ENSEMBLE

EUROPEAN COMMISSION

HORIZON 2020
H2020-ART-2016-2017/H2020-ART-2017-Two-Stages
GA No. 769115

ENSEMBLE

ENabling **S**af**E** **M**ulti-**B**rand p**L**atooning for **E**urope

Deliverable No.	D2.9	
Deliverable Title	Security framework of platooning	
Dissemination level	Public	
Written By	Boris Atanassow, VOLVO Per Sandström, VOLVO Dennis Millard, Scania Roman Alieiev, MAN Soheil Gherekhloo, BOSCH Ralph Prenzel, BOSCH	29-05-2019

	William Whyte, Qualcomm Joost van Doorn, NXP Sergi Guarnich, Idiada Alejandro Manilla, Idiada	
Checked by	Marika Hoedemaeker, TNO Lina Konstantinopoulou, CLEPA	11-06-2019 29-05-2019
Status	Final, approved by EC	13-05-2020

Please refer to this document as:

Boris Atanassow, (2019). *Security framework for platooning.* D2.9 of H2020 project ENSEMBLE, (www.platooningensemble.eu)

Disclaimer:

ENSEMBLE is co-funded by the European Commission, DG Research and Innovation, in the HORIZON 2020 Programme. The contents of this publication is the sole responsibility of the project partners involved in the present activity and do not necessarily represent the view of the European Commission and its services nor of any of the other consortium partners.

Revision history

Version	Date	Author	Summary of changes	Status
0.1	02-06-2019	Boris Atanassow (Volvo AB)	Document prepared	Prepared
0.2	05-13-2019	Boris Atanassow (Volvo AB)	Updated PKI and security profiles	Draft
0.3	05-17-2019	Boris Atanassow et al. (Volvo)	Updated with contributions from Scania and Idiada	Draft
0.4	05-20-2019	Boris Atanassow (Volvo)	Refined Chapter 2, 3 and 4	Draft
0.5	05-22-2019	Ralf Prenzel et al. (Bosch)	Updated Chapter 3 and 4	Draft
0.6	05-23-2019	Ralf Prenzel (Bosch)	Update due to comments	Draft
0.7	05-24-2019	Boris Atanassow et al. (Volvo)	Updates due to comments	Draft
0.8	05-29-2019	Boris Atanassow et al. (Volvo)	Updates from WP leader	Draft
0.9	06-11-2019	Boris Atanassow (Volvo)	Updated list of contributors	Final
1.0	02-04-2020	David Hitchman (Scania)	Fixes from rejection letter	Draft
1.1	25-05-2020	Marika Hoedemaeker (TNO)	Cross reference error deleted	final

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Context

Platooning technology has made significant advances in the last decade, but to achieve the next step towards deployment of truck platooning, an integral multi-brand approach is required. Aiming for Europe-wide deployment of platooning, 'multi-brand' solutions are paramount. It is the ambition of ENSEMBLE to realise pre-standards for interoperability between trucks, platoons and logistics solution providers, to speed up actual market pick-up of (sub) system development and implementation and to enable harmonisation of legal frameworks in the member states.

Project scope

The main goal of the ENSEMBLE project is to pave the way for the adoption of multi-brand truck platooning in Europe to improve fuel economy, traffic safety and throughput. This will be demonstrated by driving up to seven differently branded trucks in one (or more) platoon(s) under real world traffic conditions across national borders. During the years, the project goals are:

- Year 1: setting the specifications and developing a reference design with acceptance criteria
- Year 2: implementing this reference design on the OEM own trucks as well as perform impact assessments with several criteria
- Year 3: focus on testing the multi-brand platoons on test tracks and international public roads

The technical results will be evaluated against the initial requirements. Also, the impact on fuel consumption, drivers and other road users will be established. In the end, all activities within the project aim to accelerate the deployment of multi-brand truck platooning in Europe.

Abstract of this Deliverable

This deliverable provides a specification of the V2X security framework. It describes which measure should be applied to ensure trucks can communicate with each other in a secure and private way.

In ENSEMBLE, a new facilities layer protocol supporting the platooning application is developed. This makes use of already standardized lower layer protocols in ETSI TC ITS. The platooning protocol uses already available message types and signals, and where necessary new ones are introduced. The protocol logic for joining, platooning, and leaving has been derived from the use cases in deliverable D2.2 of ENSEMBLE. The available security framework for cooperative intelligent transport system (C-ITS) in Europe is used for signing and verifying messages to establish a trust domain. This deliverable develops and extends the already available security concept with the encryption of platoon application data using symmetric keys.

This is the first agreed version as an input and starting point for the development and testing of the platooning functionality within ENSEMBLE. Based on findings and learnings from those activities the specification will be updated accordingly.

By the time the document was finalized there exists an open issue of a clear description of a communication behaviour being missing, that could not be addressed in the development of that specification.

1. INTRODUCTION

Cooperative Intelligent Transport Systems (C-ITS) refers to applications using wireless communication between vehicles, vehicle-to-vehicle communication (V2V), and between vehicles and smart road infrastructure, vehicle-to-smart road infrastructure communication (V2I), for increasing road traffic safety and efficiency. V2V and V2I communications are collectively known as V2X communication. Present document specifies a facilities layer protocol for supporting truck platooning using the wireless technology ITS-G5 (a.k.a. IEEE 802.11p [2]/WLANp) at 5.9 GHz band.

Direct communication between vehicles and between vehicles and smart infrastructure has the potential to save lives and reduce the environmental impact. Recently the EC has adopted the "Delegated Act" for deployment of C-ITS to create a minimal set of requirements for interoperability and to enable large scale deployment [8] in Europe. Frequency bands for V2X were allocated in 2008 in Europe and already in 1999 in the US at a carrier frequency of 5.9 GHz. In Europe, standardization has been carried out in the EC acknowledged standards development organization (SDO) ETSI[1] and its Technical Committee on Intelligent Transport Systems (TC ITS). Pre-standardization and deployment issues are treated in CAR 2 CAR Communication Consortium[2] (C2C-CC), a non-profit organization collecting OEMs, suppliers, universities and research institutes. More information about ETSI's protocols and deployment plans are found in [1,2], respectively. It should be noted that the wireless technology IEEE 802.11p is also called ITS-G5 and WLANp in Europe. Standards are necessary to create an interoperable system between different brands.

SAE[3] and IEEE[4] have created an interoperable V2X system in the US. SAE has focused on message sets for V2X and IEEE has developed all lower layer protocols. Crash Avoidance Metric Partnership (CAMP) has collected OEMs and CAMP has run several public funded research projects and conducted pre-standardization tasks. The wireless technology (IEEE 802.11p) is used both in Europe and in the US. An overview of the protocol stack in the US is found in [1].

