Security in Hybrid Vehicular Communication based on ITS-G5, LTE-V, and Mobile Edge Computing

Norbert Bissmeyer, ESCRYPT GmbH - Embedded Security, Bochum, Germany, Norbert.Bissmeyer@escrypt.com
Jan-Felix van Dam, ESCRYPT GmbH - Embedded Security, Bochum, Germany, Jan-Felix.vanDam@escrypt.com
Christian Zimmermann, Robert Bosch GmbH, Renningen, Germany, Christian.Zimmermann3@de.bosch.com
Kurt Eckert, Robert Bosch GmbH, Renningen, Germany, Kurt.Eckert@de.bosch.com

Abstract

Communication in a Cooperative Intelligent Transportation System needs to be protected against attacks in order to ensure trust in received data in terms of data integrity and sender authenticity. In addition, the reliability of communication channels should be considered, which is not possible with a single technology or physical channel that cannot be easily protected against radio jamming attacks. Hybrid vehicular communications using different radio technologies and channels is mainly introduced to further increase channel bandwidth and the communication range with the goal to speed up the deployment of intelligent transportation systems. However, hybrid communication could also support the reliability of communication capabilities by using the potential of redundant communication technologies. In this paper, a security concept is described to secure data in presence of multiple radio technologies using different physical channels to transmit V2X information. The security is considered for different radio-level communication technologies, i.e. direct ITS-G5 communication based on IEEE 802.11p (DSRC), device-to-device communication based on Cellular-V2X using different configurations and Mobile Edge Computing.

1 Introduction

The introduction of a Cooperative Intelligent Transportation System (C-ITS) is an enabler for increased safety on roads and future autonomous vehicle deployments. Further, traffic efficiency is intended to be increased by having smoother and more efficient traffic flow. New applications are planned in the area of driver convenience, public transportation and commercial carriage of goods. In this context, the term vehicle-to-everything (V2X) communication is used to describe real-time communication in transportation.

V2X communication is based on wireless radio technology that allows the transmission of short messages between enabled devices. Instead of using only one radio technology (ITS-G5), the 5G Automotive Association (5GAA) proposes to use cellular radio technology in addition to leverage V2X communications and to address future ITS use cases [1]. Cellular-V2X (C-V2X) radio technology considers the implementation in different broadband cellular network generations, i.e. LTE-V in 4G and future generations such as 5G.

In Section 2 the architecture of the considered C-ITS is described including the entities and communication paths. In Section 3 the radio-level communication technologies are introduced. The security requirements are summarized in Section 4 which are considered by security measures in Section 5. A conclusion is provided in Section 6.

2 Architecture of C-ITS

Several entities and systems are involved in communication in C-ITS. In this paper, we focus on a hybrid architecture that considers direct communication via ITS-G5 and C-V2X as well as indirect communication via cell tower. In Figure 1, the considered communication paths between C-ITS stations are depicted.

- The end entities in the communication are referred to as C-ITS stations, which could be in practice any kind of vehicles, roadside units, two-wheelers or pedestrians.
- The required accurate time and location information is provided by Global Navigation Satellite System (GNSS).
- The cell tower may be involved depending on the C-V2X mode.
    - In “operator managed” mode, the cell tower provides network related actions to optimize direct V2X communication by supporting with channel utilization and quality of service. The Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) is responsible for scheduling and interference management as well as synchronization and discovery. This supporting communication is performed via control signaling over the interface between C-ITS station and E-UTRAN. In the managed mode, the Public Land Mobile Network (PLMN) may also be responsible to perform access control to direct C-V2X autonomous communication by performing authorization tasks and transmitting permission parameters. [2]
    - In classical cellular mode, the cell tower provides a data interface to the Internet in order to allow connecting with backend services, a C-ITS central station or a cloud service. Depending on the use case the station might only use the uplink or only the downlink to transmit or receive data. In particular, the cellular network might be used to multicast V2X messages to multiple receivers via Multimedia Broadcast Multicast Service (MBMS). [3]

  - In a Mobile Edge Computing (MEC) scenario, the cell tower hosts a V2X service to allow local communication not routed through backbone and internet to consider scalability and low latency requirements of the V2X use cases. For example, a V2X application running on the cell tower equipment may be used to relay event-driven V2X messages in order to cover a larger area.
- A C-ITS central station may be involved in the V2X communication as data provider or consumer. For example, a central Traffic Management Center collects traffic density information in order to calculate traffic light phases or detour information.

