CA and issue a new CRL with a list of revoked sub-CAs;
- archive all audit logs and other records prior to terminating the PKI;
- transfer archived records to an entity designated by the root CA.

(303) In the event of termination of the CA's services, the CA shall be responsible for keeping all relevant records regarding the needs of CA and PKI components.

6. TECHNICAL SECURITY CONTROLS

6.1. Key-pair generation and installation

6.1.1. TLM, root CA, EA, AA

(304) The key-pair generation process shall fulfil the following requirements:

- each participant shall be able to generate its own key pairs in accordance with sections 6.1.4 and 6.1.5;
- the process of deriving symmetric encryption keys and a MAC key for certificate requests (ECIES) shall be carried out in line with [1] and [5];
- the key-generation process shall use the algorithms and key lengths described in sections 6.1.4.1 and 6.1.4.2;
- the key-pair generation process shall be subject to the requirements of 'secure storing of private keys' (see section 6.1.5);
- the root CAs and their subscribers (sub-CAs) shall ensure that the integrity and authenticity of their public keys and any associated parameters are maintained during distribution to sub-CA registered entities.

6.1.2. EE — mobile C-ITS station

(305) Each mobile C-ITS station shall generate its own key pairs in accordance with sections 6.1.4 and 6.1.5.

(306) The process of deriving symmetric encryption keys and a MAC key for certificate requests (ECIES) shall be carried out in accordance with [1] and [5].

(307) The key-generation processes shall use the algorithms and key lengths described in sections 6.1.4.1 and 6.1.4.2.

(308) The key-pair generation processes shall be subject to the requirements of ‘secure storing of private keys’ (see section 6.1.5).

6.1.3. EE — fixed C-ITS station

(309) Each fixed C-ITS station shall generate its own key pair in accordance with sections 6.1.4 and 6.1.5.

(310) The key-generation processes shall use the algorithms and key lengths described in section 6.1.4.1 and 6.1.4.2.

(311) The key-pair generation processes shall be subject to the requirements of ‘secure storing of private keys’ (see section 6.1.5).

6.1.4. Cryptographic requirements

(312) All PKI participants shall satisfy the cryptographic requirements set out in the following paragraphs as regards signature algorithm, key length, random number generator and link certificates.

6.1.4.1. *Algorithm and key length - signature algorithms*

(313) All PKI participants (TLM, root CA, EA, AA and C-ITS stations) shall be able to generate key pairs and use the private key for signing operations with selected algorithms at the latest two years after entry into force of this Regulation in accordance with Table 4.

(314) All PKI participants that must check the integrity of the ECTL, certificates and/or signed messages in accordance with their role, as defined in section 1.3.6, shall support the corresponding algorithms listed in Table 5 for verification. In particular, C-ITS stations shall be able to check the integrity of the ECTL.

	TLM	root CA	EA	AA	C-ITS station
ECDSA_nistP256_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	-	-
X indicates mandatory support					

Table 4: Generating key pairs and use of private key for signing operations

	TLM	root CA	EA	AA	C-ITS station
ECDSA_nistP256_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	X	X
X indicates mandatory support					

Table 5: Verification overview

(315) If the CPA so decides on the basis of newly found cryptographic weaknesses, all C-ITS stations shall be able to switch to one of the two algorithms (ECDSA_nistP256_with_SHA 256 or ECDSA_brainpoolP256_with_SHA 256) as soon as possible. The actual algorithm(s) that is/are used shall be determined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

6.1.4.2. *Algorithm and key length - encryption algorithms for enrolment and authorisation*

(316) All PKI participants (EA, AA and C-ITS stations) shall be able to use public keys to encrypt enrolment and authorisation requests/responses with selected algorithms at the latest two years after entry into force of this Regulation in accordance with Table 6. The actual algorithm(s) that is/are used shall be determined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

(317) The named algorithms in Table 6 indicate the key length and hash algorithm length and shall be implemented in accordance with [5].

	TLM	root CA	EA	AA	C-ITS station
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X indicates mandatory support					

Table 6: Use of public keys for encryption of enrolment and authorisation requests/responses

(318) All PKI participants (EA, AA and C-ITS stations) shall be able to generate key pairs and use the private key to decrypt enrolment and authorisation requests/responses with selected algorithms at the latest two years after entry into force of this Regulation in accordance with Table 7:

	TLM	root CA	EA	AA	C-ITS station
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X indicates mandatory support					

Table 7: Generate key pairs and use of private key for the decryption of enrolment and authorisation requests/responses

6.1.4.3. *Crypto-agility*

(319) Requirements on key lengths and algorithms must be changed over time to maintain an appropriate level of security. The CPA shall monitor the need for such changes in the light of actual vulnerabilities and state-of-the-art cryptography. It will draft, approve and publish an update of this certificate policy if it decides that the cryptographic algorithms should be updated. Where a new issue of this CP signals a change of algorithm and/or key length, the CPA will adopt a migration strategy, which includes transition periods during which old algorithms and key lengths must be supported.

(320) In order to enable and facilitate the transfer to new algorithms and/or key lengths, it is recommended that all PKI participants implement hardware and/or software that is capable of a changeover of key lengths and algorithms.

(321) Changes of root and TLM certificates shall be supported and executed with the help of link certificates (see section 4.6) that are used to cover the transition period between the old and new root certificates (‘migration of the trust model’).

6.1.5. Secure storing of private keys

This section describes the requirements for the secure storage and generation of key pairs and random numbers for CAs and end-entities. These requirements are defined for cryptographic modules and described in the following sub-sections.