Focus on standardization has been to increase the awareness horizon for the driver by alerting the driver about impending dangerous situations and then the driver needs to take appropriate action (no automated control of the vehicle based on received V2X data). A number of so-called day-one applications (or services) have been defined such as stationary vehicle warning, slow vehicle

[1] European Telecommunications Standards Institute, see http://www.etsi.org/
[2] CAR 2 CAR Communication Consortium, https://www.car-2-car.org/
[3] Society of Automotive Engineers, see http://www.sae.org/
[4] Institute of Electrical and Electronics Engineers, see https://www.ieee.org/

warning, emergency electronic brake light etc., by C2C-CC and further elaborated in the Commission work “C-ITS deployment platform” [7]. These day-one services are using two distinct facilities layer protocols developed by ETSI TC ITS called Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Message (DENM), where the former are always present triggered by vehicle dynamics containing information about the vehicle such as type, speed, position and heading. DENMs are only triggered on behalf of a dangerous situation and contains information about the dangerous event itself. The V2X communication is closing the gap between line-of-sight (LOS) sensors such as camera, lidar and radar, and the long-range cellular technology, by providing the possibility to see beyond physical barriers within milliseconds.

In platooning and cooperative adaptive cruise control (C-ACC) V2X data is seen as one sensor input together with other sensor data such as radar and camera for controlling the vehicle laterally and longitudinally automatically. Platooning and C-ACC are regarded as safety applications as well as efficiency applications. C-ACC can mitigate shockwaves through traffic and thereby, avoid rear-end collisions but at the same time increase the number of vehicles on the roads without increasing congestion.

Platooning can make today’s spontaneous platooning safer (trucks are already today driving too close without help from technology, violating regulation and safety) and support the driver in the monotonous task of driving in a highway environment by alerting the driver about impending hazardous events. The first truck in a platoon sees further ahead using conventional line-of-sight (LOS) technologies (radar and camera), and when the first truck detects any anomalies it will inform the other trucks in the platoon facilitating orchestrated braking for example. Regardless of distances between the trucks, a truck using only conventional radar cannot see beyond physical barriers, by adding the V2X component the driving of trucks will be made safer since the first truck can inform other trucks behind it about dangerous situations. And of course, from a fuel economy perspective less jerky driving and reduced air drag due to decreased distances between the trucks will reduce the environmental impact due to fuel consumption reduction.

1.1. Purpose

The purpose of this deliverable is to define the security framework for the platooning function. The framework is created to ensure the integrity and confidentiality of the participants in a pan-European multi-brand platooning system.

1.2. Scope

This deliverable describes the security measure that shall be applied to the newly developed platooning protocol logic, message sets and data formats, for enabling platooning on public roads using IEEE 802.11p/ITS-G5 communication on a carrier frequency of 5.9 GHz (this deliverable does not address cellular communication for accessing a back-office system).

1.3. Outline

Chapter 2 provides the background and the reasons why a security framework is needed for platooning. Further, in Chapter 3, an overview of current security solutions in the domain of C-ITS is provided. The ENSEMBLE platooning security framework is detailed in Chapter 4 and a summary is outlined in Chapter 5. References are provided in Chapter 6.

2. BACKGROUND

2.1. V2X Communication security

The European V2X standards, ITS-G5, require cyber security in terms of authorization for all transmitted messages. The reasoning behind this is that since the information received via the ITSG5 interface can be safety related and may in a direct or an indirect way affect the behaviour of the vehicle, the information must be reliable.

For most common applications, there is no method used to ensure confidentiality in the day-1 applications. The reasoning behind this is that all ITS-S (ITS-Station), that are close enough, should be able to receive and understand the broadcast message.

2.2. Platooning

In addition to the general security requirements on the ITS-G5 interface, most of the platooning messages will also be confidential. The confidentiality is added for three reasons,

1. No vehicle should be able to follow behind a platoon of vehicles and use the platoon specific messages to platoon without being a part of the platoon. This should not be allowed since the following vehicle might be a vehicle that has not paid (if that is required) for the platoon application and it might not fulfil the platooning requirements (for instance requirements on the sensors or driver) which could be a safety risk.

2. Since the platooning specific messages include more information than the ordinary CAM, confidentiality is required to ensure privacy and to be able to avoid traceability of the vehicles within the platoon. Data that is only included in platooning messages are vehicle weight, vehicle length and a vehicle ID. This information together with what is already available in the CAM messages makes it easier to trace the vehicle.

3. Information about the behaviour of the vehicle systems – e.g. braking performance – may be proprietary and the vehicle manufacturer or fleet owner may wish only to share it with other parties that have an absolute need to know.

3. V2X STANDARDIZED SECURITY

This chapter explains which security measures have been developed and standardized in ETSI and IEEE so far. Based on the following concept the platooning security framework is developed and explained in Chapter 4 and shall be based on available standards. The platooning application should be compatible with other C-ITS applications.

3.1. Security in the V2X stack

The V2X protocols that have been developed allow for the communication between different brands supporting the day-one applications. These protocols are divided in different layers (explained in Figure 1) with certain responsibilities to break down the complexity of communication. Deliverable 2.8 [9] already defines and locates the platooning protocol as a facility layer application as depicted in . In addition to the cleanly structured layer approach the security block in the V2X communication stack could be rather understood as a cross layer that provides security related functionality to more than one layer.

