# Securing the C-ITS: a PKI Perspective

**Ștefan-Ciprian ARSENI[1,2], Dan AVRAM[1], Mirabela MEDVEI[1,3], Mihai TOGAN[1], Andrei DIMA[1,3]**
[1]Faculty of Information Systems and Cyber Security, "Ferdinand I" Military Technical Academy, Bucharest
[2]Faculty of Electronics, Telecommunications and Information Technology, University "Politehnica" of Bucharest
[3]Faculty of Automatic Control and Computer Science, University "Politehnica" of Bucharest
stefan.arseni@mta.ro, dan.avram@mta.ro, mirabela.medvei@mta.ro,
mihai.togan@mta.ro, andrei.dima@mta.ro

**Abstract**: Emergent technologies have led to significant improvements in many industry sectors and, sometimes, facilitated the rapid adoption of these technological advances in different layers of society. The automotive industry, an important one for society and the economy, has seen many advances in the past few years. Through the slow integration of technology and algorithms, basic vehicles transformed into "intelligent" systems, capable of increasing the safety and reliability of transportation. These systems, called ITS (Intelligent Transport Systems), are now close to entering a new phase, one where ITS will communicate with each other and collaborate to ensure a higher degree of passenger safety, improve traffic management and provide means of "smarter" planning for goods transports. Yet, before entering this new phase, entitled C-ITS (Collaborative ITS), enforcing security mechanisms is a top priority. One solution, considered a good starting point for future developments of security aspects, is the use of a custom PKI (Public Key Infrastructure) that can ensure authenticity and user privacy in the context of C-ITS. In this paper, we present how the PKI is tailored, from the architectural point of view, to suit the C-ITS requirements and how this effort is supported by standards and legislation, with a focus on the proposal made by the European Union. We also highlight the main message flows that any car manufacturer will need to be compliant with, in the same scenario of the EU proposed C-ITS PKI.
**Keywords:** C-ITS Security, PKI, ETSI PKI Architecture

## INTRODUCTION

Benefiting from the continuous advances seen in the majority of IT&C areas, transport systems have been a key subject in recent technology presentations, where vehicle manufacturers tried to implement as many technical advances as possible. IoT (Internet of Things), one of the buzzwords of recent years, has been the primary element that empowered innovation in many industries, and the automotive industry is one of them. By adapting the means of communication that IoT proved to be efficient in different environments, vehicles can now become intelligent and connected, aware of their surroundings and able to communicate with other vehicles that have similar features.

Defined in (European Union, 2010) as hybrid entities (a hardware component, represented by the vehicle, and a software component, represented by algorithms providing a form of "intelligence") that can improve the reliability and safety of transportation, Intelligent Transport Systems (ITS) are

viewed as an important step in the future of transportation. This direction has been taken into consideration not only by the EU, but also by the majority of states around the world, thus the need for a common framework of standards and means of interaction needs to be established and provided. Standardization efforts have been consistent over the past years, as described in one of the following sections, and some of them have taken into account the need of ensuring a sufficient level of security and privacy in this new "smart" network of ITS.

While ITS embed technologies to construct intelligent vehicles or other equipment that can provide sufficient data for an operator to make competent decisions, the next step is to enable ITS to communicate between each other, thus opening the way to novel applications and capabilities. This step is represented by C-ITS (Collaborative ITS). To better express the improvement that C-ITS can provide over disconnected ITS, consider the following situation: in case of an accident on the motorway, ITS can provide rapid and sufficient data to the traffic operator, who will then try to signal the traffic interruption to other drivers; this can take from a few seconds (if there are some types of automated response and control mechanisms implemented) to a few minutes (in case an operator needs to spot and report the accident, then follow-up based on a specific procedure); C-ITS will enable vehicles to communicate between themselves, thus not only will the drivers be notified rapidly of the situation in front of them, but, also, the vehicle could automatically reduce its cruising speed, providing the driver more time to safely react. Similar to this example, there are many others, ranging from passenger safety or reckless driving to detecting contraband or avoiding disasters.

As with any other new technology or concept, ITS and C-ITS can provide many improvements, but, in order to securely benefit from them, their embedded security mechanisms need to be tailored to this type of applications, for providing, especially, data confidentiality and user privacy.

## SECURITY OF ITS AND C-ITS

Both components of the ITS or C-ITS, namely the vehicle and the roadside units, are susceptible to physical or cyber-attacks, thus security has to be a primary factor when designing the architecture of these systems. News that report the hacking of several brands of ITS, starting with traditional car manufacturers (such as BMW (Zorz, 2018), Hyundai (Cimpanu, 2019), Mercedes Benz (Kovacs, 2020) or Jeep (Greenberg, 2015) and ending with newer manufacturers (the most visible one is Tesla (Winder, 2020)), have appeared at an increasing rate in the past years. With the migration towards a functional C-ITS, security mechanisms need to be included in deeper layers than before, inside the vehicle control unit. In the context of ITS, this is represented by the OBU (On-Board Unit).

There are many research articles that have followed the advances in ITS/C-ITS and analyzed them from a security perspective. Zhao, Walker & Wang (2012), Hamida, Noura & Znaidi (2015) and Harvey & Kumar (2020) assess the security challenges introduced by the ITS and present several approaches that can eliminate the security risks or limit their impact on the entire system. Besides the OBU, security design needs to cover also the communication channels that, from the C-ITS perspective, can be layered into: DSRC (direct shot-range communications), V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), V2P (vehicle-to-pedestrian) or V2X (vehicle-to-anything). Thus, security algorithms need to ensure data confidentiality not only "at rest", but also "in transit".

