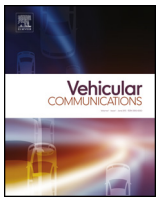
Vehicular Communications 38 (2022) 100531

Contents lists available at ScienceDirect

Vehicular Communications

journal homepage: www.elsevier.com/locate/vehcom



PKIs in C-ITS: Security functions, architectures and projects: A survey

Badis Hammi [a,*], Jean-Philippe Monteuuis [b], Jonathan Petit [b]

[a] EPITA Engineering School, France
[b] Qualcomm Technologies, Inc., Boxborough, MA, USA

ARTICLE INFO

Article history:
Received 5 April 2022
Received in revised form 15 August 2022
Accepted 27 September 2022
Available online 4 October 2022

Keywords:
ETSI
IEEE
Intelligent Transportation Systems
Security and privacy
Public Key Infrastructure

ABSTRACT

In the smart cities context, Cooperative Intelligent Transportation Systems (C-ITS) represent one of the main use cases that aim to improve peoples' daily lives. Within these environments, messages are exchanged continuously. The latter must be secure and must ensure users' privacy. In this regard, Public Key Infrastructures (PKIs) represent the major solution to meet security needs. In this work, we present a holistic survey that describes all the different functions and services of a C-ITS PKI and focus on the different standards and consortia works that have been adopted to regulate such PKIs. Relying on the survey, we highlight the main research problems and open challenges for ITS PKIs. Then, we propose a generic model for a C-ITS PKI architecture.

1. Introduction

In the current smart cities context, Cooperative Intelligent Transportation Systems (C-ITS) represent one of the main use cases that aim to improve peoples' daily life [1]. A C-ITS is primarily composed of vehicles (called Intelligent Transportation System's Station-Vehicle (ITSS-V) in the C-ITS context)[1] and road side infrastructure (Intelligent Transportation System's Station-Road Side Unit (ITSS-R)),[2] and a traffic management center.

C-ITS technologies aim at increasing road safety, efficiency and comfort by sensing, communicating, deciding, and acting based on the surrounding road environment. As Fig. 1 shows, there are numerous types of communication modes (mainly ad hoc communications) like (1) Vehicle-to-Vehicle (V2V) mode, (2) Vehicle-to-Infrastructure (V2I) mode and (3) Vehicle-to-Pedestrian (V2P) mode. In the remainder of this paper, we define this set of vehicular communication modes as Vehicle-to-Everything (V2X) communication.

C-ITS components communicate using wireless communication standards/protocols that will determine the various aspects of communication such as data transmission range and rate, latency and security. Data delivery is considered among the key challenges due to the fast topology change, frequent signal disruptions, and contact opportunities of stations [2]. In C-ITS context, multiple networking technologies can be used according to the scenario and the deployment constraints and policies [3]. Indeed, along the use of cellular networks for some specific scenarios, two main vehicular communication standards using the specially allocated 5.9 GHz unlicensed band have emerged in recent years: (1) Dedicated Short-Range Communications (DSRC) protocol developed in the US [4] and (2) the Intelligent Transportation System (ITS)-G5 protocol developed by the European Telecommunications Standards Institute (ETSI) [5]. These standards are based on the IEEE 802.11p access layer developed for vehicular networks. A competing alternative commonly called C-V2X has recently emerged with the introduction of Proximity Services (ProSe) in 3GPP LongTerm Evolution (LTE) Release 14 and evolved in Release 15 [6]. The latter has been designed to satisfy bounded low latency requirements and accommodate a given levels of density of vehicles for V2X communications combined with the support of high speed [3].

Within a C-ITS, large amounts of data are continuously exchanged in order to ensure proper functioning of the different C-ITS applications. In ETSI-based infrastructures/projects, ITSS-Vs use Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM). In IEEE-based projects, ITSS-Vs use Basic Safety Messages (BSM). As an example of the importance of these messages, BSM has the potential to prevent up to 75% of all roadway crashes according to [7] and [8]. Thus, the correctness and reliability of the exchanged messages have a direct impact on the efficiency and effectiveness of the deployed appli-

* Corresponding author.
E-mail addresses: badis.hammi@epita.fr (B. Hammi), jmonteuu@qualcomm.com (J.-P. Monteuuis), petit@qualcomm.com (J. Petit).

[1] In the remaining of this paper, we use the terms vehicle, node, and ITSS-V to refer to a connected vehicle.

[2] In the rest of this paper, we use the terms RSU and ITSS-R interchangeably to refer to a connected road side unit.

https://doi.org/10.1016/j.vehcom.2022.100531
2214-2096/

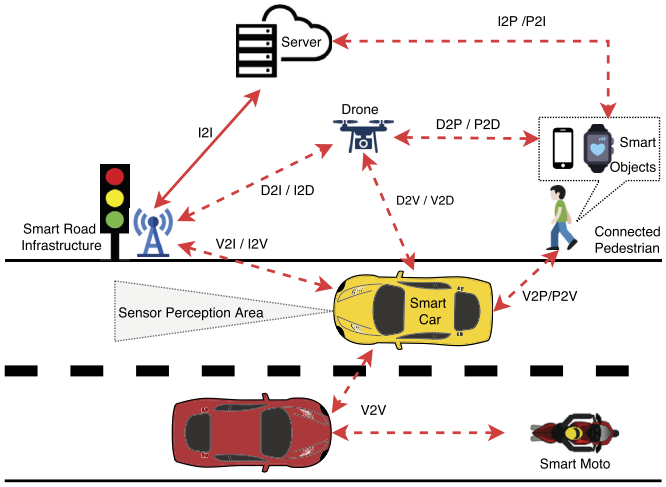


Fig. 1. C-ITS scenario. V2I: Vehicle to Infrastructure, V2V: Vehicle to Vehicle, I2V: Infrastructure to Vehicle, I2I: Infrastructure to Infrastructure, D2I: Drone to Infrastructure, I2D: Infrastructure to Drone, D2V: Drone to Vehicle, V2D: Vehicle to Drone, I2P: Infrastructure to Pedestrian, P2I: Pedestrian to Infrastructure, V2P: Vehicle to Pedestrian, P2V: Pedestrian to Vehicle, D2P: Drone to Pedestrian, P2D: Pedestrian to Drone.

cations. Moreover, due to their spatio-temporal nature, broadcast messages must be protected such that to protect users' privacy. For these reasons, most of the exchanged messages must be secured.

In order to handle these security requirements, multiple mechanisms were proposed [9], and the most common solution is the use of a Public Key Infrastructure (PKI). A PKI represents a set of authorities and protocols that binds public keys with respective identities of entities. The binding is established through a process of registration and issuance of cryptographic materials. Thus, a PKI creates, manages, distributes, uses, stores, and revokes these security credentials [10].

C-ITS PKIs are very different from traditional Information Technology (IT) systems' PKIs. Indeed, in traditional IT systems, PKI implementations follow the same schema. They only differ in the size and the hierarchy depth. However, due to C-ITS security requirements, a C-ITS PKI comprises other authorities, and can be implemented through different architectures. Consequently, there exist multiple proposals and implementations of C-ITS PKIs.

1.1. Related work and motivations

In this section we highlight the need for a survey on PKIs in C-ITS. Indeed, a search of the major scientific databases IEEE, ACM, Elsevier and others, reveals the lack of a survey devoted exclusively to the topic of PKIs in C-ITS, their architectures, their security functions and how the different projects used them. In the following, we describe the related works in the area of C-ITS security. We classify them according to their contribution similarity, and demonstrate that they do not treat PKIs or consider them as a blackbox and not as a research topic. Hence, the need for a holistic survey dedicated to C-ITS PKI.

Security in C-ITS and Vehicular Ad-hoc Networks (VANET) have been extensively studied over the last years. Numerous surveys such as [9,11–21] studied and discussed security issues and challenges in C-ITS environments as well as possible cryptographic solutions. Almost all studies agreed that network size, trust and information verification, key distribution, anonymity, privacy and liability are the top security challenges. They also agreed that authentication, confidentiality, integrity, privacy, data verification and revocability are the security requirements in VANETs. In the same context, *Sumanth et al.* [22] focuses on the security challenges and solutions at the application level.

In order to address the aforementioned challenges and to ensure the security requirements needed, multiple protocols and frameworks were proposed, e.g., [23–34]. Multiple surveys were conducted to analyze the different security solutions proposed over the literature. For instance, [35–41] provided a detailed description and a taxonomy of authentication schemes, and discussed their mechanisms, advantages, disadvantages and performance. *Dahiya et al.* [42] surveyed various user authentication protocols in VANETs and described the efficiency of user verification algorithms. Also, [43–46] provided a quick description of authentication techniques and protocols. In [36], *Riley et al.* provided a survey and categorization of authentication mechanisms in VANETs according to three criteria: asymmetric, symmetric, and infrastructure requirement, in order to identify their suitability under various conditions. [47] discussed the challenges for trust management caused by the highly dynamic nature of VANET environments. Then, the authors analyzed the existing trust models and summarized their key issues. They identified decentralization, sparsity, scalability, confidence, security, privacy and robustness as key properties that a trust management system should incorporate. However, this study focused on multi-agent based approaches. [48,49] also surveyed trust models and provided the same conclusions as [47].

[50–53] identified the requirements to secure VANETs. [54] argued that PKI is the most viable solution to secure them. Furthermore, it pointed out some PKI's limitations such as location privacy and revocation delays. Finally, it introduced a set of mechanisms to mitigate revocation problem through distributed and fine grained revocation. *Khandelwal et al.* [55] surveyed location privacy problem and the limitation of proposed approaches.

[56,57] surveyed various mechanisms to improve different ad-hoc routing protocols for secure routing process by enhancing the trust among the different nodes in VANETs. They proposed PKI as a possible option rather than past interaction experience based approaches [56], incident reports based approaches [58], symmetric cryptography based approaches [59] or the use of public cryptography without certificates [60]. In [61,62] authors surveyed security problems and threats regarding data dissemination. They also discussed different solutions and trust-based approaches to ensure data dissemination in VANETs.

[63–71] focused on security and privacy issues and cyberattacks in VANET. They also discussed some proposed solutions. But, did not focus on PKIs.

[72,73] discussed privacy of VANET data aggregation techniques and concluded that PKI and pseudonym certificates are the best ways to achieve this goal. Also, *Gupta et al.* [74] surveyed approaches that rely on data aggregation to ensure security features using the data collected. But, did not focus on PKIs.

[75] provided a quick description of some frameworks that ensure encryption and authentication of nodes in a VANET environment and proposed Signcryption Message Authentication Protocol (SMAP), which combines digital signature and encryption functions. [76] presented a comparison of asymmetric-based and symmetric-based encryption solutions in a VANET context regarding average loss ratio, communication overhead ratio and traffic load. However, no details about the algorithms studied were given. [77] surveyed vehicular clouds and described how a PKI can ensure C-ITS security requirements.

Petit et al. [80] focused on the pseudonymity requirements. *Van Huynh et al.* [85] investigated the main security and privacy challenges for the design of automotive applications and platforms. Then, they reviewed existing protection mechanisms. However, none of these works discussed PKI architectures.

Despite the large body of literature on C-ITS security, there is so far no comprehensive survey specifically on vehicular PKIs. Table 1 summarizes the majority of the existing related surveys. It is worth noting that the existing works are mainly focused on

academic research, and do not discuss or analyze standards and consortia efforts. This is a significant gap we propose to fill in order to help adoption and deployment of C-ITS. Finally, none of the existing works is interested in the different PKI architectures, standards, deployment projects and the certificates lifecycle such as the certificate's request mechanisms, intra PKI trust mechanisms and so on. To the best of our knowledge, the only works that were interested in standardization works and consider PKI as a set of functions and not as a blackbox tool are [83] [80] and [85]. However, [83] only introduced Security Credential Management System (SCMS) PKI [91], since, its main contribution is the proposal of a new taxonomy of the different attacks.

In summary, our paper is carefully positioned to avoid overlap with existing surveys by filling the gaps and reporting the latest advances regarding C-ITS PKI. However, in this work, we do not perform a formal safety analysis.

1.2. Contributions of this work

This survey is intended for researchers from industry and academia interested in the field of privacy and security management in C-ITS which will provide them with a good understanding of such an ecosystem. To the best of our knowledge, this is the first survey that analyzes standards and consortia work related to C-ITS PKI architectures. We highlight the contributions of this paper as follows:

- We provide an extensive survey of the different PKI architectures used in C-ITS environments and deployment projects.
- We provide an extensive survey of the different privacy management/lifecycles in the C-ITS environments.
- We discuss the different open challenges for the future C-ITS.
- We propose a generic model for a PKI architecture that respects a tradeoff between the number of authorities, modularity and infrastructure complexity.

Fig. 2 describes the organization of the paper. It is organized as follows: Section 2 describes the different security and performance requirements for the C-ITS. Then, Section 3 describes the different certificate standards. Section 4 depicts the different standard and projects that designed and deployed PKIs in C-ITS and describes their architectures. Next, Section 5 details how PKI requests and responses are performed. Then, Section 6 describes the different existing Certificate Revocation and Trust service Status Lists (CRLs and TSLs). Afterwards, Section 7 describes our proposal of a generic PKI in C-ITS. Section 8 highlights open research and operational challenges. Finally, Section 9 concludes the paper.

2. Public Key Infrastructure requirements

In this section, we describe the requirements needed for PKIs in the C-ITS domain. We present the requirements according to three categories as highlighted in Table 2:

- Organizational requirements
- Security requirements
- Performance requirements

2.1. Organizational requirements

1) Policy enforcement: The policy enforcement aims to foster the interoperability between the organizations involved in the C-ITS PKI, as well as the technical and legal supervision of the PKI. Indeed, a PKI requires the cooperation of dozens of organizations such as internal and national governmental agencies, car manufacturers, road operators, suppliers, IT and security solution providers. This cooperation has its pros and cons. Indeed, in order to ensure the cooperation resilience, all the involved organizations must meet a minimal set of requirements, which are defined in a set of documents (e.g., certificate policy, security policy).

2) Flexibility: Each organization must fulfill different levels and ranges of requirements. For instance, governmental agencies do not have to ensure the constant technical availability of the PKI services, but will focus on the policies used by the PKI. Moreover, a national organization might prefer the use of security algorithms recommended by its national security agency instead of other security algorithm. Therefore the PKI requirements need to be flexible while ensuring security and performance.

3) Interoperability: The PKI must be interoperable between the different organizations involved. In the following, we consider a geographical taxonomy: (1) at the national level, an ITSS manufacturer can choose a security supplier different from his national competitor. However, the two security solutions must interface with each other. A common standard for the country forces suppliers to be interoperable, making the different ITSS produced by the different manufacturers communicate with each other. (2) at international level, an ITSS entering a foreign country, must be interoperable with local ITSS and with local PKI. Indeed, an ITSS of a foreign country, will probably use certificates provided by another PKI. If no interoperability between different ITSSs and between PKIs is supported, the messages sent by foreign ITSS will not be accepted, which implies a deny of the C-ITS services. Thus, it is mandatory that international organizations must find common requirements. For example the European projects C-Roads and InterCor [92] used the mechanism of Trusted Status List (explained in more details in Section 6.2) in order to ensure this interoperability of ITSS and PKIs among the different participating countries in Europe.

4) Naming convention: The C-ITS PKI should support a standard naming convention. Indeed, there will be millions of entities used in the C-ITS ecosystem that need to be identified. Without a naming convention, numerous problems can occur, e.g., the collision of identifiers.

5) Legacy support: The PKI must ensure legacy support. That is, it must allow an ITSS working with an ancient version of one or more components of the ecosystem (e.g., certificate, secured message format) being able to communicate in order to update its version and thus comply with the C-ITS ecosystem.

6) Scalability: The number of ITSS is continuously increasing. Therefore, the PKI that manages them must be scalable to ensure system's continuity and operation. Moreover, the C-ITS PKI rely on multiple organizations. One difficulty is to manage all the organizations involved according to a scalability policy. Indeed, if there is no agreement on the scalability strategy, the divergent organizations may jeopardize the organizational system of the PKI.

7) Hierarchical organization: A PKI by definition is hierarchical [93] due to the different trust levels and responsibilities of the authorities. Also, due to the increasing number of ITSS it must be scalable. However, a high level of hierarchy limits scalability because some services (e.g., authorities) can represent a bottleneck and a single point of failure. Therefore, C-ITS PKIs must find a tradeoff between hierarchy and decentralization.

2.2. Security requirements

C-ITS security requirements have been largely studied and discussed in literature [17,21,36,47,80]. Thus, in the following we will not focus on their description, but on how, the most important ones, are accomplished.

1) Confidentiality: Some C-ITS applications require that the content of a message must be accessible only by the sender and the

Table 1
Comparison of the existing related surveys on C-ITS security. Green color is used for a suitable feature and the red color for an unsuitable feature. (For interpretation of the references to color please refer to the web version of this article.)

Survey	Year[a]	Considers PKI as a blackbox	Focus on PKI only ?	Describes all the ITS's identity lifecycle ?	Considers works from standards and consortia in security field ?	Considers works from academia ?	Limitations
Dahiya et al. [42]	2001	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia -Does not discuss PKI
Fonseca et al. [78]	2006	/	No	No	No	Yes	-Focuses only on routing security
Riley et al. [36]	2011	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia -Does not discuss PKI
Mishra et al. [17]	2011	/	No	No	No	Yes	-Focuses on security issues -Does not discuss PKI
Zhang et al. [47]	2011	Yes	No	No	No	Yes	-Focuses only on trust models from academia -Does not discuss PKI
Rivas et al. [73]	2011	Yes	No	No	No	Yes	-Focuses only on security issues -Does not discuss PKI
Mohanty et al. [72]	2012	/	No	No	No	Yes	-Focuses only on secure data aggregation
Das et al. [79]	2013	Yes	No	Briefly	No	Yes	-Focuses mainly on signature schemes -Does not discuss PKI
Gillani et al. [12]	2013	/	No	No	No	Yes	-Interested in security in general and does not discuss PKI
Saranya et al. [75]	2013	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia and on signcryption -Does not discuss PKI -5 pages long
Engoulou et al. [9]	2014	Yes	No	No	No	Yes	-Interested in security in general and does not discuss PKI
Jeeva et al. [15]	2014	/	No	No	No	Briefly	-Does not discuss PKI -3 pages long
Shaikh et al. [19]	2014	Yes	No	No	No	Briefly	-Discusses ITS security requirements and some generic security solutions -Does not discuss PKI -5 pages long
Mejri et al. [21]	2014	Yes	No	No	Briefly	Yes	- Interested in security in general and on attacks specifically -Does not focus on security solutions
Singla et al. [56]	2014	/	No	No	No	Yes	-Focuses only on routing security
Li et al. [61]	2014	Yes	No	No	No	Yes	-Focuses only on data dissemination and routing security
Qu et al. [13]	2015	Yes	No	No	No	Yes	-Focuses on privacy issues -Does not discuss PKI
Bariah et al. [14]	2015	Yes	No	No	No	Yes	-Focuses on attacks and security issues -Does not discuss PKI -7 pages long
Tiwari et al. [16]	2015	/	No	No	No	Briefly	-Focuses on some academia works on privacy preservation -Does not discuss PKI -6 pages long
Kudlikar et al. [18]	2015	Yes	No	No	No	Briefly	-Focuses on some academia works on privacy preservation -Does not discuss PKI -6 pages long
Patel et al. [57]	2015	Yes	No	No	No	Yes	-Focuses only on routing security
Kiruthika et al. [62]	2015	/	No	No	No	Yes	-Focuses only on secure data dissemination and routing
Petit et al. [80]	2015	No	No	Partially	Yes	Yes	-Focuses only on pseudonymity
Ponikwar et al. [81]	2015	Yes	No	No	No	Yes	-Focuses on academic security solutions and compare their architectures -Does not discuss PKI
Jadoon et al. [20]	2016	/	No	No	No	Yes	-Focuses on attacks -Does not discuss PKI -3 pages long
Sumanth et al. [22]	2016	Yes	No	No	No	Yes	-Focuses on application level attacks specifically -Does not discuss PKI -6 pages long
Manvi et al. [35]	2017	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia -Does not discuss PKI
Sathe et al. [45]	2017	/	No	No	No	Briefly	-Focuses on explaining different signature schemes -Does not discuss PKI -3 pages long
Khan et al. [82]	2017	No	No	Partially	No	Yes	-Focuses only on revocation
Hasrouny et al. [83]	2017	No	No	No	Yes	Yes	- Discusses the SCMS PKI only -Not interested in the certificates lifecycle through the PKI
Ahmed et al. [63]	2017	Yes	No	No	No	Briefly	-Focuses mainly on security Issues -Does not discuss PKI -7 LNCS pages long
Vaibhav et al. [48]	2017	Yes	No	No	No	Yes	-Focuses only on authentication schemes and trust models from academia -Does not discuss PKI
Lu et al. [84]	2018	Yes	No	No	No	Yes	- Focuses on academia works on privacy and trust issues and solutions -Does not discuss PKI
Van Huynh et al. [85]	2018	Yes	No	No	Briefly	Yes	-Does not discuss PKI (projects, architectures and certificates' lifecycle)
Al-ani et al. [50]	2018	Yes	No	No	No	Briefly	-Interested in the security features of safety applications -Does not discuss PKI -6 pages long
Muhammad et al. [64]	2018	Yes	No	No	No	Yes	-Focuses only on authentication issues related to vehicular cellular communications from academia -Does not discuss PKI
Sheikh et al. [66] [67]	2019	Yes	No	No	No	Yes	-Interested in security attacks and solutions from academia -Does not discuss PKI

Table 1 (*continued*)

Survey	Year[a]	Considers PKI as a blackbox	Focus on PKI only ?	Describes all the ITS's identity lifecycle ?	Considers works from standards and consortia in security field ?	Considers works from academia ?	Limitations
Zhang et al. [37]	2019	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia -Does not discuss PKI -5 pages long
Raghupathi et al. [38]	2019	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia -Does not discuss PKI -7 pages long
Ali et al. [49]	2019	Yes	No	No	Briefly	Yes	-Focuses only on authentication and privacy schemes from academia -Does not discuss PKI
Goyal et al. [51]	2019	Yes	No	No	No	Briefly	-Interested in ITS architectures and security in general -Does not discuss PKI -8 pages long
Hussain [86] *et al.*	2019	Yes	No	No	Yes	Yes	-Focuses only on security issues that need to be considered in order to enable the secure integration of 5G in VANETs -Does not discuss PKI
Farooq et al. [39]	2020	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia -Does not discuss PKI
Mustafa et al. [68]	2020	Yes	No	No	No	Briefly	-Focuses on security Issues -Does not discuss PKI -6 pages long
Al-Shareeda et al. [69]	2020	Yes	No	No	No	Yes	-Interested in security attacks and solutions -Does not discuss PKI
Malhi et al. [52]	2020	No	No	No	No	Yes	-Discusses ITS security requirements, cyberattacks and some security solutions -Not interested in the certificates lifecycle through the PKI
Kohli et al. [70]	2020	Yes	No	No	No	Briefly	-Focuses mainly on security Issues and attacks -Does not discuss PKI -4 pages long
Manivannan et al. [40]	2020	Yes	No	No	No	Yes	-Focuses only on authentication schemes from academia -Does not discuss PKI
Afzal et al. [41]	2020	Yes	No	No	No	Yes	-Focuses only on security Issues -Does not discuss PKI
Obaidat [87] *et al.*	2020	Yes	No	No	No	Yes	-Focuses only on security Issues and attacks -Does not discuss PKI
Hussain [88] *et al.*	2020	Yes	No	No	No	Yes	-Focuses only on trust in VANET -Does not discuss PKI
Rao et al. [65]	2021	Yes	No	No	No	Yes	-Focuses only on Privacy Issues -Does not discuss PKI
Islam et al. [71]	2021	Yes	No	No	No	Briefly	-Focuses mainly on security Issues -Does not discuss PKI
Sharma et al. [53]	2021	Yes	No	No	No	Yes	-Interested in ITS architectures and security in general -Does not discuss PKI
Our survey	2021	No	Yes	Yes	Yes	Yes	/

[a] We consider the works before 2017 as old because it represents the year where the majority of security standards and deployment projects were published or updated e.g., [89] [90].

