Attribute-Based Credentials in High-Density Platooning

Christian Zimmermann
Robert Bosch GmbH
Renningen, Germany
christian.zimmermann3@bosch.com

Markus Sontwoski
Chair for Privacy & Security, TU Dresden
Dresden, Germany
markus.sontowski@tu-dresden.de

Stefan Köpsell
Chair for Privacy & Security, TU Dresden
Dresden, Germany
stefan.koepsell@tu-dresden.de

ABSTRACT

Intelligent transport systems (ITS) rely on V2X communication for allowing coordination and cooperation of traffic participants and increasing traffic efficiency and safety. Communication between traffic participants needs to be secured, especially with respect to authenticity and integrity. Further, a high level of privacy-preservation needs to be ensured. The current European ITS system relies on the use of pseudonym certificates to achieve trust and security while providing a high level of privacy by ensuring unlinkability of messages in the long term. This paper sets out to investigate whether privacy-preserving attribute-based credentials (ABCs) constitute a viable alternative or complement to the current approach. In particular, this paper focuses on the use case of high-density platooning and investigates the applicability of ABCs in that context.

CCS CONCEPTS

• **Security and privacy** → **Pseudonymity, anonymity and untraceability**;

KEYWORDS

Attribute-Based Credentials, Privacy, Security, V2X, Platooning

ACM Reference Format:
Christian Zimmermann, Markus Sontwoski, and Stefan Köpsell. 2019. Attribute-Based Credentials in High-Density Platooning. In *CSCS19*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Currently, road traffic is plagued by inefficiencies in traffic flow and a death toll that, while generally decreasing, still adds up to several thousand every year. For instance, in Germany, almost 3200 people lost their lives in traffic accidents in 2017[1]. To address these problems, the European Union has established a strategy to foster cooperative intelligent transportation systems (C-ITS) [14]. The strategy aims at increasing traffic efficiency and safety through communication between traffic participants. This includes the communication between vehicles (V2V), vehicles and infrastructure such as traffic light signals (V2I) and vehicles and back end, cloud or edge cloud systems (V2N). The afore-listed communication modes are often subsumed under the general term "vehicle-to-everything communication" (V2X).

A broad variety of use cases for V2X has been established in the European C-ITS strategy [14] and, currently, so-called Day-1 use cases are being implemented and deployed. Those use cases encompass hazardous location information and in-vehicle signage but no communication directly effecting actuation. For example, in the *road works warning* use case, V2X messages are used to notify drivers of road works lying ahead, possibly unrecognizably located behind curves of the road. Besides these solely warning-oriented use cases, more challenging use cases and applications are being researched. Among those are collaborative maneuvering, traffic light coordination or (high-density) platooning. In platooning [2], several vehicles drive in a single file in close succession with the goal to save energy by exploiting slipstream effects. While platooning often refers to the platooning of trucks, it is not restricted to commercial vehicles but could also be performed by passenger cars.

Obviously, connected vehicles and C-ITS face challenges regarding security and privacy. In order to cooperate with each other or to warn each other, vehicles are envisaged to broadcast a multitude of information with high frequency. In Europe, this is intended to be achieved by the constant broadcasting of so-called Cooperative Awareness Messages (CAMs), which contain information on speed, position, vehicle type, heading, last positions and many more properties regarding a vehicle's status [16]. CAMs are envisioned to be sent with a frequency of 10Hz and, clearly, some of the transmitted information constitutes personal data (cf. [1]). Consequently, data protection regulation applies and measures to protect vehicle owners' and drivers' privacy need to be in place.

Further, C-ITS need to be secured and a trust architecture needs to be in place in order to protect message integrity, authenticity and, where applicable, confidentiality. This also includes the necessity of authentication and authorization of participating vehicles. In order to ensure the fulfillment

CSCS 19, October 8, 2019, Kaiserslautern

ACM ISBN 978-1-4503-9999-9/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

[1] https://www.dvr.de/unfallstatistik/de/jahre/

of these security goals while at the same time protecting participants' privacy, a security and trust architecture featuring a public key infrastructure (PKI) has been specified [13]. However, while the architecture facilitates trust in the system's participants and does provide a high level of privacy protection, it is also highly complex and exhibits further shortcomings (see Section 2.1).

This paper sets out to investigate alternative approaches towards privacy-friendly authentication for platooning. In particular, we focus on privacy-preserving attribute-based credentials (ABCs)[3] and investigate their suitability to be utilized in security and privacy concepts for high-density platooning. In the following section, we provide basic information on security and privacy in C-ITS and high-density platooning. Section 3 provides a brief introduction to privacy-preserving attribute-based credentials. In Section 4, we investigate the state of the art regarding privacy-preserving attribute-based credentials in the V2X domain. We propose an application of privacy-preserving attribute-based credentials for securing platoon booking in a privacy-friendly manner in Section 5. Finally, we conclude the paper in Section 6.

2 SECURITY AND PRIVACY IN PLATOONING

In the following, we first provide a basic overview on privacy and security in C-ITS. Subsequently, we introduce high-density platooning and discuss its security and privacy requirements.

