Smart Card-Based Identity Management Protocols for V2V and V2I Communications in CCAM: a Systematic Literature Review

Stefano Berlato, Marco Centenaro, *Member, IEEE*, and Silvio Ranise

***Abstract*—Besides developing new Cooperative, Connected and Automated Mobility (CCAM) services for the improvement of road safety and travel experience, researchers are considering protection mechanisms to ensure the security of these services and the safety of involved users (drivers but also, e.g., cyclists and pedestrians). In particular, several Identity Management (IDM) protocols have been designed as the first line of defence against external attackers. Among these protocols, a promising trend in research consists in the use of a Smart Card (SC) as a technical enabler for strong authentication. Indeed, many SC-based IDM protocols for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications in real-time CCAM services have been proposed in the literature which present interesting features and promising usability experimental results. However, this research line is far from being exhausted, especially considering the recent spread of SC technologies and use cases. For this reason, in this paper we propose a systematic literature review on SC-based IDM protocols for real-time CCAM services. In particular, we identify characterising assumptions of CCAM scenarios and extrapolate a unified high-level view of the steps composing a SC-based IDM protocol. Then, we present a detailed survey of several SC-based IDM protocols. Finally, we identify trends in research and formulate guidelines and useful recommendations to provide a solid base which researchers can use as a starting point for the design of new and improved SC-based IDM protocols for CCAM scenarios.**

***Index Terms*—Cooperative Connected and Automated Mobility, Identity Management, Smart Card, Authentication, Systematic Literature Review.**

I. Introduction

In recent years, Intelligent Transportation Systems (ITS) have emerged as a prominent paradigm for the development of Cooperative, Connected and Automated Mobility (CCAM) services. In this vision, vehicles exchange information among themselves (Vehicle-to-Vehicle (V2V) communication) by creating a so-called Vehicular Ad-hoc NETwork (VANET). In conjunction with the support of road infrastructure nodes (yielding Vehicle-to-Infrastructure (V2I) information exchanges), these communications are the ground to provision real-time CCAM services that assist drivers (or autonomous vehicles) in performing complex manoeuvres securely and extend their situation awareness to increase road safety. Regarding the specific radio technologies for implementing vehicular communications, recently we have been witnessing the dualism between sheer Peer-to-Peer (P2P), i.e., leveraging short-range wireless link following the 802.11p standard by the Institute of Electrical and Electronics Engineers (IEEE), and Vehicle-to-Network (V2N), i.e., leveraging long-range mobile network technologies by the Third Generation Partnership Project (3GPP). In the rest of the paper, we remain agnostic with respect to this dualism.

While coming with great benefits, CCAM opens new challenges and security, trust, and privacy aspects must be thoroughly addressed. Security aspects are particularly relevant as even the smallest attempt to disrupt CCAM services can seriously affect the safety of involved users. Therefore, these services should be coupled with proper protection mechanisms. In particular, the first line of defence against external attackers is the authentication of involved users and vehicles. A proper authentication mechanism prevents attacks like data injection and spoofing and guarantees accountability and non-repudiation. As a matter of fact, the need for strong (i.e., cryptography-based) authentication in CCAM has already been highlighted in the context of the most recent testing activities held in the European project 5G-CARMEN.[1]

The steps of generation, distribution, use and revocation of authentication credentials are usually considered together and referred to as Identity Management (IDM). In CCAM, many IDM protocols have been proposed, each embodying particular features and employing different cryptographic primitives, e.g., Public Key Infrastructure (PKI) and Identity-Based Encryption (IBE). In this context, a promising research line consists of those IDM protocols that employ Smart Cards (SCs) to provide strong authentication. Essentially, a SC is a tamper-proof hardware element equipped with limited computational resources that contains secret cryptographic material (e.g., private keys) usually protected by a PIN. Given this definition, it is clear that SCs can be used as a key enabler for strong authentication in CCAM. Indeed, the necessity to ensure users' safety demands for high-level security which can hardly be provided by traditional (e.g., password-based) techniques. Moreover, SCs naturally enable Multi-Factor Authentication (MFA) which further increases the security level of IDM

Manuscript received Month XY, 2020; revised Month XY, 2020; accepted Month XY, 2020.

S. Berlato and S. Ranise are with the Center for Information and Communication Technology, Fondazione Bruno Kessler, 38123 Trento, Italy. E-mail: {sberlato, ranise}@fbk.eu.

S. Berlato is with the Department of Informatics, Bioengineering, Robotics and Systems Engineering, University of Genoa, 16145, Genoa, Italy, E-mail: 4770592@studenti.unige.it.

M. Centenaro is with Athonet, 36050, Bolzano Vicentino, Italy, E-mail: marco.centenaro.it@ieee.org.

S. Ranise is with the Department of Mathematics, University of Trento, 38123, Trento, Italy, E-mail: silvio.ranise@unitn.it.

[1] https://5gcarmen.eu

solutions. Finally, SCs are now largely adopted and widely available, e.g., Universal Subscriber Identity Modules (USIMs) cards embedded in smartphones are, in fact, SCs. Furthermore, the eIDAS project[2] in the European Union (EU) is fostering the adoption of electronic IDentity (eID) cards, which contain secret cryptographic material and can thus be used as SCs.

A. Applications of Smart Cards in CCAM

The capability to associate users and vehicles to digital identities with tamper-proof hardware and a high level of assurance made SCs a flexible tool for IDM in a wide variety of CCAM scenarios, especially when different roles are involved. For instance, the regulated application of the Digital Tachograph in the European Union[3] employs SCs to record professional drivers' activities (e.g., rest and driving hours), increase road safety and ensure minimum working conditions standards. This scenario uses SCs to enforce privilege separation among several roles; through different SCs, drivers can record their activities, road operators (e.g., highway managers) can perform mandatory back-ups and authorities (e.g., the police) can check the compliance of drivers' activities with the law. Other prominent CCAM scenarios were proposed, e.g., in the framework of the 5G-CARMEN project. For instance, the Back-Situation Awareness scenario allows emergency vehicles to use the ITS infrastructure to warn other drivers of their presence and ask to clear the lane in advance. In this scenario, we can identify three different roles, i.e., normal drivers, emergency vehicles drivers and city traffic administrators with the capability to control the flow of vehicles. In [9], the authors proposed a practical strong authentication method for this scenario leveraging SCs as a second factor for authentication. The final goal is to correctly enforce access control policies to prevent unauthorized (i.e., normal) drivers from misusing the ITS infrastructure. Another CCAM scenario envisioned in the 5G-CARMEN project is the Cooperative Lane Merging scenario, in which drivers (or autonomous vehicles) optimize their trajectories by exchanging relevant data (e.g., speed and intents). Clearly, the protection against injection of false data by external attackers is of paramount importance to avoid incidents and car crashes. As such, this scenario expects SCs to be the basic building block to manage digital identities by providing strong authentication of drivers and vehicles. Finally, according to the vision promoted in a proposal to establish a European Partnership for CCAM,[4] the administration of (fleet of) shared vehicles will be a prominent CCAM scenario in future years. Intuitively, one critical aspect of this scenario is accountability, i.e., the ability to link drivers to shared vehicles in case of disputes or incidents. In this regard, we observe that the only way to guarantee accountability of digital identities with a high level of assurance is through SCs.

Summarising, there exist numerous CCAM scenarios, each involving several roles using SCs in a different way to achieve specific purposes. However, we note that all these CCAM scenarios share at their foundation the same technical core, i.e., the use of SCs for IDM. Indeed, the secure and proper management of digital identities is required to then guarantee further properties such as privilege separation, accountability, strong authentication and access control. Therefore, in the rest of the paper we focus on the foundational security service supporting CCAM scenarios (i.e., SC-based IDM) rather than on the scenarios themselves.

B. Motivations and Contributions

CCAM poses strict security and functional requirements on V2V and V2I communications, especially when considering safety-critical scenarios. As presented in Section I-A, one of the main building blocks for enabling real-time CCAM services is SC-supported IDM. In this context, we note that the life-cycle of digital identities is composed of several steps, which may be subject to different requirements. For instance, the enrollment of users can support computational demanding tasks but must achieve high levels of assurance,[5] while the authentication of moving vehicles needs to respect stringent latency constraints. A fine-grained characterization of IDM protocols allows to determine which steps can sustain more secure (and computationally expensive) security mechanisms and which steps instead has to rely on previous computation (e.g., derive credentials from previously shared secrets). The first IDM protocol for CCAM relying on SCs was proposed by Paruchuri and Durresi in 2010 [36]. Since then, several researchers sharing this vision proposed SC-based IDM protocols enriched with new features (e.g., conditional privacy, use of biometrics) and implementing new functionalities (e.g., batch verification). However, we remark that it may be complex to propose new SC-based IDM protocols having such a rich State-of-the-Art (SotA), the main problem being the difficulty in reviewing the ever-growing literature. Therefore, in this paper we present a self-contained systematic literature review of SC-based IDM protocols for V2I and V2V communications in CCAM intending to "distil" the available literature and propose guidelines and useful considerations for the design of new SC-based IDM protocols. While IDM covers also privacy-related aspects, in this survey we focus on security only. In particular, our contributions are as follows:

- we extensively describe characterising assumptions and requirements of CCAM which need to be carefully addressed during the design of SC-based IDM protocols;
- we extrapolate a unified high-level view of the *8 steps* composing a SC-based IDM protocol (e.g., system setup, user registration, user login);
- we thoroughly review 12 SC-based IDM protocols and highlight similarities and differences, main focus and other noticeable aspects. Moreover, we study these protocols and map them to the high-level unified view previously presented;
- we analyse trends and shortcomings in research and formulate *9 concrete guidelines* grouped in 3 topics for the design of new SC-based IDM protocols for CCAM.

[2]https://ec.europa.eu/digital-single-market/en/discover-eidas

[3]https://dtc.jrc.ec.europa.eu/

[4]https://ec.europa.eu/info/sites/default/files/research_and_innovation/funding/documents/ec_rtd_he-partnerships-connected-and-automated-driving-ccam.pdf

[5]https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

The paper is structured in six sections. In Section II we present the related work, while in Section III we introduce the background and cover the basic notions of CCAM. In Section IV we present the systematic literature review and discuss our findings in Section V. Finally, we conclude the paper with final remarks in Section VI.

II. Related Work

The literature offers plenty of surveys and SotA analyses on security and privacy aspects of CCAM. Mainly, researchers studied the underlying architecture and constituting assumptions [12], highlighted privacy and security issues [22], collected possible attacks and challenges [1] or proposed solutions and countermeasures [41]. Below, we consider those studies which focused on analysing security protocols for CCAM and are thus similar (i.e., comparable) to our work. Also, we report a visual comparison between these studies and our work in Table I.

Qu et al. [39] investigated security and privacy issues in VANETs by considering primary requirements such as confidentiality, non-repudiation, availability, scalability and conditional privacy. Starting from the usual network model (i.e., Trusted Authority (TA), Road-Side Unit (RSU)s and On-Board Unit (OBU)s), they described the general authentication process of vehicles for V2I and V2V communications. The authors reviewed IDM protocols by focusing on the employed cryptographic algorithms. In particular, they mapped the algorithms to the aforementioned requirements and highlighted advantages and drawbacks. For instance, symmetric cryptography alone is not enough to guarantee non-repudiation, while Public Key Cryptography (PKC) has eventually to manage large Certificate Revocation List (CRL)s. Finally, they also discussed conditional privacy-preserving methods.

In [32], the authors highlighted the importance of authentication in VANET with respect to broadcast safety messages exchanged to preserve the safety of involved users. In particular, the authors emphasized that authentication protocols should be lightweight, scalable and equipped with the possibility to revoke malicious users. The authors classified authentication protocols into three categories, i.e., based on the type of cryptography systems, signature and verification methods used. Then, they provided a further fine-grained classification based on the underlying cryptographic mechanisms (e.g., a/symmetric encryption, IBE, single and group signatures, batch verification). The authors first provided a general description of the protocols for each category. Then, they discussed security requirements, attacks and performance, mainly by reviewing different cryptographic mechanisms.

Ali et al. [3] classified IDM protocols in CCAM according to the underlying cryptography mechanisms. They identified four different groups of IDM protocols, i.e., based on pseudonymous, group signatures, ID-PKC and hybrid anonymity. The authors explored the performance of these protocols and investigated their robustness against possible attacks (e.g., Denial of Service (DoS), replay attack, tampering, Sybil attack). In the conclusions, the authors highlighted the need for lightweight and scalable privacy-preserving IDM protocols, the computational overhead of asymmetric cryptography and the issue of efficient key distribution for group signature-based authentication. However, besides general considerations, the authors did not provide specific guidelines for new protocols.

In [30], the authors proposed a rich SotA analysis on security, privacy and trust aspects in VANETs. Starting from a detailed presentation of the background (e.g., network model, threats and attacker), they identified key security services such as availability, confidentiality, authenticity, data integrity and non-repudiation. To avoid overlapping with existing surveys, the authors reviewed IDM protocols with a focus on anonymity and privacy. Then, they categorized the protocols based on the underlying cryptographic algorithm. After a detailed discussion on trust management, the authors concluded the paper with a review of VANET simulation tools and platforms.

