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 for platooning	
Dissemination level	Public	
Written By	Boris Atanassow, Katrin Sjöberg, Marcus Larsson VOLVO Roman Alieiev, MAN Soheil Gherekhloo, Ralph Prenzel, BOSCH William Whyte, Qualcomm Joost van Doorn, NXP	03-03-2020

	Arne Ehlers, Tobias Werle ZF Sergi Guarnich, Alejandro Manilla, Idiada	
Checked by	Edoardo Mascalchi, CLEPA	31-01-2022
Approved by	Marika Hoedemaeker, TNO	04-03-2022
Status	APPROVED BY EC	13-10-2022

Please refer to this document as:

Boris Atanassow, Katrin Sjöberg et all (2022). *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.

TABLE OF CONTENTS

Revision history

Version	Date	Author	Summary of changes	Status
0.1	03/03/2020	Boris Atanassow (Volvo AB)	Initial input starting from previous version of the deliverable	Prepared
0.2	09/11/2021	VOLVO/CLEPA	Feedback by partners implemented	Draft
1.0	22/12/2021	VOLVO/CLEPA	Ready for WP Leader review	Final
1.1	31/01/2022	CLEPA	Ready for Coordinator review	Final
1.2	04/03/2022	CLEPA	Feedbacks from Coordinator Implemented	Final
2.0	01/08/2022	TNO	Update after PO review	Final

FIGURES

TABLES

EXECUTIVE SUMMARY

Context and need of a multi brand platooning project

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 traffic safety, fuel economy, and throughput. This has been demonstrated by driving up to seven differently branded trucks in one (or more) platoon(s) under real world traffic conditions. During the years, the project was organised as follows:

- Year 1: setting the specifications and developing a reference design;
- Year 2 and 3: implementing this reference design on the OEM own trucks, as well as performing impact assessments with several criteria;
- Year 4: focus on testing the multi-brand platoons on test tracks and public road.

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

Platooning levels

Two levels of platooning have been defined:

- **Platooning Support Function**: the driver is responsible for the driving task. Hence (s)he is also responsible to choose a safe following distance and monitor the system e.g. whether the right platooning partner is being followed (though supported by the system as much as possible). To give the driver sufficient time to react, minimum time gaps around 1.5 s have to be respected. The Platooning support function is a longitudinal control function, but lateral driver assistance systems, such as e.g. lane keeping, might be optionally available as well.

- **Platooning Autonomous Function**: The lead truck has a driver responsible for the driving task, but the following trucks are fully automated, i.e. the system performs the complete

driving task within the specified (limited) operational design domain. Taking the driver(s) out-of-the-loop offers the possibility to reduce time gaps to a minimum of 0.3 s.

In contrast to the Platooning Support Function, implementation of the Platooning Autonomous Function is not part of the ENSEMBLE project and the specification of the Platooning Autonomous Function and its use cases is solely done on theoretical considerations to sketch a future vision of platooning. The latter is also due to the low technology readiness level of certain required autonomous driving subfunctions at the time of writing.

For the interest of the reader, the main documents that describe the two platooning levels defined in ENSEMBLE are:

- Levels definitions and Use Cases – D2.3 [13]
- Requirements and Specifications - D2.5 [14]

Additional details on the Communication protocol and the strategic and services layers can be also found in:

- V2X Protocol - D2.8 [12]
- Security - D2.9 (this deliverable)
- Intelligent infrastructure - Strategic and Services Layers – D2.6 [15] and D2.7 [16]

Furthermore, the deliverable related to the safety analysis performed on the two levels are:

- Safety of the intended functionality (SOTIF) - D2.13 [17]
- Functional Safety - D2.14 [18]
- Item Definition - D2.15 [19]

Abstract of this Deliverable

This deliverable provides a specification of the V2X security framework. It describes which measures 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 D2.3 [13] and the requirements and specifications in deliverable D2.5 [14] 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. Deliverable D2.5 contains the lessons learned and future considerations on the communication protocol including the security implementation as concluded from the final testing of

the PSF with seven-brands in Spain taking place in September 2021. Deliverable D6.15 [20] will also provide guidance for the upcoming standardization on platooning.

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. 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 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

[1] European Telecomunications 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/

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.
Platooning and cooperative adaptive cruise control (C-ACC) are enabled through the transmission of V2X data and they 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. C-ACC is a distributed application using longitudinal information contained in V2X packets whereas platooning is a closed-loop application between well-known participants which can use both longitudinal as well lateral V2X data for operation.
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 sensors 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 the information received via the ITS-G5 interface can be safety related and may in a direct or an indirect way affect the behaviour of the vehicle, thus the information must be reliable.

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

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 pose a safety risk since, for example requirements, on sensors and/or driver for being able to platoon are not fulfilled. Further, the vehicle following behind without being part of the platoon might not have paid for the service.

2. The platoon control messages include more information than ordinary CAMs then confidentiality is required to ensure privacy and to avoid traceability of individual vehicles in the platoon by outside sources.

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 STANDARDISED 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

V2X protocols have been developed to allow for communication between different brands supporting day one applications. The protocols are divided among three different layers having certain responsibilities in order to break down the complexity of communication. Deliverable 2.8 [12] already defines and locates the platooning protocol as a facilities layer application as depicted in Figure 1. In addition to the structured layered approach, the security block in the V2X communication stack is cross-layer providing security-related functionality to more than one layer.