6.1.5.1. *Root CA, sub-CA and TLM level*

(322) A cryptographic module shall be used for:

- generating, using, administering and storing private keys;
- generating and using random numbers (assessment of the random number generation function shall be part of the security evaluation and certification);
- creating backups of private keys in accordance with section 6.1.6;
- deletion of private keys.

The cryptographic module shall be certified with one of the following protection profiles (PPs), with assurance level EAL-4 or higher:

- PPs for HSMs:
  - CEN EN 419 221-2: Protection profiles for TSP cryptographic modules – Part 2: Cryptographic module for CSP signing operations with backup;
  - CEN EN 419 221-4: Protection profiles for TSP cryptographic modules – Part 4: Cryptographic module for CSP signing operations without backup;
  - CEN EN 419 221-5: Protection profiles for TSP cryptographic modules – Part 5: Cryptographic module for trust services;
- PPs for smartcards:
  - CEN EN 419 211-2: Protection profiles for secure signature creation device – Part 2: Device with key generation;
  - CEN EN 419 211-3: Protection profiles for secure signature creation device — Part 3: Device with key import.

Manual access to the cryptographic module shall require two-factor authentication from the administrator. In addition, this shall require the involvement of two authorised persons.

The implementation of a cryptographic module shall ensure that keys are not accessible outside the cryptographic module. The cryptographic module shall include an access control mechanism to prevent unauthorised use of private keys.

6.1.5.2. *End-entity*

(323) A cryptographic module for EEs shall be used for:

- generating, using, administering and storing private keys;
- generating and using random numbers (assessment of the random number generation function shall be part of the security evaluation and certification);
- secure deletion of a private key.

(324) The cryptographic module shall be protected against unauthorised removal, replacement and modification. All PPs and related documents applicable for the security certification of the cryptographic module shall be evaluated, validated and certified in accordance with ISO 15408, applying the Mutual recognition agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS), or an equivalent European cybersecurity certification scheme under the relevant European cybersecurity framework.

(325) Given the importance of maintaining the highest possible security level, security certificates for the cryptographic module shall be issued under the common criteria certification scheme (ISO 15408) by a conformity assessment body recognised by the management committee in the framework of the SOG-IS Agreement, or issued by a conformity assessment body accredited by a

national cybersecurity certification authority of a Member State. Such a conformity assessment body shall provide at least equivalent conditions of security evaluation as envisaged by the SOG-IS Mutual Recognition Agreement.

Note: the link between the cryptographic module and the C-ITS station shall be protected.

6.1.6. Backup of private keys

(326) The generation, storage and use of backups of private keys shall fulfil the requirements of at least the security level required for the original keys.

(327) Backups of private keys shall be made by root CAs, EAs and AAs.

(328) Backups of private keys shall not be made for ECs and ATs.

6.1.7. Destruction of private keys

(329) The root CAs, EAs, AAs, and mobile and fixed C-ITS stations shall destroy their private key and any corresponding backups, if a new key pair and corresponding certificate has been generated and successfully installed, and the overlap time (if any — CA only) has passed. The private key shall be destroyed using the mechanism offered by the cryptographic module used for the key storage or as described in the corresponding PP as referred to in section 6.1.5.2.

6.2. Activation data

(330) Activation data refer to authentication factors required to operate cryptographic modules to prevent unauthorised access. The usage of the activation data of a CA's cryptographic device shall require action by two authorised persons.

6.3. Computer security controls

(331) The CAs' computer security controls shall be designed in accordance with the high security level by adhering to the requirements of ISO/IEC 27002.

6.4. Life-cycle technical controls

(332) The CA's technical controls shall cover the whole life-cycle of the CA. In particular, this includes the requirements of section 6.1.4.3 ('Crypto-agility').

6.5. Network security controls

(333) The networks of the CAs (root CA, EA and AA) shall be hardened against attacks in line with the requirements and implementation guidance of ISO/IEC 27001 and ISO/IEC 27002.

(334) The availability of the CA's networks shall be designed in the light of the estimated traffic.

7. CERTIFICATE PROFILES, CRL AND CTL

7.1. Certificate profile

(335) The certificate profiles defined in [5] shall be used for the TLM, root certificates, EA certificates, AA certificates, ATs and ECs. National governmental EAs may use other certificate profiles for ECs.

(336) Root CA, EA and AA certificates shall indicate the permissions for which these CAs (root CAs, EA and AA) are allowed to issue certificates.

(337) On the basis of [5]:

- each root CA shall use its own signing private key to issue CRLs;
- the TLM shall use its own signing private key to issue the ECTL.

7.2. Certificate validity

(338) All C-ITS certificate profiles shall include an issue and an expiry date, which represent the validity time of the certificate. At each PKI level, certificates shall be generated in good time before expiry.

(339) The validity time of CA and EC certificates shall include an overlap time. TLM and root CA certificates shall be issued and put on the ECTL a maximum of three months and at least one month before their validity starts based on the start time in the certificate. This preloading phase is required to safely distribute the certificates to all correspondent relying parties in accordance with section 2.2. This ensures that, from the beginning of the overlap time, all relying parties are already able to verify messages issued with a new certificate.

(340) At the beginning of the overlap time, the successive CA, EC and AT certificates shall be issued (if applicable), distributed to and installed by the correspondent relying parties. During the overlap time, the current certificate shall be used only for verification.

(341) As the validity periods listed in Table 8 must not exceed the validity period of the superior certificate, the following restrictions apply:

- maximumvalidity(Root CA) = privatekeyusage(Root CA) + maximumvalidity(EA,AA);
- maximumvalidity(EA) = privatekeyusage(EA) + maximumvalidity(EC);
- maximumvalidity(AA) = privatekeyusage(AA) + preloadingperiod(AT).

(342) The validity of (Root and TLM) link certificates starts at the corresponding private key usage and ends at the maximum validity time of the root CA or TLM.