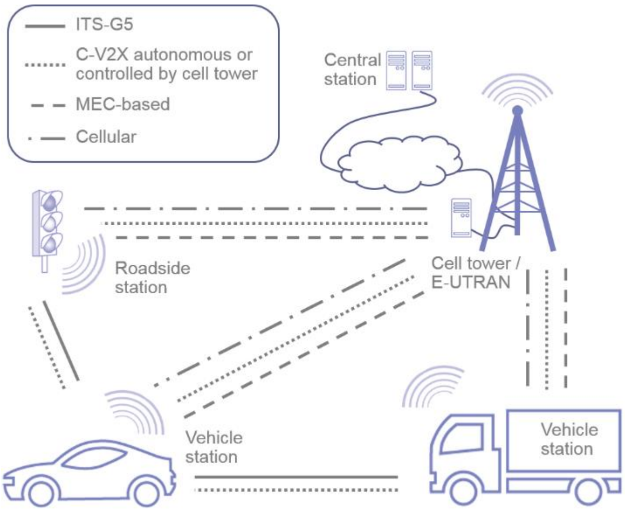

Figure 1: Hybrid V2X communications architecture

In case of autonomous V2X communication (ITS-G5 or C-V2X in “non-operator managed” mode) infrastructure components are not required for initialization and enabling end-to-end data exchange between C-ITS stations. For direct communication in C-V2X “operator managed” mode the cell tower is involved to support the direct data exchange between C-ITS stations.

3 Radio-level Communication Technologies

In a hybrid V2X communication scenario different radio technologies are used. As shown in Figure 1 the C-ITS station may communicate with a backend using the cellular network via E-UTRAN, Mobility Management Entity (MME) and S/P-Gateway. In this case the cellular radio-level technology is applied as well as the related frequencies.

More interesting is the case where the C-ITS station communicates directly with another station in range. For this case the radio frequencies in the 5.9 GHz band are foreseen as depicted in Figure 2. In this band three safety channels (G5CC, G5SC1, G5SC2) can be used for ITS road safety and traffic efficiency applications according to ETSI ES 202 663 [4]. Since there is no direct limitation with respect to radio technology, a cellular radio (C-V2X) could use them in the same way as an ITS-G5 radio.

Even both radio-level communication technologies could coexist as long as different channels are used. One could imagine that for example the channel G5SC1 with 10 MHz is used by ITS-G5, the second channel G5SC2 with 10 MHz is shared by both radios and the third channel G5CC with 10 MHz is used by C-V2X [5]. However, it should be ensured that different technologies do not interfere each other, for example by out of band emissions and that bandwidth is not wasted if same messages are broadcasted over multiple radios at the same time.

As a result, it might be reasonable to operate only one radio on the channels depicted in Figure 2.

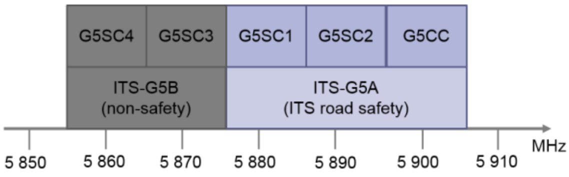

Figure 2: C-ITS frequencies according to [4]

In the following list, the four different communication channels are described that are shown in Figure 1.

- Device-to-device communication
  - via ITS-G5 based on IEEE 802.11p [6],
  - via C-V2X based on 3GPP Release 14 [2] (PC5 reference point for autonomous “non-operator managed” and “operator managed” device-to-device communication).
- Device-to-cell tower communication
  - using C-V2X based on 3GPP Release 14 [2] (V3 reference point via LTE-Uu to optimize the direct “operator managed” device-to-device communication by scheduling and other tasks),
  - via cell tower using MEC (LTE-Uu reference point for device-to-cell tower communication).

Device-to-network communication using traditional cellular links is based on LTE (LTE-Uu reference point via network gateway to provide device-to-Internet communication according to 3GPP [3]).

4 Security Requirements

ITS communication is threatened due to its open character. Each participant of road traffic including vehicles, bicycles, pedestrians, etc. should be able to send and receive trustworthy information concerning traffic safety and efficiency. According to the ETSI threat, vulnerability and risk analysis [7] most critical threats are the denial of transmission and reception of data, modification and deletion of transmitted information, masquerade of a station, and acquisition of personal information.

For all use cases, data integrity, sender authentication and authorization, replay protection, and availability is required whereas confidentiality and accountability is only required for selected use cases.