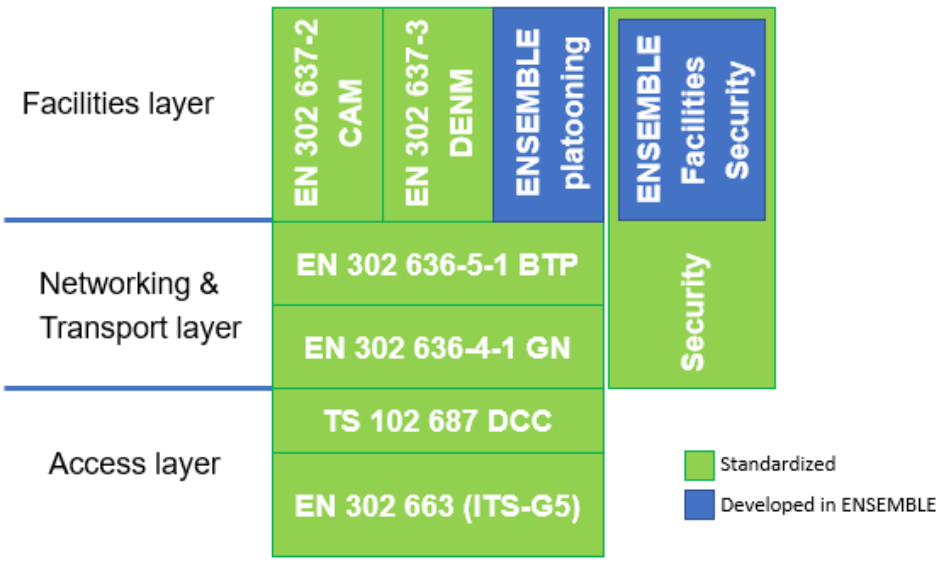

Figure 1 - Security in the V2X communication stack

The concept for platooning security is treated and elaborated in Chapter 4. The security approach for V2X communication supporting day one applications is based on a public key infrastructure (PKI) where messages are signed and verified using a temporarily authorization ticket (AT). Signage and verification are applied for all kinds of messages in the V2X domain, e.g. CAM and DENM. No day one applications are using encryption yet, but encryption is supported by ETSI specifications.

3.2. The V2X security header

Each message consists of different headers fulfilling 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 of the Geonetworking (GN) protocol also including the payload as shown in Figure 2.

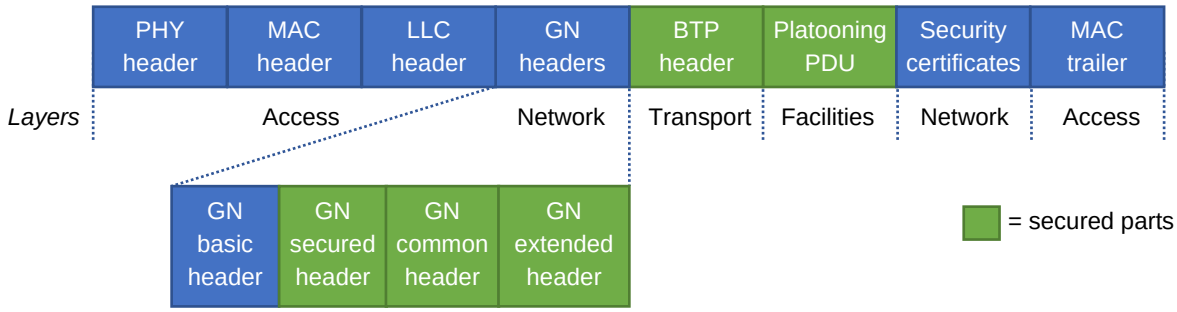

Figure 2 - V2X secured packet

Note, that although the ETSI specifications provide for security services to be applied at the network & transport layer, they do 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 design in this proposal for platooning makes use of this feature of the ETSI architecture, applying authentication services (signing) at the networking & transport layer for the GN protocol but encryption services (confidentiality) is applied at the facilities layer in the platooning protocol.

3.3. V2X Public key infrastructure

The PKI for European C-ITS is defined in ETSI TS 102 940 v1.3.1 [21] and it is depicted in Figure 3: Public Key Infrastructure.

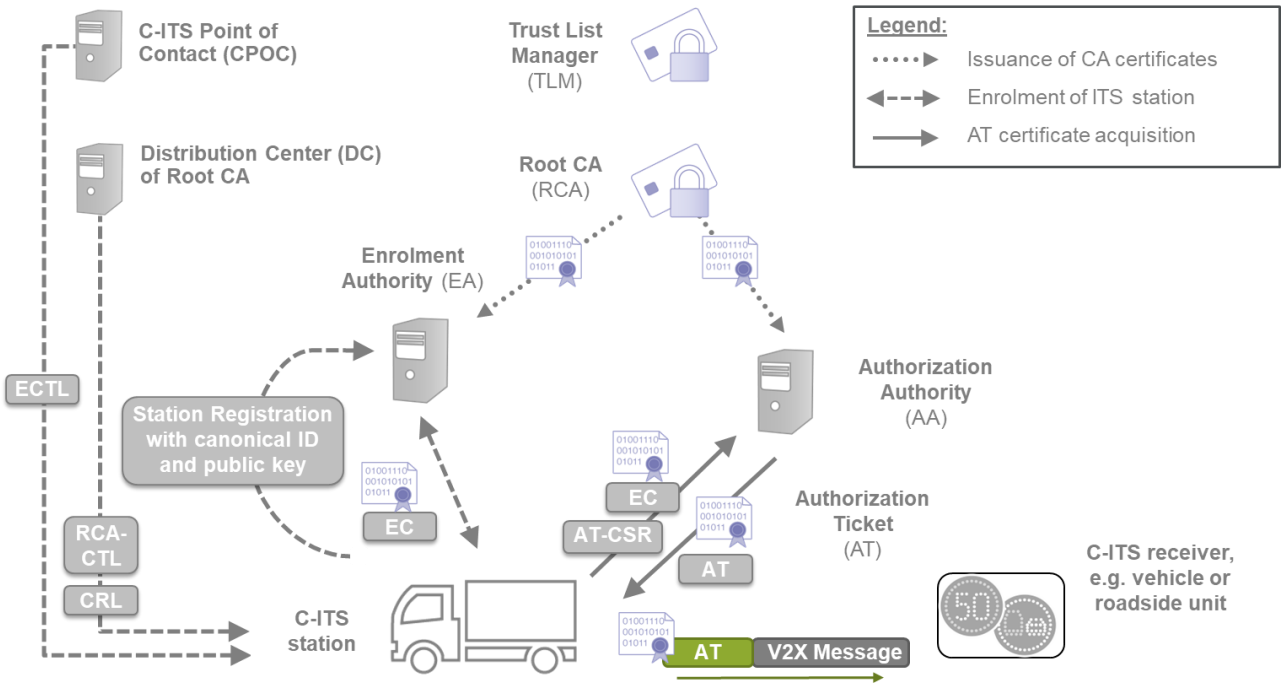

Figure 3 - Public key infrastructure

The purpose of the Trust List Manager (TLM) is to put certificates of trusted Root Certificate Authorities (Root CA, or RCA) 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 information about sub CAs is provided in the RCA-CTL (RCA-Certificate Trust List). Furthermore, the RCA signs a Certificate Revocation List (CRL) in order to allow the revocation of issued sub CAs.