(343) Table 8 shows the maximum validity time for C-ITS CA certificates (for AT validity periods, see section 7.2.1).

Entity	Max. private key usage period	Maximum validity time
Root CA	3 years	8 years
EA	2 years	5 years
AA	4 years	5 years
EC	3 years	3 years
TLM	3 years	4 years

Table 8: Validity periods of the certificates in the C-ITS trust model

7.2.1. Pseudonym certificates

(344) In this context, pseudonyms are implemented by ATs. As a consequence, this section refers to ATs rather than pseudonyms.

(345) The requirements set out in this section apply only to ATs of mobile C-ITS stations sending CAM and DENM messages, where the risk of location privacy is applicable. No specific requirements on AT certificates apply to ATs for fixed C-ITS stations and mobile C-ITS stations used for special functions where location privacy is not applicable (e.g. marked emergency and law-enforcement vehicles).

(346) The following definitions shall apply:

- ‘validity period for ATs’ – the period for which an AT is valid, i.e. the period between the AT’s starting date and its expiry date;
- ‘preloading period for ATs’ – preloading is the possibility for C-ITS stations to obtain ATs before the validity period starts. The preloading period is the maximum allowed time period from the request of ATs to the latest end of validity date of any requested AT;
- ‘usage period for ATs’ – the period during which an AT is effectively used to sign CAM/DENM messages;
- ‘maximum number of parallel ATs’ – the number of ATs from which a C-ITS station can choose at any given time when signing a CAM/DENM message, i.e. the number of different ATs issued to one C-ITS station that are valid at the same time.

(347) The following requirements shall apply:

- the preloading period for ATs shall not exceed three months;
- the validity period for ATs shall not exceed one week;
- the maximum number of parallel ATs shall not exceed 100 per C-ITS station;
- the usage period of an AT depends on the AT change strategy and the amount of time that a vehicle is in operation, but is limited by the maximum number of parallel ATs and the validity period. More specifically, the average usage period for one C-ITS station is at least the operational time of the vehicle during one validity period divided by the maximum number of parallel ATs.

7.2.2. Authorisation tickets for fixed C-ITS stations

(348) The definitions in section 7.2.1 and the following requirements apply:

- the preloading period for ATs shall not exceed three months;
- the maximum number of parallel ATs shall not exceed two per C-ITS station.

7.3. Revocation of certificates

7.3.1. Revocation of CA, EA and AA certificates

Root CA, EA and AA certificates shall be revocable. Revoked certificates of root CAs, EAs and AAs shall be published on a CRL as soon as possible and without undue delay. This CRL shall be signed by its corresponding root CA and use the profile described in section 7.4. For revocation of root CA certificates, the corresponding root CA issues a CRL containing itself. In addition, in cases of a security compromise, section 5.7.3 applies. In addition the TLM shall remove revoked root CAs from the trust list and issue a new trust list. Expired certificates shall be removed from the corresponding CRL and trust list.

(349) Certificates are revoked where:

- the root CAs have reason to believe or strongly suspect that the corresponding private key have been compromised;
- the root CAs have been notified that the contract with the subscriber has been terminated;
- information (such as name and associations between CA and subject) in the certificate is incorrect or has changed;
- a security incident takes place that affects the certificate owner;
- an audit (see section 8) leads to a negative result.

(350) Subscriber shall immediately notify the CA of a known or suspected compromise of their private key. It must be assured that only authenticated requests result in revoked certificates.

7.3.2. Revocation of enrolment credentials

(351) Revocation of ECs may be initiated by the C-ITS station subscriber (flow 34) and shall be implemented by an internal blacklist in a revocation database with a timestamp, which is generated and maintained by each EA. The blacklist is never published and shall be kept confidential and used only by the corresponding EA to verify the validity of the corresponding ECs in the context of requests for ATs and new ECs.

7.3.3. Revocation of authorisation tickets

(352) As ATs are not revoked by the corresponding CAs, they shall have a short lifetime and cannot be issued too far in advance of becoming valid. The permissible certificate life-cycle parameter values are set out in section 7.2.

7.4. Certificate revocation list

(353) The format and content of the CRL issued by root CAs shall be as laid down in [1].

7.5. European certificate trust list

(354) The format and content of the ECTL issued by the TLM shall be as laid down in [1].

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Topics covered by audit and audit basis

(355) The purpose of a compliance audit is to verify that the TLM, root CAs, EAs and AAs operate in accordance with this CP. The TLM, root CAs, EAs and AAs shall select an independent acting and accredited PKI auditor to audit their CPS. The audit shall be combined with an ISO/IEC 27001 and ISO/IEC 27002 assessment.

(356) A compliance audit is ordered by a root CA (flow 13) for the root CA itself, and for a sub-CA by its subordinate EA/AA.

(357) A compliance audit for the TLM is ordered by the CPA (flow 38).

(358) When requested, an accredited PKI auditor shall perform a compliance audit on one of the following levels:

(1) conformity of the TLM's, root CA's, EA's or AA's CPS with this CP;

(2) conformity of the TLM's, root CA's, EA's or AA's intended practices with its CPS prior to operation;

(3) conformity of the TLM's, root CA's, EA's or AA's practices and operational activities with its CPS during operation.

(359) The audit shall cover all requirements of this CP to be fulfilled by the TLM, root CAs, EAs and AAs to be audited. It shall also cover the operation of the CA in the C-ITS PKI, including all processes mentioned in its CPS, the premises and responsible persons.

(360) The accredited PKI auditor shall provide a detailed report of the audit to the root CA (flow 36), EA, AA or CPA (flow 16 and 40), as applicable.