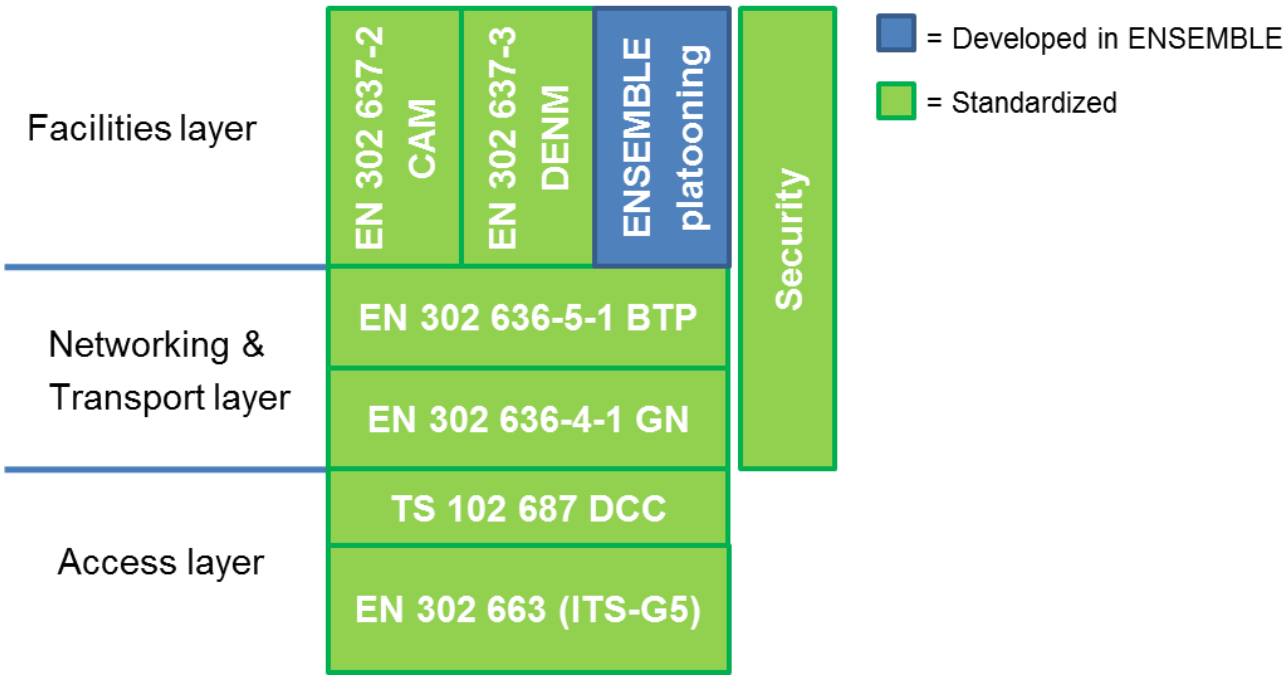

Figure 1, security in the V2X communication stack

The concept for platooning security is treated and elaborated in Chapter 4 and might be subject to changes. The current available security approach is enabled for the use of a public key infrastructure (PKI) developed for C-ITS. There messages are signed and verified using a temporarily authorization ticket. Signature and signature verification are applied for all kinds of messages in the V2X communication, e.g. CAM and DENM. No day-one application is using

encryption yet, but encryption is used in ETSI specifications, for communication with the certificate authorities.

3.2. The V2X security header

Each V2X packet consists of different headers that fulfill different purposes. ETSI EN 103 097 [6] defines the security headers in the V2X communication stack. The secured part of the packet spans over the common and extended header also including the payload as shown in Figure 2, V2X secured packet.

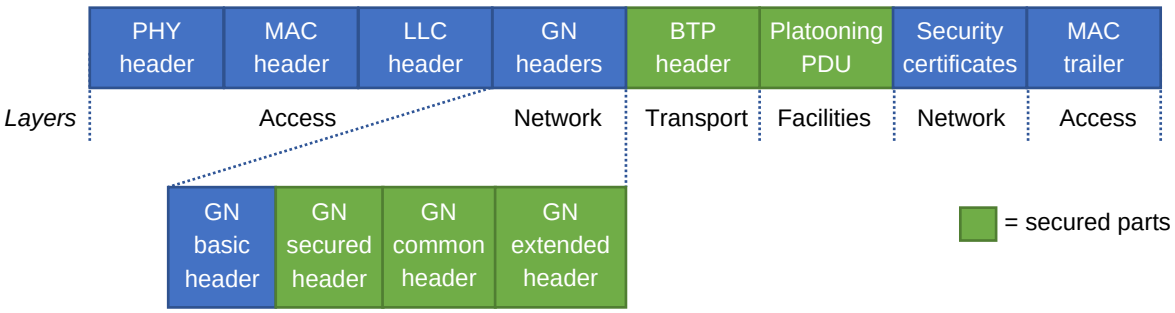

Figure 2, V2X secured packet

Note that although the ETSI specifications provide for 103 097 security services to be applied at the network layer, this does not require that security is applied there:

- The Geonetworking protocol allows the sending application to request “null” security services at the Geonetworking layer. If this is the case, the receiving application is notified by the receiving Geonetworking layer that no security was applied at that layer.
- The ETSI security services can be applied at any layer – and in fact a project is currently ongoing to specify facility layer security services for communications using the “Uu” cellular link.

The design in this proposal makes use of this feature of the ETSI architecture, applying authentication services (signing) at the geonetworking layer but encryption services (confidentiality) at the application layer.

3.3. V2X Public key infrastructure

The Public Key Infrastructure for European C-ITS is defined in ETSI TS 102 940 v1.3.1. It consists in general of four entities (TLM, RCA, EA, AA) as depicted in Figure 3, Public Key Infrastructure.