The EA is used to register new C-ITS stations where the registration API is not standardized by ETSI. Registered C-ITS stations can request Enrolment Credential (EC) certificates from the EA. Using these EC certificates, C-ITS stations can request Authorization Tickets (AT) from the AA with Authorization Ticket Certificate Signing Requests (AT-CSR).

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

The impact on privacy of road users should be minimised. Accordingly, EC has published C-ITS Security Policy release 1 (C-ITS SP) [8], describing a security architecture supported by a PKI using frequently changing pseudonym certificates. According to the 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 provided in ETSI TR 103 415 [9].

3.5. Signage and encryption

All messages sent by fixed and mobile C-ITS stations shall be signed according to ETSI TS 103 097 [6] as detailed in the C-ITS SP [8]. The vehicle C-ITS station shall use one end-to-end security header at the networking & transport layer and a signature per message in accordance with ETSI TS 103 097 [6] and EN 302 636-4-1 [10]. The integrity of all messages used by ITS applications shall be validated by the receiver according to TS 103 097 [6].

3.6. Application ID

Each ITS application is globally identified by an Intelligent Transport Systems Application Object Identifier (ITS-AID) and these are outlined in ETSI TS 102 965 [3]. ISO 17419 [22] 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 the template available at [4] should be used. 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 detailed and added security profiles are outlined. It is 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. The new message types introduced by the platooning protocols are outlined in Table 1. The security terminology is found in **Error! Reference source not found.**.

Table 1 - New message types in the platooning protocol

Message type		**Description**
Platoon Management Message (PMM)	JoinRequest	The JoinRequest message is transmitted by a vehicle who wants to join a platoon.
	JoinResponse	The JoinResponse message is transmitted as a reply to a JoinRequest message.
	PlatoonUpdate	PlatoonUpdate is transmitted approx. every minute and it is also triggered if the platoon has changed leader. The PlatoonUpdate message was earlier called KeyUpdate.
Platoon Control Message (PCM)		When vehicles are connected in the platoon, they exchange PCMs. Every vehicle in the platoon will transmit 20 PCMs per second (20 Hz).

Table 2 - Terminology

Terminology	**Description**
Platoon Group Key (PGK)	A symmetric key distributed to all platoon members to enable platoon wide privacy. Used for encrypting PCMs.
Platoon Participant Key (PPK)	A symmetric key to encrypt the private communication between two trucks following one after the other. Used for encrypting PlatoonUpdate messages.
Join Response Encryption Key (JREK)	An asymmetric key to encrypt the JoinResponse message to provide joining trucks with platoon relevant information, e.g., PGK, PPK, position in the platoon, PlatoonID, etc.

4.2. Concept of signing and encryption

As described in Chapter 3, platooning is based on trust. By following the C-ITS certificate policy [11], trust can be established between vehicles from different manufacturers to ensure integrity on all platooning related messages and confidentiality when required.

4.2.1. Signing of messages

Signage is initiated at the networking & transport layer by the GN protocol and the security profile for platooning, which is defined in Chapter 4.3. It is compatible with ETSI TS 103 097 [6].

4.2.2. Encryption of messages

Encryption is initiated at the facilities layer by the platooning protocol. Necessary interfaces 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 deliverable proposes some additional mechanisms, such as regularly renewing the platoon group key (PGK) to enhance unlikability. These mechanisms do currently not have a specified interface and this will be developed as part of the ENSEMBLE project.

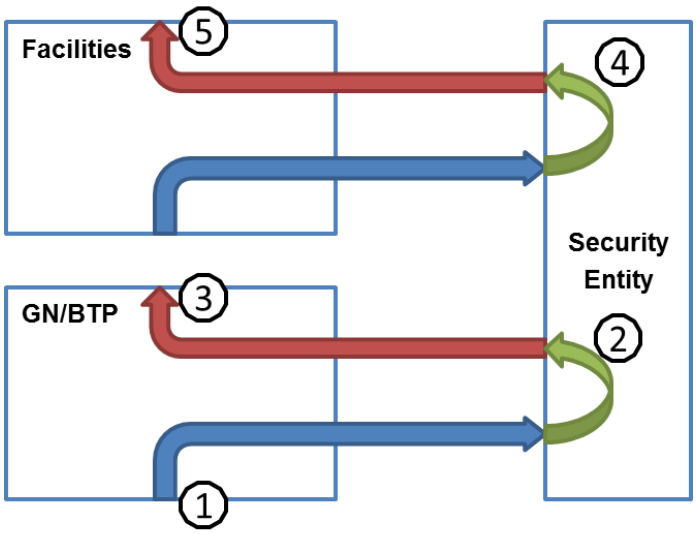

Figure 4 - Platooning message flow in the V2X communication stack

In **Error! Reference source not found.**the platooning message flow of a received packet on access l ayer up to the facilities layer is depicted. In Step (1), a signed packet is received at the network & transport layer by the GN protocol, and passed on to the security entity. In the secure element of the GN packet (see Figure 2), the attached signature is verified in Step (2) and a result is sent back to the network & transport layer. If the verification is OK (a trusted party sent the packet with a valid certificate for platooning), the packet will be passed to the facilities layer using the platooning BTP port, through Step (3). In Step (4), the platooning facility passes the received packet forward to the

security entity again where the payload is decrypted and if successful the data packet is forwarded to the control unit in need of the received data in Step (5).