Kelarestaghi, Foruhandeh, Heaslip & Gerdes (2019) have addressed the problem of in vehicle networks, formed as VANETs (Vehicular Ad-hoc Networks) and consisting of communication between the main control unit and other secondary control units

specialized on a specific task (e.g.: steering, braking or airbag). For a better understanding of the vulnerabilities and their impact on the entire ITS, they have used a risk assessment methodology proposed by the US National Institute of Standards and Technology (NIST).

Focusing on user privacy, a challenge that ITS need to prioritize as much as data confidentiality, Lang & Schreiner (2015) propose the implementation of advanced access control mechanisms, based on proximity, filtering and attributes, and different policy enforcing components. On the same topic, Chavhan et al. (2020) present a policy-based privacy preservation scheme in the context of ITS used in a metropolitan area for public transportation. Addressing the means of how depot staff interact with these ITS, the proposed privacy preservation scheme consists of three levels, depending on where an employee is in the depot staff hierarchy.

Moving from the localized communications inside the ITS to the V2X communications between multiple ITS, in the C-ITS perspective, a new security approach needed to be identified. If we consider ITS as modern computers with access to different networks, then a solution for ensuring device authentication and the means of securely exchanging security elements (for ensuring user privacy and data confidentiality), could be the PKI (Public Key Infrastructure). This solution was chosen by nations worldwide, with the European Union and United States of America being the main promoters of it, having also formed working groups and initiated standards and regulations to ease the adoption and ensure the interoperability between car manufacturers and national C-ITS infrastructure. Several papers have either assessed the performance of a PKI in the C-ITS domain, as presented in (Haidar, Kaiser, Lonc & Urien, 2019), or proposed methods for reducing the number of security elements required by an ITS, as presented in (Fouchal, 2019), or for securing the requests that ITS is making in the PKI, as presented in (Monteuuis et al., 2017).

## THE PUBLIC KEY INFRASTRUCTURE

Designed as an architecture that provides trust and proof of identity in an environment that uses public key cryptography, the PKI (Public Key Infrastructure) offers the means to enable authentication, integrity, confidentiality and non-repudiation, as mentioned in (Adams & Lloyd, 2003). In RFC 3647 (Chokhani, Ford, Sabett, Merrill & Wu, 2003), this definition is enforced by introducing the notion of a public-key certificate as a mean of binding an entity (user, organization, device or digital service) to its digital entity, a set of personal information and a public key (the private key is kept secret by the entity), that are validated by a universally trusted third-party, known as a CA (Certification Authority).

The design of the PKI implies a central repository, managed by a CA, that contains certificates of each entity that requested such a security element. Given the multitude of digital identities that a single CA would need to issue in order to ensure the functioning of the Internet-based business, the PKI architecture has been divided into three main components:

- EE - the End Entity, defines the entity that requires a digital certificate to offer or obtain access to different Internet-based services;
- CA and Sub-CAs - the Certification Authorities, create a hierarchical structure, starting with the globally trusted CA that empowers secondary CAs (Sub-CAs) to issue certificates to entities. These Sub-CA are often national or state CAs that are acknowledged as a trust service provider after passing a series of audits and validations.
- RA - the Registration Authority, defines a specific element of the PKI that is closely linked to a CA. It validates the information that an EE has submitted in its certificate request and, if everything is vetted, emits a digital certificate and sends it to the CA for signing.

The structure of the digital certificate, the security element that bounds a public key to its owner, is defined in (ITU-T, 2019) and primarily contains:

- Information related to the certificate - version number, serial number, validity, value of the digital signature applied by the CA on the certificate;
- Information related to the entity it is bound to - subject name, subject public key info;
- Information related to the CA that created and signed the certificate - issuer name, digital signature algorithm used to sign the certificate.

If the certificate has expired or it has been revoked, for motivated reasons, a CRL (Certificate Revocation List) update is issued by the CA that issued that certificate. Specific protocols are used to retrieve a certificate from the CA repository (e.g.: LDAP protocol) or query the revocation status of a certificate from a CA (OCSP protocol). In the majority of use cases, the entity that offers services through a secured communication channel, will also provide its digital certificate to the user accessing its service.

## USING PKI TO SECURE THE C-ITS

In the context of C-ITS, the PKI has been adapted to comply with the security constraints introduced by this new concept, while the digital certificate has some variations, depending on where and by whom it is used. In this section we will try to offer an overview of how the PKI is structured in the C-ITS context, how it is supported in standards and how it is enabling information flows in an C-ITS environment.

**The standardization effort**

Being a topic of interest for many states, standardization efforts have been intense in the past years, trying to ease the process of integrating C-ITS in different industries and aspects of society, while ensuring car manufacturers of compatibility between their ITS and the national "smart" infrastructures or enforcing interoperability measures. Leaders in this regard, standardization entities in the EU and US have introduced several standards that address how communications are established between IS, how the PKI is structured or what are the primary data flows between entities in the PKI.