Manivannan et al. [31] presented a high-level but very comprehensive review of IDM for CCAM. The authors classified protocols based on the problems they address as well as tools and techniques used to solve these problems. For instance, they clustered protocols based on identity-based and group signatures, protocols using RSUs for authentication and key distribution and those employing bilinear pairing cryptography. Moreover, they also reported some IDM protocols based on SCs and tamper-proof devices. However, since writing a comprehensive survey, they just provided a shallow description of three SC-based IDM protocols, among which the most recent work is by Ying et al. [51] from 2017.

Bagga et al. [7] provided a comprehensive report of security requirements (e.g., authentication, integrity, availability) and threats (e.g., replay attack, Sybil attack, DoS) in Internet of Vehicles (IoV). The authors linked each threat to one or more security requirements and discussed the network and the threat model. Moreover, they provided a taxonomy of IDM protocols in IoV with a focus on authentication. Again, the authors categorized protocols based on specific features (e.g., hash-based and privacy-preserving protocols). Finally, they extensively compared their performance and concluded with an overview of open challenges. In particular, they highlight the need for efficient and real-time IDM protocols, the possibility of blockchain-based authentication, secure big data analytics and granular auditing. Therefore, while providing a rich taxonomy of IDM protocols, the authors mainly investigate their performance and provide high-level considerations.

From Table I, it is possible to see that there is no related work which covers all topics considered in our paper. The work most similar to the present one is by Bagga et al. [7], which however discusses IDM and SC in a more general context than CCAM (i.e., IoV). Indeed, differently from related work, which usually aims at providing comprehensive yet high-level surveys about security, privacy and trust in CCAM, our work proposes a reasoned systematic literature review on a specific topic, i.e., SC-based IDM protocols for CCAM. While having a narrower view, this allows us to formulate concrete and practical guidelines and useful considerations for the design of new SC-based IDM protocols in CCAM.

As a final remark, besides CCAM, we note that SCs are used for strong authentication in other scenarios as well. For instance, Wazid et al. [47] discussed the use of SCs in IDM

TABLE I: Comparison with respect to existing surveys

Survey	Topics Covered: CCAM Characterisation	IDM Protocols	Use of SCs	Future Guidelines and Research Directions	Main Focus
[39] (2015)	✗	✓	✗	✗	Threats, Security vs. Privacy, Users Revocation
[32] (2017)	✗	✗	✗	✓	Authentication, Protocols Classification, Cryptographic Primitives
[3] (2019)	✗	✓	✗	✓	Performance Analysis, Protocols Classification, Privacy
[30] (2019)	✓	✗	✗	✗	Attacks on Privacy, Trust Management, Simulators
[31] (2020)	✗	✗	✓	✓	Security Issues, Authentication, Protocols Classification
[7] (2020)	✗	✓	✓	✓	Security Requirements, Attack Taxonomy, Testbeds
This work	✓(Section III-B)	✓(Section IV-B)	✓(Section IV-C)	✓(Section V-B)	CCAM Assumptions and Requirements, SC-based IDM, Guidelines

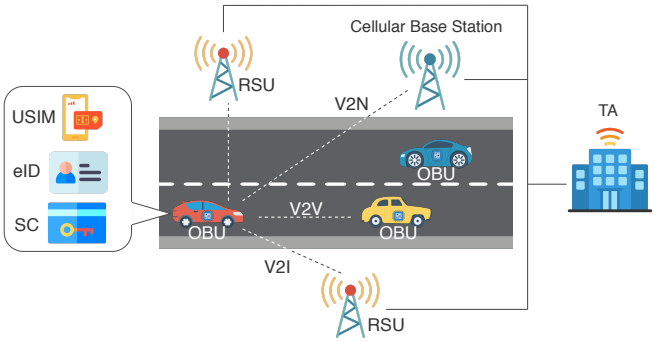

Fig. 1: Network Model for SC-Based IDM Protocols in CCAM

protocols in Internet of Things (IoT) and Wireless Sensor Network (WSN) environments. While sharing some assumptions (e.g., limited computational power, dynamic security updates), CCAM presents a set of peculiar assumptions (e.g., high mobility, standards, confidential privacy) which are not considered in other environments.

III. Background

In this section, we first present entities involved in CCAM scenarios and discuss peculiar assumptions and characteristics of CCAM. Then, we report the threat model usually assumed in the literature. Finally, we introduce the notation used in this survey to represent cryptographic operations.

A. Network Model

While some specific SC-based IDM protocols consider the presence of additional entities (e.g., anchor nodes [26] and trace managers [35]), the most commonly assumed network model is composed by the following 4 entities (see Figure 1[6]):

- *Smart Card (SC)*: in our survey, we are concerned about SCs as technical enablers for IDM in CCAM. In this context, each driver (or vehicle) is provided with a SC containing secret cryptographic material. The protection level of the cryptographic material guaranteed by a SC against external attackers and manipulation is usually certified through the FIPS 140-2[7] standard mandated by the National Institute of Standards and Technology (NIST) (a new revision of the standard, FIPS 140-3, is effective as of September 2020). The FIPS 140-2 standard specifies security requirements related to the design and implementation of cryptographic modules by considering four increasing, qualitative levels of security. To be effective enablers for strong authentication, SCs shall present anti-tampering capabilities, corresponding to security levels 3 and 4. Besides FIPS 140-2, it is worth mentioning that there exists other frameworks for SCs security certification, like the Common Criteria agreement.[8] Depending on their security level, also eID cards and cellular USIMs can be considered as SCs. The cryptographic material contained in the SC is usually generated by a trusted authority and is used through the authentication process. Each vehicle is equipped with additional hardware (e.g., SC readers) or software (e.g., Bluetooth applications) to interact with the SC;
- *OBU*: each vehicle embeds an OBU, i.e., an Engine control unit (ECU) that integrates (limited) computational and communication capabilities. The OBU is a logical gateway placed between the sensors of the vehicle (e.g., Radar, Lidar) and the outside environment (e.g., other vehicles). From now on, we use the "user", "vehicle" and "OBU" terms interchangeably, since strictly related to each other. Note that users (and thus vehicles and OBUs) are usually assumed to be untrusted, although some researchers exclude the collusion of malicious users [51, 4];
- *RSU*: RSUs are wireless access points distributed alongside the road and mainly provide traffic information and connectivity support to OBUs. Some protocols refer to RSUs as "sink nodes" [52], as RSUs usually receive and aggregate traffic-related data from nearby vehicles.

[6]Icons made by DinosoftLabs, Freepik, Linector, mavadee, photo3idea_studio and smashicons from www.flaticon.com

[7]https://csrc.nist.gov/publications/detail/fips/140/2/final

[8]https://www.commoncriteriaportal.org/ccra/index.cfm

Commonly, RSUs are used to authenticate OBUs in their area, either directly [29, 36, 4] or by forwarding the authentication requests to the back-end infrastructure [11, 51, 35]. Some researchers also proposed to use RSUs to verify [26], relay [29] or replace [17] V2V communications. However, other researchers argue that there may be some roads or areas which are not covered by any RSU [35]. Finally, RSUs are commonly assumed to be trusted [29, 11, 35] but they may be compromised by attackers [26, 50, 35, 27];

- *TA*: ITS always assume the presence of a Trusted Third-Party (TTP) called either Certificate Authority (CA) [42], Registration Authority (RA) [52], Pseudonyms Provider (PP) [37] or more commonly TA [36, 6, 51, 26, 29, 4, 35, 46]. Even though there may be different nuances of meaning (e.g., a RA focuses on the users' subscription while a CA mainly handles cryptographic certificates and a TA is active during the whole protocol [40]), the main goal of this TTP (TA hereafter) is to provide IDM, e.g., by authenticating OBUs, enrolling RSUs and revoking certificates. While logically being a single entity, the TA may consist of multiple physical sub-entities; for instance, the ITS security architecture proposed by the European Telecommunications Standards Institute (ETSI) distinguishes between enrollment and authorization authorities [19] to provide authentication and authorization credentials, respectively. Moreover, the TA can delegate its functions to other TTPs (e.g., Office of Motor Vehicles [36]). Usually, the TA has full knowledge of the system, holds secret parameters (e.g., master keys and pseudonyms resolutions), generates cryptographic materials for OBUs and RSUs (e.g., issuing SCs and distributing certificates) and cannot be compromised [26, 35, 6, 46].

OBUs and RSUs communicate through wireless channels. Originally, V2V and V2I communications leveraged the 802.11p Dedicated short-range communications (DSRC) standard by the IEEE only. However, since a few years, the 3GPP radio access technologies represent a valid alternative, due to the flexibility and ubiquitous coverage derived from the use of cellular networks (e.g., 4G and 5G). As a consequence, some SC-based IDM protocols expect the use of DSRC [26, 36, 6, 46], while others assume the presence of cellular networks technologies [51, 4]. In our survey, we remain agnostic with respect to this dualism as, either way, wireless communication channels are always assumed to be insecure [29, 35, 27].

RSUs and the TA communicate either through wired (e.g., if the RSU is deployed within a city) or wireless (e.g., if the RSU is deployed in unattended areas, like highways or motorways) channels [26]. While wireless channels are always assumed insecure, researchers still debate whether wired channels should be deemed secure [36, 29, 11, 4, 46] or not [26, 35, 27].

B. Context Assumptions and Requirements

CCAM includes a large set of applications ranging from safety-critical services (e.g., lane merging, collision risk detection, road hazard warning) to services aiming at improving the driving experience (e.g., traffic jam re-routing, infotainment) [19]. While sharing common elements (e.g., wireless channels, limited computational resources) and needs (SCs distribution, revocation and update), we note that VANETs differ from traditional WSNs, especially in terms of security trade-offs and requirements in the use of SCs. Mainly, this is due to the particular deployment context (i.e., transportation), characterized by the following assumptions:

- *high mobility* - vehicles constantly change position, creating a dynamic network of variable topology and unpredictable density. This condition introduces a delay in communications and poses serious challenges to the reliability of the connections and the scalability of the services offered by the back-end infrastructure. Moreover, it also makes connections extremely volatile and time-limited, differently from traditional WSNs in which devices are static in nature. Therefore, IDM protocols in CCAM have to design efficient procedures to manage authentication handover to transfer the context of a vehicle (e.g., information such as status and pseudonyms) among RSUs;
- *untrusted environment* - due to the public nature of the network, V2V and V2I communications happen with random and untrusted entities [17], requiring security mechanisms to ensure the authenticity of exchanged messages. Usually, this need is fulfilled by authenticating vehicles with certificates and temporary keys. We note that the use of SCs to distribute cryptographic credentials entails additional requirements and trade-offs due to the particular deployment context. For instance, SCs can be either embedded in vehicles [36, 27, 43, 11] or distributed to drivers [46, 42, 6, 51, 26, 29, 4, 35]. In the surveyed papers, while the former limits flexibility and accounts for the authentication of vehicles only (and not drivers), the latter requires the presence of a SC reader in all vehicles and it is prone to the SC-loss attack. To mitigate such an attack, SCs usually require users to input PINs or biometric features. To increase security, MFA is often enforced. However, drivers would be required to input these credentials every time they start the vehicle, with a consequent degradation on usability.
- *users' privacy* - the need for authentication has to be balanced with the users' privacy, for instance through provisioning of temporary identities (i.e., pseudonyms). Still, relevant authorities (e.g., police) should be able to map a pseudonym to the user's real identity (i.e., the concept of "conditional privacy"). However, a malicious user could abuse his pseudonyms to conduct Sybil attacks, i.e. to create multiple (virtual) identities with the goal of gaining influence on the system. This delicate trade-off between security and conditional privacy is typical of CCAM and poses further requirements in the design of IDM protocols. However, as mentioned in the introduction, in this survey we focus on security aspects only and refer the reader interested in privacy aspects of CCAM to dedicated surveys such as [30] and [31];
- *limited resources* - even though not as stringent as in WSNs, OBUs have limited computational capabilities.

Therefore, security mechanisms should be lightweight enough to not exhaust all available resources. SCs should provide alternative cryptographic primitives to fine-tune the trade-off between security (e.g., the use of strong but heavy cryptographic algorithms) and functionality (e.g., the capability to aggregate and elaborate data from internal sensors and external vehicles) [9];

- *real-time analysis* - fast elaboration of information is essential, especially in safety-critical services with low latency requirements (e.g., lane merging). As such, IDM protocols should yield minimum overhead;
- *real-world impact* - CCAM has an immediate impact on the physical world. As many CCAM services integrate external information to formulate driving recommendations (e.g., lane change), tampered messages may seriously affect the safety of involved users. Therefore, it is crucial to ensure the integrity of exchanged messages and to devise fail-safe mechanisms to avoid worst-case situations (e.g., car crashes). In this context, the use of SCs helps to guarantee accountability in case of incidents;
- *long-time functioning* - differently from other contexts (e.g., WSN), vehicles usually stay on the road for 15-20 years. Unfortunately, the discrepancy of in-vehicles technologies across such a considerable timespan significantly hampers the adoption of new paradigms such as CCAM. Moreover, we note that it may be complex to design and propose CCAM services (e.g., lane merging) when not all involved vehicles actively participate. For instance, in [34], the authors assessed through simulations the effectiveness of a lane-merging CCAM service when varying the market penetration of V2V and V2I capable vehicles. Their work showed that the threshold market penetration rate of cooperative vehicles for effective CCAM is 30%. Furthermore, when all vehicles participate in cooperative maneuvers, maximum lane capacity increases by 300%;
- *heterogeneous market* - differently from traditional WSNs, vehicles are produced by distinct car manufacturers. As such, the integration of a common service (e.g., IDM) is difficult due to both the lack of common interfaces and the heterogeneous pool of vehicles. For instance, SCs employed in different countries (and possibly under different regulations) should offer the same cryptographic primitives to promote interoperability. In this regard, standardisation efforts play a crucial role;
- *standardisation* - To ensure a high level of security, safety and compliance of CCAM, there exist several standardisation bodies like the Society of Automotive Engineers (SAE) in the United States of America (US) and the ETSI in the EU, which are working on distinct technical aspects of ITS. While the SAE is concerned about the cybersecurity of single vehicles [14], the ETSI focuses with a dedicated technical committee[9] on the communication aspects of ITS. Therefore, international standards should be considered when designing CCAM services (e.g., IDM protocols). For instance, the ETSI specifies ITS security services for the establishment and maintenance of identities and cryptographic material in ITS communications [44]. Besides, the ETSI is researching SC-based authentication with a technical committee[10] dedicated to the development of specifications for SCs in a multi-application capable environment and the secure provisioning of SC-based services. Finally, we highlight the presence of other standardisation bodies which are not focused on ITS only but that nonetheless may be relevant, such as the International Organization for Standardization (ISO) and the European Committee for Standardization (CEN) in the EU. For instance, ISO proposed a series of standards related to the use of both contact and contactless SCs for digital authentication [21].

