# Securing V2X Communications for the Future - Can PKI Systems offer the answer?

**Giannetsos, Thanassis; Krontiris, Ioannis**

*Published in:*
Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019

*Link to article, DOI:*
10.1145/3339252.3340523

*Publication date:*
2019

*Document Version*
Publisher's PDF, also known as Version of record

*Citation (APA):*
Giannetsos, T., & Krontiris, I. (2019). Securing V2X Communications for the Future - Can PKI Systems offer the answer? In *Proceedings of the 14th International Conference on Availability, Reliability and Security, ARES 2019* Article 3340523 Association for Computing Machinery. https://doi.org/10.1145/3339252.3340523

# Securing V2X Communications for the Future - Can PKI Systems offer the answer?

Thanassis Giannetsos
Cyber Security, Department of Applied Mathematics and
Computer Science, Technical University of Denmark
atgi@dtu.dk

Ioannis Krontiris
European Research Center, Huawei Technologies
Munich, Germany
ioannis.krontiris@huawei.com

## ABSTRACT

Over recent years, emphasis in secure V2X communications research has converged on the use of Vehicular Public Key Infrastructures (VPKIs) for credential management and privacy-friendly authentication services. However, despite the security and privacy guarantees offered by such solutions, there are still a number of challenges to be conquered. By reflecting on state-of-the-art PKI-based architectures, in this paper, we identify their limitations focusing on scalability, interoperability, pseudonym reusage policies and revocation mechanisms. We argue that in their current form such mechanisms cannot capture the strict security, privacy, and trust requirements of all involved stakeholders. Motivated by these weaknesses, we then proceed on proposing the use of trusted computing technologies as an enabler for more decentralized approaches where trust is shifted from the back-end infrastructure to the edge. We debate on the advantages offered and underline the specifis of such a novel approach based on the use of advanced cryptographic primitives, using Direct Anonymous Attestation (DAA) as a concrete example. Our goal is to enhance run-time security, privacy and trustworthiness of edge devices with a scalable and decentralized solution eliminating the need for federated infrastructure trust. Based on our findings, we posit open issues and challenges, and discuss possible ways to address them.

## CCS CONCEPTS

• **Security and privacy → Pseudonymity, anonymity and untraceability**; *Privacy-preserving protocols.*

## KEYWORDS

V2X Communications, Public Key Infrastructure, Location Privacy, Trusted Computing, Direct Anonymous Attestation

**ACM Reference Format:**
Thanassis Giannetsos and Ioannis Krontiris. 2019. Securing V2X Communications for the Future - Can PKI Systems offer the answer?. In *Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019) (ARES '19), August 26–29, 2019, Canterbury, United Kingdom.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3339252.3340523

## 1 INTRODUCTION

As vehicles become more automated, integrating more consumer devices and emerging IoT technologies, a new trajectory of commercial applications and services is becoming prominent. Vehicular Communications (V2X) play a central role in this effort encompassing Vehicle-to-Vehicle (V2V) and Vehicle-to Infrastructure (V2I) messaging. This cooperative architecture is gaining more and more outline opening new dimensions for *road safety*, *traffic efficiency* and *driving convenience* [1].

By enabling vehicles to take up the role of *information prosumers* (acting as both a recipient and source of information), it allows them to create an almost omniscient knowledge of their surroundings that can lead to better decision making [2]. Providing valuable information for private transport and logistics, information on traffic flow and disseminating hazard warnings are some of the critical use cases of this intelligent network that can have great impact on the ever-growing safety concerns for citizens' well-being.

However, despite their benefits, privacy is a key concern in this facet of Intelligent Transportation Systems (ITS) since the involved vehicle transmissions can be used to infringe the users' location privacy [3]. Many V2X applications rely on continuous and detailed location information, which if misused (all exchanged messages can be eavesdropped within radio range) can lead to the extraction of detailed location profiles of vehicles and path tracking [4]. Since there is usually a strong correlation between a vehicle and its owner [5], location traces of vehicles have the potential to reveal the movement and activities of their drivers. Two of the most prominent types of messages that are exchanged in the context of V2X are known as Cooperative Awareness Messages (CAM) and Decentralised Environmental Notification Messages (DENM) [6].

The correctness and reliability of these messages are key enablers towards the provision of enhanced security and privacy for the envisioned applications. Such requirements have been well documented in the European Telecommunications Standard Institute (ETSI) highlighting the paramount importance of properties like *anonymity*, *pseudonymity*, *unlinkability* and *unobservability* [7]. Intensive research efforts suggested, early on, the use of certificates for authenticating messages and preventing attackers from injecting false data in the vehicular network [8]. The distribution and management of these certificates is achieved through the use of appropriate Public Key Infrastructures (PKIs) [9].