4.3. Security profiles

This chapter is to be seen as an extension to Clause 7.1 of ETSI TS 103 097 [6].

4.3.1. Platooning

The secure data structure containing a platooning message shall be of type `EtsiTs103097Data-Signed` as defined in Clause 5.1 and Annex A of ETSI TS 103 097 [6], containing the JoinRequest 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

JoinRequest message

The secure data structure containing JoinRequest message shall be of type `PlatooningData-Unencrypted` as defined in “Platooning ASN.1 encryption module” below, containing the JoinRequest Message as the `unsecuredData`.

JoinResponse message

The secure data structure containing positive JoinResponse message shall be of type `PlatooningData-PublicKeyEncrypted` as defined in “Platooning ASN.1 encryption module” below, containing the JoinResponse 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 contain the digest of the join response encryption key (the lower 8 bytes of the hash of the encoded structure of the key).

The secure data structure containing negative JoinResponse message shall be of type `PlatooningData-Unencrypted` as defined in "Platooning ASN.1 encryption module" below, containing the JoinRequest message as the `unsecuredData`.

PlatoonUpdate message

The secure data structure containing PlatoonUpdate message shall be of type `PlatooningData-SymmetricKeyEncrypted` as defined in "Platooning ASN.1 encryption module" below, containing the PlatoonUpdate 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 (the lower 8 bytes of the hash of the encoded structure of the key).

Platoon control message

The secure data structure containing platoon control message (PCM) shall be of type `PlatooningData-SymmetricKeyEncrypted` as defined in "Platooning ASN.1 encryption module" below, containing the PCM 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 (the lower 8 bytes of the hash of the encoded structure of the key).

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

In the ENSEMBLE project, three types of encryption keys have been identified and shall be used to secure the ENSEMBLE platooning protocol:

- **Platoon group key** (PGK) is symmetric key to encrypt the messages dedicated to multiple receivers, used for 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, used for PlatoonUpdate message

- **Join response encryption key** (JREK) is a asymmetric key to encrypt the JoinResponse message

4.4.1. Providing new keys for the platoon

There are three ways to distribute keys, within the JoinRequest, JoinResponse and PlatoonUpdate message.

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

- **JoinResponse**:
  In the payload of the JoinResponse message, two keys are provided from the last vehicle in platoon to the joining vehicle: platoon group key (PGK) and a platoon participant key (PPK). Notice that since the JoinResponse is asymmetrically encrypted, the keys are not available to others except for the joining vehicle.

- **PlatoonUpdate:**
  A newly generated platoon group key (PGK) has to be provided by the leading vehicle to the other members of the platoon when the time for the current PGK has expired. In this process, also the individual platoon participant keys (PPK) are newly generated. To do this, the PlatoonUpdate message is used, which is always sent from the vehicle in front to the one behind. It is encrypted with the respective active symmetric participant key (i.e., PPK) and provides the new group key PGK, which is created by the leader of the platoon, and the new individual participant key PPK, created by the vehicle in front of the ego-vehicle. The PlatoonUpdate message is triggered by a process that checks every 10 secs the current key age (of the key in use, MAX_KEY_AGE = 60 secs) and if the platoon will get a new leader.

JoinResponse

The JoinResponse message is sent in response to a received JoinRequest message and it is always sent by the last vehicle in the platoon (in ENSEMBLE only joining from behind is specified). An overview of the join procedure with key distribution is provided in **Error! Reference source not found.** and details are found in Figure 6. The join procedure is triggered by a vehicle following another vehicle, which transmits cooperative awareness messages (CAM) containing information about platooning capability (i.e., isJoinable = TRUE, see Figure 5). The follower transmits a JoinRequest message which the CAM transmitting vehicle will react upon by sending either a positive JoinResponse or a negative JoinResponse.

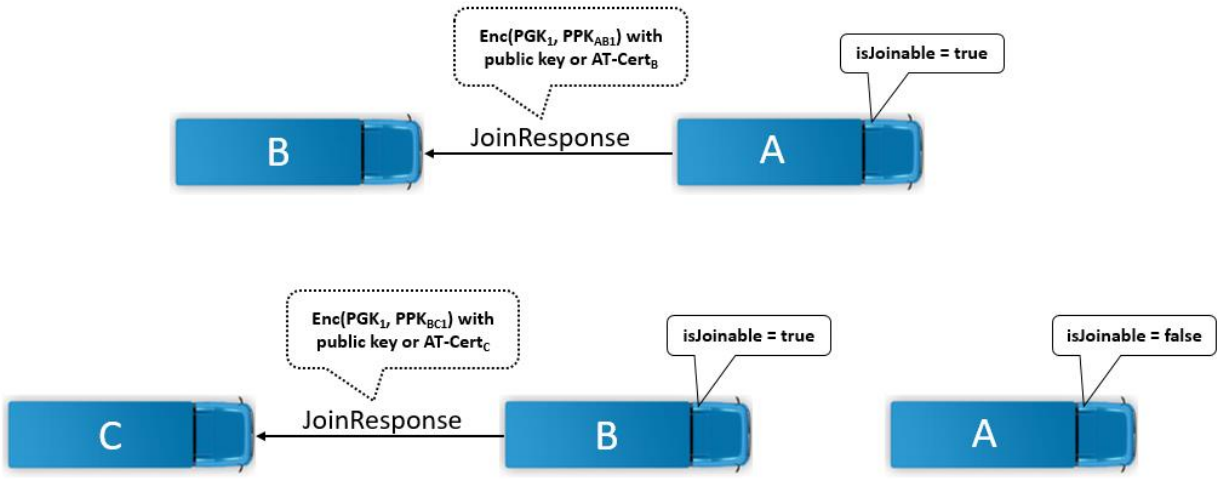

Figure 5 - Key distribution during joining procedure; two separate examples.