Table 2
Overall PKI requirements.

Requirement	Organizational	Security	Performance
Policy Enforcement	✓		
Flexibility	✓		
Interoperability	✓		
Naming Convention	✓		
Legacy Support	✓		
Scalability	✓		✓
Hierarchical organization	✓		
Confidentiality		✓	
Integrity		✓	
Authentication/mutual authentication		✓	
Non repudiation		✓	
Privacy and pseudonymity		✓	
Authorization		✓	
Availability		✓	✓
Real-Time Operation			✓
Upgradeability			✓

receiver. Confidentiality is performed through encryption [94]. Due to C-ITS environment features, only few types of messages are encrypted. Indeed, C-ITS environment is characterized by the high speed of nodes (e.g., vehicles). Therefore, in order to achieve an efficient service, the processing of messages must be fully optimized. For example, messages' encryption induces to additional processing costs and is avoided as much as possible. Nonetheless, encryption still be mandatory for some scenarios, such as for certificate requests for example [91] [95].

Symmetric-key encryption field was extensively studied and many algorithms were developed [96–98]. In C-ITS, the AES counter with CBC-MAC (CCM) (Cipher Block Chaining Message Authentication Code) operation mode is used in IEEE and ETSI security standards. Symmetric-key encryption algorithms are very efficient and fast. However, they suffer from scalability issues. Indeed, in a system that includes multiple users, two solutions are possible; (1) all the users use the same key. However, if one user's key is compromised, all the security of the group is also compromised. (2) each pair of users use a different secret key. However, this solution induces to management problems [99]. In order to address this issue, asymmetric cryptography was proposed.

Public key cryptography area was extensively studied and numerous algorithms were proposed, e.g., Rivest-Shamir-Adleman (RSA) [100–102] which represents the most widely deployed public key cryptosystem [103], El-Gamal [104], Elliptic Curve Cryptography (ECC) algorithms [105] [106]. In C-ITS environments, only elliptic curve based asymmetric algorithms are used. More precisely, the Elliptic Curve Integrated Encryption Scheme for encryption [106–108] and Elliptic Curve Digital Signature Algorithm for signature [109] [106].

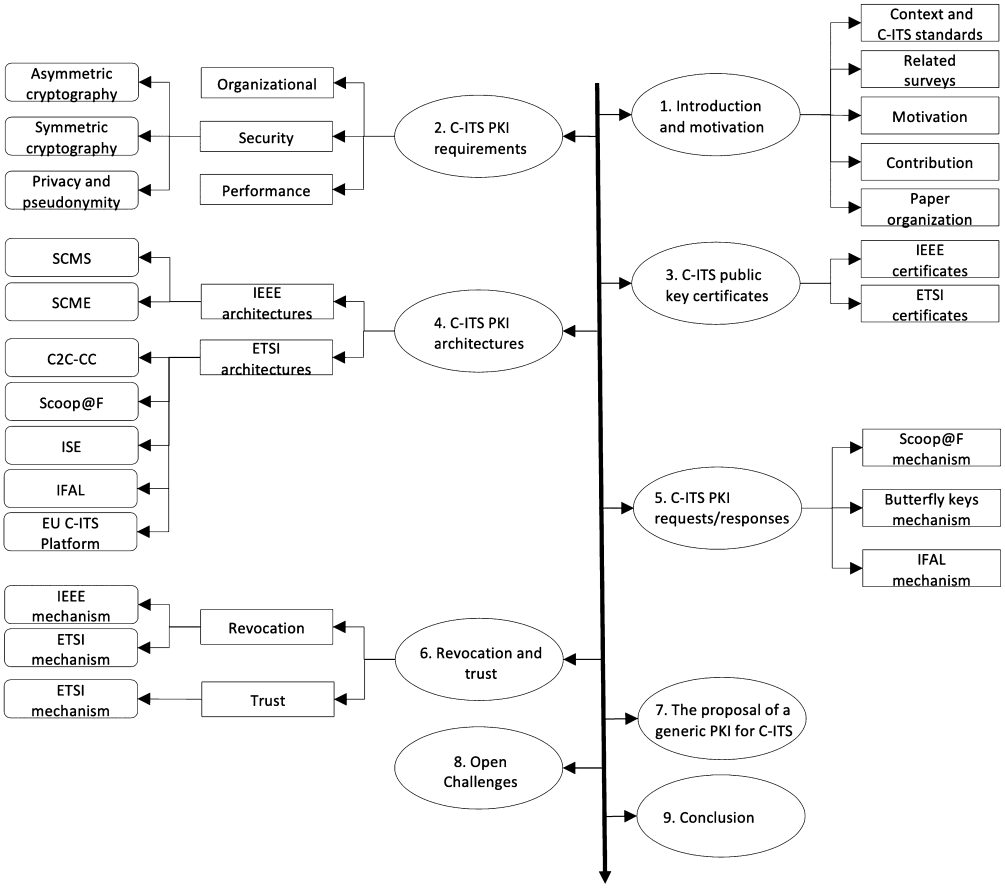


Fig. 2. Roadmap of the paper.

Table 3
Key sizes for equivalent robustness (in bits) [112].

ECC	DH/DSA/RSA
163	1024
283	3072
409	7680
571	15360

Table 4
Algorithms per ECIES Function for V2X.

Function	V2X Cryptography Standards	
	IEEE 1609.2 [95]	ETSI 103 097 [89]
Curve definition	NIST-P256, BrainpoolP	NIST-P256, BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1
Key Agreement	ECSVDP-DHC	
Key Derivation	KDF2	
Encryption	AES-128-CCM	
MAC	MAC1	
Hash	SHA-256	

Elliptic curve cryptography (ECC) was introduced by Victor Miller and Neil Koblitz in 1985 [110] [111]. The aim was to create an alternative mechanism for public key cryptography. ECC is based on the elliptic curve discrete logarithm problem. The advantage of such algorithms is that they require smaller keys compared to other algorithms such as RSA, in order to provide equivalent security. A shorter key implies lesser powerful hardware, easier data management and storage and a longer battery life in devices. Table 3 compares the key sizes of ECC with other algorithms.

ECIES combines a Key Encapsulation Mechanism (KEM) with a Data Encapsulation Mechanism (DEM). The system independently derives a session encryption key and a Message Authentication Code (MAC) key from a common secret. Plaintext is first encrypted under a symmetric cipher, and then a MAC function is applied on the ciphertext for authentication. More precisely, ECIES relies on four cryptographic functions. For each function, multiple algorithms can be used. Table 4 describes the possible algorithms for the different ECIES cryptographic functions, according to the different C-ITS standards. The ECIES encryption algorithm needs the generation of sender's EC key pair and receiver's EC key pair. To achieve this operation, both sender and receiver must agree on the elliptic curve on which the key generation is based (domain parameters). NIST-P elliptic curves or BrainPool curves are required by ETSI, IEEE and ISO standards.

2) Authentication, mutual authentication, integrity and non repudiation: Authentication requirement ensures that entities involved in a communication are correctly identified and authentic. The integrity ensures that the information exchanged are not altered between sender and receiver, and the non repudiation ensures that a station cannot deny having sent a message (e.g. a wrong warning).

All the described requirements are fulfilled using signature algorithms which rely on cryptographic hash functions. Hash functions are primarily used to insure messages' integrity. Hash functions are combined with encryption functions in order to provide digital signatures. A digital signature is a mathematical scheme that proves the sender's authentication, message's integrity and non repudiation.

IEEE, ETSI and ISO ITS standards require the sole usage of Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signature. ECDSA [113] is the elliptic curve analogue of the DSA algorithm. It was first proposed by Scott Vanstone in 1992 [114]. It was ac-

Table 5
Algorithms per ECDSA Function for V2X.

Function	V2X Cryptography Standards	
	IEEE 1609.2 [95]	ETSI 103 097 [89]
Curve definition	NIST-P256, BrainpoolP	NIST-P256, BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1
Hash algorithm	SHA-256/384	

Table 6
Time calculations for signing operations for RSA and ECDSA [122].

Year	Level of security (key size [bits])		Time for signature generation [ms]		Time for signature verification [ms]	
	ECDSA	DSA	ECDSA	DSA	ECDSA	DSA
1999	113	512	2.8	13.7	7.5	1.3
2006	131	704	3.8	32.4	11.5	2.5
2015	163	1024	5.7	78.0	17.9	4.3
2016	193	1536	7.6	251.9	26.0	9.7
2039	233	2240	10.1	731.8	37.3	20.4

cepted in 1998 as an ISO standard in ISO/IEC 14888 [115], accepted in 1999 as an ANSI standard in ANSI X9.62 [116], and accepted in 2000 as an IEEE standard in IEEE 1363-2000 [117] [118] and a FIPS standard in FIPS 186-2 [119] [120].

Table 5 describes the ECDSA's parameters and algorithms used according to the different V2X standards.

ECDSA offers multiple advantages over traditional signature algorithms such as DSA, especially concerning key sizes and signature time [112] [121]. Table 6 describes a comparison study of DSA and ECDSA key size, signature generation time and signature verification time for the same security level [122]. It is worth to note that ECDSA have shorter keys and better signature generation time. However, it takes more time to verify a signature compared to DSA.

3) Privacy and Pseudonymity: ITSS diffuse periodically messages which contain - among others - information about their position and localization. Using these information, an attacker can track the station or create detailed mobility patterns of individual drivers [80]. This problem can be addressed by providing a vehicle with a set of pseudonyms, where it uses each pseudonym for a limited duration. More precisely, by relying on a PKI, each ITSS uses simultaneously two certificates: (1) an Enrollment Certificate (EC) (also called Long Term Certificate (LTC)) and (2) a Pseudonym Certificate (PC) (also called Short Term Certificate (STC)). Known only by the EC Authority (ECA) and its owner (ITSS), the EC is not used in common communications, but used only to authenticate the ITSS to the PKI in order to request new PCs. However, the PC is used for the ITSS communications. In order to protect the privacy of the road users, a regular change of pseudonyms is required. The European standard ETSI TS 102 867 [123] recommends that pseudonyms are changed every five minutes, whereas the American standard SAE J2735 [124] recommends that this is done every 120 seconds or 1 km, whichever occurs last. For example in SCMS project, an ITSS uses more than 1000 PCs per year [7] and this number can even reach 100000 according to [125]. In SCOOP@F project an ITSS uses 520 PCs per year [126].

During one journey, an ITSS can change many times its PC. However, due to C-ITS communication constraints, like vehicles' speed and the use of wireless technologies (e.g., ITS-G5/802.11p), an ITSS can not always successfully realize a PC request. To resolve this problem, the common solution is to preload multiple certificates and to store them locally. Then, when an ITSS needs to change its PC, it draws from its stock of preloaded PCs.

4) Authorization: In C-ITS context, authorization requirement is the process of giving an entity the permission to access some services, to receive some information or to diffuse some information.

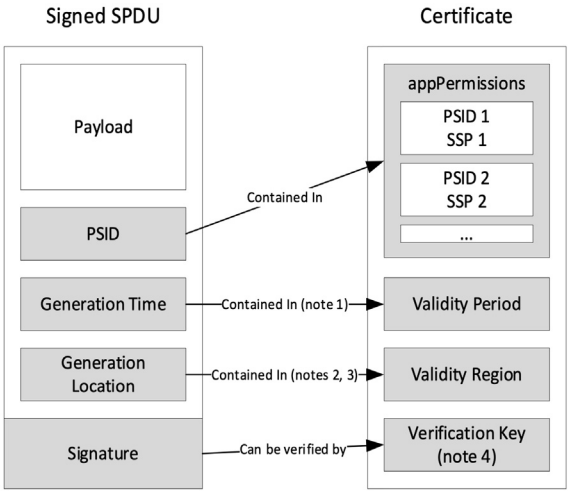


Fig. 3. Consistency conditions to be checked by the security services [129].

Table 7
Mechanisms and algorithms that ensure security requirements in C-ITS environments.

Requirement	Mechanism/Algorithm
Confidentiality	Encryption (ECIES)
Authentication	Certificate/Signature (ECDSA)
Integrity	Signature (ECDSA)
Non repudiation	Signature (ECDSA)
Authorization	Certificate/Provider Service Identifiers (PSID)/(SSP)
Privacy	Pseudonym certificate change

Generally, the set of these permissions is included in the station's certificate. More precisely, the ITS certificates include one (or more) field called Service Specific Permissions (SSP) [127] [128] [89], which represents the list of the services that the station is authorized to access and use. For example, an ITSS can have the permission to broadcast a message that informs about an accident, thus, it has the SSP for it, but, cannot broadcast a message that informs about an animal on the road because it has not the suitable SSP for it. Fig. 3 describes the consistency conditions to be checked by the security services before the acceptance of a packet (Secured Protocol Data Unit (SPDU)).

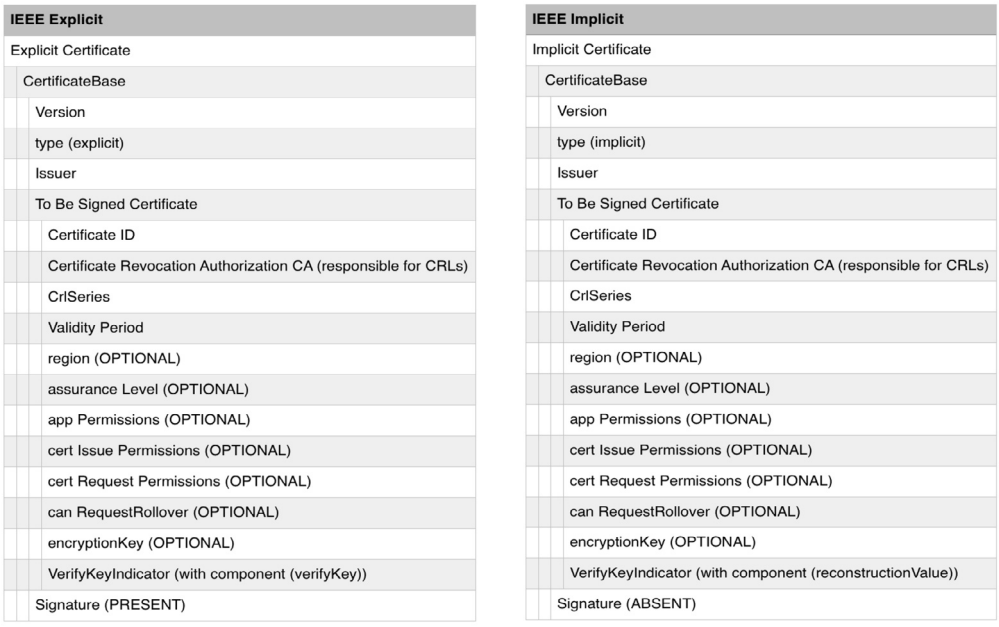
2.3. Performance requirements

1) Availability and real time Operation: The availability implies that the PKI and its services must be accessible to legitimate users on demand. Thus, a system must be resilient against availability targeting attacks such as denial of service. Moreover, the operation must be in real time to insure the system's resiliency and freshness.

2) Upgradeability: It represents the capability of being improved in functionality by the addition or replacement of components. Therefore, the PKI must easily support to add or to modify one or a set of new services or components (e.g., authority) if there is a need for it.

2.4. Summary

The Table 7 summarizes the different algorithms and mechanisms used to ensure the main communications' security requirements described above, in the C-ITS context for the different standards and deployment projects.



(a) (b)

Fig. 4. IEEE certificate's structure; (a) IEEE Explicit certificate; (b) IEEE Implicit certificate.

The different cryptographic operations and algorithms descried above rely on cryptographic keys. Most of these keys are provided to the different entities as part of public key certificates. In the next section, we focus on C-ITS public key certificates.

3. Public key certificates

Web PKIs manage X.509 certificates [130]. However, C-ITS PKIs manage specific C-ITS public key certificates.[3] The latter are designed to respond to the constraints of C-ITS ecosystems. In this section we present and describe the formats and structures of ITS certificates for both IEEE and ETSI standards.

1) IEEE1609V2 certificate: IEEE 1609.2 [95] is a security standard for C-ITS PKI. The standard introduces a new certificate format. The latter supports two forms: explicit and implicit. Fig. 4 depicts their formats.

Explicit certificate is the conventional certificate format. In contrary to implicit certificate, it includes a verification public key and a digital signature computed by the certificate issuer. Thus, one can authenticate the certificate owner's identity by verifying the certificate's signature.

Vanstone et al. [131–133] proposed implicit certificate use and its enhancement against attacks. It differs from explicit certificate format by not including the complete public key. Instead, it contains a partial key value called *reconstruction value*. The acquisition of the implicit certificate's public key value requires a computation that involves its reconstruction value and the CA's public key.

IEEE 1609.2 implicit certificate uses Standards for Efficient Cryptography (SEC 4) Elliptic Curve Qu-Vanstone (ECQV) scheme [134]. The latter suits resources' constrained environments such as C-ITS limited bandwidth, computation power or storage space [135]. It represents an efficient alternative to traditional certificates. Indeed, the use of an implicit certificate does not require explicit CA signature verification.

A generic IEEE certificate contains the following fields:
Version: specifies the certificate's version value. Currently, it is set to 3 [95].
Type: defines the certificate's format such as implicit or explicit.
Issuer identifies the certificate's issuer.
ToBeSigned contains the fields covered by the issuer's signature, it includes:

- Certificate ID: represents an identifier for the certificate's holder.
- Certificate Revocation Authorization Certification Authority (CRACA): identifies the authority responsible for Certificate Revocation Lists (CRLs) issuance.
- CrlSeries: specifies the CRL in which the present certificate will be published if revoked.
- Validity period: defines the certificate's validity time period value.
- Region: defines the certificate's validity geographical zone (e.g., a country). If the region field is set, the system considers the following cases: (1) Self-signed certificates' region validity is worldwide, or, (2) Not self-signed certificates' inherits the certificate issuer's region validity value.
- Assurance level: indicates the certificate's owner assurance level value. The assurance level will serve as a reputation metric to ensure the node's trustworthiness regarding the messages and their content (data allowance). It also can be used by misbehavior trust mechanisms in order to manage misbehaving nodes [7].
- App permissions: defines a sequence of PSID/SSP associations. A PSID specifies permitted application area. An SSP authorizes the sender to perform specific "application activities" within the associated PSID application area.
- Cert issue permissions: are application permissions (combination of PSID-SSP) that the CA can issue to subordinates.
- Cert request permissions: are the application permissions that the Enrollment Certificate can request when demanding new certificates.
- Request rollover: indicates that the certificate owner's private key may sign certificate requests.
- Encryption key: is the certificate's public key value used for encryption.

[3] In the rest of the paper, we use indifferently the terms public key certificate and certificate.

ETSI
Certificate
Version
Signer Info
Subject Info
Subject Attribute
Subject Attribute Type : verification key
Subject Attribute Type : encryption key (MANDATORY or OPTIONNAL)
Subject Attribute Type : assurance level
Subject Attribute Type : ItsAidSsp list or ItsAid list
ITS AID
Service Specific permissions
Validity Restriction
Validity Restriction Type : time start and end // time end // time start and duration
Validity Restriction Type : region (OPTIONNAL)
Signature

Fig. 5. ETSI generic certificate.

- Verify key indicator: contains the verification key value for explicit type or reconstruction value for implicit. In sum, it represents the certificate's public key value used for signature.

signature: represents the signature value in the explicit certificate.