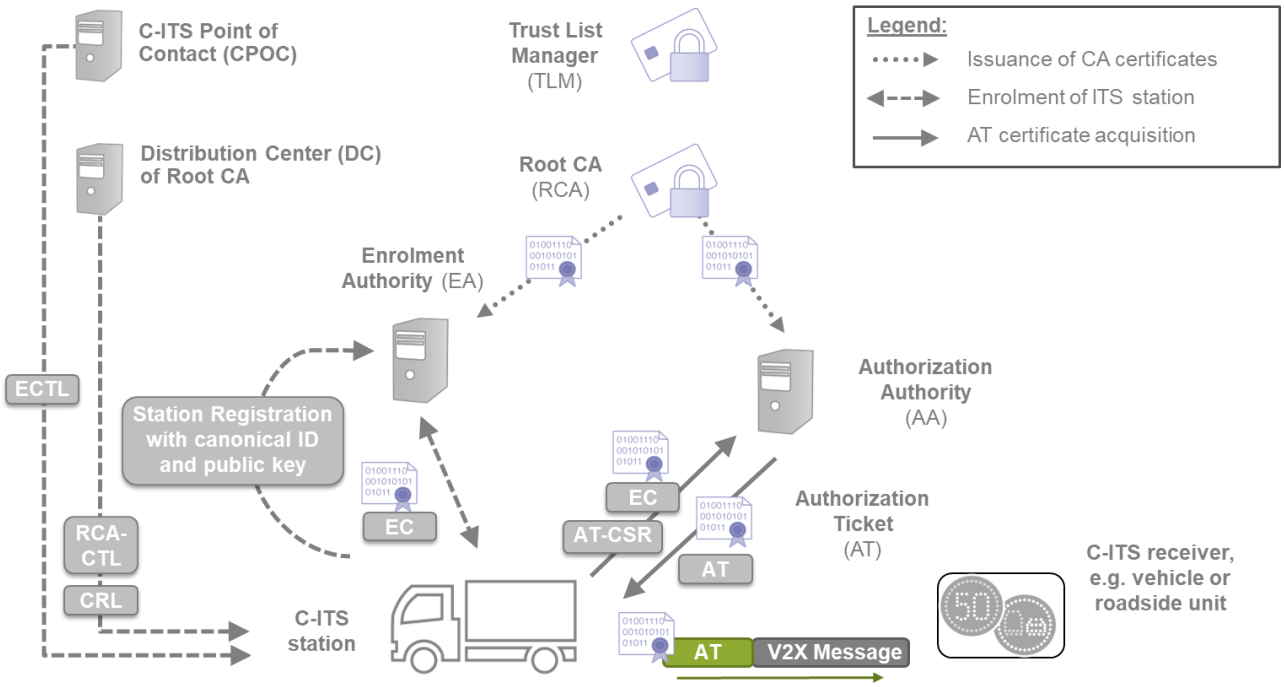

Figure 3, Public Key Infrastructure

The purpose of the Trust List Manager (TLM) is to put trusted RCA certificates on a European Certificate Trust List (ECTL) and to sign this list with the TLM current valid private key. The ECTL is downloaded by C-ITS stations from the C-ITS Point of Contact (CPOC) to verify messages from other stations which are assigned to another root.

The Root CA (RCA) is responsible for issuing two types of sub CAs: the Enrolment Authority (EA) and the Authorization Authority (AA). The RCA signs a Certificate Revocation List (CRL) in order to allow the revocation of issued sub CAs. ESCRYPT operates the RCA as a managed service.

The EA is used to register new C-ITS stations where the registration API is not standardized by ETSI or considered in the European Delegated Act for C-ITS. Registered C-ITS stations can request Enrolment Credential (EC) certificates from the EA and the AA can request the authorization and validation of C-ITS Authorization Ticket (AT) certificate requests.

The PKI, and the underlying design in IEEE 1609.2 [5] / ETSI TS 103 097 [6], supports issuing certificates with permissions for specific applications, which are identified by an ITS Application Identifier (ITS-AID). The platooning application will be associated with a different ITS-AID from the ones associated with CAM and DENM. A certificate can contain more than one ITS-AID, so it is possible for a device that has authorizations for multiple applications to have either one set of certificates with all the ITS-AIDs, or more than one set of certificates where different sets of certificates contain distinct ITS-AIDs or sets of ITS-AIDs.

3.4. Pseudonym change

As stated in the European Delegated Act for C-ITS the impact on the privacy of road users should be minimised. Accordingly, the C-ITS platform has developed a security architecture supported by a public key infrastructure (PKI) using frequently changing pseudonym certificates.

According to the C-ITS Security Policy release 1 (C-ITS SP), the Personally Identifying Information (PII) contained in messages of mobile C-ITS stations shall be secured using an adequate AT change procedure to ensure a level of security adequate to the risk of re-identification of drivers based on their broadcasted data. Therefore ITS-Stations shall change ATs adequately when sending messages and shall not re-use ATs after a change.

A pre-standardization study on pseudonym change management is given in ETSI TR 103 415 V1.1.1.

According to the European Delegated Act for C-ITS all addresses and identifiers transmitted through short-range communication shall be changed when the AT certificate is changed.

3.5. Signing and encryption

All messages sent by fixed and mobile C-ITS stations shall be signed according to TS 103 097 v1.3.1 as detailed in the C-ITS SP and the European Delegated Act for C-ITS. The vehicle C-ITS station shall use one end-to-end security header on geonetworking layer and a signature per message in accordance with ETSI TS 103 097 v1.3.1 and EN 302 636-4-1 v1.3.1. The integrity of all messages used by ITS applications shall be validated by the receiver according to TS 103 097.

3.6. Application ID

Each ITS application is globally identified by an ITS-AID and these are outlined in ETSI TS 102 965 V1.4.1 [3]. ISO 17419 regulates allocation of new ITS-AID globally. When starting the ENSEMBLE project no ITS-AID number has been defined for platooning. To request the assignment of a new ITS-AID during the project we shall use the template available at [4]. Until a new Application ID is assigned for platooning, a testing/private ITS-AID shall be used.

4. ENSEMBLE PLATOONING SECURITY

In the current Chapter the ENSEMBLE security framework is described. First the agreed terminology within the ENSEMBLE project for certain items is explained. After this short introduction the security profiles are developed and added security profiles are lined out. It is as well explained how signage and encryption is used on certain message types. Since the ENSEMBLE security approach is a V2X application that is using encryption it is pointed out how and when keys are distributed and updated within an active platoon.

4.1. Terminology

The security framework is depicted in this chapter and it requires the use of security terminology to avoid possible misunderstandings in the interpretation of the described ENSEMBLE protocols. In Table 1, Terminology these are outlined.

Terminology	Description
JoinRequest	PMM, that is sent by a truck willing to join another joinable single truck or an already existing platoon (from behind).
JoinResponse	PMM, which is sent as an answer to the JoinRequest by the last truck in the platoon to the joining truck. It informs about if joining truck is allowed to join and credentials needed to participate in group communication.
LeaveRequest	PMM, which is sent by a truck that has received a trigger to leave the platoon.
KeyUpdateRequest	PMM, which is sent by a following truck to the truck in front, which has received a trigger to request an updated group key.
KeyUpdate	PMM, to provide the trailing truck with the update group key.
GroupKey	A Key distributed to all platoon members to enable platoon wide privacy. Used by both PCMs and PMMs.
ParticipantKey	A key to encrypt the private communication between two trucks following one after the other.
AsymmetricKey	A key to encrypt PMMs (JoinResponse) to provide joining trucks with platoon relevant information, e.g. with the GroupKey, position in

	the platoon, PlatoonID, etc.
Platooning-distance	Distance between the ego and preceding vehicle when a truck is platooning, after having joined and closed the gap.
Standalone-distance	Distance between ego and preceding vehicle where the ego vehicle can drive by itself with all inputs from its sensors.

Table 1, Terminology

This terminology should be used to avoid having different terms for the same description or vice versa.

4.2. Concept of signing and encryption

As described in Chapter 3, truck platooning is based on trust. By following the C-ITS certificate policy trust can be estabilished between trucks from different manufacturers. This is done to ensure integrity on all platooning related messages and confidentiality when required.

4.2.1. Signing of messages

Signage is initiated by the geonetworking layer and a security profile for platooning which is defined Chapter 4.3 and is compatible with the ETIS TS 103 097 1.3.1 standard.

4.2.2. Encryption of messages

Encryption is initiated by the Application layer. Some of the necessary interfaces to do so are already defined, either in the ETSI security interface standards (which provide a high level interface to the security services) or in IEEE 1609.2 [5], which provides a low-level interface to those standards. However, this specification proposes some additional mechanisms, such as regularly applying a known Key Derivation Function (KDF) to an existing symmetric key to enhance unlinkability. These mechanisms do not currently have a specified interface and this will be developed as part of this project.