2.1 C-ITS

Cooperative intelligent transport systems (C-ITS) are envisages to increase traffic efficiency and safety [14]. To achieve these goals, messages exchanged within the system need to be protected against manipulation. Further, it must be ensured that only authorized participants are able to send messages and only properly authorized participants are able to send special messages, e.g., messages indicating that the sender is an emergency vehicle. As described above, a PKI-approach is utilized in the European Strategy on C-ITS to facilitate integrity and authenticity, as well as privacy protection. Slightly different, but largely harmonized, PKI architectures are utilized in the US and the EU, with the European version specified by ETSI in [13] being depicted in Figure 1.

As can be seen in the figure, the ETSI ITS PKI architecture comprises three types of authorities. The Root CA acts as trust anchor for the whole PKI and issues certificates to Enrollment Authority (EA) and Authorization Authority (AA). Enrolment Authorities are responsible for providing authorized ITS stations with credentials they can use to demonstrate that they are authorized to send specific types of V2X messages. To that end, ITS stations are issued Enrollment Credentials (ECs). Using their EC, ITS stations can obtain Authorization Tickets (ATs) from Authorization Authorities. To obtain ATs, the ITS station does not disclose the EC to the AA. Rather, it transmits its EC in encrypted form to the AA, which lets the EA verify whether the ITS station is authorized to obtain the requested ATs.

Authorization Tickets are the certificates an ITS station uses to sign the V2X messages it sends[4] and do not contain static identifiers of the ITS station. Hence, an ITS station can sign messages while at the same time not revealing its long-term identity (EC) but only a temporary pseudonym (contained in the AT).

This way the separation of EA and AA aims at increasing ITS stations' privacy by enabling them to trustworthy sign messages without the need to reveal their identity. Receiving ITS stations can still trust in the authenticity and legitimacy of received messages, as ATs are only issued to ITS stations that have been authorized to send the respective messages by an EA, which in turn has been authorized to enroll ITS stations by a commonly trusted Root CA.

In order to reduce the risk of long-term traceability, i.e., linkability of messages sent over time, ITS stations need to regularly change their ATs. For the European C-ITS, the strategy for changing ATs is defined in the C-ITS Platform's Security Policy [15]. Obviously, to actually preserve privacy, a change of ATs needs to be conducted simultaneously with a change of all other identifiers used by a vehicle in V2X communication, e.g., MAC address, IP address and other identifiers. However, while this is doable in principle, it is rather hard to realize in practice and the pseudonym change approach cannot provide unlinkability under all circumstances [28].

2.2 High-Density Platooning

High-density platooning is the linking of vehicles such that they drive in very close succession in order to benefit from fuel savings by exploiting slipstream effects. Figure 2 provides an overview on the platooning life-cycle.

For platoon candidates (PC) to find a suitable platoon, a platoon booking process, controlling the registration of PCs, can be integrated into the traditional route planning. Different booking approaches exist, e.g. ad-hoc, static and dynamic booking [2]. However, Bhoopalam et al. [2] note that ad-hoc platooning will play a smaller role due to its limitation regarding finding optimal platoons. Hence, in this paper we will focus on static booking, meaning trips in platoons are planned before the platoon starts. After a PC is assigned to a fitting platoon and holds all necessary information, it can join the platoon. In the "Join" phase of the platoon life-cycle the PC negotiates with the platoon management system (which can be located, e.g., in the lead vehicle or in the cloud) the parameters and cryptography keys to be used by the platoon members (PLMs) for intra-platoon communication to protect against external attackers. After successful joining the PC becomes a PLM as well. During the "Maintain Platoon"

[3] As this paper only investigates *privacy-preserving* attribute-based credentials we will use the shorter term attribute-based credentials (or the abbreviation: ABCs) in order to enhance readability.

[4] In order to increase readability, we use the phrase "to sign a message with a certificate" instead of the more correct one: "to sign a message with the private key which belongs to the public key certified with the certificate".

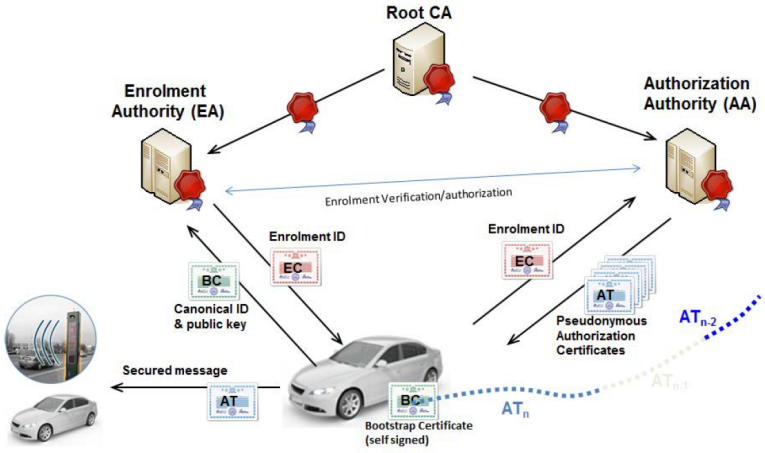

Figure 1: European ITS PKI architecture (taken from [13])[2]

phase, the PLMs drive as a platoon until the platoon dissolves. Individual PLMs can also leave the platoon without the platoon being dissolved, provided more than one PLM remains in the platoon.

