FAQ regarding Data Protection in C-ITS

CAR 2 CAR Communication Consortium

About the C2C-CC

Enhancing road safety and traffic efficiency by means of Cooperative Intelligent Transport Systems and Services (C-ITS) is the dedicated goal of the CAR 2 CAR Communication Consortium. The industrial driven, non-commercial association was founded in 2002 by vehicle manufacturers affiliated with the idea of cooperative road traffic based on Vehicle-to-Vehicle Communications (V2V) and supported by Vehicle-to-Infrastructure Communications (V2I). Today, the Consortium comprises 88 members, with 18 vehicle manufacturers, 39 equipment suppliers and 31 research organisations.

Over the years, the CAR 2 CAR Communication Consortium has evolved to be one of the key players in preparing the initial deployment of C-ITS in Europe and the subsequent innovation phases. CAR 2 CAR members focus on wireless V2V communication applications based on ITS-G5 and concentrate all efforts on creating standards to ensure the interoperability of cooperative systems, spanning all vehicle classes across borders and brands. As a key contributor, the CAR 2 CAR Communication Consortium works in close cooperation with the European and international standardisation organisations such as ETSI and CEN.

Disclaimer

Document information

Number:	TR 2051	**Version:**	1.0.0	**Date:**	2018 – 09 – 18
Title:	**FAQ regarding Data Protection in C-ITS**			**Document Type:**	Technical Report
Release:					
Release Status:	Released for public sharing				
Status:	Completed				

Author:

Company /Institute	Author	Chapter
	Task Force Privacy	

Approval:

Function	Name, Company	Date	Signature
	Steering Committee		

Outstanding Issues

Issue	Author	Chapter

Changes since last version

Title:	
Explanatory notes:	

Issue	Rev.	Date	Changes	Edited by	Approved

Content

List of figures

List of tables

1 Introduction

1.1 Abstract

This paper presents answers from the CAR 2 CAR Communication Consortium of frequently reappearing questions and comments on privacy aspects especially related to the sharing of the safety related Common Awareness Message (CAM), in the context of the preparation of the EU Delegated Act on C-ITS.

The scope is therefore limited to mainly 4 chapters:

- Systematic description of the envisaged processing operations and the purposes of the processing,
- Assessment of the necessity and proportionality of the processing operations in relation to the purpose,
- Assessment of the risks to the rights and freedoms of data subjects
- Measures envisaged to addresses the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Regulation considering the rights and legitimate interests of data subjects and other persons concerned.

This paper is applicable for short range direct communication only in which vehicles and other road users share directly within a distance of in average 300m without involvement of any network their dynamic state. Even if it focusses primary on Day1 applications, it has been necessary to include processing needs for services beyond these applications as they are directly built on and depending of the equipment's capabilities deployed before.

The provided background information is as much exhaustive as possible and related to the questions answered. Complementary information is available in ETSI norms [RD-1], EU security policy papers [RD-2] and C2C Position Paper regarding personal data protection aspects in C-ITS [RD-3].

2 Processing operations and purpose of the processing

2.1 What is the exact content of the CAM message?

ETSI EN 302 637-2: *"Cooperative Awareness Messages (CAMs) are messages exchanged in the ITS network between ITS-Ss* ***to create and maintain awareness of each other and to support cooperative performance of vehicles using the road network.*** *A CAM contains* ***status and attribute information*** *of the originating ITS-S. The content varies depending on the type of the ITS-S. For vehicle ITS-Ss the status information* ***includes time, position, motion state, activated systems, etc.*** *and the attribute information includes data about the* ***dimensions, vehicle type and role in the road traffic, etc****. On reception of a CAM the receiving ITS-S becomes aware of the presence, type, and status of the originating ITS-S. The received information can be used by the receiving ITS-S to support several ITS applications. For example, by comparing the status of the originating ITS-S with its own status, a receiving ITS-S is able to estimate the collision risk with the originating ITS-S and if necessary may inform the driver of the vehicle via the HMI. Multiple ITS applications may rely on the CA basic service. It is assigned to domain application support facilities in ETSI TS 102 894-1 [i.6]. Besides the support of applications, the awareness of other ITS-S gained by the CA basic service may be used in the networking & transport layer for the position dependent dissemination of messages, e.g. DENM by GeoBroadcasting as specified in ETSI EN 302 636-4-1 [i.5]. The generation and transmission of CAM is managed by the CA basic service by implementing the CAM protocol."*