Summarising, CCAM scenarios are characterised by several assumptions, requirements and trade-offs which influence and make difficult designing SC-based IDM protocols.

C. Threat Model

The most common threat model considers both external and internal attackers [6]. External attackers try to impersonate authenticated parties and disrupt communications through DoS or jamming attacks. Internal attackers are authenticated or compromised vehicles or RSUs that, either maliciously or accidentally (e.g., due to faulty sensors), endanger the security of communications and the users' safety, for instance by injecting bogus information.

The Dolev-Yao (DY) adversary model [13] is widely adopted to formally express the capabilities of an external attacker [47]. In the DY model, the attacker has full control over the network, i.e., he can eavesdrop, intercept, modify and replay any message. However, an attacker in the DY adversary model cannot break cryptography (e.g., brute-force) nor affect the physical world. Therefore, the Canetti-Krawczyk (CK) adversary model [8], in which an attacker can conduct physical attacks (e.g., on OBUs and RSUs) and retrieve secrets from SCs, is more suitable for CCAM [47]. Finally, we note that it is often assumed that attackers cannot tamper or compromise neither the TA, nor the system initialisation phase (i.e., the definition of public and private cryptographic parameters) nor the registration process of OBUs and RSUs [51, 29, 11, 4, 35].

While the majority of attacks (e.g., DoS, replay, forgery) can be detected and addressed with proper security mechanisms, reliability of information does not strictly depend on security, but rather on trust. Indeed, the fact that a message was properly signed by a correctly authenticated vehicle does not ensure the accuracy of its content. In some CCAM services (e.g., lane merging), unreliable information (e.g., vehicle position or speed) may lead to safety risks. This issue requires the design of frameworks to assess the reliability of information exchanged in V2V and V2I communications. In this regard, some researchers proposed frameworks to evaluate the trustworthiness of data exchanged between authenticated entities [2, 16]. However, we note that the literature tends to deal with the two issues of ensuring the security of communications and evaluating the messages content trust separately. Since we are

[9]https://www.etsi.org/committee/1402-its

[10]https://www.etsi.org/committee/1411-scp

surveying SC-based IDM protocols, we focus on the security aspects only and omit trust management.

D. Notation

We introduce the notation used in the paper in Table II. We use primes to distinguish multiple instances of the same (logical) element. For example, in presence of two random numbers, we reference them as r and r', respectively. The e symbol is a placeholder for a generic entity, while the $(\cdot)$ symbol is a wildcard for data. For instance, $\mathbf{k}_e^{\mathbf{s}}$ reads as the secret cryptographic key of the entity e, where e can be a user, an OBU, a SC, a RSU or the TA. Consequently, $\{\cdot\}_{\mathbf{k}}$ reads as the encryption of some data $(\cdot)$ (i.e., the plaintext) with a generic key $\mathbf{k}$, where $\mathbf{k}$ can be a symmetric or an asymmetric key, and $\{\cdot\}_{\mathbf{k}}^{-1}$ is the decryption of some data $(\cdot)$ (i.e., the ciphertext). Symmetric cryptography uses a single cryptographic key $\mathbf{k}^{\mathbf{sym}}$ for both encryption and decryption. For example, given a plaintext m, the corresponding ciphertext is $c = \{m\}_{\mathbf{k}^{\mathbf{sym}}}$ and the decryption is $m = \{c\}_{\mathbf{k}^{\mathbf{sym}}}^{-1}$. Instead, asymmetric cryptography uses a pair of public $\mathbf{k}^{\mathbf{p}}$ and secret $\mathbf{k}^{\mathbf{s}}$ cryptographic keys. While $\mathbf{k}^{\mathbf{p}}$ is known to everyone, $\mathbf{k}^{\mathbf{s}}$ is kept private by the owner of the key pair. Usually, $\mathbf{k}^{\mathbf{p}}$ is used to encrypt a plaintext m and $\mathbf{k}^{\mathbf{s}}$ is used to decrypt the corresponding ciphertext $c = \{m\}_{\mathbf{k}^{\mathbf{p}}}$, i.e., $m = \{c\}_{\mathbf{k}^{\mathbf{s}}}^{-1}$. Asymmetric cryptography is also used to create (with $\mathbf{k}^{\mathbf{s}}$) and verify (with $\mathbf{k}^{\mathbf{p}}$) digital signatures, which guarantee the authenticity and integrity of given data. As the secret key $\mathbf{k}^{\mathbf{s}}$ is assumed to be known only by the owner of the key pair, a digital signature also provides accountability. Moreover, digital signatures can be used to create certificates, i.e., cryptographic proofs binding a key pair with an identity (or pseudo-identity). We use the $\mathbf{Cert}_e(e')$ symbol to represent a cryptographic certificate for e issued by e'. Certificates can be self-signed (i.e., an entity creates a certificate binding his key pair to himself) or endorsed by a (trusted) party in the context of a PKI operated by one or more CAs (in ITS, the role of the CA is usually assumed by the TA). The $\mathbf{H}(\cdot)$ symbol represents a (cryptographic) hash function, which takes as input an arbitrary sequence of bytes and produces outputs of fixed size called hash values or digests. Hash functions are often used in combination with symmetric cryptography to create Message Authentication Codes (MACs), i.e., special digest values which guarantee the authenticity and integrity of messages. We highlight that, while MACs are faster to compute with respect to digital signatures (i.e., symmetric vs. asymmetric cryptography), they do not provide non-repudiation of the sender, as the symmetric key used to create the MAC is known by multiple entities. Finally, to describe the exchange of information between two or more entities, we use the widely known Alice & Bob notation. For example, $e \rightarrow e' : m$ reads as the entity e sends a message m to the entity e' over an insecure channel $\rightarrow$. Additionally, we use $\Rightarrow$ to indicate a secure channel (e.g., offline exchange) and $*$ as the recipient entity to indicate a broadcast message.

TABLE II: Notation and symbols

Element	Symbol	Description
Entities	e	A generic entity
	u	A user (e.g., driver)
	OBU	An On-Board Unit
	SC	A Smart Card
	RSU	A Road-Side Unit
	TA	The Trusted Authority
Cryptographic Material	PW_e	The password of e
	BIO_e	The biometric feature of e
	ID_e	The identifier of e
	PID_e	The pseudo-identifier of e
	S_e	A secret value known by e
	$\mathbf{k}$	A generic cryptographic key
	$\mathbf{k}_e^{\mathbf{s}}$	The secret key of e
	$\mathbf{k}_e^{\mathbf{p}}$	The public key of e
	$\mathbf{k}^{\mathbf{sym}}$	A symmetric key
	$\mathbf{k}^{\mathbf{group}}$	A group key
	$\mathbf{Cert}_e(e')$	A cryptographic certificate of e issued by e'
Mathematical Elements	r	A random number
	n, q	Two prime numbers
	F_n	A finite field over n
	f	A generator for F_n
	$E(F_n)$	An Elliptic Curve (EC) over F_n
	P	A point on $E(F_n)$
	G_q	A group over q
	g	A generator for G_q
	b	A point in G_q
	ts	A timestamp
	Exp_{ts}	An expiration time
Cryptographic Operations	$\oplus$	Exclusive OR
	$\|$	Concatenation
	$\{\cdot\}_{\mathbf{k}}$	Encryption operation with $\mathbf{k}$
	$\{\cdot\}_{\mathbf{k}}^{-1}$	Decryption operation with $\mathbf{k}$
	$\mathbf{H}(\cdot)$	Hash function
	$G_q \times G_{q'} \rightarrow G_{q''}$	A pairing operation
Message Exchange	$\rightarrow$	Insecure channel
	$\Rightarrow$	Secure channel
	$*$	Broadcast communication
	m	Exchanged message

IV. Protocols Survey

In this section, we introduce the analysis of the surveyed SC-based IDM protocols. Again, we highlight that we only consider protocols involving SCs as key enablers for strong authentication. Our approach is to identify the basic structure of an SC-based IDM protocol and compare available protocols to infer similarities and differences to then formulate guidelines for the design of new SC-based IDM protocols for CCAM. In particular, we present the methodology adopted for surveying papers in Section IV-A. Then, in Section IV-B we introduce a unified high-level view of the 8 common steps (e.g., system setup, users registration, V2I authentication) which compose SC-based IDM protocols in CCAM. Finally, in Section IV-C we highlight the most important features of the protocols, report them in Table III and describe how they implement the 8 common steps previously identified.

As a final remark, we highlight that many of the surveyed papers present their protocols as "authentication protocols" rather than "identity management protocols". Mainly, this is because their focus is on the authentication of vehicles and RSUs. However, we deem "identity management" to be a more proper keyword, as it is comprehensive with respect to the different aspects considered in the surveyed protocols (e.g., generation, distribution, use and revocation of credentials).

A. Methodology

We limit the SotA to a 10 years time span, i.e. from 2010 to 2020, as the first SC-based IDM protocol for CCAM was proposed in 2010 [36]. We define a set of relevant keywords (i.e., CCAM, ITS, VANET, Smart Card, Authentication) to find related literature on popular search engines (i.e., IEEE explore[11], Google Scholar[12], Research Gate[13]). Then, we employ a bi-directional snowball process by checking both cited and citing papers. From an initial collection of 30 papers, we eliminate those which do not propose SC-based IDM protocols in CCAM and kept 19 papers. Then, we limit the scope to SC-based IDM for V2V and V2I communications in real-time CCAM services and discarded 7 papers, which instead focus on management and offline use of data generated by vehicle sensors (see excluded papers in Section IV-A1). Finally, we kept 12 papers for our survey. The SotA was performed from May to July 2020. We report in Figure 2 the citing/cited relationship among the surveyed papers, where an arrow going from a paper to another means that the first paper cites the second one. We group [50] and [51] in a single box as the latter is an extension of the former.

1) Excluded Papers: Even though proposing an SC-based IDM protocol for CCAM, the following articles address a different use case, as they focus on the management and the offline use of data generated by vehicle sensors and not on V2V or V2I communications in real-time CCAM services. As such, we exclude them from the survey. Mohit et a. [33] designed an IDM protocol in which vehicles can send traffic-related data to RSUs (sink nodes) distributed alongside the road. Then, by analysing these data, traffic managers can prevent or react to emergencies. In both [5] and [25], the authors highlighted the vulnerabilities present in [33] and then proposed a refined IDM protocol. Again, vehicles send data to sink nodes where special users (e.g., police officers) can monitor the traffic situation. Yu et al. [52] proposed an IDM protocol for vehicular communications based on SC. The network model considers vehicle sensors, sink nodes and traffic managers which can control the response to traffic jams, speed, and emergencies based on the data collected by sink nodes. The authors used Burrows–Abadi–Needham (BAN) logic for formal analysis and the AVISPA tool for formal verification in the DY attack model. Kumar et al. [24] proposed an IDM protocol for Vehicular Cloud Computing (VCC) based on biometrics and Elliptic-curve cryptography (ECC). VCC is yet another paradigm that aims at coordinating the computational and storage resources of idling vehicles to elaborate data. In other words, VCC is a profitable method to promote the use of surplus resources to offer maximum benefit to the users. Chandrakar et al. [10] proposed a new SC-based IDM protocol to solve the shortcomings of previous protocols. They verified the security of their protocol through formal analysis with AVISPA and briefly evaluated the performance. In [40], the authors highlighted and addressed the vulnerabilities in [52]. Consequently, the authors proposed an IDM protocol using biometrics instead of passwords and demonstrated the security of the protocol with BAN logic. Again, the network model consists of vehicle sensors, sink nodes and traffic managers who use data for traffic management.

