Connected Motorcycle Consortium

CMC Basic Specification

System Specification

A C-ITS system for cars cannot simply be applied to powered two-wheelers due to their different characteristics. This document describes the system architecture, challenges for the various components and the potential solutions for powered two-wheelers.

Document Information

Document Title:	System Specification
Version:	1.0
Release Date:	11/12/2020

Disclaimer

This document has been developed within the Connected Motorcycle Consortium and might be further elaborated within the consortium. The Connected Motorcycle Consortium and its members accept no liability for any use of this document and other documents from the consortium.

Index

1 System Specification

1.1 Background and Objective

C-ITS System is an interoperable communication system that exchange information between vehicle and vehicle, vehicle and infrastructure. To do this, C-ITS system should have the minimum required functions.
The Basic Specification Profile created by the CAR 2 CAR Communication Consortium (C2C-CC) describes the system requirements for C-ITS system and ETSI also defines the technical specifications for C-ITS communication. However, these specifications are basically targeting cars. Therefore, CMC has defined a system architecture for PTW while securing communication with existing standards defined by the C2C-CC and ETSI.
Due to the different characteristics from cars, some functions of C-ITS system need special consideration for PTWs. In this specification, detailed specification of each function are described.
The description in this document does not set the requirements that all PTW OEMs have to follow, but it is one of the examples of how to implement C-ITS solution for PTW.

1.2 Architecture of C-ITS system for PTWs

1.2.1 Hardware Diagram

Hardware Diagram to enable C-ITS communications for PTW is defined in *Figure 1*.

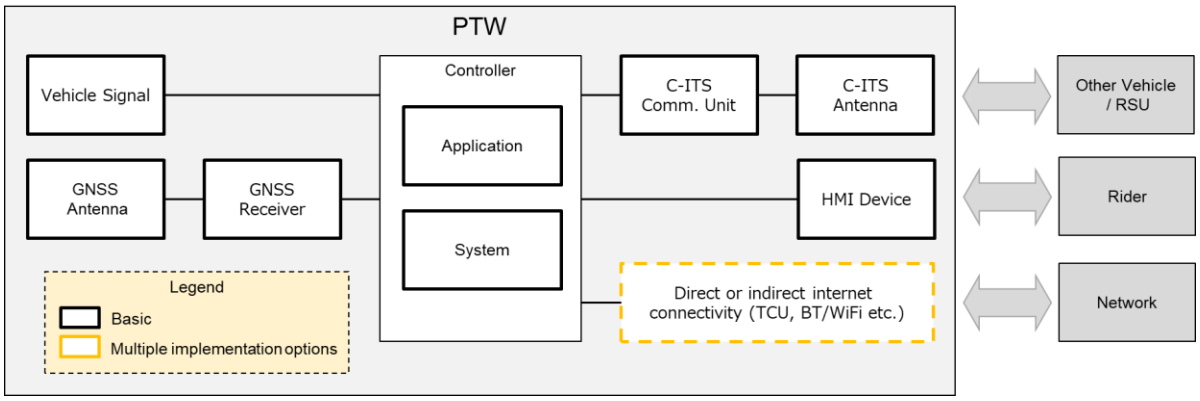


Figure 1: Hardware Diagram

C-ITS applications require Cooperative Awareness Message (CAM) transmission, CAM reception, Decentralized Environment Notification Message (DENM) transmission and DENM reception. The components shown in *Figure 1* are defined as the elements that are required when CAM and DENM messages are transmitted and received for related C-ITS applications. Furthermore, the C-ITS security implementation requires a data channel for intermittent exchange of security certificates. With the current state of the technology, an internet connection is the only practical method. This can be implemented in one of several ways, e.g. via a Telematics Control Unit or via an infotainment subsystem connectivity such as Wi-Fi or Bluetooth.

1.2.2 System Architecture

The functions of C-ITS system are defined in technical specifications by ETSI. For example, ETSI TS 102 894-1 defines reference communication architecture and functional specifications for Facility layer[1]. Fundamentally, PTWs should follow these specifications to communicate with other vehicles.

However, there are some challenges for PTWs when it comes to implementing these specifications. These challenges are described in Chapter 2.

In this specification, the system architecture was redrawn as *Figure 2* to focus on PTW specific considerations and challenges.

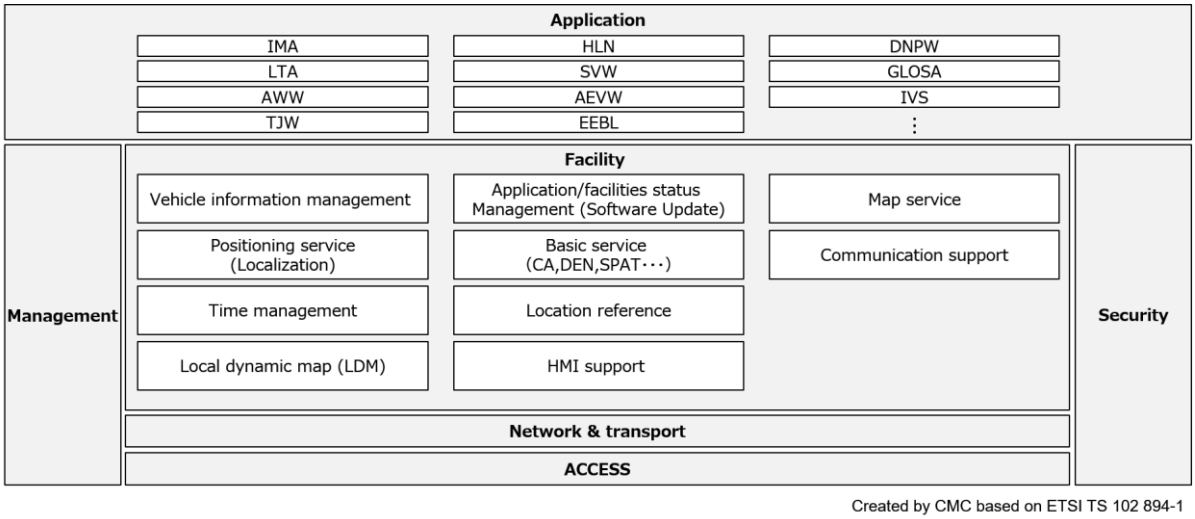


Figure 2: System Architecture

The main functions that require special considerations for PTW are in Application layer and Facility layer. C-ITS applications included in Application Layer are defined for PTW and are described in the CMC Basic Specification “Application Specification”. Therefore, functions of Facility layer are the main target of this System Specification.

General explanation of each function in Facility layer is described in Table 1.

Table 1: Function description

Function	Description
HMI support	Support data exchanges between applications and HMI devices.
Vehicle information management	Manage vehicle signal and provide applications and facilities.

[1] ETSI EN 102 894-1, V1.1.1 (2013-08), accessed on 05.11.2020: https://www.etsi.org/deliver/etsi_ts/102800_102899/10289401/01.01.01_60/ts_10289401v010101p.pdf

Basic service (CA, DEN, SPAT…)	Support protocol processing of each message.
Application/facilities status management(Software Update)	Manage and monitor active applications and facilities within the C-ITS station and its configuration.
Positioning service(Localisation)	Calculate real time position of C-ITS station and provide information to the facilities and applications layers.
Location reference	Calculate location referencing information and provide location referencing data to the applications/facilities layer.
Local dynamic map (LDM)	Local Dynamic Map database and management of the database.
Communication support	Provide services for communications and session management.
Time management	Provide time information and time synchronisation service within the C-ITS station.
Map service	Provide map matching functionality.

2 Function and component

The main functions and components of C-ITS which require special considerations for PTW comprise of the followings.

1. Localisation (Positioning Service):
   This function collects information used for geographical positioning of the vehicle and outputs its calculated geographical positioning information application/facility layer. The information input to the function could be from the Global Navigation Satellite System (GNSS) as the primary data and augmented by inertial data from the vehicle by IMU and speed sensor. In particular, as PTWs lean to change direction, IMU data is especially important to augment the geographical positioning of the vehicle.

2. C-ITS Antenna:
   C-ITS antenna is used to send and receive data such as CAM and DENM for communication between C-ITS stations. PTW needs special consideration for the C-ITS antenna because its characteristics can be affected by the antenna mounting position and leaning in a curve.

3. Application support:
   Collecting PTW vehicle signals is important for realising C-ITS applications.
   This function collects information from the vehicle through a dedicated communication bus, e.g. a CAN bus, and processes the information required at other management systems. Examples of vehicle information collected would be speed pulse, turn signal and stop lamp activation and IMU signal but others are possible. For PTW applications, the differences in

information collected from the vehicle compared with cars such as lean angle, need to be considered.

4. HMI:
   This function notifies the rider of the operation results of the C-ITS applications. Since the HMI guidelines are explained in the CMC Basic Specification “HMI Guideline”, HMI is out of scope of this document.

5. Security
   Security layer requires the vehicle to exchange certificates with certification authorities in the network. These certificates need to be updated regularly before its expiration in order to continuously communicate with other C-ITS stations. Special consideration is needed for PTWs because
   - Most PTWs are not equipped with cellular network connectivity interface to exchange certificates.
   - Some PTWs can be left inactive for long period of time, by which certificates could be expired.

2.1 Localisation

2.1.1 General description of Localisation

Many C-ITS applications require the transmission of vehicle state such as position, speed and heading. The localisation system outputs the geographical positioning information calculated by using GNSS, IMU sensor and other means. In the case of PTWs, the localisation system is more challenging than it is for cars due to the different dynamics. The localisation requirements for cars are defined for different scenarios to account for inevitable degradations due to the satellite environment. This section describes the points to consider for PTWs to build the localisation system and also the results of an investigation of whether the localisation requirements for cars can be applied to PTWs.