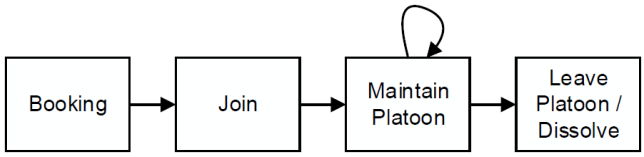

Figure 2: Platooning life-cycle

In order to achieve a stable platoon and to be able to safely perform driving with very short distances, PLMs need to synchronize their driving behavior and, hence, constantly communicate with each other. Obviously, this communication needs to be secured. However, the security and privacy requirements for platoon communication are not necessarily identical with those of general C-ITS use cases, particularly not with those of Day-1 use cases, which do not include safety-critical communication. In the following, security and privacy requirements for platoon communication are briefly introduced.

Integrity of platoon communication is as relevant as integrity of general V2X communication in order to prevent the manipulation of messages. It is particularly important as forged messages (e.g. regarding a new target speed or demanding an emergency brake action) could very easily lead to severe accidents in case of PLMs driving in very close succession.

Authenticity and authorization are also equally relevant in platooning as in other C-ITS use cases. In particular, potential platoon members need to be able to demonstrate that they are suited to drive within a specific platoon, e.g., with respect to their brake path, weight, length and other properties. Further, it might be necessary to demonstrate the authorization to take on specific roles within a given platoon, for example, as the lead vehicle. Moreover, authenticity will also be necessary in case of business models where platoon members reimburse each other, for instance, to compensate for fuel saving effects. Authenticity and identifiability will also be relevant in case of accidents.

In contrast to Day-1 use cases where messages are mostly broadcasted to be read by everyone, confidentiality is required in platooning. For example, forwarding companies need to protect information relating to fleet management, route optimization or pricing schemes. Highly efficient confidentiality protection mechanisms are required as delays in intra-platoon communication will lead to an increase in the minimum distance required between vehicles for safety reasons and, hence, a decrease in fuel saving potential.

Unlinkability and privacy protection are relevant in platooning, but platoon members will have to be able to link each other's messages during the platoon's lifetime. However, external tracking of platoon members needs to be prevented not only for reasons of drivers' privacy, but also to protect business-critical information in case of commercial platoons, e.g., routes, start and end points of platoon members.

The EU ITS trust model and PKI architecture in combination with a respective pseudonym change strategy can be used to address the above-listed requirements. However, platooning might benefit from or even require additional means for authentication and authorization. For example, information on authorization to act as lead vehicle is very specific and might not necessarily need to be included into general ITS certificates. Further, communication with private entities such as fleet managers (see, e.g., [12]), which are not necessarily integrated into the EU C-ITS security architecture would require further measures.

[4]Figure used with permission of ETSI. ©European Telecommunications Standards Institute 2018. Further use, modification, copy and/or distribution are strictly prohibited.

Attribute-based credentials seem to be a promising approach to the authenticity and authorization challenges in ITS and platooning. Recently, they have gained increased attention as potential solution to the privacy challenges in V2X communication. In the following, we investigate attribute-based credentials (ABCs) with respect to their applicability in platooning and their suitability for integration into existing security concepts for platooning.

3 ATTRIBUTE-BASED CREDENTIALS

Credential systems are deployed to allow users to obtain credentials from a trusted credential issuer and to demonstrate the possession of these credentials to a verifier, who also trusts the issuer. Anonymous or pseudonymous credential systems aim at providing this functionality while preserving users' privacy by providing unlinkability of users' credential demonstrations. Pseudonymous credential systems have been subject to research for several decades, with seminal work on the subject having been presented by Chaum already in the 1980s [8].

In attribute-based credential systems, users obtain credentials and prove the possession of those credentials without necessarily revealing the values contained within them. For example, such systems can allow users to prove that they are of legal age without disclosing their birth date or actual age [7]. Two main classes of approaches towards attribute-based credentials exist: those based on blind signatures (e.g. U-Prove [22]) and those based on zero-knowledge proofs (e.g. Idemix [7] or Persiano's approach [24]). A blind signature scheme allows an entity to sign a message without knowing the content of the message. A zero-knowledge proof confirms that an entity has knowledge of a certain value, without disclosing or transmitting that value itself. Figure 3 provides a generic overview on the entities in an ABC system and their interactions.

If needed, attribute-based credentials can be used for key binding, where "a credential can be bound to a user's secret key, i.e., it cannot be used without knowing the secret key" [4]. That way, ABCs can be used "somewhat analogous[ly] to traditional public-key certificates, [...] but unlike traditional public-key certificates, a Privacy-ABC is not bound to a unique public key: it is only bound to a unique secret key" [4]. The "secret key can be used to derive pseudonyms, which behave like public keys corresponding to the [...] secret key, in the sense that a verifier can check that a user knows the secret key" [21]. However, "arbitrarily many unlinkable pseudonyms [can be derived from a secret key], in the sense that a verifier cannot tell whether two pseudonyms originated from the same [...] secret key" [21]. Such pseudonyms can be included in an ABC presentation token which thus proves that the credential is bound to the corresponding secret key.