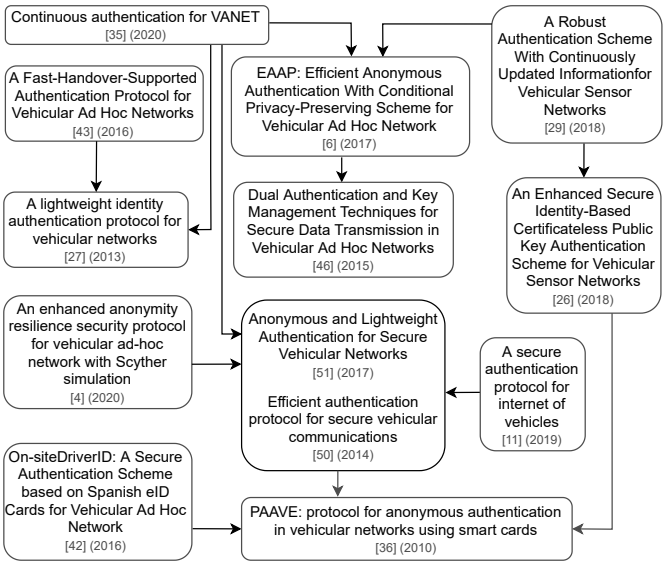

Fig. 2: Citing/cited relationship among surveyed papers

B. Common Steps

As explained in the introduction, we identify 8 common steps in SC-based IDM protocols. Generally, a protocol starts with a first phase concerning the initialisation of the system and the distribution of cryptographic material to users and RSUs. Then, the protocol enters its operational phase in which entities communicate and exchange messages. Finally, the last steps regard the management of cryptographic material (e.g., revocation, update) distributed to users and RSUs. Below, we describe in detail these 8 common steps:

1) *system setup*: the TA defines and shares with RSUs and OBUs public parameters such as cryptographic algorithms (e.g., RSA and ECC) and hash functions (e.g., MAC) used in the protocol. Internally, the TA chooses secret parameters like secret keys and seeds for random number generation. Moreover, the TA registers and authenticates RSUs, usually by distributing certificates. It is always assumed that attackers cannot interfere with the system setup nor acquire any knowledge of the secret parameters [51, 29, 11, 4, 35, 46];
2) *user registration*: before hitting the road (e.g., during matriculation), each vehicle usually undergoes a one-time registration process with the TA by submitting the OBU's or the user's identifier (e.g., driving license ID) to receive a SC embedding cryptographic material (e.g., Keyed Hash Message Authentication Code (HMAC)s or PKC certificates). Usually, this step also includes the definition of a password by the user to unlock the SC functionalities. Note that the SC may be released by a delegated TTP, like the Office of Motor Vehicles [36], or may be already in possession of the user (e.g., eID

[11]https://ieeexplore.ieee.org/Xplore/home.jsp
[12]https://scholar.google.it/
[13]https://www.researchgate.net/

cards or USIMs). Again, it is usually assumed that no attacker can interfere with the registration process [26, 29, 11, 4, 35], although attackers can register with the TA to receive a SC (i.e., internal attackers);

3) *user login*: during the login step, a user inputs the chosen PIN [36], password [51] or biometric features [29] to unlock the SC. Usually, these credentials are either (salted and then) hashed and checked with a previously stored value [26, 50, 4] or used to derive authentication information, for instance by XORing the credentials with stored values [29]. Finally, to resist offline guessing attacks, the SC can set a threshold for the number of login attempts [51]. Differently from all the other SC-based IDM protocols, the authors of [11] do not expect any credential to unlock the SC. Indeed, these authors argue that modern vehicles have security standards (i.e., anti-thief security system) good enough to prevent stolen SC attacks and that the majority of vehicles are not equipped with secure input devices for passwords anyway;
4) *V2I authentication*: vehicles need to authenticate with the nearest RSU by using credentials derived in previous steps by cryptographic material contained in the SC. This process may [11, 51, 35, 27] or may not [29, 36, 26, 4] involve the TA. We note that, in the second case, there is the need to distribute to RSUs revocation lists (e.g., CRLs) to prevent revoked users from successfully authenticating. After a positive outcome, vehicles usually receive a symmetric key to encrypt future communications. Sometimes, this key is shared with all vehicles connected to the same RSU to implicitly enable fast broadcast communications among vehicles [36]. More often, each vehicle shares a unique symmetric key with the RSU for improving accountability and to avoid impersonation. Either way, messages are usually timestamped Global Navigation Satellite Systems (GNSSs) such as Global Positioning System (GPS) [51, 4] to avoid replay attacks [36, 26, 28, 37];
5) *RSU handover*: as they travel, vehicles move through different RSUs coverage areas. Whenever an already authenticated vehicle enters the coverage area of a new RSU, an RSU handover procedure happens. This procedure consists in transferring the context of the vehicle (e.g., related information such as status, pseudonyms and temporary keys) among RSUs to guarantee continuity in CCAM services. The default approach to implement RSU handover is to repeat the V2I authentication step [46, 42, 6, 50, 51, 26, 29, 11, 4]. However, as RSU handover happens on a frequent basis, an ad hoc procedure should be designed to enhance efficiency and avoid performance degradation [36, 27, 43, 35].
6) *V2V authentication*: to enable direct V2V communication, two vehicles need to share a symmetric key. One possible solution is to use an RSU to help vehicles in deriving a common key [29], while the common alternative is that vehicles derive a common key by exchanging their certificates; these are usually temporary and refer to pseudonyms to preserve users' privacy. A drawback of the second approach is that computing and verifying cryptographic signatures for each V2V communication is a burdensome task for OBUs;
7) *login update*: as for any system involving passwords, many of the surveyed IDM protocols expect the possibility to update the credentials needed to unlock the SC. Several different approaches has been chosen for this task; the most simple (and inefficient) solution is to execute again the registration process with the TA [26, 35] or to interact with RSUs [29] to update internal parameters. Other protocols allow instead for a completely offline credentials update [4, 51], as the SC itself can compute the hash of the new credentials;
8) *revocation*: to exclude internal attackers and misbehaving users from CCAM services, IDM protocols should expect a revocation phase, i.e., a process in which the cryptographic material contained in the SC is invalidated. We note that this process strictly depends on the cryptographic algorithms used to implement the protocol. For instance, a PKC-based protocol will distribute CRLs [36, 35], which, however, are known to affect scalability by adding a further computational burden at the infrastructure level (i.e., on RSUs). Other protocols may require to login in the OBU and delete all information stored in the SC [29], thus shifting the scalability issue from the infrastructure to the user level. Unfortunately, the majority of protocols do not even address the revocation problem [11, 26, 51, 50, 4]. Moreover, only one protocol proposed a sub-protocol through which a vehicle can report malicious activities [35].

As a final remark, note that some protocols may not address all of these steps. This may happen either because the authors left some of these steps out (often as future work) or because that step is pointless in the protocol. For instance, without a user login step, there cannot be a login update step [11].

C. Analysis of Protocols

SC-based IDM protocols in CCAM share many common elements (e.g., network model, assumptions). However, each protocol employs different cryptographic algorithms and parameters and proposes a different design for the authentication of vehicles and the exchange of messages. Below, we describe surveyed SC-based protocols ordered by publication year; we report those characteristics that differentiate the protocols from each other while also highlighting similarities and common features. Besides, we present a detailed view of how the surveyed protocols implement the 8 common steps identified in Section IV-B. We highlight that we do not aim at thoroughly describe each step of the protocols, as some steps are really complex and involve the exchange of many messages and cryptographic operations; in this case, we just describe the high-level functioning of the step. Indeed, our goal is to give the intuition of the protocols main features, functioning, cryptographic primitives employed and actors involved. For a deeper understanding, we refer the interested reader to the related protocol. Finally, we report a summary of the surveyed protocols in Table III.

TABLE III: Summary of surveyed protocols

Protocol	Focus	Cryptographic Primitives	Symmetric Key Generation	Security Analysis	Batch Verification	Communication Technology	Steps Implemented
[36] (2010)	SCs for strong authentication in CCAM.	symmetric cryptography, PKC (PKI), hash	By RSUs	none	no	DSRC	All but 7
[27] (2013)	Fast handover among RSUs.	symmetric cryptography, PKC, hash	Pre-computed	informal	no	DSRC	1, 2, 4, 5
[46] (2015)	2-factor authentication with biometrics.	symmetric cryptography, PKC, hash	Pre-computed	informal	no	DSRC	All but 5, 7
[43] (2016)	Use hash functions and XOR operations only.	Hash	No symmetric keys	formal	no	DSRC, 4G-5G	1, 2, 4, 5
[42] (2016)	Fast conditional privacy resolution and eID.	PKC (PKI), hash	No symmetric keys	none	no	Unspecified	3, 4, 6
[6] (2017)	Conditional privacy and efficiency.	PKC (PKI), hash	No symmetric keys	formal	no	DSRC	1, 2, 4, 6, 8
[50, 51] (2017)	Local update of SC login credentials.	symmetric cryptography, PKC, hash	By the TA	formal	no	DSRC, 4G-5G	All but 5, 8
[26] (2018)	The first to mention the relevance of standards.	ECC, hash	No symmetric keys	formal	yes	DSRC	All but 5, 8
[29] (2018)	Tool-supported analysis, authentication via RSUs.	Symmetric cryptography, hash	Agreed by OBU and RSU	AVISPA[14]	yes	Unspecified	All but 5
[11] (2019)	Correct vulnerabilities in [27].	Symmetric cryptography, hash	Variant of Diffie-Hellman	formal	no	Unspecified	1, 2, 3, 4
[4] (2020)	All messages flow through RSUs.	symmetric cryptography, PKC (PKI), hash	By RSUs	Scyther[15]	no	DSRC, 4G-5G	All but 5, 8
[35] (2020)	Possibility to report malicious activities.	symmetric cryptography, PKC (PKI), hash	Agreed by OBU and RSU	Tamarin[16]	no	DSRC	All

1) System Setup	The TA defines secret $\mathbf{k}^{\mathbf{s}}_{TA}$ and public parameters $G_q, \mathbf{k}^{\mathbf{p}}_{TA}, \mathbf{H}$
2) User Registration	· $TTP \Rightarrow u : SC(ID_u, ID_{TTP}, \mathbf{k}^{\mathbf{p}}_u, \mathbf{k}^{\mathbf{s}}_u, \mathbf{k}^{\mathbf{p}}_{TA}, \mathbf{Cert}_u(TTP))$
3) User Login	· $u \Rightarrow SC : PIN_u$
4) V2I Authentication	· $RSU \rightarrow * : ID_{RSU}, \mathbf{Cert}_{RSU}(TA)$ · $u \rightarrow RSU : \{\{r_u\}_{\mathbf{k}^{\mathbf{s}}_u}, ID_u, ID_{TTP}, \mathbf{Cert}_u(TTP)\}_{\mathbf{k}^{\mathbf{p}}_{RSU}}$ · $RSU \rightarrow u : \{r_u, \mathbf{k}^{\mathbf{sym}}, Exp_{ts}\}_{\mathbf{k}^{\mathbf{p}}_u}$ Note that $\mathbf{k}^{\mathbf{sym}}$ is the same for each user
5) RSU Handover	RSUs share in advance multiple session keys
6) V2V Authentication	· $u \rightarrow * : \{m, \{ID_u, \{\mathbf{H}(m)\}_{\mathbf{k}^{\mathbf{s}}_u}\}_{\mathbf{k}^{\mathbf{p}}_{RSU}}\}_{\mathbf{k}^{\mathbf{sym}}}$ Note that u can only broadcast messages
8) Revocation	By distribution of CRLs to RSUs

Algorithm 1: Paruchuri and Durresi [36] (2010)

In 2010, Paruchuri and Durresi [36] (Algorithm 1) were the first to propose SCs for vehicle strong authentication in CCAM. Each SC stores a pair of public-private keys along with a certificate issued by a TTP (i.e., the Office of Motor Vehicles) and the public key of the TA. RSUs broadcast beacon messages to which OBUs answers with a challenge (i.e., an encrypted nonce). If not under direct coverage, an OBU can ask other OBUs to relay RSUs beacon messages. However, we note that malicious OBUs could ignore the request, leading to DoS attacks. After a successful authentication, RSUs share a new session key with OBUs for future communications and handover procedures. Forward secrecy is guaranteed as session keys are not related to each other. We highlight that each RSU shares the same session key with all authenticated OBUs under the coverage area of the RSU, so to enable fast V2V communication. However, while promoting efficiency, only the RSU can verify the authenticity and integrity of a message (as the signature of the message is encrypted with the RSU public key). For this reason, malicious insider attackers can easily spread bogus information. In the worst case, other OBUs may use this information to make safety-critical decisions (e.g., lane merging) before the RSU can raise a warning to distrust the message. As a solution, OBUs could wait for the RSU to confirm the message, but this approach would lead to a greater delay in communications. Finally, we note that this IDM protocol provides broadcast (and not direct) V2V communication only and that user's privacy is preserved with respect to other drivers but not RSUs.