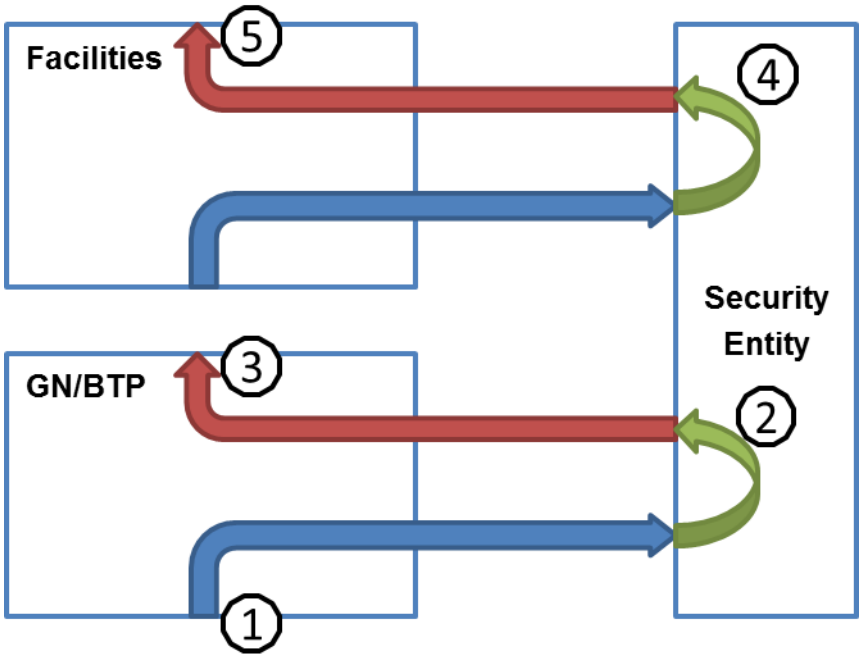

Figure 4, Platooning message flow in V2X communication stack

In Figure 4, Platooning message flow in V2X communication stack the flow of a received packet on MAC layer up to the application layer is depicted. In step (1) a signed packet is received in Geonetworking layer, and passed on to the security entity. In the secure element the attached signature is verified in step (2) and a result is sent back to the GN/BTP layer. If the result is OK, it is verified that the packet was sent by another truck that is trusted since it attached a valid certificate allowing it to platoon. In step (3) the packet is passed up to the facilities layer using the platooning BTP port. The platooning facility passes the received packet forward to the security entitiy again where the payload is decrypted.

4.3. Security profiles

This Chapter is to be seen as an extension to ETSI TS 103 097 V1.3.1 [6] chapter 7.1.

4.3.1. Platooning

The secure data structure containing a Platooning Message shall be of type `EtsiTs103097Data-Signed` as defined in ETSI TS 103 097 V1.3.1 [6] Clause 5.1 and [6] Annex A, containing the Join Platoon Request Message as the `ToBeSignedDataContent`, with the additional constraints defined in [6] Clause 5.2 and this clause:

- The component signer of `SignedData` shall be constrained as follows:

- `SignerIdentifier` shall be of choice certificate

- The component `tbsdata.headerInfo` of `SignedData` shall be further constrained as follows:
  - psid: this component shall encode the ITS-AID value for platooning.
- All other components of the component `tbsdata.headerInfo` allowed to be present according to [6] Clause 5 shall not be used and be absent.

4.3.2. Platooning Encryption Profiles

Join Request

The secure data structure containing Join Request Message shall be of type `PlatooningData-Unencrypted` as defined in Clause Platooning ASN.1 encryption module, containing the Join Request Message as the `unsecuredData`.

Key Update Request

The secure data structure containing Key Update Request Message shall be of type `PlatooningData-SymmetricKeyEncrypted` as defined in Clause Platooning ASN.1 encryption module, containing the Key Update Request Message as the `ccmCiphertext`, with the additional constraints:

- The component recipients of `EncryptedData` shall be of type `SequenceOfRecipientInfo` as defined in IEEE Std 1609.2 [1] clause 6.3.31 and further constrained as follows:
  - The SequenceOfRecipientInfo shall only contain one entry
    - The recipientId shall contain the digest of the PGK.

Join Response

The secure data structure containing Join Response Message shall be of type `PlatooningData-PublicKeyEncrypted` as defined in Clause Platooning ASN.1 encryption module, containing the Join Response Message as the `ccmCiphertext`, with the additional constraints:

- The component recipients of `EncryptedData` shall be of type `SequenceOfRecipientInfo` as defined in IEEE Std 1609.2 [1] clause 6.3.31 and further constrained as follows:
  - The SequenceOfRecipientInfo shall only contain one entry
    - The recipientId shall contain the digest of the PGK.

Key Response

The secure data structure containing Key Response Message shall be of type `PlatooningData-SymmetricKeyEncrypted` as defined in Clause Platooning ASN.1 encryption module, containing the Key Response Message as the `ccmCiphertext`, with the additional constraints:

- The component recipients of `EncryptedData` shall be of type `SequenceOfRecipientInfo` and further constrained as follows:
  - `SequenceOfRecipientInfo` shall only contain one entry
    - The `recipientId` shall contains the digest of the receivers PPK

Leave Platoon

The secure data structure containing Leave Platoon Message shall be of type `PlatooningData-SymmetricKeyEncrypted` as defined in Clause Platooning ASN.1 encryption module, containing the Leave Platoon Message as the `ccmCiphertext`, with the additional constraints:

- The component recipients of `EncryptedData` shall be of type `SequenceOfRecipientInfo` and further constrained as follows:
  - The `SequenceOfRecipientInfo` shall only contain one entry
    - The `recipientId` shall contains the digest of the PGK

Platoon Control

The secure data structure containing Platoon Control Message shall be of type `PlatooningData-SymmetricKeyEncrypted` as defined in Clause Platooning ASN.1 encryption module, containing the Platoon Control Message as the `ccmCiphertext`, with the additional constraints:

- The component recipients of `EncryptedData` shall be of type `SequenceOfRecipientInfo` and further constrained as follows:
  - The `SequenceOfRecipientInfo` shall only contain one entry
    - The `recipientId` shall contains the digest of the PGK