8.2. Frequency of the audits

(361) A root CA, TLM, EA or AA shall order a compliance audit of itself from an independent and accredited PKI auditor in the following cases:

- at its first setting-up (levels 1 and 2 compliance);
- at every change of the CP. The CPA shall define the CP change content and time-plan of deployment and determine the needs for audits (including the necessary compliance level) accordingly;
- at every change of its CPS (levels 1, 2 and 3 compliance). Since the managing entities of root CAs, the TLM and EAs/AAs decide what implementation changes follow the update of their CPS, they shall order a compliance audit before implementing those changes. In cases of only minor changes of the CPS (e.g. of an editorial nature), the managing entity may send the CPA a duly justified request for its approval to skip level 1, 2 or 3 compliance audits;
- regularly, and at least every three years during its operation (level 3 compliance).

8.3. Identity/qualifications of auditor

(362) The CA to be audited shall select an independently acting and accredited company/organisation ('auditing body') or accredited PKI auditors to audit it in accordance with this CP. The auditing body shall be accredited and certified by a member of European Accreditation[1].

8.4. Auditor's relationship to audited entity

(363) The accredited PKI auditor shall be independent of the audited entity.

[1] Members of the European Accreditation Body are listed at: http://www.european-accreditation.org/ea-members

8.5. Action taken as a result of deficiency

(364) Where an audit report finds the TLM to be non-compliant, the CPA shall order the TLM to take immediate preventive/corrective action.

(365) Where a root CA with a non-compliant audit report makes a new application, the CPA shall reject the application and send a corresponding rejection to the root CA (flow 4). In such cases, the root CA will be suspended. It must take corrective action, re-order the audit and make a new request for CPA approval. The root CA shall not be allowed to issue certificates during the suspension.

(366) In cases of a regular root CA audit or a change to a root CA's CPS, and depending on the nature of the non-compliance described in the audit report, the CPA may decide to revoke the root CA and communicate this decision to the TLM (flow 2), causing the deletion of the root CA certificate from the ECTL and insertion of the root CA on the CRL. The CPA shall send a corresponding rejection to the root CA (flow 4). The root CA must take corrective action, re-order a full audit (level 1 to 3) and make a new request for CPA approval. Alternatively, the CPA may decide not to revoke the root CA, but to give it a grace period in which the root CA shall take corrective action, re-order an audit and re-submit the audit report to the CPA. In this case, the root CA operation must be suspended and it is not allowed to issue certificates and CRLs.

(367) In case of an EA/AA audit, the root CA shall decide whether or not to accept the report. Depending on the audit result, the root CA shall decide whether to revoke the EA/AA certificate in accordance with rules in the root CA's CPS. The root CA shall at all times ensure the EA/AA's compliance with this CP.

8.6. Communication of results

(368) The root CA and the TLM shall send the audit report to the CPA (flow 16). The root CA and TLM shall store all audit reports they have ordered. The CPA shall send a corresponding approval or rejection (flow 4) to the root CA and TLM.

(369) The root CA shall send a certificate of conformity to the corresponding EA/AA.

9. OTHER PROVISIONS

9.1. Fees

(370) One principle of the implemented EU C-ITS trust model is that the root CAs together fully finance the regular recurrent costs of operation of the CPA and the central elements (TLM and CPOC) relating to the activities set out in this CP.

(371) The root CAs (including the EU root CA) are entitled to take fees from their sub-CAs.

(372) Throughout their period of operation, every participant of the C-ITS trust model shall have access to at least one root CA, EA and AA on a non-discriminatory basis.

(373) Each root CA is entitled to pass on the fees it pays for CPA and the central elements (TLM and CPOC) to the registered participants of the C-ITS trust model, including the enrolled and authorised C-ITS stations.

9.2. Financial responsibility

(374) The initial establishment of a root CA shall cover a period of at least three years of operation, in order for it to become a member of the EU C-ITS trust model. The CPS of a root CA operator shall also contain detailed provisions on root CA revocation or closure.

(375) Each root CA must demonstrate the financial viability of the legal entity implementing it for at least three years. This financial viability plan is part of the initial set of documents for enrolment and must be updated every three years and reported to the CPA.

(376) Each root CA must report the structure of charges applied to EAs/AAs and the enrolled and authorised C-ITS stations each year to the operations manager and the CPA to demonstrate its financial sustainability.

(377) All financial and legal responsible entities of the root CA, EA, AA and the central elements (CPOC and TLM) of the C-ITS trust model must cover their operational duties with adequate insurance levels to compensate for operational errors and financial recovery of their duties if one of the technical elements fails.

9.3. Confidentiality of business information

(378) The following shall be kept confidential and private:

- root CA, EA, AA application records, whether approved or rejected;
- root CA, EA, AA and TLM audit reports;
- root CAs', EAs', AAs', CPOCs' and TLM's disaster recovery plans;
- private keys of the elements of the C-ITS trust model (C-ITS stations, TLM, EA, AA, root CAs);
- any other information identified as confidential by the CPA, root CAs, EA, AA, TLM and CPOC.

9.4. Privacy plan

(379) The CPSs of the root CAs and the EAs/AAs shall set out the plan and the requirements for the treatment of personal information and privacy on the basis of the GDPR and other applicable legislative (e.g. national) frameworks.

10. REFERENCES

The following references are used in this Annex.

[1] ETSI TS 102 941 V1.2.1, Intelligent transport systems (ITS) – security, trust and privacy management.

[2] ETSI TS 102 940 V1.3.1, Intelligent transport systems (ITS) – security, ITS communications security architecture and security management.

[3] Certificate policy and certification practices framework (RFC 3647, 1999).

[4] ETSI TS 102 042 V2.4.1 Policy requirements for certification authorities issuing public key certificates.