1) System Setup	The TA defines secret $\mathbf{k}^{\mathbf{s}}_{TA}$ and public parameters $\mathbf{k}^{\mathbf{p}}_{TA}$ and $\mathbf{H}_{inv}$, where $\mathbf{H}_{inv}$ is an invertible hash function
2) User Registration	· TA computes $\mathbf{k}^{\mathbf{sym}} = \mathbf{H}(ID_u \| PW_u)$ · $TA \Rightarrow u : SC(ID_u, PW_u, \mathbf{k}^{\mathbf{sym}})$
4) V2I Authentication	· u computes $mID_u = \{ID_u\}_{\mathbf{k}^{\mathbf{p}}_{TA}}$ · $u \rightarrow RSU : mID_u$ · $RSU \rightarrow u : ID_{RSU}, r_{RSU}$ · u computes $As = \mathbf{H}_{inv}(\mathbf{k}^{\mathbf{sym}}, r_u, r_{RSU})$ and $IS = Sr \oplus As$, where As is the authentication sequence, Sr is a random session secret sequence. RTA is a challenge sequence and ATA is the response sequence · $u \rightarrow TA : mID_u, r_u, r_{RSU}, IS, RTA_u$ · $TA \rightarrow RSU : \{Sr, ts, r_{TA}\}_{\mathbf{k}^{\mathbf{p}}_{RSU}}$ · $RSU \rightarrow u : RTA_{RSU}, ATA_{RSU}$ · $u \rightarrow RSU : ATA_u$ · $RSU \rightarrow TA : \{ID_{RSU}, r_{TA}\}_{\mathbf{k}^{\mathbf{p}}_{TA}}$ Note that $\mathbf{k}^{\mathbf{sym}}$ is different for each user
5) RSU Handover	The TA pre-distributes the authentication sequence As of a vehicle to all RSUs on the route of the vehicle

Algorithm 2: Li and Lui [27] (2013)

Given the high mobility of vehicles in CCAM scenarios, the handover of authentication credentials among RSUs happens regularly. Therefore, the authors of [27] (Algorithm 2) proposed a Lightweight Identity Authentication Protocol (LIAP) with the main goal of reducing the handover authentication delay and minimize the impact on CCAM services. The

authors assumed that each user derives from his ID and password a common key $\mathbf{k^{sym}}$ together with the TA (called "Authentication Server"). The key is stored in a SC and used during the authentication process. In detail, each OBU generates a secret random sequence that is sent to the TA and then distributed to all RSUs that cache this information to speed up the handover procedure. Although the authors proposed a security analysis of their protocol, several vulnerabilities (e.g., parallel session attack) were discovered [20, 54, 43]. For instance, using the same pseudo-identifier (i.e., mID_u) for all V2I authentications allows attackers to track vehicles with a consequent impact on drivers' privacy. Moreover, as $\mathbf{k^{sym}}$ is never updated, the protocol is vulnerable to brute-force and online-guessing attacks. Finally, the protocol does not expect V2V communication and the access to the SC is not protected with a login procedure.

1) System Setup	The TA defines secret $q, q', G_{q'}$ and public parameters $\mathbf{H}$
2) User Registration	· $TA \Rightarrow u : SC(\mathbf{k}_u^{\mathbf{sym}}, BIO_u), \mathbf{k^{group}}$
3) User Login	· $u \Rightarrow SC : BIO_u$
4) V2I Authentication	· u creates $hc = \mathbf{H}(\mathbf{k}_u^{\mathbf{sym}} \| r_u)$ and computes $ar = \{r_u, hc, ID_u\}_{\mathbf{k}_u^{\mathbf{sym}}} \| ID_u \| ID_{TA} \| ts$ · $u \rightarrow RSU : ar$ · $RSU \rightarrow TA : \{ar \| ID_{RSU} \| ts'\}_{\mathbf{k}_{RSU}^{\mathbf{sym}}}$ · TA generates authentication code $ac = \mathbf{H}(hc)$ and signature $sig = \{ac \| ID_u \| ts'' \| Exp_{ts}\}_{\mathbf{k}_{TA}^{\mathbf{s}}}$ · $TA \rightarrow RSU : \{\{ac, sig\}_{\mathbf{k}_u^{\mathbf{sym}}}\}_{\mathbf{k}_{RSU}^{\mathbf{sym}}}$ · $RSU \rightarrow u : \{ac, sig\}_{\mathbf{k}_u^{\mathbf{sym}}}$
6) V2V Authentication	· $u \rightarrow * : \{m\}_{\mathbf{k^{group}}} \| sig$ Note that u can only broadcast messages
8) Revocation	By updating and then re-distributing $\mathbf{k^{group}}$

Algorithm 3: Vijayakumar et al. [46] (2015)

In [46] (Algorithm 3), the authors proposed a protocol with users' login toward the SC through biometrics (i.e., fingerprint). In detail, a user first provides to the OBU his fingerprint, which is compared with the one stored in the SC. Afterwards, the vehicle secret key ($\mathbf{k}_u^{\mathbf{sym}}$) contained in the SC authenticates the user toward the TA. Upon a successful authentication, the vehicle receives from the TA a temporary signature to append to broadcast V2V messages. The protocol considers three groups of users, i.e., primary (or premium), secondary and unauthorized. The TA generates two different group keys which are used for broadcast within the first two groups. Whenever a vehicle joins or leaves a group, the TA has to derive new group keys to guarantee forward and backward secrecy. Interestingly, the authors considered the presence of multiple TA, ideally one for each country (i.e., nation), and accounted for SC-loss attacks. However, the privacy of users' location was left as future work, and the protocol only enables broadcast (and not direct) V2V communications. Most importantly, as the signature appended to a message is not directly linked to the message (e.g., through hash functions) but is statically computed during the V2I authentication step, it provides neither non-repudiation nor accountability nor integrity. Finally, as $\mathbf{k}_u^{\mathbf{sym}}$ is never updated, the protocol is vulnerable to brute-force and online-guessing attacks.

Tai et al. [43] (Algorithm 4) started from the flawed protocol in [27] to propose a new SC-based IDM protocol for CCAM

1) System Setup	The TA defines secret $S_{TA,OBUs}, S'_{TA,RSUs}$, $S''_{TA,OBU}, S'''_{TA,RSU}$ and public parameters $\mathbf{H}$. The TA loads $S_{TA,OBUs}$ into all OBUs, $S'_{TA,RSUs}$ into all RSUs and a different $S'''_{TA,RSU}$ into each RSU
2) User Registration	· $TA \Rightarrow u : SC(ID_u, PW_u)$ · The SC derives $S''_{TA,OBU}$, i.e., the secret shared between the TA and u
4) V2I Authentication	· $u \rightarrow RSU$: initialization request · RSU computes $m_1 = \mathbf{H}(ts \| ID_{RSU} \| S'_{TA,RSUs} S'''_{TA,RSU})$ · $RSU \rightarrow u : ID_{RSU}, ts, m_1$ · u computes $m_2 = \mathbf{H}(ts \| ID_{RSU} \| S_{TA,OBUs}) \oplus ID_u$ and $m_3 = \mathbf{H}(m_1 \| m_2 \| S''_{TA,OBU})$ · $u \rightarrow RSU : m_2, m_3$ · $RSU \rightarrow TA : m_2, m_3, ID_{RSU}, ts$ · TA checks all hashes and computes w, a periodically updated secret for authentication and its lifetime LT · $TA \rightarrow RSU : w, LT$ · $RSU \rightarrow u : w, LT$
5) RSU Handover	· $u \rightarrow RSU'$: handover request · RSU' computes $m_1 = \mathbf{H}(ts' \| ID'_{RSU} \| S'_{TA,RSUs} \| w \| LT)$ · $RSU' \rightarrow u : ID'_{RSU}, ts', m_1$ · u computes $m_2 = \mathbf{H}(ts' \| ID'_{RSU} \| LT \| w \| S_{TA,OBUs}) \oplus ID_u$ and $m_3 = \mathbf{H}(m_1 \| m_2 \| ts \| ID'_{RSU} \| LT \| w)$ · $u \rightarrow RSU' : m_2, m_3, ts$ · RSU' computes $m_4 = \mathbf{H}(m_2 \| ID'_{RSU} \| ts'' \| w \| LT)$ and $m_5 = \mathbf{H}(ts' \| ts'' \| ID'_{RSU} \| m_2 \| w \| LT \| S'_{TA,RSUs} \| S'''_{TA,RSU'})$ · $RSU' \rightarrow u : ID'_{RSU}, ts'', m_4$ · $RSU' \rightarrow TA : ID'_{RSU}, ts', ts'', m_2, m_5$

Algorithm 4: Tai et al. [43] (2016)

supporting fast-handover of vehicles authentication. Particularly, the author used neither asymmetric nor symmetric cryptography. Instead, the protocol is composed of a sequence of hash and XOR operations. For this to be possible, during the system setup, all OBUs and all RSUs receives a unique secret value from the TA in the SC, that is assumed to be embedded in the OBU. It follows that the TA is involved in both V2I authentication and handover steps. Unfortunately, the authors did not provide a performance analysis to gauge the trade-off between the efficiency of hash and XOR operations with the overhead of involving the TA in all steps, including the lookup time for retrieving the unique secret values. Also, they neither discuss users' privacy nor direct V2V nor broadcast communications, so many CCAM services (e.g., lane merging) cannot be provided. Finally, users' revocation was not addressed, so it is not possible to react to a CK attacker.

3) User Login	· $u \Rightarrow SC : PIN_u$
4) V2I Authentication 6) V2V Authentication	· Assume the presence of an authority A · $A \rightarrow u : ID_A, \mathbf{Cert}_A(A)$ · $u \rightarrow A : \{\mathbf{Cert}_u(A)\}_{\mathbf{k}_A^{\mathbf{P}}}$ · $A \rightarrow u : \{r_A\}_{\mathbf{k}_u^{\mathbf{P}}}$ · $u \rightarrow A : \{\{r_A\}_{\mathbf{k}_u^{\mathbf{s}}}\}_{\mathbf{k}_A^{\mathbf{P}}}$

Algorithm 5: Sánchez-García et al. [42] (2016)

In [42] (Algorithm 5), the authors gave great relevance to the concept of conditional privacy. However, they argued that the process of mapping pseudonyms to real users' identities is time-consuming for authorities, as it usually involves a manual interaction with the TA and RSUs. Therefore, they proposed an IDM protocol for urban ITS employing (Spanish) eID cards as SCs to allow authorities to solve pseudonyms in

real-time. Either with a vehicle (e.g., a police car) physically present on the road (V2V) or remotely through RSUs (V2I), an authority broadcasts its certificate and public key to all nearby vehicles. These vehicles answer by encrypting their certificate and public key with the authority's public key. To avoid replay attacks, the authority then sends a random nonce (i.e., the challenge) encrypted with the user's public key. Finally, vehicles decrypt the challenge and send it back (encrypted) to the authority along with additional information (e.g., registration plate number). While introducing an innovative element (i.e., the use of eID cards as SCs), the protocol is limited to pseudonyms solving. Moreover, as the authentication request can only be broadcast, in case of intense traffic, it may saturate the communication channel. Finally, malicious vehicles can simply ignore the authentication request.

1) System Setup	The TA defines secret r, r', r' and public parameters $q, e, g, g', G_q, G_{q'}, G_{q''}, A = g^r, B = g^{r'}, \mathbf{H}$
2) User Registration	· TA generates ID_u and pseudonyms of the form $p = g^{r+r_{TA}}$. Then, TA computes $Ti = g^{\frac{1}{r'_{TA}+r+r'}}$ and $Ei = g^{-r_{TA}}$ · $TA \Rightarrow u : SC(p, Ti, Ei)$
4) V2I Authentication 6) V2V Authentication	u generates a short-time anonymous certificate $\mathbf{Cert}_u(u)$ from one of the pseudonyms provided by the TA. Note that u can only broadcast messages
8) Revocation	The TA maintains an identity revocation list

Algorithm 6: Azees et al. [6] (2017)

Also the authors in [6] (Algorithm 6) focused on the concept of conditional privacy. In their protocol, users can autonomously generate anonymous certificates to protect their privacy starting from a pool of pseudonyms provisioned by the TA. Moreover, the authors argue that, even though commonly found in IDM protocols, a PKI is not suitable for securing CCAM services, as signatures and certificates verification is computationally expensive. As usual, the network model comprehends SCs (distributed offline and containing authorisation keys), TA, RSUs and OBUs. Differently from other protocols, the authors acknowledge that there may be more than one TAs. Moreover, their protocol can guarantee non-repudiation and integrity of exchanged messages and accounts for revocation of malicious users and compromised SCs. However, the authors considered broadcast communication only, i.e., there is no possibility for direct and confidential exchange of messages through V2V communication. Moreover, the authors employ bilinear pairings, which are known to be computationally expensive operations [51, 26, 29]. Finally, the possibility of a Sybil attack given the pool of pseudonyms provisioned by the TA was not discussed.

