"Processing personal data in the context of C-ITS" 01/03/2017

Document prepared by the Data Protection WG

of the C-ITS Platform

Contents

1.) INTRODUCTION

The aim of this document is to provide a background concerning processing of personal data in the context of Cooperative Intelligent Transport Systems (C-ITS) and skeleton for further steps to be taken. The C-ITS platform is an initiative of DG MOVE that started in the end of 2014 with creation of 11 working groups to address the various aspects of C-ITS deployment. Working group on data protection and privacy under the C-ITS platform is seeking guidance and points to be taken into account from Article 29 in order to be able to take further steps with sound level of data protection.

C-ITS is based on type of machine-to-machine communication: The basic idea is that vehicles inform their environment about their behaviour and in return receive information about their direct environment, through so-called cooperative awareness messages (CAM). If the analysis of the CAM detects an event a so-called de-centralised environmental notification message (DENM) is sent to warn of a risk. The road infrastructure also participates in this system and contributes its own analysis of the traffic situation. Based on this communication, vehicles are able to make better predictions about their environment and improve accident prevention. C-ITS is designed to also enable higher levels of automation: Through its low latency it would allow vehicles to instantly react to risks and to use different levels of automation in a more efficient and safe way. C-ITS is based on a broadcast and is "always on", it forms ad-hoc communication and does not require permanent communication links or networks. Various forms of C-ITS are emerging world-wide and start shaping the transport industry.

The objective of the C-ITS platform is to gather in a single framework all the factors that should be taken into account in order to achieve a seamless and harmonised introduction of C-ITS in the European Union in a way that it also fulfils the required level of protection of personal data. In January 2016, the C-ITS Platform issued its final Phase I report[1]. This report laid the ground for the Commission's Communication establishing the European Strategy on C-ITS[2] adopted in the end of 2016. Amongst several findings in the report, two inter-related factors were identified: The privacy and data protection of road users, and the security of these systems.

The document outlines the purpose of C-ITS: Road safety and efficiency. It demonstrates that they are intertwined. This will be followed by an introduction of the policy and legal environment in the fields of road safety, data protection and cooperative intelligent transport systems (C-ITS), as well as the regulatory framework. C-ITS is a means to improve road safety. A section of the document is dedicated describing how C-ITS works, which messages it broadcasts, their content and the foreseen privacy by design measure – the public key infrastructure (PKI). An analysis of C-ITS in the light of the principles of data processing is presented, highlighting the risks to privacy and the foreseen mitigation measures.

It should be noted that in this document only the so-called ‘day one’ applications of C-ITS are analysed.

[1] http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf

[2] COM/2016/0766 final "A European strategy on Cooperative Intelligent Transport Systems, a first milestone towards cooperative, connected and automated mobility"

However, this does not exclude other applications in the future. Inevitably they will require their own data protection analysis.

1.1) Glossary

The text starts looking at the policy environment first to then gain technical depth. The text tries to avoid mixing policy with technical discussions as much as possible. Hence occasionally technical terms will be used that are more elaborated upon later in the text. Detailed information on the technical set up of C-ITS is to be found in Section 3 of the document dedicated to C-ITS.

C-ITS – cooperative ITS = ITS based on V2X communication

V2V – vehicle-to-vehicle communication

V2I – vehicle-to-infrastructure communication

I2V – infrastructure-to-vehicle communication

V2X – vehicle-to-everything communication

CAM – cooperative awareness message

DENM – decentralised environmental notification message

PKI – public key infrastructure

'day-one' services or use cases – applications to be analysed for initiating C-ITS, as defined in the EU C-ITS Strategy COM 2016/766

ETSI – European Telecommunications Standardisation Institute

WAVE – Wireless Access for Vehicular Environments (V2X microwave technology used in US)

2.) PURPOSE & POLICY AND LEGAL ENVIRONMENT

This section of the document briefly outlines the purpose of the 'day-one' C-ITS applications and introduces the policy and legal framework that were considered, when elaborating the document. The list does not claim to be complete, it aims to set out a framework for the analysis to evaluate the further steps to be taken and a flavour of the policy environment in which C-ITS and data protection operate in the EU.

2.1) Purpose

C-ITS is an instrument to implement the transport policy goals of road safety and traffic efficiency, reduction of environmental effects of transport and access to transport means. The goals are closely intertwined since for example improving traffic flow also helps preventing accidents. Accident prevention involves predicting the traffic environment and hence limited snapshots of how vehicles move[3]. Initial 'day-one' applications have advisory/informative character and not intervene into driving, the driver remains in full control hence is liable for the actions of the vehicle. With increasing level of automation the importance of C-ITS will increase as vehicles may gradually take over driving decisions from the driver.

2.2) Policy and legal environment

The Treaty on the functioning of the European Union (TFEU)[4] lays down that transport safety and protection of personal data are responsibilities of European Union, both of those being essential in the context of C-ITS. In addition the Treaty acknowledges[5] the "Charter of Fundamental Rights of the European Union", which recognises the protection of personal data as one of the freedoms.

2.2.1) EU transport policy framework

C-ITS primarily serves public goals, namely road safety and traffic efficiency[6]. The Common Transport Policy is part of the TFEU[7] and one of the original 'Common Policies' of the Treaty of Rome. Hence a core piece of the internal market. The TFEU tasks the European Commission to improve transport safety[8].This is further reflected in the EU's transport policies, which have safety, environmental sustainability and

[3] US Department of Transportation: 'Status of the Dedicated Short-Range Communications Technology and Applications'; FHWA-JPO-15-218 Final Report, July 2015, p3

[4] The Treaty on the functioning of the European Union, consolidated version C326/47

[5] TEU, Article 16

[6] Declaration of Amsterdam should we here refer to the C-ITS strategy as that one is European wide, whereas the declaration was in the end of the not from all MS but from the Dutch presidency

[7] TFEU, part one Article 4

[8] TFEU Article 91

efficiency at their core and also identify ITS as a key instrument to improve road safety and efficiency[9]:

The ITS Directive 2010/40/EU is one of the key legal instruments, implementing EU transport policy in the field of road safety, transport efficiency and environmental sustainability. It aims to ensure the compatibility, continuity and interoperability of ITS services. It allows the European Commission to adopt specifications in certain fields. These specifications would be binding for all actors who decide to implement the specified ITS elements. The so-called priority areas specified in the ITS Directive cover road safety and security, as well as linking the vehicle with the infrastructure and amongst each other[10]. The specifications may take the form of delegated acts under the ITS Directive and not exceeding its scope. The ITS Directive would be well suited to support the introduction of C-ITS via the possibility to specify C-ITS and its architecture. The CAM and DENM, could be harmonised using the ITS directive, the security and certification policies could be made binding in such a way.

One of the- specifications under the ITS Directive is Delegated Act 886/2013 "with regard to data and procedures for the provision, where possible, of road safety-related minimum universal traffic information free of charge to user" already gives a first and rudimentary legal definition of road safety related use cases[11] for ITS. These use cases cover the 'day-one' use cases discussed in this document.

EU market regulation plays a key role assuring that the C-ITS communication is interoperable and technically fit for use. The New Legislative Approach[12] regulates market access and product certification and strongly relies on standardisation. The EU here explicitly recognises the standardisation procedures of ETSI as technically thorough, inclusive and transparent[13]. EU regulation permits ETSI to draft European Standards, so-called EN standards and lends them their legitimacy. European Standards may gain legal significance when the European Union recognises them in the Official Journal as proof of legal compliance with a piece of EU legislation or part thereof. A European Standard that is published in the Official Journal is referred to as a harmonised standard. C-ITS relies on the following ETSI documents: harmonised standards, European standards, technical specifications and technical reports.

EU market regulation is also implemented through radio spectrum policy. In this field the Commission Decision 2008/671/EC 'on harmonised radio spectrum in the 5875-5905 MHz frequency band for safety-related applications of Intelligent Transport Systems (ITS)' dedicates radio spectrum to transport safety. This decision reserves frequency bands for the transport safety. This covers all transport modes. C-ITS safety related services based on short range communication operate in the above-mentioned frequency bands.

[9] See COM (2001) 370 White Paper European Transport Policy: Time to Decide & COM (2011) Roadmap to a Single European Transport Area

[10] 2010/40/EU ITS Directive, Article 2 & Annex I

[11] Delegated Regulation (EU) 886/2013, Article 3

[12] Regulations: 764/2008 „procedures on the application of certain national rules on products lawfully marketed in another Member State", 765/2008 "setting requirements for accreditation and market surveillance relating to the marketing of products", 768/2008 "common framework for the marketing of products"

[13] Regulation 1025/2012 „on European Standardisation"

Vehicles and parts thereof have their own specific market regulation - vehicle type approval rules[14]. EU vehicle type approval relies on the United Nations Economic Commission for Europe (UNECE) for the actual regulation and the related stakeholder dialogue. This may at a later stage impact in-vehicle ITS Stations, as UNECE may have to take data protection considerations into account for the type approval specifications. Furthermore UNECE is itself working on guidelines on data protection for cyber security and data protection for intelligent transport systems and automated driving. These guidelines are not legally binding and are intended as an interim solution[15].

With a view to enabling co-operative and connected vehicles to be deployed, the European Commission has issued a strategy[16], which responds to the call from the Member States and European Industry to have common rules in place in 2019 for cooperative and connected vehicles. The opening up of large scale deployment of cooperative and connected vehicles also with a view to pave the way to automated vehicles, requires an adequate regulatory framework to be in place in order to ensure a sound level of data protection and privacy when deployed.

The European Commission initiated an inclusive, transparent and thorough consultation with industry and societal stakeholders in the C-ITS Platform that concluded that ITS-G5 WIFI based communication is currently the only mature technology and best suited to achieve short range vehicle-to-vehicle and vehicle-to-infrastructure communication required for C-ITS[17]. The European Commission adopted the results of the consultation and they are reflected in the 5G Action Plan COM (2016) 588 and the accompanying staff working document[18] and the EU C-ITS Strategy[19], where a hybrid communication approach has been defined to combine complementary short range (ITS-G5 based) and longe range (existing cellular networks) communication technologies. The EU C-ITS Strategy also adopted the 'day-one' use cases established by the consultation. This paper clearly focuses on the data protection aspects of newly introduced short range communication in vehicles. Aspects on existing C-ITS services provided through long range communication technologies, such as transmission of services and data through existing cellular (mobile) network operators is not covered within this analysis and might be subject for further future analysis covering the full hybrid communication approach. However, it is currently assumed that the privacy regime of existing mobile network telecom operations and there provided services is already based on a well-established framework and does not fundamentally change through the provision of mobility related applications (e.g. nowadays navigation devices or existing smart phone apps provide information and guidance services already making use of personal data like position data to provide traffic information and management services).