In addition, system security of C-ITS stations and cellular network equipment is identified in the 3GPP report on V2X security [3] as relevant security requirement. In the following list, the C-ITS security requirements are summarized.

- Message integrity has to be ensured in order to detect manipulations made by attackers. System and software integrity of C-ITS station equipment has to be ensured in order to protect keys, certificates and configurations against manipulation. The secure environment of the station may check the integrity of the entity's boot process.
- Authenticity and authorization of senders shall be ensured to allow only trusted systems to participate actively in C-ITS communications. The provision of authentication and authorization shall be revocable to exclude systems from C-ITS if necessary. Further, the secure environment of stations shall be protected against illegitimate access.
- Replay of valid messages has to be detected.
- Availability of C-ITS services should not be prevented by malicious activity.
- Confidentiality of V2X message content is required if a C-ITS service shall only be used by selected authorized stations. Sensitive data such as symmetric and private keys in transition and at rest shall not be exposed to external entities. Credentials for cellular network access shall reside on the Universal Integrated-Circuit Card (UICC).
- Privacy protection is required in order to prevent ITS-internal or external entities to collect personal identifying information. Neither a network operator nor a security infrastructure operator shall be able to link a pseudonymous identifier of a C-ITS station to its long-term ID. Furthermore, it shall not be possible to link different pseudonyms to the same owner. Attackers shall not be able to track a vehicle by collecting V2X messages from the wireless radio.
- Detection of malicious station behavior shall be considered in order to achieve trust and confidence in V2X messages on top of cryptographic authentication measures.

In this paper we focus on security in hybrid C-ITS. Non-security requirements such as low latency, throughput and costs need to be considered but are not further analyzed in detail.

5 Security Concept for Hybrid V2X Communication

The security concept provides security measures for all requirements listed in Section 4. An overview of existing solutions is given in Section 5.1 and detailed with focus on the security goals in Section 5.2.

5.1 Overview of Existing Security Concepts

There are at least two relevant security architectures for C-ITS that have been developed in Europe [8] and the USA [9]. The European variant is standardized by European Telecommunications Standards Institute (ETSI) [10] and is the basis for the European C-ITS Certificate Policy (C-ITS CP) [11]. In contrast, the US variant is the basis for initial deployments under control of the US Department of Transportation.

Both solutions rely on the same basic principle. Each C-ITS station owns at least one asymmetric key pair whereby the public key is part of a certificate, which is signed by a trusted Certificate Authority (CA) that is part of a Public Key Infrastructure (PKI).

For securing a V2X message, the sender is signing the message payload with its private key and transmits the signed message together with its certificate. Each receiver is then able to trust in the integrity of the message by verifying the message signature and is able to trust in the authentication of the originator by verifying the signature of the sender's certificate.

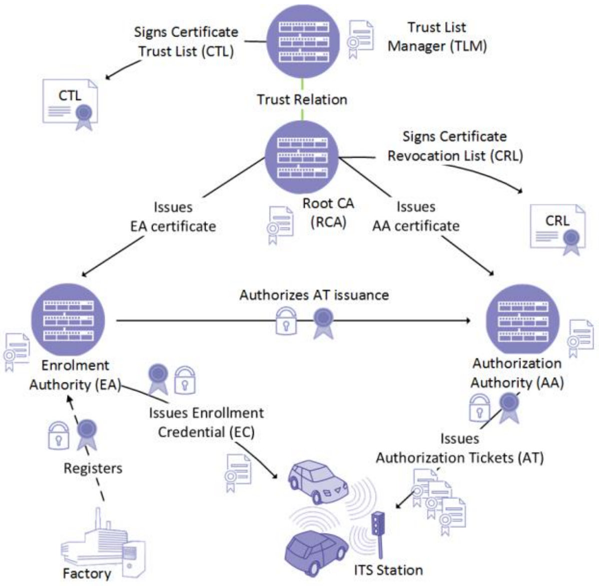

Figure 3: C-ITS Public Key Infrastructure [11]

Since this general security proceeding is harmonized in the European and US variants the formats for security header and certificate are based on the same IEEE standard [12]. In particular, the ETSI security formats [13] are described as a profile of the IEEE 1609.2 standard [12]. A V2X specialized certificate format is used to minimize the size of secured messages which contain the certificate of the sender in the security header.

Main difference between both security architectures can be found in the structure and functionality of the PKI. In this paper we focus on the European PKI variant shown in Figure 3.