*ETSI standards*

ETSI (European Telecommunications Standards Institute), as one of the main standardization bodies of the EU, has developed a series of documents, each one of them approaching a specific part of the C-ITS. Figure 1 presents an overview of these ETSI standards related to ITS security in the C-ITS context.

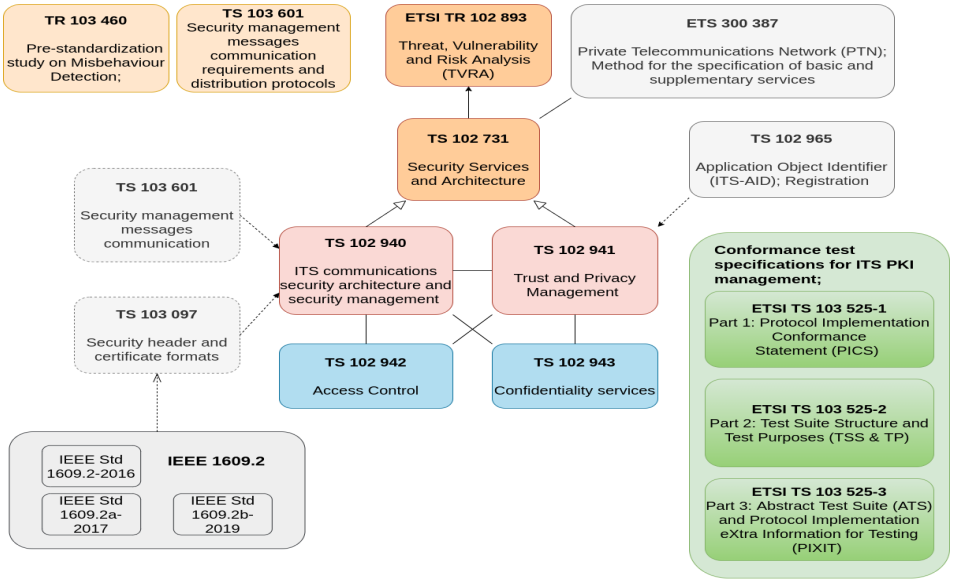


***Fig.1:*** *Overview of ETSI standards related to ITS security*

A better overview of the ETSI standards that regulate the functionality of a PKI can be achieved after a deep understanding of the following standards:

- ETSI TS 102 731 (ETSI, 2010) - describes the security services and security architecture of ETSI ITS-S (ITS Station).
- ETSI TS 102 940 (ETSI, 2018) - contains the detailed architecture for Intelligent Transportation Systems based on reference architecture in ETSI TS 102 731.
- ETSI TS 102 941 (ETSI, 2021) - based on the security services defined in ETSI TS 102 731 and the architecture in ETSI TS 102 940, the document presents the services needed to establish and maintain identity and cryptographic keys.
- ETSI TS 103 097 (ETSI, 2020a) - describes the format of data structure, of the transmitted messages and certificates.
- ETSI TS 102 942 (ETSI, 2012a) - specifies authentication and authorization services for ITS services access as well as the services required for security and privacy of the transmitted messages.
- ETSI TS 102 943 (ETSI, 2012b) - presents information privacy assurance services.

ETSI TS 102 940 presents the basic architecture for ITS communications and identifies the functional entities required for communication security. It also identifies the security services an ITS-S should implement to communicate securely. It also identifies the functional entities and the services and interfaces they should provide to support the life-cycle management of Trusted C-ITS Stations.

ETSI TS 102 941 describes the main entities needed to assure trust and privacy management inside the C-ITS system. There are presented the roles of these entities, the types of messages they exchange in order to obtain different types of certificates, the format of these messages and how data should be encapsulated and encrypted/signed.

ETSI TS 103 097 specify the structure of a certificate with all the fields needed and what these fields should contain. The format of the certificates is closely related with the format described in IEEE Std 1609.2 (IEEE, 2016) with some defined constraints. The standard also defines the format of various types of messages the ITS-S may use, like CAM, DENM, etc. The standard comes with ASN.1 modules that can be used to implement the elements it discusses.

*IEEE standards*

One of the most relevant directions for C-ITS standards is represented by the IEEE with its working groups on 1609 (IEEE, 2016) and 802.11 (IEEE, 2010). IEEE 802.11 provides specifications regarding wireless connectivity of stations within a local area. It describes one medium access control (MAC) and several physical layer (PHY) specifications. On the other hand, the IEEE 1609 family of standards presents a group of protocols for wireless access in vehicular networks (WAVE - Wireless Access in Vehicular Environments). It provides the architecture, mechanisms, suite of protocols and interfaces used to develop V2V and V2I communications. IEEE 1609 is organized as follows:

- IEEE 1609.0 - provides a description of the WAVE system architecture and operations.
- IEEE 1609.1 - describes the resource allocation entity (WAVE Resource Manager) and all the services provided by it.
- IEEE 1609.2 - defines the security algorithms and mechanisms regarding vehicular environment. Moreover, the standard presents secure message formats and methods to secure management and application messages in a WAVE architecture. The major security requirements identified in IEEE 1609.2 are: authenticity, authorization, integrity and non-repudiation. For authentication, the standard presents the use of implicit and explicit certificates.
- IEEE 1609.3 - presents the network and transport services of the WAVE protocol, including addressing and routing. It also specifies the WAVE Short Message Protocol (WSM). Furthermore, this standard defines

the Management Information Base (MIB) for the WAVE protocol stack.