[14] 2007/46/EC „establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical nits intended for such vehicles"

[15] ECE/TRANS/WP.29/2017/46

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

[17] C-ITS Platform, Final Report, January 2016, Executive Summary

[18] SWD (2016) 306, page 9

[19] COM (2016) 766

The Connecting Europe Facility[20], a major EU budget line funding infrastructure projects in the EU, is funding a series of projects in Austria, Belgium, Czech Republic, France, Germany, Netherlands, Slovenia and the United Kingdom that gather under the C-ROADS umbrella with € 150 million of funding. C-ROADS is piloting various 'day-one' use cases in the EU.

2.2.2) EU data protection framework

Regulation (EU) 2016/679 of the European Parliament and of the Council 'on the protection of natural persons with regard to the processing of personal data and on the free movement of such data' (GDPR), provides a comprehensive legal framework concerning personal data. As GDPR sets out the principles relating to processing of personal data[21] and different grounds for lawful processing[22] of personal data[23], it therefore offers protection against unauthorised and unlawful processing of personal data. GDPR also offers a robust legal framework also in relation to C-ITS.

In addition to the General Data Protection Regulation the EU also applies sectorial data protection legislation - 2002/58/EC 'concerning the processing of personal data and the protection of privacy in the electronic communication sector', also known as 'Privacy and Electronic Communication Directive' or 'ePrivacy Directive'. The current directive strongly focusses on obligations for providers of electronic communication services. C-ITS 'day-one' applications based on short range communication do not foresee the presence of a provider for the communication between the vehicles themselves and the road infrastructure. For the distribution of authorisation tickets, that the security system uses the directive may apply, since cellular communication services could be involved here.

COM (2017) 10 'concerning the respect for private life and protection of personal data in electronic communications' (Regulation on Privacy and Electronic Communication) is a legislative proposal that would repeal the current ePrivacy Directive[24], however the legislative process has only began in European Parliament and Council and therefore the final outcome cannot be foreseen. It was considered since it covers terminal equipment and may also apply to electronic communication services that do not require a provider[25]. Still even if ITS Stations fall into the scope of the proposed directive it is not clear what impact a new directive may have, since the obligations it outlines mainly apply to commercial service providers. The C-ITS day-one applications based on currently available short range communication do not rely on a service provider. The future ePrivacy Directive may apply to the updates of the authorisation tickets, should their distribution rely on cellular networks.

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

[21] 2016/676/EU General Data Protection Regulation, Article 5

[22] 2016/676/EU General Data Protection Regulation, Article 6

[23] 2016/676/EU General Data Protection Regulation, Article 4 (1). The concept of personal data explicitly contains location data.

[24]EU legislative procedures vary time-wise, they average around two years from proposal to adoption

[25] COM (2017) 10, Article 4 (1) (b) defines an „electronic communication service" and refers to another legislative proposal COM (2016) 590 "establishing a European Communications Code", which its Article 2 updates the definition of 'electronic communications service'. COM (2016) 590 is not yet adopted.

2.2.3) International developments

The US are currently at an advanced stage in their legislative efforts to mandate the introduction of C-ITS Stations into vehicles for the US market[26]. C-ITS is referred to as V2V in the US policy context. The US Department of Transportation submitted a report to the US Congress arguing the case for the mandatory introduction of V2V for road safety purposes[27]. The US foresees using a technology similar to the one to be used in the EU, called WAVE, which is a wireless local area network technology adapted for a transport environment. Introduction in the US and the EU are going on in parallel. Data protection is also an issue in the US. Since the legal environment in the US differs from the one in the EU it is not further considered in the analysis below. The developments in the US are of relevance to EU industry intending to export there.

In 2013 Australia has started participating in international harmonisation efforts on C-ITS security, together with the US and the EU. Furthermore first C-ITS demonstrations took place in Australia in 2016.

Singapore's Land Transport Authority is starting to equip its infrastructure V2X technology to enable V2X communication in 2017. An according tender was awarded in February 2017[28]. Singapore's ITS strategy foresees various V2X applications using afore-mentioned WAVE technology[29].

Japan is also deploying V2X, using a similar technology but a slightly different frequency band. Japan is considering various collision prevention systems for motorcycles and intersections. The Japanese Automotive Research Institute (JARI) has reviewed the European CAM and DENM standards[30].

3.) Cooperative Intelligent Transport Systems – C-ITS

This section introduces C-ITS. The basic idea is to give vehicles a better awareness of their surroundings. It complements existing vehicle sensors and extends them beyond the line of sight, around corners, in front of vehicles, curves or hills ahead. C-ITS enables vehicles and infrastructure managers to predict traffic behaviour to prevent accidents.

C-ITS and the CAM and DENM message sets offer road operators advantages over other technologies[31] in use. Traffic observation is currently done using either radar, fixed loops or triple sensors (a

[26] Notice of Proposed Rulemaking: DEPARTMENT OF TRANSPORTATION, National Highway Traffic Safety Administration, [Docket No. NHTSA-2016-0126]: Federal Motor Vehicle Safety Standards; V2V Communications

[27] US Department of Transportation: 'Status of the Dedicated Short-Range Communications Technology and Applications'; FHWA-JPO-15-218 Final Report, July 2015, p3

[28] http://www.straitstimes.com/singapore/transport/ncs-mhi-to-build-islandwide-satellite-based-erp-for-556m

[29] Land Transport Authority and Intelligent Transport Society Singapore: 'Smart Mobility 2030 – ITS Strategic Plan for Singapore', 2014 & Infocomm, Media Development Authority Singapore, Telecommunications Standards Advisory Committee (TSAC): 'Technical Specification – Dedicated Short-Range Communication in Intelligent Transport Systems'

[30] Ministry of Internal Affairs and Communications 'ITS Radiocommunications Standards and Development in Japan' https://docbox.etsi.org/workshop/2014/201402_ITSWORKSHOP/S02_ITS_SomeBitsFromtheWorld/MIC_Ueno.pdf

[31] See footnote 24

combination of radar, infrared, ultrasound) and information conveyed to vehicles via radio broadcast or variable message signing (VMS). These methods do not yield personal data. Wi-Fi and Bluetooth detection are used for the analysis of travel times and already in wide-spread use on motorways and in cities. This method generates personal data. CAM deliver higher quality data at a lower cost compared to the roadside radars, fixed loops or triple sensors that are currently used for monitoring traffic. VMS may be gradually phased out and replaced with in-vehicle signage. CAM also offer better privacy than Wi-Fi or Bluetooth based monitoring systems, since the associated security certificates of C-ITS messages to establish trust of V2V and V2I communication in the system are pseudonymised, using randomly generated and frequently changing pseudonyms. C-ITS does not require permanent radio coverage, the system only works where two ITS Stations are in each-others range, which is several hundred metres only.

In order for C-ITS to achieve its purpose the location, speed and direction of a vehicle is broadcast. This has been taken into account and addressed through minimising the use of data and the public key infrastructure (PKI) that pseudonymises the certificates associated to the vehicles and protects vehicles from identification. C-ITS short range communication relies on broadcasts and is for the initial deployment technologically related to wireless local area networks and the IEEE 802.11 family of standards. ITS stations within range[32] can receive each other's messages, C-ITS V2V short range communication does not rely on cells or built-up infrastructure.

This section describes in short:

1.) the C-ITS 'day-one' applications;

2.) vehicle-to-vehicle communication (V2V), vehicle-to-infrastructure (V2I) or vice-versa (I2V), altogether referred to as V2X communication, performed using CAM and DENM messages;

3.) the security system, the so-called public key infrastructure or simply PKI and

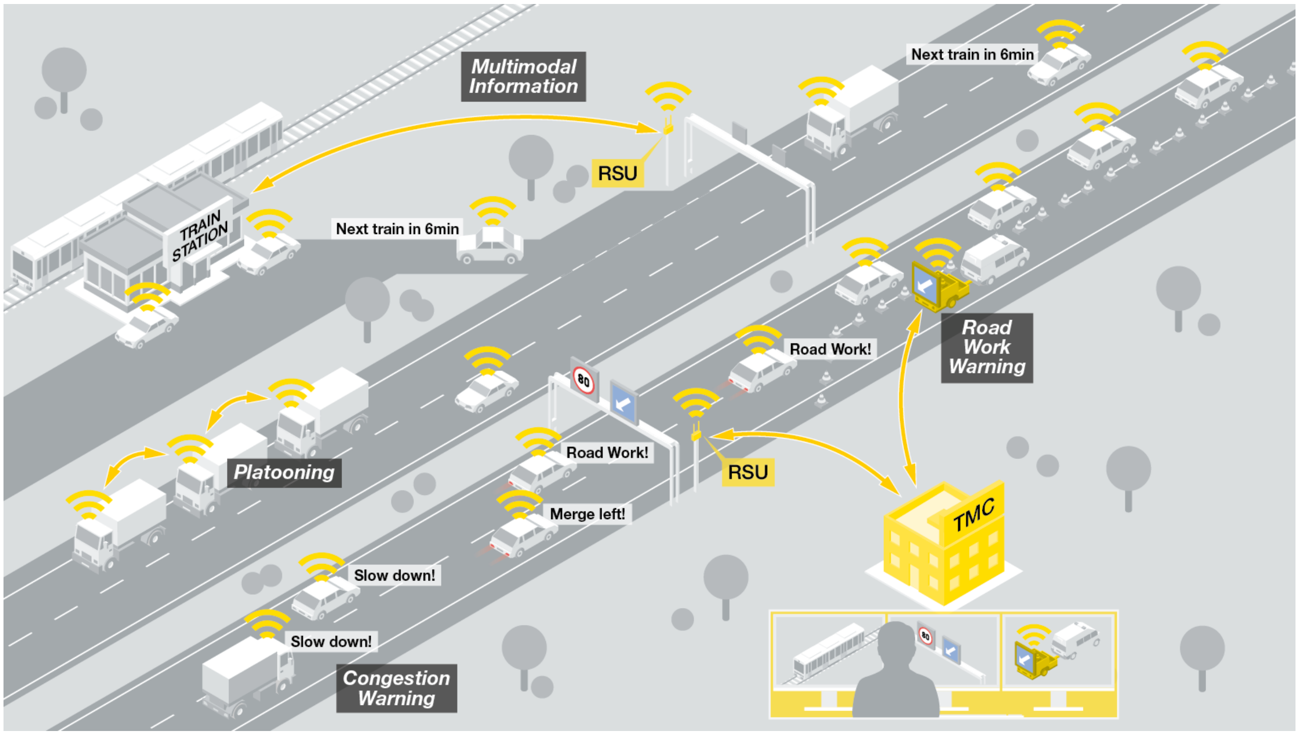
4.) the key actors involved in C-ITS.