2.1.2 Challenges for PTWs

2.1.2.1 Basic definitions and properties of PTWs

PTW can be described by its mainframe, including the swingarm and rear wheel, and by the front frame, including the steering-system and front wheel (Figure 3). The vehicle's position and orientation are defined by the translations of the vehicle reference frame relative to a fixed reference frame and its yaw- (Ψ), pitch-(Θ) and roll-(φ)-angle around the vertical-(z), lateral-(y) and longitudinal-(x)-axis respectively (Figure 4).

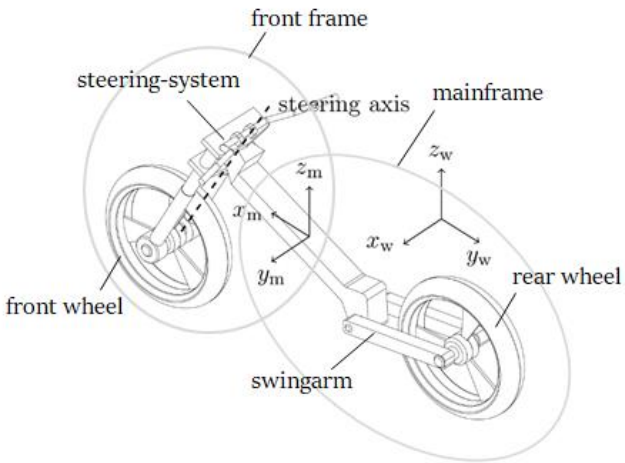


Figure 3: Vehicle Reference Frame

The yaw angle Ψ(around the vertical axis z) describes the direction the PTW is heading (e.g. north). The pitch angle Θ (around the lateral axis y) describes the dive and squat of the PTW. Last but not least, the roll angle φ around the longitudinal axis x is the key to manoeuvring a PTW, while this same roll angle is negligible on cars (known from many investigations about driving dynamics).

Figure 4: Rotation Angles of PTW (yaw / pitch / roll)

These properties allow a PTW to turn in a very different manner from cars. In the case of cars, cornering force is generated due to the slip angle of the tire (Figure 5); while for PTWs camber thrust is generated due to the roll angle (camber angle) generated in the vehicle body (Figure 6).

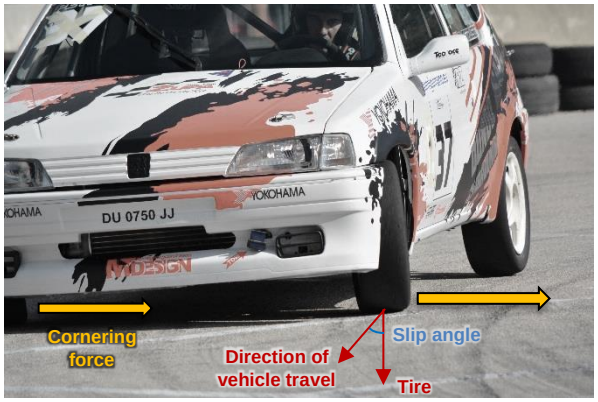


Figure 5: Cornering force on cars

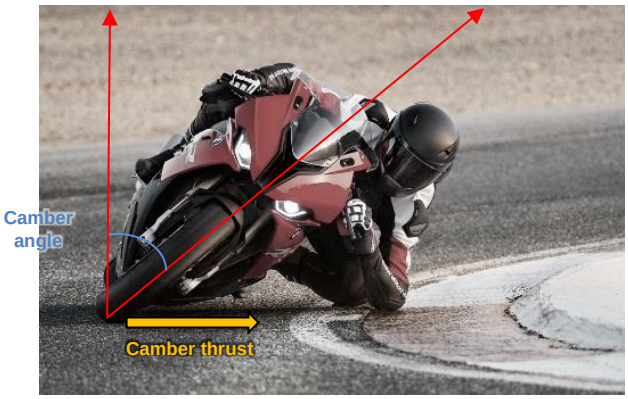


Figure 6: Camber thrust on PTWs

This makes the PTW cornering dynamics significantly less dependent on the steering angle compared to cars. To illustrate this last point, Figure 7 correlates the steering angle and curvature radius on PTWs at different travelling speeds.

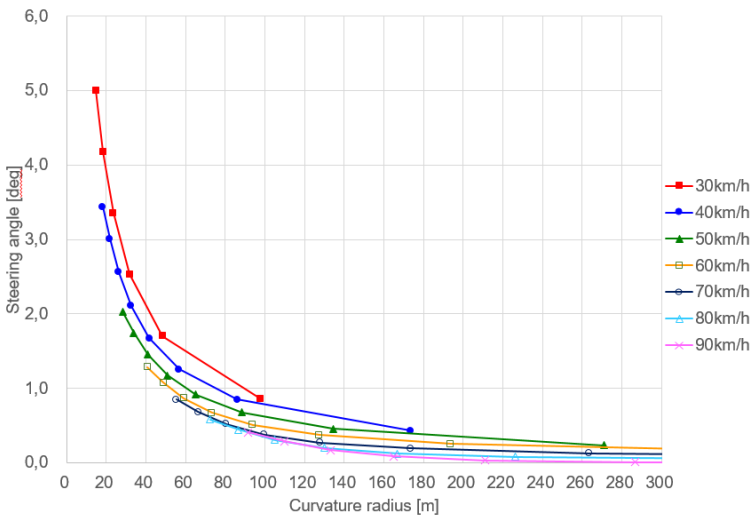


Figure 7: Steering angle versus curvature radius for PTWs

2.1.2.2 The necessity of a PTW-specific algorithm

As explained, the riding of a PTW is highly dynamic; and compared to cars, the steering angle of PTWs when turning is negligible, and it is difficult to accurately estimate the turning radius from that value alone.
Furthermore, since the z axis rotates along with the vehicle body while turning (Figure 8), it is not easy to calculate the yaw rate out the values given by the IMU.
For those reasons, PTWs need a GNSS correction algorithm, which differs from cars, in order to consider those factors and provide an accurate position.

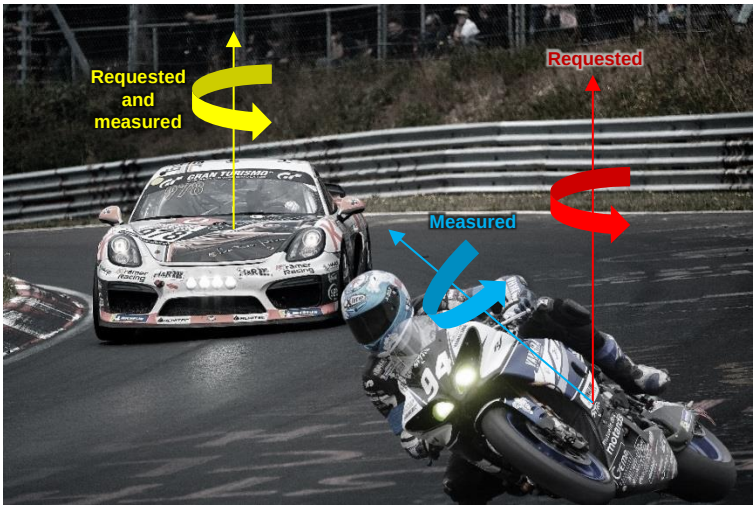


Figure 8: Requested and measured values of IMUs on cars and PTWs

As a reference, describe the importance of considering yaw rates in axes perpendicular to the ground rather than yaw rates in sensor or vehicle coordinates. Using the evaluation data described in the section 3.3 Localisation in the Evaluation Report document, compared the heading accuracy due to the difference in the reference coordinates. Figure 9 shows the

results of heading error when using yaw rate on the world coordinate system and yaw rate on the vehicle coordinate system. This data is an excerpt from the Day 1 City scenario where many changes of travel direction are included. Moreover, regarding the calculation of yaw rate on the vehicle coordinate system, the yaw rate on the world coordinate system was converted into the yaw rate on the vehicle coordinate system. Looking at the transition of the heading error, which is a comparison with the ground truth in the upper right, the accuracy of the heading is closer to the ground truth when yaw rate on the world coordinate system is adopted than when yaw rate on the vehicle coordinate system is adopted.

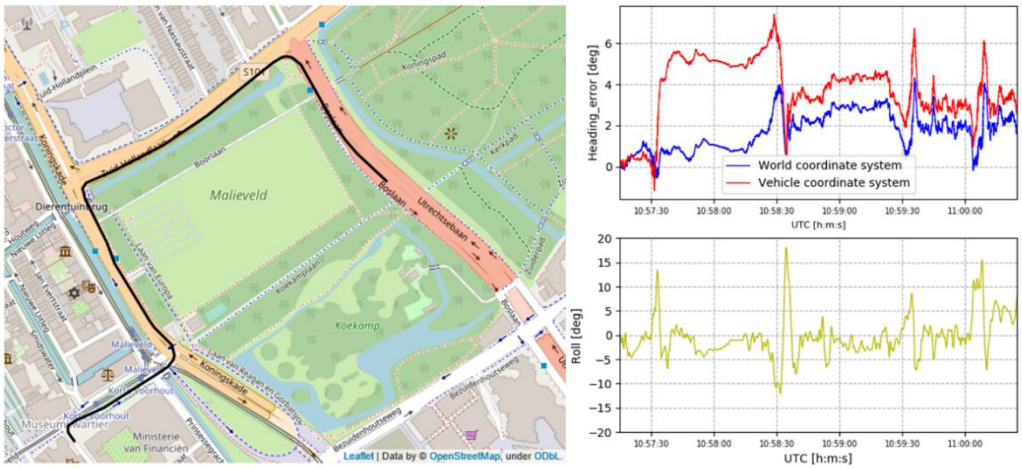


Figure 9: Trajectory (Left) and Heading error (Upper right) and Roll (Bottom right) in City scenario

2.1.2.3 Effect of output time delay/frequency

The output time delay/frequency required for localisation is defined by the CAM generation frequency and the calculation time requested from the upper application.