[5] ETSI TS 103 097 V1.3.1, Intelligent transport systems (ITS) – security, security header and certificate formats.

[6] Calder, A. (2006). Information security based on ISO 27001/ISO 1779: a management guide. Van Haren Publishing.

[7] ISO, I., & Std, I. E. C. (2011). ISO 27005 (2011) – information technology, security techniques, information security risk management. ISO.

EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 4

ANNEX

to the

Commission Delegated Regulation

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

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

TABLE OF CONTENTS

1. C-ITS security policy 2
1.1. Definitions and acronyms 2
1.2. Definitions 2
1.3. Strategy for information security 3
1.3.1. Information security management system (ISMS) 3
1.4. Information classification 4
1.5. Risk assessment 6
1.5.1. General 6
1.5.2. Security risk criteria 6
1.5.2.1. Risk identification 6
1.5.2.2. Risk analysis 7
1.5.2.3. Risk evaluation 8
1.6. Risk treatment 8
1.6.1. General 8
1.6.2. Controls for C-ITS stations 8
1.6.2.1. Generic controls 8
1.6.2.2. Controls for communication between C-ITS stations 8
1.6.2.3. Controls for C-ITS stations as an end-entity 10
1.6.3. Controls for EU CCMS participants 10
1.7. Compliance with this security policy 10
2. References 11

ANNEX IV

1. C-ITS SECURITY POLICY

1.1. Definitions and acronyms

EU CCMS	European Union C-ITS security credential management system
CAM	cooperative awareness message
CP	certificate policy
DENM	decentralised environmental notification message
ISMS	information security management system
IVIM	infrastructure-to-vehicle information message
SPATEM	signal phase and timing extended message
SREM	signal request extended message
SSEM	signal request status extended message

1.2. Definitions

availability	being accessible and usable on demand by an authorised entity (ISO 27000) [2]
C-ITS infrastructure	system of facilities, equipment and applications needed for the operation of an organisation that provides C-ITS services related to fixed C-ITS stations.
C-ITS stakeholders	individual, group or organisation with a role and responsibility in the C-ITS network
confidential information	information that is not to be made available or disclosed to unauthorised individuals, entities or processes (ISO 27000) [2]
information security	preservation of the confidentiality, integrity and availability of information (ISO 27000) [2]
information security incident	an unwanted or unexpected information security event, or series of events, that has a significant probability of compromising business operations and threatening information security
integrity	property of accuracy and completeness (ISO 27000) [2]
local dynamic	an in-vehicle C-ITS station’s dynamically updated repository of data relating to local driving

map (LDM)	conditions; it includes information received from on-board sensors and from CAM and DENM messages (ETSI TR 102 893) [5]
protocol control	The protocol control assets select an appropriate message transfer protocol for an outgoing message request and send the message to the lower layers of the protocol stack in a format that can be processed by those layers. Incoming messages are converted into a format that can be handled within the C-ITS station and passed to the relevant functional asset for further processing (ETSI TR 102 893) [5]

1.3. Strategy for information security

1.3.1. Information security management system (ISMS)

(1) Each C-ITS station operator shall operate an ISMS in accordance with ISO/IEC 27001 and with the constraints and additional requirements laid down in this section.

(2) Each C-ITS station operator shall determine external and internal issues relevant to C-ITS, including:

- COM(2016) 766 final [10];
- the GDPR [6].

(3) Each C-ITS station operator shall determine parties that are relevant to the ISMS and their requirements, including all C-ITS stakeholders.

(4) The ISMS scope shall include all the operated C-ITS stations and all other information-processing systems that process C-ITS data in the form of C-ITS messages that comply with the following standards:

- CAM [7]
- DENM [8]
- IVIM [9]
- SPATEM [9]
- MAPEM [9]
- SSEM [9]
- SREM [9]

(5) Each C-ITS station operator shall ensure that its information security policy is consistent with this policy.

(6) Each C-ITS station operator shall ensure that its information-security objectives include and are consistent with the security objectives and high-level requirements in this policy.

(7) C-ITS station operators shall classify the information referred to in section 1.4.

(8) C-ITS station operators shall apply an information security risk assessment process as set out in section 1.5 at planned intervals or when significant changes are proposed or occur.

(9) C-ITS station operators and/or C-ITS station manufacturers shall determine requirements for mitigating security risks identified in the information security risk assessment process, in line with section 1.6.

(10) C-ITS station manufacturers shall design, develop and assess C-ITS stations and other information processing systems so as to ensure that they meet applicable requirements.

(11) C-ITS station operators shall operate C-ITS stations and all other information-processing systems that implement appropriate information security risk treatment controls in line with section 1.6.

1.4. Information classification

This section lays down the minimum requirements for information classification. This does not prevent any C-ITS stakeholder from applying more stringent requirements.

(12) C-ITS station operators shall classify handled information, whereby a security category can be represented as:

Security Category information = {(confidentiality, impact), (integrity, impact), (availability, impact)};

(13) C-ITS stakeholders shall classify managed information, whereby a security category system can be represented as:

Security Category information system = {(confidentiality, impact), (integrity, impact), (availability, impact)};

(14) The acceptable values for potential impact are low, moderate and high, as summarised Table **1**.

Table 1 Potential impact definitions for each security objective of confidentiality, integrity and availability

	Potential impact		
Security objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	The unauthorised disclosure of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.
Integrity Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity	The unauthorised modification or destruction of information could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The unauthorised modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.

	Potential impact		
Availability Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organisational operations, organisational assets or individuals.