C-ITS relies on far more standards than those mentioned here. This document focusses strongly on the CAM and DENM standards, in addition to the CAM and DENM various functional standards exist[33] and more than 70 other standards including testing standards exist or are under development.

[32] On average 300-500 metres

[33] E g: In Vehicle Information (IVI) ISO TS 19321, Signal Phase and Time supported by Topology SPAT/MAP (ISO TS 19091-3 and SAE J2735), Position and Time (PoTi) TS 102 890-2, Collective Perception (CPM) TS 103 324

Figure 1: illustration of C-ITS



3.1) Day-one applications & role in connected, cooperative and automated mobility

The 'day-one' applications are the starting applications for C-ITS. The C-ITS Deployment Platform established a list of 13 'day-one' applications to be discussed in the second phase of the C-ITS Deployment Platform[34].

The C-ITS 'day one' applications fulfil a public purpose[35] , avoiding collisions between vehicles, mitigate collisions and accidents, hence improving road safety or improving traffic flow. An improved traffic flow is the key to preventing accidents and reducing fuel consumption and emissions, as well reducing travel time, creating a positive environmental and economic impact.

The 'day-one' applications do not interfere with the driving functions yet, they initially have an advisory function. With increasing automation though the advisory function is foreseen to gradually turn into interventions into the driving process. The communication is laid out for future levels of automation, hence the communication system is designed for extremely low latency communication, meaning the instant notification of other ITS stations, as well as instant intervention into driving. The system is laid

[34] C-ITS Deployment Platform: Final Report, p 9

[35] See General Data Protection Regulation 2016/679 Article 5 (1) (b): *collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')*

out to also operate in environments were vehicles move at high speed.

A basic description of different C-ITS use cases, including the 'day one' use cases, can be found in ETSI TR 102 638 "Basic Set of Applications"[36]. This document does not standardise the applications, some of them are standardised in separate standards. Further the day one services have been laid down in the European Commission's strategy for the deployment of cooperative, connected and automated mobility[37].

The references to ETSI documents in this table are not exhaustive, but they serve to illustrate the interconnection between key standards and the attributes they use. More on the content of Common Data Dictionary, CAM and DENM can be found below.

Application:	**Emergency electronic break light**
Purpose:	Warn all following vehicles of a sudden slowdown of the traffic so limiting the risk of longitudinal collision.
Description:	This use case consists for any vehicle to signal its breaking hard to following vehicles. In such a case, the hard braking is corresponding to the use of the emergency electronic brake lights.
Comment:	In practice, the application triggers the propagation of a DENM (hard braking conditions ahead) to the following vehicles. Emergency braking is covered by the 'AccelerationControl' attribute in the Common Data Dictionary. This application triggers a DENM. With increasing levels of automation, this DENM may trigger an intervention into the behaviour of other surrounding vehicles, causing them to break, change path or reduce speed.
ETSI:	Basic Set of Applications TR 102 638 C1.1.1 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2 Common Data Dictionary TS 102 894-2 v1.1.1
Application:	**Emergency Vehicle Approaching**
Purpose:	By emergency vehicles to reduce their intervention time to rescue and/or protect people. It reduces also the risk of collision between an emergency vehicle and another vehicle.
Description:	This use case allows an active emergency vehicle to indicate its presence. In many countries the presence of an emergency vehicle imposes an obligation for vehicles in the path of the emergency vehicle to give way and to free an emergency corridor.
Comment:	This application relies on the CAM, the 'VehicleRole' attribute in particular. This application triggers a DENM. With increasing levels of automation, this DENM may trigger an intervention into the behaviour of other surrounding vehicles, causing them to break, change path or reduce speed. Only emergency vehicles have the permission to send this type of DENM. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 1.2.1

[36] ETSI TR 102 638 v1.1.1 (2009-06) Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions

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

	Decentralised Environmental Notification Message EN 302 637-3 v1.2.2 Cooperative Basic Awareness Service EN 302 637-2 v1.3.2 Common Data Dictionary TS 102 894-2 v1.1.1
Application:	**Slow Stationary Vehicles**
Purpose:	Signals a road safety risk and contribute to the improvement of the traffic fluidity by encouraging other vehicles to take another itinerary if possible.
Description:	This use case consists from any slow vehicle to signal its presence (vehicle type) to other vehicles. The vehicle compares its own behaviour with the traffic flow in its environment. If it detects that it is significantly slower, it triggers a DENM.
Comment:	To detect the traffic flow around itself the vehicle analyses sensor data and CAM (see above 'vehicle probe data') With increased levels of automation this could trigger an automated response from surrounding vehicles. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 1.2.2 & C 1.3.2 Cooperative Basic Awareness Service EN 302 637-2 v1.3.2 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2 Road Hazard Signalling (RHS) application requirements specification TS 101 539-1
Application:	**Hazardous location notification**
Purpose:	Reduce the risk of accident which could be caused by a hazardous location.
Description:	This use case informs vehicles of any hazardous location either temporary or permanent (i.e. long term).
Comment:	Generic, geographical warning information, offering a better anticipation to drivers knowing that a potential hazard is located in a given area. This application triggers a DENM. With increased levels of automation this could trigger an automated response from surrounding vehicles. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 1.5.3 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2 Road Hazard Signalling (RHS) application requirements specification TS 101 539-1
Application:	**Traffic jam ahead warning**
Purpose:	Reducing the risk of longitudinal collision on traffic jam forming.
Description:	The application leads to a better anticipation of road congestion. The ITS Station senses consecutive emergency breaks or strong breaks, or stationary traffic. This application is based on the analysis of CAM in the vicinity to trigger the DENM. The end of the condition is likewise established through detecting consecutive accelerations in the vicinity.
Comment:	This is a cooperative awareness application based on 'vehicle probe data'.
ETSI:	Basic Set of Applications TR 102 638 C 1.3.3 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2 Cooperative Basic Awareness Service EN 302 637-2 v1.3.2 Road Hazard Signalling ETSI TS 101 539-1 v1.1.1
Application:	**Road works warning**
Purpose:	Reduce the risk of accident at the level of roadwork.
Description:	Road infrastructure to vehicle communication, provides information on current valid roadwork and associated constraints.
Comment:	Updated information to drivers approaching a road works area. This application

	triggers a DENM and with increasing levels of automation will activate an automatic response from the vehicle. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 1.3.5 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2
Application:	**Weather conditions**
Purpose:	warning road users of hazardous weather conditions
Description:	Geographical warning information, offering a better anticipation to drivers knowing that potential difficult road conditions due to weather are existing ahead. This application triggers a DENM. Will be deployed under C-ROADS.
Comment:	This DENM would be triggered via sensors linked to the ITS Station.
ETSI:	Basic Set of Applications TR 102 638 C 1.3.6 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2
Application:	**Shockwave damping**
Purpose:	Mainly to improve the road safety and to enhance the traffic flow and reduce the vehicles' pollution.
Description:	This application aims to even out shockwaves in traffic that cause traffic jams.
Comment:	With increased levels of automation this could trigger an automated response from the receiving vehicle. The application is described in the ETSI TR mentioned below, it is not standardised yet. This is also application that would rely on ‘vehicle probe data’. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 1.3.6 Cooperative Basic Awareness Service EN 302 637-2 v1.3.2
Application:	**In-vehicle speed limits**
Purpose:	Mainly to improve the road safety through improving the traffic flow preventing accidents. Secondary, vehicles' pollution.
Description:	This use case consists for a capable Road Side Unit to broadcast at a given frequency the current local speed limits (regulatory and contextual).
Comment:	It offers the possibility for traffic management authorities to monitor in real time the traffic speed. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 2.1 ETSI TS 103 301
Application:	**In-vehicle signage**
Purpose:	Advising on ideal driving behaviour.
Description:	Via road infrastructure to vehicle communication, information on current valid traffic signs is given to the driver.
Comment:	This is mainly Infrastructure to vehicle information flow (replacing road panel's info) and therefore not processing personal data. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 2.8 ETSI TS 103 301
Application:	**Green light optimal speed advice (GLOSA)**
Purpose:	Traffic regulation at an intersection.
Description:	This use case allows a traffic light to broadcast timing data associated to its current state (e.g. time remaining before switching between green, amber, red).
Comment:	Traffic optimization and real impact on emissions, in particular for heavy vehicles.

	Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 2.2 ETSI 103 301
Application:	**Signal violation/intersection safety**
Purpose:	Reduce the risk for other vehicles of a stop/traffic violation.
Description:	Signal violation: This use case allows a detecting ITS station (most likely a road side unit) to signal to affected users that a vehicle has violated a road signal and increased the risk of an accident. This application triggers a DENM. Intersection safety: This is a collision risk warning application. a.) equipped intersection, a roadside ITS Station analyses the CAM messages of surrounding traffic and other sensors around the intersection and send warnings, if necessary; b.) non-equipped intersection; vehicles analyse CAM and act.
Comment:	The ETSI standard awaits adoption soon. Signal violation: That application is a warning for surrounding vehicles, to allow drivers anticipating a possible unexpected irruption of a vehicle violating a signal. This application triggers a DENM. Here with increasing automation an immediate response would be required from all vehicles involved to either avoid a collision or, if a collision is inevitable, ameliorate the impact. Intersection safety: This application triggers a collision warning DENM and works with and without roadside infrastructure: a.) roadside ITS Station monitors CAM and other sensors and detects a collision risk and generates a collision risk warning DENM; b.) vehicles monitor CAM in their surroundings, upon detection of a collision risk, they generate an according DENM. This application relies on ‘vehicle probe data’. Its sister application ‘Longitudinal Collision Risk Warning’ ETSI TS 101 539-3 works is no ‘day-on’ use case. Will be deployed under C-ROADS.
ETSI:	Basic Set of Applications TR 102 638 C 1.3.4 & C 1.5.4 Cooperative Basic Awareness Service EN 302 637-2 v1.3.2 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2 Intersection Collision Risk Warning TS 101 539-2
Application:	**Probe Vehicle Data**
Purpose:	Allows a traffic analysis of the immediate vicinity.
Description:	Vehicle probe data is a concept, on which a range of applications is based. The CAM are sent by ITS Stations in regular intervals allowing receiving ITS Stations be they vehicular or roadside an analysis of their direct vicinity (around 500m). This extends the line of sight of vehicle sensors and allows to ‘look around corners’. This extended awareness allows a better risk assessment, should a risk be identified, other ITS Stations would be notified instantly through a DENM. Hence extending the response to a given risk beyond the individual vehicle. Most collision warnings rely on probe vehicle data (e.g.: slow moving vehicle, intersection collision warning, longitudinal collision warning, motorcycle approaching warning, traffic jam warning). These applications play a key role in preventing accidents[38].

[38] US Department of Transportation: ‘Status of the Dedicated Short-Range Communications Technology and Applications’; FHWA-JPO-15-218 Final Report, July 2015, p3

Comment:	Probe vehicle data is not an application per se, it rather enables a whole category of applications. C-ROADS is piloting Probe Vehicle Data. Probe Vehicle Data strictly serves accident prevention. The governance of C-ITS has to assure that data are only stored as long as strictly necessary or stripped of their personal attributes, if archived by traffic managers.
ETSI:	Cooperative Basic Awareness Service EN 302 637-2 v1.3.2 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2 Longitudinal Collision Risk Warning ETSI TS 101 539-3
Application:	**Traffic signal priority request by designated vehicles**
Purpose:	Reduce the risk of collision with speeding and 'in a hurry' emergency vehicles, while improving the intervention time.
Description:	Temporary priority given to e.g. emergency vehicles by unlocking traffic lights 'on request'. This is a sub-case of traffic light management function.
Comment:	That application is useful in exceptional emergency situations.
ETSI:	Basic Set of Applications TR 102 638 C 2.6
Application:	**Wrong way driving**
Purpose:	Limit as much as possible frontal collisions due to wrong way driving.
Description:	This use case indicates to vehicles in the affected area that a vehicle is driving against the planned direction of traffic. The affected area is primarily the road in which the vehicle is driving in the wrong direction and the affected vehicles are those vehicles approaching the violating vehicle.
Comment:	That application is a warning for surrounding vehicles, to allow drivers anticipating a possible unexpected irruption of a vehicle driving in front opposition on the same lane. This application triggers a DENM. Here with increasing automation an immediate response would be required from all vehicles involved to either avoid a collision or, if a collision is inevitable, ameliorate the impact.
ETSI:	Basic Set of Applications TR 102 638 C 1.3.1 Decentralised Environmental Notification Message EN 302 637-3 v1.2.2

3.2) Common Data Dictionary, CAM & DENM

The CAM, DENM and Common Data Dictionary (see below) are closely intertwined and are essential for V2X communication. CAM and DENM messages are broadcast, they are sent and can be received by all ITS stations within range[39]. The broadcast does not establish a communication link between the ITS stations, the sending ITS station does not know who will receive the messages. The ITS Station is capable of distinguishing between authentic and fake messages using the PKI. The technology for initial deployment of short range communication, ITS-G5, is based on the Wireless Local Area Networks family of standards IEEE 802.11 and is specifically adapted to a vehicular environment.

3.2.1) Common Data Dictionary – ETSI TR 102 894

The Common Data Dictionary specifies 112 types of data, that CAM and DENM fill their various data containers with.

[39] around 300-500 metres

The following illustration shows the structure of a CAM and its non-optional types of data. The data types marked with the letter ’A’ followed by a number are attributes defined in the Common data Dictionary.

3.2.2) CAM

The ‘Cooperative Awareness Message’ (CAM) is standardised in ETSI EN 302 637-2 ‘Intelligent Transport Systems “ITS; Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service’.

CAM are broadcast by C-ITS Stations, that can be either vehicle or infrastructure based, in some cases C-ITS Stations belong to other transport actors.

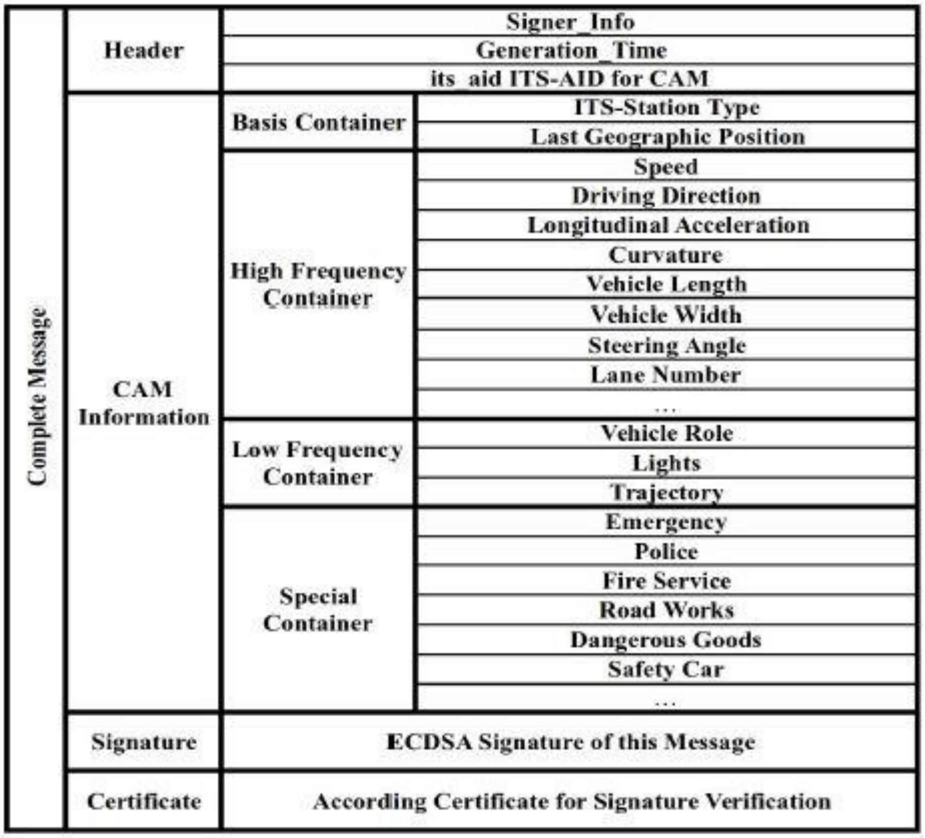
C-ITS equipped vehicles communicate with their close environment via the short range IEEE 802.11p protocol. The signal broadcast from the vehicle ranges between 300 and 500 meters depending on the circumstances. This technique has been chosen because of the low latency of short range communication directly between the vehicles involved and to be less dependent from other means of information and communication. This low latency is necessary because safety related messages require very short reaction times, for instance warnings for parts of the road covered with black ice broadcast to vehicles approaching from behind. The short reaction time becomes even more relevant in higher levels of automation. A cellular signal will take more time and is dependent on the cellular network. Broadcast messages will be received and understood in other vehicles or by road side units.

CAM are standardised to be ‘single-hop’ messages. They can only be processed by vehicles in range and are not meant to be forwarded to other vehicles, since their relevance outside of their range would be limited and forwarding of CAM would create excessive volumes of data traffic.

A CAM consists of a collection of data elements that are arranged in a hierarchical order. The CAM contains by default a heading, a timestamp, then basic data like vehicle pseudo ID and position. There is also a sub-set refreshed in high frequency mode (HF) that includes data like: speed, acceleration and curvature. Other vehicle status information are given in low frequency refreshing mode, like vehicle role or category and some basic sensors. There is also an optional container relating to vehicle category details (public transport, rescue). The CAM contains data elements that indirectly, in combination with other data could appear to be identifiable personal data. The aim of the CAMs is to inform other ITS Stations about current vehicle/C-ITS status and presence.

CAM are signed to provide integrity and authenticity properties to the receiver. The signature is accompanied by a pointer to the signing certificate, which is a static identifier linked to the CAMs.

Figure 2: structure of a CAM



Complete Message	Header	Signer_Info	
		Generation_Time	
		its_aid ITS-AID for CAM	
	CAM Information	Basis Container	ITS-Station Type
			Last Geographic Position
		High Frequency Container	Speed
			Driving Direction
			Longitudinal Acceleration
			Curvature
			Vehicle Length
			Vehicle Width
			Steering Angle
			Lane Number
			...
		Low Frequency Container	Vehicle Role
			Lights
			Trajectory
		Special Container	Emergency
			Police
			Fire Service
			Road Works
			Dangerous Goods
			Safety Car
			...
	Signature	ECDSA Signature of this Message	
	Certificate	According Certificate for Signature Verification	

The vehicle generates CAMs based on: current vehicle values for the data elements that are combined with the currently valid authorisation tickets (see below) stored in the vehicle. Combination is done in such a way that the integrity ("trust") of the CAM can be validated by recipients qualified through the PKI. This is the most appropriate and efficient method for addressing the security and privacy of this type of data broadcast and regulated by the C-ITS security policy.

A vehicle will generate a CAM when the driving direction changes with more than 4°, when a distance between current and past position has been changed more than 4 meters or the speed is changed more than 0.5 m/s compared to the last time a CAM is sent but at least once a second and at the most once 0.1 second under normal conditions. The above time related requirements are the current specifications.

The vehicle sends CAM messages immediately after generation. The frequency of transmission depends on the context of a vehicle. A CAM can be sent up to ten times per second if need be. The validity (life time) is 1 sec. Again these are the currently defined specifications that may change according to the actual needs of the new functions emerging, e.g. for higher levels of vehicle automation. The communication range typically is a few hundred meters, depending on local circumstances. In the context of C-ITS, it is currently assumed that there is no necessity for the ITS Station to keep a record of CAMs it has sent.