The CAM generation frequency is managed by the CA basic service; it defines the time interval between two consecutive CAM generations. Considering the requirements as specified in ETSI TS 101 539-1[2], ETSI TS 101 539-2[3] or ETSI TS 101 539-3[4] the upper and lower limits of the transmission interval are set as follows:

· The CAM generation interval shall not be less than T_GenCamMin = 100 ms. This corresponds to a CAM generation rate of 10 Hz.

[2] **ETSI TS 101 539-1, V1.1.1 (2013-08)**, accessed on 05.11.2020: https://www.etsi.org/deliver/etsi_ts/101500_101599/10153901/01.01.01_60/ts_10153901v010101p.pdf

[3] **ETSI TS 101 539-2, V1.1.1 (2018-06)**, accessed on 05.11.2020: https://www.etsi.org/deliver/etsi_ts/101500_101599/10153902/01.01.01_60/ts_10153902v010101p.pdf

[4] **ETSI TS 101 539-3, V1.1.1 (2013-11)**, accessed on 05.11.2020: https://www.etsi.org/deliver/etsi_ts/101500_101599/10153903/01.01.01_60/ts_10153903v010101p.pdf

· The CAM generation interval shall not be greater than T_GenCamMax = 1 000 ms. This corresponds to a CAM generation rate of 1 Hz.

On the other hand, the calculation time should be short enough that the system satisfies class A performance described in ETSI TS 101 539-3.

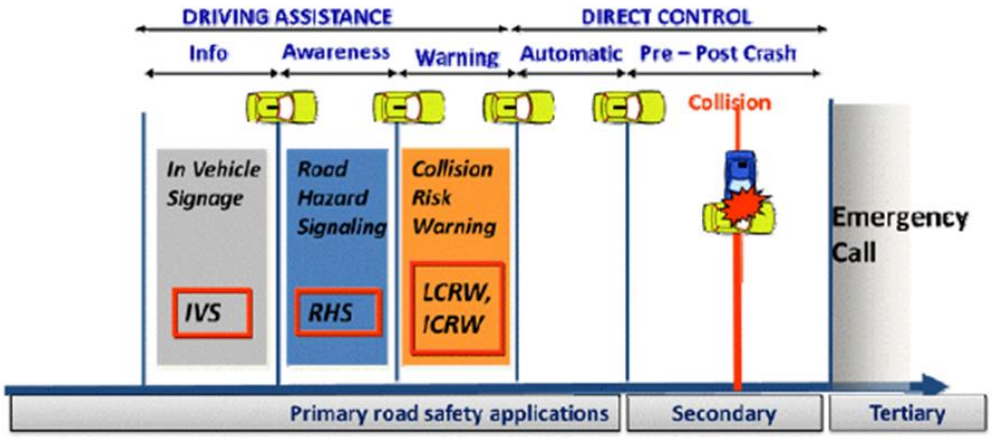


Figure 10: Overview of road safety applications

For example, IMA / LTA applications belong to the same “Collision Risk Warning” as Longitudinal Collision Risk Warning (LCRW)/Intersection Collision Risk Warning (ICRW) (Class A) shown in Figure 10.
“Class A” is defined in ETSI TS 101 539-3.
Class A: a class A C-ITS station shall guarantee a T0 to T1 less than 150 milliseconds. (Figure 11)

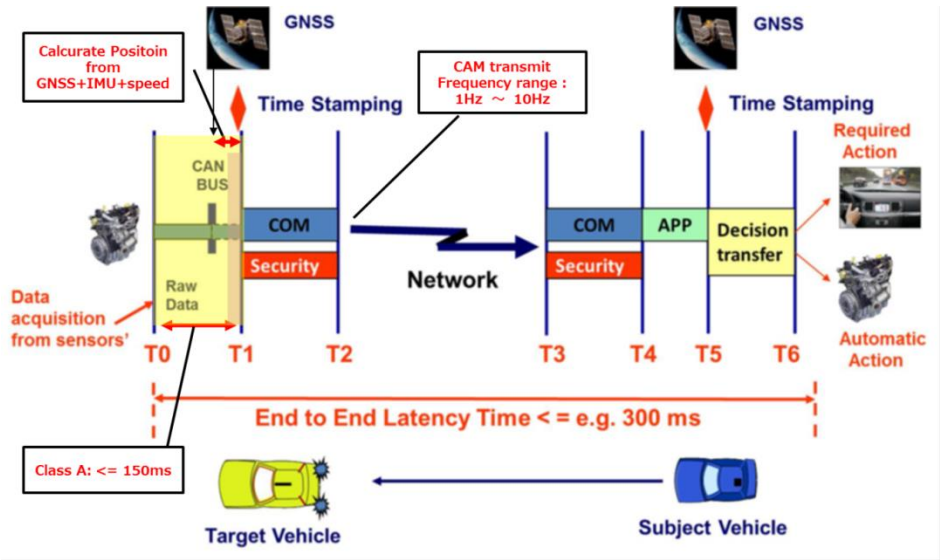


Figure 11: Application end-to-end latency time

From the “Class A” point of view, the time required to calculate the position from GNSS data, IMU and vehicle speed information should be less than 150 ms.

However, since the upper limit of the CAM generation frequency is 10 Hz, the localisation processing time from the acquisition of GNSS, IMU, and vehicle speed information to the completion of CAM transmission should be set to 100 ms (10 Hz) or less.

2.1.2.4 Integrated navigation/sensing algorithm

The localisation requirement for PTWs is aimed to be equivalent to cars. The requirement for cars is presented by C2C-CC, and the required values are defined for multiple scenarios. Positioning accuracy is required not only in scenarios such as Open Sky where GNSS positioning is enough, but also in environments with poor satellite environments such as cities and tunnels.
This section describes the points to consider in order to meet this cars localisation requirement for PTWs. In addition, as PTWs have different dynamics from cars, what is necessary as a unique algorithm is described.

First, as a system for estimating the position of vehicles, a positioning method using satellites called GNSS is generally used. The positioning by GNSS can acquire reception times, position, and other moving status of the vehicle only after receiving signals from at least four observed satellites. In an Open Sky scenario where there are almost no obstructions in the sky, such as when driving on a rural road, it is possible to estimate the vehicle position by a sufficient number of satellites. On the other hand, in a city scenario with many obstructions such as high-rise buildings or in a tunnel scenario, it is likely that the minimum number of satellites required for positioning cannot be observed. Under such a circumstances, the accuracy of position measured by GNSS deteriorates, and in the worst case, the position information becomes unavailable.

Therefore, technology is used that can continuously calculate the speed and attitude of the vehicle to estimate the position of the vehicle with high accuracy, even in an environment where positioning by GNSS is unavailable. This technology is called Dead Reckoning (DR) and is realised by mounting the IMU on the vehicle. A typical IMU for DR purpose contains three orthogonal rate-gyroscopes and three orthogonal acceleration sensors to estimate continuously the three-dimensional velocity and attitude of the vehicle from the measured angular velocity and linear acceleration. In particular, as PTWs has dynamics that are different from cars, and yaw and pitch change continuously during riding, it is essential to accurately estimate the three-dimensional attitudes of the vehicle. Also, since the IMU is rigidly mounted on the vehicle, it is necessary to consider the coordinate system in this estimation method. Specifically, as described in 2.1.2.2, the orientation of the vehicle in the earth coordinate system is ultimately used instead of the sensor or vehicle coordinate system.

However, no matter how high the accuracy of the sensor used is, measurement errors exists and errors accumulate over time (drift error), so that the estimated position will deviate from the ground truth position. In order to avoid this situation, it is necessary to combine the information output by DR, the external vehicle information obtained by GNSS and the wheel speed provided by the vehicle to estimate the most probable attitude, speed, and position of

the vehicle. This technology is called integrated navigation, and probabilistic position estimation methods exist and the Kalman filter is the current de facto standard.

2.1.3 Potential Solution

This section describes the examination of the solution required to ensure the same position accuracy for a PTW and a car. In order to investigate this solution, CMC prepared the following four levels of calculation models (hereinafter called “Localisation System”) and travelled along the travel route specified by C2C-CC to estimate the position of the ego vehicle in each travel scenario. At the same time, CMC calculated the error from the acquired ground truth value and evaluated which solution could satisfy the position accuracy requirement defined in C2C-CC. (For details of evaluation, refer to the section 3.3 Localisation in the Evaluation Report document.)

The outline of the Localisation System at each level is as follows.

- Level 1. GNSS positioning
  - Only the position information measured by GNSS positioning is used.
- Level 2. GNSS positioning + GNSS constant-speed and heading
  - The position prediction results obtained from simple extrapolation of GNSS velocity and heading information, are incorporated to interpolate between the update intervals of position information in Level 1.
- Level 3. Integrated Navigation Algorithm (GNSS and IMU)
  - The sensor fusion algorithm is used in DR. The vehicle position/state obtained from GNSS is used as the observed update value, and the vehicle state calculated using the sensor information obtained from the IMU is also used as the time update value. The optimum estimated solution of the vehicle position is obtained using both pieces of information.
- Level 4. Integrated Navigation Algorithm (GNSS, IMU and Odometry speed)
  - Speed information obtained as vehicle odometry data is added to the time update value in Level 3 to improve the accuracy of vehicle position estimation.

Additionally, the performance was evaluated by mounting the M8U manufactured by u-blox. This is a commercially available product, which is equipped with the Level 3 solution described above, on the vehicle.

2.1.4 Conclusion

Localisation System created by CMC and u-blox M8U, equivalent to Level 3 of Localisation System were mounted on a PTW and an evaluation test was conducted. Unfortunately, the position accuracy requirements in all scenarios defined by C2C-CC could not be satisfied. (See the CMC Basic Specification “Evaluation Report” section 3.3 for detailed results). However, since the knowledge about the required solutions as a specification that satisfying the C2C-CC requirements was obtained from this evaluation tests, it is described below.