- IEEE 1609.4 - illustrates multi-channel operations that provide enhancements to IEEE 802.11 Media Access Control (MAC) to support WAVE operations.
- IEEE 1609.12 - provides the description of WAVE Provider Service ID (PSID).

Figure 2 illustrates the stack of protocols in the IEEE WAVE architecture that consists mainly of the IEEE 1609 family of standards, accompanied and extended by various other standards, like IEEE 802.11p. As can be seen in Figure 2, the access to the communication channels is controlled by IEEE 802.11p and IEEE 1609.4. The WAVE stack supports applications that are based on both IPv6 and WSMP. The security services are managed in 1609.2 and the management component is specified in 1609.3.

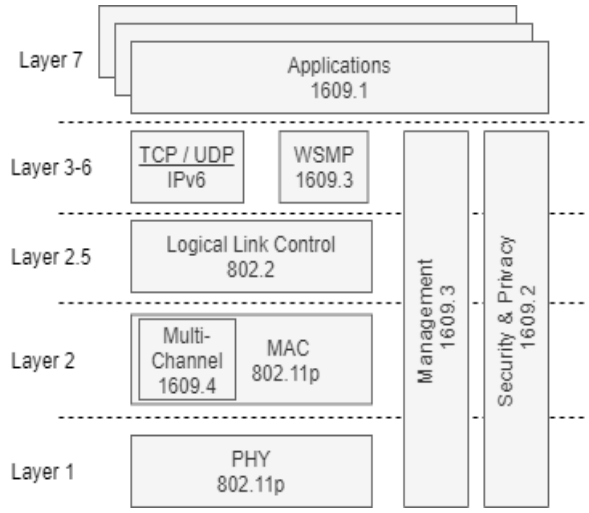


***Fig.2:*** *IEEE WAVE protocol stack*

From a PKI perspective, the 1609.2 standard is of particular interest. It consists of a detailed description given in (IEEE, 2016) and the two amendments (IEEE, 2017, 2019). The security services presented in IEEE 1609.2 are divided into two major components, namely: WAVE Internal Security Services and WAVE Higher Layer Security Services. Each component is further subdivided into two other components, as follows:

1. WAVE Internal Security Services

- Secure data service (SDS) - deals with the transformation of non-secure data units (Protocol Data Units - PDUs) into secure data units (Secured Protocol Data Units - SPDUs), as well as the reverse process. PDUs are datagrams that are transferred between SDEE (Secure Data Exchange Entity) instances.
- Security management - the Security Services Management Entity (SSME) stores certificates and certificate information.

2. WAVE Higher Layer Security Services

- Certificate revocation list (CRL) verification entity (CRLVE) - this entity is responsible for processing and storing the received CRLs.
- Peer-to-peer certificate distribution (P2PCD) entity (P2PCDE) - allows peer-to-peer certificates distribution.

*Other standards*

Besides the standards issued by ETSI (in EU) and the IEEE (in the US), there are also other organizations that contributed with proposals to the effort of defining a common framework for implementing C-ITS worldwide. Therefore, the following organizations have proposed a series of standards regarding the implementation and security of C-ITS systems:

1. SAE (Society of Automobile Engineers), an organization based in the US, has issued two notable standards regarding C-ITS:

a. SAE J2945/X (SAE International, 2017) - is a set of standards consisting of 12 standards, addressing requirements for different C-ITS use-cases and establishing a basic set of messages and parameters of DSRC communications, thus ensuring a certain level of interoperability. The individual standards included in this set are the following:

I. SAE J2945/1 - On-Board System Requirements for V2V Safety Communications;

II. SAE J2945/2 - DSRC Performance Requirements for V2V Safety Awareness;

III. SAE J2945/3 - Requirements for V2I Weather Applications;

IV. SAE J2945/4 - DSRC Messages for Traveler Information and Basic Information Delivery;

V. SAE J2945/6 - Performance Requirements for Cooperative Adaptive Cruise Control and Platooning;

VI. SAE J2945/9 - Vulnerable Road User Safety Message Minimum Performance Requirements;

VII. SAE J2945/10 - Recommended Practices for MAP/SPaT Message Development;

VIII. SAE J2945/11 - Signal Preemption Related;

IX. SAE J2945/12 - Traffic Probe Use and Operation.

b. SAE J2735 (SAE International, 2020) - defines a set of messages and data frames that can be integrated in applications using 5.9 GHz DSRC communications channels. Messages defined in this standard are used in the SAE J2945/X standards, according to the specific use-case that the standard covers.

2. ARIB (Association of Radio Industries and Businesses), an organization based in Japan, issued the ARIB STD-T109 standard. This standard defines a communication framework that enables roadside-to-vehicle (V2I) and vehicle-to-vehicle (V2V) data exchanges. As an extent to the V2I application, the standard offers means to create infrastructure-to-infrastructure (I2I) message flows, with the purpose of enhancing the infrastructure. It covers mainly the data transmission aspects of a C-ITS environment, offering few details regarding the security aspects, more specifically about the use of a PKI or similar infrastructure.

**Generic high-level architecture**

In the standards issued by ETSI and mentioned in the previous section, a generic overview of the PKI was formed and the main elements of it were mentioned in the brief description of the standards. As presented in figure 3, in contrast to the classic PKI implementation, the C-ITS PKI implements three types of certificate authorities:

- Root-CA - generates and signs the certificate of the other authorities;
- Enrollment Authority - emits long term certificates;
- Authorization authority - emits short-term pseudonym certificates.