The sequence diagram in **Error! Reference source not found.** illustrates the security key handling i n the joining procedure. The PGK and PPK are provided from the last vehicle in the platoon to the

joining vehicle as part of the JoinResponse message. These will be distributed in the JoinResponse message's payload.

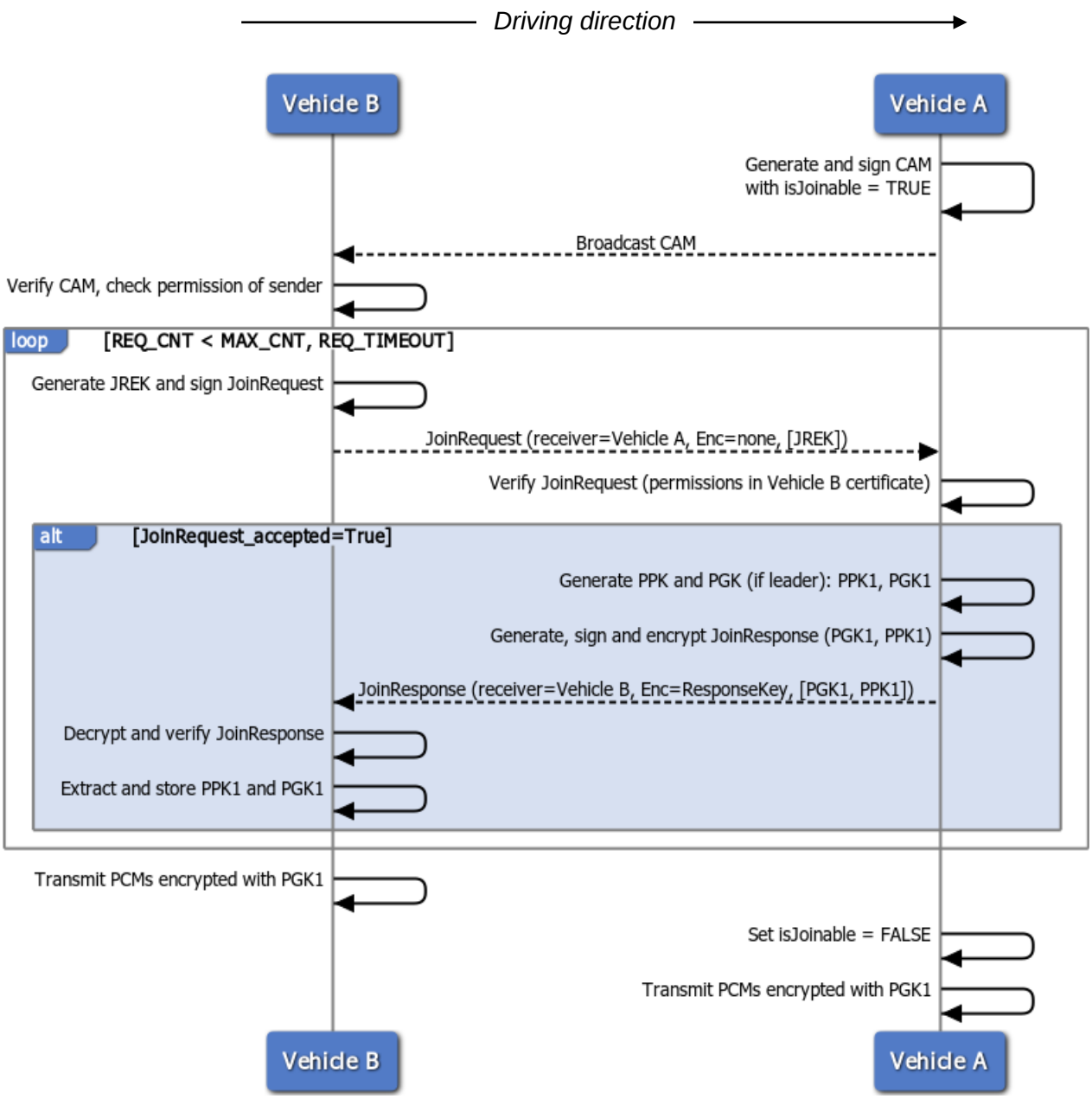

Figure 6 - Key handling at the joining procedure

PlatoonUpdate

Continuously running key age check process

The leading vehicle is responsible for initiating the process of updating the security keys through sending the PlatoonUpdate message. Every 10 s the current age of the PGK used to encrypt the PCMs is checked (see requirement REQ_V2V_035 in D2.8 [12]). The maximum key age is set to 60 s. If the maximum key age has expired, a new PGK and PPK are generated and transmitted in the PlatoonUpdate message to the direct follower. At the direct follower (of the leader) the received PGK and PPK are stored, a new PPK is generated and the PlatoonUpdate message is sent further backwards (including the received PGK). Each follower has to run the same procedure, receive the PlatoonUpdate message, store the new PGK and PPK, generate itself a new PPK, send the PlatoonUpdate further backwards (PPK, PGK). When the trailing vehicle receives the PlatoonUpdate message, it can directly use the new PGK for encryption, since it knows that all preceding trucks are aware of the new PGK (every follower has stored it).

The vehicle directly in front of the last vehicle in the platoon will directly recognize the PCMs being encrypted with the updated PGK, and will itself start to use it for the PCMs it is broadcasting. At this point in time, also the new PPK, used for encrypting all upcoming PlatoonUpdate messages, is activated. That continuous for each preceding truck. The awareness of the new PGK will now travel from the back to the front of the platoon.

When the leader notices that the direct follower is encrypting with the new PGK, it switches itself to this new PGK and it becomes the key "in use".

If within the next 10 s check for the key in use, the leader recognizes that the key is not yet used by its direct follower it triggers a new PlatoonUpdate message, including generation of a new PGK, a new PPK, etc. and sends it backwards. The whole chain repeats and the key sent just before becomes an obsolete key.