Ying and Nayak, first in [50] and then in [51] (Algorithm 7), designed a protocol allowing users to dynamically generate pseudonyms to preserve their privacy. Users first register to the TA to obtain a SC containing secret cryptographic material. To login, a user has to input his identity, password and also a secret random number. Noticeably, users can update these credentials locally without the intervention of the TA. However, we highlight that later work identified serious vulnerabilities in this protocol, such as offline identity guessing, and masquerading attacks [11, 4, 35]. Besides, we

1) System Setup	The TA defines secret $\mathbf{k}^{\mathbf{s}}_{TA}$ and public parameters G_q, $\mathbf{k}^{\mathbf{p}}_{TA}$, $\mathbf{H}(\cdot)$ and $\mathbf{H}'(\cdot)$
2) User Registration	· u computes $HPW_u = \mathbf{H}(PW_u \| r_u)$ · $u \Rightarrow TA : HPW_u, ID_u$ · TA computes $HID_u = \mathbf{H}(ID_u)$, $Ai = \mathbf{H}(HPW_u \| HID_u), ks = \mathbf{H}(\mathbf{k}^{\mathbf{s}}_{TA} \| HID_u \| ts)$ and $Ni = HPW_u \oplus ks$ · $TA \Rightarrow u : SC(Ai, Ni, ks)$
3) User Login	· $u \Rightarrow SC : ID^*_u, PW^*_u, r_u$ · SC compares Ai with $Ai^* = \mathbf{H}(\mathbf{H}(PW^*_u \| r_u) \| \mathbf{H}(ID^*_u))$ Note that, to resist offline guessing attacks, the SC has a threshold for the number of login attempts
4) V2I Authentication	· SC computes $dk = Ni \oplus (PW_u \| r_u)$, $C_1 = \mathbf{k}^{\mathbf{p}}_{TA}{}^{\mathbf{H}(ID_u)} \bmod q$, $DID_u = \mathbf{H}(C_1 \| \mathbf{H}(ID_u) \| r'_u)$ and $CV = \mathbf{H}(DID_u \| dk)$ · $u \rightarrow RSU : DID_u, CV, r'_u, ts$ · RSU computes $DID_{RSU} = DID_u \oplus \mathbf{H}(ID_{RSU})$ · $RSU \rightarrow TA : DID_{RSU}, CV, r'_u, ts$ · TA computes $C_3 = \mathbf{H}'(\mathbf{H}(ID_u) \| dk)$ and $M = \{r_{TA} \oplus dk\}_{\mathbf{H}'(C_3)}$ · $TA \rightarrow RSU : C_3, M, ts$ · $RSU \rightarrow u : C_3, M, ts$ · u retrieves r_{TA} from M and stores it
6) V2V Authentication	Based on two hash chains [49]
7) Login Update	· u logs in the SC · $u \Rightarrow SC : PW^{new}_u$ · SC updates $Ai^{new} = \mathbf{H}(\mathbf{H}(ID_u) \| \mathbf{H}(PW^{new}_u \| r_u))$ and $Ni^{new} = \mathbf{H}(PW^{new}_u \| r_u) \oplus ks$ Note that the TA is not involved

Algorithm 7: Ying and Nayak [50, 51] (2017)

note that the login procedure may be tedious for the user, considering that the random number has high entropy and it is, therefore, difficult to remember. Moreover, even though the SC blocks after three (wrong) login attempts, thus mitigating the consequences of the loss or theft of the SC, users' revocation was not discussed. As such, it is not possible to react to a CK attacker. Finally, even though all messages are timestamped to avoid temporal replay attacks, there is no protection against spatial replay attacks.

1) System Setup	A TTP and the TA defines secret $\mathbf{k}^{\mathbf{s}}_{TTP}, \mathbf{k}^{\mathbf{s}}_{TA}$ and public parameters $F_n, E(F_n), G_q, P, \mathbf{k}^{\mathbf{p}}_{TTP}, \mathbf{k}^{\mathbf{p}}_{TA}, \mathbf{H}(\cdot), \mathbf{H}'(\cdot), \mathbf{H}''(\cdot)$
2) User Registration	· $u \Rightarrow TA : ID_u$ · $TA \Rightarrow u : SC()$ · $u \Rightarrow SC : ID_u, PW_u$ · SC creates $\mathbf{k}^{\mathbf{s}}_u, , \mathbf{k}^{\mathbf{p}}_u$ and computes $s_u = \mathbf{H}(PW_u \oplus S_{SC}) \oplus ID_u$ and $s'_u = s_u + \mathbf{k}^{\mathbf{s}}_u$ · $u \Rightarrow TA : \{ID_u, s_u, \mathbf{k}^{\mathbf{p}}_u\}_{\mathbf{k}^{\mathbf{p}}_{TA}}$ · TA creates PID_u from $\mathbf{k}^{\mathbf{s}}_{TA}$ and PW_u · $TA \Rightarrow u : PID_u$ · $u \Rightarrow TTP : PID_u$ · $TTP \Rightarrow u$: partial secret keys
3) User Login	· $u \Rightarrow SC : ID^*_u, PW^*_u$
4) V2I Authentication 6) V2V Authentication	u chooses a pseudo-identity PID_u and use the related partial keys, ts, $\mathbf{k}^{\mathbf{s}}_u$ and PW_u to sign a message m. The receiving entity (either another vehicle or an RSU) uses public parameters to check the validity of m. Note that the protocol supports batch verification
7) Login Update	Repeat the user registration phase. Note that this is also the only way to obtain new pseudo-identities

Algorithm 8: Li et al. [26] (2018)

Li et al. [26] (Algorithm 8) used certificateless PKC supported by elliptic curve multiplication instead of bilinear pairings for improved efficiency. As certificateless PKC can generate key pairs only through an interaction between users

and a TTP, the authors assumed the presence of an additional TTP named Private Key Generator (PKG). The TA generates self-expiring pseudo-identities for users while the PKG generates partial keys, and RSUs verify messages and transfer data among vehicles. Noticeably, the authors considered international standards (i.e., ISO/IEC 7816 and ISO/IEC 14443) related to the use of electronic identification cards (i.e., SCs) during the design of the protocol and the CK adversary model. The authors considered batch authentication (i.e., authenticate multiple vehicles simultaneously rather than sequentially), the possible violation of an RSU and the possibility for users to change their login password, though this step requires the intervention of the TA, as the login update consists in repeating the registration phase. However, the authors neither discussed RSUs handover nor Sybil attacks due to the abuse of users' pseudo-identifiers nor their protocol can guarantee the confidentiality of exchanged messages.

1) System Setup	The TA pre-registers all ID_{SC}, ID_u, ID_{OBU} and defines public parameters $\mathbf{HMAC}(\cdot)$, $\mathbf{H}(\cdot)$
2) User Registration	· $u \Rightarrow SC : PW_u, BIO_u$ · SC computes $CN_i = r_u \oplus \mathbf{H}(ID_u \| BIO_u \| PW_u)$ and $RPW = \mathbf{H}(r_u \| BIO_u PW_u)$ · $u \Rightarrow TA : RPW, ts, r_u$ · TA derives authentication information AR · $TA \Rightarrow RSUs : AR$ · $TA \Rightarrow u : AR$
3) User Login	· $u \Rightarrow SC : ID_u, PW_u, BIO_u$
4) V2I Authentication	· $u \rightarrow RSU : AR$ · RSU updates AR to AR' and changes u's status to "trusted" · $RSU \rightarrow u : \mathbf{k^{sym}}$ · $RSU \rightarrow RSUs : AR'$ Note that the TA is not involved Note that $\mathbf{k^{sym}}$ is different for each u
6) V2V Authentication	When u_i (authenticated with RSU_i) wants to communicate with u_j (authenticated with RSU_j), the two RSUs share random numbers to compute secret parameters that are then sent to u_i and u_j. The parameters are used to derive a common $\mathbf{k^{sym}}$. Note that broadcast V2V communication is not considered
7) Login Update	After a successful login and V2I authentication, u chooses a new PW_u^* and BIO_u^*. These are used to update u's AR in all RSUs
8) Revocation	The TA (or a TTP) logins in the SC, deletes all stored information and commands to all RSUs to delete the authentication information AR

Algorithm 9: Liu and Zhang [29] (2018)

Even though securing CCAM services through centralized IDM with a TA is the most common approach, Liu and Zhang [29] (Algorithm 9) considered it to be too slow and computationally inefficient for practical use. Therefore, they proposed a decentralized protocol in which RSUs can autonomously authenticate vehicles once they registered with the TA. To unlock the functionalities of the SC, the protocol expects users to input both a password and also a biometric feature through a biometric extraction device. The authors conducted a formal security analysis using AVISPA[17], a tool for automated validation of internet protocols. However, even though the authors consider both direct and broadcast communications, V2V communication can only happen if mediated by RSUs, as they contribute during the agreement phase of the communication key. Consequently, in unattended environments with no available RSUs, vehicles cannot communicate. Besides, we note that assuming vehicles to be equipped with both biometric extraction devices and screens for password input may not always be true, especially on budget vehicles.

[17]http://www.avispa-project.org/

1) System Setup	The TA defines secret $\mathbf{k}^{\mathbf{s}}_{TA}$, S_{TA} and public parameters F_n, f, $\mathbf{k}^{\mathbf{p}}_{TA}$ $\mathbf{H}(\cdot)$, $\mathbf{H}'(\cdot)$
2) User Registration	· $u \Rightarrow TA : ID_u$ · TA computes $HID_u = \mathbf{H}(ID_u \oplus S_{TA})$ · $TA \Rightarrow u : SC(HID_u)$
3) User Login	No credentials needed to authenticate toward the SC
4) V2I Authentication	· SC computes $D_i = f^{r_u \bmod n}, E_i = \mathbf{k}^{\mathbf{p}}_{TA}{}^{r_u \bmod n}$, $AID_i = ID_u \oplus \mathbf{H}(E_i)$, $DIDV = \mathbf{H}(HID_u \| E_i)$, $CV_i = \mathbf{H}(AID_i \| DIDV_i \| E_i \| ts)$ · $u \rightarrow RSU : D_i, AID_i, DIDV, CV_i, ts$ · $RSU \Rightarrow TA : D_i, AID_i, DIDV, CV_i, ts, ID_{RSU}$ · TA computes $G_i = f^{r_{TA} \bmod n}, \mathbf{k^{sym}} = \mathbf{H}'(D_i{}^{r_{TA} \bmod n})$ and $C_i = \mathbf{H}'(D_i{}^{r_{TA} \bmod n} \| E_i \| HID_u)$ · $TA \Rightarrow RSU : AID_i, G_i, C_i$ · $RSU \rightarrow u : AID_i, G_i, C_i$ · u computes $\mathbf{k^{sym}} = \mathbf{H}'(G_i{}^{r_u \bmod n})$ Note that $\mathbf{k^{sym}}$ is different for each u

Algorithm 10: Chen et al. [11] (2019)

Chen et al. [11] (Algorithm 10) proposed a new IDM protocol to solved some vulnerabilities present in [51]. While assuming the same network model of [51], the new protocol eliminates the use of passwords to unlock the functionalities of SCs. Indeed, the authors claim that the user's login step is both redundant, as nowadays vehicles provide a good level of physical security, and insecure, as no vehicle integrates proper secure hardware (e.g., touch screen) to input passwords. However, the authors did not discuss whether the SC is removable and could therefore be lost outside the vehicle, leading to possible SC loss attacks. Besides, the authors did not discuss users' revocation, a fundamental procedure in presence of a CK attacker. Finally, the authors did not specify a mechanism for V2V communications, thus limiting the utility of the protocol.

1) System Setup	The TA defines secret $\mathbf{k}^{\mathbf{s}}_{TA}$ and public parameters $\mathbf{k}^{\mathbf{p}}_{TA}, \mathbf{H}$. Then, for each RSU_i, TA defines secret r_i, $\mathbf{k}^{\mathbf{s}}_{RSU_i}$ and public parameters $\mathbf{k}^{\mathbf{p}}_{RSU_i}$, ID_{RSU_i} and finally $HID_i = \mathbf{H}(ID_{RSU_i} \| r_i)$.
2) User Registration	· u computes $A = \mathbf{H}(ID_u \| PW_u)$ · $u \Rightarrow TA : ID_u, A$ · TA computes $B_i = \mathbf{H}(ID_u \| HID_i)$ and $C_i = \mathbf{H}(B_i \| A)$ $\forall RSU_i$ · $TA \Rightarrow u : SC(A, B_i, C_i, ID_{RSU_i}) \forall RSU_i$
3) User Login	· $u \Rightarrow SC : ID_u^*, PW_u^*$ · SC checks if $A = \mathbf{H}(ID_u^* \| PW_u^*)$
4) V2I Authentication	· u computes $D = \mathbf{H}(ID_u \| ID_{RSU_i} \| r_u \| A \| ts)$ and $G = \{\mathbf{H}(ID_u \| r_u \| A)\}_{\mathbf{k}^{\mathbf{p}}_{RSU_i}}$ · $u \rightarrow RSU_i : D, G, ts$ · RSU_i creates $\mathbf{k^{sym}}$ and shares it with u Note that $\mathbf{k^{sym}}$ is different for each u
6) V2V Authentication	· $u \rightarrow RSU_i : \{ID_u \| m\}_{\mathbf{k^{sym}}}$ · RSU_i computes signature $sig = (ID_{RSU_i} \| ts \| m)^{\mathbf{k}^{\mathbf{s}}_{RSU_i} \bmod g}$ · $RSU_i \rightarrow * : (ID_{RSU_i}, sig, m)$
7) Login Update	· u logs in the SC · $u \Rightarrow SC : PW_u^{new}$ · SC updates $A^{new} = \mathbf{H}(ID_u \| PW_u^{new})$ and $C^{new} = \mathbf{H}(B_i \| A^{new})$ Note that the TA is not involved

Algorithm 11: Amin et al. [4] (2020)

Also Amin et al. [4] (Algorithm 11) outlined critical security issues in [51] and then proposed a new and improved IDM protocol for CCAM. The authors provided a formal security analysis using the Scyther[18] formal verification tool. Particularly, the authors made all messages flow through RSUs; this design avoids direct V2V communication and ensures the authenticity of all messages. However, this approach deteriorates performance (e.g., by increasing latency of the user-plane traffic) and does not provide confidentiality and privacy with respect to the RSU. Moreover, as vehicles only send to the RSU the message along with their identity, there is no protection against tampering or replay attacks in (RSU-relayed) V2V communications. The protocol assumes that each SC stores the identifiers and public keys of all RSUs. Unfortunately, we note that storing such a large amount of data in a single SC may not be feasible. Furthermore, handover and revocation of RSUs and SCs were not discussed.