Also, the certificates differ, because the system should permit ITS-S (ITS-Station) authorization while also protecting its real identity. Because of that, the PKI should manage a new type of certificates (authorization tickets) with anonymous identity which should be used by the ITS-S for a single action (given that the ITS-S has the permission to execute that action), using the AT for securing communication and as proof of authorization.

The EA will emit a long term certificate (EC) which will include the real identity of the ITS-S and will be used to request short-term certificates (AT) from AA.

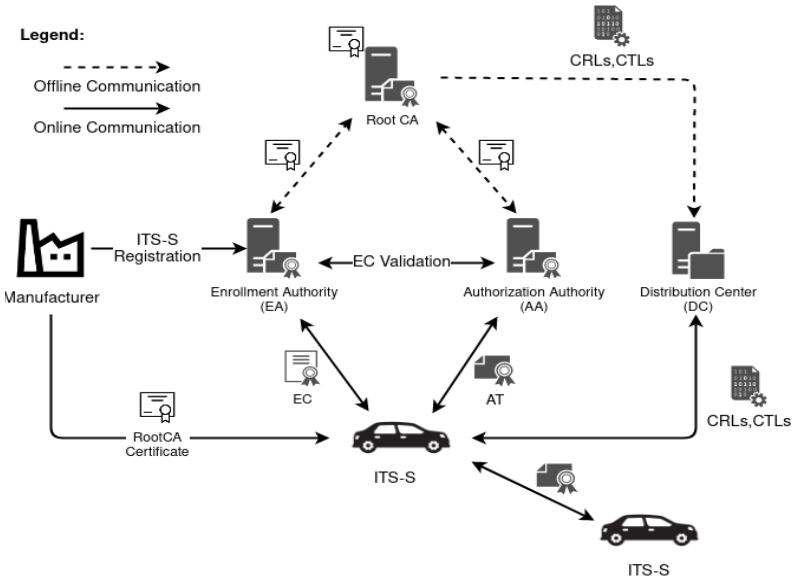


***Fig.3:*** *High level architecture of the PKI environment in the C-ITS context*

In accordance with ETSI (2018), the proposed PKI system has the following entities:

1. **Root Certificate Authority (Root-CA)**: is the entity of the proposed PKI system providing the root of trust for the PKI hierarchy. The Root-CA performs the following technical functionalities:
   a. Generation of the signing key-pair for Root-CA and its self-signed certificate;
   b. Registration of subordinate CAs (EA and AA);
   c. Generation of Certificate Trust List (CTL) and of Certificate Revocation List (CRL);
   d. Publishing CRLs and CTLs in the Distribution Center (DC);
   e. Logging of the performed operations for audit purposes.
2. **Distribution Center (DC)**: ensures the access to CRLs and CTLs to all actors in the ITS system.
3. **Enrolment Authority (EA)**: emits identity proof as Enrollment Certificates (ECs) to ITS-S. This certificate is needed for authentication to an Authorization Authority and obtaining Authorization Tickets. It has the following functionalities:
   a. The initial registration of ITS by the manufacturer;
   b. Issues Enrollment Certificates as response to an Enrollment Request (ER);
   c. Manages the permissions of ITS-Ss;
   d. Revocation of Enrollment Certificates;
   e. Logging of the performed operations for audit purposes.
4. **Authorization Authority (AA)**: has the following functionalities:
   a. Issues Authorization Tickets to ITS-Ss;
   b. Integrates with Enrollment Authority to validate the Authorization Request (AR).

The Trust List Manager (TLM) is a unique entity that is responsible for issuing and managing the ECTL (European Certificate Trust List), reception of Root-CA certificates from the CPOC entry, signing and distribution of the ECTL.

The **C-ITS Point of Contact** (CPOC) is a unique entity appointed by the C-ITS Certificate Policy Authority and is responsible for "establishing and contributing to the secure communication exchange between all entities of the C-ITS trust model, reviewing the procedural change requests and recommendations submitted by other trust model participants and transmitting the Root-CA certificates to the Trust List Manager" (JRC Technical Reports, 2019).

The PKI should support integration with the CPOC system. The Root-CA is able to carry out three main flows with the CPOC system: adding a new root certificate, adding a new root certificate with linkage to previous root and revocation of the Root-CA certificate.

**Message flows in the C-ITS PKI**

The messages exchanged inside the C-ITS system may be classified in two categories: messages exchanged at the high level of the PKI, which includes the messages exchanged between authorities, and messages exchanged with the ITS-S to ensure the access and secure communication between different ITS-Ss inside the C-ITS system. All these messages and their format are defined in the ETSI standards (ETSI, 2021).