(15) The following information classification impact types shall be considered in terms of the degree of damage or costs to the C-ITS service and C-ITS stakeholders caused by an information security incident:

- road safety — where the impact places road users at imminent risk of injury;
- safety — where the impact places any of the C-ITS stakeholders at imminent risk of injury;
- operational impacts — where the impact is substantially negative for road traffic efficiency, or other societal impact such as environmental footprint and organised crime;
- legal — where the impact results in significant legal and/or regulatory compliance action against one or more of the C-ITS stakeholders;
- financial — where the impact results in direct or indirect monetary costs for one or more of the C-ITS stakeholders;
- privacy – the GDPR having both legal and financial impact;
- reputation — where the impact results in reputational damage for one or more C-ITS stakeholders and/or the C-ITS network, e.g. adverse press coverage and/or major political pressure on a national or international scale.

(16) C-ITS stakeholders shall respect the following minimum impact values for the information handled:

Table 2: Impacts

	Information originated by fixed C-ITS stations	**Information originated by mobile C-ITS stations**
Confidentiality	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: low	CAM: low DENM: low SREM: low personal data contained in any of the three messages: moderate
Integrity	CAM: moderate	CAM: moderate

	Information originated by fixed C-ITS stations	**Information originated by mobile C-ITS stations**
	DENM: moderate IVIM: moderate MAPEM: moderate SPATEM: moderate SSEM: moderate	DENM: moderate SREM: moderate
Availability	CAM: low DENM: low IVIM: low MAPEM: low SPATEM: low SSEM: moderate	CAM: low DENM: low SREM: moderate

1.5. Risk assessment

1.5.1. General

(17) Risk assessment shall be periodically conducted in line with ISO/IEC 27005. It shall include appropriate documentation of:

- the scope of the risk assessment, i.e. the system being assessed and its boundaries and system purpose, and the information that is handled;
- the security risk criteria;
- risk assessment, including identification, analysis and evaluation.

1.5.2. Security risk criteria

(18) Risk evaluation criteria shall be determined considering the following aspects:

- the strategic value of the C-ITS service and C-ITS network to all C-ITS stakeholders;
- the strategic value of the C-ITS service and C-ITS network to the C-ITS station operator of the service;
- the consequences for the reputation of the C-ITS network;
- legal and regulatory requirements and contractual obligations.

(19) Risk impact criteria shall be determined in the light of the information classification impact types referred to in section 1.4.

(20) Risk acceptance criteria shall include the identification of risk levels that are unacceptable for the C-ITS service and C-ITS stakeholders, by impact type.

1.5.2.1. Risk identification

(21) Risks shall be identified in accordance with ISO/IEC 27005. The following minimum requirements shall apply:

- the main assets to be protected are C-ITS messages as referred to in section 1.3.1;

- supporting assets should be identified, including:
  - information used for C-ITS messages (e.g. local dynamic map, time, protocol control, etc.);
  - C-ITS stations and their software, configuration data and associated communication channels;
  - central C-ITS control assets;
  - every entity within the EU CCMS;
- threats to those assets, and their sources, shall be identified;
- existing and planned controls shall be identified;
- vulnerabilities that can be exploited by threats to cause harm to assets or to the C-ITS stakeholders shall be identified and described as incident scenarios;
- the possible consequences of security incidents on the assets shall be identified on the basis of the information classification.

1.5.2.2. Risk analysis

(22) The following minimum requirements apply to risk analysis:

- the impact of the identified information security incidents on the C-ITS service and the C-ITS stakeholders shall be assessed on the basis of the information and information system security category, using at least the three levels set out in section 1.4;
- the levels of impact shall be identified for:
  - the total existing C-ITS network/services; and
  - an individual C-ITS stakeholder/organisational entity;
- the highest level shall be taken as total impact;
- the likelihood of the identified incident scenarios shall be assessed using at least the following three levels:
  - unlikely (value 1) – the incident scenario is unlikely to occur / difficult to realise or the motivation for an attacker is very low;
  - possible (value 2) – the incident scenario may occur/ is possible to realise or the motivation for an attacker is reasonable;
  - likely (value 3) – the incident scenario is likely to occur / easy to realise and the motivation for an attacker is high;
- the levels of risk shall be determined for all identified incident scenarios on the basis of the product of impact and likelihood, resulting in at least the following risk levels: low (values 1,2), moderate (values 3,4) and high (values 6,9), defined as follows:

Table 3: Risk levels

Risk levels as product of impact and likelihood		Likelihood		
		unlikely (1)	**possible (2)**	**likely (3)**
Impact	**low (1)**	low (1)	low (2)	moderate (3)
	moderate (2)	low (2)	moderate (4)	high (6)
	high (3)	moderate (3)	high (6)	high (9)

1.5.2.3. Risk evaluation

(23) Levels of risk shall be compared against risk evaluation criteria and risk acceptance criteria to determine what risks shall be subject to treatment. At least moderate- or high-level risks applicable to the C-ITS service and C-ITS network shall be treated, in line with section 1.6.

1.6. Risk treatment

1.6.1. General

(24) Risks shall be treated in one of the following ways:

- risk modification by using controls identified in section 1.6.2 or 1.6.3, so that the residual risk can be reassessed as being acceptable;
- risk retention (where the level of risk meets the risk acceptance criteria);
- risk avoidance.

(25) Risk sharing or transfer is not allowed for risks to the C-ITS network.

(26) Risk treatment shall be documented, including:

- the statement of applicability in line with ISO 27001, which sets out the necessary controls and determines:
  - the residual likelihood of occurrence;
  - the residual severity of impact;
  - the residual risk level;
- the reasons for risk retention or avoidance.

1.6.2. Controls for C-ITS stations

1.6.2.1. Generic controls

(27) C-ITS stations shall implement appropriate countermeasures to modify risk, in line with section 1.6.1. Those countermeasures shall implement generic controls as defined in ISO/IEC 27001 and ISO/IEC 27002.