Different constructions of ABC schemes have been proposed over time. One-show constructions [9], [20] allow credentials to be shown only once and for each service and point in time a new credential needs to be created. This is expensive and resource consuming. In later work, approaches for multiple unlinkable presentations of one credential to one or more parties were proposed [6], [24], [27]. These so-called multi-show credentials, which can be used more than once, provide the advantage of lower cost (time and computing resources), since the issuing organization does not need to be involved every time a credential is shown. At the core of the multi-show idea lies the principle that to get the credential certified, a user only needs to get into contact with the issuing organization once. This improves efficiency as only one certificate is needed for different services and different times. Additionally, these schemes also ensure unlinkability during a proof of possession in the protocol. Furthermore, sharing credentials with other users can be disincentivized by including a valuable external secret (e.g. credit card PIN). In case a user wanted to transfer the credential certificate, she would also need to make this data available [7].

4 STATE OF THE ART IN ATTRIBUTE-BASED CREDENTIALS FOR V2X

Traditionally, attribute-based credentials are used or envisaged to be used for identity management and access control in domains such as eCommerce or online chats[5]. However, the above-described characteristics of ABCs also seem to be useful for ensuring authenticity and authorization in V2X communication while possibly providing better privacy protection than the current approach based on periodic pseudonym change.

As described above, attribute-based credentials are designed for specific use cases where a user needs to demonstrate possession of a credential or possession of certain attributes certified in the credential. Clearly, this makes ABCs conceptually well suited for V2X use cases where users need to demonstrate some authorization information or that they exhibit some attribute (e.g. having paid some fee or being authorized to platoon with vehicles of type t1, t2 and t3 but not t4) without necessarily revealing the actual attribute values or information. Further, in V2V communication as envisaged in the EU ITS, the certificates used to sign messages attest that a vehicle is authorized to participate in the ITS in general and, specifically, to send particular messages types (*application IDs*) [14]. Prima facie and as described below, both of this can theoretically be achieved using ABCs.

Generally, two main approaches to integrate ABCs into the existing ETSI ITS trust architecture (see above) lend themselves to further investigation:

(1) ABCs could be used to replace the pseudonym certificates currently used in ITS, either in general or for specific use cases and applications.
(2) ABCs could be used in specific steps of the existing certificate management, e.g., to demonstrate a vehicle's authorization to obtain ATs (cf. [17]), thereby replacing the currently used ECs.

[5] See, e.g., https://www.zurich.ibm.com/identity_mixer/

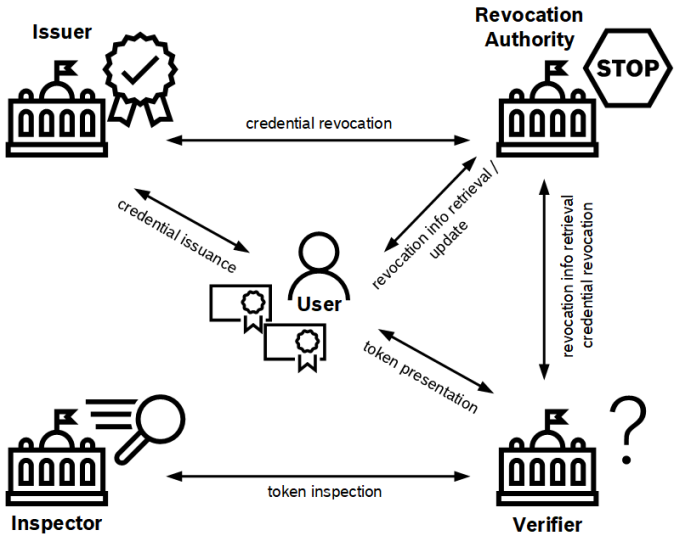

Figure 3: Entities in an ABC system and their interactions (adapted from [4])

Attribute-based credential systems for V2X communication have indeed become subject to increased research during recent years. However, ABCs for vehicular communications are still sparsely researched and only few publications on the topic can be found.

An overview and extensive survey on pseudonym schemes in VANETs in general has been presented by Petit et al. [25]. They focus particularly on V2V communication and do not further consider V2N communication such as communication between platoon members and a platoon management system. They identify four rough categories of approaches towards pseudonymization for V2V:

- Pseudonym schemes based on symmetric cryptography
- Pseudonym schemes based on asymmetric cryptography
- Pseudonym schemes based on identity-based cryptography
- Pseudonym schemes based on group signatures

However, while they provide a broad overview on pseudonym schemes for VANETs, they do not consider ABCs.

In contrast, de Fuentes et al. [10] provide a VANET-focused analysis of attribute-based credential systems. In particular, they analyze three "representative" [10] ABC techniques: Idemix [7], U-Prove [22] and a VANET-adjusted variant of Persiano's approach [18]. The authors analyze these approaches regarding their applicability in road traffic services by first investigating which applications from the ITS Basic Set of Application (see ETSI TR 102 638) would benefit from the usage of ABCs. They identify *Cooperative Navigation*, *Location-based Services* and *Communities Services* (see ETSI TR 102 638) as viable candidates for the usage of ABCs. *Active Road Safety* applications are not considered suitable candidates. Subsequently, de Fuentes et al. investigate the suitability of the three analyzed ABC approaches in the context of the selected applications with respect to conceptual fit and performance. They find that Idemix is the best fit, with U-Prove following relatively close behind and the adjusted Persiano approach lagging far behind. However, only "Day-1 applications" [14] (see Section 1) and use cases without direct safety-relevance are considered.