Platooning ASN.1 encryption module

```
PlatooningModule
{ itu-t(0) identified-organization(4) etsi(0) itsDomain(5) wg5(5) v1(0) }
DEFINITIONS AUTOMATIC TAGS ::= BEGIN
IMPORTS
Ieee1609Dot2Data
FROM
IEEE1609dot2 {iso(1) identified-organization(3) ieee(111)
standards-association-numbered-series-standards(2) wave-stds(1609)
dot2(2) base (1) schema (1) major-version-2(2)};
```

```
PlatooningData-Unencrypted::=Ieee1609Dot2Data (WITH COMPONENTS {
 content (WITH COMPONENTS {
    unsecuredData PRESENT
 })
})

PlatooningData-PublicKeyEncrypted::=Ieee1609Dot2Data (WITH COMPONENTS {...,
   content (WITH COMPONENTS {
      encryptedData (WITH COMPONENTS {
         recipients (WITH COMPONENT (
            (WITH COMPONENTS {
               pskRecipInfo ABSENT,
               symmRecipInfo ABSENT,
               certRecipInfo ABSENT,
               signedDataRecipInfo ABSENT,
               rekRecipInfo PRESENT
            })
         )),
         ciphertext (WITH COMPONENTS {
            aes128ccm PRESENT
         })
      })
   })
})

PlatooningData-SymmetricKeyEncrypted::=Ieee1609Dot2Data (WITH COMPONENTS {...,
   content (WITH COMPONENTS {
      encryptedData (WITH COMPONENTS {
         recipients (WITH COMPONENT (
            (WITH COMPONENTS {
               pskRecipInfo ABSENT,
               symmRecipInfo PRESENT,
               certRecipInfo ABSENT,
               signedDataRecipInfo ABSENT,
               rekRecipInfo ABSENT
            })
         )),
         ciphertext (WITH COMPONENTS {
            aes128ccm PRESENT
         })
      })
   })
})


END
```

4.4. Key distribution and update process

Three types of encryption keys shall be used within a platoon.

- **Platoon group key** (PGK) is symmetric key to encrypt the messages dedicated to multiple receivers, e.g., the platoon control messages (PCM)

- **Platoon participant key** (PPK) is a symmetric key to encrypt platoon messages which should not be accessible by any user except the dedicated one, e.g., KeyUpdate massage.

- **Join response encryption key** (JREK) is a asymmetric key to encrypt the join response.

4.4.1. Key update

We have three ways of distribute keys, JoinRequest, JoinResponse and KeyUpdate.

- JoinRequest:
  In the payload of the JoinRequest a Join Response Encryption Key (JREK) is provided. The purpose of this key is to encrypt the join response. The key shall be be an asymmetric, ephemeral key generated explicitly for one join procedure.

- JoinResponse:
  In the payload of JoinResponse message two keys are provided from the last truck in platoon to the joining truck: platoon group key (PGK) and platoon participant key (PPK). Notice that since the JoinResponse is asymmetric encrypted, the keys cannot be available at any other users except the joining truck.

- KeyUpdate:
  For example by leaving a truck, a new generated group key by the first truck needs to be provided to the other trucks in platoon. To do this, the KeyUpdate message is used which is encrypted with symmetric participant key and provides the new group key from the truck in front to the one behind. The reason for a keyUpdate is always if someone leaves the platoon.

JoinResponse

An overview of the join manoeuvre is exemplary depicted in Figure 5, Key distribution during Joining procedure. Details about the join maneuver are shown in Figure 6, Illustration of the Joining procedure. The join manoeuvre is initiated by the CAM message (with PlatooningContainer) generated by the last truck in the platoon. The signed CAM message is sent via broadcast on the respective channel, so it can be received by surrounding trucks. If the CAM is received by a truck with activated platooning function and intention to join, the message is first verified and checked for permission.

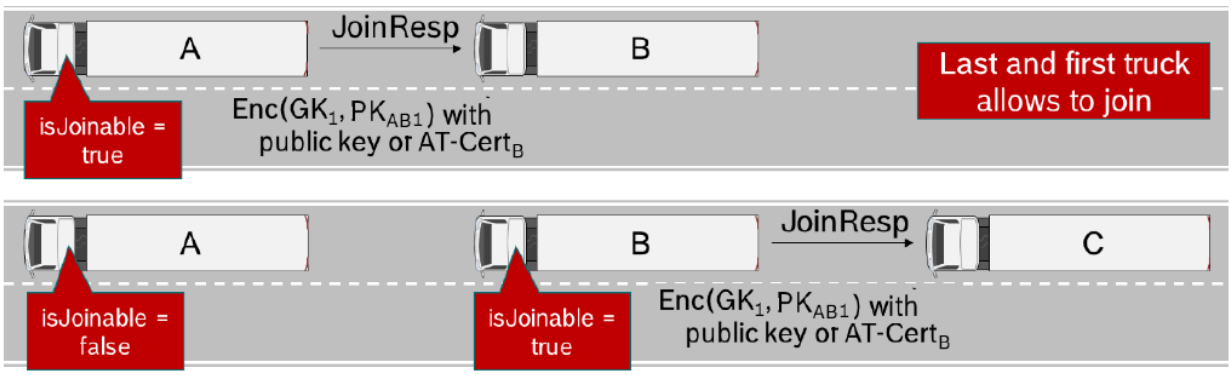

Figure 5, Key distribution during Joining procedure

The following sequence of Figure 6, Illustration of the Joining procedure is done in analogues way according to the specification in D2.8 [9]. In special, a symmetric group key and a participant key are given from the last truck in the platoon to the joining truck as part of the Join Response message.