2) ETSI certificate: The European Telecommunications Standards Institute (ETSI) is a standardization organization working on various fields such as C-ITS security. The standard ETSI TS 103097 [136] [89] specifies the V2X message security header and the various certificates' formats. The last version of the standards [137] introduces new certificate profiles as well as the support to use implicit certificates. Fig. 5 depicts ETSI certificate fields:
Version specifies the certificate's version value based on standard version number. Currently, this value is set to 3.
Signer info: contains the certificate's issuer information which can be:

- Self: the owner self-signs its certificate.
- Certificate digest with SHA256: the issuer's identity is presented by the first 8 bytes of the issuer's certificate's SHA256 digest.
- Certificate: the issuer's identity is the entire issuer's certificate value.
- Certificate chain: contains the whole certificate chain starting from the owner's certificate up to the root certificate.
- Certificate digest with other algorithm: the issuer is presented by the first 8 bytes of the issuer's certificate digest realized with another algorithm than SHA256.

Subject info: contains (1) a Subject name field which includes the certificate's owner name. (2) a Subject type field containing the certificate's type. The latter can be either:

- enrollment_credential: also known as Long Term Certificate (LTC). Enrollment Authority enrolls ITS stations in the PKI by issuing these certificates. The latter is mandatory for the Authorization Ticket request.
- authorization_ticket: also known as Pseudonym Certificate (PC) or short term certificate. The Authorization Authority (AA) issues these certificates to ITS stations. PC is mandatory for securing V2X communications.
- root_ca: is a self signed Root CA certificate.
- enrollment_authority: is the Enrollment Authority (EA) certificate.
- authorization_authority: is the Authorization Authority (AA) certificate.
- crl_signer: represents the CRL Authority certificate.

Subject attributes: contains multiple technical fields:

- verification_key: represents the certificate public key used for signature.
- encryption_key: represents an optional public key used for encryption.
- reconstruction_value is an EC point used in ECQV scheme. Used by the implicit certificate type as for the IEEE certificate described above.
- assurance_level: scores both ITS platform and secret keys storage security as well as the confidence in this assessment.
- its_aid_list: contains the authorized applications list of the certificate's owner. It has the same role as PSID in IEEE certificate. For instance, the ITSS AID list authorizes the ITSS to send Decentralized Environmental Notification Messages (DENM).
- its_aid_ssp_list is a list of ITS AID and their Service Specific Permissions (SSP). The latter represent the authorized cases and scenarios. For instance, an ITSS having the AID DENM and the SSP *On Road Accident* allow an ITSS to send DENM *On Road Accident* message. However, it could not send a DENM *construction site* without the proper SSP.

Validity restrictions: specifies the restrictions regarding to the certificate's validity. A certificate includes a time validity restriction and sometimes a region validity restriction (e.g., a country). A restriction type can be:

- time_end: represents the certificate's expiration date.
- time_start_and_end: describes the certificate's beginning and expiration date.
- time_start_and_duration: represents the certificate's beginning date and the certificate's validity duration;
- region: represents the certificate's geographical validity. It includes multiple forms such as "Circular Region", "Rectangular Region", "Polygonal Region" or a "country code" as described by ISO 3166-1 [138].

Signature: represents the certificate's signature value signed by the issuer. If the Subject Attributes field contains the type reconstruction_value. Then, the signature field is omitted.

3) Summary: X.509 certificate has a detailed and complete structure. However, it is not adapted to C-ITS due to numerous constraints such as the limited bandwidth and numerous different fields needed by the C-ITS environment compared to web infrastructures, which incurs the need for lighter certificates [139]. Therefore, IEEE and ETSI standards have proposed new C-ITS certificate structures. Aforementioned certificates descriptions show numerous similarities between the standards. Moreover, current standardization efforts try to propose a common format for ITS certificates. Indeed, the last ETSI certificates are based upon IEEE ASN.1 defined structures [89].

As described above, the management of public key certificates requires a Public Key Infrastructure (PKI). While web X.509 PKIs

Table 8
Summary of the main PKI deployment projects.

PKI/Project	Applied standards	Required authorities	Possible duplicated authorities	Misbehavior detection	Country	Year of project launch	Project's state
IEEE	IEEE 1609.2	RCA, SDE CA, WSE CA	RCA, SDE CA, WSE CA	No	US Standard	2006	ongoing
ETSI	ETSI	RCA, EA, AA	RCA, EA, AA	No	European Standard	2012	ongoing
SCMS	IEEE 1609.2	Electors, RCA, ECA, PCA, RA, LA, MA, ICA	Electors, RCA, ECA, PCA, LA, RA, ICA	Yes	USA	2014	ongoing
C2C-CC	ETSI and IEEE 1609.2	RCA, LTCA, PCA	RCA, LTCA, PCA	No	Europe	2011	ongoing
SCME	IEEE 1609.2	RCA, ECA, PCA, Revocation CA, ACA, RA	Not specified	Yes	China	2019	ongoing
ESCRYPT/CycurV2X-PKI	ETSI and IEEE 1609.2	Electors, RCA, ECA, PCA, RA, LA, MA, ICA	Electors, RCA, ECA, PCA, LA, RA, ICA	Yes	Germany	2014	ongoing
ECo-AT	ETSI	RCA, LTCA, PCA	RCA, LTCA, PCA	No	Austria	2011	ongoing
InterCor	ETSI	Policy Authority, RCA, EA, AA	RCA, EA, AA	No	Europe	2016	ongoing
C-Roads	ETSI	PA, RCA, EA, AA	RCA, EA, AA	No	Europe	2016	ongoing
IFAL	ETSI	RCA, EA, AA	EA, AA	No	Netherlands	2016	ongoing
SCOOP@F	ETSI	RCA, LTCA, PCA	LTCA	No	France	2014	Finished in 2019
ISE	ETSI	RCA, EA, AA, MA, Privacy Authority	AA	yes	France	2014	Finished in 2017
PRESERVE	ETSI	RCA, LTCA, PCA	RCA, LTCA, PCA	No	Europe	2011	Finished in 2015

have a common hierarchical structure, C-ITS PKIs are very different. Moreover, because C-ITS standards describe only high level PKI architectures, numerous projects have designed and deployed different PKIs according to their needs. Therefore, in the next section we describe the different PKI architectures and highlight their deployment projects.

4. Cooperative ITS PKI architectures

In this section we describe different PKI architectures that belong to different standards and deployment projects. Each PKI is composed of a set of authorities. Some authorities are common to almost all the existing projects. However, they may have different additional functions.

4.1. Summary

Table 8 provides a summary of the different PKI projects discussed above. It presents the different PKI authorities for each project and their associated names. Some authorities exist in every project such as the trust anchor authority, the enrollment authority or the pseudonym authority. On the contrary, some entities can be unique or very specific to a project e.g. linkage authority for SCMS and SCME. Table 8 also allows to understand the list of all certificate types found in the different PKI architectures designed for the different projects and allows to identify the different existing certificate profiles for each PKI project and the respective names as mentioned in the specification documents. For instance, an enrollment certificate exists in all project. However, its given name can be different e.g. Long Term Certificate in SCOOP@F and Enrollment Certificate in SCMS.

It is worth noting that the majority of the projects presented are only experimental projects. Only SCMS, EU CITS and SCME will be deployed on the field involving citizens. However, because some of them were pilot projects, and because we wanted a holistic survey on the PKI standards and projects, we presented them in this work.

4.2. IEEE PKI architecture

IEEE 1609.2 standard [95] specifies a set of security services to support ITS communications. It defines secure messages formats and processing in Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions. For PKI infrastructure, the standard classifies all the entities that provide or use IEEE 1609.2 security services into two categories; Certificate Authority entities (CA entities) and End Entities (EE):

1) Certificate Authority entities (CA entities): Issue certificates and Certificate Revocation Lists (CRLs). There are defined three types of CA entities.

- Root CAs: Root CAs are trusted by all entities and issue certificates to all other CA entities and End Entities within a defined region. The latter is specified by the region field in the Root CA's certificate and can indicate that the Root CA is worldwide. The goal behind issuing certificates to other CA entities, is to authorize them to issue certificates or CRLs to end entities.
- Secure Data Exchange CAs: SDE-CAs issue certificates to end entities that use/send application secured messages. An SDE-CA is responsible for issuing certificates to SDE Entities (SDEE) and to other SDE-CAs. It is authorized to issue the following types of certificates:
  - SDE-CA;
  - SDE-Enrolment: used by an entity to request new certificates;
  - SDE-Identified-Localized: used by the SDEE in order to secure its communications (also called communication certificate);
  - SDE-Anonymous: do not own any identity information about the owner. Their usage ensures anonymity and no tracking of the owner [80];
  - CRL-Signer: The CRL Signers are CRLs distribution centers, which represent entities that store and distribute certificates revocation lists (CRLs).
- WAVE Service Advertisements (WSA) CAs: WSA-CAs issue certificates to end entities that broadcast WSAs in order to advertise specific set of services e.g., log upload.

2) End Entities: All other entities that use IEEE certificates, but cannot issue certificates or CRLs, are end entities. There are defined two types of end entities: Secure Data Exchange Entity (SDEE) and

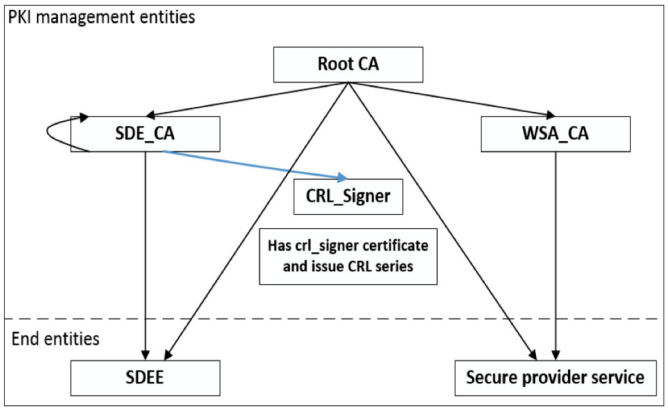


Fig. 6. IEEE generic PKI architecture [95].

Secure Provider Service Entity (SPSE). End Entities include ITSS-V, ITSS-R, application servers and software applications.

For the user's privacy protection, the IEEE 1609.2v2 standard defines anonymous certificates issued by the Root CA or SDE-CA to SDEEs. The IEEE 1609.2v2 anonymous certificates are communication certificates without identification information.

Fig. 6 describes a generic IEEE PKI architecture. Multiple projects adopt this architecture as the rest of this section shows.

4.3. ETSI PKI architecture

The ETSI ITS Technical Committee Working Group 5 is responsible for the ITS security architecture, providing security standards as well as guidance on the use of security standards. ETSI TS 102 940 [140] and ETSI TS 102 941 [90] [141] standards specify a security architecture and the trust and privacy management for ITS communications. They identify: (1) functional entities required to support security in an ITS environment; (2) relationships that exist between the entities themselves and the elements of the ITS reference architecture; and (3) roles and locations of a range of security services for the protection of transmitted information and the management of essential security parameters. The latter include identifier and certificate management, PKI processes and interfaces as well as basic policies and guidelines for trust establishment.

In order to provide communications' security between ITSSs, a range of security services are available. Indeed, different categories of security services are defined such as enrollment, authorization, integrity, plausibility and validation. Security services are provided on a layer-by-layer basis, such that, each service operates within one or several ITS architectural layers, or within the security management layer of the communication stack.

Communications' security services require numerous components to ensure their functional model:

- Enrollment Authority: authenticates an ITSS and grants its access to ITS services and communications.
- Authorization Authority: provides an ITSS with authoritative proof that it may use specific ITS services.
- Sending ITSS: (1) acquires rights to access ITS communications from Enrollment Authority, (2) negotiates rights to invoke ITS services from Authorization Authority, and (3) sends single-hop and relayed broadcast messages.
- Relaying ITSS: receives broadcast messages from the sending ITSS and forwards them to the receiving ITSS if required.
- Receiving ITSS: receives broadcast messages from the sending or relaying ITSS.

The documents also present the ITS security reference points through which information are exchanged, the types of information carried across these security reference points (CAM, DENM, authorization parameters, request for permissions and so on), and security services that each security reference point supports.

It is necessary for an ITSS to get/provide a secure access to common resources such as services, information and protocols. These security requirements can be separated into two parts: external security and internal security. External security represents the security related to the behavior of the ITSS as a communication end-point, while internal security represents the security related to the ITSS as a processing platform and application host.

ITS communication system relies on indirect trust relationships built upon certification ensured by trusted third parties such as the Enrollment Authority (EA). EA allows an ITSS to be a part of the ITS communications by providing access control and permissions. The described standards [90,140,141] explain how ITS communications should support trust, privacy, access control, and confidentiality regarding ITSSs: (1) trust is supported by provisioning ITS stations with certificates allowing it to assert their permission to use the ITS system and to use specific ITS services and applications. (2) privacy is supported by using pseudonyms that can be used to replace a more meaningful and traceable identifier. (3) access control is ensured by giving ITSSs cryptographically signed certificates from the Authorization Authority (AA), which allows it to use specific services, or send particular information. (4) confidentiality of transmitted information in unicast communications is protected by the encryption of messages within an established security association.

Security features are ensured by a PKI composed of an Enrollment Authority, Authorization Authority and a Root CA, and used for distribution and maintenance of trust relationships between ITSSs and authorities or other ITSSs as Fig. 7 describes.

Root CA: issues certificates to all other Certificate Authorities. It is the root of trust for all certificates within the hierarchy. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. In order to trust an incoming message, an ITSS must have access to the root certificate at the summit of the hierarchy for the authorization certificate attached to the message.

Enrollment Authority: the EA issues a proof of identity to authenticate the canonical identifier of the ITSS by delivering an Enrollment Certificate (EC). This proof of identity allows to not revealing the canonical identifier to a third party and may be used by the ITSS to request authorization of services from an Authorization Authority.

Authorization Authority: having received the enrollment credentials, the ITSS requests its authorization certificate(s) from the AA. These certificates allow the ITSS to have specific permissions. The separation of enrollment and authorization is an essential component of privacy management.

The ITSS security lifecycle begins with the manufacture phase, and passes to the enrollment phase, authorization phase and maintenance phase as Fig. 8 shows. (1) at the manufacture phase multiple information elements are established in the ITSS. The main elements are:

- canonical identifier.
- contact information for EA and AA: network addresses and public key certificates.
- the set of current known trusted EA and AA that an ITSS may use/request to initiate the enrollment process and trust communications from other ITSS respectively.
- a canonical public/private key pair for cryptographic operations.

(2) at the enrollment phase, the ITSS requests its enrollment certificate from the EA. (3) at the authorization phase, having received

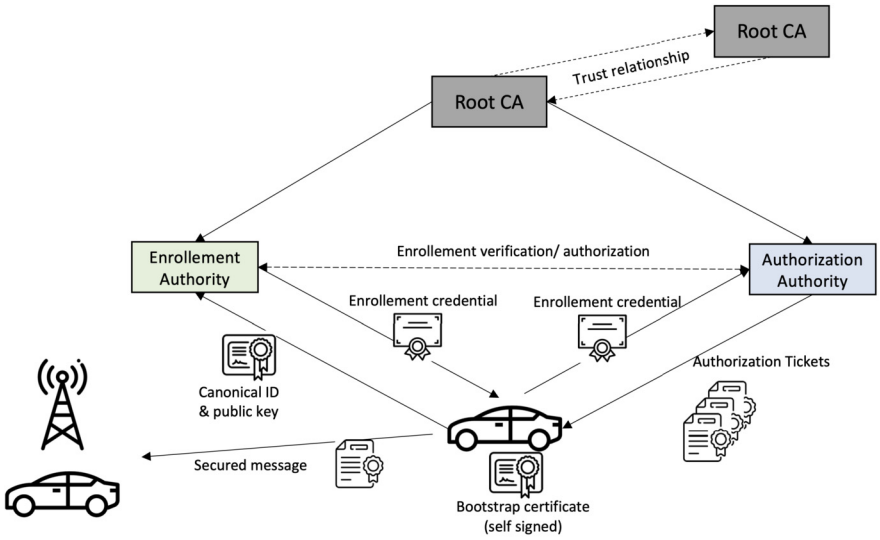


Fig. 7. ETSI generic PKI architecture [140].

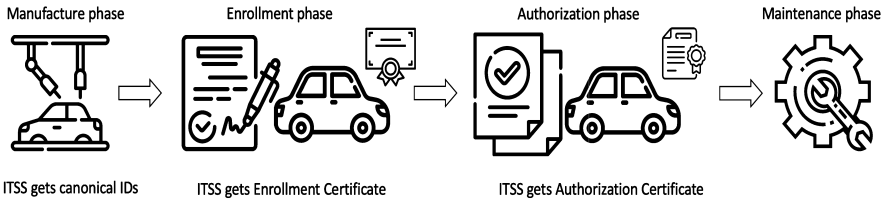


Fig. 8. The ITSS security lifecycle.

the enrollment credentials, the ITSS requests its authorization certificates from the AA. (4) finally, at the maintenance phase, the ITSS will be informed with any changes in EA and AA lists (adding or removing of authorities). The maintenance phase also includes the ITSS certificates renewal and update.

For ETSI based architecture, broadcasted communication messages do not require confidentiality. Indeed, CAMs and DENMs are signed using authorization certificates. Whereas, for some multicast cases and for unicast, communications are encrypted, and key management is required.

ETSI TS 102 731 standard [142] provides high level descriptions of the security services and security architecture. It describes the general ITS G5 security model, and presents related security services for each countermeasure. These security services are divided into two levels: first level, and lower level. Security services identified as first level are those that are invoked directly by applications or other components or layers in the ITS Basic Set of Application (BSA) [142]. Services identified as of lower level are those that are invoked by other security services. The document mapped also countermeasures to CIA paradigm (Confidentiality, Integrity and Availability), and it divides ITS security services into two different groups: security services at transmission (Tx) and security services at reception (Rx). Then, an overview of the ITS security architecture is presented. It includes sending ITSS, receiving ITSS and the ITS network. Connections, associations and interfaces between these three entities are also presented. After, the document presents the ITS authoritative hierarchy that the manufacturer, Enrollment Authority, and Authorization Authority builds. It gives also, the role of each of these entities, the different trust assumptions on which relies the security of an ITS system, and ITS security parameters' management such as identities and identifiers, and authorization and privacy with authorization tickets. The last part of the standard presents the ITS security services such as enrollment credentials, authorization tickets, security associations, single message services, integrity services, replay protection services, accountability services, plausibility validation, remote management and report misbehaving ITSS.

Table 9
Mapping of ETSI and C2C-CC CAs' names.

ETSI Certification Authorities	C2C-CC Certification Authorities
Root Certificate Authority (RCA)	Root Certificate Authority (RCA)
Enrolment Authority (EA)	Long Term Certificate Authority (LTCA)
Authorization Authority (AA)	Pseudonym Certificate Authority (PCA)

4.4. Car-2-Car Communication Consortium PKI architecture

The Car-2-Car Communication Consortium (C2C-CC) [143] is a non-profit organization consisting of nearly all European vehicle manufacturers, several suppliers, research organizations and other partners. The overall objective of the C2C-CC is to implement C-ITS. The technological focus is on a 5.9 GHz ad-hoc network providing low latency communication and geo-routing. It closely works together with the European standardization organizations in particular ETSI TC ITS in order to achieve commonly agreed European standards for ITS.

As Fig. 9 shows, the security working group of the C2C-CC defined the same PKI architecture as ETSI. However, names of ITS authorities are different. Table 9 maps C2C PKI authorities into ETSI ones. Nonetheless, C2C-CC PKI does not use ETSI certificates, but, IEEE ones [144] instead.

A C2C-CC PKI contains the following authorities:

Root CA (RCA): defines common policies among all subordinate LTCAs and PCAs. The RCA only issues certificates for Long-Term CAs and Pseudonym CAs. A certification process which needs interaction with the RCA is only required once a new LTCA or PCA is created, and when the lifetime of an LTCA or PCA certificate expires. In C2C-CC proposal, it is possible to have multiple RCAs.

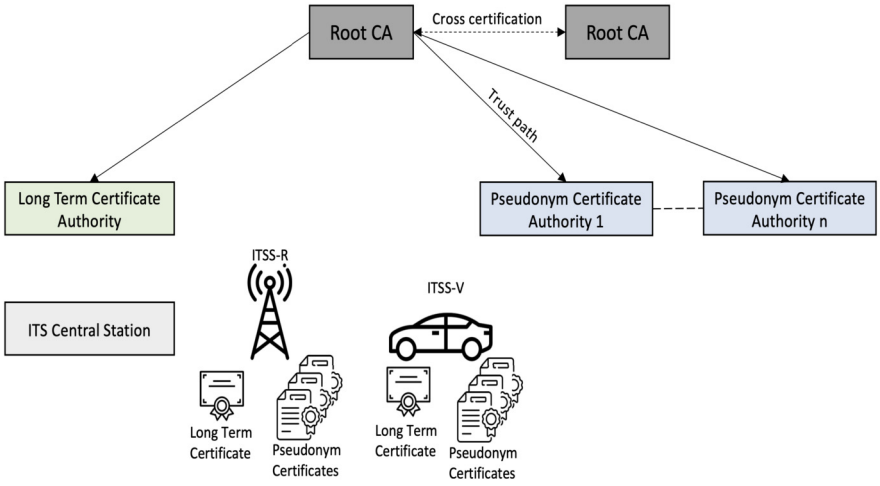


Fig. 9. C2C-CC PKI architecture [144].

In this case, they may cross-certify each other. Every cross certification is done with two new certificates stating the mutual trust status between both Root CAs [144].