At first, considering stand-alone GNSS positioning, which is Level 1 of Localisation System, even in the Open Sky scenario where a sufficient number of satellites can be observed, positioning using GNSS was not possible even for a short time when passing under the overpass. In the Half Open Sky scenario, the positioning accuracy by GNSS deteriorated due

to the decrease in the number of observation satellites. Since the accuracy of stand-alone GNSS positioning affects the positioning accuracy of all levels, the positioning accuracy of the Localisation System of all levels deteriorates as a result, and the positioning accuracy of the entire Localisation System could not satisfy the C2C-CC requirement. In order to satisfy the C2C-CC requirement for the Localisation System, it is necessary to increase the number of satellites observations, which is factor in improving the accuracy of stand-alone GNSS positioning. Specifically, it is effective to select an antenna with a high reception sensitivity. And as a result, in the Tunnel scenario and the Mountain scenario where a sufficient number of satellites were not observed for a long time, it was confirmed that the positioning value was not available, or even if it was available, the value deviated significantly from the true value.

In this case, it is necessary to estimate the vehicle position by the above-mentioned DR. In the Open Sky scenario, Level 4 of Localisation System were able to interpolate the positioning values when passing under the overpass in the Open Sky scenario. On the other hand, there was a lack of positioning by GNSS for about 3 minutes in the Tunnel scenario and about 1 minute in the Mountain scenario. In the Tunnel scenario, it was confirmed that if the positioning by GNSS is missing, it is possible to sufficiently correspond to the C2C-CC requirement only by DR positioning. However, in the Mountain scenario, the positioning time by DR is shorter than that of the Tunnel scenario, but unlike the tunnel, the driving route is not a simple straight, so the Heading deviates from the ground truth with the passage of time, and it was found that the positioning value also deviated significantly. To overcome this, it is necessary to improve the estimation accuracy of the vehicle attitude, and more specifically, to improve the Localisation System algorithm rather than the IMU measurement accuracy.

On the other hand, the u-blox M8U equipped with the functions equivalent to the above Localisation System Level 3 was unable to satisfy the C2C-CC requirement only in the Tunnel scenario only. As shown in Figure 12, the estimated heading could be accurately estimated with a difference of less than 1 degree, but the estimated velocity deviated with time until the GNSS is observed, and the maximum speed error was about 12 km/h. This deviation is the main cause of position error. This error is caused by the cumulative error due to the integral calculation of acceleration, and it seems that the C2C-CC requirement can be achieved by using the vehicle speed value obtained by the speed pulse from the vehicle.

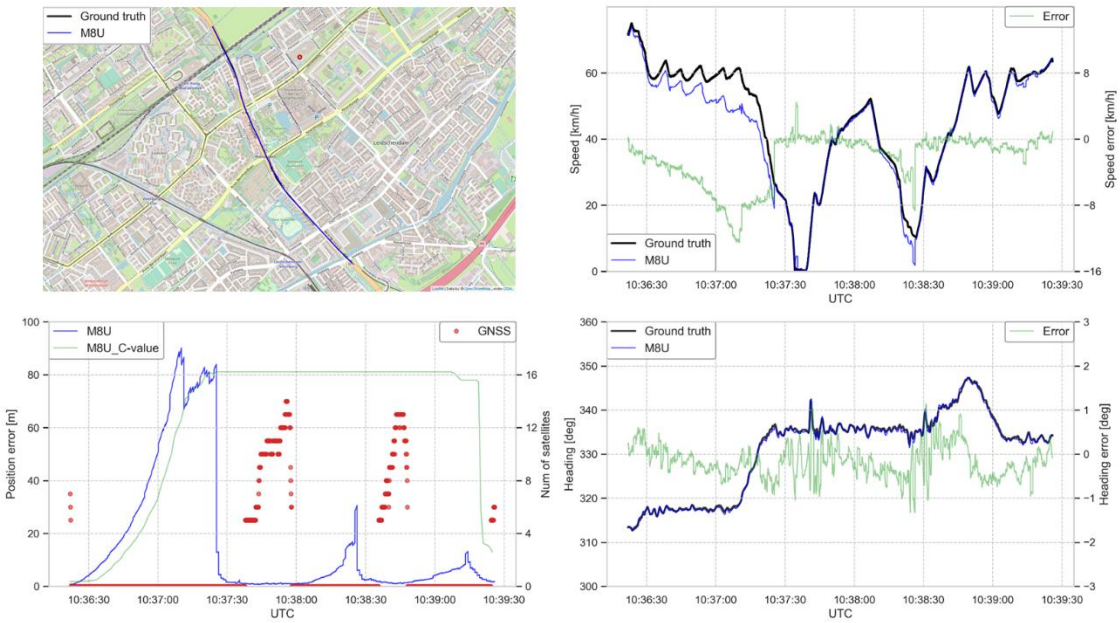


Figure 12: Output by M8U when riding in Tunnel scenario of Day

From the above facts, as a solution required to satisfy the C2C-CC requirement, the positioning by GNSS, the integrated navigation algorithm using 6-axis IMU, and the vehicle speed pulse as the vehicle speed value are the minimum recommended.

2.2 C-ITS antenna

2.2.1 General description

To share the vehicle status, position and intentions, antennas are needed at the sender and receiver side. There are several types of antennas considered for V2X communication usage in the 5.9 GHz frequency band, like dipole, monopole and directional antennas. To support at least a reasonable distance in all directions with a packet error rate less than 10% several challenges for PTW arose. In that context “reasonable” is related to the use case, a short example is illustrated below.

Simplified example for a traffic jam on a highway:

v (example speed) = 130 km/h = 36,11 m/s
a (smooth braking) = 2 m/s²
t (safety margin) = 2s
s (braking distance)

$$\boldsymbol{s} = v * t + \frac{v^2}{2a} = 36{,}11\frac{m}{s} * 2s + \frac{\left(36{,}11\frac{m}{s}\right)^2}{2 * 2\frac{m}{s^2}} = \mathbf{398{,}2\ m}$$

For that scenario, a minimal communication distance of 400 m shall be achieved. With higher velocities the required distance will increase.

2.2.2 Challenge for PTW

2.2.2.1 Mounting point

The standard mounting position on a car – the roof top – is not available on PTWs. Therefore, a suitable solution (dimension, position, integration) must be found.
The type of PTW (there are many categories ranging from scooters, touring bikes, off-road oriented up to sports bikes) impacts the antenna position and performance reaching the goal of an omnidirectional radiation characteristic.
Due to the fact, that mirrors might end up inducing unpredictable reflections and due to different types of PTW using different kinds of mirrors, this would lead to a huge amount of measurements.
At the end three alternatives were considered as being most relevant:

One antenna mounted at the rear.
One antenna mounted at the front.
Two antennas mounted, one at the rear and one at the front.

Figure 13: *Mounting positions of the antennas*

For PTW it turned out that antenna positions in the rear and/or front of the vehicle seem appropriate.

2.2.2.2 Rider and pillion

Due to the fact that a rider (and pillion) sit upright on a PTW the antenna has to be mounted different compared to a car. The bodies will change the overall shape and probably the characteristics of the radiation pattern.

2.2.2.3 Leaning in curves

Antennas mounted on a PTW might not achieve ideal vertical transmission due to the roll angle in curves. Therefore, the polarization of the transmitted waves will shift accordingly. The minimum requirement for the communication range shall still be supported at a sufficient roll angle (e.g. up to 25°) on both sides.

2.2.3 Potential solution

To face issues of the mounting position and unpredictable obstacles, such as rider, pillion, side/top-cases and other equipment mounted on the PTW the usage of two antennas in diversity mode is one potential solution. Those antennas need to be equipped in an appropriate manner, for example front and rear, to be able to complement each other reducing the impacts in between.
Antenna diversity is one of several wireless diversity schemes that uses two or more antennas to improve the quality and reliability of a wireless link. In urban and indoor environments, there is often no clear line-of-sight (LOS) between transmitter and receiver.
Antenna diversity is especially effective at mitigating multipath situations. This is because multiple antennas offer the receiver several observations of the same signal. Collectively such a system can provide a robust link. While this is primarily seen in receiving systems (diversity reception), the analogue has also proven valuable for transmitting systems (transmit diversity) as well.
Typically, signal reliability is paramount and using multiple antennas is an effective way to decrease the number of dropouts and lost connections.

Due to those theoretical advantages, measurements using a front and a rear mounted antenna are recommended.

In addition, measurements made with roll angles up to 30° generated an acceptable performance within the driving direction. A reduced performance in the opposite direction is deemed acceptable.

2.2.4 Conclusion

PTWs are recommended to use two antennas for transmitting and receiving C-ITS messages. Diversity mode results in an almost circular horizontal radiation pattern with the advantage of using the optimal gain in each direction which leads to a higher communication range in some directions. The second advantage is, that the whole PTW system is only marginally affected by obstacles such as vehicle itself, rider, pillion and/or baggage.
Some PTWs might need just one antenna, but in that case, measurements shall be investigated for ensuring a sufficient range. Some use cases, which require a long range, might not work properly by only using one antenna. For example during hard braking (EEBL) when using only a front mounted antenna.
The lean angle and the human body affect the range insignificantly, those results can be referred to in the evaluation report.

2.3 Cellular Communication

Even though cellular communication is not a requirement for C-ITS system, when in use, a cellular antenna which usually supports a different frequency band from the C-ITS antenna will be required. Any requirements related to cellular antenna are not described in this document, however, similar approaches to C-ITS antenna may be useful. The antenna pattern is highly influenced by the shape of the PTW and location of the antenna and therefore, diversity technology may help to secure a longer communication range.