In this context, the actual identity of the sender is not required for ensuring the trustworthiness of a transmitted message. It rather suffices to verify the origin correctness; a message has been sent by a valid V2X participant. Indeed, since broadcast messages contain the exact location information of the transmitting vehicle, what is

*ARES '19, August 26–29, 2019, Canterbury, United Kingdom*

ACM ISBN 978-1-4503-7164-3/19/08…$15.00
https://doi.org/10.1145/3339252.3340523

required is that certificates should not contain any identifying information that could *trace* them back to a particular vehicle or owner. Addressing this challenge led to the enhancement of the proposed PKI-based solutions [10] with privacy-friendly authentication services through the use of short-term anonymous credentials, i.e., *pseudonyms* [11]. The common denominator in such architectures is the existence of trusted (centralized) infrastructure entities for the support of services such as authenticated vehicle registration, pseudonym provision, revocation, etc.

If a vehicle uses a single pseudonym certificate through its lifetime, then this enables an attacker who observes the certificate at different locations to link the CAM messages. This can be done by using additional off-line information obtained via cameras, or correlating profiles to specific areas. To address this problem, solutions in the literature propose that each vehicle use multiple pseudonyms, changing frequently from one pseudonym to another [10]. Each vehicle uses a pseudonym certificate to sign CAM and DENM messages for a limited amount of time and change it afterwards. Use of changing pseudonyms can be considered the state-of-the-art in VANET privacy enhancing technologies like the one that was recently proposed in [12]; such schemes were designed with the intention to thwart adversaries that eavesdrop parts of the network.

However, the accurate location information included in these messages together with the need for the very frequent vehicle transmissions (typically, for transportation safety, 10 messages per second) raise significant questions on the suitability of such centralized PKI-based approaches. For example, one of the main challenges inherent to the deployment of such credential management systems is *operability*, both in very sparse and in highly overloaded networks [13]. One very important prerequisite in V2X communications is the scalability of the applied information dissemination schemes. The autonomously acting PKI must ensure delivery of data to those nodes which are interested in it with low latency, while efficiently leveraging network resources; a requirement that is not straightforward due to the high mobility of network nodes resulting in frequent topology changes. As a result, all involved stakeholders have expressed concerns on the infrastructure and management costs of PKI deployments, the inability of some proposals to scale to today's needs, and performance penalties to communication sessions [14].

*Contributions:* In this paper, we investigate these questions by dwelling on the underpinnings of the current PKI-based solutions and their limitations. We argue that if we are to fruitfully benefit from the evolution of ITS, all presented challenges need to be resolved while taking into consideration the key technological transformations of the automotive industry [15]. New types of secure and privacy-preserving protocols might be needed to provide the envisioned level of security and privacy while augmenting the efficiency of the current infrastructure model. Towards this direction and to escape from today's conundrum, we then move on proposing the use of trusted computing technologies as an enabler for more decentralized approaches where trust is shifted from the back-end infrastructure to the edge (i.e, vehicles) [16]. We debate on the advantages offered, for all aforementioned aspects and limitations, and we underline the specifics of such a novel approach based on the use of advanced cryptographic primitives, using Direct Anonymous Attestation (DAA) [17] as a concrete example. In such approaches, vehicles will be responsible for generating their own pseudonyms resulting in simplified infrastructure models where there is no need for a dedicated entity to take up this role, as is the case in current PKIs. Overall, given today's situation, now is the time to start envisioning a healthy V2X ecosystem with such multiple enhancements that can be used according to the needs of all involved parties (clients, domains, and CAs).

## 2 V2X COMMUNICATIONS BACKGROUND

Following the IEEE and ETSI standards specifications, each vehicle has a unique, long-term identifier $L_{\text{id}}$, a public key $LK$ and the corresponding private key $Lk$. The $LK$ is bound to $L_{\text{id}}$ by means of certificates. Each vehicle is also provided with a set of anonymous credentials, the pseudonyms $Ps_i$, which correspond to ephemeral asymmetric key-pairs $(PK_i, Pk_i)$. In contrast to $L_{\text{id}}$, pseudonyms contain no information that can identify the vehicle. To enhance the trustworthiness of the system, the Hardware Security Module (HSM) securely stores $Lk$ and $Pk_i$ keys and generates digital signatures.