The CAM consists of a collection of data elements that are arranged in a hierarchical order:

- mandatory information i.e. a heading indicating the StationID (vehicle pseudo ID), then
- basic data like a timestamp and position,
- status data as a sub-set refreshed in high frequency mode (HF) that includes vehicle static and dynamic data like: speed, heading, acceleration and curvature,
- attribute data in low frequency refreshing mode, like vehicle role or category and some basic sensors,
- optional container relating to vehicle category details (public transport, rescue).
- Signature
- Certificate

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	

Table 2-1: CAM Structure

A vehicle will generate a CAM approximately every 4 meters and 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. This rule applies for the all CAM elements except for the Low Frequency and Special Containers. The Low Frequency container contains static information and therefore the transmission rate is limited to its purpose and generally not transmitted more often than twice a second. In general, special care has been taken to only send what strictly is required for ensuring safety, the special containers tailored to the specific purpose in general have a similar rate as the Low Frequency container based on their more static nature. The above time related requirements are detailed in the current ETSI specifications. For privacy and efficiency reasons the repetition rate of the CAMs is limited to the bare minimal, this in contrast with the approach in the USA where the BSM (read CAM) has a fixed rate of 10 Hz.

For the same reasons, upon receiving a CAM, the CA basic service makes the content of the CAM available to the ITS applications and/or to other facilities within the receiving ITS-S, such as a Local Dynamic Map (LDM). The time that indicates the maximum tolerable time a CAM packet can be buffered until it reaches its destination is called lifetime and is normalized in EN 302 636-4.

Furthermore, CAM are standardized to be 'single-hop' messages. They can only be processed by vehicles within their direct communication range (around 300m) and are not meant to be forwarded to other vehicles, since their relevance outside of their range would be limited.

ETSI 302 637-2 § 5.3.4.1: *"A CAM may relay on the services provided by the GeoNetwork/BTP stack. If this stack is used, the GN packet transport type Single-Hop Broadcasting (SHB) shall be used. In this scenario only nodes in direct communication range may receive the CAM."*

2.2 What are the broadcast range and receivers of the message?

Reception of CAMs broadcast from the vehicle according to the standard has been demonstrated to range **between 300 and 500 meters in average** depending on the circumstances in non-urban areas in view sight and by using standard in vehicle equipment. In urban areas this can be below 100 meters.

These distances are practical distances based on normal equipment. There are both functional and technical arguments why eaves dropping over a larger range is not realistic.

1. In case it would technically be possible to enhance the listening range of the eavesdropper equipment, this would mean that this equipment would hear more standard ITS Stations (ITS-Ss) while standard ITS-Ss can't. As the C-ITS radio channel management is decentralized, such that ITS-Ss are not interfering with each other, there is a high probability that eavesdropping equipment will here several ITS-Ss transmitting at the same time and therefore it will be very difficult for such equipment to distinguee information transmitted by different ITS-Ss while standard ITS-Ss do not have any problem. This depends of cause on the penetration of ITS equipment and density of ITS-Ss in the same area.
2. To increase the area and be able to listen to much more ITS-Ss and track one specific ITS-S in case the security measures are not considered, basically the sensitivity of the eavesdropping equipment needs to be increased by using very large visible antennas and increasing the sensitivity of the receiver. This may look possible and may work partly in none urban areas but in those areas, generally there are not too much roads or it is known where the road is heading to. Increasing the range will not provide additional information. Increasing the sensitivity in urban areas look more beneficial however there are many obstacles resulting in more visibility when installed (large antennas) but as the performance will not be very well predictable. The performance will be very much influenced by factors such as reception blocked by obstructing, the in band (other ITS-Ss) transmissions and out band other radio's such as Cellular, WiFi, Fixed Link, radar and other transmissions in dense areas increasing noise such that listening to ITS-Ss is limited or even blocked. Furthermore, weather conditions influence the performance.