PlatoonUpdate triggered by merging platoons

The PlatoonUpdate message is also triggered when two platoons merge. Reason for an immediate trigger of a PlatoonUpdate in the joining platoon is that all members in the joining platoon need to be informed about the new PGK to be used (and new PlatoonID, new position in the merged platoon, etc.). Looking at the example in Figure 7, as long as the new PGK (received in the JoinResponse from the trailing truck V0) is not known by vehicle, V1 and V2, in the joining platoon, the leader V1 cannot start using the new PGK. It must make sure that every one of the followers has it before it itself can start using it, and by that confirm to the trailing truck V0 of the platoon in front that the join is complete.

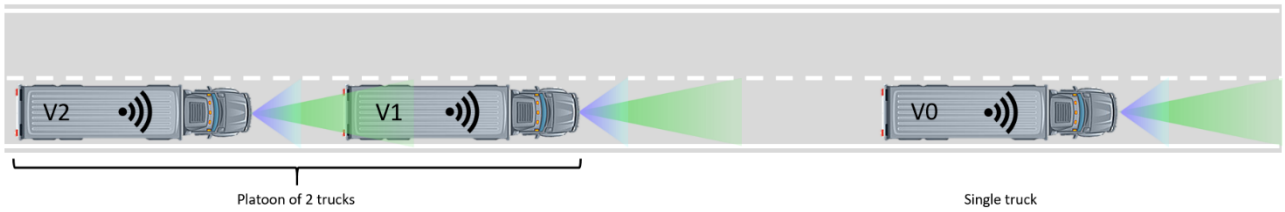

Figure 7 - Joining (merging)

Starting from the reception of the JoinResponse message at V1. The JoinResponse message contains a new PlatoonPosition, PlatoonID and a new PGK.

Upon reception of the JoinResponse message at V1:

V1 has to send the new PlatoonID and new PGK onwards to the next vehicles of the joining platoon. To do this, V1 creates and sends a PlatoonUpdate message containing the new PlatoonID, and the new PGK. The updated position in this PlatoonUpdate message is the value of the "joiningAtPosition" field + 1 in the JoinResponse message sent by V0. This PlatoonUpdate message is sent onwards to each following vehicle of the joining platoon while each vehicle increments the value of "updatedPosition" field in the PlatoonUpdate message by 1. The trailing vehicle will start to use the new PlatoonID in its PCMs and it will encrypt its PCMs with the new PGK. PCMs encrypted with the new PGK, using the new PlatoonID will arrive at V1. Only after the first reception of a PCM containing the new PlatoonID and encrypted using the new PGK, V1 will switch over to use the new PlatoonID as its current PlatoonID and V1 will, at the same time, switch over to the new PGK to use for encryption of the PCMs it sends and a new PPK to use for encryption of the PlatoonUpdate messages it sends to the vehicle behind. The joining will be complete when V0 receives the first PCM with the provided PGK from the transmitted JoinResponse message.

4.4.2. Pseudonym change and group key update

To prevent tracking of single vehicles in platoons from infrastructure, pseudonym change is regularly required, based either on time or distance driven. The messages sent throughout the platoon are encrypted but in the security header of the messages the id of the encryption key is provided unencrypted. To prevent platoons to be tracked, the PGK is updated periodically. This leads to an update of the recipient ID in the security header of the messages. The update of PGK and PPK in the PlatoonUpdate message is performed much more often than the pseudonym change for single vehicles. A new PGK is provided once a minute. This overlapping key validity increases the robustness by increasing the window in which a message can be decoded that is still using the "old" key. This prevents tracking of single vehicles as well as tracking of platoons by decoupling pseudonym change and PGK 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 [6]. The security framework developed for C-ITS day-one applications based on PKI is used to create a trusted domain with the addition of encrypting platooning data.

It is shown how a vehicle can join a platoon and by attaching an asymmetic, ephemeral key to its JoinRequest message, the responding vehicle uses this to encrypt the JoinResponse message, which in turn contains the platoon group key of the platoon. The joining vehicle is part of the platoon where it listens to and sends out encrypted platoon control messages. Furthermore, it is explained how platooning group keys are updated periodically or triggered by a join of more than one vehicle. The deliverable also provides a first version of the ASN.1 Platooning ASN.1 encryption module.

Deliverable D2.5 contains the lessons learned and future considerations on the communication protocol including the security implementation as concluded from the final testing of the PSF with seven-brands in Spain taking place in September 2021.

6. BIBLIOGRAPHY

[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] European Commission, “Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS),” Release 1, December 2017.

[9] ETSI TR 103 415 V1.1.1 (2018-04), “Intelligent Transport Systems (ITS); Security; Pre-standardization study on pseudonym change management,” April 2018.

[10] ETSI EN 302 636-4-1 V1.4.1 (2020-01), “Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality,” January 2020.

[11] European Commission, “Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS),” Release 1.1, June 2018.

[12] ENSEMBLE project Deliverable D2.8, “Platooning protocol definition and communication strategy,” January 2022. https://platooningensemble.eu/library.

[13] ENSEMBLE project Deliverable D2.3, “V2 Platooning use cases, scenario definition and Platooning Levels,” January 2022. https://platooningensemble.eu/library.

[14] ENSEMBLE project Deliverable D2.5, “Final Version Functional specification for white-label truck” January 2022. https://platooningensemble.eu/library.

[15] ENSEMBLE project Deliverable D2.6, “Functional specification for intelligent infrastructure - Strategic and Services Layers,” January 2022. https://platooningensemble.eu/library.

[16] ENSEMBLE project Deliverable D2.7, “V2 Functional specification for intelligent Infrastructure (Strategic/Services layers),” January 2022. https://platooningensemble.eu/library.

[17] ENSEMBLE project Deliverable D2.13, “SOTIF Safety Concept” January 2022. https://platooningensemble.eu/library.

[18] ENSEMBLE project Deliverable D2.14, Final version Hazard Analysis and Risk Assessment and Functional Safety Concept,” January 2022. https://platooningensemble.eu/library.

[19] ENSEMBLE project Deliverable D2.15, “Final version of Iterative development process and Item Definition” January 2022. https://platooningensemble.eu/library.