Long-Term certificate authority (LTCA): issues Long-Term certificates (LTCs) to ITSS. It provides suitable processes to associate an LTC to an ITSS, to revoke and to update it. For the provisioning of PCs, an efficient refill process is required, but it is sufficient for an ITSS to prove ownership of the private key of its LTC to acquire new pseudonyms. LTCs are valid for a longer time period and are dedicated to identify and authenticate the respective ITSS within the PKI and potentially other services, but they are never exposed to V2X communications for privacy reasons. Each ITSS has only one valid LTC at a time. Within a C2C PKI it is possible to have multiple LTCAs and because of the close relationship of LTCs to ITSS devices, C2C standard recommends that LTCAs are operated by entities that build or maintain the stations such as manufacturers or their suppliers [144].

Pseudonym certificate authority (PCA): issues Pseudonym Certificates (PCs). An ITSS have multiple valid PCs at the same time. These PCs are used for V2X communications and have to be changed frequently. A PC has a short lifetime and minimal information to preserve the privacy of the sender. Within a C2C-CC PKI it is possible to have multiple PCAs.

4.5. Security Credential Management System

In 2014, the National Highway Traffic Safety Administration (NHTSA) Department of Transportation (DOT) published a Request for Information (RFI) named Vehicle-to-Vehicle Security Credential Management System (V2V SCMS) [145]. The purpose of this RFI, is to seek responses concerning the establishment of an SCMS, security approaches for a V2V environment, and technical and organizational aspects of the SCMS. As conclusion, PKI system was selected as the security solution to adopt.

Further, in 2016, DOT and NHTSA, along with Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium[4] published parts of the SCMS Proof-of-Concept specification [91]. The latter extends the last RFI to V2I communications and consider RSU usage. [91] focus primarily on PKI description, the used certificates and their management.

SCMS PKI extends IEEE proposal and its entities are grouped into 4 classes: (1) Overall Management, (2) Registration and Enrollment, (3) Certificate Management, and (4) Misbehavior Management.

As Fig. 10 describes, the SCMS PKI relies on multiple authorities called SCMS components and on ITSSs (ITSS-V and ITSS-R) called End Entities (EE). All EE own implicit type certificates in order to save storage space and over-the-air bytes, while, all the SCMS component certificates are of explicit type [91].

Currently, there exist three Department of Transportation pilot projects that implement SCMS PKI in the U.S.: the New York City pilot,[5] the Wyoming pilot[6] and the Tampa-Hillsborough Expressway Authority pilot.[7] The aforementioned projects are part of the Connected Vehicles Pilots Deployment Program that the USDOT launched. It seeks to combine connected vehicle and mobile device technologies in innovative and cost-effective ways to improve traveler mobility and system productivity, while reducing environmental impacts and enhancing safety.

1) Certificates: According to its type, an ITSS can have multiple certificates of different types; enrollment, pseudonym, application, identification and many others.

ITSS Enrollment Certificate: it serves as the main identification document of the ITSS. It helps to identify the ITSS during the request of other certificates. Each ITSS owns only one Enrollment Certificate, provided during the initialization phase (called bootstrap process in SCMS context). It has a long validity period. Generally, equal to the operational lifetime of the ITSS-V. Nonetheless, it can be revoked by the Registration Authority through the use of its internal blacklist. It includes also an SSP list that defines the authorized application activities.

ITSS-V Pseudonym Certificate: it serves to authenticate Basic Safety Messages (BSM) and misbehavior reporting through messages signature using a butterfly key [146] in a way to ensure anonymity and non tracking of the user (ITSS-V). PCs do not include an encryption public key. Furthermore, in contrast with the Enrollment Certificate, an ITSS-V is given multiple simultaneously valid PCs that have a short lifetime, so that it can change them as often as necessary and possible.

Identification Certificate: Like Pseudonym Certificate, the Identification Certificate serves to authorize the use of V2I applications. The provisioning process of identification certificates is very similar to that of pseudonym certificates. However, an ITSS-V has only one identification certificate valid at a time for a given application.

[4] Members of the consortium are Ford Motor Company, General Motors LLC, Honda R&D Americas Inc, Hyundai-Kia America Technical Center Inc, Mazda, Nissan Technical Center North America Inc, and Volkswagen Group of America.

[5] https://www.its.dot.gov/pilots/pilots_nycdot.htm.

[6] https://www.its.dot.gov/pilots/pilots_wydot.htm.

[7] https://www.its.dot.gov/pilots/pilots_thea.htm.

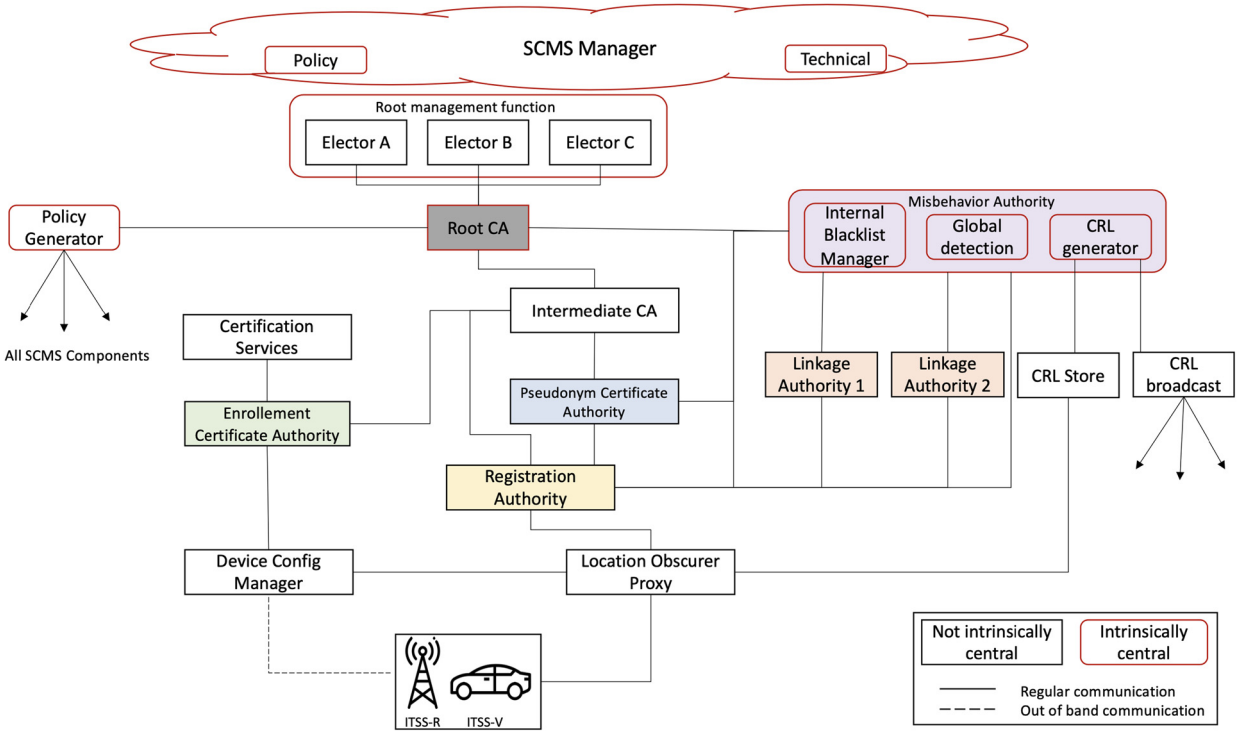


Fig. 10. SCMS PKI architecture [91].

It includes an optional encryption public key because none of the current V2I applications require encryption. Also, like pseudonym certificates, butterfly keys are used to facilitate efficient bulk generation of identification certificates by the RA, using only a single certificate request.

Application Certificate: The Application Certificate serves for authentication and encryption features by the ITSS-R. The application certificate might contain an encryption public key. Since the ITSS-R is always motionless, there is no need to pseudonymity and non tracking features. Thus, only one valid certificate at a time is provided to the ITSS-R. Nonetheless, for continuity reasons, an ITSS-R has extra certificates that are valid for the next time periods.

2) Authorities and entities: Concerning authorities, SCMS introduces multiple new authorities such as Electors concept or Intermediate authorities. Authorities' certificates are of explicit type to support P2P certificate distribution.

Electors: the Electors are offline entities involved in the management of the Root CA. They are used primarily for the Root CA certificate management, including adding and removing a Root CA. These actions are possible through votes done by a quorum composed of more than 50% of the electors. As elector certificates are self-signed, their integrity must be ensured by other means than cryptographic signatures, e.g. tamper-proof hardware. For the same reason, provisioning and update of elector certificates are realized through out-of-band means.

Root Certificate Authority (Root CA): the Root Certificate Authority represents the center of trust of the system, and the end of trust chain. It produces a self-signed certificate verifying its own trustworthiness. Usually the Root CA certificate has a very long lifetime, as its changing is extremely difficult, time consuming, and financially expensive [91]. Only a quorum of Electors can issue root management messages and add them to a CRL to revoke a Root CA certificate. The main role of this authority is to issue certificates to subordinate CAs such as Misbehavior Authorities, Linkage Authorities, Registration Authorities and so on. Root CA also operates in offline environment to prevent any security threat which can have a critical impact on the security of the whole system.

Intermediate Certificate Authority (ICA): the intermediate Certificate Authority is considered as an extension of the Root CA. It is used in the sole goal of issuing certificates to other SCMS components. Thus, it provides flexibility by removing needs to connect to RCA, which is offline, each time a new SCMS entity is added to the system. However, Intermediate CA does not hold the same authority as the Root CA since it cannot self-sign a certificate.

Enrollment CA (ECA): the ECA assigns a long term certificate to EE at their first connection to the SCMS system at the bootstrap process.

Pseudonym Certificate Authority (PCA): the main roles of the PCA are: (1) to issue short term certificates to ITSSs (Pseudonym, Identification and Application certificates). And (2) to collaborates with the Misbehavior, Registration, and Linkage Authorities in order to identify linkage values to place on the CRL if a misbehaving ITSS is detected.

CRL generator: when a certificate is revoked, the CRL generator adds it to the CRL. CRL generator certificates are issued by the Root CA and can be used only to sign CRLs. The revocation of CRL generator certificates can be realized only by either Root CA or ICA.

Policy Generator: policy Generator certificates are issued by the Root CA. The Policy generator uses its private key (associated to its certificates) to sign the global policy configuration files that are distributed to SCMS components.

Linkage Authority (LA): the Linkage Authority is responsible for: (1) generating linkage values as response to RA and PCA requests. And (2) Communicate only with the RA to provide these values. The Linkage values help PCA calculating a certificate ID in a way to connect all short-term certificates from a specific device for ease of revocation if a misbehavior is detected.

Location Obscurer Proxy (LOP): the main roles of LOP are. (1) to obscure the location of the EEs seeking to communicate with the SCMS functions. (2) to shuffle misbehavior reports that the EEs send to the Misbehavior Authority. And (3) to increase the partic-

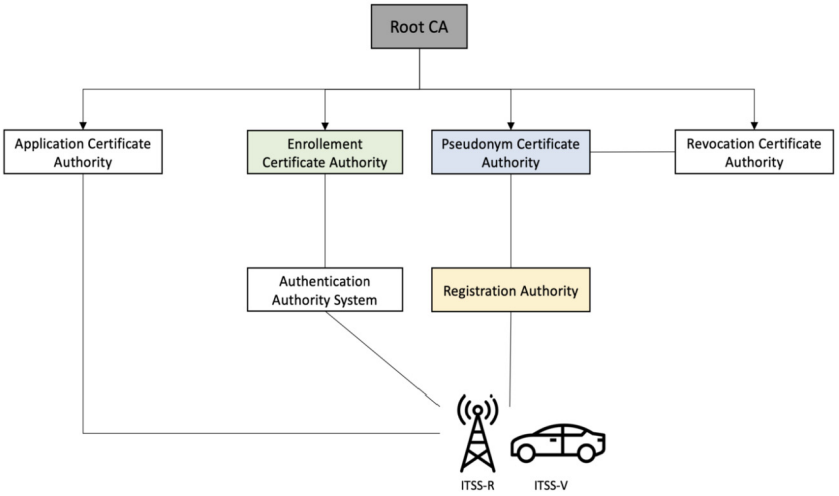


Fig. 11. SCME PKI architecture.

ipants privacy. For privacy purposes, the LOP can mask the source IP address and route of the EE from the RA.

Registration Authority (RA): the Registration Authority (RA) is an intrinsically non-central component of the SCMS. It is possible to have multiple RAs active at the same time in the SCMS. However, an ITSS is configured to contact only one RA. The main roles of this authority are: (1) to receive and to respond to certificate requests from authorized ITSSs via LOP. (2) to initiate certificate requests to a PCA to generate certificates. (3) to initiate requests and to receive linkage values from both LAs used in ITSSs revocation. (4) to perform the necessary key expansions before the PCA performs the final ones. (5) to send certificate requests to the PCA. And (6) the RA must respond to requests from the central MA to add ITSSs to its internal blacklist and to support misbehavior investigation. The RA receives requests from different ITSSs. Therefore, in order to prevent correlating certificates IDs with users, it shuffles these requests before sending them to the PCA. Additionally, it maintains a blacklist of enrollment certificates to reject any request from a revoked ITSS.

Misbehavior Authority (MA): this entity is responsible for detecting misbehaviors by performing plausibility checks to messages, or detecting potential malfunctions or malfeasances within the system. Its main roles are: (1) to process misbehavior reports. (2) to collaborate with the CRL generator on the production of CRL. And (3) to collaborate with the PCA, the RA, and the LA to acquire necessary information about a certificate and create entries to the CRL though CRL Generator.

SCMS Manager: SCMS Manager is the primary managerial component of the SCMS. It is responsible for managing all other component entities called Certificates Management Entities (CME). It provides the policy and technical standards for the V2X system, ensures interoperability, security, privacy and auditing of the system, and manages the activities required for operation of the SCMS.

Device Configuration Manager (DCM): DCM is responsible for: (1) providing the devices access to new trust information such as updates to authorities certificates, policy decisions, and technical guidelines issued by SCMS Manager. (2) sending software updates to devices. (3) coordinating initial trust distribution with devices by passing on credentials for other SCMS entities. (4) providing devices with information it needs, in order to request short-term certificates from the RA. (5) providing a secure channel to the ECA to communicate Enrollment Certificates to devices.

Two types of connections are used between devices and DCM, an in-band communication that passes through LOP, and an out-of-band communication that passes directly from the device to the ECA via the DCM.

4.6. Security Credential Management Entity (SCME)

The Chinese Ministry of Industry and Information Technology (MIIT) currently standardizes a secure V2V communications architecture and a PKI design [147] [148] [149] that Fig. 11 shows. The SCME design includes the following authorities:

- **Root Certificate Authority (Root CA):** represents the root of the trust chain and issues certificates for the lower-level CAs.
- **Enrollment CA (ECA):** issues Enrollment Certificates (EC) to V2X devices which allow them to request other certificates such as Pseudonym Certificates (PC) and Application Certificates (AC). One ITSS-V can have multiple ECs, e.g., for different geographic regions of state authorities depending from different ECAs.
- **Pseudonym CA (PCA):** issues Pseudonym Certificates (PC) to ITSS. The PCs are used to sign the messages sent. The number of PCs and the validity period is configurable, and the current MIIT recommendation is to use 20 PCs per week.
- **Application CA (ACA):** issues application authorization certificates for selected applications. This function is not fully defined yet [148].
- **Revocation CA (RCA):** issues and manages the CRLs. The RCA also manages the Misbehavior Authority (MA) in order to directly revoke the misbehaving nodes.
- **Authentication Authority System (AAS):** authorizes the ITSS to request and receive an EC from the ECA e.g., through the use of tokens.
- **Registration Authority (RA):** helps in the PC requests through (1) the validation of PC requests from ITSS. (2) the performance of supporting functions e.g., the butterfly key expansion [150] [125]. (3) the forwarding of requests to the PCA. And (4) the reception of PCA's responses and the bundle of the received PCs for ITSS. The RA also provides configuration information, CRLs, and certificate chain information to ITSS. It also provides linkage values because it comprises a Linkage Authority (LA). The linkage values are used by the MA for misbehavior investigation and efficient revocation.

4.7. SCOOP@F

SCOOP@F project is a French initiative launched by the ministry of sustainable development. It is divided into two parts: (1) the

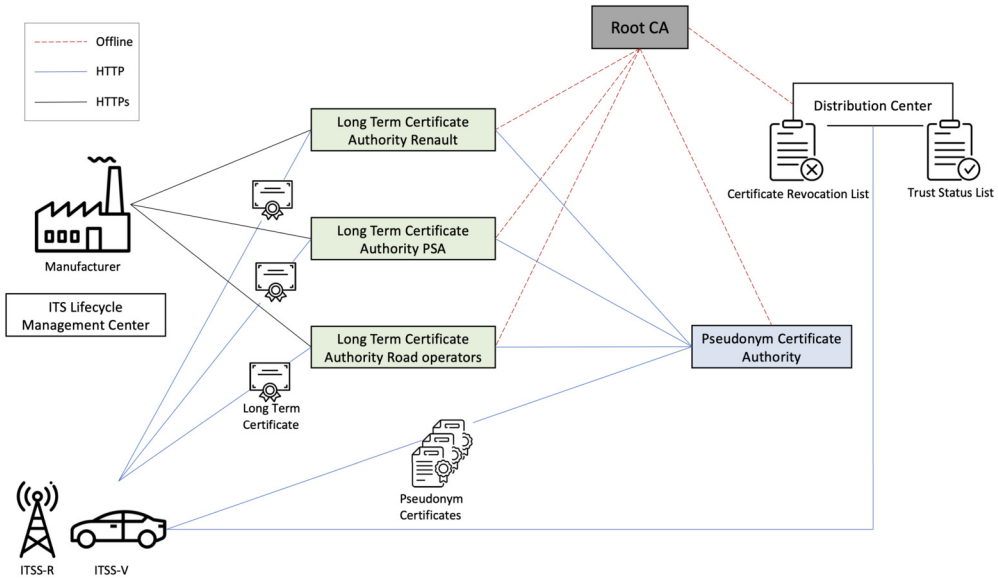


Fig. 12. SCOOP@F PKI architecture.

first part *SCOOP@F Phase 1* involves several partners such as local authorities, state services in charge of national road management, automotive industries such as Renault and PSA, automotive suppliers, universities and research centers. It represents a Cooperative ITS pilot deployment project that intended to connect approximately 3000 vehicles with 2000 kilometers of roads at the national scale [151]. (2) the second part aims at the evolution of the project and the development of a common interoperable C-ITS infrastructure at the European level and involves other European countries such as Spain, Portugal, Netherlands, Austria, Belgium, the Czech Republic, Germany, Slovenia, Sweden, Denmark, Hungary, Greece, Ireland and the UK in the context of two other projects (1) C-Roads platform[8] [92] and (2) InterCor (Interoperable Corridors).[9] One of the main purposes of this project is the deployment of a dedicated ITS PKI. Fig. 12 describes the architecture of SCOOP@F PKI. The PKI proposed is based on ETSI standards. However, authorities' names are different:

Root Certificate Authority (RCA): within SCOOP@F only one RCA is considered. It is a CA characterized by having a self-signed certificate (issuer and signer are the same). There is no cross-certification of RCA certificate with other CAs and it can not be revoked in a normal manner i.e. being included in a Certificate Revocation List. RCA is always used offline, thus it is never connected to any network.

The RCA supports the following PKI services: (1) the generation of Root CA keypair and self-signed certificate. (2) the generation of CA certificates. (3) the signature of CRL and Trust Status List (TSL). (4) the revocation of CA certificates. (5) the update of CRL and TSL. And (6) the log trail generation.

Long Term Certification Authority (LTCA): within SCOOP@F three LTCAs are implemented, two LTCAs for cars' manufacturers (Renault and PSA) and one for road operators. Each LTCA is responsible for: (1) the authentication of manufacturers to register ITSSs. (2) the authentication of ITSS deactivation requests. (3) the management of ITSS status. (4) the generation, issuance and signature of Long Term Certificates (LTCs). And (5) the management of PCA validation requests for PC requests.

Pseudonym Certification Authority (PCA): SCOOP@F PKI includes one PCA which role is: (1) the management of Pseudonym Certificates (PCs) requests. (2) the generation, issuance and signature of PCs. (3) the management of communication with the LTCA and the DC in order to validate PC Request. (4) the authentication of other authorities using TSL.

Distribution Center (DC): The DC is the entity that publish CRL and TSL after getting them from the RCA. The DC is also responsible for the log trail generation.

4.8. ISE

ITS Security (ISE) is a French project that studied security challenges related to Intelligent Transportation Systems (ITS) communication and messages authentication. The project's main objective is the design and implementation of a security management infrastructure for C-ITS [152] [153]. Fig. 13 describes the PKI architecture proposed by ISE project which is based on ETSI standards. Its RCA, EA, AA and DC have the same role as in SCOOP@F. In addition, it includes two entities related to the PKI without being involved in its functioning: (1) Misbehavior Authority and (2) Privacy Authority. The Misbehavior Authority analyzes the collected ITSS' logs for misbehavior detection purposes. In the logs, the ITSSs are identified using PCs. In order to correlate the different Pseudonyms of the same ITSS, Misbehavior Authority cooperates with the Privacy Authority.

4.9. Issue First Activate Later

Issue First Activate Later (IFAL) [154] is an ETSI based PKI, supported and developed by the Dutch ministry of the infrastructure and the environment. It relies on almost the same authorities as designed by the ETSI standards and uses the same nomenclature. Except, due to the complexity of the management and the distribution of CRLs, IFAL does not consider them in its design.

In IFAL, the AA provides the ITSS by a batch of pseudonym certificates that are valid in the far future. The set of certificates is issued in the form of an *IFAL certificate file*. However, the certificates can only be used when they are activated. Indeed, the ITSS receives periodically activation codes that aim at the activation of the certificates in groups corresponding with specified periods of time called *epochs*. To overcome the lack of CRLs, the revoked ITSSs will not be sent such codes.