A vehicle digitally signs outgoing messages with the private key corresponding to the current pseudonym, and attaches the pseudonym to the message as well, in order to facilitate verification on the receiver side. Thus, message transmission do not reveal the identity of the vehicle, and messages signed under different pseudonyms are, in principle, unlinkable. However, vehicles need to switch from one pseudonym to another, not previously used.

Here we need to clarify that a degree of short range tracking is necessary to enable V2X applications, since it allows for the connection between road conditions and the vehicles driving in the area [18]. Protecting location privacy of individuals is about preventing long term tracking, which is not essential for road safety.

To be able to guarantee privacy, pseudonyms must satisfy the following requirements: 1) A pseudonym has to be used for a limited time, 2) be unique, meaning that no other vehicle can use the same one, and 3) a new pseudonym must always be available for the vehicle to enable the pseudonym change [9].

Any system that will be used to secure V2X communications should satisfy the following constraints:

- The system must scale to support a large number of vehicles;
- The system must be fast to support critical applications, like collision-avoidance. That is, communication exchange should not be burdened by the security overhead;
- The system must operate in a highly mobile environment, where there is only a sporadic availability of the communication channel between the car, the road infrastructure an the back-end infrastructure;
- The system must support user privacy;
- The system must support revocation of misbehaving users.

## 3 REQUIREMENTS & THREAT MODEL

**Security, Privacy and Legal Requirements.** The Data Protection and Privacy Working Group of the Cooperative Intelligent Transport Systems has issued an analysis, which makes it explicit that the broadcast CAM and DENM messages are personal data [19]. The reason for that is that even though they do not contain any unique identifier, the data subject can be indirectly identifiable, either through the location data and the dimensions of the vehicle contained in the CAM messages, or through the PKI certificate, attached to both massages.

The EU Commission [20] and the Article 29 Data Protection Working Party [21] also make it clear that data broadcasted by vehicles qualify as personal data, as it relates to an identifiable natural person. So the implementation of V2X communications requires compliance with the General Data Protection Regulation (GDPR).

GDPR explicitly emphasises on the principles of ’privacy by design’ and ’privacy by default’. Any V2X communication system should incorporate technical means to protect privacy in its design. We can translate this to a list of technical requirements, which we identify as follows (see also [22] for additional details):

- *Minimum disclosure*: The amount of information revealed by a user in a communication should be kept to the minimum and should be no more than what is required for the normal operation of the system.
- *Conditional Anonymity*: Vehicles should be anonymous within a set of potential participants. In case a vehicle deviates from system policies, the corresponding long-term identity can be retrieved by the PKI entities, and accordingly revoked.
- *Unlinkability*: In order to achieve unlinkability, no entity should be able to link pseudonyms of a specific vehicle with each other.
- *Forward and backward privacy*: The revocation of a credential does not affect the unlinkability of previously signed messages. Also, recovering the identity of the sender of a particular credential should not affect the privacy of other messages signed by the same sender.

**Threat Model**. Vehicular Communication systems are susceptible to both *outsider* and *insider* attackers [10, 16]. The former are unauthorized entities (i.e., no credentials or trust relationships with other system entities) that seek to compromise the system and disrupt its operation. An outsider adversary can eavesdrop on the broadcast messages in V2X communications, physically compromise V2X units, run side-channel attacks, etc. In contrast, the primary goal of insider attackers would be to intercept, block or modify network communications or impersonate a legitimate vehicle (Sybil attack [23]). They setup as registered and authorized participants, with access to the PKI components, that focus on eavesdropping and/or manipulating data for the purpose of gaining access to privacy sensitive information.

Furthermore, we have to also consider *Honest-But-Curious* [4] (HBC) adversaries who represent legitimate participants (i.e., infrastructure entities and/or vehicles). Their goal is not to disrupt the functionality of the network but to breach a vehicleâĂŹs privacy. The HBC does not deviate from the defined protocol rules but possibly learns information from legitimate message exchange and information monitoring.

## 4 CURRENT SOLUTIONS & SHORTCOMINGS

### 4.1 The PKI Promise in V2X

Aiming to cope with the requirements mentioned in Section 3, intensive efforts in academia, industry and standardization bodies have spurred a number of proposals towards creating a Vehicular Public Key Infrastructure (for a survey, see [24]).