As result of all these functional, technical and environmental limitations any eavesdropping equipment but especially in urban environment will have to be tailored to the specific situation and location while such installation will be visible by its tailored antenna(s). It also requires specific highly trained knowledge to design, realize and install such equipment for each specific location.

"*A fundamental reason is the cost of the network. The cost of setting up a new IEEE 802.11-based infrastructure and cover all the necessary areas may be prohibitive – it could be in the order of 4000 €/km^2. Utilizing the current cellular infrastructure – with appropriate software upgrades – the goal can be achieved in a fraction of that cost. There are, however, many challenges. The business model for a Mobile Network Operator (MNO) to provide V2X services is not so straightforward."* [RD-4]

Therefore, eavesdropping via none standard C-ITS equipment ranging over 300 – 500 meters is considered impracticable for the purpose it could be used.

CAM are not encrypted. Therefore, any other vehicle or roadside equipment in their direct communication range can receive and process the data.

Any vehicle or roadside equipment seeking to utilize CAM has to adopt the same communication technology, the same spectrum / channel, the same specifications and uniform methods to receive and process the information as the vehicle that is generating the CAM.

2.3 What do the sender and receiver gain from exchanging the message?

As defined under 2.1., CAM allows vehicles to **create and maintain awareness** of each other in a limited aria around the station to support cooperative performance. The time-critical provision of state information received from surrounding vehicles to alert or warn the driver of potential crashes would be the primary and most beneficial use of the CAM for road safety improvement. Such performance extends from Day 1 services as “Dangerous end of traffic queue” to more advanced services like Cooperative Adaptive Cruise Control (C-ACC), Platooning, Vulnerable Road User (VRU) or other forms of automated driving.

From both the short and midterm perspectives, the CAM will increase the vehicle’s capability to better anticipate traffic situations due its greater line of sight range and its ability in non-line of sight conditions to “see” around the corner or “through” other vehicles than any other current sensor. These performance features are already usable in current Advanced Driver Assistance Systems (ADAS) applications like Adaptive Cruise Control (ACC), Blind Spot Monitor, Lane Change Assistant, Collision Avoidance Systems, etc. as they extend the visibility on the neighbouring horizon (“e-horizon”). There is furthermore a real benefit not only to create awareness of potential hazards to supplement driver awareness but to maintain awareness to stabilize the traffic flow of a limited number of vehicles as well as there is interest to increase the safety of Vulnerable Road Users (VRUs) such as pedestrians. Therefore, some capabilities are not only needed to improve service operations in the first few years of deployment but will also be necessary for more advanced partially- or full-automated driving and VRU safety. Because the entire fleet will not be equipped at the same time, it is fundamental that first deployments include CAM functionality to jump-start the penetration rate and the efficiency for further generations of services.

3 Assessment of the necessity and proportionality of the processing operations

3.1 Why is the CAM needed to deliver the services?

The aim of the CAMs is to inform **permanently** other vehicles and road equipment about current road safety related vehicle/C-ITS **status, type and presence** information. This to let the road user or its equipment be better informed of the current situation around such it can make better safe decisions.

To complement the CAM, there is the **event-based DENM** (= Decentralized Environmental Notification Message). It is sent if a vehicle **senses special conditions or incidents** such as black ice or sudden upcoming fog. It is meant for emergency situations. The DENM is sent in addition to the CAM but not instead of. It is important to note that it might be triggered by the status of **neighbouring vehicles received towards their CAM that might conduct to crash imminent situations.**

Examples include: “Dangerous end of traffic jam queue” where the application provides benefits in addition to rear-end crash avoidance, namely to a better anticipation of road congestion. In these applications, the transmitting vehicle senses consecutive emergency braking, hard braking, or stationary traffic in its vicinity. Individual hard braking events or stationary traffic do not necessarily lead to a DENM transmission. Rather, this example application protocol is based on the analysis of CAM in the vicinity to trigger the alert on the transmitting vehicle. Specifically, the triggering conditions are based on detecting consecutive accelerations / decelerations in the vicinity that might lead to a road safety critical situation.