[8] https://www.c-roads.eu/platform.html.
[9] https://intercor-project.eu/.

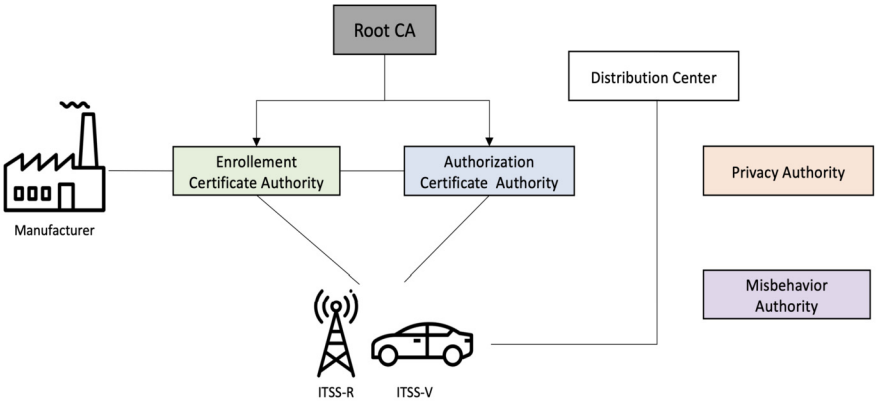


Fig. 13. ISE PKI architecture [152].

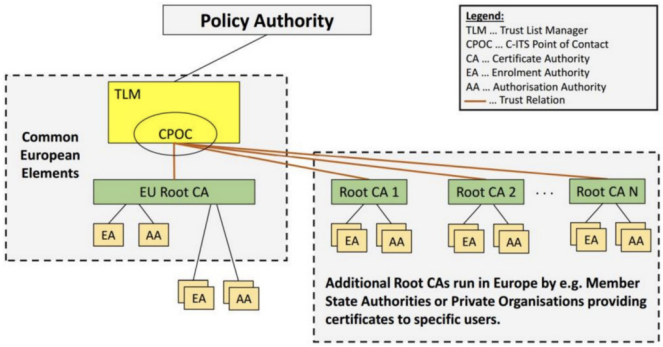


Fig. 14. C-ITS platform project PKI architecture [156].

4.10. European C-ITS platform project

European Cooperative Intelligent Transport Systems (Eu C-ITS Project) [155] [156] also called C-Roads is an upper layer PKI including national or industrial PKI for C-ITS usage. Fig. 14 describes its architecture. This project is launched under the authority of the European commission and includes several members from different European countries such as academics, public entities and industrials. For now, a Certificate Policy (CP) presenting the entities and the interactions between them is under review [156].

The **Policy Authority (PA)** is an organizational authority in the Eu C-ITS Trust Model which: (1) reviews, approves or rejects Trust-List Manager (TLM) registration requests. (2) reviews, approves or rejects RCAs' of the Europe C-ITS membership. But, also their Certificate Practice Statement (CPS), their incident reports, audit reports and their CP change requests. (3) notifies to the TLM the actions needed regarding RCA's certificate (revocation or approval). (4) reviews updates from the TLM about the European Certificate Trust List (ECTL). And (5) notifies all the Eu C-ITS RCAs when an update of the CP occurs.

The **Trust-List Manager (TLM)** is an operative authority which: (1) creates its self-signed TLM certificate (Super Root Certificate) following PA's approval and delivers its certificate to the C-ITS Point of Contact (CPOC). (2) signs the ECTL with its own private key. (3) follows the actions needed to be taken for an RCA's membership regarding information sent by the PA. And (4) notifies the PA about changes made on the ECTL.

The **C-ITS Point of Contact (CPOC)** is an operative entity which: (1) forwards RCA requests to the PA. (2) publishes the ECTL and TLM certificates to all C-ITS PKI entities. And (3) sends the TLM certificate so each entity from the European sub-PKI can verify the ECTL.

An interesting feature in this architecture is the offer of a common Eu Root CA to countries which do not want to get involved in the management of their own PKI. But at the same time, let countries or private entities which desire to be part of the Eu C-ITS trust model to plug their own PKI (RCA and sub CAs) to the Eu C-ITS PKI. Another interesting feature relies on the choice to not consider a sub PKI per European country but to let any European actor (governmental or private) to be part of this trust model. For instance, if a private company has some factories in two European countries and its IT team with its RCA in another country. If each country has a conflictual CP/CPS with another country, things can become legally complex. This is why private companies can deploy their own PKI independently of the multiple European countries where they are involved.

As described earlier, there exist different ITS communications. Among them PKI requests/responses are of a particular criticality because of the sensitive data they carry. Therefore, advanced security mechanisms are applied to secure them. In the next section we describe the different PKI requests/responses and their security mechanisms.

5. PKI requests

In this section, we describe the different PKI communications, which aim to provide ITSSs with different types of certificates (Enrollment and Pseudonym Certificates). The communication profile used to achieve a PKI communication changes from a project to another. For example, In SCOOP@F, IP over G5 communication profile is used. These communications, often called PKI requests and responses, mostly comprise critical data that must be protected and authenticated for users' privacy. However, the main standards that aim the design of PKIs suffer from the lack of a complete end-to-end process, adapted to the different types of PKI requests and responses. To the best of our knowledge, sole SCMS, SCME, SCOOP@F, IFAL, PRESERVE, and C2C-CC projects define such a protocol. In this section we describe three different approaches for PKI requests achievement: a traditional approach implemented by SCOOP@F and PRESERVE[10] projects, and two optimized approaches. The first relies on butterfly keys [125], performed by SCMS and SCME and the second called Issue First Activate Later (IFAL) implemented within IFAL PKI. [154].

5.1. SCOOP@F PKI requests mechanism

Fig. 15 describes the generic message format used to secure and send LTC and PC requests.

[10] The following description concerns SCOOP project. PRESERVE implementation of the protocol is almost the same.

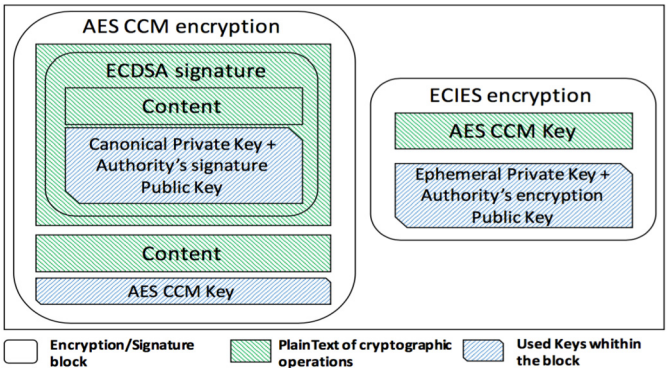


Fig. 15. Generic request and response format [10].

The content of the request (generated public key and the requested certificate profile[11]) or the response (certificate and response code) are, in a first time, signed using an ECDSA private key to ensure the sender's authentication. Afterwards, the content and its associated signature are encrypted using an AES CCM key, which provides confidentiality and integrity thanks to the authentication tag produced by CCM mode. Finally, the AES CCM key is encrypted using ECIES encryption, lowering the risk of eavesdropping. The nonce used in the AES CCM encryption is sent in clear within the PKI request or response.

In order to secure PKI requests and responses, *SignedData* and *EncryptedData* structures have been defined in ASN.1 and encoded following the Distinguished Encoding Rules (DER) scheme in [10].
SignedData: SignedData is a structure that is built to authenticate the sender using the ECDSA signature. This structure specifies the identity of the signer in order to associate the signature to an existing certificate. It consists of: (1) the content to be signed in clear, (2) the digest of the content to be signed, (3) the identity of the signer, and (4) the signature of the cited components.
EncryptedData: the purpose of this structure is to encrypt a message by using AES CCM symmetric encryption. Then, ECIES algorithm encrypts the used symmetric key. Furthermore, a nonce is used for the AES CCM encryption and it is sent in clear to allow the receiver to decrypt and verify the integrity of the content encrypted.

For the ECIES encryption, the sender creates an ephemeral key pair. The ephemeral private key and the receiver's certified Encryption Public Key (EPK) are used to compute the shared secret value required for ECIES encryption. For decryption, the receiver uses its certified Encryption Secret (private) Key (ESK) and the ephemeral public key generated by the sender to compute the shared secret. To allow the receiver to do ECIES decryption, the sender includes the ephemeral public key within the EncryptedData structure.

To summarize, the EncryptedData structure consists of: (1) the AES CCM encrypted content, (2) the AES CCM key encrypted using ECIES, (3) the nonce used for the AES CCM encryption, (4) the ephemeral public key used for ECIES decryption, and (5) the ECIES tag used to verify the integrity of the encrypted AES CCM key.

Table 10 provides a list of the keys generated and used during interactions between the ITSSs and PKI entities. As explained, each ITSS uses two certificates (LTC and PC). Therefore, there are two types of certificate request communications; LTC request/response and PC request/response. However, before an ITSS can execute such requests, the manufacturer provides an initialization phase for each ITSS.

[11] The profile includes the certificate's specific related information.

Table 10
List of used keys for certificates requests in SCOOP@F project [10].

Notation	Name	Description
TSK	Technical Secret Key	Generated by the ITSS and saved in the HSM during the initialization phase
TPK	Technical Public Key	Generated by the ITSS and registered in the PKI during the initialization phase
VSK	Verification secret key	The verification secret key is the used key for the signatures. Its associated public key is contained in the certificate for the signature verification
VPK	Verification public key	The verification public key is included in the certificates. This key is used for the verification of signatures performed by the owner of the certificate
ESK	Encryption secret key	The encryption secret key is used for asymmetric encryption. Its associated public key is contained in the certificate for asymmetric decryptions
EPK	Encryption public key	The encryption public key is, optionally, included in the certificates. This key is used for the asymmetric decryption for encryptions performed by the owner of the certificate
REK	Response encryption key	The response encryption key is included in the PKI requests to allow the PKI servers to asymmetrically encrypt the responses. This key is ephemeral and just used once
RDK	Response decryption key	The response decryption key is used for the asymmetric decryption of the PKI responses

1) Initialization phase: The initialization phase is performed by the manufacturer and consists in the registration of the ITSSs on the PKI. The initialization is performed as follows: (1) the manufacturer generates a technical key pair composed of Technical Public Key (TPK) and Technical Secret Key (TSK). (2) it selects a "Profile" and associates the technical public key to a unique canonical IDentifier (ID), which represents the permanent ID of the ITSS. (3) it specifies the associated Service Specific Permissions (SSP) related to the services supported [136]. (4) it sends a registration request. And (5) the LTCA replies by a registration response to the manufacturer. As a result, the ITSS is registered in LTCA's database and the authorities' (RCA, LTCA and PCA) certificates are stored in the ITSS.

The initialization phase has some requirements: (1) The canonical ID of the ITSS must be unique per LTCA, (2) TSK is generated in the Hardware Security Module (HSM)[12] [157], the NIST P-256 curve is used [136]. TPK is generated outside the HSM. And (3) the certificates of Certification Authorities (CAs) and their access points are installed into the ITSS during the initialization phase as mentioned above.

The communication between the ITSS manufacturer and the LTCA for the registration of the ITSS needs to be secured. Therefore, the communications are achieved through a secured channel or a dedicated separated physical network to avoid eavesdropping.

2) LTC request and response: Fig. 16 describes an ITSS-V sending an LTC request to the LTCA. Fig. 17 describes the details of this

[12] HSM is a Hardware Security Module used for fast cryptographic operations. It provides security features such as a temper proofed environment to store security elements, strong authentication required and functioning without an operating system that makes it resistant to attacks over the network. It is embedded within the ITSS and provides a temper proof environment to generate cryptographic material.

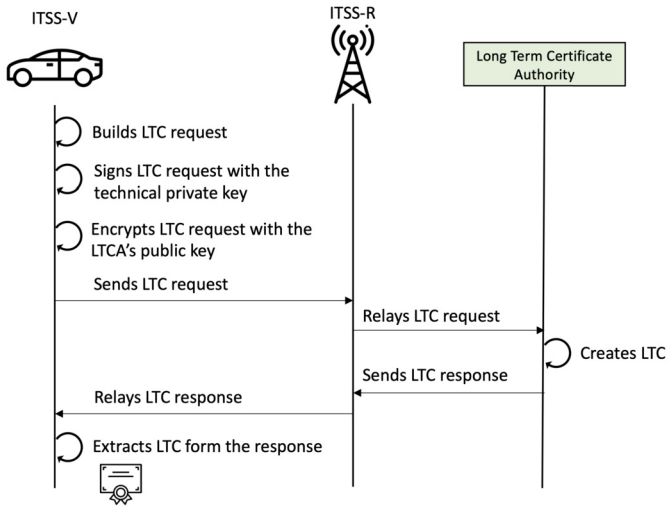


Fig. 16. LTC request and response [10].

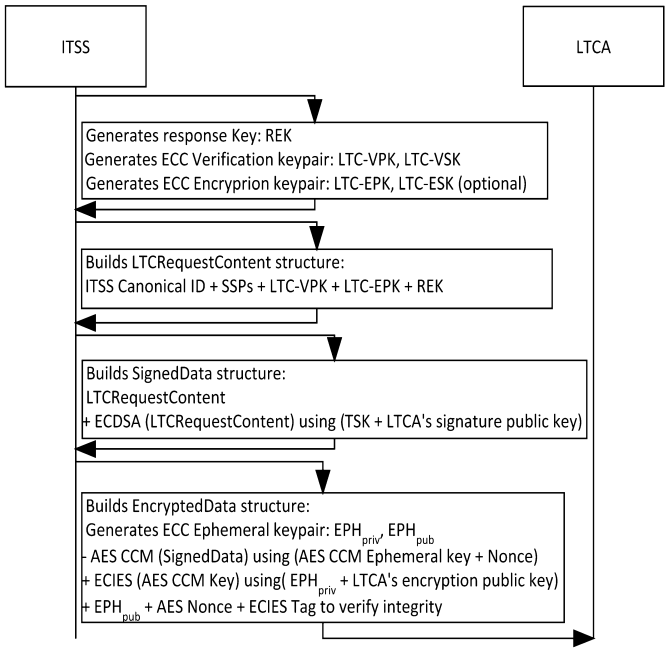


Fig. 17. Sequence diagram of an LTC request [10].

request and how they are secured for the communication relying on the scheme presented in Fig. 15. If the ITSS is registered in the LTCA's database, the latter replies by an LTC response that contains the LTC.

For the LTC request decryption, the LTCA decrypts the EncryptedData structure using its LTCA-ESK and the ITSS's ephemeral public key, contained in the EncryptedData structure. Consequently, the LTCA, first, checks the existence of the canonical identifier and if the verification succeeds, the LTCA creates the ITSS's LTC and sends it through the LTC response. The LTC response's purpose is to provide an answer, either positive or negative, to a received LTC request. If the response is positive, it contains the requested LTC. Otherwise, if the response is negative, it contains an error code.

3) PC request and response: Fig. 18 describes an ITSS-V sending a PC request to the PCA. The PC request requires a verification step that the LTCA must perform. Indeed, when the ITSS sends a PC request signed with its LTC associated private key, the request is relayed to the PCA. Then, the PCA sends a validation request to the LTCA in order to verify the ITSS's LTC. The LTCA replies to the PCA by a validation response. If the LTC is valid, then the PCA creates and sends a PC to the seeker ITSS. Indeed, in order to obtain a PC, the PC request affects both the PCA and the LTCA. More precisely, the PC request includes two structures: "PCRequestContent", earmarked for the PCA and "PCRequestSharedContent" shared between PCA and LTCA (the PCRequestSharedContent is included in PCRequestContent structure) as Fig. 19 describes and which follows the scheme that Fig. 15 presents.

As for the LTC response, the PC response is an answer from the PCA to the ITSS. The response can be positive, containing the requested PC, or negative, specifying the error code. This structure is sent after the validation of the PC request between the PCA and the LTCA.

5.2. Butterfly keys mechanism

Butterfly keys rely on the principle of Elliptic Curve Discrete Logarithm Problem (ECDLP). Fig. 20 describes the process of Butterfly keys generation within SCMS architecture as described in [125] [150]: (1) the ITSS generates two EC key pairs (called Cocoon key-pairs) $(a, A = a\mathcal{G})$ which is the seed for the signing keys and $(p, P = p\mathcal{G})$ which represents the seed for the result's (certificates) encryption keys. Where $\mathcal{G}$ represents the agreed generator point of the curve $\mathcal{E}$ as Equation (1) describes [146].

$$\begin{cases} \mathcal{E} =< \mathcal{G} > \\ \forall A \in \mathcal{E},\ \exists\, a \in \mathbb{N} \textit{ such as} \\ A = a.\mathcal{G}\ (\textit{signing key pair}), \\ \forall P \in \mathcal{E},\ \exists\, p \in \mathbb{N} \textit{ such as} \\ P = p.\mathcal{G}\ (\textit{encryption key pair}) \end{cases} \tag{1}$$

(2) the ITSS generates two Advanced Encryption Standard (AES) keys ck and ek for, respectively, the expansion functions[13] of the signing keys ($f1$) and the encryption keys ($f2$). (3) the ITSS sends ck, ek, A and P to the RA. (5) By receiving these information, the RA is able to generate an extremely large number of derived points. Thus, for each ι,[14] the RA derives signing and encryption public keys as Equation (2) describes.

$$\begin{cases} B_\iota = A + f1(ck, \iota) * \mathcal{G}\ (\textit{signing keys}), \\ Q_\iota = P + f2(ek, \iota) * \mathcal{G}\ (\textit{encryption keys}) \end{cases} \tag{2}$$

The corresponding private keys to these derived public keys are obtained as Equation (3) describes.

$$\begin{cases} b_\iota = a + f1(ck, \iota)\ (\textit{signing keys}) \\ q_\iota = p + f2(ek, \iota)\ (\textit{encryption keys}) \end{cases} \tag{3}$$

(6) the RA sends each pair (B_ι, Q_ι) to the PCA. The PCA does not have a knowledge about which public keys are provided by the same device thanks to the IP source obscurer (LOP). However, the RA can associate each public key to its request. Hence, the PCA must further randomize the public keys to hide them from RA. (7) For each request, the PCA generates a unique random integer c and sets the public key in each certificate to the "butterfly" value $(B_\iota + cG)$. Then, the PCA uses $Q\iota$ in order to encrypt the response towards the RA. The response contains:

[13] An expansion function maps a variable integer ι to another integer in a range from 0 to l, the order of the elliptic curve.

[14] ι goes from 1 to the desired number of certificates.

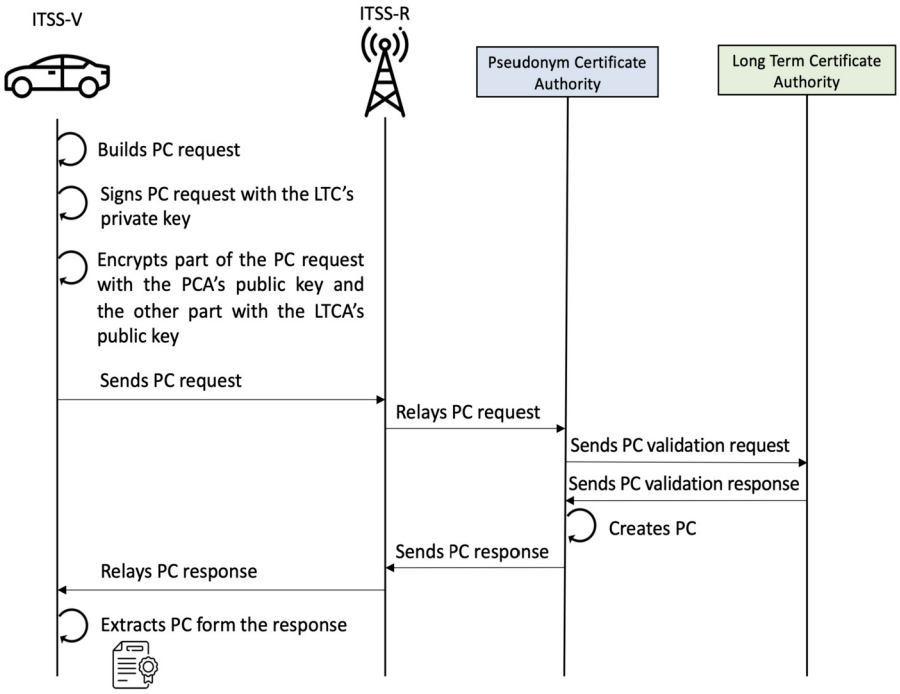


Fig. 18. PC request and response [10].

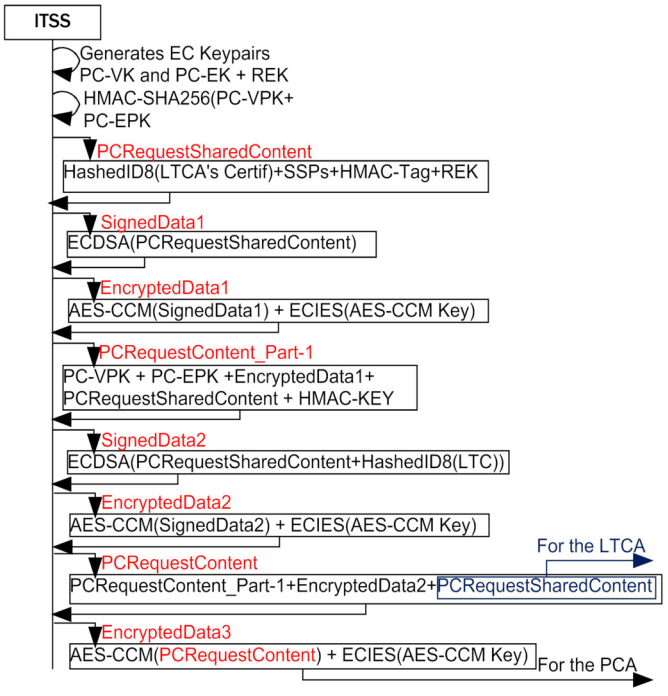


Fig. 19. PC request format [10].