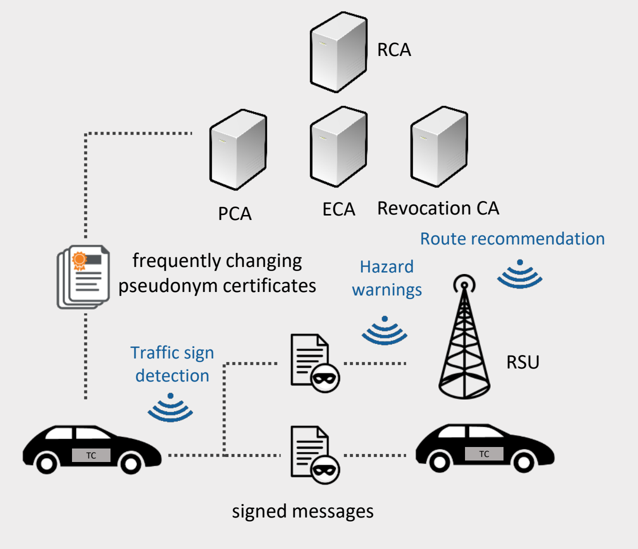

**Figure 1: A V2X security solution based on PKI**

One can trace the efforts starting from the first type of vehicular communication security architectures [25], based on a number of European projects, until the most recent solutions, notably the Security Credential Management System (SCMS) [12], which is a product of vehicle OEM consortia and the US Department of Transport (USDOT), and the European Cooperative Intelligent Transport Systems (C-ITS), developed by CEN and ETSI with support from the European Commission. The E-Safety Vehicle Intrusion protected Applications (EVITA) project [26] developed a prototype for securing in-car networks, while the Secure Vehicle Communication (SeVeCom) [27] and Privacy Enabled Capability in Co-operative Systems and Safety Applications (PRECIOSA) [28] projects addressed the complex security and privacy challenges over the wireless channel. Most recent efforts such as the Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) and COmmunication Network VEhicle Global Extension (CONVERGE) [29] projects worked towards the implementation of a complete secure and privacy-preserving subsystem that employs a Hardware Security Module.

The aforementioned research efforts have proposed the use of pseudonym-based schemes as the main privacy preserving mechanism for V2X. The question then becomes, *how the vehicles are provided with the set of pseudonyms.* In the PKI approach, a set of certification authorities (CAs) are responsible for providing credentials to the participating vehicles (Figure 1). In the general case, there is a set of different authorities with distinct roles:

- Root Certificate Authority (RCA): This entity is the trust anchor of the PKI that is responsible for issuing certificates to sub-CAs. The certificate of the RCA is self-signed.
- Enrollment Certification Authority (ECA): This entity is responsible for registering vehicles and issuing long-term certificates. Entities with enrollment certificates can then apply

to other CAs, like for instance to the pseudonym CA for issuing pseudonym certificates.

- Pseudonym Certification Authority (PCA): This entity is responsible for issuing certificates that do not contain any identifying information.
- Certificate Revocation CA: The entity responsible for the revocation of the anonymity of offending vehicles (e.g., vehicles tha disrupt the system or try to perform data pollution). It mainly issues Certificate Revocation Lists (CRLs) for all kinds of certificates.

Key material associated with pseudonym credentials should be stored securely inside vehicle OBUs and should not be extracted or transferred outside the vehicle. For this reason, the integration of HSMs or tamper-proof devices (TPD) in OBUs have been proposed for secure key storage and management [30].

As aforementioned in Section 2, a new pseudonym must always be available for the vehicle, to enable the pseudonym changing scheme. This can be ensured by storing a large set of pseudonym certificates on the vehicle, which requires that the vehicle downloads them periodically from the back-end infrastructure.

Maybe the most important difference between SCMS and C-ITS is the assumption they make on connectivity. SCMS was designed to cope with very intermittent connectivity between the vehicles and the back-end infrastructure. For this reason, vehicles are provided with a batch of approximately 3000 pseudonym certificates, which should be enough for about 3 years, assuming 20 pseudonyms per week. On the other hand, C-ITS system was designed to operate with the assumption of frequent connectivity of vehicles to the back-end. So the number of concurrently valid ATs is at most 60, and their pre-loading period, i.e. the period they can be issued before the start of their validity, cannot be longer than 3 months.

#### 4.1.1 Separation of duties.

As was described in Section 3, security and privacy-preserving architectures should protect not only against outsider attackers, but also insiders. The idea of changing pseudonyms, mainly targets the protection against outsider adversaries. In order to protect against the latter, additional mitigation measures are needed: One common approach is to divide the PKI operations among its components, which should have organizational separation between them [31]. That means, each component of the architecture is managed by a separate organizational entity, such that information exchange can be controlled.