3.2 Is the CAM necessary for any other services than the dangerous end of traffic jam?

The C-ITS specifications define only the transmitting side, not the receiving side. The receiving side can use the CAM information for any safety related service. It can combine the received CAM information with other available internal information and create additional safety services beyond the list of services defined in the ETSI TR 102 638. When looking ahead to services such as C-ACC, Platooning and VRU, extension of the CAM or similar awareness information sharing messages can be expected. In case a DENM is shared with another vehicle to inform it about a potential danger, the transmitting vehicle will not be insured that the other vehicle got the message and will react respectively, sharing the CAM as a minimum allows the vehicular system to have at least a minimum set of awareness

Most of the Collision Risk Warning examples in ETSI TR 102 638 (e.g., longitudinal, across traffic turn, intersection) and lane change or merging assistance use cases are based on CAM as a first indicator of critical status data in the vicinity. However, sometimes vehicles will face critical driving situations where a crash between two vehicles is highly likely or even unavoidable. This is the PreCrash phase.

Among the priority road safety related messages of **Day1** figures two important use cases that imperatively use CAM:

- Special vehicle warning
- Request of ImpactReduction Container (IRC)

Special vehicles can face different situations: Emergency Vehicle in Operation, Stationary Safeguarding Emergency Vehicle, Stationary Wrecking Service Warning. Those vehicles can be recognized by other vehicles thanks to the field “stationType” that is set to 10 for special vehicles. But only the switch from a setting at 0 (default) in the field vehicleRole to 6 (emergency) is indicating that the vehicle is in operation. This setting is triggering detailed emergency DENM.

The service "**Request of IRC**" applies to a PreCrash phase as mentioned above. In this case, the transmitting vehicle requests from the potential collision opponent a DENM "Response of IRC" containing several physical data and information about the occupants **in order to reduce the injury impact from a crash**.

A "Request of IRC" is based on position and speed data identified in the CAM of the potential collision opponent.

Alacarte Container: ImpactReductionContainer	
heightLonCarrLeft	Height of left longitudinal carrier of the vehicle from base to top. Shall be set according to [AD-3].
heightLonCarrRight	Height of right longitudinal carrier of the vehicle from base to top. Shall be set according to [AD-3].
posLonCarrLeft	Longitudinal distance from the centre of vehicle front bumper to the front of the left longitudinal carrier of vehicle. Shall be set according to [AD-3].
posLonCarrRight	Longitudinal distance from the centre of vehicle front bumper to the front of the right longitudinal carrier of vehicle. Shall be set according to [AD-3].
positionOfPillars	Vehicle pillars refer to the vertical or near vertical support of vehicle, designated respectively as the A, B, C or D. Shall be set according to [AD-3].
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 according to [AD-3].
wheelBaseVehicle	Perpendicular distance between front and rear axle of the wheel base of vehicle. Shall be set according to [AD-3].
turningRadius	The smallest circular turn (i.e. U-turn) that the vehicle is capable of making. Shall be set according to [AD-3].
posFrontAx	Perpendicular distance between the vehicle front line of the bounding box and the front wheel axle. Shall be set according to [AD-3].
positionOfOccupants	BitString that indicates whether a passenger seat is occupied or whether the occupation status is detectable or not. Shall be set according to [AD-3].
vehicleMass	Mass of an empty loaded vehicle. Shall be set according to [AD-3].

Table 3-1: AlaCarteContainer OF IRC use case

Another example of CAM usage during Day1 deployment might concern urban infrastructure where messages like SPaT (Signal Phasing and Timing) and MAP for the Green Light Optimal Speed Advisory (GLOSA) or other services might be emitted less frequently as far as no vehicle enters in the dissemination area. The presence of a C-ITS capable vehicle is detected by its CAM.

Road safety, efficiency and automated services will depend on the CAM as well. Therefore, transmitting the CAM for Day 1 applications enables these crucial additional future services.

3.3 Why does the CAM need to be broadcasted?

The examples shown here illustrate the need for every vehicle in the vicinity to permanently maintain awareness about the status and presence of other vehicles to avoid crash imminent situations and to optimize / stabilize the flow of traffic. To limit the CAM to only certain vehicles (e.g. to vehicles just behind a transmitting vehicle) would exclude vehicles posing danger from a lateral side.