As can be seen, neither of the extensive surveys performed by Petit et al. and de Fuentes et al. consider ABCs for authentication of messages in safety-related V2V communication. Rather, ABCs are considered (if at all) viable approaches for applications which do not have direct impact on safety and, therefore, do not have to satisfy high performance and low latency requirements. It is to be discussed whether this is a result of ABCs' performance or of conceptual misalignment of ABCs for usage in safety-relevant applications in V2V communication.

González-Tablas et al. [18] focus on the authorization of vehicles and data protection. They use ABCs for verification of administrative documentation of vehicles "while guaranteeing minimal disclosure information [sic!] of the private attributes encoded in the credentials and unlinkability between different credential shows" [18]. Their work is based on Persiano's approach, which they modified to be non-interactive and to additionally allow the validation of different credentials kept "by the same entity and encoding the same private attribute (cross-credential proving)" [18]. The proposed system makes use of a "specific set of pseudonym-based certificates" to retrieve "identity of vehicles unobservant of mandatory requirements" [18]. Further, the authors claim that it is able to collect non-repudiation evidence of such participants in the system, and they are able to revoke the authorizations. They also state, in an exemplary setup, that the system is able to issue an anonymous credential in 188ms. They consider Idemix

and U-Prove inapplicable due to their revocation attributes. Idemix uses white-listing revocation based on accumulation which is, according to [18], not efficient in the V2X scenario due to scalability issues. Revocation in U-Prove can only be achieved if untracebility is not required, which does not apply to V2X.

As described above, on a conceptual level ABCs do seem to be well suited for safety-relevant V2V use cases. Hence, and hardly surprising, several authors addressed using ABCs for securing safety-relevant V2V communication. Singh and Fhom [26] provide protocols for using ABCs for signing and verifying V2V and V2I messages, where vehicles and RSUs act as provers and verifiers. The authors build upon Idemix [7] and provide a proof-of-concept implementation of their approach. Huang [19] presents and implements the CLIBA authentication scheme, which constitutes a modified version of Idemix adjusted to the V2X domain. However, in both approaches, verification requires high computational overhead and message sizes are large which leads to them being "prohibitively inefficient" [17] for the envisaged use cases [3].

Neven et al. [21] aim at addressing, among others, these performance issues. They propose a "generic approach of C-ITS based on Privacy-preserving Attribute-Based Credentials" [21]. The presented approach builds upon the PRESERVE security architecture [23] to which the European ITS security and trust architecture corresponds and can "to a certain extent be seen as a generalization of the direct cryptographic scheme of Singh & Fhom" [26]. In contrast to Singh & Fhom's approach and the EU ITS security architecture, the presented scheme uses an ABC issued by a Pseudonym Authority to locally generate and sign pseudonym certificates. To that end, the ABC acting as a short-term credential includes an attribute indicating a validity period. The ABC is used to generate a presentation token that reveals the period and to "sign" a locally generated public key. Finally, the secret key corresponding to the generated public key is used to sign messages such as CAMs and DENMs and the presentation token is used as part of the pseudonym certificate. Further attributes could be integrated into the ABC to signal further vehicle properties, e.g., such regarding authorizations to participate in platooning. Neven et al.'s approach also supports identification and revocation of misbehaving vehicles. While the presented approach should be more performant than the approach presented by Singh & Fhom due to not using ABCs to directly sign messages but to certify public key pseudonyms, Neven et al. do not present an implementation of their scheme and no performance analysis. They argue that "currently available Privacy-ABC implementations are unlikely to meet the efficiency requirements of practical C-ITS scenarios, especially in term of signature size" [21].

As can be seen, the very few existing schemes for utilizing ABCs for securing safety-relevant V2X communication seem not to satisfy the high performance requirements of these ITS use cases. On the one hand, ABC-based signatures lead to large message sizes (cf. e.g. [19]). On the other hand, computational overhead of ABC token generation and verification is higher than for standard signatures [21], [19].

Still, this does not mean that ABCs can not be beneficial in V2X communication. As described above, ABCs can not only be used to act as a means to authenticate V2V messages. They can also be used for non-safety critical (and potentially seldom performed) V2N communication, e.g., for obtaining specific ATs, ECs or other credentials. For example, Förster et al. [17] introduce PUCA, a pseudonym scheme where vehicles utilize n-show credentials [5] (which can be enhanced with attributes) to authenticate against AAs in order to obtain ATs. In the PUCA, privacy takes precedence over accountability, i.e., while revocation of pseudonyms is supported, de-pseudonymization is possible only with the pseudonym holder's collaboration. The proposed scheme is in general compatible with the current European ITS system and only changes pseudonym issuance.

Büttner & Huss [3] provide an approach that is somewhat similar to that presented by Förster et al. They present an approach in which vehicles use ABCs to obtain service-specific ATs for non-safety services. They provide an extension of the EU ITS PKI where EAs or, alternatively, a trusted third party (TTP) issues ABCs, which in turn are used to obtain service-specific ATs from a service provider. The ATs are used to signal authorization regarding service usage and, optionally, to indicate payment.