The Root CA (RCA) is the trust anchor in the system. Since there might be several RCAs in C-ITS, a Trust List Manager (TLM) creates and distributes a signed Certificate Trust List (CTL) containing root certificates of trusted RCAs as well as access information to contact the RCAs from the end entities.

Each C-ITS station needs to be registered at one Enrolment Authority (EA) in order to get a valid pseudonym certificate for the V2X communication in form of an Authorization Ticket (AT). For private C-ITS stations the EA and AA need to be operated by different organizations in order to protect the station's privacy. The AA gets the request for a new AT but is not able to identify the requesters identity because the signer of the AT request can only be decrypted by the EA. After issuing an AT certificate the EA only knows that a specific trusted station has requested an AT but has never seen any content of the AT. On the other hand, the AA has issued the AT without having seen the identity of the requester.

The message protection in cellular networks is mainly based on a symmetric key architecture described in [14].

As a result, there exists a security solution for protecting the direct V2X communication between the stations (PC5 link) and for the communication between the station and the cell tower (LTE-Uu link). In the following section we propose a security concept considering the hybrid V2X communication scenario.

5.2 Security Concept Protecting Security Goals

According to the security requirements listed in Section 4 message integrity, sender authenticity and authorization, replay protection and privacy shall be ensured on all channels whenever a V2X message is transmitted. The communication stack used in a hybrid communication system could look like as illustrated in Figure 4.

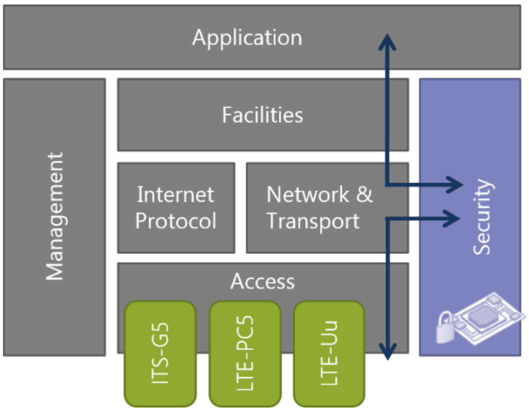

Figure 4: Hybrid V2X communication stack (European C-ITS variant)

On the sender C-ITS station the V2X message is generated on application or facilities layer and then handed over to the network & transport layer. On this layer the interface of the security component is used to include the security header into the V2X packet. A reference specification of this interface is given by ETSI [15]. Depending on the information provided by the upper layer, i.e. required sender permissions, security operation (sign / sign & encrypt), etc., the security component checks that an appropriate pseudonym certificate is loaded that can be used to sign the payload. The security layer creates a security header according to ETSI [13] including a signature over the payload, signer information in form of a digest or an AT certificate, generation time, and the payload Application ID (AID). If the confidentiality of the message payload needs to be protected the signed payload is encrypted in a second step with a symmetric key. Information about the applied symmetric key are added to the security header to allow one or multiple receivers to select the correct key for decryption. Since the encrypted message is also used to protect the privacy of the communicating end entities the message is first signed and then encrypted.

By applying security measures on network & transport layer the security goals can be fulfilled independent of the radio-level communication technology.

This security solution can also be applied to secure known hybrid communication scenarios. In the device-to-device communication over ITS-G5 or C-V2X the C-ITS station and the cell tower based roadside unit applies the ETSI ITS security [13] to secure V2X messages on network & transport layer [16]. In the device-to-cell tower communication, the end entities apply LTE security according to [14] to establish a mutual authenticated security channel based on symmetric cryptography. V2X messages sent though this channel are secured in addition with the AT certificates according to [13]. That enables end-to-end security if data is transmitted from a vehicle to an application server in the cloud where the LTE network is covering only a part of the communication. In this scenario the application server would like to verify that the V2X message was generated by a valid and trustworthy C-ITS station. In a MEC scenario where the cell tower distributes V2X messages to neighboring cells the receiving station needs to check integrity and freshness of the original message and authenticity and authorization of the originator or the message.

5.2.1 Message Integrity

Message integrity is ensured by creating a digital signature over the message payload and packet routing information using the private key related to AT certificate that is currently loaded by the sending station. The AT key pair needs to be generated, administered and stored inside a cryptographic security hardware module [11].