2.4 Application Support

2.4.1 Time Synchronisation

Time Synchronisation does not require any PTW specific functionality. Therefore, the information for time synchronisation can be obtained from a Galileo or other GNSS receiver or from a Network Time Protocol (NTP) service and

$|\text{station clock time} - \text{C-ITS time}| < pPotiMaxTimeDiff$.

Where

- 'C-ITS time' or 'time base' means the number of elapsed International Atomic Time (TAI) milliseconds since 2004-01-01 00:00:00.000 Coordinated Universal Time (UTC)+0 as defined in [ETSI EN 302 636-4-1].
- 'station clock' means a clock representing C-ITS time in a C-ITS station.
- $pPotiMaxTimeDiff$ = 20 ms

2.4.2 HMI output prioritisation

Since multiple applications could operate at the same time, and multiple messages from multiple vehicles could be received, C-ITS system should be able to determine which application or message should be prioritised and therefore notified to riders through HMI.
If an application with higher priority requests to display a message through the HMI while a lower priority application is accessing HMI, C-ITS applications should be able to request HMI to show the higher priority message.
In summary, C-ITS system should have following two functionalities related to HMI.

- Set priority to applications and its messages
- Request HMI to show the high priority messages

2.4.3 V2X stack : CAM

CAM is a message exchanged between C-ITS stations 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 C-ITS station. The content varies depending on the type of the C-ITS station. 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 C-ITS station becomes aware of the presence, type, and status of the originating C-ITS station. The received information can be used by the receiving C-ITS station to support several C-ITS applications. For example, by comparing the status of the originating C-ITS station with its own status, a receiving C-ITS station is able to estimate the collision risk with the originating C-ITS station and if necessary may inform the driver of the vehicle via the HMI.
Compliant with ETSI EN 302 637-2 V1.4.1 (2019-04)

2.4.4 V2X stack : DENM

DENM is a facility layer message that is mainly used by C-ITS applications in order to alert road users of a detected event using ITS communication technologies. DENM is used to describe a variety of events that can be detected by C-ITS stations.
The DEN basic service is a facility layer entity that operates the DENM protocol. It provides services to entities at the C-ITS application layer. At the originating C-ITS station, a C-ITS station application may trigger, update and terminate the transmission of DENMs. At the receiving C-ITS station, the DEN basic service processes received DENMs and makes the information available for usage in C-ITS applications process.
Compliant with ETSI EN 302 637-3 V1.3.1 (2019-04)

2.4.5 Vehicle Signal

All CAMs generated by a vehicle C-ITS station shall include at least a high frequency vehicle (Vehicle HF) container, and optionally a low frequency vehicle (Vehicle LF) container. The Vehicle HF container contains all fast-changing (dynamic) status information of the vehicle C-ITS station such as heading or speed. The Vehicle LF container contains static or slow-changing vehicle data like the status of the exterior lights. Therefore, these data need to be obtained from vehicle.
Furthermore, a DENM is triggered when specific triggering conditions are satisfied depending on applications and its use cases. Any vehicle data which are required to judge the triggering conditions need to be obtained from vehicle.
The list of required vehicle signals for CAM and DENM are described in Table 2. Note that the vehicle data for DENM is required only when the applications and use cases are implemented.

Table 2: Vehicle Signal

Category	Vehicle data	Unit	CAM	DENM											
				EEBL	AEVW			AWW			SVW			TJW	
					EViO	SSEV	SRSW	Fog	Precipitation	Traction loss	Stopped	Broken down	Post crash	DEoQ	TJA
Vehicle odometry signal	Speed	[m/s]	M	M	M	M	M	M		M	M	M		M	
	Longitudinal Acceleration	[m/s²]	M	M						M				O	
	Lateral Acceleration	[m/s²]	O												
	Vertical Acceleration	[m/s²]	O												
	Yaw Rate	[deg/s]	M												
	Roll Angle	[deg]	M*1												
Vehicle control signal	GripThrottleAngle	[%]								M*3					
	Braking pressure	[%]		O						M*4					
	Gear Shift Position	status									O	O			
	Front Brake Status	ON/OFF		O											
	Rear Brake Status	ON/OFF		O											
	Parking Brake Status	ON/OFF				O	O				O	O			
	Anti-Slip Regulation (ASR) status	ON/OFF								M*3					
	Anti-lock Braking System (ABS) status	ON/OFF		O						M*4					
Vehicle illumination signal	Hazard light Status	ON/OFF	O*2			M	M		Not triggered by PTWs		M	M	To be confirmed	O	Not triggered by PTWs
	Left turn signal status	ON/OFF	O												
	Right turn signal status	ON/OFF	O												
	Rear-fog light status	ON/OFF	O					M							
	High-beam Status	ON/OFF	O												
	Low-beam Status	ON/OFF	O					M							
Other vehicle data	Vehicle Stand Status	ON/OFF									O	O			
	Light bar status (emergency vehicle)	ON/OFF			M	M	M								
	Tell-tale status	N/A										M			
	Engine relay	ON/OFF				O									
	Siren status (emergency vehicle)	ON/OFF			O										
	Seat occupancy	ON/OFF			O										
	Automatic transmission (AUT)	status				O	O				O	O			
	Ignition terminal	ON/OFF									O	O			
	Emergency stop switch status	ON/OFF									O	O			
	eCall status	ON/OFF											O		
	On-board camera sensor	N/A												O	

M: Mandatory O: Optional

*1: Roll angle is not a parameter in CAM, but needed for a calculation of curvature and vehiclewidth

*2: CAM consider Hazard light status is on when both Left turn signal status and Right turn signal status are on.

*3: Not mandatory if both of M*4 are satisfied. *4: Not mandatory if both of M*3 are satisfied.

2.5 Security

2.5.1 General description of C-ITS Security model

As C-ITS implementation is based on the exchange of messages between C-ITS stations such as vehicle-to-vehicle and vehicle-to-infrastructure, it is a fundamental requirement for the entire system to ensure that C-ITS stations such as PTWs can trust other station's data (authenticity) and also that the messages sent were not altered during the transmission (integrity).

2.5.1.1 Public key cryptography

This trust is, on the basic level, achieved by means of public key cryptography – algorithms that use various mathematical one-way functions for combining specially devised sets of data known as "keys" with the message data. The keys are devised in a way that creates corresponding pairs of keys called "public key" and "private key".

In most common scenarios, the C-ITS station that sends message would use these algorithms to combine the message with a private key to obtain a "signature" – a data sequence smaller than the original message that is appended to the original message and then transmitted to the other participants. A C-ITS participant that receives a message, would use similar algorithms and a corresponding public key to verify that the signature that was received is matching the message data that was received, thus confirming the integrity of the data. The nature of the mathematical functions used makes it computationally infeasible for a party who does not have access to the private key used by the sender, to create a signed message that could be verified by the receiving station, which uses original sender's public key.

There are also situations when the C-ITS station utilises similar cryptographic methods to not only sign, but also maintain fully encrypted communication with other parties.

2.5.1.2 Security Certificates and Public Key Infrastructure

Apart from the algorithmic part, this system of verification assumes that a receiving station has access to the public key of the sending station, and it can trust that the sending station is authorized for taking active part in the C-ITS system. This assumption is fulfilled by Public Key Infrastructure (PKI) – a system of distribution and management of public keys and associated data among C-ITS stations and other system participants. The keys and associated data (permissions for specific C-ITS applications, expiration time limits etc.) are bundled together in a data files called "certificates" that also include information about the origin (issuer) of such certificate.
Vehicle and equipment manufacturers and public agencies also participate in the PKI. Using the above-mentioned methods of asymmetric cryptography on creation and distribution of certificates themselves, PKI can link all its participants into a cryptographical "chain of trust". This chain links an appointed and generally trusted public or governmental agency known as Root Certification Authority (RootCA) with individual C-ITS stations throughout their lifetime.

2.5.1.3 Security credential management system

The actual implementation of a PKI, that defines certificate policies, security policies and credential data exchange protocols, is called a Security Credential Management System.

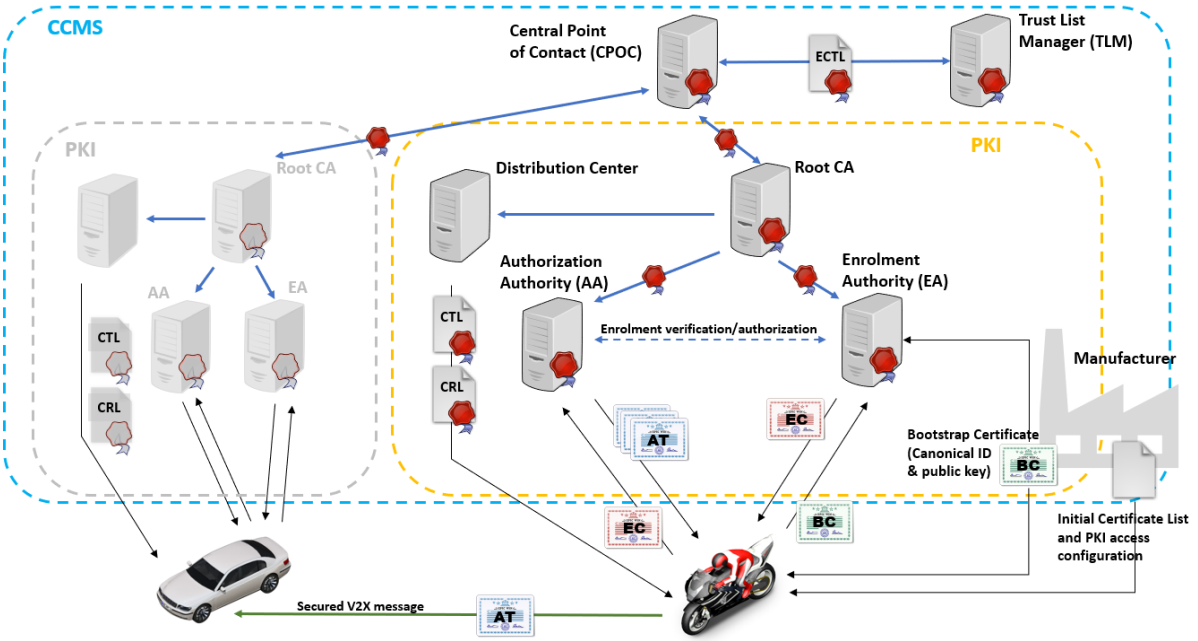
Several individual implementations of such system exist globally, such as EU C-ITS security Credential Management System (EU CCMS) and US SCMS.