1) System Setup	The TA defines secret STA, S'_{TA}, S''_{TA} and public parameters $\mathbf{H}(\cdot), g, g', G_q, G_{q'}, G_{q''}, F_n, E(F_n)$.
2) User Registration	· $u \Rightarrow TA : ID_u, PW_u$ · TA creates $\mathbf{Cert}_u(TA)$ by hashing S'_{TA} with ID_u and multiplying it by P and computes $m = \mathbf{H}(PW_u), n = \mathbf{H}(m \Vert S'_{TA} \Vert ID_u)$, $y = (m \oplus n), c = \mathbf{H}(y)$ · $TA \Rightarrow u : SC(c, m, n, \mathbf{Cert}_u(TA))$
3) User Login	· $u \Rightarrow SC : PW_u$
4) V2I Authentication	Tri-party key dissemination protocol for vehicle to
5) RSU Handover	infrastructure communication (TV2I) [35]
6) V2V Authentication	Two vehicles can derive a common $\mathbf{k^{sym}}$ by verifying the respective certificates
7) Login Update	· $u \Rightarrow TA : PW_u^{new}$ · $TA \Rightarrow u : m^{new}, n^{new}, y^{new}$
8) Revocation	The TA adds $\mathbf{Cert}_u(TA)$ to the CRL

Algorithm 12: Palaniswamy et al. [35] (2020)

Following the same trend, also in [35] (Algorithm 12) the authors discussed the vulnerabilities present in [51] and then designed a new protocol as a solution. The authors added to the network model other entities called "Trace Managers", i.e., law authorities distributed alongside the road to trace and react to malicious activities. In fact, the authors discussed the possibility for vehicles to report and signal misbehaving users or RSUs to the nearest Trace Manager. Furthermore, the authors focused on continuous handover of vehicles authentication among RSUs. As usual, the SC contains authentication credentials. After registration, vehicles receive multiple temporary certificates to provide privacy and anonymity. However, the authors did not discuss the possibility of Sybil attacks. A group key is used for V2I communications within the coverage of each RSU, while vehicles employ temporary certificates to derive a common symmetric key to enable direct V2V communications.

V. Discussion

In this section, we derive further insights on SC-based IDM protocols for CCAM. First, in Section V-A we discuss trends and shortcomings observed in the literature by considering the surveyed protocols in temporal order. Then, in Section V-B we propose some guidelines and useful considerations for the design of new protocols.

[18]https://people.cispa.io/cas.cremers/scyther/

A. Trends and Shortcomings in Research

As presented in Table III, many SC-based IDM protocols surveyed in Section IV-C use the same base cryptographic primitives, i.e., RSA and ECC for asymmetric encryption and AES for symmetric encryption. PKC supported by a PKI is the most common approach to secure CCAM services [39, 6, 18]. After authentication, OBUs receives from the RSUs or the TA temporary keys (or other secrets) used to encrypt (for confidentiality) and sign (for integrity) V2V and V2I communications. Temporary keys can also be derived from material obtained during the user registration phase or contained in the SC to avoid (resource expensive) key exchange protocols, especially in CCAM services characterized by strict latency constraints.

Another trend we observe is that recent protocols cover more steps (e.g., V2V authentication) than those developed early; this implies an increased awareness of the importance of each one of the steps identified in this work. However, the login update, revocation and RSU handover steps are seldom specified (only in around 1 protocol out of 3). This is a noticeable shortcoming that needs to be addressed to propose usable IDM protocols. Credentials update and misbehaving or malicious users revocation are not negotiable, and RSU handover is a necessity for CCAM services, especially those involving vehicles moving at high speed (e.g., on highways).

Then, many papers consider related work as a starting point. In particular, the authors in [11, 4, 35] have all first outlined the vulnerabilities in [51] and then each has proposed an enhanced version of the flawed protocol that supposedly solves the identified vulnerabilities. Besides, the authors in [4, 35] provided a tool-supported formal analysis of their protocol, denoting that strong security is becoming increasingly important.

We note that, in some protocols, SCs are assumed to be embedded in vehicles [36, 27, 43, 11]. However, more recent protocols tend to rely on trusted components storing credentials for vehicles while users are supposed to obtain SCs from other TAs [46, 42, 6, 51, 26, 29, 4, 35], such as those providing digital identity infrastructures for citizens. Indeed, here the challenge is to combine the vehicle's and the driver's identities to derive credentials that can be used to access CCAM services while guaranteeing the necessary security goals. We elaborate more on this in Section V-B.

As a final remark, we note that there is more research in authenticating messages rather than vehicles [51]. However, sometimes the two problems are reduced to one, i.e., when there is no V2V direct communication but only V2I communications and RSUs are responsible for the authenticity of both vehicles and messages [53, 17]. While solving the problem of direct V2V authentication, this approach always requires the presence and availability of (at least one) RSUs.

B. Guidelines for New Protocols

After comparing several SC-based IDM protocols by highlighting similarities and differences and identifying relevant trends and shortcomings, we now present our recommendations for future research. Below, we propose guidelines and useful considerations for the design of new SC-based IDM protocols for CCAM, grouping them by topic.

1) Protocol: SC-based IDM protocols should be complete, secure, efficient and compliant with the most recent standards:

- *coverage of steps*: to be complete and comparable with recent work, new protocols should cover all the 8 steps in Section IV-B, providing (confidential) V2V direct and V2V (or RSU-aided) broadcast communication. In particular, even though not always addressed, we highlight that the revocation of malicious users and compromised RSUs is fundamental to block internal and CK attackers, so to prevent them from further endangering the system. Also, misbehavior detection (e.g., based on trust frameworks [2, 16]) should be tightly coupled with IDM. Finally, as said in Section I-B, the design of these steps should take advantage of the diversity of functional and security requirements, e.g., by offloading expensive computation to non time-sensitive steps (e.g., user registration), so to verify digital identities with a high level of assurance and derive credentials for fast authentication at run-time;
- *security verification*: besides guaranteeing basic security properties (e.g., confidentiality, integrity), new IDM protocols should discuss defences against Sybil attacks and both temporal and spatial replay attacks. Moreover, the security of IDM protocols should be verified, where possible, with tool-supported analysis (e.g., with Tamarin or Scyther) instead of more error-prone manual analysis;
- *simulations*: the performance of new protocols should be compared with previous work. To abstract from concrete execution environments, the computational complexity of a protocol should be defined by decomposing each step into basic cryptographic operations (e.g., those reported in Table II). To obtain accurate experimental results, new protocols should be tested with appropriate system-level simulation tools [30] such as SUMO[19] (for vehicles mobility) and ns-3[20] (for radio channel propagation aspects);
- *compliance*: standardisation bodies in both the EU and the US have published standards which should be considered when designing IDM protocols for CCAM services. For instance, the ETSI specifies security services for the establishment and maintenance of identities and cryptographic material in ITS communications [44], where the legal and technical requirements for the management of public key certificates for vehicular applications across European Countries are defined by the framework of the EU C-ITS Certificate Management System (CCMS).[21] Also the United States Department of Transportation (USDOT) has proposed a PKI-based message security solution for V2V and V2I communications, called Security Credentials Management System (SCMS).[22] We note that these standards may be the key to provide a common interface for the harmonisation of different technologies proposed by car manufacturers.

2) SCs and Cryptography: : there are several options for using and interfacing with SCs in CCAM. Moreover, the use of cryptography should take into account the requirements of different scenarios and the long life-cycle of vehicles:

- *SCs for drivers and vehicles*: several surveyed protocols assume vehicles to be equipped with a SC reader [46, 42, 6, 51, 26, 29, 4, 35]. As this assumption may not hold for all vehicles, new approaches should also consider different technologies to interface with the SC. For instance, the driver's smartphone could interact with the SC via Near-Field Communication (NFC) and then enable secure vehicular communication leveraging a Bluetooth connection with the car. Another possible approach could be to use the USIMs contained in the drivers' smartphone as SCs. While enabling interesting synergies with the mobile network technology (e.g., 5G), especially if this is chosen as the preferred way of conveying vehicular information, the second approach could suffer from vulnerabilities imported from the mobile context. As an example, the Simjacker vulnerability allows attackers to send to a smartphone a maliciously crafted Over-The-Air (OTA) SMS capable of injecting malware code into the USIMs.[23] Therefore, different assumptions and security risks should be considered, e.g., as investigated in [48]. Finally, as in [42], new protocols could use eID cards or other digital IDM solutions to uniquely identify drivers. A clear advantage of using eID cards is relying on a (secure) infrastructure already in place. Moreover, as usually the same body (i.e., the government) issues both eID cards and driving licenses, the user registration step would be already performed. Also, this approach could allow to easily integrate multiple TAs through solutions similar to eIDAS[24]. Besides, the use of eID cards would enable further use cases, like blockchain-based charge of electric vehicles [23] and instant rental of shared cars with automatic billing. Still, we remark that the drivers' identity should be tightly coupled with the vehicle to provide accountability, and this is one of the challenges that future protocols in this domain need to address;
- *tuning cryptographic primitives*: signature verification [6] and bilinear pairings [26] are computationally more expensive than symmetric encryption and hash functions. Therefore, their use should be limited and, when necessary, more performant (albeit secure) algorithms should be preferred. For instance, The ETSI proposes a list of cryptographic suites used for generation and validation of digital signatures [45]. However, there is hardly a one-size-fits-all cryptographic algorithm, as the choice heavily depends on the protocol itself [15]. For instance, while ECC is faster for signature generation, RSA is better for signature verification. Depending on the expected number of these operations, one algorithm may be better than the other. For a thorough discussion on cryptographic algorithms for ITS, we refer the interested reader to [15];
- *post-quantum threat*: vehicles stay on the road for many years. As such, besides OTA updates, it is important to consider the use of cryptographic primitives guaranteeing

[19]https://www.eclipse.org/sumo/

[20]https://www.nsnam.org/

[21]https://ec.europa.eu/transport/sites/default/files/c-its_certificate_policy-v1.1.pdf

[22]https://www.its.dot.gov/resources/scms.htm

[23]https://srlabs.de/bites/sim_attacks_demystified/

[24]https://ec.europa.eu/digital-single-market/en/discover-eidas

long-term security since the early design of the protocol. For instance, while asymmetric algorithms are threatened by quantum cryptography, symmetric algorithms (given the right key size) can still guarantee a proper level of security. Also, protocols should be capable to adjust to new cryptographic primitives in case the currently used primitives become deprecated (e.g., see SHA-1[25]).

3) TAs: the development of real-time CCAM services calls for integration among TAs and proper trust management:

- *multiple TAs*: given the presence of many independent car manufacturers (i.e., heterogeneous market) and international mobility, new protocols should expect more than one TA and address cross-border scenarios. For instance, the protocol proposed in [4] expects each SC to store the identifiers and public keys of all RSUs; intuitively, this kind of approaches cannot scale to accommodate scenarios with multiple TA. Instead, new protocols should consider how different TAs may interact regarding the authentication of a vehicle in a foreign country. Only two of the surveyed protocols acknowledged the possible presence of multiple TAs [6, 46];
- *trust management*: all protocols assume that the TA cannot be compromised. Differently, except for specific scenarios, RSUs should not be assumed to have the same level of security. Also, the communication channel between TA and RSUs should not always be assumed to be secure, as RSUs may be deployed in unattended environments [26]. Therefore, new protocols should consider the *mutual* authentication of vehicles and RSUs. As highlighted in [38], another important aspect in trust management is PKI migration. Indeed, the update of cryptographic certificates prevents brute-force attempts and mitigates key leakages, attacks whose probability of success increases over time. However, while OBUs' and RSUs' certificates can be easily renewed, the migration of the root certificate (i.e., the TA's certificate) is more complicated, as the TA is the trust anchor of the whole PKI. Therefore, appropriate mechanisms for PKI migration which guarantees the availability of CCAM services should be devised and proposed in IDM protocols.

There are other challenges to address besides the major ones considered above. For instance, while enhancing performance, batch verification does not seem essential, as it is supported by only two of the surveyed protocols, i.e., [26] and [29]. Perhaps, more comprehensive experimental analyses (even by simulation) are needed to measure the efficiency improvement due to batch verification. Finally, to enable V2V communication under all conditions, IDM protocols should not always rely on RSUs as mediators among vehicles, as instead proposed in [17, 26, 29]. When no RSUs are available, vehicles should anyway be able to securely communicate (e.g., as in [35]).

VI. Conclusion

In this paper, we presented a systematic literature review on SC-based IDM protocols for V2I and V2V communication in CCAM. First, we characterized CCAM services by discussing assumptions and requirements affecting the design of SC-based IDM protocols. Then, we extrapolated a unified high-level view of the 8 common steps composing a SC-based IDM protocol in CCAM. Finally, we thoroughly reviewed 12 SC-based IDM protocols, analysed trends and shortcomings in research and formulated concrete guidelines for the design of new protocols. In particular, the most interesting points are considering standardisation bodies (e.g., ETSI) as enablers to foster harmonisation and common interfaces and the use of different SCs (e.g., eID cards, USIMs) to enable synergies with technologies like 5G and blockchain [7], with the final goal to enable further use cases and make CCAM even smarter.