5 ABCS IN PLATOON BOOKING

As shown above, ABCs are not well suited for authentication in safety-critical, low latency communication. However, as already mentioned, platooning does not exclusively require low latency intra-platoon communication but also relies on communication between PCs or PLMs and (central) management systems external to the platoon. This communication does not necessarily have the same strict latency requirements as the communication used to coordinate PLMs' driving behavior. These lesser critical (from a safety perspective) communication can, for example, occur between platoon candidates and a platoon booking system (cf. [11]), a platoon and some central management system operated by a forwarding company or between a platoon and other central systems, e.g., such for fleet management. We consider these communication paths viable candidates for the usage of ABCs. In the following, we focus on the use case of a central booking system (see Section 2.2) and substantiate our assessment.

The primary data protection challenge associated with a central booking system relates to the linkability of different booking events. We consider the booking system a system-internal "attacker" (honest but curious). Due to its position and tasks, the attacker will be able to identify participants and learn about trips taken by a vehicle across different platoons. This information can be used to spy on certain vehicles and forwarding companies and for example learn about their costumers, utilization, or maybe even the goods transported (e.g. critical or dangerous goods). Hence, the goal is to protect against linkability of different trips booked by one participant (i.e. one specific vehicle). We also need to consider that information about a truck (especially what

kind of goods the truck is transporting, its planned route and position inside the running platoon) would allow targeted attacks on the truck (e.g. robbery or acts of terrorism).

In principle it would be possible to use a secure multi-party computation scheme or a scheme based on homomorphic encryption to create platoons without revealing sensitive information to the booking system. However, these schemes are known to have very high computational and communication complexity and are therefore infeasible from a practical point of view. Another approach would be to run the booking system within a trusted execution environment (TEE) (e.g. based on Intel SGX). This would ensure that the information learned by the booking system cannot be misused. However, this approach would require to trust the manufacturer of the TEE as well as the software of the booking system. Therefore, we propose using ABCs to avoid the disclosure of sensitive information. ABCs can be used to selectively present the information needed by the booking system without disclosing additional information. Furthermore, remember that, depending on the ABC approach, presenting the same credential multiple times or presenting different credentials issued to the same entity cannot be linked by the entity verifying the credentials.

In particular, we consider a booking system as depicted in Figure 4 and described in the following.

(1) To be able to prove their authorization to take part in platooning, vehicles (platooning candidates (PCs)) receive credentials (p_c) issued centrally by a public body. This body can, for instance, be a governmental motor transport authority. Moreover this body will issue additional credentials which can be used by a PC to prove certain safety-relevant parameters of the vehicle (e.g. braking power, weight without payload, maximum payload).
(2) p_{ci} is presented to the platoon booking system (PBS) by PC_i together with the starting point, end point, and time frame of the planned route.
(3) The PBS verifies the correctness of p_{ci}.
(4) After collection of all PCs' inquiries, based on the received start points, end points and time frames, the PBS creates a list of possible platoons. The PBS publishes that list.
(5) A PC selects an appropriated platoon and sends a booking request to the PBS. This booking request again contains the credential (p_{ci}).
(6) After the PBS has received the booking requests from the PCs it updates the list of possible platoons, removing any platoon for which an insufficient number of booking requests have been made.
(7) For each remaining platoon the PBS checks whether the PCs are compatible, i.e., if the properties of the involved vehicles allow to form a platoon (speed, weight, braking power etc.). To that end, the PBS asks the respective PCs for the credentials to prove that they fulfill the necessary requirements, e.g., "top speed ≥ 70 km/h".
(8) Each PC_i shows the requested credentials r_{ci}.
(9) The PBS checks the received answers and, in case of requirements fulfillment, adds the PCs to the fitting platoon.
(10) A platoon joining credential j_{ci} is finally sent to each PC_i. This credential will later on be presented by the PC to the platoon management system to prove that the PC is allowed to join the given platoon, i.e., to become a platoon member.

In the "booking stage", vehicles (platooning candidates (PCs)) first need to prove to the booking system their authorization to take part in platooning (step 2). We assume that a respective credential is issued centrally by a public body, for instance a governmental motor transport authority. The authority also issues credentials that include safety-relevant parameters (e.g. braking power, weight without payload, maximum payload). While it would require checking the vehicle before every issuance, the authority could additionally issue short-lived credentials that include less static attributes such as current payload weight or hazard class. Second, starting point, destination and time frame is presented to the booking system. Further parameters of the platooning candidate are checked later on by the booking system (step 9) to ensure all requirements to join a specific platoon are satisfied.

In our proposal, credentials are constructed in such a way to not reveal identifiable information and that they not necessarily disclose exact parameter values. For instance, PCs can present a range for the speed with which they are able to safely perform platooning ("my maximal speed is above 70km/h") instead of the exact maximal speed. Platoon candidates could also prove that they belong to a limited set of specific forwarding companies. Remember that the credential itself contains the exact values - but what is proven to the verifier is only a "yes/no"-answer to a question (e.g., regarding maximal speed). Further, the booking system can define different classes of requirements for different classes of platoons or vehicles, e.g., "with a weight of 8 metric tonnes (t) the breaking power needs to be at least x" or "with a weight of 10t the breaking power needs to be at least y". Using ABCs, the platooning candidate can prove that it fulfills these requirements without giving away its exact maximal speed, owner, payload, weight, braking power or other attributes, thus making it harder for the attacker to uniquely identify the participant. Besides mandatory information, optional information can be included to improve the results of finding possible platoons. However, each candidate needs to decide if the additional information fits its data protection profile, meaning it will not expose itself more than individually desirable regarding linkability and secret information.