5.2.2 Sender Authentication

Sender authentication is given by adding the AT certificate to the security header. The receiver needs to be equipped with all root certificates which are distributed as CTL. The signature of the AT certificate can be verified with the public key contained in the certificate of the AA and the validity of the AA certificate can be checked with the public key contained in the securely stored root certificate. In case an AA certificate is not available the receiver can request the missing certificate from the sender on demand using the ETSI protocol [13].

Only trusted and certified C-ITS stations should be able to get a valid AT certificate from the PKI. In a first step the station or the communication device is registered at the EA with a non-standardized process. Subsequently, the C-ITS station generates an asymmetric key pair for an Enrolment Credential (EC) and sends an EC certificate request to the EA using an ETSI protocol [17]. The EA issues the EC certificate with a potentially long validity lifetime and replies the certificate back to the station. The EA has to ensure that only registered devices are able to request an EC and that requests from blacklisted or deactivated stations are rejected. In order to get an AT certificate from an AA, the C-ITS station is generating an asymmetric key pair, puts the public key into an AT request message according to [17] and signs it with the EC private key. The AA issues the AT certificate and provides it back to the requesting station.

A receiver of a V2X message can trust the owner of an AT as long as the related root in the certificate chain is trusted. The cryptographic algorithms ensure that only one private key can belong to an AT certificate that cannot be guessed by an attacker.

5.2.3 Sender Authorization

The authorization of the sender is considered by having encoded the sender's permission in the AT certificate in form of AIDs. Also the permissions of the AA and root can be limited by having AIDs also in their related certificates.

5.2.4 Replay Detection

Replay detection is enabled by adding a generation timestamp to the security header. Depending on the use case, a receiver can reject messages older than some seconds. For messages with longer lifetimes, the ITS station stores the hash digest of previously received messages. Incoming messages can then be compared with that list of previously received messages.

5.2.5 Confidentiality

Confidentiality can be ensured by encrypting the signed packet with a key shared with the recipient.

5.2.6 Revocation of Trust

Revocation of misbehaving or compromised C-ITS stations is enabled by using AT certificates with a short lifetime. The AA of the PKI checks that only AT certificates are issued with a relatively short validity period. In addition, AT certificates are only issued with validity for the near future. The specific parameters for private and non-private roadside stations are specified in the C-ITS CP [11].

Revocation of root certificates is done by removing the affected certificate from the CTL. An AA certificate, however, is revoked with a Certificate Revocation List (CRL) which is issued by the RCA that issued the AA certificate. As a consequence, the receiver needs to ensure that the latest CTL and CRL is used when the certificate chain from AT to root certificate is checked.

5.2.7 Privacy Protection

Privacy protection is considered by measures performed by the message sending C-ITS station, the cellular network, and the PKI.

A mobile C-ITS station, i.e. vehicle, needs to ensure that it is equipped with multiple AT certificates that are valid for the same period of time. Depending on the time and moved distance, the station changes all identifiers contained in a V2X message. In particular, the IDs added to the packet by the different layers of the communication stack need to be changed in a coordinated way together with the AT certificate. Even if most V2X messages are not encrypted, an attacker listing on the wireless channel cannot link a message to a specific person / vehicle since the V2X message does not contain identifying information. In addition, a local attacker is not able to link different pseudonyms of a station to each other since the attacker can only receive messages inside its communication range which is usually limited to a few hundred meters.

The PKI is designed in a way that no single entity is able to link a pseudonym of a station to its real or long-term identity, cf. section 5.1. To prevent that an AA can collect a list of all pseudonyms of a station, the C-ITS station changes its IP address between each request of AT certificate according to [17].

In order to protect the privacy against the Mobile Network Operator (MNO), the station can hide its real identity (International Mobile Subscriber Identity, IMSI) and change its pseudonym identity (P-IMSI) frequently by re-attaching to the E-UTRAN. As proposed by 3GPP [3], a dedicated V2X Mobile Virtual Network Operator (MVNO) can be introduced to hide the IMSI against the MNO. Only the vehicle and the Home Subscriber Server (HSS) of the V2X MVNO know the IMSI. The MNO is handling only a pseudonymous IMSI in order to perform required tasks. If a linking of IMSI and P-IMSI is required, for example for legal investigations, the MNO and MVNO have to cooperate.

For the communication between a C-ITS station and an application server in the cloud using a cellular network, end-to-end encryption with changing IDs needs to be applied [3]. For the purpose of securing the hybrid V2X communication and for protecting the driver's privacy the ETSI ITS security formats and procedures could be applied [13] [5].