The option to choose to transmit or not transmit a CAM or to limit the information exchanged as specified in the current CAM specification currently defined should not be allowed for 2 reasons:

- The information exchanged has been carefully limited during the specification, evaluation and testing on analyses and measurements for 2 reasons.
  - To make most effective use of the spectrum possibilities and system resources.
  - To increase the privacy (for instance the weight of the vehicle is not provided while this is important information to identify the braking possibilities)

  Please note that the CAM transmission rate is conservatively adopted to the needs of the circumstances while in the USA the rate is fixed progressive to 10Hz. Incomplete state and other definition from the CAM therefore would in turn lead to incomplete information on the movement of the target vehicles and would decrease the effectiveness of the CAM to prevent collision between two moving vehicles. Therefore, the vehicle manufacturer could be held liable for C-ITS services beyond Day1 because information that could have prevented a crash was not used.
- It would undermine cooperative principle and design of C-ITS, which is based on a contribution-to-benefit of all principle. Withholding sending of an information captured in the CAM would cause the transmitting vehicle to accrue some benefit without giving a similar contribution. For example, one could consider transmitting CAMs only when receiving a DENM; however, this approach is unrealistic, because DENM emission is in turn dependent on receiving CAM information. In addition, this would have the same disadvantages as the hypothesis of the preceding item.

Prohibiting the broadcast of CAM data would greatly impede and render ineffective the C-ITS services related to road safety (e.g.: collision avoidance services).

It should be noted that there is a natural range limitation due to the communication range and the use of a single hop. **This limited broadcast over 300 to 500 meters is still sufficient enough to enable V2V crash avoidance applications in neighbouring vehicles, while limiting access by more geographically distant vehicles that can only benefit from safety information relayed by multi-hopping DENM.**

4 Assessment of the risks to the rights and freedoms of data subjects

4.1 What are the key risks associated to the use of personal data in the CAM? Are there specific high-risk cases?

In order to address the risk of a personal data breach due to the transmission and subsequent reception of single CAMs, the vehicle and road equipment security architecture standardized by ETSI and adopted by the C-ITS Certificate Policy foresees that CAMs and DENMs are only transmitted in a pseudonymised form, i.e. in a form that cannot be directly attributed to a data subject with the use of data that is publicly available or available to a single entity. Pseudonymisation means that the CAMs and DENMs include a pseudonym, i.e. and identifier that can only be related to an individual with the collusion of two certification authorities, and only if those certification authorities previously archived information related to the issuing of the certificates to the vehicle or road equipment. Additionally, CAMs and DENMs should be deleted or stripped of the identifiers after reception and processing in order to ensure that they do not contain personal data so to avoid further data breaches to insiders.

An additional risk that has been identified is that of location linking, i.e. the risk of re-attributing the CAMs to a vehicle/person due to the transmission and subsequent reception of a chain/trace of CAMs during the entire duration of an individual's trip. Therefore, it is planned that the data that would enable the attribution of single positions as a trace to an individual, appropriately changes during the trip, so to prevent the linking of the CAMs. So, in order to avoid location linking, the equipment mounted shall change all protocol identifiers at the same time. In addition, the unique CAM content such as the trace of last positions shall be systematically deleted.

The CAM contains data elements that **never directly** identifies a concrete vehicle, its owner or its driver as through license plates, registration information, vehicle VIN or via the radio physical fingerprint (each transmitter has its own radio unique characteristics). CAM have been conceived to **exclude any data that might be used to reasonably link – as a practical matter - a CAM to a specific person** "*on a persistent basis without unreasonable cost or effort, either in real time or retrospectively, given available data sources"* as mentioned in the Privacy Impact Assessment of the US Department of Transportation (PIA US-DOT) [RD-5]. The vehicle for example does not provide the weight of the vehicle although this would be very attractive to do dynamic behavioural analyses.

4.2 In how far, and in which cases, are these risks additional to already available means of identification?

Already available means of identification *"include physical surveillance (i.e., following a car by visual observation), placement of a specialized GPS device on a motor vehicle, physical access to Onboard GPS logs, electronic toll transactions, cell phone history, vehicle specific cell connections (BT signals), traffic surveillance cameras, electronic toll transponder tracking, and databases fed by automated license plate scanners"* [RD-5] *"… many of these non V2V tracking methods may be cheaper, easier, require less (and/or no skill) under certain scenarios".*

The novelty of C-ITS communication is that, compared to the passivity of the vehicles in the above-mentioned cases where external efforts are needed to collect the data, the vehicle becomes active and shares voluntarily, but indirectly, pseudonymized personal data.