2.5.2 C-ITS station role in the security model

A detailed explanation of C-ITS security model is provided in several specification documents listed in the reference section. Following parts will only describe those parts of the model that involves C-ITS stations. Although the security model does not make any distinctions between PTWs and other types of vehicles, there are implementation aspects that are particularly challenging for PTWs. This will be discussed in greater detail in later sections.

2.5.2.1 PKI architecture and credential flows

To fulfil its role in the C-ITS security model, a C-ITS station interacts with various parts of the PKI during its lifetime, applying for and exchanging certificates (security credentials). The general overview of the PKI is depicted in Figure 14.



© This picture was created using the C2C-CC Illustration Toolkit, owned by the CAR 2 CAR Communication Consortium

Figure 14: PKI architecture (Created based on ETSI TS 102 940[5])

RootCA is the top element of the architecture and the origin of the chain of trust. Trust of RootCA is assumed – by the way of its establishment by a governmental authority etc. In implementations such as EU CCMS, there can be multiple RootCA. In such case, there are

[5] **ETSI TS 102 940, V1.3.1 (2018-04)**, accessed on 05.11.2020: https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

additional entities above the RootCA, such as the Trust List Manager and C-ITS Point of Contact (CPOC).

RootCA generates a pair of public and private keys and provides this public key for distribution in the form of a certificate. As RootCA's trust is assumed (this is the only case in the entire PKI), it uses its own private key to sign its own certificate.

RootCA then authorises underlying roles – Enrolment Authorities (EAs), which are used to initialize and enrol new C-ITS stations into the C-ITS system, and Authorisation Authorities (AA), which are used to periodically provide C-ITS stations with certificates used to exchange messages with other C-ITS stations. These authority roles can be performed by various organisations – public or governmental offices, vehicle OEMs or private providers, if they fulfil technical and organisational requirements specified by SCMS policies.

There can be multiple EAs and AAs in the PKI. They are generally called Sub-Certification Authorities (SubCA) in the standard documentation. Their authorisation is done using public key cryptography (simplified description):

- A SubCA generates a private/public key pair.
- The public key is then provided to the RootCA via a certification request.
- RootCA will use this public key from SubCA and create a certificate for the SubCA, that will be signed by the RootCA's private key, then provide this certificate to the SubCA.
- SubCA is then able to distribute this certificate and use its private key to sign certificates provided to C-ITS stations.

C-ITS stations, which have access to the RootCA's certificate, can then verify the Sub CA's certificate to check that it has been certified by the Root CA.

2.5.2.1.1 Trust List and Revocation List distribution

It is assumed that C-ITS station has access to the RootCA's certificate in order to verify any SubCA certificate. In case of PKI with multiple RootCAs, a list of all RootCAs is required. Similarly, there can be situations when a particular SubCA or one of the RootCAs is removed from the PKI.

To provide the information about existing RootCAs and removed RootCAs and SubCAs, a Certificate Trust List (CTL) and Certificate Revocation List (CRL) must be distributed to the C-ITS stations and other entities. The Trust List Manager (TLM) is a high-level single entity in charge of maintaining the trust lists, while CPOC oversees their publication and distribution.

2.5.2.2 C-ITS station related security procedures

There are several procedures that must be performed so that a C-ITS station such as a PTW can be a functional part of the C-ITS security model. The general assumption for these procedures is that the C-ITS station has a communication interface which can be used to connect to the PKI, and is equipped with a device for safe generation, storage and management of cryptographical keys, most commonly implemented as a Hardware Security Module (HSM).

2.5.2.2.1 Initialisation

The Initialisation part is performed in conjunction with the manufacturer of the C-ITS station, that means either during the manufacturing process of the vehicle or during "provisioning" of the C-ITS unit that is to be assembled into the vehicle.

The goal is to establish a set of the initialisation credentials:

- Canonical (unique and immutable) identity of the station
- Canonical public and private key pair
- Generic profile of the stations's properties
- Bootstrap (self-signed) certificate (BC) that links the public key with the generic profile of the station

This procedure is expected to be only done once during the lifetime of the C-ITS station.

Apart from the above-mentioned steps, the manufacturer shall also:

- Register (subscribe) the C-ITS station at selected EA using the C-ITS station's canonical credentials (identity and public key).
- Provide the C-ITS station with the initial set of trusted Root CA, EA and AA certificates.
- Configure the C-ITS station with connection information (network addresses) necessary for communication with EA, AA and associated certificate distribution endpoints.

2.5.2.2.2 Enrolment

This procedure enables a C-ITS station to be able to request and receive authorization credentials for signing C-ITS application messages. It is different from the initialization process as it can be performed multiple times during the lifetime of the vehicle and does not necessarily require direct involvement of the manufacturer. The procedure consists of following steps (simplified):

- C-ITS station creates an enrolment request using the canonical identity established during initialisation. This request also includes description of applications, services and system capabilities that the station will be using, and for which it will be requesting authorisation.
- This request is then signed using the C-ITS station's canonical private key.
- The request message is sent to the EA through an encrypted message based on the public key from EA's certificate.
- The EA verifies the request based on the provided canonical credentials and checks whether the C-ITS station has been previously registered by the manufacturer.
- If the request is verified, the EA will issue an Enrolment Certificate (EC) that includes the C-ITS station's public key and information about its applications, services and system capabilities. This certificate is signed by the EA.
- The EA will send a response message including the EC, using encryption based on the same keys that were used for the request.
- Upon reception, the C-ITS station can verify EA's signature and start using the EC.

2.5.2.2.3 Authorisation

When the C-ITS station is enrolled, it can finally request the AA to issue certificates called Authorisation Tickets (ATs), that can be used for sending C-ITS application messages such as CAM and DENM. This procedure is done periodically many times during the lifetime of the C-ITS station, as ATs have a short expiration period. Moreover, the C-ITS station needs to rotate several ATs during single journey – each time it changes its temporary ID in the C-ITS application, to fulfill the requirements of pseudonymity.
The procedure involves both AA and EA, with the following steps (simplified):

- C-ITS station generates a private and public key pair that is to be used for C-ITS application messages.
- C-ITS station prepares Authorisation Request that specifies the services and applications for which it requires authorisation. It includes the public key generated in the previous step (verification key).
- This request is signed using private key that is corresponding to the public key including in the previously received EC.
- This request is then encrypted using public key provided with the AA certificate.
- This request is then sent to the AA.
- AA decrypts the request using its private key corresponding to the public key from AA certificate C-ITS.
- AA validates the C-ITS station authorisation by forwarding this request to EA.
- EA validates C-ITS station authenticity and authorisation by verifying the request signature using its private key associated with public key that was provided to the C-ITS station inside the EC.
- EA informs AA that C-ITS station is authentic and requested services and applications can be authorised.
- AA issues AT and provides it back to the C-ITS station in an authorisation response message, using encryption based on the same keys that were used for the request.
- C-ITS station is now ready to use the private key corresponding to the verification key to sign C-ITS application messages.

2.5.2.2.4 Secure communication between C-ITS stations

The AT is used to secure the message exchange between C-ITS stations for authorised C-ITS applications. The sending C-ITS station uses the private key associated with the AT to sign a message (e.g. CAM).
Receiving C-ITS stations must be provided with the AT, so they are able to verify the signature. This is done via several mechanisms:

- The sending C-ITS station is periodically attaching an AT to the application message. To preserve bandwidth, this is done with different frequencies depending on the application – e.g. once per second for CAM messages, every time for DENM messages.
- The sending C-ITS station is reactively attaching an AT when a new C-ITS station is detected in the vicinity.
- The receiving C-ITS station can request a particular AT (using information from the received message's signature) from the other C-ITS stations by sending its own messages with special flag in the application message container.

Receiving C-ITS stations can then verify the AT by reconstructing its chain of trust (until the AA and RootCA), and consequently use it to verify signatures on the application messages.

2.5.3 Certificate exchange

The general description of PKI assumes there is some way C-ITS stations can communicate with other PKI entities to exchange certificates or trust lists. In this section, concrete methods of certificate provisioning, as well as its timing, are described. In the following text, the term

PKI endpoint is used as overarching identification of all PKI entities with which a C-ITS station could communicate, that is EA, AA and distribution centre of CTL and CRL.

2.5.3.1 Communication profiles

In general, the amount of data required for provisioning necessary certificates for a C-ITS station is low relative to other types of traffic such as infotainment or even telemetry, typically hundreds of bytes for a single certificate or incremental trust-list update and less than ten kilobytes for a complete European Certificate Trust List (ECTL).

The communication from a C-ITS station to the PKI endpoints is generally assumed to use HTTP/1.1 over TCP/IP connection (IPv6 as a default). As the security of the message exchange is already defined by the C-ITS security model itself, no additional, commonly used lower layer security protocols such as Transport Layer Security (TLS) are required.

One exception to this is the initialisation, that involves initial download of RootCA certificate as well as configuration of the PKI connection points. This shall be done in a secured environment, which is assumed for manufacturers' on-premises procedure, and is likely to involve wired connection to the vehicle, using its diagnostic/configuration interface.

For other procedures, almost any method of connectivity, direct or relayed, that will allow a C-ITS station to reach the PKI entity, shall be sufficient, and it can involve even non-IP paths (as long as these paths are relayed to IP protocol before reaching PKI, or there is a special non-IP implementation of the PKI endpoint).