If, in our proposed system, a platoon candidate PC_i fulfills all requirements and can be booked into a suitable platoon, a credential j_{ci} is issued by the booking system allowing the platoon candidate to join a specific platoon (step 10). This credential will provide unlinkability between the booking process and the joining process. After presenting its credential to the platoon management system in order to be allowed to

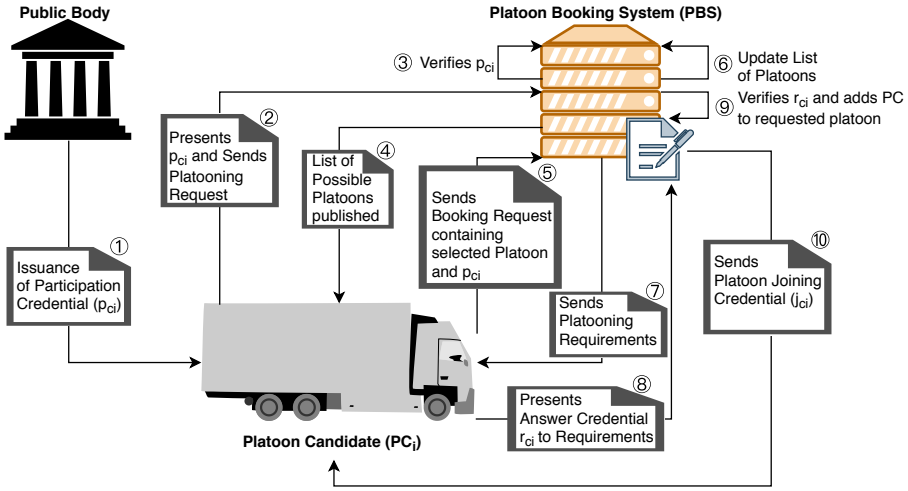

Figure 4: ABCs in Platooning

join the platoon, a PC negotiates the platooning parameters and cryptographic keys used for securing intra-platoon communication directly with the platoon management system as mentioned in Section 2.2. Note, that we do not utilize ABCs for authentication of messages exchanged during platooning, i.e., in the "maintain platoon" phase. Hence, safety-critical intra-platoon messages are authenticated using other means, e.g., more traditional mechanisms such as Message Authentication Codes (MACs) or signatures. On the one hand, using ABCs would require rather high computational power (each member broadcasts platoon control messages with a frequency of 10 Hz). On the other hand, we do not see a real advantage of using ABCs. We assume that throughout the "maintain platooning" phase platoon members can identity each other anyhow due to the physical proximity of the vehicles and the visibility of identifiers such as license plates.

In our scenario and approach, ABCs can further be used for increased privacy preservation within platooning-specific compensation schemes. As the vehicle in the first position of the platoon will not be able to benefit from platooning, i.e., will not benefit from slipstream effects, following PLMs might need to pay the lead vehicle's operator for the privilege to platoon. While regularly switching positions could also be imagined, it will decrease the efficiency of the system and might negatively impact the overall traffic flow on the road. To the best of our knowledge, no solution proposals regarding privacy-preserving compensation schemes tailored to platooning exist in the literature. The linkability issues obviously also apply to compensation-related transactions, as a participant might use a unique ID (e.g. credit card number, or other identifier) which will allow the attacker to link transactions. Attribute-based credentials can facilitate a compensation system (e.g. financially or point based) which will make it hard for an attacker to link transactions. A basis for this system could be, for example, digital money based on ABCs as mentioned in [6].

6 CONCLUSION AND OUTLOOK

In this paper we have analyzed the literature corpus on the usage of attribute-based credentials in the V2X domain. Based on our analysis, we argued that attribute-based credentials are ill-suited for securing safety-critical communication between members of a platoon. However, we have shown that ABCs can be utilized for increasing unlinkability in communication between a platoon and central systems for platoon management or booking. To do so, we proposed an ABC-based approach towards platoon booking and briefly discussed the usage of ABCs for platoon-internal compensation schemes.

We aim at providing a prototypical implementation of our proposal and a detailed evaluation of its performance and privacy properties in future work. Further, it is our intention to investigate privacy-preserving compensation schemes for platooning in more detail.

ACKNOWLEDGMENTS

This work has been supported in part by the Federal Ministry of Education and Research of the Federal Republic of Germany (BMBF) in the framework of the project 5G NetMobil with funding number 16KIS0677K. The authors alone are responsible for the content of the paper.