1.6.2.2. Controls for communication between C-ITS stations

(28) The following minimum mandatory controls shall be implemented on the sender side:

Table 4: Controls on the sender side

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality	-	The personal data contained in messages shall be secured using an adequate AT change procedure to ensure a level of security adequate to the risk of re-identification of drivers based on their broadcasted data. Therefore, C-ITS stations shall change ATs adequately when sending messages and shall not re-use ATs after a change, except in cases of non-average[1] driver behaviour.
Integrity	All messages shall be signed in accordance with TS 103 097 [14].	All messages shall be signed in accordance with TS 103 097 [14].
Availability	-	-

(29) The following minimum mandatory controls shall be implemented on the receiver side:

Table 5: Controls on the receiver side

	Information originated by fixed C-ITS stations	Information originated by mobile C-ITS stations
Confidentiality		Received personal data should be retained for as short a time as possible for business purposes, with a **maximum retention of five minutes** for raw and identifiable data-elements. A received CAM or SRM shall not be forwarded/broadcast. A received DENM may be forwarded/broadcast only within a limited geographical area.
Integrity	The integrity of all messages used by ITS applications shall be validated in accordance with TS 103 097 [14].	The integrity of all messages used by ITS applications shall be validated in accordance with TS 103 097 [14].
Availability	-	A received SRM shall be processed and produce an SSM broadcast to the originator of the SRM.

(30) To support the security requirements of confidentiality, integrity and availability set out in the tables above, all C-ITS stations (mobile C-ITS stations (including vehicle C-ITS stations) and fixed C-ITS stations) shall be assessed and certified using security assessment criteria as specified in the ‘common criteria’ / ISO 15408[2]. Due to the different features of the different types of C-ITS station and different location privacy requirements, different protection profiles may be defined.

[1] The definition of average driving behaviour shall be based on relevant statistical analysis of the driving behaviour in the European Union, e.g. based on data from the German Aerospace Centre (DLR).

[2] ‘Common criteria’ portal: http://www.commoncriteriaportal.org/cc/

(31) All protection profiles and related documents applicable for the security certification of the C-ITS stations shall be evaluated, validated and certified in line with ISO 15408, applying the *Mutual Recognition Agreement of information technology security evaluation certificates* of the Senior Officials Group on Information Systems Security (SOG-IS)[3], or an equivalent European cybersecurity certification scheme under the relevant European cybersecurity framework. In the development of such protection profiles, the scope of the security certification of the C-ITS station may be defined by the manufacturer, subject to assessment and approval of the CPA and a SOG-IS conformity assessment body or at least equivalent as described in the next paragraph.

(32) Given the importance of maintaining the highest possible security level, security certificates for C-ITS stations shall be issued under the common criteria certification scheme (ISO 15408) by a conformity assessment body recognised by the management committee in the framework of the SOG-IS agreement, or issued by a conformity assessment body accredited by a national cybersecurity certification authority of a Member State. Such a conformity assessment body shall provide at least equivalent conditions of security evaluation as envisaged by the SOG-IS Mutual Recognition Agreement.

1.6.2.3. Controls for C-ITS stations as an end-entity

(33) C-ITS stations shall comply with the certificate policy [1] according to their role as an EU CCMS end-entity.

1.6.3. Controls for EU CCMS participants

(34) EU CCMS participants shall comply with the certificate policy [1] according to their role in the EU CCMS.

1.7. Compliance with this security policy

(35) C-ITS station operators shall periodically request and obtain certification for compliance with this policy following the guidelines for an ISO 27001 audit in [12].

(36) The auditing body shall be accredited and certified by a member of European Accreditation. It shall fulfil the requirements of [11].

(37) With the objective of obtaining certification, C-ITS station operators shall generate and maintain documents addressing the requirements on documented information in [3], clause 7.5. In particular, C-ITS station operators shall generate and maintain the following documents related to the ISMS:

- scope of the ISMS (section 1.3.1 and [3], clause 4.3);
- information security policy and objectives (section 1.3.1 and [3], clauses 5.2 and 6.2);
- risk assessment and risk treatment methodology details (section 1.5 and [3], clause 6.1.2);

[3] In the road transport sector, SOG-IS has already been involved in the smart tachograph security certification, for example. The SOG-IS Agreement is currently the only scheme in Europe that can support the harmonisation of security certification of electronic products. At this stage, SOG-IS supports only the ‘common criteria’ process, so the C-ITS stations must be assessed and certified in line with the ‘common criteria’; see https://www.sogis.org/

- risk assessment report (section 1.5 and [3], clause 8.2);
- statement of applicability (section 1.6 and [3], clause 6.1.3d);
- risk treatment plan (section 1.6 and [3], clauses 6.1.3e and 8.3);
- documents required for the implementation of selected controls (section 1.6 and [3], Annex A).

(38) In addition, C-ITS station operators shall generate and maintain the following records as evidence of results achieved:

- records of training, skills, experience and qualifications ([3], clause 7.2);
- monitoring and measurement results ([3], clause 9.1);
- internal audit programme ([3], clause 9.2);
- results of internal audits ([3], clause 9.2);
- results of the management review ([3], clause 9.3);
- results of corrective action ([3], clause 10.1).