The specification enlists (non-exhaustively) the following generally assumed methods:

- Cellular Network Link (3G, 4G, 5G)
- WLAN consumer network (public hotspot, home network etc.)
- ITS G5 communication via roadside stations – there are actually two complementary methods:
    - IPv6 over GeoNetworking, which is used for the usual request-response flow for certificate and trust list provisioning.
    - Broadcast of CTL and CRL via dedicated GeoNetworking messages. This method is not applicable for certificate exchange with EA and AA.
- Wired or wireless connection at EV charging stations – protocols not specified.
- Using the Vehicle On-Board Diagnostic (OBD) interface

2.5.3.2 Certificate expiration and renewal

As explained in the introduction, the basic concept of public-key cryptography, on which is the entire C-ITS security model is based, depends on the assumption of computational infeasibility for a third party entity to derive a private key, or produce messages that seems to be signed by a private key of another entity. That means that such computation can be done in theory, but, given the state-of-art equipment, it can take such a long time to perform that it would not be practical for any malicious intent.

There is an inherent risk in this strategy, that depends on the state-of-art technology level. In case of a breakthrough development of computational methods, or discovery of cryptographical weaknesses in currently used methods, the possible cryptographic attack difficulty level could be reduced from infeasible to merely time-consuming. For that reason, the

private-public key pairs cannot be used for infinite time intervals and shall be regularly exchanged. This is implemented in the form of certificate validity and renewal/re-keying procedures.

2.5.3.2.1 Validity and expiration

Every certificate contains an information about its validity start and expiration date, after which it can no longer be verified by the other entities. PKI participants are aware of this information and before the old certificate expires, they perform a certificate renewal procedure similar to the original certificate request, when a new key-pair is generated, and a new certificate is issued. The old (still valid) certificate is used in this procedure to ensure integrity and authenticity of the procedure.

The validity intervals are specified by the certificate policy of the PKI, and generally depends on both cryptographical and organisational aspects. The general rule is that a certificate's validity period must not exceed the validity period of the superior certificate (e.g. EA certificate validity period shall be shorter than RootCA certificate validity period).

2.5.3.2.2 Preloading, private key usage

Certificate policy defines not only the validity period, but also the overlap of validity intervals for consecutive certificates. As certificates can be generated with a validity start in a future date, this is utilised in a process called preloading, that allows PKI to distribute the certificates to all required entities in time before their validity starts. The length of the preloading phase is also specified in the certificate policy of the PKI.

From a cryptographical security point of view, there is a distinction between how long a certificate is valid (i.e. can be used for verification), and how long a private key, associated with the certificate, shall be used (i.e. can be used for signing). This is defined as private key usage period, and this is also specified in the certificate policy.

2.5.3.2.3 Certificate validity periods in EU-CCMS

As a practical example of the certificate validity and associated time periods, the certificate policy of the EU-CCMS is outlined in Table 3.

Table 3 Validity periods of the certificates in the EU C-ITS trust model

Entity	Max. private key usage period	Maximum validity time
Root CA	3 years	8 years
EA	2 years	5 years
AA	4 years	5 years
EC	3 years	3 years
TLM	3 years	4 years

There is a preloading phase specification for RootCA and TLM certificate, that is at least one month and maximum three months before the start of their validity period.

Specific conditions apply to the ATs. As there is no process for revocation of ATs, their validity period must be kept short. At the same time, a mobile C-ITS station needs to use many ATs

during the movement to fulfill the requirements of privacy/pseudonymity, therefore it needs to keep a pool of usable ATs that can be rotated in use while driving. EU CCMS therefore specifies the following policies:

- The preloading period for ATs shall not exceed three months.
- The validity period for ATs shall not exceed one week.
- The pool size of valid ATs for the C-ITS station shall not exceed 100.
- The average usage period per AT shall be at least the operational time of the vehicle during one validity period divided by the maximum number of parallel ATs.

For ECTL and CRLs, certificate policy specifies a maximum period of three months for regular update publications. This update shall be then distributed to the C-ITS stations within one week of the publication.

2.5.4 PTW implementation challenges

The way PTWs differ from other vehicles partaking in the C-ITS system from security point of view is not related to the physical characteristics of the PTW. The difference is largely caused by two factors:

- Most PTWs are not equipped with cellular network connectivity interface.
- The mode of PTW utilisation has long periods of inactivity when the vehicle is stored, and electronics are powered off, such as in the winter time when it is not possible to ride due to snow or other harsh weather conditions.

These two factors complicate the PTW's participation in the PKI, as they limit both the method and frequency of the certificate exchange.

2.5.4.1 Certificate exchange frequency

Assuming specifications of EU CCMS certificate policy, when a PTW is initialised, enrolled, and provided with RootCA, EA and AA certificates, the factors defining the minimum frequency of certificate exchange are:

- Three-month preloading limit for ATs – this factor can be in theory further limited by the amount of ATs that a PTW is able to download from PKI and store in HSM in one session, however current generation of V2X HSMs is fully capable of this amount of private key storage even for a maximum AT pool size.
- One-week distribution limit for ECTL, CRL update – this factor can be further extended if there is a possibility of only updating the trust lists when actual update publication has occurred (which is specified by the policy as minimum once in three months)

Turning these factors into system requirements, we can say that operational PTWs need to connect to PKI at least once in the interval range of one week to three months:

- If a PTW is able to receive ECTL and CRLs via ITS-G5 roadside station during its regular travels, the three months maximum interval applies.
- If a PTW has some alternative notification downlink that can inform it about a new ECTL, CRL update publication, then the interval will be variable, depending on the rate of ECTL and CRL update publications.
- If a PTW has no way to check the status of ECTL and CRLs updates, then the one-week minimum interval applies, as the trust list update must be checked by polling.

If a PTW cannot fulfill the requirement for timely connection to the PKI, the following problems can occur:

- The ATs will expire and PTW will no longer be able to sign the messages it sends (i.e. the messages will not be considered trusted by other C-ITS stations).
- The ECTL will not be updated and PTW will lose its ability to validate (confirm the chain of trust) ATs for received messages signed by other C-ITS stations.

2.5.4.1.1 EC update

Due to its long-term validity, EC renewal does not have an impact on the minimum certificate exchange frequency. It is however a factor in the concept of long-term inactivity of a PTW, such as winter storage etc.

To guarantee a valid EC when the PTW is re-activated after a period of extended inactivity, there are two possible approaches:

a) **EC renewal** – the PTW tries to avoid EC expiration by requesting a new EC using an existing (valid) EC sufficiently in advance (before the period of extended inactivity).
b) **Re-enrolment** – no actions are taken in advance, and if EC expires during the period of extended inactivity, the enrolment procedure, as described in section 2.5.2.2.2, is repeated using canonical credentials.

Regarding technical aspects of interaction with the EA endpoint, there are no significant differences between these two methods. EC renewal is however more in-line with the standard PKI workflows.

To accommodate PTW usage patterns with long-term inactivity periods with the EC renewal scheme, it is preferred to increase the duration *pSecECRemainingLifetimeThreshold* parameter of the C2C-CC Security profile (RS_BSP_456) from 12 weeks to 12 months.

2.5.4.2 Certificate exchange methods

Typically, a PTW can only support a subset of the typical communication methods for certificate exchange, described in 2.5.3.1. We can exclude some of them from the following considerations:

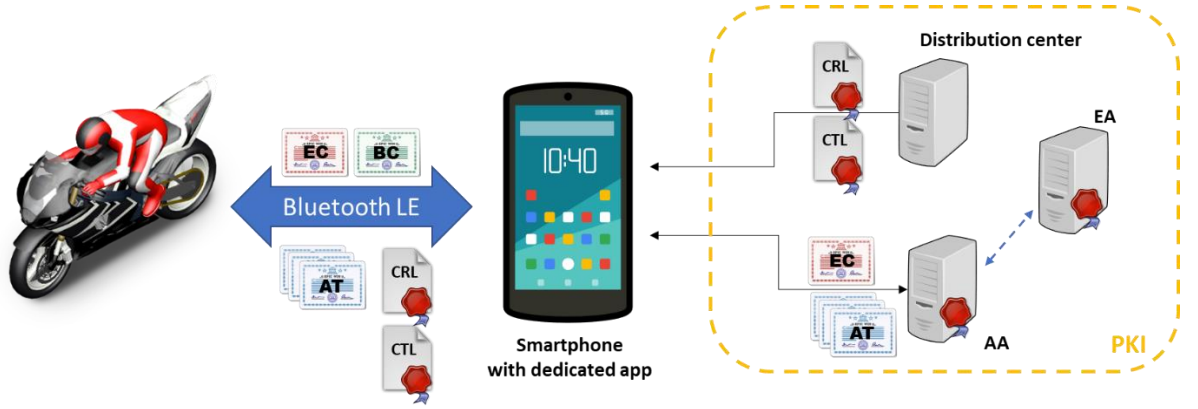
- Cellular data network connections (3G, 4G) – if present, the problem of certificate exchange is fully solved, but most PTWs do not implement these modems.
- Certificate exchange over ITS-G5 – is supported even with basic C-ITS equipment and current C-ITS standards, but is dependent on the availability of supporting Road Side Units.
- Wired or wireless connection at EV charging stations – viable only for electric PTWs, there is no standard yet for certificate exchange protocol over the charging cable.

Other methods are considered in the following sections, sorted by implementation feasibility:

2.5.4.2.1 Bluetooth Low Energy

This method implements communication with PKI endpoints via a smartphone that is serving as a communication proxy. The On-Board Unit (OBU) is communicating with a dedicated smartphone application over Bluetooth Low Energy (BLE) link, the application is then communicating with the PKI endpoint. Due to the message-oriented security scheme of the C-ITS PKI, there is no need for a direct connection/encryption session between the OBU and PKI endpoint.