CAM messages can be received in the vicinity of the transmitting ITS Station by any appropriately equipped fixed or mobile ITS Station. Any ITS Station when in communication range can receive any of these messages, check the authenticity, and exploit the data carried out for a large variety of applications. Usual receiving stations are either surroundings vehicles or stationary roadside stations from road authorities or road operators (traffic management, traffic statistics, etc.).

The recipient validates and decodes the CAM message. Subsequently the CAM message is used for purposes and time periods decided by the recipient and with the adapted means. The primary purpose for CAM messages is to allow recipients to maintain a dynamic and trustworthy overview of vehicles and roadside equipment in the interest of drivers and road safety.

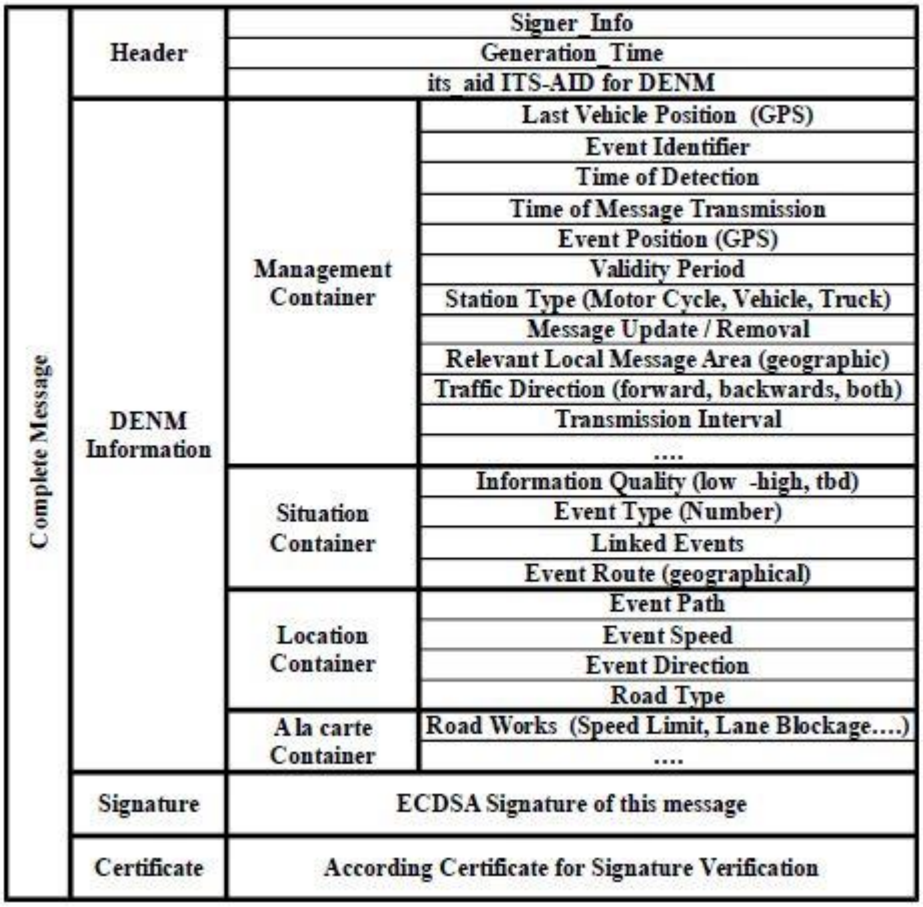
3.2.3) DENM

The ‘Decentralised Environmental Notification Messages’ (DENM) is standardised in ETSI EN 302 637-3 ‘Intelligent Transport Systems ITS; Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralised Environmental Notification Basic Service’.

The DENM is event-based, it is sent, if a vehicle senses special conditions or incidents like black ice or a sudden upcoming fog. It is meant for urgent emergency situations. The DENM is sent in addition to the CAM. It contains location information about the event (not the transmitting vehicle) and complements that data with a range of events or conditions (e.g.: different weather conditions, visibility, road adhesion or collision warnings). DENM are ‘multi-hop’ messages. They could be sent from an ITS Station to a certain area and get there ‘hopping’ from ITS station to ITS station. It could also be sent by an ITS Station and remain in an area as long as the event remains. Theoretically a DENM could also stay in a certain area being passed from one car to another.

Similar to the CAM it also consists of data containers that are mainly filled with data defined in the Common Data Dictionary (see above).

Figure 3: structure of a DENM



Complete Message	Header	Signer_Info	
		Generation_Time	
		its_aid ITS-AID for DENM	
	DENM Information	Management Container	Last Vehicle Position (GPS)
			Event Identifier
			Time of Detection
			Time of Message Transmission
			Event Position (GPS)
			Validity Period
			Station Type (Motor Cycle, Vehicle, Truck)
			Message Update / Removal
			Relevant Local Message Area (geographic)
			Traffic Direction (forward, backwards, both)
			Transmission Interval
			....
		Situation Container	Information Quality (low -high, tbd)
			Event Type (Number)
			Linked Events
			Event Route (geographical)
		Location Container	Event Path
			Event Speed
			Event Direction
			Road Type
		A la carte Container	Road Works (Speed Limit, Lane Blockage....)
			....
	Signature	ECDSA Signature of this message	
	Certificate	According Certificate for Signature Verification	

The DENM, similar to the CAM, also comes with a signature and a pointer to an authorisation ticket, that allows the recipient to check the authenticity of the DENM to establish trust in the system.

DENM processing follows the same steps as CAM processing: dissemination, collection and subsequent processing. The originator (ITS Station) detects, generates and broadcasts a DENM. At the receiver ITS Station, the DENM is processed and the information is checked. The DENM messages have a timestamp and estimates the event or variation duration, making these messages representative and valid only for a certain duration.

3.3) Public Key Infrastructure (PKI)

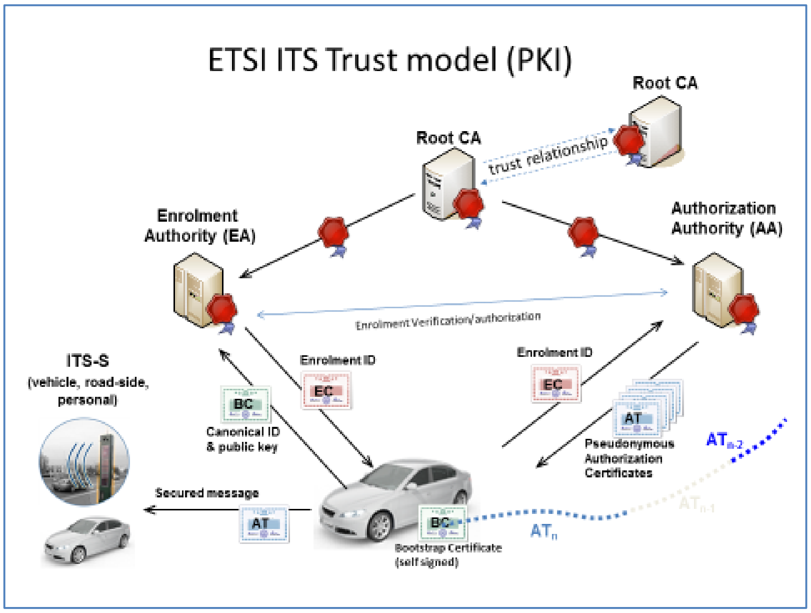
CAM and DENM include cryptographically signed certificates, using pseudonyms [40]. The PKI enables the ITS Station to guarantee that the messages are authentic and allows ITS Stations to distinguish between:

[40] As defined in the General Data Protection Regulation (EU) 2016/679 Article 4 (5*)*. Technically speaking the ‘pseudonym’ is a cryptographic signed certificates, that corresponds to a public key certificate called authorisation ticket. The authorisation ticket represents the ITS Station, without revealing the identity of the vehicle or its driver.

a.) messages that are authentic and should be processed and b.) fake, untrusted messages that are to be ignored. In other words, the PKI supports the authentication of the messages and their integrity. If a malicious attacker changes a CAM message, the security solutions in place by the PKI, guarantees that an ITS station can check that the message has been tampered. In addition to the security function of integrity, the authorisation ticket also serves as measure to conceal the identity of the vehicle and prevent tracking[41] by design. The authorisation ticket 'pseudonymises'[42] the vehicle or user.

The PKI is a governance structure that works according to principles laid down in a certificate policy and uses several security certificates to achieve its goal.

Figure 4: Security PKI overview


ETSI ITS Trust model (PKI)
Root CA
Root CA
trust relationship
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
ITS-S (vehicle, road-side, personal)
Enrolment ID
EC
Enrolment ID
EC
BC
Canonical ID & public key
AT
Pseudonymous Authorization Certificates
AT_{n-2}
AT_{n-1}
AT_n
Secured message
AT
BC
Bootstrap Certificate (self signed)

The usage period of an authorisation ticket relates to the amount of time a vehicle can be identified through its certificate, hence tracked. It should be noted that a short period of tracking is indeed desirable and absolutely necessary for road safety purposes as an important C-ITS design component to enable the system and make applications work. The usage period has an impact on the consumption of authorisation tickets by vehicles, which again impacts on: a.) how often they need to be updated and b.) the design of the C-ITS-Station. In other words, there is a trade-off between the need to reduce the frequency of generation of authorisation tickets to minimize the storage and processing power in the C-ITS stations/PKI and the need to decrease the traceability of the C-ITS-Station.