*Messages exchanged at the upper level of the PKI*

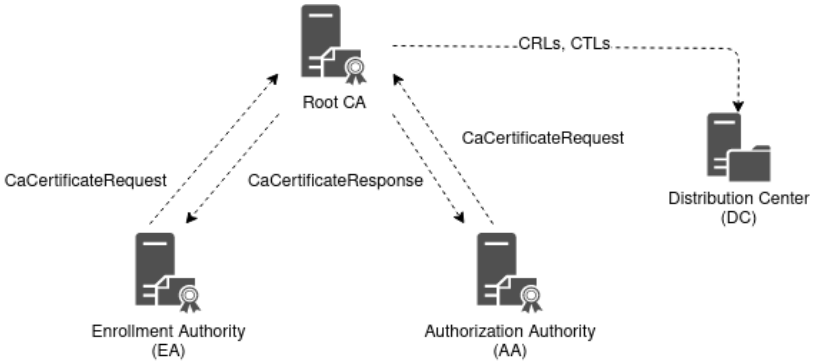


***Fig.4:*** *Messages Exchanged with Root Certificate Authority*

Figure 4 presents the message flows that are found in the upper level of the PKI, involving entities that are under a strict control and supervision by the EU committees. In order to fulfill their roles inside the PKI, the Root-CA, EA and AA must have a proof of identity. This is ensured through CA Certificates emitted by the Root-CA.

The Root-CA will be authenticated through a self signed certificate that will be loaded inside the ITS-S in the manufacturing process. In order to be authenticated in the system, EA and AA have to obtain a certificate from the RootCA. Each Subordinate CAs (Sub-CAs - EA and AA) generate a CaCertificateRequest (as defined in ETSI ETSI TS 102 941 V1.4.1, section 6.2.1) and then send it to the Root-CA. After approval, the Root-CA will generate the certificate and provide it to the corresponding Sub-CA. For subsequent requests, the Sub-CA should send a CaCertificateRequest for re-keying, which is similar to the first request but it is also signed with the current valid private key.

The communication between the Root-CA and the Distribution Center (DC) consists in the offline transmission of the CRLs and CTLs.

*Messages exchanged with the ITS-S*

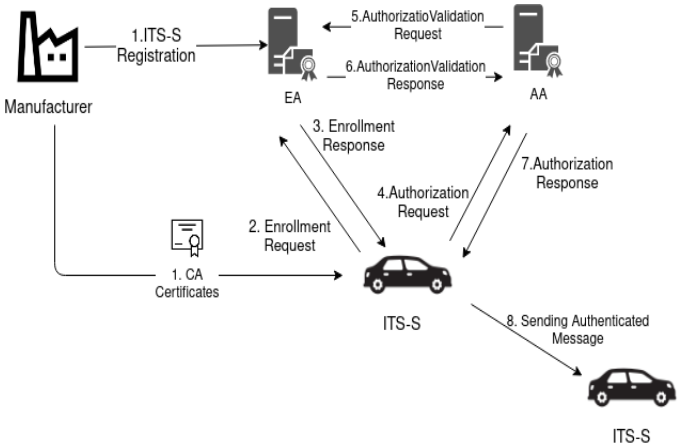


***Fig.5:*** *ITS-S steps to establish secure communication with other ITS-Ss*

For an ITS-S to be able to communicate with another ITS-S (vehicle or road-side unit) it has to obtain an *Authorization Ticket* which will be included in any future exchanged message, so that it can be authenticated. This flow is presented in figure 5.

The first step consists in registering the ITS-S by the manufacturer with an EA to which it provides information about the vehicle, including its *public key*. The vehicle is also provided with a list of certificates (Root-CA, EA, AA) and the address of these entities in order to contact and authenticate them. Next, the vehicle sends an *EnrollmentRequest* message to the EA in order to obtain a *long term certificate* needed for later authorizations. After validation of the request, EA emits an *Enrollment Certificate* (EC) and sends it to the ITS-S inside an *EnrollmentResponse* message.

After enrollment, the ITS-S may proceed to obtain an *Authorization Ticket* (AT) needed to obtain specific permissions inside the C-ITS. To achieve this, the ITS-S has to send an *AuthorizationRequest* to the AA which has to contain the *Enrollment Certificate* (EC) obtained previously.

When the AA receives the request, it contacts the EA in order to verify the ownership and validity of the EC. This is realised by sending an *AuthorizationValidationRequest* to the EA which responds with an *AuthorizationValidationResponse*. If the EC is valid and the ITS-S has the needed permissions, the AA will generate a corresponding certificate (AT) and send it to the requesting ITS-S inside an AuthorizationResponse message.

After obtaining the AT, the ITS-S may proceed to communicate with other entities using signed/encrypted messages and authenticate itself with the AT.

It has to be noted that the ITS-S can request from the DC the *Certificate Trust List* containing the

CA certificates issued by the Root-CA and the access points of its subordinate EAs and AAs and the *Certificate Revocation List* (CRL) containing the self-revoked certificate of the Root-CA, and/or the revoked CA certificates of subordinate EAs and AAs.

## CONCLUSIONS

Among other industries, the automotive one presented some major innovations in these past few years, the most notable ones being related to the transformation of regular vehicles into "intelligent" systems (ITS) that can automatically intervene in the driving act in case of an emergency, thus ensuring passenger and road safety, as well as transport efficiency, through economy of fuel, for instance. Moving forward, the next phase in the ITS evolution is to make them able to securely collaborate, therefore increasing the level of safety and reliability that passenger or goods transportation offer to their users. In this direction, efforts have been made worldwide to design communication and security frameworks that will ensure a desired level of interoperability between car manufacturers and compatibility with the national "smart" infrastructures. In this regard, the EU and US can be considered leaders, by proposing several standards and technical guidelines and, also, by organizing several projects and workshops to test the interoperability of actual ITS-S. In this paper we focused on the custom PKI architecture that is proposed by the EU in several standards issued by ETSI.