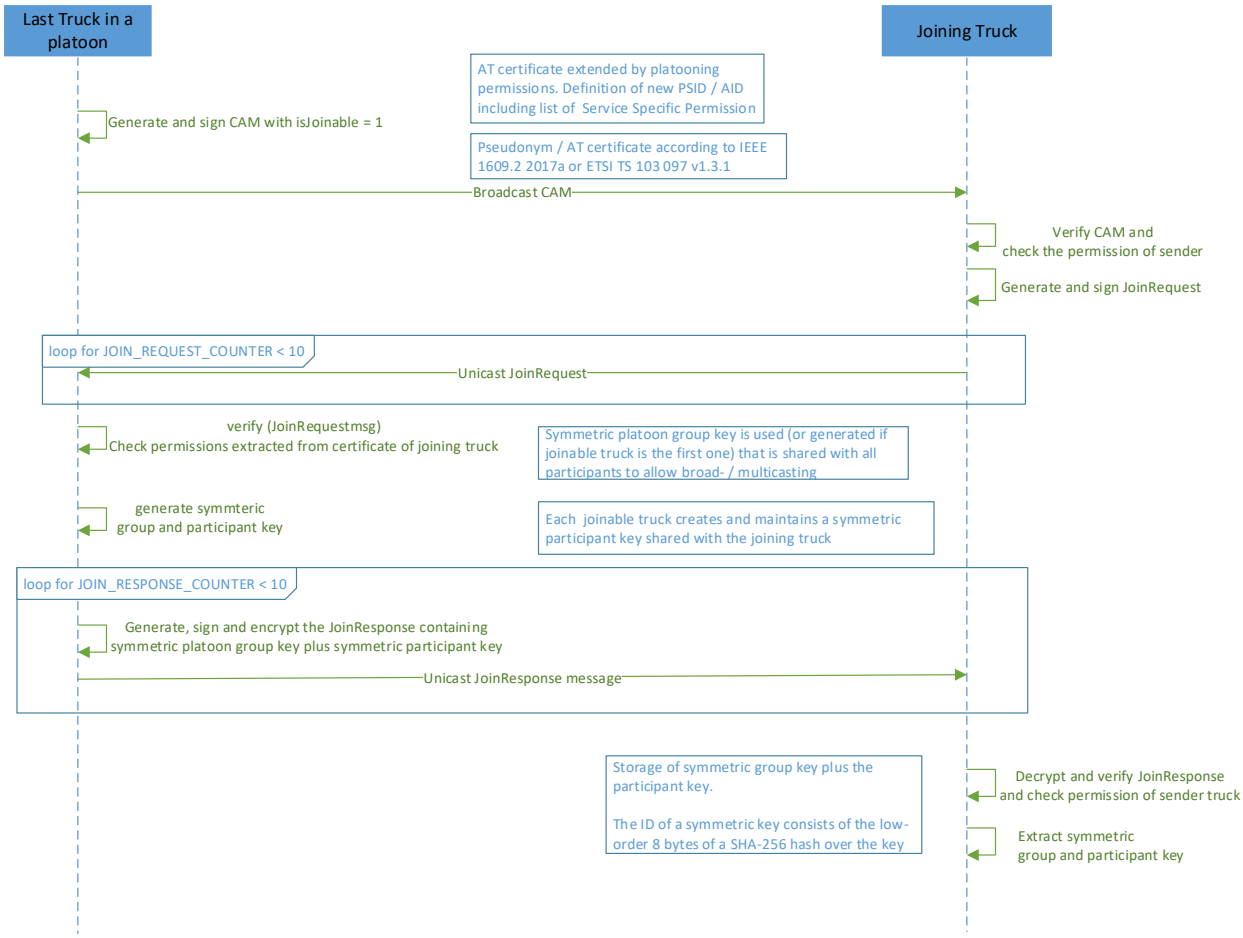

Figure 6, Illustration of the Joining procedure

The keys used for platooning will be distributed as a part of the facility message payload. The reason for not using the security header is that it does not fulfil our need to attach more than one symmetric encryption key, i.e. Group Key and Participant key, to the join response and key update messages. In favour of consistency the choice was made to move all platooning related key distribution to the facility layer messages.

KeyUpdate (someone left the platoon)

- One vehicle leaves the platoon: When a vehicle is part of a platoon, this vehicle has the keys for the message exchange. If this vehicle wants to leave the platoon, it would not have to being able to communicate when the leave is complete.

- One vehicle stops sending PCMs for a while: When a vehicle is part of a platoon, this vehicle stops sending the PCMs and for security issues it is mandatory to initiate a keyUpdate process, having in consideration safety issues too.

- Split of the platoon: When standalone distance is reached, the two resultant platoons must update the keys to avoid vehicle of the other part decrypt the exchanged messages.

- One vehicle requests the join, obtain the key but not completes the joining process to the platoon: As the vehicle has the key when it receives the joinResponse, the key must be changed if the join is not completed at all to avoid this vehicle access to the messages exchanged in the platoon.

4.4.2. Key derivation

In order to avoid the traceability of the users in a platoon, the unencrypted ID's used in different communication layers need to be changed time to time. Since the contents of the security header are not encrypted, the key-ID and subsequently the symmetric key which is used for the communication (i.e., Re-keying), have to be also changed.

In order to avoid extra communication for providing the new group key, a key derivation function (KDF) which is available at all trucks in the platoon, is used for generating the new key. This mechanisms is used for generating both group key and participant key.

- All platoon members in the platoon know the current platoon group key (PGK_c).

- All platoon members in the platoon know the platoon key derivation function (PKD). The specific key derivation function that is going to be used is not yet decided.

- Using the specific platoon key derivation function, the platoon members can generate a reserve platoon group key PGK_r = PKD(PGK_c) with the current platoon group key as basis. All platoon members can generate the same PGK_r locally without exchanging an additional information.

- By the next rekeying, PGK_r will be PGK_c and used for encrypting the messages. The next reserve key will be then generated as mentioned above.

For identifying the use of a rekeyed platoon group key in the platoon messages the ID of the key in the security header can be used, which is defined as recipient ID in IEEE1609.2 [5]. The recipient ID can be extracted easily from the key. It's calculated from the COER (Canonical Octet Encoding Rules) encoded ASN1 structure containing the key (SymmetricEncryptionKey structure) defined in IEE1609.2 [5]. For each Platoon using a unique platoon group key the reserve Platoon group key is different for each platoon, because the key derivation function is used on the current platoon group key.

In Figure 7, Key derivation the generating the new platoon group key using the PKD function is shown as sequence diagram. All trucks of the platoon had created as describe above a reserve platoon group key. One of the trucks, here Truck i, changes from the current platoon group key to the reserved platoon group key on a time basis. The truck sends the PCM encoded with new platoon group key as broadcast to all other trucks in the platoon. The other trucks in the platoon identified the key change, switch from the reserve key to the new group key and decodes the message. All trucks generates a new platoon reserve key. The PCMs are now provided by all platoon members with the new platoon group key.

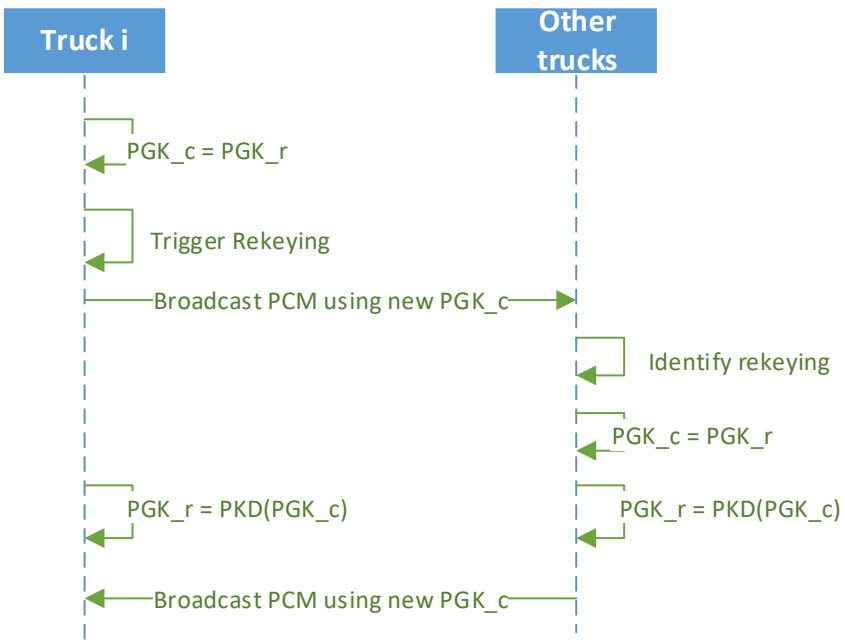

Figure 7, Key derivation

The same method of rekeying used for the platooning group key shall be used to update each of the platoon participant keys of the platoon members.