[20] ENSEMBLE project Deliverable D6.15, “ENSEMBLE standardisation process” March 2022.

[21] ETSI TS 102 940 V1.3.1 (2018-04), “Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management“, April 2018.

[22] ISO 17419 “Intelligent transport systems — Cooperative systems — Globally unique identification“, May 2018.

APPENDIX A. – SEQUENCE DIAGRAM SOURCE

Sequence diagrams were produced in https://www.websequencediagrams.com/. In the present chapter the source code is provided.

The source code to Figure 6 “Key handling at the joining procedure”.

```
participant Vehicle B
participant Vehicle A

Vehicle A->Vehicle A: Generate and sign CAM\nwith isJoinable = TRUE
Vehicle A-->Vehicle B: Broadcast CAM
Vehicle B->Vehicle B: Verify CAM, check permission of sender

loop REQ_CNT < MAX_CNT, REQ_TIMEOUT

    Vehicle B->Vehicle B: Generate JREK and sign JoinRequest
    Vehicle B-->Vehicle A: JoinRequest (receiver=Vehicle A, Enc=none, [JREK])
    Vehicle A->Vehicle A: Verify JoinRequest (permissions in Vehicle B certificate)

    alt JoinRequest_accepted=True
        Vehicle A->Vehicle A: Generate PPK
        Vehicle A->Vehicle A: Generate, sign and encrypt JoinResponse (PGK, PPK)

        Vehicle A-->Vehicle B: JoinResponse (receiver=Vehicle B, Enc=ResponseKey, [PGK1,
PPK1])
        Vehicle B->Vehicle B: Decrypt and verify JoinResponse
        Vehicle B->Vehicle B: Extract and store PPK1 and PGK1
    end
end
Vehicle B->Vehicle B: Transmit PCMs encrypted with PGK1
Vehicle A->Vehicle A: Set isJoinable = FALSE
Vehicle A->Vehicle A: Transmit PCMs encrypted with PGK1
```

APPENDIX B. – GLOSSARY

Term	Definition
Convoy	A truck platoon may be defined as trucks that travel together in convoy formation at a fixed gap distance typically less than 1 second apart up to 0.3 seconds. The vehicles closely follow each other using wireless vehicle-to-vehicle (V2V) communication and advanced driver assistance systems
Cut-in	A lane change manoeuvre performed by vehicles from the adjacent lane to the ego vehicle's lane, at a distance close enough (i.e., shorter than desired inter vehicle distance) relative to the ego vehicle.
Cut-out	A lane change manoeuvre performed by vehicles from the ego lane to the adjacent lane.
Cut-through	A lane change manoeuvre performed by vehicles from the adjacent lane (e.g. left lane) to ego vehicle's lane, followed by a lane change manoeuvre to the other adjacent lane (e.g. right lane).
Ego Vehicle	The vehicle from which the perspective is considered.
Emergency brake	Brake action with an acceleration of <-4 m/s2
Event	An event marks the time instant at which a transition of a state occurs, such that before and after an event, the system is in a different mode.
Following truck	Each truck that is following behind a member of the platoon, being every truck except the leading and the trailing truck, when the system is in platoon mode.
Leading truck	The first truck of a truck platoon
Legal Safe Gap	Minimum allowed elapsed time/distance to be maintained by a standalone truck while driving according to Member States regulation (it could be 2 seconds, 50 meters or not present)
Manoeuvre ("activity")	A particular (dynamic) behaviour which a system can perform (from a driver or other road user perspective) and that is different from standing still, is being considered a manoeuvre.
ODD (operational design domain)	The ODD should describe the specific conditions under which a given automation function is intended to function. The ODD is the definition of where (such as what roadway types and speeds) and when (under what conditions,

Term	Definition
	such as day/night, weather limits, etc.) an automation function is designed to operate.
Operational layer	The operational layer involves the vehicle actuator control (e.g. accelerating/braking, steering), the execution of the aforementioned manoeuvres, and the control of the individual vehicles in the platoon to automatically perform the platooning task. Here, the main control task is to regulate the inter-vehicle distance or velocity and, depending on the Platooning Level, the lateral position relative to the lane or to the preceding vehicle. Key performance requirements for this layer are vehicle following behaviour and (longitudinal and lateral) string stability of the platoon, where the latter is a necessary requirement to achieve a stable traffic flow and to achieve scalability with respect to platoon length, and the short-range wireless inter-vehicle communication is the key enabling technology.
Platoon	A group of two or more automated cooperative vehicles in line, maintaining a close distance, typically such a distance to reduce fuel consumption by air drag, to increase traffic safety by use of additional ADAS-technology, and to improve traffic throughput because vehicles are driving closer together and take up less space on the road.
Platoon Automation Levels	In analogy with the SAE automation levels subsequent platoon automation levels will incorporate an increasing set of automation functionalities, up to and including full vehicle automation in a multi-brand platoon in real traffic for the highest Platooning Automation Level. The definition of “platooning levels of automation” will comprise elements like e.g. the minimum time gap between the vehicles, whether there is lateral automation available, driving speed range, operational areas like motorways, etc. Three different levels are anticipated; called A, B and C.
Platoon candidate	A truck who intends to engage the platoon either from the front or the back of the platoon.
Platoon cohesion	Platoon cohesion refers to how well the members of the platoon remain within steady state conditions in various scenario conditions (e.g. slopes, speed changes).
Platoon disengaging	The ego-vehicle decides to disengage from the platoon itself or is requested by another member of the platoon to do so. When conditions are met the ego-vehicle starts to increase the gap between the trucks to a safe non-platooning gap. The disengaging is completed when the gap is large enough (e.g. time gap of 1.5 seconds, which is depends on the operational safety based on vehicle dynamics and human reaction times is given). A.k.a. leave platoon