The SCMS design accounts for outsider and insider attackers at a level that at least two institutions need to collude in order to compromise users' privacy, i.e. there is a technical privacy protection included such that organizational protection can easily be implemented. Similarly, C-ITS specifies different entities responsible for providing the different security and privacy services [32].

Moser et al. [33] further differentiate between the operator in charge and the technical operator. The former is the responsible institution which instructs, controls and also pays the CA operation. So, it must be an industry-wide accepted institution, e.g. a consortium of all OEMs or a governmental body. The latter is the institution that actually implements, operates and maintains the CA. This role could be taken by the operator in charge itself, or an external supplier of CA/PKI services.

A basic element of PKI, is that all participants in the system need to trust that the CAs are honest and un-compromised (semi-trusted environment). Thus, the question becomes, *how to establish and maintain this federated trust.* The typical solution consists of audits that verify that the CAs implement a high standard of operational and technical security [33]. The CAs declare that they follow a so-called certificate policy (CP) or certificate practice statement (CPS) as defined in RFC 3647 [34] and they conform to the specifications therein on when and how an audit takes place, what is covered by an audit and who the auditor can be.

However, this reliance on multiple infrastructure entities even under the "separation of duties" paradigm, is a double-edge sword: while the proposed solutions can achieve their goals under weakened trust assumptions on the trustworthiness of the PKI infrastructure, it raises questions on the system's availability and scalability in the case of a technical fault or attack. If the infrastructure (or part of it) is unavailable for a specific period of time, this might lead to vehicles having obsolete information (i.e., non-updated CRLs due to no-connectivity) which can lead to wrong decisions, thus rendering the V2X systems useless. Furthermore, an open question is, *how such service-oriented PKI-based architectures can transparently establish strong trust relations (federations) among different entities of the system.* Considering the variety of involved stake-holders in automotive applications, this need for a scalable Web of Trust is not a straightforward task [10].

#### 4.1.2 Change of Pseudonyms.

When changing pseudonyms while no other vehicles are in the vicinity, a vehicle can fall victim of tracking attacks [4]. One popular approach to resolve this, is to require that the change happens at the same time with neighboring vehicles, which introduces the concept of mix-zones. There are many papers suggesting variations of this technique, but at the end it remains unclear which one is the most effective in practice. A recent study showed that in a scenario with vehicles broadcasting messages at 1 Hz and changing pseudonyms every 10 seconds, an attacker can effectively track vehicles and their drivers with high accuracy using techniques based on Kalman filters [35].

#### 4.1.3 Revocation of Pseudonyms.

Certificate revocation is a standard consideration for any PKI system. In case of misbehavior, the wrongdoer can be evicted, i.e., prevented from further participation. The revocation of back-end entities can be done in standardized ways by including the revoked certificates in a Certificate Revocation List (CRL) and then published by the CA responsible for that trust domain. But for vehicles using short-lived pseudonym certificates, things are more complicated. If a vehicle possesses multiple certificates that are unlinkable, every single certificate needs to be put on the CRL, which would increase the bandwidth requirement to a non-practical level.

One approach, followed by C-ITS, is not to revoke pseudonym certificates, but rather revoke only the long-term identity of the vehicle. The vehicle can continue participating in the system until all of its existing pseudonym certificates are expired. Then, it has to request renewal of its certificates from the system using its enrollment certificate. Since the system included the vehicle's enrollment certificates in an internal revocation blacklist, this update request will be denied. However, this does not prevent the vehicle from misbehaving while using any pseudonym it already has.

Another approach, followed by SCMS, is to still use CRLs to revoke existing pseudonym certificates, and find ways to address the bandwidth problem. For example Nowatkowski et al. [36] has shown that the CRL list may grow as much as 2.2 GB, depending on the policy for the number of pseudonyms carried by the vehicle. SCMS resolves this by including a linkage value in pseudonym certificates that is derived from cryptographic seed material. Publication of the seed is sufficient to revoke all certificates belonging to the revoked vehicle. For protection against insider attacks, the seed is the combination of two seed values produced by two Linkage Authorities (LAs).

One advantage of the SCMS's revocation process is that CRLs' size grows with the number of revoked vehicles and not with the number of certificates revoked. However, the problem is that a CRL entry's lifespan corresponds to the duration of the batch of pseudonym certificates carried by the revoked vehicle. So CRL entries are not so short-lived and this can lead to large CRLs again, because pseudonym batches are expected to cover a long time period (maybe even years).