- Change in the unique identification of a member of the platoon: When a member of the platoon, for tracking reasons, requests for a new unique id, the key should be changed too.

- After certain time: Also, for avoiding tracking issues, when the same key is used for a certain time, the key should be changed using the keyUpdate process.

4.4.3. Pseudonym change and group key update

As defined for the V2X messages (e. g. CAM) [see ETSI 102 731 / section 3.1] the pseudonym change is requested to be done on a regular basis either by time or by distance driven. This prevents tracking of a single vehicle via outside infrastructure, conform with ETSI standardization.

Additionally not only the single platoon vehicles should be prevented from tracking via outside infrastructure, but the complete platoon should be prevented too. The messages send throughout the platoon are encrypted but in the security header of the platoon messages the id of the encryption key is provided unencrypted. To prevent the platoon to be tracked, the group key is updated using KD method. This leads to an update of the recipient ID in the security header of the platoon messages. The key update is done on a time basis which is much more often than the pseudonym change done for single vehicles.

The key update is provided once a minute based on the GPS time. More specifically the change is performed once every minute at second 13 of the minute, using the TAI time.

The current key remains valid for some time after the intended change. This overlapping key validity increases the robustness by increasing the window in which a message can be decoded that is still using the current key.

This prevents tracking of a single vehicle as well as tracking of the platoon using decoupling of Pseudonym change and platoon group key update.

5. CONCLUSION

The present deliverable specifies the V2X security framework applied to the platooning messages to ensure trust and a secured communication within the platoon. It makes use of already standardized protocols such as ITS-G5, GeoNetworking and BTP and standards such as IEEE 1609.2 [5] and ETSI TS 103 097 V1.3.1 [6]. The security framework developed for C-ITS day-one applications based on PKI is used to create a trust domain with the addition of encrypting platooning data.

It is shown how a truck can join a platoon and by attaching an asymmetric, ephemeral key to its JoinRequest which the responding truck uses to encrypt the JoinResponse, whereas it includes the symmetric key of the group. The joining truck is part of the platoon where it listens to and sends out symmetrical encrypted platoon control messages. Furthermore it is explained how platooning group keys are updated using either the KDF or, if someone leaves the platoon, using a key distribution mechanism. The deliverable also develops a first version of ASN.1 Platooning ASN.1 encryption module.

6. NEXT STEPS

This specification is the first agreed version as an input and starting point for the development and testing of the platooning functionality within ENSEMBLE. Based on findings and learnings from those activities the specification will be updated accordingly.

6.1. Communication strategies

By the time the document was finalized there exists an open issue of a clear description of a communication behaviour being missing, that could not be addressed during the development of that specification. The issue relates more to D2.8 Platooning protocol definition and communication strategies but has impact on D2.9 and the way of how keys are updated. In further steps the group that worked out the deliverable will align about, and define the communication strategy.

6.2. Key derivation function

It is not decided what the platoon key derivation function (PKD) is going to be. After finalization of this specification the group intends to work on selecting the PKD.

7. REFERENCES

[1] J. Kenney, “Dedicated Short-Range Communications (DSRC) Standards in the United States,” in Proceedings of the IEEE, Vol. 99, No. 7, July 2011, pp. 1162-1182.

[2] IEEE Std. 802.11-2016, “IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”

[3] ETSI TS 102 965 V1.4.1 (2018-11), “Intelligent Transports Systems (ITS); Application Object Identifier (ITS-AID); Registration,” November 2018.

[4] Respitory for Application IDs, http://standards.iso.org/iso/ts/17419/TS17419%20Assigned%20Numbers/

[5] IEEE Std 1609.2™-2016, “IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages – Amendment 1,” January 2016.

[6] ETSI TS 103 097 V1.3.1 (2017-10), “Intelligent Transport Systems (ITS), Security; Security header and certificate formats,” October 2017.

[7] C-ITS Deployment Platform, https://ec.europa.eu/transport/themes/its/c-its_en

[8] COMMISSION DELEGATED REGULATION (EU) …/... of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems, https://ec.europa.eu/transport/sites/transport/files/legislation/c20191789.pdf

[9] Atanassow, Boris, Sjöberg, Katrin (2018). Platooning protocol definition and Communication strategy . D2.8 of H2020 project ENSEMBLE

APPENDIX B – GLOSSARY

Abbreviation	Meaning
ACC	Adaptive Cruise Control
ASN.1	Abstract Syntax Notation One
BTP	Basic Transport Protocol
C2C-CC	CAR 2 CAR Communication Consortium
C-ACC	Cooperative Adaptive Cruise Control
C-ITS	Cooperative ITS
CA	Cooperative Awareness
CAM	Cooperative Awareness Message
CCH	Control Channel
DCC	Decentralized Congestion Control
DE	Data Element
DF	Data Frame
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
DSRC	Dedicated Short-Range Communications
CAMP	Crash Avoidance Metric Partnership
e.i.r.p	Effective Isotropic Radiated Power
ETC	Electronic Toll Collection
ETSI	European Telecommunications Standards Institute
EU	European Union
GN	GeoNetworking
GUI	Graphical User Interface
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITS	Intelligent Transport System
LOS	Line Of Sight
LLC	Logical Link Control

Abbreviation	Meaning
MAC	Medium Access Control
MAP	MapData message
OBU	Onboard Unit
OEM	Original Equipment Manufacturer
PCM	Platoon Control Message
PKI	Public Key Infrastructure
PMM	Platoon Management Message
PMC	Platooning Mode Control
PGK	Platoon Group Key
PKD	Platoon Key Derivation Function
PPK	Platoon Participant Key
RSU	Road Side Unit
SAE	SAE International, formerly the Society of Automotive Engineers
SCH	Service Channel
SDO	Standard Developing Organisation
SHB	Single Hop Broadcast
SPAT	Signal Phase and Timing message
TC	Technical Committee
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to any (where x equals either vehicle or infrastructure)
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WP	Work Package