3.3.1) Authorisation tickets

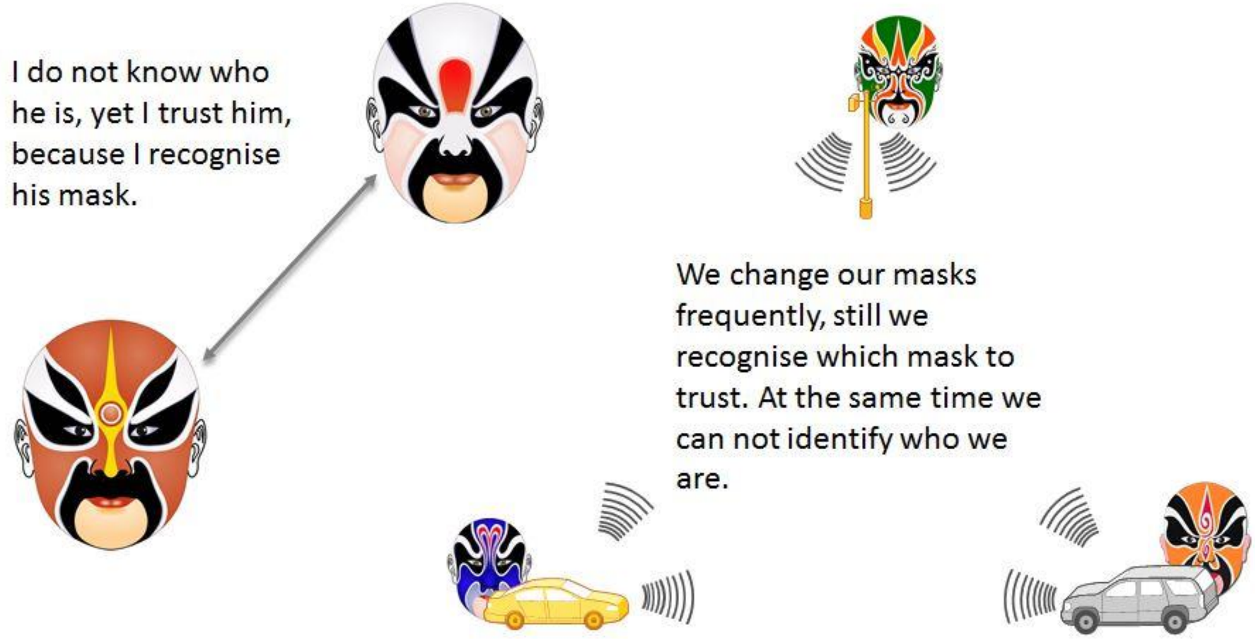
The authorisation ticket is standardised in ETSI TS 103 097 'Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats'. It is also sometimes referred to as short-term certificate or

[41] See ETSI TS 103 097 'Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats'

[42] 2016/676/EU General Data Protection Regulation, Article 4, (5)

pseudonym certificate. Authorisation tickets are public key certificates. The authorisation ticket pseudonymises the vehicles' identity, whilst at the same time showing that the user is recognised by the system and can be trusted. The authorisation tickets are changed in regular intervals to prevent the tracking of a vehicle. Since a short amount of trackability is necessary for road safety, each vehicle will use an authorisation ticket to sign CAMs and DENMs for a limited amount of time, and change it afterwards. The exact usage time and how the certificates are changed is regulated by the security policy. The authorisation ticket can be compared to a mask that a C-ITS Station wears for a certain amount of time. It is issued by the authorisation authority, which is an element of the PKI structure (compare with Figure 4).

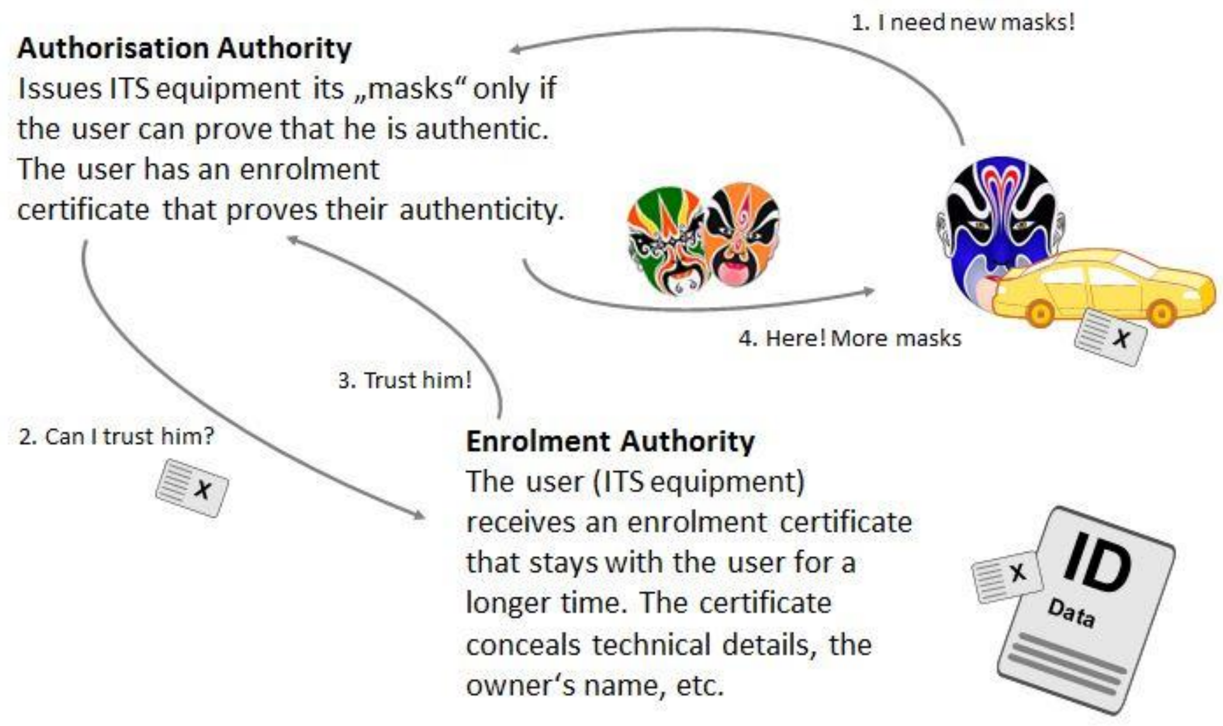
Figure 5: Security PKI pseudonymisation using authorisation tickets


I do not know who he is, yet I trust him, because I recognise his mask.
We change our masks frequently, still we recognise which mask to trust. At the same time we can not identify who we are.

3.3.2) Enrolment certificates

An authorisation ticket can only be issued to a vehicle that can prove that it is a part of the C-ITS system. That is achieved through the enrolment certificate. The enrolment certificate is also sometimes referred to as long-term certificate. The enrolment certificate makes sure that the user is not known to the authorisation authority. The authorisation authority and the enrolment authority have to be separate entities and trust each other.

Figure 6: Security PKI relationship between the authorisation and the enrolment authorities



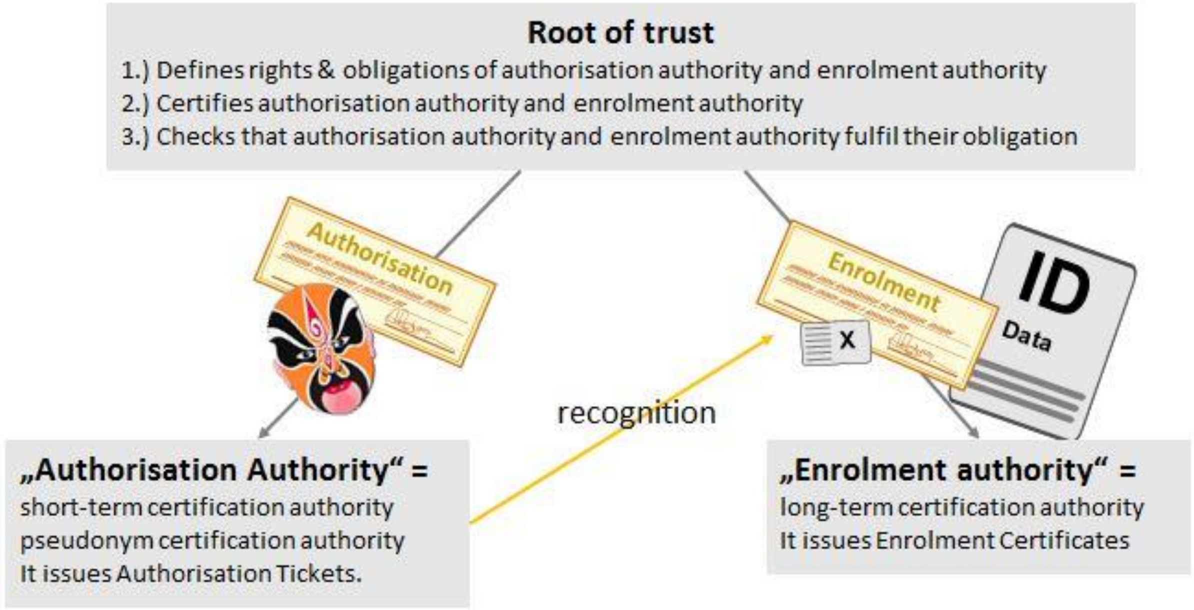
Authorisation Authority
Issues ITS equipment its „masks" only if the user can prove that he is authentic. The user has an enrolment certificate that proves their authenticity.

Enrolment Authority
The user (ITS equipment) receives an enrolment certificate that stays with the user for a longer time. The certificate conceals technical details, the owner's name, etc.

3.3.3) The root certification authority

The root certification authority establishes trust between the enrolment and the authorisation authorities and supervises them. A PKI can have one or more root certification authorities depending on the Certificate Policy ("the rules of the PKI"), in case of several root certification authorities within a single PKI they all need to adhere to the same Certificate Policy. In Europe a common certificate policy for all C-ITS stations is currently being drafted within the scope of the C-ITS Platform.

Figure 7: Security PKI –root certification authority


Root of trust
1.) Defines rights & obligations of authorisation authority and enrolment authority
2.) Certifies authorisation authority and enrolment authority
3.) Checks that authorisation authority and enrolment authority fulfil their obligation
Authorisation
Enrolment
ID
Data
X
recognition
„Authorisation Authority“ =
short-term certification authority
pseudonym certification authority
It issues Authorisation Tickets.
„Enrolment authority“ =
long-term certification authority
It issues Enrolment Certificates

3.3.4) Revocation of trust

The PKI also allows the so-called ‘revocation of trust’, which removes senders of unauthentic messages from the system by refusing the provision of new authorisation tickets (see below). The old authorisation tickets will simply expire. The choice of revocation through expiry has been made for privacy reasons as it eliminates the need for storing and publishing any linkage between pseudonyms and the real identity of a C-ITS Station. Revocation is key to maintaining the overall integrity of C-ITS and guarantees that C-ITS achieves its purpose. It also requires the identification of an offender, if necessary and is hence privacy sensitive.