## 4.2 Remaining challenges

While intensive research efforts have proven the security and privacy guarantees provided in the aforementioned PKIs, there are still a number of pending challenges to be conquered that harden their deployment in a healthy PKI ecosystem that can be used according to the needs of all involved stake-holders [37].

**Privacy & Trust.** While the previously described concepts foresee a technical separation of different PKI authorities, it is yet not clearly defined who will operate the identity and credential provision and how trust relationships will be established. It is not precluded that multiple authorities can be operated by one organization. This is not necessarily a problem as long as there are appropriate policies in place that prevent, for example, one person from being able to access information at more than one component of the PKI. The employment of a PCA (or multiple virtual instances of it) that issues all pseudonyms to the requesting vehicles, is an indicative example of the raising privacy and trust concerns with a direct impact on the anonymity of the vehicles. Since the PCA has access to all provided pseudonyms, in the case of a sparse V2X deployment, what is the impact on the underlying anonymity set? It has been shown that when a change of pseudonyms is triggered by a relatively small number of vehicles (i.e., $< 20$ vehicles in a mix-zone), the PCA can with a certain probability (around 33%) link pseudonymous location samples to each other (even when constructed under different pseudonyms) [35].

The possibility of security breaches has the potential to seriously weaken the technical privacy protection measures, since they shift the focus on trust. However collusion or security incidents affecting certification authorities have grown more frequent in the recent past [38], so the existence of a PKI architecture does not guarantee per se the enactment of trust between the peers and additional measures are necessary to reinforce a scalable Web of Trust [21].

**Scalability.** The efficiency of V2X communications and their scalability are important factors given the large scale of the employed multi-domain automotive environment. In the V2X scenario, scalability issues arise in several different contexts. The number of active nodes (vehicles) has an impact on network connectivity and on the likelihood of congestion on the wireless channel. In addition, protocol design has a great impact on scalability. The most crucial bottleneck is the bandwidth limitation: Due to the shared wireless channel with a CSMA/CA medium access scheme and multihop communication between distant nodes, the limited bandwidth is further decreased by poor channel utilization [13].

While in sparse VANETS, low connectivity must be overcome with intelligent "store-and-forward" algorithms, controlling the network load is the most important challenge for operability in densely populated network scenarios. The number of messages which have to be sent over the shared medium is predominantly influenced by the number of vehicles and the number of applications deployed in these vehicles. However, network load is additionally influenced by the fact that active safety messages have to be rebroadcast within their target area for the duration of their validity. This ensures the availability of the message for new vehicles entering the area after the initial broadcast.

Another important aspect of scalability is the performance of the computationally intensive asymmetric cryptography mechanisms employed. The real-world performance of such primitives has been summarized by PRESERVE [29], where it is shown that a vehicle should be able to perform about 1,000 verifications per second, in order to support a secured service. On the other side, the need for strong privacy guarantees has led to even more complex PKIs with many entities and layers that make it harder to scale.

**Revocation.** In the context of revocation policies for removing misbehaving nodes from the network, this can only be achieved when the employed pseudonym scheme supports the resolution of participants' long-term identities from their pseudonyms [9, 17]. In this case, information about the revocation of a vehicle's long-term credentials, is disseminated to other participants through the CRLs or other means. Besides being computationally intensive (i.e., the use of CRLs also assumes enhanced connectivity so that all vehicles can periodically retrieve any updated lists [39]), this is harmful to the protection of their privacy [4].

Overall, while the need for pseudonym revocation is addressed by several PKI proposals, there has not been a consensus on the method that could address this efficiently. This is because there is a trade-off between vulnerability and cost, especially connected to the size of Certificate Revocation Lists.

# 5 TOWARDS DECENTRALIZED ROOTS OF TRUST

Seeking to design successful secure and privacy-preserving architectures for V2X systems comprising of millions of autonomous vehicles, one has to cater for the aforementioned challenges and the strict trust requirements of a wide variety of multi vendor devices and platforms. The security, interoperability and connectivity in a dynamic network of vehicles, gateways, services and applications across operations technology and information technology stakeholders requires strategic rethinking of policies and processes in the context of cyber-security, privacy and trust establishment.

Furthermore, a gamut of diverse applications and services are expected to find their way to the vehicular ecosystem. Existing Internet-based service providers with multiple security policies and service agreements will be soon offering their services to V2X users. Moreover, users seeking personalized services will wish to subscribe to many of them. As vehicle mobility cannot be geographically constrained, it is likely that such services will span over multiple administrative domains.