5 Measures envisaged to address the risks

5.1 What data protection measures have already been taken in the current design, and how was their stringency decided?

The current security mechanisms in the C-ITS communications are designed to fulfil the requirements of road safety applications, i.e. **satisfying the needs for real-time, low-latency communications and high data reliability and integrity**. A short period of vehicle tracking is necessary for road safety purposes as an important C-ITS design component to enable the system and make applications work. The design of C-ITS security system provides solution for authentication and authorization of C-ITS entities to access safety-based services and send messages on the communication network. Privacy and Cyber Security features have been realized by design by defining the EU Certificate and Security Policy based on PKI management and pseudonymizing of the messages [RD-2] [RD-3].

How pseudonymizing is designed: it's based of 2 kinds of certificates, delivered by 2 separate Authorities:

- EC=Enrolment certificate (long term certificate) – to certify that the ITS station is enrolled in the data exchange system, in accordance with a policy defined by the European Authorities - delivered by the Enrolment Authority, which is the sole able to link the EC to the car identifier.
- AT=Authorization Ticket (short term certificate) – to sign the messages - the Authorization Authority delivers a batch of ATs to a user only identified by his EC.

Remark: Enrolment Authorities (EA) and Authorization Authorities (AA) responsibility can be entrusted to the same operator, under condition that information systems, operations and staff be completely separated.

In addition, for the EC delivery, the vehicle identifier is the vehicle communication unit number. The link between this unit number and the VIN is only kept in the OEM's database. This link will never be disclosed, except in case of a legal authority requirement.

Why pseudonymizing is needed:

- the AT shows that the user is recognized by the system and can be trusted;
- the system also allows the so-called 'revocation of trust', which removes senders of unauthentic or unauthorized messages from the system by refusing the provision of new authorization tickets.

How to control the risk of tracking: by changing frequently the AT as defined in the EU Security Policy and by segregation of duties as identifying the ATs would require

- To link ATs to the relevant ECs – this is only possible by the Authorization Authority
- To link ECs to the vehicle communication device number – this is only possible by the Enrolment Authority
- To link the vehicle communication device number to the VIN – this only possible by the OEM

As mentioned under § 4.1., CAM have been conceived to exclude any data that might be used to reasonably link – as a practical matter - a CAM to a specific person on a persistent basis without unreasonable cost or effort, either in real time or retrospectively, given available data sources.

Indirectly, and in combination with other data this could appear. Establishing the link between 2 or more Authorization Tickets (AT) used in different sequences by the same vehicle is limited by the communication range, the velocity of neighbouring vehicles inside and the usual distance between Road Side Units (RSU) as they have higher ranges thanks to their higher positioning

This has been analysed in the C2C Position Paper regarding personal data protection aspects in C-ITS [RD-3].

How is the issue of data retention addressed:

- A received CAM shall not be forwarded/multi-broadcast (ETSI EN 302 637-2. § 5.3.4.1).
- A received DENM may be forwarded/ broadcast only within a limited predefined geographical area (ETSI TS 101 539-1/2/3 and ETSI EN 302 637-3 § 6.1.3.3).
- Driving conditions data are kept in memory from a few seconds to a few minutes, depending on the need of the service. They are erased as soon as their emission conditions are over, and at each start of the engine (ETSI EN 302 637-3 § 6.1.2).
- No CAM is relayed to a vehicle manufacturer backend

5.2 If and why are the proposed additional mitigation measures below not be suitable / feasible (at this stage)?

The C2C-CC took note of following proposed additional mitigation measures from the Article 29 WG that might not be exhaustive:

- Data minimization
- Silent period
- Cryptographic protection
- Decrease the sending frequency,
  Decrease the emission power,
- Inject noise to the signal

Data minimization was addressed in European standards for CAM & DENM messages (see ETSI EN 302 367-2 for CAM and EN 302 637-3 for DENM). Data minimization is per se required by system due to the size of the frequency bandwidth, which does not allow the collection of a huge amount of data. Other data are also broadcasted only in specific situations (e.g. size of the vehicle is only displayed in dense traffic situations and the weight is not provided).