The discussed architecture is meant to solve some of the ITS-S security concerns including authentication of the C-ITS entities, authorization of performing specific actions, message confidentiality and the privacy of the ITS-Ss in the system, through pseudonymous certificates (AT).

Given that the PKI architecture is used to ensure security on the Internet and the fact that, in the last couple of years, many standardization entities (ETSI, IEEE) published several standards regarding security schemes based on certificates, it looks like this could be the technology powering the security of the C-ITSs of tomorrow. The ETSI technical specifications are a good starting point for developing a PKI solution as they present the entities needed, their roles, the message flow between actors and the description of data structures needed for implementation. Aside from these, there are many pilot projects implementing the security architecture discussed earlier. ESCRYPT launched a pilot public key infrastructure for the CAR 2 CAR Consortium (C2C-CC) to be used by its members, for tests (ESCRYPT, 2019). The project respects the ETSI technical specifications and can emit enrollment certificates and pseudonymous short-term certificates as specified in ETSI TS 102 941. There are also other projects like Microsec V2X PKI (Microsec, 2020) and TeskaLabs SeaCat PKI (TeskaLabs, 2021), indicating that the solution is promising. A plugtest was organized in 2020 (ETSI, 2020b) to test the interoperability between ITS stations and PKI vendors (ESCRYPT, MICROSEC, TESKA LABS, etc), assess the level of interoperability and validate the understanding of ETSI security standards. The participant companies from automotive sectors also ran conformity tests to assess their compliance with ETSI specifications (ETSI, 2020c).

It is clear that there are many entities interested in this solution and that steps are being taken towards a PKI security solution for the automotive industry. Still, the PKI will represent only the backbone of the final and viable security framework, the remaining elements being filled in by different security mechanism that can guarantee the safety of the private keys, can generate secure cryptographic keys (depending of the use case) or can ensure data confidentiality "at rest" or "in transit". Therefore, future research directions could be focused not only on increasing the performance of the PKI, but also on how it can be complemented with other security measures and procedures, in order to achieve a secure environment for C-ITS.

**AKNOWLEDGEMENTS**

This work was supported by a grant of the Romanian Ministry of Research and Innovation, CCCDI – UEFISCDI, project number PN-III-P2-2.1-PTE-2019-0817 / Advanced Security Mechanisms for Autonomous Systems (MASSA), within PNCDI III.

**REFERENCE LIST**

Adams, Carlisle & Lloyd, Steve (2003). "Understanding PKI. Concepts, Standards, and Deployment Consideration", Second Edition, Addison-Wesley Professional, ISBN 9780672323911.

Chavhan, S., Gupta, D., Garg, S., Khanna, A., Choi, B. J. & Hossain, M. S. (2020). "Privacy and Security Management in Intelligent Transportation System," in IEEE Access, vol. 8, pp. 148677-148688, DOI: https://doi.org/10.1109/ACCESS.2020.3015096

Chokhani, S., Ford, W., Sabett, R., Merrill, C. & Wu, S. (2003). "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647. Available at:
https://www.ietf.org/rfc/rfc3647.txt

Cimpanu, Catalin (2019). "BMW and Hyundai hacked by Vietnamese hackers, report claims", ZDNet digital magazine. Available at:
https://www.zdnet.com/article/bmw-and-hyundai-hacked-by-vietnamese-hackers-report-claims/

ESCRYPT (2019). "CAR 2 CAR: New pilot PKI complies with latest security standards", 15 May 2019. Available at:
https://www.escrypt.com/en/news-events/car-2-car-new-pilot-pki-complies-latest-security-standards

ETSI (2010). "Intelligent Transport Systems (ITS);Security;Security Services and Architecture", Technical Specification: TS 102 731 V1.1.1 (2010-09). Available at:
https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf

ETSI (2012a). "Intelligent Transport Systems (ITS); Security; Access Control", Technical Specification: TS 102 942 V1.1.1 (2012-06). Available at:
https://www.etsi.org/deliver/etsi_ts/102900_102999/102942/01.01.01_60/ts_102942v010101p.pdf

ETSI (2012b). "Intelligent Transport Systems (ITS); Security; Confidentiality services", Technical Specification: TS 102 943 V1.1.1 (2012-06). Available at:
https://www.etsi.org/deliver/etsi_ts/102900_102999/102943/01.01.01_60/ts_102943v010101p.pdf

ETSI (2018). "Intelligent Transport Systems (ITS);Security; ITS communications security architecture and security management", Technical Specification: TS 102 940, V1.3.1 (2018-04). Available at:
https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

ETSI (2020a). "Intelligent Transport Systems (ITS); Security; Security header and certificate formats", Technical Specification: TS 103 097 V1.4.1 (2020-10). Available at:
https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.04.01_60/ts_103097v010401p.pdf

ETSI (2020b). Sophia Antipolis, "ETSI C-V2X Plugtest achieves interoperability success rate of 94%", 18 August 2020. Available at:
https://www.etsi.org/newsroom/news/1810-etsi-c-v2x-plugtest-achieves-interoperability-success-rate-of-94