A key challenge, in this context, is to establish and manage trust between entities, starting from bi-lateral interactions between two single system components and continuing as such systems get connected to ever larger entities. But *how can we make sound statements on the security and privacy properties of single systems and transfer this to statements on the security properties of hierarchical compositions of systems ("Systems-of-Systems")?*

Towards this direction, we argue that this pressing need for establishing federated trust between services and devices cannot be solely secured with common centralized solutions like PKIs. What is needed are solutions capable of shifting trust from the back-end infrastructure to the edge (i.e., vehicles) so as to reduce the vector of entities for which we want to make sound statements in terms of their configuration, security settings and trustworthiness; essentially, exclude all infrastructure entities from the trust model and focus on neighboring vehicles. Trusted computing is one approach that enhances the security on these devices by installing a "root of trust" (RoT). These roots of trust can be used to both: (i) attest that devices are in a "trustworthy" state, meaning that the devices behave as expected for a specific purpose, and (ii) enhance their privacy posture. For the latter, anonymous credentials can be leveraged through the use of advanced cryptographic primitives such as Direct Anonymous Attestation [17].

Direct Anonymous Attestation is an anonymous digital signature mechanism, where for each signature no entity can discover the signer's identity. However, DAA still has the property that only a legitimate signer (e.g., vehicle) can create a valid signature through the use of trusted computing hardware or software. Under DAA, vehicles will be responsible for generating their own pseudonyms resulting in simplified infrastructure models where there is no need for a dedicated entity to take up this role.

A root of trust (RoT) anchor may be implemented in hardware (e.g., automotive variant of Trusted Platform Module [40] (TPM)), software (e.g., Trusted Execution Environments [41] (TEEs)) and/or Physically Unclonable Functions [42] (PUFs).

## 6 DIRECT ANONYMOUS ATTESTATION FOR INTERTRUSTABILITY OF V2X SYSTEMS

DAA [17] is a platform authentication mechanism that enables the provision of privacy-preserving and accountable authentication services. DAA is based on group signatures that give strong anonymity guarantees. The key security and privacy properties of DAA documented in [43] are:

- *User-controlled anonymity*: Identity of user cannot be revealed from the signature.
- *User-controlled linkability*: User controls whether signatures can be linked.
- *Non-frameability*: Adversaries cannot produce signatures originating from a valid trusted component.
- *Correctness*: Valid signatures are verifiable, and linkable, where needed.

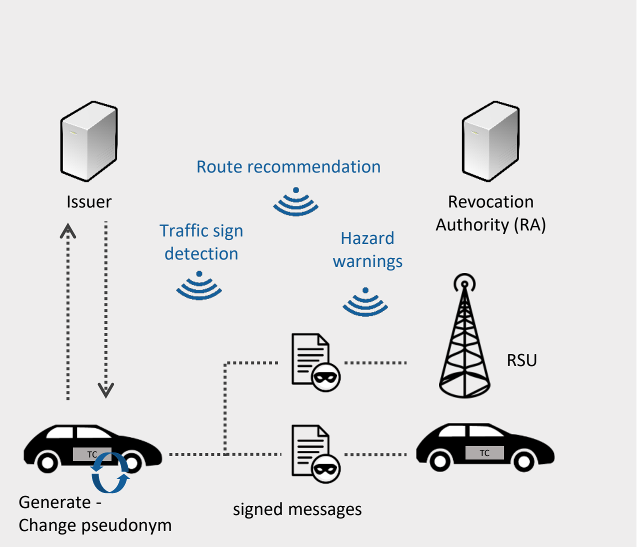

**Figure 2: Merging V2X with Trusted Computing - DAA-based Conceptual Architecture**

A DAA scheme considers a set of Issuers, hosts, TCs, and verifiers; the host and TC together form a trusted platform and ROT. The Issuer is a trusted third-party responsible for attesting and authorizing platforms to join the network. This entity is responsible for providing the same set of authentication services as the CA of existing V2X security architectures (Figure 1). A verifier is any other system entity or trusted third-party that can verify a platforms' credentials in a privacy-preserving manner using DAA algorithms; without the need of knowing the platform's identity. The Elliptic-curve cryptography (ECC) based DAA is comprised of five algorithms Setup, Join, Sign, Verify and Link.

- Setup - The system parameters must be chosen and the Issuer needs to generate its keys. The system parameters and the Issuer's public keys are then published and available to the group and to anyone who needs to verify the validity of a signature.
- Join - A Host using a TC joins the group and obtains an Attestation Key Credential (AKC) for an ECC-DAA key created by the TC. The he key can then be used to anonymously sign a message, or attest to data from this TC.
- Sign - Using the ECC-DAA key, for a range of signing operations.
- verifyX - Verifying a signature and returning true (valid) or false (invalid).
- linkX - Checking two signatures to see if they are linked and returning true (linked) or false (un-linked).