Data likely to identify a vehicle has been specifically studied and minimized as an example, in the aforementioned European standards, the vehicle size is defined at a precision level which does not enable the recipient to precisely recognize a model within a very broad range of car dimensions. Although knowing the weight of another vehicle is beneficial for vehicle dynamic behavioural; analysed this by this it could be concluded that there is something of interest in a particular vehicle.

In CAM, many dynamic vehicle parameters such as heading, curvature, acceleration, yaw rate are given with their associated accuracy levels. These accuracy levels are not static data and are specified in ETSI TS 102 894-2 (CDD) as discretized values (i.e. range of values) which significantly reduce the risk of tracking individual sensors of a vehicle with its quality information. Removing the accuracy level information or increasing the specified ranges for these vehicle data has negative impact on the safety systems of the vehicle or even render the parameters useless. If it would have been possible to minimize the accuracy it would have been done as there are costs related to that.

In a dangerous safety situation or pre-crash situation, the receiving vehicles will evaluate the collision risk processing speed and heading data (value and confidence), e.g. using Kalman filters.

The WP29 Opinion pointed out the risk of vehicle tracking by establishing the relation between 2 successive ATs used by the same device which disappear / appear in the same time (pseudonym change-over).

This risk could be mitigated by **introducing a silent period between 2 certificates, or a cryptographic protection of the change period.**

These solutions can be studied, although they are not included in the current ETSI release 1 standards or in deployment specifications (e.g. from the CAR 2 CAR Communication Consortium). However, a silent period would have a negative impact in terms of safety because the silent period, the vehicle would not deliver CAM information to its direct environment, significantly affecting use cases as described in 3.1. and 3.2. Moreover, it is unclear how long the silent period should be, given that there is a trade-off between data protection and road safety. For road safety purposes the silent period should be as short as possible (ideally zero). For data protection it depends which type of road users we are addressing. It is impossible to address 100% of the road users, since there will always be an exceptional case of somebody living in the remote places and being easily identifiable despite the silent period.

With respect to **encryption** of the C-ITS basic communications (i.e. safety messages such as CAM and DENM) this has been considered but found not to provide any benefit. This because of the nature of the system that is an ad-hoc network with a many to many communications, which is very different to the normal cases where encryption is used, such as peer to peer communication or broadcast (one to many). As the receiver needs to be able to process with no delay the first message received from transmitting equipment that appears in the range, the receiver would have to know the decryption key in advance. However, the receiver has no knowledge of who the sender is, so it is not possible to use different keys for different transmitters, thus everyone will have the same keys. This very wide distribution of the same key in combination with the short messages means that the encryption will be broken relatively fast and the encryption will be worthless.

Decreasing the sending frequency more than currently specified by the standards would either be useless in terms of data protection and would make road safety impossible. As identified in 3.3., contrary to the USA where the BSM (CAM) is sent with a progressive fixed rate of 10Hz, European norms consider to reduce the rate as much as possible when possible that resulted in rather complex CAM generation rules adopting the frequency to the situation and speed where the rate can go down to 1 Hz or less. The CAM rule has been specified, evaluated and tested with privacy in mind in advance to the GDPR and it has maximized the privacy while achieving safety, whereas it was maximized for safety in the USA. Further decrease of the CAM frequency would harm the safety objectives significantly.

Decrease the emission power has also been considered with the result that not the maximum by spectrum regulation allowed transmit power of 33 dBm is used but 23dBm. The current CAM transmission power has already been optimized considering road safety applications range, channel congestion and data protection. This limited transmit power of the CAM supports the safety related objectives through the reception in only a limited area relevant to realize increased safety. The transmit power of each message set is considered the same way.

Injecting noise to the signal would bear the question how a normal vehicle would be able to filter out the noise and an attacker not. Radio Frequency noise is in contradiction with the spectrum regulation and the efficient use of a spectrum. Noise in terms of blurring data such as GPS data is counterproductive to the targets of road safety to predict dangerous situations with the right accuracy.

5.3 Why are the residual risks deemed acceptable?

Let's define risk as usual in information security & privacy: impact * likelihood (i.e. probability of occurrence). Note that this definition is consistent with the recommendations of WP29 [RD-6].