2. REFERENCES

The following references are used in this Annex:

[1] Annex III to this Regulation

[2] ISO/IEC 27000 (2016): Information technology – security techniques – information security management systems – overview and vocabulary

[3] ISO/IEC 27001 (2015): Information technology — security techniques – information security management systems – requirements

[4] ISO/IEC 27005 (2011): Information technology – security techniques – information security risk management

[5] ETSI TR 102 893 V1.2.1, Intelligent transport systems (ITS) – security; threat, vulnerability and risk analysis (TVRA)

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[7] ETSI EN 302 637-2 V1.4.0, Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 2: Specification of cooperative awareness basic service

[8] ETSI EN 302 637-3 V1.3.0, Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Part 3: Specifications of decentralised environmental notification basic service

[9] ETSI TS 103 301 V1.2.1: Intelligent transport systems (ITS) – Vehicular communications; Basic set of applications; Facilities layer protocols and

communication requirements for infrastructure services

[10] A European strategy on cooperative intelligent transport systems – a milestone towards cooperative, connected and automated mobility (COM(2016) 766, 30 November 2016)

[11] ISO/IEC 27006:2015 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

[12] ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing

[13] ETSI EN 302 665 V1.1.1 Intelligent transport systems (ITS); Communications architecture

[14] ETSI TS 103 097 V1.3.1. Intelligent transport systems (ITS) security; security header and certificate formats

EUROPEAN
COMMISSION

Brussels, 13.3.2019
C(2019) 1789 final

ANNEX 5

ANNEX

to the

Commission Delegated Regulation

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

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

ANNEX V

PART A

CONFORMITY ASSESSMENT PROCEDURES

Module A

Internal production control

1. Internal production control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the C-ITS stations concerned satisfy the requirements of this Regulation that apply to them.

2. **Technical documentation**

The manufacturer shall establish technical documentation enabling assessment of the C-ITS station's conformity with the relevant requirements and including an adequate analysis and assessment of the risk(s). The documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product. As applicable, it shall contain at least:

- a general description of the C-ITS station;
- conceptual design and manufacturing drawings, and schemes of components, sub-assemblies, circuits, etc.;
- descriptions and explanations as required for the understanding of those drawings and schemes, and the operation of the C-ITS station;
- a list of harmonised standards and/or other relevant technical specifications the references of which have been published in the *Official Journal of the European Union* or international standards, applied in full or in part, and descriptions of the solutions adopted to comply with this Regulation where such harmonised standards have not been applied. Where harmonised standards have been applied in part, the technical documentation shall specify which parts have been applied;
- results of design calculations, examinations, etc.; and
- test reports.

3. **Manufacturing**

The manufacturer shall take all necessary measures to ensure that the manufacturing process and its monitoring guarantee that the C-ITS stations comply with the technical documentation referred to in point 2 and with the requirements of the legislative instruments that apply to them.

4. **Conformity marking and declaration of conformity**

4.1. The manufacturer shall affix the conformity marking required by this Regulation to each individual C-ITS station that satisfies the applicable requirements of this Regulation.

4.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the C-ITS station for which it has been drawn up.

A copy of the declaration shall be made available to the relevant authorities on request.

5. **Authorised representative**

The manufacturer’s obligations, as set out in point 4, may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that they are specified in the mandate.

PART B

EC DECLARATION OF CONFORMITY

1. No (unique identification of the C-ITS station): …

2. Name and address of the manufacturer or its authorised representative: …

3. This declaration of conformity is issued under the sole responsibility of the manufacturer (or installer): …

4. Object of the declaration (identification of the C-ITS station allowing traceability; this may include a photograph, where appropriate): …

5. The object of this declaration is in conformity with the relevant Union harmonisation legislation: …

6. References to the relevant harmonised standards used or references to the other specifications in relation to which conformity is declared: …

8. Additional information: …

Signed for and on behalf of: ………………………….

(place and date of issue)

(name, function) (signature)

PART C

CENTRAL C-ITS STATIONS: CONFORMITY ASSESSMENT PROCEDURES

Module A

Internal production control

1. Internal production control is the conformity assessment procedure whereby the operator fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the central C-ITS stations concerned satisfy the requirements of this Regulation that apply to them.

2. **Technical documentation**

The operator shall establish technical documentation enabling assessment of the central C-ITS station's conformity with the relevant requirements and including an adequate analysis and assessment of the risk(s). The documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product. As applicable, it shall contain at least:

- a general description of the central C-ITS station;
- conceptual design and manufacturing drawings, and schemes of components, sub-assemblies, circuits, etc.;
- descriptions and explanations as required for the understanding of those drawings and schemes, and the operation of the central C-ITS station;
- a list of harmonised standards and/or other relevant technical specifications the references of which have been published in the *Official Journal of the European Union* or international standards, applied in full or in part, and descriptions of the solutions adopted to comply with this Regulation where such harmonised standards have not been applied. Where harmonised standards have been applied in part, the technical documentation shall specify which parts have been applied;
- results of design calculations, examinations, etc.; and
- test reports.

4. **Declaration of conformity**

The operator shall draw up a written declaration of conformity for a product model and keep it together with the technical documentation at the disposal of the national authorities as long as the central C-ITS station is in operation. The declaration of conformity shall identify the central C-ITS station for which it has been drawn up.

A copy of the declaration shall be made available to the relevant authorities on request.

5. **Authorised representative**

The operator's obligations, as set out in point 4, may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that they are specified in the mandate.

PART D

CENTRAL C-ITS STATIONS: EC DECLARATION OF CONFORMITY

1. No (unique identification of the C-ITS station): …
2. Name and address of the operator or its authorised representative: …
3. This declaration of conformity is issued under the sole responsibility of the operator: …
4. Object of the declaration (identification of the central C-ITS station allowing traceability): …
5. The object of this declaration is in conformity with the relevant Union harmonisation legislation: …
6. References to the relevant harmonised standards used or references to the other specifications in relation to which conformity is declared: …
8. Additional information: …

Signed for and on behalf of: ………………………….

(place and date of issue)

(name, function) (signature)