REFERENCES

[1] Article 29 Data Protection Working Party. 2017. *Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).* Technical Report WP 252. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171

[2] Anirudh Kishore Bhoopalam, Niels Agatz, and Rob Zuidwijk. 2018. Planning of truck platoons: A literature review and directions for future research. *Transportation Research Part B: Methodological* 107 (2018), 212 – 228. https://doi.org/10.1016/j.trb.2017.10.016

[3] C. Büttner and S.A. Huss. 2017. Attribute-based authorization tickets for Car-to-X communication. In *2016 IEEE Conference on Communications and Network Security, CNS 2016*. 234–242. https://doi.org/10.1109/CNS.2016.7860490

[4] Jan Camenisch, Maria Dubovitskaya, Anja Lehmann, Gregory Neven, Christian Paquin, and Franz-Stefan Preiss. 2013. Concepts and Languages for Privacy-Preserving Attribute-Based Authentication. In *Policies and Research in Identity Management*. Springer, Berlin, Heidelberg, 34–52. https://doi.org/10.1007/978-3-642-37282-7_4

[5] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. 2006. How to Win the Clonewars: Efficient Periodic N-times Anonymous Authentication. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*. ACM, New York, NY, USA, 201–210. https://doi.org/10.1145/1180405.1180431

[6] Jan Camenisch and Anna Lysyanskaya. 2001. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Advances in Cryptology — EUROCRYPT 2001*. Springer, Berlin, Heidelberg, 93–118. https://doi.org/10.1007/3-540-44987-6_7

[7] Jan Camenisch and Els Van Herreweghen. 2002. Design and Implementation of the Idemix Anonymous Credential System. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02)*. ACM, New York, NY, USA, 21–30. https://doi.org/10.1145/586110.586114

[8] David Chaum. 1985. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Commun. ACM* 28, 10 (1985), 1030–1044. https://doi.org/10.1145/4372.4373

[9] Lidong Chen. 1995. Access with pseudonyms. In *International Conference on Cryptography: Policy and Algorithms*. Springer, 232–243.

[10] J. M. de Fuentes, L. Gonzalez-Manzano, J. Serna-Olvera, and F. Veseli. 2017. Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities. *Personal and Ubiquitous Computing* 21, 5 (2017), 869–891. https://doi.org/10.1007/s00779-017-1057-6

[11] Sönke Eilers. 2015. Information Model for Platoon Services - Deliverable D3.2 - COMPANION.

[12] Söenke Eilers, Jonas Martensson, Henrik Pettersson, Marcos Pillado, David Gallegos, Marta Tobar, Karl Henrik Johansson, Xiaoliang Ma, Thomas Friedrichs, Shadan Sadeghian Borojeni, and Magnus Adolfson. 2015. COMPANION–Towards Co-operative Platoon Management of Heavy-Duty Vehicles. In *2015 IEEE 18th International Conference on Intelligent Transportation Systems*. IEEE, 1267–1273.

[13] ETSI. 2018. ETSI TS 102 940 v1.3.1 - Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management. https://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.03.01_60/ts_102940v010301p.pdf

[14] European Commission. 2016. A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility. https://ec.europa.eu/transport/sites/transport/files/com20160766_en.pdf

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

[16] European Commission. 2019. COMMISSION DELEGATED REGULATION (EU) .../... of 13.3.2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282019%291789

[17] David Förster, Frank Kargl, and Hans Löhr. 2016. PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. *Ad Hoc Networks* 37 (2016), 122 – 132. https://doi.org/10.1016/j.adhoc.2015.09.011

[18] A. I. González-Tablas, A. Alcaide, J. M. de Fuentes, and J. Montero. 2013. Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations. *Ad Hoc Networks* 11, 8 (2013), 2693 – 2709. https://doi.org/10.1016/j.adhoc.2013.05.008

[19] Liting Huang. 2012. *Secure and privacy-preserving broadcast authentication for IVC*. Master's Thesis. University of Twente.

[20] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. 1999. Pseudonym Systems. In *Selected Areas in Cryptography*. Springer, Berlin, Heidelberg, 184–199. https://doi.org/10.1007/3-540-46513-8_14

[21] Gregory Neven, Gianmarco Baldini, Jan Camenisch, and Ricardo Neisse. 2017. Privacy-preserving attribute-based credentials in cooperative intelligent transport systems. In *2017 IEEE Vehicular Networking Conference (VNC)*. 131–138. https://doi.org/10.1109/VNC.2017.8275631

[22] Christian Paquin and Greg Zaverucha. 2011. *U-prove cryptographic specification v1. 1, Revision 3*. Technical Report. Microsoft Corporation.

[23] PERSERVE Consortium. 2015. PRESERVE Project - Preparing Secure V2X Communication Systems. https://www.preserve-project.eu/

[24] Giuseppe Persiano and Ivan Visconti. 2004. An Efficient and Usable Multi-show Non-transferable Anonymous Credential System. In *Financial Cryptography*. Springer, Berlin, Heidelberg, 196–211. https://doi.org/10.1007/978-3-540-27809-2_21

[25] J. Petit, F. Schaub, M. Feiri, and F. Kargl. 2015. Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE Communications Surveys & Tutorials* 17, 1 (2015), 228–255. https://doi.org/10.1109/COMST.2014.2345420

[26] Ankit Singh and Hervais C. Simo Fhom. 2017. Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. *International Journal of Information Security* 16, 2 (2017), 195–211. https://doi.org/10.1007/s10207-016-0328-y

[27] Eric R Verheul. 2001. Self-blindable credential certificates from the Weil pairing. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 533–551.

[28] Bjorn Wiedersheim, Zhendong Ma, Frank Kargl, and Panos Papadimitratos. 2010. Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. In *2010 Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*. IEEE, 176–183. https://doi.org/10.1109/WONS.2010.5437115