- The certificate containing the public key $(B_\iota + cG)$
- The PCA's contribution to the private key c

(8) the RA sends the encrypted message to the ITSS along with the corresponding ι. (9) the ITSS uses ek, p, ι to calculate q_ι. It uses q_ι to decipher the response and recover the certificate that contains the public key $(B_\iota + cG)$ and c. It then uses ck, a, ι to calculate b_ι. (10) the private key for the certificate is calculated as follows: Butterfly private key $= b_\iota$ (calculated above) $+ c$ (provided by CA). Finally, (11) the ITSS must verify that the private recovered key corresponds to the public key certified by the certificate.

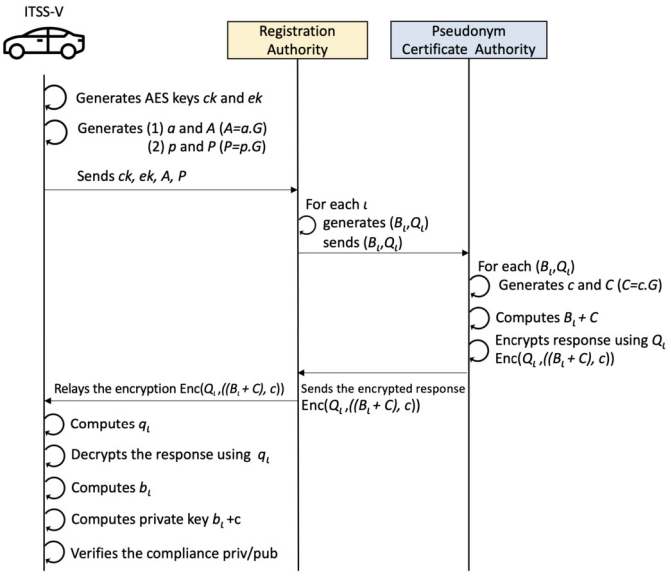


Fig. 20. Butterfly keys scheme for providing PCs [146].

5.3. Issue First Activate Later

As Section 4.9 described, the AA provides the ITSS with an *IFAL Certificate File (ICF)* that contains a set of certificates which can be activated through the reception of activation codes. The *ICF* consists of: (1) an IFAL policy which defines the certificates requested parameters such as the certificate's validity time T_V (in seconds), the overlap time T_O between two consecutive certificates, the total number of certificates N_C, and the number of *epochs*[15] N_E. (2) a start time S corresponding to the start time of the first certifi-

[15] An *epoch* represents a period of time, in which a set of certificates are activated together.

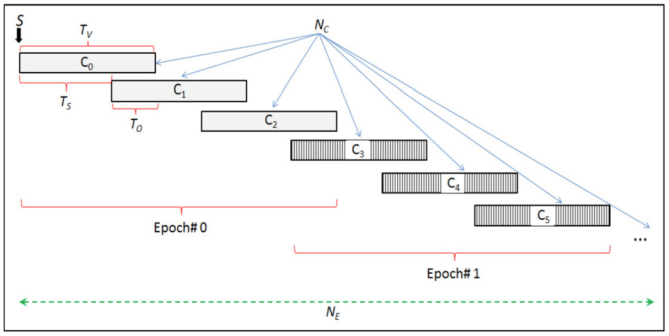


Fig. 21. IFAL certificates' parameters [154].

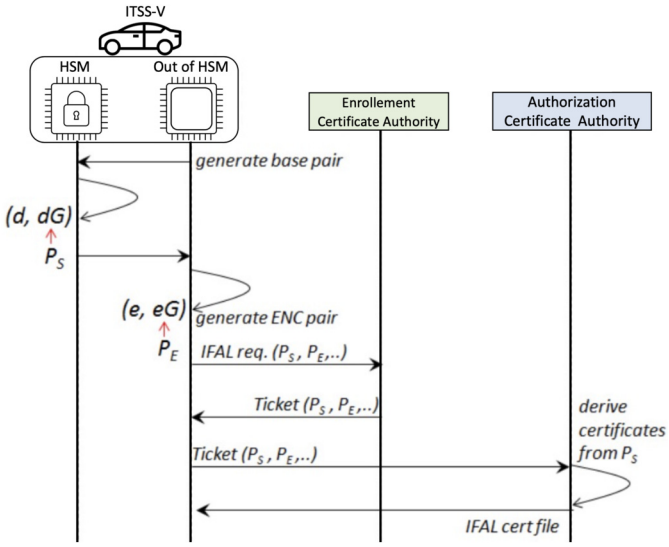


Fig. 22. IFAL certificates' parameters [154].

cate in the file. And (3) a sequence of certificates $C_0, C_1, ..., C_{N_C}$. See Fig. 21.

We describe in the following the main phases of an IFAL certificate lifecycle.

1) IFAL issuance: Fig. 22 describes the certificate file request process. In the latter, the ITSS's generates two ECC keypairs. The first, generated in the HSM and called base keypair (d, dG). The public key dG is noted as P_S. The second keypair (e, eG), used for EA and AA's data encryption, is generated out of the HSM. We note $P_E = eG$. Then, the ITSS sends, to the EA, a first request for an authorization to request *ICF* of a certain IFAL policy (validity time, and so on). The EA registers the request and validates it. On success, it will provide the ITSS with an authorization credential. The latter includes the base certificate request, the public key as well as a unique identifier Id_O. This identifier does not contain direct/indirect identifying information and is only shared by the EA and AA in order to later exchange activation information related to the *ICF* to be issued. Next, the ITSS sends the credential to the AA and requests the *ICF*. On reception, the AA uses the identifier Id_O to register a new entry for the generation of a new *ICF*. Afterwards, relying on the IFAL policy requested, (1) the AA determines the number N_E of *epochs* that the file needs to cover, (2) generates for each *epoch* an associated symmetric key :$K_0, K_1, ..., K_{NE-1}$, (3) stores that in the registry under the new entry, and finally (4) generates the *ICF* which contains a sequence of signed certificates as well as additional metadata such as file's encoding format and the start validity time of the first certificate. The file also contains a secret symmetric transport key K_T encrypted with the public key P_E that was part of the certificate request.

Each certificate in the *ICF* contains a public key P_i. The latter is computed as Equation (4) describes:

$$P_i = \mathcal{K}_2(K_j, ToString(i)) * P_S \tag{4}$$

where $\mathcal{K}_2$ represents a key derivation function [158], i is the certificate's index, K_j is the *epoch* symmetric key, and P_S represents the base public key. The private key corresponding to this public key is equal to the product of the ITSS's base private key d and the derived secret $\mathcal{K}_2(K_j, ToString(i))$. Because, only the ITSS can access and use d, it is the only entity that can use the certificate associated to this public key P_i.

2) Activation and usage of IFAL certificates: Periodically, especially at the near end of the *epochs*, the AA creates a list that contains the identifiers Id_O corresponding to the ITSS that are still activated. For each Id_O, the AA retrieve the corresponding epoch key and encrypts it with the symmetric transport key K_T included in the corresponding *ICF*. This encrypted key represents an IFAL activation code. The latter, is then sent to the EA accompanied with the Id_O. Finally, the EA sends the encrypted *epoch* key to the ITSS in the form of activation code.

When an ITSS needs to sign a message, first, it determines the current time t. Second, it determines the current certificate's index i and the *epoch's* index j as Equation (5) describes.

$$\begin{aligned} i &= (t - S)/T_S \\ j &= i/N_C \end{aligned} \tag{5}$$

Third, it computes the private key associated to the public key P_i of the current certificate (C_i). Fourth, it uses the computed private key to sign the message

5.4. Comparison of PKI requests schemes

PKI requests are vital to C-ITS functioning. Indeed, vehicles need to change frequently their certificates for privacy purposes. Therefore, most of the certificate requests relate to PC requests. Requesting a certificate represents a challenging task for vehicles because of the network's constraints like mobility and speed. Furthermore, the protocol used for the request plays a significant role in this task and has an impact on the resources allocated to it. In this context, *Haidar et al.* [159] provided an experimental study to evaluate the performance of the protocols regarding PKI requests. Their results show that the end-to-end latency between a requesting vehicle and the PKI and the vehicles' speed have an important impact on the success rate of the PKI requests.

[146] describes a performance comparison between the scheme of PKI requests that SCOOP@F uses (described in Section 5.1) and the Butterfly keys scheme that SCMS and SCME use (Section 5.2). The experiments show that the Butterfly keys scheme completely overcomes SCOOP scheme, in terms of time needed to perform PKI requests and to download certificates, as well as their impact on the communication channel.

Currently, there is no implementation study, that compares IFAL scheme, with the others. However, it is clear that IFAL realizes better performances than SCOOP scheme regarding provisioning time. However, the ITSS spends a consequent time in searching the correspondent certificate and to calculate its private key for each operation, especially, knowing that in ETSI based infrastructures, the ITSS can send more than 10 messages per second.

6. Node revocation & trust

Revocation of issued certificates and the trustworthiness of nodes and systems having certificates from different PKIs are

among the biggest challenges to the development of C-ITS. Therefore, in this section we describe these two main concepts and how the current C-ITS systems ensure them.

6.1. Certificate Revocation List (CRL)

Certificates ensure the authentication of system components such as ITSS or authorities in order to operate as trusted entities for V2X communications. The ability to revoke previously-issued certificates is critical to the security of any PKI, that is, to invalidate a certificate before it expires [160] [161]. In traditional web PKIs, there exist numerous revocation methods and systems such as Certificate Revocation Lists (CRL), Online Certificate Status Protocol (OCSP), and Certificate Revocation Tree (CRT) [160]. However, in the C-ITS standards, The technique adopted is CRL. A CRL contains a list of revoked certificates. There are multiple reasons to revoke a certificate, e.g. the detection of a malicious behavior of the ITSS owner. The freshness of the CRL is very important to a C-ITS system. Indeed, having an updated CRL, allows the C-ITS system's users to be aware of current stolen, faulty, misbehaving ITSSs, or about unreliable certification authorities.

The scalability of C-ITS infrastructures is continuously increasing. Therefore, the corresponding CRL sizes are also increasing. As a consequence, it will not be always feasible to download it easily due to C-ITS communication constraints. Hence, most of the systems will implement an incremental number of updates. Nonetheless, this solution does not completely solve the problem and have shortcomings. For example, DSRC requires ITSS-R devices to send the CRL. However, in order to receive large chunks of data, the vehicle must travel past the ITSS-R devices slowly enough that they have enough time to receive the CRL. Therefore, this solution is difficult to achieve in highway scenario (except when there is a traffic jam) and is more suited for an urban scenario (because of the lower speed of vehicles).

Another possible way to distribute an updated CRL is through vehicles communicating updates to each other via the V2V interfaces. While a vehicle may not be in contact with a roadside device longtime enough to complete an update, it is sure to encounter other vehicles.

The use of public certificates in C-ITS implies the need for a revocation system. The CRL described in RFC 5280 [130] and used for X509 certificates, is not suitable for C-ITS systems due to multiple reasons: (1) the presence of non mandatory fields which makes the X.509 CRL unnecessarily size costly for 802.11p/G5 communications. (2) the semantic used in X.509 standard is not compatible with the naming used in the C-ITS context. Therefore, new standards (IEEE and ETSI) were required to define a new CRL structure for V2X context.

1) IEEE CRL: IEEE 1609.2 defines the CRL structure as Fig. 23 shows. This CRL structure is used in multiple projects such as SCMS, SCME and PRESERVE projects.

2) ETSI CRL: In 2012, ETSI defined 2 CRL formats [90] inspired by IEEE 1609.2 as Fig. 24.a and Fig. 24.b describe.

The CRL formats described above do not fulfill the actual needs in V2X specifications, especially due to size constraints. Indeed, the structure proposed is not size scalable, especially in the case where the number of authorities increases.

3) ISE and SCOOP@F CRL: Due to the lack of performant CRL format proposal, the team behind ISE project provided a CRL format for their own PKI project as Fig. 25.a describes. SCOOP@F project also uses this CRL format. It represents a lighter structure than the CRL structures described above. It also requires lesser management by the entities involved compared to the other CRL structures due to the lesser number of its fields.

Fig. 23. IEEE1609.2 CRL.

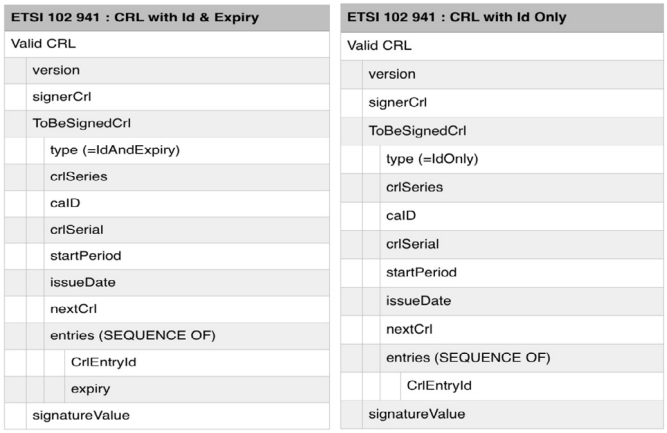


Fig. 24. CRL Structure; (a) ETSI CRL with ID & Expiry; (b) ETSI CRL with ID only.

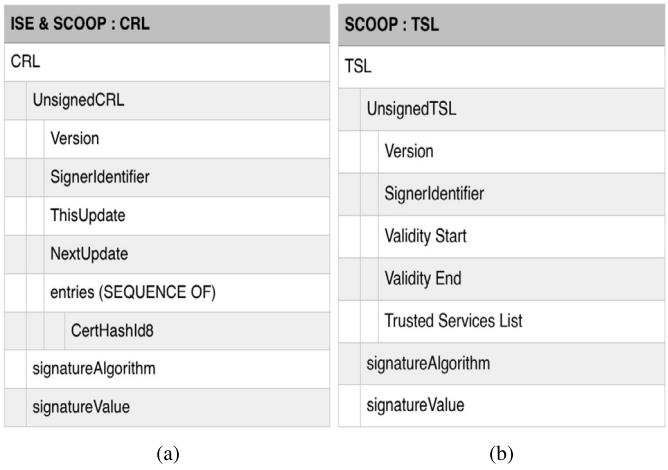


Fig. 25. ISE and SCOOP@F: (a) CRL format; (b) TSL format.

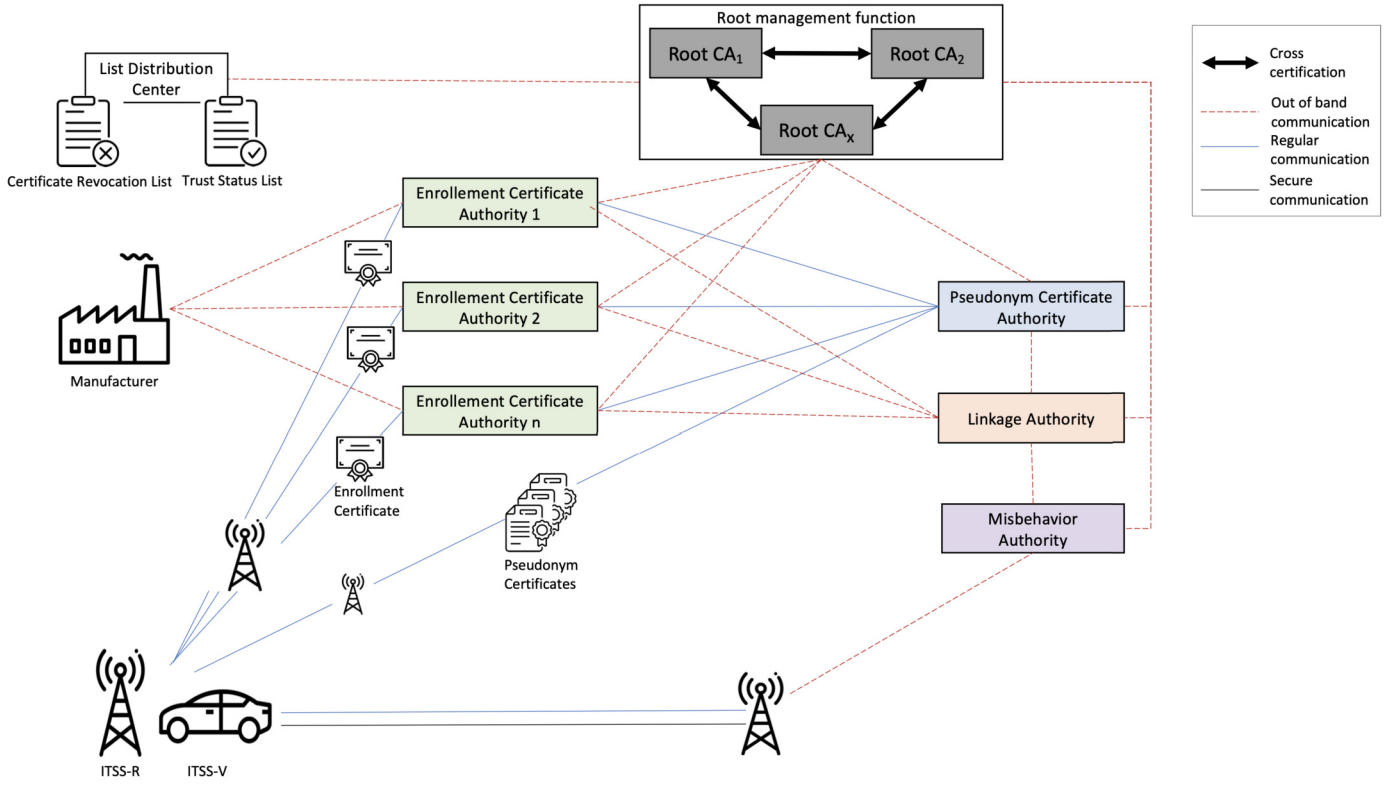


Fig. 26. Generic PKI architecture proposal.

6.2. Trust-service Status List

In addition to the CRL, the Trust-service Status List (TSL) is a list of trusted entities among the V2X environment. This list of entities can be identified with an ID, a string Name, a certificate or a combination of the previous elements.

ISE and the SCOOP@F project define the TSL as a signed list which contains new RCA certificates, LTCA and PCA certificates and PKI service addresses (PCA and DC). It is signed by the RCA [162]. An example of the use of the TSL, is the case where an ITSS receives a message from an ITSS that belongs to a foreigner authority (e.g., a tourist from Germany with his car on a French road). The receiver can verify on the TSL if the sender's authority is trustworthy or not.

1) ETSI: The TSL format in ETSI is under definition (at the time of writing this paper). The lack of standardization is a problem for project deployment. This situation leads to different proposals coming from European deployment project.

2) IEEE: There is no TSL in IEEE. The standard considers that an entity can be either trusted or not trusted and therefore revoked. Thus, the existence of gray zone of trust does not exist in the standard.

3) Others: The SCOOP@F project used its own TSL structure as Fig. 25.b describes. This structure is similar to the one used in ISE. However compared to ISE, the project did not implement the use of link certificate even if the actual TSL structure allows it.

7. The proposal of a generic PKI architecture

In this section we propose a generic PKI architecture. Based on the different projects studied, the PKI proposed includes the most common authorities and ensures the security requirements needed. The authorities were chosen respecting a tradeoff between the number of authorities, modularity and infrastructure complexity. Indeed, from the one hand, if an architecture owns a high number of authorities, it leads to deployment complexity and problems. From the other hand, if the PKI contains a very limited number of authorities, the latter will be overloaded, which can cause multiple problems and slow the whole C-ITS system operation.

Fig. 26 describes our proposal. In the following we describe the different authorities, and we discuss their roles and the reasons behind their architectural choice.

7.1. Root Certification Authority (RCA)

This Root Certification Authority is the top main trust anchor of the PKI. The deployment of multiple RCAs is advised for the following reasons: (1) for scalability and interoperability. Indeed, in order to extend the PKI coverage zone or to merge two or more interoperable PKIs e.g. multiple countries' PKIs. If the solution adopted is to rely on always one RCA, the process will be very long and costly. Indeed, because the hierarchy order of the authorities within each of the PKIs will change, the dependencies to those authorities will also change and all the certificates of these authorities will change which leads to change all the existing certificates on the C-ITS system in addition to the CRL and TSL. However, if there is an addition of the new RCA, with cross certification with the existing RCAs, the hierarchy of the new PKI remains the same, and the dependencies remain the same. Nonetheless, some certificates must change after the cross validation. (2) for resiliency purposes. If an RCA is compromised, all the underlying hierarchy is also compromised and all the certificates need to be changed. However, if the infrastructure owns multiple RCAs, only the hierarchy of the compromised RCA is compromised.

In the case of this proposal, an RCA is responsible for:

- If the PKI includes only one RCA, the latter creates its RCA key pair and its self-signed certificate

- If the PKI includes more than one RCA, each RCA cross certify other RCAs
- Issue certificates for underlying authorities: LTCA, PCA, LA, MA and Lists Distribution Center (LDC)
- Generate and sign the TSL and the CRL

For security purposes RCA is offline and can be reachable only by other authorities.

7.2. Enrollment Certification Authority (ECA)

Enrollment Certification Authority is a core component of the PKI infrastructure because it serves as an entrance gate to the PKI for each ITSS. Thus, it plays the role of a Registration Authority during the Initialization/Bootstrap phase. Within this solution, the implementation of multiple LTCAs is possible. We also recommend that LTCAs are operated by entities that build or maintain the stations such as manufacturers or their suppliers, as advised by C2C-CC standards [144].