Checking for CTL/CRL updates can be done by the smartphone application in the background, even when not connected to the OBU.



© This picture was created using the C2C-CC Illustration Toolkit, owned by the CAR 2 CAR Communication Consortium

Figure 15: PKI connection with Bluetooth Low Energy over smartphone proxy (Created based on ETSI TS 102 940)

The connection with the OBU for the actual data exchange is managed via BLE connection establishment schemes and can be happening in the background after initial pairing.

Due to the low complexity of BLE HW, the possibility of re-use of BLE-compatible equipment in the infotainment unit of the PTW and maintaining the internet connection only on the rider's smartphone side, this method is very cost-effective from an implementation point of view. At the same time, it provides a seamless and unobtrusive user experience.

As there is no higher-level certificate exchange protocol standard for the BLE link, and the communication between the BLE module and OBU is dependent on the PTW system architecture, the BLE part including the smartphone application is expected to be vendor specific.

2.5.4.2.2 Bluetooth classic

This implementation is almost identical to the BLE method described in the previous section, with the only difference of using Bluetooth classic (BT) for the OBU-to-smartphone link.

As there are no BT profiles designed specifically for the certificate exchange, a custom protocol implemented over serial port profile (SPP) is assumed. Generally, there are more challenges regarding SPP interoperability across popular smartphones compared to BLE, it can be therefore expected that this method would require a bigger effort in terms of achieving a good user experience.

On the other side, this method could achieve better HW reuse, if the PTW already implements BT (e.g. in the infotainment unit) but does not implement BLE.

2.5.4.2.3 WLAN

This method is viable if the PTW is equipped with WLAN client device. It expects that the PTW would automatically connect to the PKI endpoints over WLAN when in range of a connectable Access Point (AP) such as home router, smartphone tethering hot spot etc.
Following problems can be expected with this approach:

- Availability of Wi-Fi client equipment in the PTW
- Radio certification challenges (equivalent to automotive external WLAN)
- User experience issues related to WLAN authentication procedures

2.5.4.2.4 IoT cellular network technologies

Due to low amount of data necessary to be transported during a certificate update procedure, most of the machine-to-machine (M2M) communication technologies such as NB-IoT and LTE-M would be sufficient as PKI connectivity method. Narrow-band M2M technologies, such as SigFox or LoRaWan are however expected to be too throughput-restrictive for a feasible implementation.

Functionally, using IoT cellular modem for PKI connection is almost equivalent to regular LTE connectivity – the update procedure would be managed by the OBU with no interaction required from the rider. The only difference from normal LTE modem would be possible connection problems when the PTW is moving, as the IoT technologies are mostly optimised for stationary clients.

As with any cellular technology, a service subscription and related costs would have to be managed either by the PTW vendor or the rider. At the current state of implementation of these technologies at cellular providers, there are also problems with roaming.

2.5.4.2.5 eCall unit

This method assumes an eCall unit present in the PTW. Due to the low amounts of data necessary for certificate update, the in-band modem of the eCall unit could be used to communicate with the PKI. For next generation eCall standard using LTE services, the situation is functionally equivalent to having telematics cellular connectivity.

2.5.4.2.6 Vehicle On-Board Diagnostic (OBD) interface

This method assumes existence of a custom proxy device (dongle) with PKI access, that can be manually plugged into the diagnostic interface of the PTW. Due to lack of existing standards in both PTW OBD diagnostic interfaces and CAN based protocol for certificate update, it is expected this method would have to be vendor specific or require further standardisation activity.

From a user experience point of view, it would require periodic manual maintenance procedures and the necessity to have the dongle device available during longer trips.

2.5.5 PTW manufacturers' responsibilities within C-ITS security model

The C-ITS security model generally assumes that the PTW manufacturer (OEM) is, at least initially, responsible for choosing and providing the PKI access for the PTW. In the related C-ITS policy standards, the role that the OEM has to assume is described as "C-ITS station subscriber".

This can be done by hosting its own PKI by installing and managing individual PKI services as software components and fulfilling the necessary security and certificate policies and procedures defined by the CCMS/SCMS standards.

Another option is using the services of a PKI provider (Software-as-a-service), that would provide the entire PKI architecture, either installed on an OEM's premises or in the cloud. The provider is usually also responsible in fulfilling the security and certificate policy requirements.

Even when the services of a PKI provider are used, there are procedural, technical and administrative requirements that require direct involvement of the OEM. Administrative and procedural requirements include providing proof of organisational identity and authenticity for the CCMS/SCMS authorities, as well as compliance assessment procedures regarding the PTW/OBU HW and manufacturing procedures involving initialisation and enrolment of this HW. The compliance assessment procedures will, in the final CCMS implementation, probably involve a third-party audit.

2.5.5.1 Responsibilities during PTW manufacturing

The technical requirements are explained in sections 2.5.2.2.1 and 2.5.2.2.2 and their fulfillment would likely involve the OEM as well as the OBU supplier and PKI provider. It can be expected that some parts, such as the generation of canonical credentials, would be implemented on OBU side, while the data exchange including assignment of canonical ID would require additional processing on OEMs manufacturing line. Finally, the registration of new PTW/OBU to the PKI would require OEMs equipment to communicate with the EA endpoint supplied by the PKI provider.

2.5.6 References

There is no singular source comprehensively describing the C-ITS security model. The following standards were used as a reference for this chapter, sorted by relevance from this chapter's point of view:

- ETSI TS 102 941 v1.3.1 (2019-02) – the actual technical specification of the security management, including description of the certification/authorization message flows within PKI/EU CCMS.
- ETSI TS 102 940 v1.3.1 (2018-04) – technical specification describing security requirements for C-ITS system and applications, as well as high-level definition of C-ITS SCMS.
- Annex 3 to the Commission Delegated Regulation Supplementing Directive 2010/40/EU – describes organisational and policy implementation of the EU CCMS. It is a compilation of two previously issued documents:
    - Certificate Policy for Deployment and Operation of EU C-ITS Release 1.1 (June 2018)
    - Security Policy & Governance Framework for Deployment and Operation of EU C-ITS Release 1 (December 2017)
- C2C-CC Basic System Profile Release 1.5.0 (27.3.2020) – section 6.1 Security
- C2C-CC Protection Profile V2X Hardware Security Module Release 1.5.0 (27.3.2020)
- ETSI TS 103 097 v1.3.1 (2017-10) – technical specification of the message formats used for exchange of the certificates within PKI.
- IEEE 1609.2 (2016 and its later revisions) – technical specification of the underlying security protocols and certificate formats on which ETSI specifications are partially build upon.

2.6 Lifecycle Management

C-ITS system and applications need to be activated before PTW is purchased and used by riders, deactivated after it was discarded. Any issues related to C-ITS need to be detected automatically and informed to its rider. Then, the issue needs to be solved by software update.

2.6.1 Activation / Deactivation

C-ITS system and application need to have a capability of activating and deactivating either locally or remotely. Deactivation will give riders a choice of not using C-ITS functionalities, especially when rider recognizes that the notification is annoying, while activation will give manufacturer to define the activation timing e.g. radio transmission from C-ITS antenna may not be allowed in some area.

2.6.2 Diagnosis

Any malfunctions of C-ITS system and applications need to be detected automatically and notified to riders so that they recognize the issues and take corrective action. Therefore, C-ITS system should have self-diagnosis functionality. Furthermore, it should be also possible that the status can be manually checked by e.g. OBD.

2.6.3 Software Update

C-ITS system and applications need to be updated on a regular basis, not only for riders to enjoy the latest functionalities but also to protect them from any issues caused by using old software. Especially, vulnerabilities or malfunctions of the software may cause critical accidents if it is not updated for a long time.
Therefore, it is recommended that each manufacturer to prepare the functionality or process of updating C-ITS software of PTW which is already on the market.

Abbreviations

AA	Authorization Authority
AC	Authorization Certificate
ACEM	European Association of Motorcycle Manufacturers
AP	Access Point (Wi-Fi)
AT	Authorization Ticket (certificate)
AWW	Adverse Weather Warning
B2C	Business to Consumer
BC	Bootstrap Certificate
BLE	Bluetooth Low Energy
BT	Bluetooth (classic)
C2C-CC	CAR 2 CAR Communication Consortium
CA	Certification Authority
CAM	Cooperative Awareness Message
CAN	Controller Area Network
CCMS (EU)	C-ITS security Credential Management System
CMC	Connected Motorcycle Consortium
C-ITS	Cooperative Intelligent Transport System
CPOC	Central Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
DENM	Decentralized Environmental Notification Message
DEoQ	Dangerous End of Queue
DR	Dead Reckoning
EA	Enrolment Authority
EC	Enrolment Certificate
ECTL	European Certificate Trust List
EEBL	Electronic Emergency Brake Light
EViO	Emergency Vehicle in Operation
ETSI	European Telecommunications Standards Institute
HMI	Human Machine Interface
ITS-S	ITS-Station
GNSS	Global Navigation Satellite System
ICRW	Intersection Collision Risk Warning
ITS	Intelligent Transport System
IMU	Inertial Measurement Unit
LCRW	Longitudinal Collision Risk Warning
LDM	Local Dynamic Map
LOS	Line Of Sight
M2M	Machine-to-Machine
NTP	Network Time Protocol
OBD	On-board diagnostics
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
PTW	Powered Two Wheeler
SCMS	Security Credential Management System

SRSW	Stationary Recovery Service Warning
SSEV	Stationary Safeguarding Emergency Vehicle
SPAT	Signal Phase and Timing
SPP	Serial Port Profile (Bluetooth)
SVW	Stationary Vehicle Warning
TAI	International Atomic Time
TJA	Traffic Jam Ahead
TJW	Traffic Jam Warning
TLM	Trust List Manager
UTC	Coordinated Universal Time
V2X	Vehicle-to-Everything
WLAN	Wireless Local Area Network