ETSI (2020c). "ETSI Plugtests Report", V1.1.0(2020-08). Available at:
https://portal.etsi.org/Portals/0/TBpages/CTI/Docs/2nd_ETSI_C-V2X_Plugtests_Report_v1.0.0.pdf

ETSI (2021). "Intelligent Transport Systems (ITS);Security; Trust and Privacy Management", Technical Specification: TS 102 941 V1.4.1 (2021-01). Available at:
https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.04.01_60/ts_102941v010401p.pdf

European Union, "Directive 2010/40/EU of the European Parliament and of the Council on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport", 7 July 2010. Available at:
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040&from=EN

Fouchal, H. (2019). "Privacy Protection with Less Certificates in C-ITS," 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, pp. 1046-1050, DOI: https://doi.org/10.1109/ISCC47284.2019.8969729

Greenberg, Andy (2015). "Hackers Remotely Kill a Jeep on the Highway—With Me in It", Wired digital magazine. Available at:
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Haidar, Farah, Kaiser, Arnaud, Lonc, Brigitte & Urien, Pascal (2019). C-ITS PKI protocol: Performance Evaluation in a Real Environment. WONS 2019 15th Wireless On-demand Network systems and ServicesConference, Jan. 2019, Wengen, Switzerland. (hal-01978179)

Hamida E. B., Noura H. & Znaidi, W. (2015). Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures. Electronics, 4(3):380-423. https://doi.org/10.3390/electronics4030380

Harvey, J. & Kumar, S. (2020). "A Survey of Intelligent Transportation Systems Security: Challenges and Solutions," 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 2020, pp. 263-268, DOI: https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00055

IEEE (2010). "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," in IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009), pp. 1-51, 15 July 2010, DOI: https://doi.org/10.1109/IEEESTD.2010.5514475

IEEE (2016). "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages," in IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1-240, 1 March 2016, DOI: https://doi.org/10.1109/IEEESTD.2016.7426684

IEEE (2017). "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1," in IEEE Std 1609.2a-2017 (Amendment to IEEE Std 1609.2-2016) , pp. 1-123, 23 Nov. 2017, DOI:
https://doi.org/10.1109/IEEESTD.2017.8065169

IEEE (2019). "IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 2--PDU Functional Types and Encryption Key Management," in IEEE Std 1609.2b-2019 (Amendment to IEEE Std 1609.2-2016), pp. 1-30, 14 June 2019, DOI: https://doi.org/10.1109/IEEESTD.2019.8734860

ITU-T (2019). "X.509: Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

JRC Technical Reports (2019). "C-ITS Point of Contact (CPOC) Protocol", 1 January 2019. Available at: https://cpoc.jrc.ec.europa.eu/data/documents/CPOC_Protocol_Release1.pdf

Kelarestaghi, K. B., Foruhandeh, M., Heaslip, K. & Gerdes, R. (2019). "Intelligent Transportation System Security: Impact-Oriented Risk Assessment of In-Vehicle Networks," in IEEE Intelligent Transportation Systems Magazine, DOI: https://doi.org/10.1109/MITS.2018.2889714

Kovacs, Eduard (2020). "Chinese Researchers Show How They Remotely Hacked a Mercedes-Benz", Security Week digital magazine. Available at:
https://www.securityweek.com/chinese-researchers-show-how-they-remotely-hacked-mercedes-benz

Lang, U. & Schreiner, R. (2015). "Managing Security in Intelligent Transport Systems," 2015 IEEE 18th International Conference on Intelligent Transportation Systems, Gran Canaria, Spain, pp. 48-53, DOI: https://doi.org/10.1109/ITSC.2015.16

Microsec (2020), "Introducing the Microsec V2X PKI security solution". Available at:
https://www.microsec.hu/sites/default/files/microsec_v2xpki.pdf

Monteuuis, Jean Philippe, Hammi, Badis, Salles, Eduardo, Labiod, Houda, Blancher, Remi, Abalea, Erwan & Lonc, Brigitte (2017). "Securing PKI Requests for C-ITS Systems," 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, pp. 1-8, DOI: https://doi.org/10.1109/ICCCN.2017.8038492

SAE International (2017). "Dedicated Short Range Communication (DSRC) Systems Engineering Process Guidance for SAE J2945/X Documents and Common Design Concepts", Id J2945_201712, 7 December 2017.

SAE International (2020)."V2X Communications Message Set Dictionary", Id J2735_202007, 23 July 2020.

TeskaLabs (2021), "SeaCat PKI Cyber security at scale for mobile applications and IoT connected devices". Available at: https://teskalabs.com/products/seacat-pki

Winder, Davey (2020). "Hackers Made Tesla Cars Autonomously Accelerate Up To 85 In A 35 Zone", Forbes digital magazine, 19 February 2020. Available at:
https://www.forbes.com/sites/daveywinder/2020/02/19/hackers-made-tesla-cars-autonomously-accelerate-up-to-85-in-a-35-zone/

Zhao, Meiyuan, Walker, Jesse & Wang, Chieh-Chih (2012). Security challenges for the intelligent transportation system. In Proceedings of the First International Conference on Security of Internet of Things (SecurIT '12). Association for Computing Machinery, New York, NY, USA, 107–115. DOI: https://doi.org/10.1145/2490428.2490444

Zorz, Zeljka (2018). "Researchers hack BMW cars, discover 14 vulnerabilities", HelpNetSecurity digital magazine. Available at: https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/