Let's agree that:

- C-ITS brings a societal benefit in terms of road safety and traffic efficiency that makes residual risks acceptable.
- Eliminating risks completely is impossible unless the system is switched off.
- Information systems such as C-ITS shall be designed to reduce risks to an acceptable level.
- It is not acceptable to design a system against undefined risks or exceptional use cases.
- It is not acceptable to design a system against risks that are not demonstrated to actually materialize in real life.

There are two kinds of residual risk against data protection in C-ITS:

- The risk that a legitimate data controller uses the data for other purposes
- The risk that an illegitimate data controller (eavesdropper) takes possess of the data.

A legitimate controller in C-ITS is a controller that operates at least one ITS-Station that is enrolled with the C-ITS Security Credential Management System and that has an active role in road safety and traffic efficiency.

The first risk is mitigated by applicable data protection laws (GDPR). Any controller, i.e. a company needs to operate some sort of information security / data protection management system that ensures that data is not processed for other purposes. **Appropriate audits are necessary.**

The second risk is addressed by the countermeasures mentioned in 4.1, especially against:

- Local eavesdroppers
- Long-range spot-check attackers (see definition in [RD-3])

Both those threat scenarios are deemed possible (i.e, with likelihood >0) and have an impact. The impact to is reduced to almost zero by the AT change strategy in most cases.

There are no other threat scenarios we see with probability > 0 . The threat scenario of ubiquitous eavesdropping is deemed as not probable (i.e., probability ~ 0) unless an illegitimate controller (i.e. an unofficial or unlawful organization – in C-ITS terms) can be demonstrated to have both the resources and the interest to build up an ubiquitous network to survey an area of interest such as a region or city.

6 Appendix 1 – References

6.1 List of abbreviations

AA	Authorization Authority
ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistant System
AT	Authorization Ticket
BSM	Basic Safety Message
BTP	Basic Transport Protocol
C2C	Car2Car
CA	Cooperative Awareness
C-ACC	Cooperative ACC
CAM	Cooperative Awareness Message
CDD	Common Data Dictionary
C-ITS	Cooperative ITS
COM	Communication
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EC	here: Enrolment Certification
ETSI	European Telecommunications Standards Institute
FAQ	Frequently asked questions
GDPR	General Data Protection Regulation
GLOSA	Green Light Optimal Speed Advisory
GN	GeoNetwork
HF	High Frequency
ID	IDentifier
IRC	Impact Reduction Container
ITS	Intelligent Transport System
ITS-S	ITS-Station
LDM	Local Dynamic Map
OEM	Original Equipment Manufacturer
PIA	Privacy Impact Assessment
SHB	Single Hop Broadcasting
SPaT	Signal Phasing and Timing
RSU	Road Side Unit
V2V	Vehicle2Vehicle
VIN	Vehicle Identification Number
VRU	Vulnerable Road User

6.2 Applicable documents

[AD-1]

6.3 Related documents

[RD-1] **ETSI norms** as available under
https://www.etsi.org/technologies-clusters/technologies/automotive-intelligent-transport
mainly
EN 302 637-2 Specification of Cooperative Awareness Basic Service
EN 302 637-3 Specifications of Decentralized Environmental Notification Basic Service
EN 302 636-4/5 GeoNetworking / Geographical addressing and forwarding for point-to-point and point-to-multipoint communications and Basic Transport Protocol
TS 102 894-1/2 Users and applications requirements / Facility layer structure and Common data dictionary
TR 102 638 Basic Set of Applications
TS 101 539 Road Hazard Signalling

[RD-2] **European C-ITS policies** as
https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf
https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf

[RD-3] C2C Position Paper regarding personal data protection aspects in C-ITS
Nota: This Position Paper has been realized in 2017 as an input contribution for the WG5 of the European C-ITS platform in order to define the European Certificate and Security Policy. Some of the options might not be applicable any more.

[RD-4] 5G-PPP-White-Paper-on-Automotive-Vertical-Sectors
https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf

[RD-5] **Privacy Impact Assessment** of the US Department of Transportation
https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf

[RD-6] **Guidelines on DPIA**
http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

■ End of Document ■