The Enrollment Authority role is:

- the registration of the newly created ITSS
- the issuance and renew of enrollment certificates
- the collaboration with Pseudonym Certification Authority in Pseudonym Certificates provision process
- the collaboration with Pseudonym Certification Authority, Misbehavior Authority and Linkage Authority in order to identify misbehaving ITSS

7.3. Pseudonym Certification Authority (PCA)

Pseudonym Certification Authority represents another vital component of the PKI infrastructure because it provides the credentials (pseudonyms) to ensure V2X communications. For each RCA hierarchy, only one PCA is deployed. However, the decentralization of the PCA is highly recommended. We made the choice of implementing only one PCA in order to avoid the complexity of inter PCA collaboration and management. The PCA's role is:

- the issuance of pseudonym certificates to ITS stations which are already enrolled with the EA
- the collaboration with the LTCA in order to verify the identity of the ITSSs that request new PCs
- the collaboration with the ECA, Misbehavior Authority and Linkage Authority in order to identify misbehaving ITSS

7.4. Linkage Authority (LA)

Linkage Authority's main role is to collaborate with PCA and LTCA in order to connect all Pseudonym Certificates of a specific device. This identification is used by the Misbehavior Authority in its detection process. For security purposes, the LA is always offline.

7.5. Misbehavior Authority

This authority's role is the analysis of the system's log stream in order to perform detection of malfunction or malfeasance within the system. In addition, it collaborates with the LA that connects the different PCs of the same ITSS, in order to keep a temporary history of the ITSS' behavior. If an ITSS is detected as misbehaving, the MA creates an entry into the CRL after the collaboration with the LA to identify the ITSS. Finally, the MA sends the identity of the ITSS detected as misbehaving to the RCA in order to add them into the CRL.

7.6. Lists Distribution Center (LDC)

The main role of the LDC is to retrieve the CRL and TSL from the RCA and to provide them to requesting ITSSs. The reason behind having an LDC lies in keeping the RCA offline for security purposes. That way, an ITSS requests CRL and TSL from LDC and not from RCA.

8. Open challenges

Despite the important evolution of C-ITS in recent years, there are still numerous major challenges that C-ITS must face. In this section, we highlight the main open research and operational challenges.

8.1. Misbehavior reporting

Misbehavior will happen and needs to be reported by vehicles to a centralized entity for investigation [163]. The SCMS has a Misbehavior Authority (MA) that allows vehicles to send misbehavior reports. However, details on how the misbehavior investigation is performed have still to be defined. Misbehavior reporting is challenging because the volume of misbehavior that can be expected on the road is unknown, and therefore, it is hard to assess the communication and computation overhead for the vehicles and the PKI (because misbehavior investigation requires collaboration between PKI components). Scalability of the Misbehavior Authority to receive and process misbehavior reports will also have to be assessed [164]. Indeed, to perform the misbehavior investigation the MA has to analyze the reports and identify (1) if the misbehavior is critical, (2) if the multiple pseudonym certificates are linked to the same end entity, and (3) if revocation is needed. Therefore, we identify four challenges: (1) the design of appropriate local misbehavior detection, (2) to define content of misbehavior report [165], (3) to define misbehavior investigation processes, and (4) to assess communication and computation overheads.

8.2. Revocation

ITSS and PKI components could be compromised, and thus, would have to be revoked. The revocation would require to start a new component and providing it with the relevant credentials. It would also require every PKI component and ITSS interacting (directly or indirectly) with it to get its new certificate. In case of the Root CA being compromised, a higher authority is required. In the SCMS design, the Elector CAs are here to solve this issue. However, it is not present in the other PKI proposals, and hence, the issue of Root CA revocation must be addressed. Furthermore, the revocation of ITSS certificates still being one of the top challenges in C-ITS environments due to their scalability [166].

8.3. Quantum Apocalypse

Current PKI implementations rely on non quantum-resistant cryptographic algorithms. In case of being broken by a quantum computer, all the PKI components will have to be re-enrolled with quantum-resistant credentials (and only use post-quantum cryptographic algorithms). This is why the top level CAs should use post-quantum algorithms as specified by NIST.[16]

8.4. New ITSS

Current Intelligent Transportation Systems research primarily consider ground vehicles (heavy-duty, light). However, it is not

[16] The NIST PQC challenge is still open at the time of writing this paper.

far-fetched to envision broadening the scope of ITS to unmanned aerial vehicles [167,168], maritime [169], rail [170], and so on. Indeed, it would make sense to leverage the PKI deployed for ground vehicles in order to simplify key management. However, this would potentially stress further the PKI and challenges its scalability [164].

8.5. Blockchain-based management trust

The use of blockchain has been widely recommended to replace centralized trust management platforms, mainly because of their vulnerability of being a single point of failure [171]. The use of blockchain has also been identified more specifically as a potential security and trust management solution for C-ITS [172] [173].

Chulerttiyawong et al. use the consortium blockchain technology to ensure pseudonym certificates issuance in a multi-jurisdictional road network. In the approach proposed smart contracts are used to issue certificates to vehicles. Therefore the decentralized blockchain replaces the centralized PKI. The blockchain and its smart contracts are also involved in the pseudonym certificates revocation management. In [174] *Benarous et al.* propose a blockchain-based pseudonym management framework where pseudonym generation is performed purely by vehicles without interference by authorities. Mainly, two blockchains are used. The first is for the storage of the pseudonym certificates and for their state verification and the second is dedicated to revocation management. Similarly, *Hui et al.* [175] propose a fine-grained access control scheme for VANET data based on blockchain (FADB). The approach proposed combines the ciphertext-based attribute encryption (CP-ABE), Ethereum blockchain and the Inter Planetary File System (IPFS) [176] technologies to provide distributed storage and fine-grained access control. Indeed, the blockchain is used to replace the centralized PKI for user identity management as well as for data storage. Moreover, different ITS data access rights can be established according to user attribute. Besides, ITSS-V can outsource complex encryption and decryption operations to powerful ITSS-R and further improve the efficiency of data access. *Zhuo et al.* [177] propose a blockchain-based key management mechanism for C-ITS called DB-KMM (Decentralized Blockchain-based Key Management Mechanism) which automatically registers, updates and revokes stations public keys. The mechanism proposed relies on smart contracts and the blockchain to ensure the aforementioned tasks. Furthermore, they propose a novel mutual authentication and key agreement protocol. Finally, using smart contracts the proposed mechanism handles key update and revocation of the different users. *Yang et al.* [178] propose a decentralized blockchain-based trust management system for C-ITS environments. In the approach proposed, ITSS-Vs can validate the received messages from neighboring vehicles using Bayesian Inference Model. Based on the validation result, the ITSS-V generates a rating for each message source ITSS-V. With the ratings uploaded from ITSS-Vs, ITSS-Rs calculate the trust value offsets of involved vehicles and pack these data into a block. Then, each ITSS-R tries to add their blocks to the trust blockchain which is maintained by all the ITSS-Rs. In the same context, *Lei et al.* [179] used the blockchain to manage the key transfer between the security managers in the ITS communication systems.

There exist numerous other works from the academia that aim to use blockchains for a decentralized trust management in C-ITS environments [180] [181] [182] [183]. However, most of the existing works suffer from different shortcomings. Mainly, they do not consider all the ITS environment standards such as the types of messages (e.g., CAM, BSM), their format or the existing standardized network functions. Which make the proposed security approaches not compatible with the existing C-ITS environments. Moreover, the proposed approaches rely a lot on the blockchain and on data storage and browsing within the blockchain. However, such tasks are very costly in time and in computation resources and cannot be considered in real time and highly scalable environments such as C-ITS. Finally, at the time of writing this paper, no standard or consortium work considered the use of blockchain technology for trust management in C-ITS.

9. Conclusion

Public Key Infrastructures represent a major solution in ensuring communications' security. Because of their ability in meeting security requirements, PKIs are increasingly adopted in C-ITS environments and represent currently the first solution deployed.

Despite the huge number of works in C-ITS security area, there is no survey devoted exclusively to the topic of PKIs in C-ITS, their security functions, their architectures and how the different projects implemented them. Thus, in this work we provided an extensive survey that analyze each part and function of the set of the existing C-ITS PKIs and their related functions.

More precisely, in this survey, we studied step by step almost all PKI components and functions. We described the different certificates that exist in C-ITS environments, their standards and formats. Then, we introduced the existing C-ITS projects and standards that proposed and deployed PKI. We described the function of their authorities as well as their global architectures. Our work focuses also on the security lifecycle of the ITSS. Indeed, we surveyed the certificates' requests and responses as well as their security mechanisms. Afterwards, we discussed the different revocation and trust management standards and approaches that the different projects deployed.

Relying on all the studied aspects of PKIs, we proposed a generic model for a PKI architecture. Our model is proposed respecting a tradeoff between the number of authorities, modularity and infrastructure complexity. Finally, we highlighted the open research and operational challenges in the area of ITSS security that are related to PKIs.

Following our study and analysis, we conclude of the lack of standardization works related to numerous aspects and functions of the PKI (e.g., revocation, trust interoperability, certificates requests, and so on). We also conclude of the need of further work to overcome the different challenges (e.g., scalability, misbehavior detection, post-quantum cryptography) to ensure the functioning and service continuity of C-ITS.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

We thank the anonymous reviewers for their valuable comments which helped us improve the quality, content, and presentation of this paper.

References

[1] John A. Stankovic, Research challenges and solutions for IOT/CPS, Keynote speech of Prof. John A. Stankovic at the 26th International Conference on Computer Communications and Networks (ICCCN 2017), http://icccn.org/icccn17/wp-content/uploads/2017/08/ICCCN17-Jack-Stankovic-PPT-file.pdf.

[2] M. Shahid Anwer, Chris Guy, A survey of vanet technologies, J. Emerg. Trends Comput. Inf. Sci. 5 (9) (2014) 661–671.

[3] Valerian Mannoni, Vincent Berg, Stefania Sesia, Eric Perraud, A comparison of the V2X communication systems: ITS-G5 and C-V2X, in: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), IEEE, 2019, pp. 1–5.

[4] Khadige Abboud, Hassan Aboubakr Omar, Weihua Zhuang, Interworking of DSRC and cellular network technologies for V2X communications: a survey, IEEE Trans. Veh. Technol. 65 (12) (2016) 9457–9470.
[5] Ribal F. Atallah, Maurice J. Khabbaz, Chadi M. Assi, Vehicular networking: a survey on spectrum access technologies and persisting challenges, Veh. Commun. 2 (3) (2015) 125–149.
[6] Rafael Molina-Masegosa, Javier Gozalvez, Lte-v for sidelink 5g v2x vehicular communications: a new 5g technology for short-range vehicle-to-everything communications, IEEE Veh. Technol. Mag. 12 (4) (2017) 30–39.
[7] W. Whyte, A. Weimerskirch, V. Kumar, T. Hehn, A security credential management system for v2v communications, in: 2013 IEEE Vehicular Networking Conference, IEEE, 2013, pp. 1–8.
[8] U.S. Department of Transportation, Reseach and Innovative Technology Administration, Vehicle-to-Vehicle (V2V) communications for safety, https://www.its.dot.gov/research/v2v.htm.
[9] Richard Gilles Engoulou, Martine Bellaïche, Samuel Pierre, Alejandro Quintero, Vanet security surveys, Comput. Commun. 44 (2014) 1–13.
[10] J.P. Monteuuis, Badis Hammi, Eduardo Salles, Houda Labiod, Remi Blancher, Erwan Abalea, Brigitte Lonc, Securing PKI requests for C-ITS systems, in: 2017 26th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2017, pp. 1–8.
[11] Priyanka Patil, Nilesh Marathe, Vimla Jethani, Survey of privacy preservation in vanets, IRACST Int. J. Comput. Sci. Inf. Technol. Secur. 6 (1) (2016) 5.
[12] Saira Gillani, Farrukh Shahzad, Amir Qayyum, Rashid Mehmood, A survey on security in vehicular ad hoc networks, in: International Workshop on Communication Technologies for Vehicles, Springer, 2013, pp. 59–74.
[13] Fengzhong Qu, Zhihui Wu, Fei-Yue Wang, Woong Cho, A security and privacy review of vanets, IEEE Trans. Intell. Transp. Syst. 16 (6) (2015) 2985–2996.
[14] Lina Bariah, Dina Shehada, Ehab Salahat, Chan Yeob Yeun, Recent advances in vanet security: a survey, in: Vehicular Technology Conference (VTC Fall), 2015 IEEE 82nd, IEEE, 2015, pp. 1–7.
[15] M. Jeeva, A survey on secure transmission on vechicles and signal devices, Int. J. Comput. Sci. Eng. Technol. 5 (7) (2014).
[16] Shashi Kant Tiwari, Nemi Chandra Rathore, Survey on vanet privacy protocols, 2015.
[17] Bharati Mishra, Priyadarshini Nayak, Subhashree Behera, Jena Debasish, Security in vehicular adhoc networks: a survey, in: Proceedings of the 2011 International Conference on Communication, Computing & Security, ACM, 2011, pp. 590–595.
[18] Godavari H. Kudlikar, Uma Nagaraj, A survey on various security schemes in vehicular ad hoc network, Int. J. Innov. Res. Comput. Commun. Eng. 3 (11) (2015) 6.
[19] Rukaiya Y. Shaikh, Disha Deotale, Survey on vspn: vanet-based secure and privacy-preserving navigation, Int. J. Eng. Res. Appl. 1 (4) (2014) 1–5.
[20] Abid Khan Jadoon, Qaiser Khan, Asif Tehseen Ilahi, Waseem Iqbal, A survey on security challenges in vanet, Int. J. Comput. Sci. Inf. Secur. 14 (9) (2016) 217–219.
[21] Mohamed Nidhal Mejri, Jalel Ben-Othman, Mohamed Hamdi, Survey on vanet security challenges and possible cryptographic solutions, Veh. Commun. 1 (2) (2014) 53–66.
[22] G.M. Sumanth, C.P. Prabodh, A survey on security in vanets and applications, Int. Res. J. Eng. Technol. 3 (7) (2016) 6.
[23] Albert Wasef, Xuemin Shen, Emap: expedite message authentication protocol for vehicular ad hoc networks, IEEE Trans. Mob. Comput. 12 (1) (2013) 78–89.
[24] Neeraj Kumar, Rahat Iqbal, Sudip Misra, Joel J.P.C. Rodrigues, An intelligent approach for building a secure decentralized public key infrastructure in vanet, J. Comput. Syst. Sci. 81 (6) (2015) 1042–1058.
[25] Yi Qian, Kejie Lu, Nader Moayeri, A secure VANET MAC protocol for DSRC applications, in: Global Telecommunications Conference, 2008, IEEE GLOBECOM 2008, IEEE, IEEE, 2008, pp. 1–5.
[26] Haowen Tan, Ilyong Chung, Secure authentication and key management with blockchain in vanets, IEEE Access 8 (2019) 2482–2498.
[27] Hongyuan Cheng, Yining Liu, An improved RSU-based authentication scheme for VANET, J. Internet Technol. 21 (4) (2020) 1137–1150.
[28] Shibin Wang, Nianmin Yao, LIAP: a local identity-based anonymous message authentication protocol in VANETs, Comput. Commun. 112 (2017) 154–164.
[29] Xiaozhen Lu, Liang Xiao, Tangwei Xu, Yifeng Zhao, Yuliang Tang, Weihua Zhuang, Reinforcement learning based PHY authentication for VANETs, IEEE Trans. Veh. Technol. 69 (3) (2020) 3068–3079.
[30] Shibin Wang, Nianmin Yao, A RSU-aided distributed trust framework for pseudonym-enabled privacy preservation in VANETs, Wirel. Netw. 25 (3) (2019) 1099–1115.
[31] Ikram Ullah, Abdul Wahid, Munam Ali Shah, Abdul Waheed, VBPC: velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET, in: 2017 International Conference on Communication Technologies (ComTech), IEEE, 2017, pp. 132–137.
[32] Hui Li, Lishuang Pei, Dan Liao, Gang Sun, Du Xu, Blockchain meets VANET: an architecture for identity and location privacy protection in VANET, Peer Peer Netw. Appl. 12 (5) (2019) 1178–1193.
[33] Rakesh Shrestha, Rojeena Bajracharya, Anish P. Shrestha, Seung Yeob Nam, A new type of blockchain for secure message exchange in VANET, Digit. Commun. Netw. 6 (2) (2020) 177–186.
[34] Uzair Javaid, Muhammad Naveed Aman, Biplab Sikdar, DrivMan: driving trust management and data sharing in VANETS with blockchain and smart contracts, in: 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), IEEE, 2019, pp. 1–5.
[35] Sunilkumar S. Manvi, Shrikant Tangade, A survey on authentication schemes in vanets for secured communication, Veh. Commun. (2017).
[36] Marshall Riley, Kemal Akkaya, Kenny Fong, A survey of authentication schemes for vehicular ad hoc networks, Secur. Commun. Netw. 4 (10) (2011) 1137–1152.
[37] Yu Zhang, Xiangyu Bai, Comparative analysis of VANET authentication architecture and scheme, in: 2019 12th International Symposium on Computational Intelligence and Design (ISCID), vol. 2, 2019, pp. 89–93.
[38] S. Raghupathi, N. Jaisankar, E. Anupriya, A recent survey on authentication schemes with privacy preservation in VANETs, Indian J. Comput. Sci. Eng. 10 (5) (2019) 7.
[39] Shaik Mullapathi Farooq, S.M. Suhail Hussain, Taha Selim Ustun, A survey of authentication techniques in vehicular ad-hoc networks, IEEE Intell. Transp. Syst. Mag. 13 (2) (2020) 39–52.
[40] Dakshnamoorthy Manivannan, Shafika Showkat Moni, Sherali Zeadally, Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs), Veh. Commun. 25 (2020) 100247.
[41] Zehra Afzal, Manoj Kumar, Security of vehicular ad-hoc networks (VANET): a survey, J. Phys. Conf. Ser. 1427 (2020) 012015.
[42] Arzoo Dahiya, Vaibhav Sharma, A survey on securing user authentication in vehicular ad hoc networks, Int. J. Inf. Secur. 1 (2001) 164–171.
[43] R. Christilda Jerlin, J. Jebila, Reconstruction of a secure authentication scheme for vehicular ad hoc networks, Int. J. Syst. Des. Comput. 4 (5) (2017) 6.
[44] C. Tripti, P. Remyakrishnan, Authentication techniques in vanets-a survey, Int. J. Adv. Res. Comput. Sci. 5 (4) (2014).
[45] Punam R. Sathe, Ganesh N. Dhanokar, A survey on effective way of message authentication using proxy vehicle in vehicular ad-hoc network, Int. J. Sci. Res. 6 (1) (2017) 3.
[46] Ahren Studer, Elaine Shi, Fan Bai, Adrian Perrig, TACKing together efficient authentication, revocation, and privacy in vanets, in: 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2009, SECON'09, IEEE, 2009, pp. 1–9.
[47] Jie Zhang, A survey on trust management for vanets, in: 2011 IEEE International Conference on Advanced Information Networking and Applications (AINA), IEEE, 2011, pp. 105–112.
[48] Akash Vaibhav, Dilendra Shukla, Sanjoy Das, Subrata Sahana, Prashant Johri, Security challenges, authentication, application and trust models for vehicular ad hoc network-a survey, Int. J. Wirel. Microw. Technol. 3 (2017) 36–48.
[49] Ikram Ali, Alzubair Hassan, Fagen Li, Authentication and privacy schemes for vehicular ad hoc networks (VANETs): a survey, Veh. Commun. 16 (2019) 45–61.
[50] Ruqayah Al-ani, Bo Zhou, Qi Shi, Ali Sagheer, A survey on secure safety applications in vanet, in: 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), IEEE, 2018, pp. 1485–1490.
[51] Amit Kumar Goyal, Gaurav Agarwal, Arun Kumar Tripathi, Network architectures, challenges, security attacks, research domains and research methodologies in VANET: a survey, Int. J. Comput. Netw. Inf. Secur. 11 (10) (2019).
[52] Avleen Kaur Malhi, Shalini Batra, Husanbir Singh Pannu, Security of vehicular ad-hoc networks: a comprehensive survey, Comput. Secur. 89 (2020) 101664.
[53] Sparsh Sharma, Ajay Kaul, Suhaib Ahmed, Surbhi Sharma, A detailed tutorial survey on VANETs: emerging architectures, applications, security issues, and solutions, Int. J. Commun. Syst. 34 (14) (2021) e4905.
[54] Albert Wasef, Rongxing Lu, Xiaodong Lin, Xuemin Shen, Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks], IEEE Wirel. Commun. 17 (5) (2010).
[55] S. Khandelwal, P. Jawandhiya, Safe geo graphic location privacy scheme in the vanets-survey methods and its limitation, Int. J. Sci. Eng. Res. (2013) 1507–1511.
[56] Rajni Singla, Namisha Sharma, A survey on data routing and security aspects in vanets 3 (5) (2014).
[57] Nirav J. Patel, Rutvij H. Jhaveri, Trust based approaches for secure routing in vanet: a survey, Proc. Comput. Sci. 45 (2015) 592–601.
[58] Cong Liao, Jian Chang, Insup Lee, Krishna K. Venkatasubramanian, A trust model for vehicular network-based incident reports, in: 2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC), IEEE, 2013, pp. 1–5.
[59] Zhou Wang, Chunxiao Chigan, Countermeasure uncooperative behaviors with dynamic trust-token in vanets, in: 2007 IEEE International Conference on Communications, IEEE, 2007, pp. 3959–3964.
[60] Subir Biswas, Jelena Misic, Vojislav Misic, Id-based safety message authentication for security and trust in vehicular networks, in: 2011 31st Interna-