Term	Definition
Platoon dissolve	All trucks are disengaging the platoon at the same time. A.k.a. decoupling, a.k.a. disassemble.
Platoon engaging	Using wireless communication (V2V), the Platoon Candidate sends an engaging request. When conditions are met the system starts to decrease the time gap between the trucks to the platooning time gap. A.k.a. join platoon
Platoon formation	Platoon formation is the process before platoon engaging in which it is determined if and in what format (e.g. composition) trucks can/should become part of a new / existing platoon. Platoon formation can be done on the fly, scheduled or a mixture of both. Platoon candidates may receive instructions during platoon formation (e.g. to adapt their velocity, to park at a certain location) to allow the start of the engaging procedure of the platoon.
Platoon split	The platoon is split in 2 new platoons who themselves continue as standalone entities.
Requirements	Description of system properties. Details of how the requirements shall be implemented at system level
Scenario	A scenario is a quantitative description of the ego vehicle, its activities and/or goals, its static environment, and its dynamic environment. From the perspective of the ego vehicle, a scenario contains all relevant events. Scenario is a combination of a manoeuvre (“activity”), ODD and events
Service layer	The service layer represents the platform on which logistical operations and new initiatives can operate.
Specifications	A group of two or more vehicles driving together in the same direction, not necessarily at short inter-vehicle distances and not necessarily using advanced driver assistance systems
Steady state	In systems theory, a system or a process is in a steady state if the variables (called state variables) which define the behaviour of the system or the process are unchanging in time. In the context of platooning this means that the relative velocity and gap between trucks is unchanging within tolerances from the system parameters.
Strategic layer	The strategic layer is responsible for the high-level decision-making regarding the scheduling of platoons based on vehicle compatibility and Platooning Level, optimisation with respect to fuel consumption, travel times, destination, and impact on highway traffic flow and infrastructure, employing cooperative ITS cloud-based solutions. In addition, the routing of vehicles to allow for platoon forming is included in this layer. The strategic layer is implemented in a

Term	Definition
	centralised fashion in so-called traffic control centres. Long-range wireless communication by existing cellular technology is used between a traffic control centre and vehicles/platoons and their drivers.
Tactical layer	The tactical layer coordinates the actual platoon forming (both from the tail of the platoon and through merging in the platoon) and platoon dissolution. In addition, this layer ensures platoon cohesion on hilly roads, and sets the desired platoon velocity, inter-vehicle distances (e.g. to prevent damaging bridges) and lateral offsets to mitigate road wear. This is implemented through the execution of an interaction protocol using the short-range wireless inter-vehicle communication (i.e. V2X). In fact, the interaction protocol is implemented by message sequences, initiating the manoeuvres that are necessary to form a platoon, to merge into it, or to dissolve it, also taking into account scheduling requirements due to vehicle compatibility.
Target Time Gap	Elapsed time to cover the inter vehicle distance by a truck indicated in seconds, agreed by all the Platoon members; it represents the minimum distance in seconds allowed inside the Platoon.
Time gap	Elapsed time to cover the inter vehicle distance by a truck indicated in seconds.
Trailing truck	The last truck of a truck platoon
Truck Platoon	Description of system properties. Details of how the requirements shall be implemented at system level
Use case	Use-cases describe how a system shall respond under various conditions to interactions from the user of the system or surroundings, e.g. other traffic participants or road conditions. The user is called actor on the system, and is often but not always a human being. In addition, the use-case describes the response of the system towards other traffic participants or environmental conditions. The use-cases are described as a sequence of actions, and the system shall behave according to the specified use-cases. The use-case often represents a desired behaviour or outcome. In the ensemble context a use case is an extension of scenario which add more information regarding specific internal system interactions, specific interactions with the actors (e.g. driver, I2V) and will add different flows (normal & alternative e.g. successful and failed in relation to activation of the system / system elements).

6.1.1. Acronyms and abbreviations

Acronym / Abbreviation	Meaning
ACC	Adaptive Cruise Control
ADAS	Advanced driver assistance system
AEB	Autonomous Emergency Braking (System, AEBS)
ASIL	Automotive Safety Integrity Level
ASN.1	Abstract Syntax Notation One
BTP	Basic Transport Protocol
C-ACC	Cooperative Adaptive Cruise Control
C-ITS	Cooperative ITS
CA	Cooperative Awareness
CAD	Connected Automated Driving
CAM	Cooperative Awareness Message
CCH	Control Channel
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
DITL	Driver-In-the-Loop
DOOTL	Driver-Out-Of-the Loop
DSRC	Dedicated Short-Range Communications
ETSI	European Telecommunications Standards Institute
EU	European Union
FCW	Forward Collision Warning
FLC	Forward Looking Camera
FSC	Functional Safety Concept
GN	GeoNetworking
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GUI	Graphical User Interface

Acronym / Abbreviation	Meaning
HARA	Hazard Analysis and Risk Assessment
HIL	Hardware-in-the-Loop
HMI	Human Machine Interface
HW	Hardware
I/O	Input/Output
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITL	In-The_Loop
ITS	Intelligent Transport System
IVI	Infrastructure to Vehicle Information message
LDWS	Lane Departure Warning System
LKA	Lane Keeping Assist
LCA	Lane Centring Assist
LRR	Long Range Radar
LSG	Legal Safe Gap
MAP	MapData message
MIO	Most Important Object
MRR	Mid Range Radar
OS	Operating system
ODD	Operational Design Domain
OEM	Original Equipment Manufacturer
OOTL	Out-Of The-Loop
PAEB	Platooning Autonomous Emergency Braking
PMC	Platooning Mode Control
QM	Quality Management
RSU	Road Side Unit
SA	Situation Awareness

Acronym / Abbreviation	Meaning
SAE	SAE International, formerly the Society of Automotive Engineers
SCH	Service Channel
SDO	Standard Developing Organisations
SIL	Software-in-the-Loop
SPAT	Signal Phase and Timing message
SRR	Short Range Radar
SW	Software
TC	Technical Committee
TOR	Take-Over Request
TOT	Take-Over Time
TTG	Target Time Gap
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to any (where x equals either vehicle or infrastructure)
VDA	Verband der Automobilindustrie (German Association of the Automotive Industry)
WIFI	Wireless Fidelity
WLAN	Wireless Local Area Network
WP	Work Package