3.3.5) Security and certificate policies

The security policy for C-ITS defines the security framework for C-ITS, it identifies risks for C-ITS and outlines remedies, such as governance systems, such as the PKI introduced above, that are underpinned with technological solutions. The security policy addresses not only threats to personal data, also wider threats such as cyber security risks.

The certificate policy defines what type of certificates C-ITS requires to address the risk of tracking. It looks at the governance of the certificates via the PKI and defines how certificates are distributed to ITS Stations, at what frequency authorisation tickets change, their validity and usage periods.

Both documents – the security and the certificate policy – are currently being drafted and finalised within the scope of the C-ITS Platform for the scope of Day 1 C-ITS services. Their establishment is steered through the European Commission, as laid down in COM 2016/766[43].

4.) ANALYSIS: C-ITS AND THE PRINCIPLES OF DATA PROCESSING

This section introduces and analyses the C-ITS in the context of the principles of processing personal data outlined in Article 5 of the GDPR. As the working group is continuing the analysis and evaluation of the suitable legal basis, it has been decided in the group that at this point the approach is to rule out those legal basis that have been analysed to be not applicable and further on to continue the analysis in the working group with those ones that might be suitable in order to ground for further development of C-ITS.

4.1) Lawfulness, fairness and transparency

During the phase I of the C-ITS platform, it was concluded that CAM and DENM messages are personal data due to the following factors. The data subject is indirectly identifiable via the CAM. The CAM contains an authorisation ticket, issued by the PKI (see section 3.3). Furthermore the CAM contains location data and the dimensions of the vehicle, which may also indirectly identify the data subject. The DENM also has an authorisation ticket, which also makes the data subject identifiable.

4.1.1.) Legal basis

In this section the C-ITS functionalities are analysed through the article 6 of GDPR. The goal is to find suitable legal basis via ruling out the ones that at this point seem to be invalid.

4.1.1.1) Consent

A possible legal basis to process personal data is to instantiate **the informed consent** given by the data subject. During the Phase 1 of the C-ITS platform, the working group dealing with data protection and privacy seriously considered that option as suitable one, recommending a gradual instantiation of the consent by providing the vehicles with ad hoc technologies allowing attaching consent markers to personal data. During the phase I the working group also took into account the opinion from article 29 (15/2011) in relation to the definition of consent.

After a more thorough analysis the C-ITS Platform working group had to eventually reconsider that position, and invalidate that legal basis, as an instantiation of a valid **informed consent** results simply impossible in practice. The required granularity of consent considering the multitude of choices and applications as well as potential processing purposes is considered too difficult to be implemented in the C-ITS context. Additionally, in the C-ITS context, the actors acting as data controllers might not even have a direct one-to-one relationship with the data subject, due to the open broadcast nature of the data. Furthermore taking into account that at this stage the controller has not been defined to a level that data subject would be aware of the identity of the controller, **consent as such**, standalone element, cannot be considered as a viable legal basis. However, the concept of consent needs to be further

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

elaborated in terms of the roles that it plays in relation to legal basis, namely performance of contract, as well as when the focus is shifted from day one applications, of non-commercial nature , towards commercial applications, with a possible C-ITS service provider.

4.1.1.2) Performance of a contract

As a second legal basis, the Working Group has considered the option to process personal data where the processing is necessary to perform a contract to which the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract. This option may be feasible in specific and limited scenarios, where the data subject actually does have a contract with the data controller. Such circumstances could exist for example in private or closed roads, where the road operator could require the existence of a contract to be able to drive on the road and could necessitate the collection of data for C-ITS purposes. The complexity of the contractual relationship in the C-ITS framework as well as the long chain of actor being involved, should be linked to the concept of joint controllership as defined in the article 26 of the GDPR if performance of the contract is to be used to be as legal basis in the C-ITS. However this requires an analysis of the various entities in relation to purposes and means as well as taking into account the principle of accountability and fulfillment of the contractual obligations distinct to data processing agreements as well as evaluation of how much power is delegated to different actors and the relationship between the actors.

4.1.1.3) Legal obligation

In some Member States, processing of personal data for C-ITS purposes may be required by applicable laws, where the controller may be subject to a legal obligation to collect the personal data in the first place. At the time of this writing, the Working Group is not aware of such Member State laws, which would necessitate the collection and/or subsequent processing and therefore the Working Group does not currently consider legal obligation as a valid basis for processing.

4.1.1.4) Vital interest

Processing being necessary in order to protect the vital interest of the data subject or of another natural person was identified as the possible legal basis as it is considered that the C-ITS system, when fully operational and introduced, can save lives. The current scenarios for ‘day-one’ applications are primarily advisory services that can be live saving for data subjects, for instance collision warnings (e.g.: wrong way driving, intersections). However, vital interest is a legal ground that can only be used in actual emergency situations, not for expected future emergency situations.. The justification of road safety and efficiency in relation to the necessity to protect an interest that is essential for the life of data subject or that of another natural person might not be viable, furthermore as this legal basis should only be used if processing cannot be manifestly based on another legal basis. In those cases public interest seems more appropriate.

4.1.1.5) Public interest

The Working Group considers the processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, particularly adapted in case of road safety and traffic efficiency purposes. This ground has an embedded requirement that the processing must be necessary to perform the task for public interest. However it needs to be taken into account that public interest should be evoked by a public body, which might not be necessarily fulfilled in the context of C-ITS as well as the fact that at this stage there is no obligation for the vehicles to be C-ITS compatible, which then complicates the use of public interest as a legal base. Furthermore a condition for applying this legal ground is that this necessity must be laid down in a national or EU law serving that public interest. In the context C-ITS this could be solved in the future, but still the question with public interest prevailing over free will of choice should be addressed.

Road safety plays a key role in transport policy and is part of the TFEU. Furthermore the ITS Directive already lays the groundwork for future ITS applications. The C-ITS 'day-one' applications clearly aim at increasing road safety.

In this case the ITS Directive would specify the technical aspects of the system, such as harmonising the CAM and DENM standards, establish a security policy, including a certification policy (establishing the PKI) and oblige C-ITS participants to comply with it, establish a privacy policy. The purpose of the system would in such a case be established through a piece of legislation that states the purpose of C-ITS and the modalities of its introduction. This model can take many shapes and could also operate with joint data controllers depending on the degree of specification of the ITS applications.

A law prescribing C-ITS would make transmission of CAM mandatory. The US is considering introducing C-ITS on a basis of road safety.

4.1.1.6) Legitimate interest

The Working Group has also considered the processing for the purpose of the legitimate interests pursued by the controller or by a third party. In this ground, the data controller is required to perform the balancing test, to ensure that the planned processing does not override the interests or fundamental rights and freedoms of the data subject(s). However with this option the working group needs to verify the balancing test that should be performed by the individual controller. Furthermore in the context of C-ITS factors to be taken into account when carrying out the balancing test should include but not limited to, the impact to the data subjects in the C-ITS context, how they are processed and additional safeguards to limit the undue impact on the data subject.

4.1.1.7) Recommendation of the possible legal basis

It can be concluded that consent will play a role in the further analysis but not as a self-standing legal basis, based on the analysis done at this point. Also it can be argued that legal obligation to collect data subjected to controller does not constitute firm ground as there are no laws in place in Member States at the moment nor at European Level. Vital interest as legal basis in relation to C-ITS does not comply with the actual accident versus of expected prevention of emergency situations.

As a summary from grounds to legitimise the processing of personal data, the C-ITS Platform Working Group considers that based on the analysis, the possible appropriate legal basis, or combination of them, that should be further analysed are:

- **public interests**, which would require enactment of supporting law(s) to legitimise the data processing activities required to perform the task(s) for public interests on the basis of a national or EU law

- **legitimate interest**, where the individual data controller would need to carry out the balancing test prior to initiating the processing
- **Performance of a contract**

Based on the analysis done at the working group concerning day one applications, it is becoming evident that lawfulness of processing might not be grounded only in one, but would be based on combination of two or more legal basis, of which it seem that for example a combination of public interest and performance of a contract might be viable way forward.

4.1.2) Fairness

Fairness in data protection requires the Data Controller to be open about why data is needed (purpose) and how it is processed (transparent) and not to use the data not to the detriment of the Data Subject. Further the data controller should be able to prove that the data is well protected from tampering or other misuse.

4.1.3) Transparency

The Data Controller is responsible for assuring that the data subject can exercise his rights. Data Subjects have the right to know for what purpose their data is being processed, which data is exactly collected and processed, furthermore that data subject has the right to access their data, the right to have their data rectified or erased. The Data Controller has to be available and answerable to the Data Subject.

The C-ITS context makes this a challenge. Whilst for roadside ITS Stations it may be reasonably simple to establish the Data Controller, for vehicle based ITS Stations this is difficult: C-ITS relies on broadcast, meaning the sender has no way of establishing which ITS Station has received the transmission. Hence a Data Subject may find it difficult to establish the Data Controllers of the ITS Stations that received their CAM or DENM. Vice-versa a Data Controller will find it difficult to establish all the Data Subjects from which his ITS Station received CAM or DENM.

The Data Controller would need additional personal information to identify the Data Subjects he is responsible for, which in itself would probably violate the ‘data minimisation’ principle to process the minimum amount of data necessary to fulfil the purpose of C-ITS. Here Article 11 of the General Data Protection Regulation is likely to apply and would relieve the Data Controller of his responsibility to give the access to data, rectify or erase data, make data portable, etc. Exception: A Data Subject explicitly requests to exercise these rights and makes additional personal data available for the purpose of exercising their rights under the GDPR.

Better transparency is probably best addressed by uniform data processing procedures, about which information is publicly or widely available.

4.2) Purpose limitation

4.2.1) Specified

The specification of the purpose of data collection outlines for which purpose data is being collected and limits the data collection, since it also allows an evaluation of which data is necessary to achieve the purpose of data collection. This concerns the amount of content, as well as the volume and links to the concept of 'data minimisation', discussed further below in the document. The Data Controller is responsible for specifying the exact purpose and assessing which data is necessary. He also establishes the according procedures concerning transparency and compliance with the principles of data processing.

Since C-ITS is developing and there is no legal base or purpose outlined yet, for the sake of discussion, the 'day-one' applications serve as our start point. They serve road safety and efficient transport. The two concepts are closely related, since a fluent flow of traffic plays a key role preventing accidents from happening. The 'day-one' applications also have to be analysed for what data they require. C-ITS also plays a key role enabling automation, by complementing sensor data with a direct data exchange between vehicles.