tional Conference on Distributed Computing Systems Workshops, IEEE, 2011, pp. 323–331.
[61] Xiaoqing Li, Hui Li, A survey on data dissemination in vanets, Chin. Sci. Bull. 59 (32) (2014) 4190–4200.
[62] C. Kiruthika, Ms.N. Gugha Priya, A survey on security based data dissemination for VANETs, Int. J. Adv. Res. Comput. Commun. Eng. 4 (11) (2015) 4.
[63] Wedad Ahmed, Mourad Elhadef, Securing intelligent vehicular ad hoc networks: a survey, in: Advances in Computer Science and Ubiquitous Computing, Springer, 2017, pp. 6–14.
[64] Mujahid Muhammad, Ghazanfar Ali Safdar, Survey on existing authentication issues for cellular-assisted V2X communication, Veh. Commun. 12 (2018) 50–65.
[65] B. Tarakeswara Rao, R.S.M. Lakshmi Patibandla, V. Lakshman Narayana, Comparative Study on Security and Privacy Issues in VANETs, John Wiley & Sons, Ltd, 2021, pp. 145–162 (chapter 8).
[66] Muhammad Sameer Sheikh, Jun Liang, A comprehensive survey on VANET security services in traffic management system, Wirel. Commun. Mob. Comput. 2019 (2019).
[67] Muhammad Sameer Sheikh, Jun Liang, Wensong Wang, A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets), Sensors 19 (16) (2019) 3589.
[68] Ahmed Shamil Mustafa, Mustafa Maad Hamdi, Hussain Falih Mahdi, Mohammed Salah Abood, VANET: towards security issues review, in: 2020 IEEE 5th International Symposium on Telecommunication Technologies (ISTT), IEEE, 2020, pp. 151–156.
[69] Mahmood A. Al-Shareeda, Mohammed Anbar, Iznan Husainy Hasbullah, Selvakumar Manickam, Survey of authentication and privacy schemes in vehicular ad hoc networks, IEEE Sens. J. 21 (2) (2021) 2422–2433.
[70] Priya Kohli, Sakshi Painuly, Priya Matta, Sachin Sharma, Future trends of security and privacy in next generation VANET, in: 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), IEEE, 2020, pp. 1372–1375.
[71] Aminul Islam, Sudhanshu Ranjan, Arun Pratap Rawat, Soumayadev Maity, A comprehensive survey on attacks and security protocols for VANETs, in: Innovations in Computer Science and Engineering, 2021, pp. 583–595.
[72] Sagarika Mohanty, Debasish Jena, Secure data aggregation in vehicular-adhoc networks: a survey, Proc. Technol. 6 (2012) 922–929.
[73] David Antolino Rivas, José M. Barceló-Ordinas, Manel Guerrero Zapata, Julián D. Morillo-Pozo, Security on vanets: privacy, misbehaving nodes, false information and secure data aggregation, J. Netw. Comput. Appl. 34 (6) (2011) 1942–1955.
[74] Arpit Gupta, Gaurav Shrivastava, Apda with data collective: a survey to prevent attacks in vanet, Edition on Wired and Wireless Networks: Advances and Applications, 3, 2013.
[75] R. Saranya, C. Yalini, A survey on secure intelligent transportation system protocol for vanet using smap, Int. J. Emerg. Technol. Adv. Eng. 3 (10) (2013) 5.
[76] Safi Ibrahim, Mohamed Hamdy, A comparison on vanet authentication schemes: public key vs. symmetric key, in: 2015 Tenth International Conference on Computer Engineering & Systems (ICCES), IEEE, 2015, pp. 341–345.
[77] Md Whaiduzzaman, Mehdi Sookhak, Abdullah Gani, Rajkumar Buyya, A survey on vehicular cloud computing, J. Netw. Comput. Appl. 40 (2014) 325–344.
[78] Emanuel Fonseca, Andreas Festag, A survey of existing approaches for secure AD HOC routing and their applicability to VANETs, NEC Netw. Lab. 28 (2006) 1–28.
[79] Abhijit Das, Dipanwita Roychoudhury, Debojyoti Bhattacharya, Rajavelu Srinivasan, Rajeev Shorey, Tony Thomas, Authentication schemes for VANETs: a survey, Int. J. Veh. Inf. Commun. Syst. 3 (1) (2013) 1–27.
[80] J. Petit, F. Schaub, M. Feiri, F. Kargl, Pseudonym schemes in vehicular networks: a survey, IEEE Commun. Surv. Tutor. 17 (1) (2015) 228–255.
[81] Christoph Ponikwar, Hans-Joachim Hof, Overview on security approaches in intelligent transportation systems, arXiv preprint, arXiv:1509.01552, 2015, p. 6.
[82] Taimur Khan, Naveed Ahmad, Yue Cao, Syed Asim Jalal, Muhammad Asif, Sana ul Haq, Haitham Cruichshank, Certificate revocation in vehicular ad hoc networks techniques and protocols: a survey, Sci. China Inf. Sci. 60 (10) (2017) 1–18.
[83] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, Anis Laouiti, Vanet security challenges and solutions: a survey, Veh. Commun. (2017).
[84] Zhaojun Lu, Gang Qu, Zhenglin Liu, A survey on recent advances in vehicular network security, trust, and privacy, IEEE Trans. Intell. Transp. Syst. 20 (2) (2018) 760–776.
[85] Van Huynh Le, Jerry den Hartog, Nicola Zannone, Security and privacy for innovative automotive applications: a survey, Comput. Commun. 132 (2018) 17–41.
[86] Rasheed Hussain, Fatima Hussain, Sherali Zeadally, Integration of VANET and 5G Security: a review of design and implementation issues, Future Gener. Comput. Syst. 101 (2019) 843–864.
[87] Muath Obaidat, Matluba Khodjaeva, Jennifer Holst, Mohamed Ben Zid, Security and Privacy Challenges in Vehicular Ad Hoc Networks, Springer International Publishing, 2020, pp. 223–251.
[88] Rasheed Hussain, Jooyoung Lee, Sherali Zeadally, Trust in vanet: a survey of current solutions and future research opportunities, IEEE Trans. Intell. Transp. Syst. 22 (5) (2020) 2553–2571.
[89] ETSI TS 103 097 V1.3.1: Intelligent Transport Systems (ITS), Security header and certificate formats, 2017, p. 23.
[90] ETSI TS 102 941 V1.3.1: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management, Technical specification, European Telecommunications Standards Institute, 2019, p. 73.
[91] Security Credential Management System Proof-of-Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.1, Technical report, Vehicle Safety Communications 5 Consortium, May 2016.
[92] The C-Roads Platform, An overview of harmonised C-ITS deployment in Europe, Technical report, European Commissioner for Transport, June 2021.
[93] A. Jancic, Matthew J. Warren, Pki-advantages and obstacles, in: AISM, Citeseer, 2004, pp. 104–114.
[94] Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
[95] Intelligent Transportation Systems Committee, et al., IEEE standard for wireless access in vehicular environments-security services for applications and management messages, IEEE Veh. Technol. Soc. Stand. 1609 (2) (January 2016) 1–884.
[96] Joan Daemen, Vincent Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Springer Science & Business Media, 2013.
[97] Joan Daemen, Vincent Rijmen, AES proposal: Rijndael, 1999.
[98] Joan Daemen, Vincent Rijmen, The block cipher rijndael, in: International Conference on Smart Card Research and Advanced Applications, Springer, 1998, pp. 277–284.
[99] A. Slagell, R. Bonilla, W. Yurcik, A survey of PKI components and scalability issues, in: 2006 IEEE International Performance Computing and Communications Conference, IEEE, April 2006, 10pp.
[100] Ronald L. Rivest, Adi Shamir, Leonard Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[101] R.L. Rivest, A. Shamir, L.M. Adleman, Cryptographic communications system and method, US Patent 4,405,829, 1983.
[102] PKCS #1 v2.2: RSA CRYPTOGRAPHY STANDARD, 2012, p. 34.
[103] Dan Boneh, Hovav Shacham, Fast variants of RSA, CryptoBytes 5 (1) (2002) 1–9.
[104] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inf. Theory 31 (4) (Jul 1985) 469–472.
[105] Julio Lopez, Ricardo Dahab, An overview of elliptic curve cryptography, 2000.
[106] SEC 1: Elliptic Curve Cryptography, Version 2.0, Standards for Efficient Cryptography, 2009, p. 144.
[107] Víctor Gayoso Martínez, Luis Hernández Encinas, Carmen Sánchez Ávila, A survey of the elliptic curve integrated encryption scheme, J. Comput. Sci. Eng. 2 (2) (2010) 7–13.
[108] Víctor Gayoso Martínez, Fernando Hernández Álvarez, Luis Hernández Encinas, Carmen Sánchez Ávila, Analysis of ECIES and other cryptosystems based on elliptic curves, 2011.
[109] Don Johnson, Alfred Menezes, Scott Vanstone, The elliptic curve digital signature algorithm (ECDSA), Int. J. Inf. Secur. 1 (1) (2001) 36–63.
[110] Neal Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (177) (1987) 203–209.
[111] Victor S. Miller, Use of elliptic curves in cryptography, in: Conference on the Theory and Application of Cryptographic Techniques, Springer, 1985, pp. 417–426.
[112] Kristin Lauter, The advantages of elliptic curve cryptography for wireless security, IEEE Wirel. Commun. 11 (1) (2004) 62–67.
[113] Darrel Hankerson, Alfred J. Menezes, Scott Vanstone, Guide to Elliptic Curve Cryptography, Springer Science & Business Media, 2006.
[114] Ronald L. Rivest, Martin E. Hellman, John C. Anderson, John W. Lyons, Responses to NIST's proposal, Commun. ACM 35 (7) (1992) 41–54.
[115] Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, ISO/IEC 14888-3:2016, 2016, p. 130.
[116] ANSI, X9.62:2005, Public key cryptography for the financial services industry: Elliptic Curve Digital Signature Algorithm (ECDSA), 2005, p. 128.
[117] Ieee standard specifications for public-key cryptography, IEEE Std 1363-2000, 2000, pp. 1–228.
[118] Ieee standard specifications for public-key cryptography - amendment 1: Additional techniques, IEEE Std 1363a-2004 (Amendment to IEEE Std 1363-2000), 2004, pp. 1–167.
[119] FIPS PUB 186-2: Digital signature standard (DSS), National Institute of Standards and Technology, 2000, p. 73.
[120] FIPS PUB 186-4: Digital signature standard (DSS), National Institute of Standards and Technology, 2013, p. 130.
[121] Erik De Win, Serge Mister, Bart Preneel, Michael Wiener, On the performance of signature schemes based on elliptic curves, in: International Algorithmic Number Theory Symposium, Springer, 1998, pp. 252–266.

[122] Wen bi Rao, Quan Gan, The performance analysis of two digital signature schemes based on secure charging protocol, in: Proceedings, 2005 International Conference on Wireless Communications, Networking and Mobile Computing, vol. 2, IEEE, 2005, pp. 1180–1182.
[123] ETSI TS 102 867 V1.1.1: Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2, 2012, p. 26.
[124] V2X Communications Message Set Dictionary J2735, March 2016, pp. 1–267.
[125] Virendra Kumar, Special cryptographic primitives in SCMS. SCP1: butterfly keys, https://wiki.camplic.org/display/SCP, March 2017.
[126] Security system: Integration guide v4, SCOOP@F Delivrable 2.4.4.8, Technical report, December 2016.
[127] Intelligent Transportation Systems Committee, et al., IEEE standard for wireless access in vehicular environments — security services for applications and management messages, amendment 1, IEEE Veh. Technol. Soc. Stand. 1609 (2a) (2017) 1–123.
[128] Intelligent Transportation Systems Committee, et al., IEEE 1609.2b-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, IEEE Veh. Technol. Soc. Stand. 1609 (2b) (Juin 2019) 1–30.
[129] Service Specific Permissions and Security Guidelines for Connected Vehicle Applications, February 2020, pp. 1–44.
[130] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, RFC 5280: Internet X. 509 Public Key Infrastructure Certificate and CRL Profile, Internet Engineering Task Force (IETF), May 2008.
[131] Daniel R.L. Brown, Robert P. Gallant, Scott A. Vanstone, Provably secure implicit certificate schemes, 2002, pp. 156–165.
[132] Leon A. Pintsov, Scott A. Vanstone, Postal revenue collection in the digital age, 2000, pp. 105–120.
[133] Daniel R.L. Brown, Matthew J. Campagna, Scott A. Vanstone, Security of ecqv-certified ecdsa against passive adversaries, IACR Cryptol. ePrint Arch. 2009 (2009) 620.
[134] SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), Standards for Efficient Cryptography, 2013, p. 32.
[135] B. Vaidya, D. Makrakis, H.T. Mouftah, Security mechanism for multi-domain vehicle-to-grid infrastructure, in: 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, IEEE, 2011, pp. 1–5.
[136] ETSI TS 103 097 V1.2.1: Intelligent Transport Systems (ITS), Security header and certificate formats, June 2015, p. 35.
[137] ETSI TS 103 097 V2.1.1: Intelligent Transport Systems (ITS), Security header and certificate formats; Release 2, October 2021, p. 22.
[138] Codes for the representation of names of countries and their subdivisions – Part 1: Country codes, ISO 3166-1:2013, 2013, p. 72.
[139] Norbert Bißmeyer, Hagen Stübing, Elmar Schoch, Stefan Götz, Jan Peter Stotz, Brigitte Lonc, A generic public key infrastructure for securing car-to-x communication, in: 18th ITS World Congress, Orlando, USA, vol. 14, 2011.
[140] 102 940: Intelligent transport systems (its); security; its communications security architecture and security management, Technical specification, European Telecommunications Standards Institute, 2012.
[141] ETSI TS 102 941 V2.1.1: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2, Technical specification, European Telecommunications Standards Institute, 2021, p. 83.
[142] Etsi ts 102 731 v1. 1.1-intelligent transport systems (its); security; security services and architecture, Technical specification, European Telecommunications Standards Institute, 2010.
[143] Car-2-car, The mission and objectives of the car 2 car communication consortium.
[144] C2C-CC, C2C-CC public key infrastructure memo (v1.20), January 2011.
[145] Vehicle-to-Vehicle Security Credential Management System; Request for Information, Technical report, National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT), October 2014.
[146] Badis Hammi, J.P. Monteuuis, Houda Labiod, Rida Khatoun, Ahmed Serhrouchni, Using butterfly keys: a performance study of pseudonym certificates requests in C-ITS, in: 1st Cyber Security in Networking Conference on, IEEE, 2017, p. 6.
[147] Working Group 2 Task Force, Draft - Technical Requirement of Security Certificate Management System for LTE-based Vehicular Communication, Technical report, 2020.
[148] Ran Tao, Lars Wolleschensky, André Weimerskirch, Security certificate management system for V2V communication in China, SAE Int. J. Transp. Cybersecur. Priv. 2 (2) (2019) 169–183.
[149] CCSA TC10 WG1 & IMT-2020 (5G) PG C-V2X WG, Standardization of CCSA, Technical report, March 2021.
[150] Benedikt Brecht, Therriault Dean, Weimerskirch André, Whyte William, Kumar Virendra, Hehn Thorsten, Roy Goudy, A security credential management system for V2X communications, IEEE Trans. Intell. Transp. Syst. 19 (12) (2018) 83–115.
[151] Hasnaâ Aniss, Overview of an ITS Project: SCOOP@F, Springer International Publishing, 2016, pp. 131–135.
[152] Hafeda Bakhti, Erwann Abalea, Remi Blancher, Brigitte Lonc, Houda Labiod, PKI system requirements specifications (v1.1), Technical report, IRT System X, March 2015.
[153] P. Cincilla, A. Kaiser, B. Lonc, H. Labiod, R. Blancher, C. Jouvray, R. Denis, A. Boulanger, Security of C-ITS messages: a practical solution the ise project demonstrator, in: 2015 7th International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2015, pp. 1–2.
[154] Eric R. Verheul, Issue first activate later certificates for V2X, combining ITS efficiency with privacy, IACR Cryptol. ePrint Arch. 2016 (2016) 1158.
[155] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) DRAFT v1.0.14, April 2017, p. 82.
[156] Working Group 2 Task Force, Draft Report on European Security Mechanism, Version 1.4, Technical report, January 2019.
[157] Marko Wolf, Timo Gendrullis, Design, implementation, and evaluation of a vehicular hardware security module, in: ICISC, Springer, 2011, pp. 302–318.
[158] Lily Chen, Recommendation for Key Derivation Using Pseudorandom Functions, NIST Special Publication 800-108, 2009, p. 21.
[159] Farah Haidar, Arnaud Kaiser, Brigitte Lonc, Pascal Urien, C-ITS PKI protocol: performance evaluation in a real environment, in: 2019 15th Annual Conference on Wireless On-demand Network Systems and Services (WONS), IEEE, 2019, pp. 52–55.
[160] Yves Christian Elloh Adja, Badis Hammi, Ahmed Serhrouchni, Sherali Zeadally, A blockchain-based certificate revocation management and status verification system, Comput. Secur. 104 (2021) 102209.
[161] Yabing Liu, Will Tome, Liang Zhang, David Choffnes, Dave Levin, Bruce Maggs, Alan Mislove, Aaron Schulman, Christo Wilson, An end-to-end measurement of certificate revocation in the web's PKI, in: Proceedings of the 2015 Internet Measurement Conference, 2015, pp. 183–196.
[162] PKI architecture and technical specifications (v1.1), SCOOP@F Delivrable 2.4.4.6, Technical report, November 2015.
[163] Badis Hammi, Yacine Mohamed Idir, Sherali Zeadally, Rida Khatoun, Jamel Nebhen, Is it really easy to detect Sybil attacks in c-its environments: a position paper, IEEE Trans. Intell. Transp. Syst. (2022).
[164] Pierpaolo Cincilla, Omar Hicham, Benoit Charles, Vehicular PKI scalability-consistency trade-offs in large scale distributed scenarios, in: 2016 IEEE Vehicular Networking Conference (VNC), IEEE, 2016, pp. 1–8.
[165] Joseph Kamel, Farah Haidar, Ines Ben Jemaa, Arnaud Kaiser, Brigitte Lonc, Pascal Urien, A misbehavior authority system for Sybil attack detection in c-its, in: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019, pp. 1117–1123.
[166] Salabat Khan, Fei Luo, Zijain Zhang, Mussadiq Abdul Rahim, Mubashir Ahmad, Kaishun Wu, Survey on issues and recent advances in Vehicular Public-key Infrastructure (VPKI), IEEE Commun. Surv. Tutor. (2022).
[167] Omar Sami Oubbati, Noureddine Chaib, Abderrahmane Lakas, Pascal Lorenz, Abderrezak Rachedi, UAV-assisted supporting services connectivity in urban VANETs, IEEE Trans. Veh. Technol. 68 (4) (2019) 3944–3951.
[168] Xiong Wang, Luoyi Fu, Yang Zhang, Xiaoying Gan, Xinbing Wang, VDNet: an infrastructure-less UAV-assisted sparse VANET system with vehicle location prediction, Wirel. Commun. Mob. Comput. 16 (17) (2016) 2991–3003.
[169] Kok-Lim Alvin Yau, Aqeel Raza Syed, Wahidah Hashim, Junaid Qadir, Celimuge Wu, Najmul Hassan, Maritime networking: bringing internet to the sea, IEEE Access 7 (2019) 48236–48255.
[170] Li Zhu, Fei Richard Yu, Yige Wang, Bin Ning, Tao Tang, Big data analytics in intelligent transportation systems: a survey, IEEE Trans. Intell. Transp. Syst. 20 (1) (2018) 383–398.
[171] Donpiti Chulerttiyawong, Abbas Jamalipour, A blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement, IEEE Access 9 (2021) 127305–127319.
[172] Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira, Koustabh Dolui, Fabio Antonelli, Mubashir Husain Rehmani, Applications of blockchains in the internet of things: a comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1676–1717.
[173] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, Cybersecurity challenges in vehicular communications, Veh. Commun. 23 (2020) 100214.
[174] Leila Benarous, Benamar Kadri, Ahmed Bouridane, Blockchain-based privacy-aware pseudonym management framework for vehicular networks, Arab. J. Sci. Eng. 45 (8) (2020) 6033–6049.
[175] Hui Li, Lishuang Pei, Dan Liao, Song Chen, Ming Zhang, Du Xu, Fadb: a fine-grained access control scheme for vanet data based on blockchain, IEEE Access 8 (2020) 85190–85203.
[176] Juan Benet, Ipfs-content addressed, versioned, p2p file system, arXiv preprint, arXiv:1407.3561, 2014.
[177] Zhuo Ma, Junwei Zhang, Yongzhen Guo, Yang Liu, Ximeng Liu, Wei He, An efficient decentralized key management mechanism for vanet with blockchain, IEEE Trans. Veh. Technol. 69 (6) (2020) 5836–5849.
[178] Zhe Yang, Kan Yang, Lei Lei, Kan Zheng, Victor C.M. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Int. Things J. 6 (2) (2018) 1495–1505.

[179] Ao Lei, Haitham Cruickshank, Yue Cao, Philip Asuquo, Chibueze P. Anyigor Ogah, Zhili Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Int. Things J. 4 (6) (2017) 1832–1843.
[180] Chao Lin, Debiao He, Xinyi Huang, Neeraj Kumar, Kim-Kwang Raymond Choo, Bcppa: a blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks, IEEE Trans. Intell. Transp. Syst. 22 (12) (2020) 7408–7420.
[181] Zhaojun Lu, Qian Wang, Gang Qu, Zhenglin Liu, Bars: a blockchain-based anonymous reputation system for trust management in vanets, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 98–103.
[182] Sonia Alice George, Arunita Jaekel, Ikjot Saini, Secure identity management framework for vehicular ad-hoc network using blockchain, in: 2020 IEEE Symposium on Computers and Communications (ISCC), IEEE, 2020, pp. 1–6.
[183] Ei Mon Cho, Maharage Nisansala Sevwandi Perera, Efficient certificate management in blockchain based internet of vehicles, in: 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), IEEE, 2020, pp. 794–797.