5.2.8 Reliability

Ensuring the reliability of communication capabilities and channel bandwidth is challenging since an attacker can jam the channel with random noise. As discussed in Section 3, different frequency bands could be used in parallel. However, by sending the same messages on neighboring channels, valuable frequency resources would be wasted and an attacker could jam the entire 5.9 GHz band which is reserved for C-ITS.

For V2X communication without low latency requirements, messages could be transmitted via device-to-device communication using ITS-G5 or LTE-PC5 and in parallel via device-to-cell tower communication using LTE-Uu. In the latter case, the cell tower could apply the enhanced Multimedia Broadcast Multicast Service (eMBMS) to distribute V2X messages efficiently.

6 Conclusion

Securing V2X communication is essential in order to prevent attacks and ensure trust in received V2X data. For a hybrid V2X solution with different radio-level communication technologies and different modes, all security requirements need to be considered.

The security solution as specified by ETSI [10] and IEEE [12] for ITS-G5 communication can be applied without major modifications. The C-ITS station applies security measures for message protection on network & transport layer independent of the radio technology used on the access layer. The standardized PKI can be used to issue pseudonymous certificates for the ITS-G5 and C-V2X communication.

The hybrid vehicular communication has the potential of making direct and low latency data exchange more reliable without introducing additional risks from security point of view.

7 Acknowledgment

This paper is created in context of the project CONCORDA which is co-financed by the European Union's Connecting Europe Facility. The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained therein.

CONCORDA
Co-financed by the European Union
Connecting Europe Facility

8 References

[1] 5G Automotive Association, "The case for cellular v2x for safety and cooperative driving.," Online, 2016.

[2] ETSI - European Telecommunications Standards Institute, „TS 123 285 v14.4.0 - Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for V2X services (3GPP TS 23.285 version 14.4.0 Release 14),“ ETSI, 3GPP, LTE, 2017.

[3] 3rd Generation Partnership Project, „TR 33.885 - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security aspects for LTE support of Vehicle-to-Everything (V2X) services (Release 14),“ 4GPP, 2017.

[4] ETSI - European Telecommunications Standards Institute, „ES 202 663 v1.1.0 - Intelligent Transport Systems (ITS); European Profile Standard for the Physical and Medium Access Control Layer of Intelligent Transport Systems Operating in the 5 GHz Frequency Band.,“ ETSI, 2010.

[5] Qualcomm, „Accelerating C-V2X Commercialization,“ Qualcomm, 2017.

[6] IEEE Computer Society, „IEEE Std 802.11p - Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specific,“ IEEE, 2010.

[7] ETSI - European Telecommunications Standards Institute, „TR 102 893 v1.2.1 - Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA).,“ ETSI, 2017.

[8] N. Bissmeyer, J. P. Stotz, H. Stübing, E. Schoch, S. Götz und B. Lonc, „A Generic Public Key Infrastructure for Securing Car-to-X Communication.,“ in *18th World Congress on Intelligent Transportation Systems*, 2011.

[9] W. Whyte, A. Weimerskirch, V. Kumar und T. Hehn, „A Security Credential Management System for V2V Communications.,“ in *IEEE Vehicular Networking Conference (VNC)*, 2013.

[10] ETSI - European Telecommunications Standards Institute, „TS 102 940 v1.1.1 - Intelligent Transport Systems (ITS); Security; ITS Communications Security Architecture and Security Management.,“ ETSI, 2012.

[11] C-ITS Platform, „Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS).,“ European Commission, 2017.

[12] IEEE Computer Society, „IEEE P1609.2a-2017 - IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages.,“ Institute of Electrical and Electronics Engineers, 2017.

[13] ETSI - European Telecommunications Standards Institute, „TS 103 097 v1.3.1 - Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats.,“ ETSI, 2017.

[14] ETSI - European Telecommunications Standards Institute, „TS 133 401 V14.4.0 - Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 14.4.0 Release 14),“ ETSI, 2017.

[15] ETSI - European Telecommunications Standards Institute, „TS 102 723-8 - Intelligent Transport Systems (ITS); OSI Cross-Layer Topics; Part 8: Interface between Security Entity and Network and Transport Layers.,“ ETSI, 2013.

[16] ETSI - European Telecommunications Standards Institute, „EN 302 636-4-1 v1.3.1 - 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.,“ ETSI, 2017.

[17] ETSI - European Telecommunications Standards Institute, „DRAFT TS 102 941 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management,“ ETSI, 2018.