C-ITS relies on the processing of CAM messages, which for many 'day-one' use cases form the data on which events are detected and DENM generated. They serve a range of applications with their basic data, including the 'day one' applications. The C-ITS architecture is also assumed to be the most data efficient way of handling road safety and traffic efficiency (see C-ITS section above).

Furthermore personal data may need to be processed to maintain the integrity of C-ITS. By this we mean that the data that needs to be processed to revoke trust should also be considered serving the purpose of the C-ITS 'day one' use cases.

4.2.2) Explicit

The purpose has to be spelt out explicitly. This links 'purpose limitation' to the concept of 'transparency' outlined above. The Data Controller has to communicate the purpose of the data processing to the Data Subject.

In a C-ITS context this poses a challenge, since the Data Controller (one or possible more) have a problem identifying their Data Subjects. They should not seek to identify their Data Subjects[44], yet they need to find ways to meet their transparency requirements towards them.

4.2.3) Legitimate

Considering the importance of road safety, climate and environmental concerns for public policy it can be assumed that the purposes of C-ITS are legitimate. Yet to fulfil this requirement Article 6 of the GDPR 'Lawfulness of processing' needs to be fulfilled. No legal basis for the processing of personal data for C-ITS exists yet.

[44] See GDPR Article 11

4.3) Data minimisation

The essence of data minimisation is that data should only be asked when adequate, relevant and necessary for the present purpose.

In order to make C-ITS operational, at least the basic data location, speed and direction of the vehicle should be broadcast. Per use case some additional data may be required. Specifically important are the data that actually could lead to identification of the subject. The CAM message itself is designed to only transmit the data necessary to allow C-ITS actors to monitor their direct vicinity. CAM messages are ‘single hop’. Special events are transmitted via DENM.

DENMs are never generated unsolicited, only if a trigger event is detected a DENM is created and sent out. The first question would be whether the DENM contains personal data. Besides the protocol and management content, DENMs only contain information which specifically describes the triggering event, no additional data is added. When a DENM is being forwarded from one vehicle to other vehicles the question is if any personal data from this vehicle will be added to the DENM.

CAMs are generated periodically as long as a C-ITS station is active. For some time-critical applications the necessary frequency of CAMs generated is 10Hz (once every 2,8 meters at 100km/h). This may happen if a DENM has been received and increasing the frequency of transmission increases visibility and reduces the risk of an accident. As the sending station has to provide enough data to enable time-critical applications all the time, it has to send CAMs at that frequency as long as other C-ITS stations are around.

CAMs contain information describing the nature of the C-ITS station, their actual position, their movement and the history of positions As C-ITS applications are specified only on a high level in ETSI standard documents, it is not defined which message attributes are used in which application.

4.4) Accuracy

The personal data processed should be accurate and, in case of inaccuracy, should be corrected without delay.

C-ITS is machine-to-machine communication, hence the motorist has no access to the data. This principle would be best addressed in vehicular ITS Stations through deleting the information after processing. Road operators collecting CAM via roadside ITS Stations may want to keep information for longer periods of time. In this case the personal identifiers should be removed, rendering the information anonymous and the identification of the Data Subject impossible.

These procedures are best made public to serve the transparency requirement of the Data Controller, since the Data Controller may not be able identifying the Data Subjects and vice-versa.

4.5) Storage limitation

Personal data should not be stored any longer than necessary for the present task. An exception being unauthorised messages, posing a threat to the integrity of C-ITS, and which may be kept to allow a revocation of trust. Depending on the legal basis of processing data may also have to be stored for limited time periods for liability reasons to support the Data Controller proving the compliance with specifications in case of legal action. The exact storage limitation will have to be established by the data controller.

Road side stations may store and relay data that could later be transferred to a traffic management centre for traffic management purposes. In this case, clear rules under which the (anonymised) data can be stored, during which period, duration, and for which purposes must be established through contracts, guidelines, etc.

4.6) Integrity and confidentiality

Personal data should be appropriately secured, including protection against unauthorised processing and against disclosure, accidental loss, destruction or damage, using appropriate technical and organisational measures (‘integrity and confidentiality’).

The design of the PKI guarantees the integrity of the messages and their authenticity (see section 3.3 on PKI description).

If a malicious attacker tampers with a CAM message, the security solutions in place by the PKI guarantee that a user will be able to notice that the message has been tampered. The PKI also allows the so-called ‘revocation of trust‘, which removes senders of unauthentic messages from the system by refusing the issue of new pseudonym certificates. Revocation is the key to maintaining the overall integrity of the C-ITS system.

4.6.1) Tracking

There is no direct unique Data Subject identifier in any messages available for the receiver of the CAM or DENM. Still collecting CAMs in a systematic way may allow the identification of the Data Subject or at least the vehicle. But this would require correlations with other possible data sources such as traffic patterns collected by other means (e.g. mobile phones, digital tachograph, etc.). It is to be understood that access to CAMs in combination with other sources can support a tracking activity, but still requiring a lot of efforts. A tracking activity based only on CAMs data collection is unrealistic or would require even more efforts. It is exactly what the Pseudonyms technique is pursuing, bringing the barrier higher, and mitigating the tracking risks.

Spot-Check tracker: If an attacker manages to have a sensor network with sensors only at some dedicated locations which are more than 600m away from each other, he will not be able to get a complete set of CAMs. The track segments the attacker gets, cannot be linked by CAM content, identifiers are necessary to achieve this. If the identifiers contained and added to a CAM (MAC, Station ID, Authorisation Ticket) are changed in a frequency high enough to have a change between sensors, it is not possible to link track segments to form a continuous track with established confidence. For an ID-change-interval of 5 minutes this would mean a sensor distance of at least 4.5 km in urban areas and a distance of at least 11 km along a highway.

Area-wide tracker: If an attacker manages it to have a sensor network active with at least one sensor every 600m (with a radius of 300m estimated ITS-G5 coverage), he has to be considered as area-wide attacker being able to receive every CAM sent in this area. As CAMs can be easily linked to form a track by their content, there is no mitigation measure to establish privacy in the current C-ITS system proposal if facing an area-wide attacker. Such a scenario seems technically and economically not viable. Should an attacker have the resources to build up a wide coverage surveillance system the added value of receiving CAM would be limited. Furthermore this option would create an unacceptable level of legal uncertainty for a company. A government actor capable of introducing mass surveillance on such a scale would probably have more efficient alternatives than CAM for tracking persons.

In addition to the C-ITS PKI security there also need to be other deterrents against tracking in place, as well as possible restrictions to access of equipment.

4.6.2.) Attacking the PKI

In this scenario an attacker would need to gain access to an Authorisation Authority and the Enrolment Authority of a given vehicle to link the Authorisation Ticket obtained from a CAM to the actual vehicle reference held by the enrolment authority.

The C-ITS PKI itself requires strict security governance only allowing access with high levels of security clearance.

4.6.3) Repurposing data

The Data Controller should set up governance structures that prevent the re-purposing of data. In case of public purpose as a legal base for processing vehicular ITS Stations ought to delete received CAM after processing, one can assume that the repurposing mainly concern the Data Controllers of roadside ITS Stations. Data Controllers here will have to implement rules regarding the stripping of any personal attributes from all data they process and anonymise them, hence making them non-personal and not infringing the rights of the Data Subject if and when repurposing the data. If data is processed in the fulfilment of a contractual obligation, personal data probably need to be stored for a period of time by the data controllers for liability reasons. In such cases it is the obligation of the data controller to prevent repurposing of personal data.

5.) CONCLUSION

This document provided the background of only the C-ITS ‘day-one’ use cases. Trust in the system as well as legal certainty is needed and coordinated deployment of C-ITS at European level requires EU action, that also makes sure that the protection of personal data and privacy goals are met on the level that legislation requires, starting from the day one applications as laid down in COM 2016/766. Due to the rapid development in the context of C-ITS and the fact that some of the issues will require more analysis in order to have a solid basis for further work, some of the controversial issues will left later, however the working group is fully committed to take align the actions to be taken with the implementation of GDPR.

As the goal is large scale deployment in 2019, the appropriate legal framework was built on the General

Data Protection Regulation. This document analyses only the C-ITS ‘day one’ use cases in the context of the principles of the processing of personal data in accordance with Article 5 of the GDPR. Further for any personal data processing to be lawful it needs to satisfy one or more of the six grounds for legitimate processing set out in Article 6 of the Regulation.

Whereas road safety is a public purpose, embedded in public policy. The C-ITS ‘day one’ use cases ought to follow this pattern. They help preventing accidents and ameliorate their impact should they be inevitable.

Whereas there is no law that justifies the processing of personal data for C-ITS.

Whereas C-ITS is highly complex and involves a broad range of actors who not necessarily define the purpose of the system and at the same time are crucial to defining the means of C-ITS.

The expert group concluded that a mix of a contractual obligation between the Data Subject and the Data Controller and between the Data Controllers themselves could be the most appropriate legal basis.

To enable C-ITS ‘day-one’ applications across the EU a set of rules and standards are required to make the system interoperable, secure and compliant with the General Data Protection Regulation. This can be covered under the ITS Directive, which could harmonise the relevant standards, establish a security and certification policy, as well as a data protection policy. The rules under the ITS Directive would need to be complied with by all who decide to implement C-ITS to assure the system functions across the EU.

The ITS Directive may stipulate how C-ITS is to be operated, yet it does not provide the legal basis for processing personal data. Here a contract between the Data Subject and the Data Controller is a prerequisite.

The Data Controller determines the purpose and the means of the C-ITS applications. Since the overall purpose is a public one, it can be assumed that there will be a public actor that has to carry a Data Controller role. ITS is to run seamless across the EU, it should hence be an actor that is able and mandated to act across the EU. At the same time C-ITS is implemented by means that lie outside the public realm, meaning that those who define the means also may have a Data Controller role.

Practically an organisation of Data Controllers would probably be best suited to assure the mutual recognition of the specification of the ‘day-one’ applications - the means of processing. At the same time a guardian of public interest would be required to control, if the ‘day-one’ applications, as specified by the Data Controllers controlling the means of processing, meet the purpose of public interest. This organisation would exercise joint control over C-ITS.