[25]https://csrc.nist.gov/news/2017/research-results-on-sha-1-collisions

Acknowledgment

This work has been performed in the framework of the European Union Horizon 2020 project 5G-CARMEN co-funded by the EU under grant agreement No. 825012. The views expressed are those of the authors and do not necessarily represent the project. The Commission is not liable for any use that may be made of any of the information contained therein.

References

[1] Ryma Abassi. VANET security and forensics: Challenges and opportunities. *Wiley Interdisciplinary Reviews: Forensic Science*, 1(2):e1324, September 2019.

[2] Mohammad Aladwan, Feras Awaysheh, Mamoun Alazab, Sadi Alawadi, Tomas Pena, and Jose Cabaleiro. TrustE-VC: Trustworthy evaluation framework for industrial connected vehicles in the cloud. *IEEE Transactions on Industrial Informatics*, pages 6203–6213, January 2020.

[3] Ikram Ali, Alzubair Hassan, and Fagen Li. Authentication and privacy schemes for vehicular ad hoc networks (VANETs): A survey. *Vehicular Communications*, 16:45–61, April 2019.

[4] Ruhul Amin, Paras Lohani, McLican Ekka, Sunay Chourasia, and Satyanarayana Vollala. An enhanced anonymity resilience security protocol for vehicular ad-hoc network with scyther simulation. *Computers & Electrical Engineering*, 82:106554, March 2020.

[5] Sima Arasteh, Maede Ashouri-Talouki, and Seyed Farhad Aghili. Lightweight and secure authentication protocol for the internet of things in vehicular systems. In *2017 14th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*, pages 1–7. IEEE, September 2017.

[6] Maria Azees, Pandi Vijayakumar, and Lazarus Jegatha Deboarh. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 18(9):2467–2476, February 2017.

[7] Palak Bagga, Ashok Kumar Das, Mohammad Wazid, Joel J. P. C. Rodrigues, and Youngho Park. Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *IEEE Access*, 8:54314–54344, March 2020.

[8] Ran Canetti and Hugo Krawczyk. Universally composable notions of key exchange and secure channels. In Lars R. Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332, pages 337–351. Springer Berlin Heidelberg, May 2002.

[9] Marco Centenaro, Stefano Berlato, Roberto Carbone, Gianfranco Burzio, Giuseppe Faranda Cordella, Silvio Ranise, and Roberto Riggio. Security considerations on 5g-enabled back-situation awareness for CCAM. In *2020 IEEE 3rd 5G World Forum (5GWF)*, pages 245–250. IEEE.

[10] Preeti Chandrakar, Ayush Jain, Sandeep Balivada, and Rifaqat Ali. A secure authentication protocol for vehicular ad-hoc networks. In *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, pages 1–7. IEEE, February 2019.

[11] Chien-Ming Chen, Bin Xiang, Yining Liu, and King-Hang Wang. A secure authentication protocol for internet of vehicles. *IEEE Access*, 7:12047–12057, January 2019.

[12] Juan Contreras-Castillo, Sherali Zeadally, and Juan Antonio Guerrero-Ibanez. Internet of vehicles: Architecture, protocols, and security. *IEEE Internet of Things Journal*, 5(5):3701–3709, October 2018.

[13] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, March 1983.

[14] ISO/TC 22/SC 32 Electrical, electronic components, and general system aspects Committee. Road vehicles — cybersecurity engineering. Standard, SAE International - Vehicle Cybersecurity Systems Engineering Committee, February 2020.

[15] Abdessamad Fazzat, Rida Khatoun, Houda Labiod, and Renaud Dubois. A comparative performance study of cryptographic algorithms for connected vehicles. In *2020 4th Cyber Security in Networking Conference (CSNet)*. IEEE.

[16] Jingjing Guo, Xinghua Li, Zhiquan Liu, Jianfeng Ma, Chao Yang, Junwei Zhang, and Dapeng Wu. TROVE: A context awareness trust model for VANETs using reinforcement learning. *IEEE Internet of Things Journal*, pages 6647–6662, February 2020.

[17] Maanak Gupta, James Benson, Farhan Patwa, and Ravi Sandhu. Secure v2v and v2i communication in intelligent transportation using cloudlets. *arXiv:2001.04041 [cs]*, January 2020.

[18] Monowar Hasan, Sibin Mohan, Takayuki Shimizu, and Hongsheng Lu. Securing vehicle-to-everything (v2x) communication platforms. *arXiv:2003.2003.07191 [cs]*, March 2020.

[19] European Telecommunications Standards Institute. ETSI TS 102 940; intelligent transport systems (ITS); security; ITS communications security architecture and security management.

[20] X.-D Jia, Y.-F Chang, C.-C Chang, and L.-M Wang. A critique of a lightweight identity authentication protocol for vehicular networks. *Journal of Information Hiding and Multimedia Signal Processing*, 6:183–188, 03 2015.

[21] Cards Joint technical committee (JTC) 1 / Sub-Committee (SC) 17 and personal identification. Iso/iec 7816. Standard, ISO - International Organization for Standardization.

[22] Joshua Joy and Mario Gerla. Internet of vehicles and autonomous connected car - privacy and security issues. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–9. IEEE, August 2017.

[23] MyeongHyun Kim, KiSung Park, SungJin Yu, JoonYoung Lee, YoungHo Park, Sang-Woo Lee, and BoHeung Chung. A secure charging system for electric vehicles based on blockchain. *Sensors*, 19(13), July 2019.

[24] Vinod Kumar, Musheer Ahmad, Adesh Kumari, Saru Kumari, and M. K. Khan. SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing: SEBAP. *International Journal of Communication Systems*, page e4103, August 2019.

[25] Chun-Ta Li, Chi-Yao Weng, Chin-Ling Chen, and Cheng-Chi Lee. A secure authentication protocol for wireless sensor network in smart vehicular system. In Andrzej M.J. Skulimowski, Zhengguo Sheng, Sondès Khemiri-Kallel, Christophe Cérin, and Ching-Hsien Hsu, editors, *Internet of Vehicles. Technologies and Services Towards Smart City*, volume 11253, pages 278–288. Springer International Publishing, November 2018. Series Title: Lecture Notes in Computer Science.

[26] Congcong Li, Xi Zhang, Haiping Wang, and Dongfeng Li. An enhanced secure identity-based certificateless public key authentication scheme for vehicular sensor networks. *Sensors*, 18(2):194, January 2018.

[27] Jung-Shian Li and Kun-Hsuan Liu. A lightweight identity authentication protocol for vehicular networks. *Telecommunication Systems*, 53(4):425–438, August 2013.

[28] Xiaonan Liu, Zhiyi Fang, and Lijun Shi. Securing vehicular ad hoc networks. In *2007 2nd International Conference on Pervasive Computing and Applications*, pages 424–429. IEEE, June 2007.

[29] Xin Liu and Ruisheng Zhang. A robust authentication scheme with continuously updated information for vehicular sensor networks. *IEEE Access*, 6:70473–70486, November 2018.

[30] Zhaojun Lu, Gang Qu, and Zhenglin Liu. A survey on recent advances in vehicular network security, trust, and privacy. *IEEE Transactions on Intelligent Transportation Systems*, 20(2):760–776, February 2019.

[31] D. Manivannan, Shafika Showkat Moni, and Sherali Zeadally. Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs). *Vehicular Communications*, page 100247, March 2020.

[32] Sunilkumar S. Manvi and Shrikant Tangade. A survey on authentication schemes in vanets for secured communication. *Vehicular Communications*, 9:19–30, July 2017.

[33] Prerna Mohit, Ruhul Amin, and G.P. Biswas. Design of authentication protocol for wireless sensor network-based smart vehicular system. *Vehicular Communications*,

9:64–71, July 2017.

[34] Arash Olia, Saiedeh Razavi, Baher Abdulhai, and Hossam Abdelgawad. Traffic capacity implications of automated vehicles mixed with regular vehicles. *Journal of Intelligent Transportation Systems*, 22, 11 2017.

[35] Basker Palaniswamy, Seyit Camtepe, Ernest Foo, Leonie Simpson, Mir Ali Rezazadeh Baee, and Josef Pieprzyk. Continuous authentication for vanet. *Vehicular Communications*, 25:100255, October 2020.

[36] Vamsi Paruchuri and Arjan Durresi. PAAVE: Protocol for anonymous authentication in vehicular networks using smart cards. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–5. IEEE, December 2010.

[37] Jonathan Petit, Florian Schaub, Michael Feiri, and Frank Kargl. Pseudonym schemes in vehicular networks: A survey. *IEEE Communications Surveys & Tutorials*, 17(1):228–255, August 2015.

[38] Jan-Felix Posielek, Norbert Bißmeyer, and Annika Strobel. A security migration concept for vehicle-to-x communication to allow long-term PKI operation. In Alain Pirovano, Marion Berbineau, Alexey Vinel, Christophe Guerber, Damien Roque, Jaizki Mendizabal, Hervé Bonneville, Hasnaâ Aniss, and Bertrand Ducourthial, editors, *Communication Technologies for Vehicles*, volume 10222, pages 107–118. Springer International Publishing. Series Title: Lecture Notes in Computer Science.

[39] Fengzhong Qu, Zhihui Wu, Feiyue Wang, and Woong Cho. A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems*, 16(6):2985–2996, December 2015.

[40] Mohammad Javad Sadri and Maryam Rajabzadeh Asaar. A lightweight anonymous two-factor authentication protocol for wireless sensor networks in internet of vehicles. *International Journal of Communication Systems*, 33(14):e4511, September 2020.

[41] Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang, Li Zhang, Junfeng Xu, and Yongping Xiong. Security and privacy in the internet of vehicles. In *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)*, pages 116–121. IEEE, October 2015.

[42] J. Sánchez-García, J.M. García-Campos, D.G. Reina, S.L. Toral, and F. Barrero. On-siteDriverID: A secure authentication scheme based on spanish eID cards for vehicular ad hoc networks. *Future Generation Computer Systems*, 64:50–60, November 2016.

[43] Wei-Liang Tai, Ya-Fen Chang, and Yung-Chi Chen. A fast-handover-supported authentication protocol for vehicular ad hoc networks. *Journal of Information Hiding and Multimedia Signal Processing*, 7:960–969, September 2016.

[44] ETSI TS. ETSI TS 102 941; intelligent transport systems (ITS); security; trust and privacy management.

[45] ETSI TS. ETSI TS 119 312; electronic signatures and infrastructures (esi); cryptographic suites.

[46] Pandi Vijayakumar, Maria Azees, Arputharaj Kannan, and Lazarus Jegatha Deborah. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems*, 17(4):1015–1028, November 2015.

[47] Mohammad Wazid, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, and Joel J.P.C. Rodrigues. Authentication in cloud-driven IoT-based big data environment: Survey and outlook. *Journal of Systems Architecture*, 97:185–196, August 2019.

[48] Haohuang Wen Wen, Qi Alfred Chen, and Zhiqiang Lin. Plug-n-pwned: Comprehensive vulnerability analysis of OBD-II dongles as a new over-the-air attack surface in automotive IoT. In *2020 29th usenix security symposium*, August 2020.

[49] Bidi Ying, Dimitrios Makrakis, and Hussein T. Mouftah. Privacy preserving broadcast message authentication protocol for VANETs. *Journal of Network and Computer Applications*, 36(5):1352–1364, September 2013.

[50] Bidi Ying and Amiya Nayak. Efficient authentication protocol for secure vehicular communications. In *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*, pages 1–5. IEEE, May 2014.

[51] Bidi Ying and Amiya Nayak. Anonymous and lightweight authentication for secure vehicular networks. *IEEE Transactions on Vehicular Technology*, 66(12):10626–10636, December 2017.

[52] SungJin Yu, JoonYoung Lee, KyungKeun Lee, KiSung Park, and YoungHo Park. Secure authentication protocol for wireless sensor networks in vehicular communications. *Sensors*, 18(10):3191, September 2018.

[53] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, and Xuemin Shen. An efficient message authentication scheme for vehicular communications. *Vehicular Technology, IEEE Transactions on*, 57:3357 – 3368, December 2008.

[54] Zhiping Zhou, Huigen Zhang, and Ziwen Sun. An improved privacy-aware handoff authentication protocol for VANETs. *Wireless Personal Communications*, 97(3):3601–3618, December 2017.

Stefano Berlato (sberlatofbk.eu) is a PhD Student of the University of Genoa at the Fondazione Bruno Kessler, Trento. His current research interests include the analysis of security and access control in cloud-edge solutions.

Marco Centenaro (marco.centenaroathonet.com) is a System Engineer at Athonet S.r.l. His research interests include the design of 5G-and-beyond mobile network and the integration of vertical industries into mobile systems.

Silvio Ranise (ranisefbk.eu) is full professor of Computer Science at the University of Trento and director of the Center for cybersecurity of the Fondazione Bruno Kessler, Trento. Before, he was a researcher at INRIA (French National Institute of Computer Science and Automation), visiting professor at the University of Milano and researcher at the University of Verona. His main research interests are digital identity management, risk assessment and legal compliance and applied cryptography.