In a nutshell, as depicted in Figure 2, DAA is essentially a two-step process where, firstly, the registration of a TC executes once and during this phase the TC chooses a secret key (Setup). This secret key is stored in secure storage so that the host cannot have access to it. Next the TC talks to the issuer so that it can provide the necessary guarantees of its validity (Join). The issuer then places a signature on the public key, producing the Attestation

Identity Credential (AIC) *cre*. The second step is to use this *cre* for anonymous attestations on the platform (Sign), using Zero-Knowledge Proofs [44]. These proofs convince a verifier that a message is signed by some key that was certified by the issuer, without knowledge of the TC's DAA key or *cre* (Verify). Of course, the verifier has to trust that the issuer only issues *cre*s to valid TCs.

## 6.1 Design Choices & Benefits

The integration of trusted computing technologies into the Vehicle Communication systems allows for the establishment of much stronger end-to-end chains of trust that can be used according to the needs of all involved parties; ranging from manufacturing, assembly to field deployment, operations and supervisory controls. The primary benefits of such a DAA solution, over state-of-the-art asymmetric pseudonym-based V2X architectures, are in terms of *security*, *privacy* and *scalability*.

Most notably one of the biggest advantages of such a decentralized approach is its scalability, as trust is shifted from the back-end infrastructure to vehicles. Applying the DAA protocols results in the redundancy (and removal) of the most of the infrastructure entities including the PCA: vehicles can now create their own pseudonyms, and DAA signatures are used to self-certify each such credential that is verifiable by all verifiers. Furthermore, vehicles have total control over their privacy, as no trusted third-party is involved in the pseudonym creation phase. This means that it is infeasible for any third-party to reveal the identity of another vehicle assuring that pseudonym resolution is not possible in such a solution. This property also simplifies the message exchange in the context of V2X services (Figure 1) as communication with the infrastructure is currently minimized; trust is shifted to the edge points (vehicles).

Analyzing the requirements specified in Section 3, it is clear that all necessary properties are achieved with the addition of security and user-controlled privacy. The *anonymity*, *pseudonymity* and *unobservability* properties are built into DAA's algorithms, Join and Sign / Verify by using anonymous digital signatures. Therefore, third-parties cannot identify and link subsequent service requests originating from the same vehicle. This is also true in the presence of colluding third-parties and other ITS entities. The Join protocol is intentionally not privacy-preserving as the Issuer needs to be aware of the vehicle to be authenticated. However, successful completion of the protocol results in the vehicle solely owning a DAA credential.

*Unlinkability* (and/or different levels of *vehicle linkability*) is controlled by the vehicle through the DAA Sign / Verify phases. A vehicle has control over its DAA credential, and can decide whether or not to "blind" it, thus, producing pseudonyms (and revocation) that are linkable. The proposed approach provides privacy-preserving linkability via DAA deterministic signatures, where the use of a pseudonym is unlinkable to any other pseudonyms owned by a vehicle. This property is of particular interest to ITS as vehicles can demonstrate unobservability and unlinkability (when using multiple services) while being accountable for these service invocations.

In addition, DAA also provides *non-frameability* and *correctness* properties which are security attributes that PKI-based solutions do not capture entirely. DAA ensures that only valid and trustworthy TCs are able to join the ITS by ensuring that the endorsed TC keys have not been previously compromised. This ensures that TCs only produce valid signatures and can only be linked when specified by a particular authorized ITS service.

As aforementioned, effective revocation has been identified as a challenge due to the decentralized nature of vehicular networks and the various pseudonym re-usage and update policies (Section 4.2). The revocation service in a DAA-based model provides strong guarantees of successful completion when a misbehaviour has been identified and reported correctly using existing protocols. This is mainly due to the presence of the TC who is responsible for executing the revocation command, thus, not allowing to be circumvented by a (compromised) vehicle. Secondly, through the use of DAA deterministic signatures and link tokens, revocation under changing pseudonyms is still possible and the RA can verify revocation without compromising the vehicles' privacy. Additionally, as demonstrated in Rewire [45], CRLs are not required. This is also true for our architecture since the revocation mechanism triggers the TC to delete all of its secrets, thus, not allowing any subsequent (authorized) communication from the misbehaving vehicle. We have to note, however, that due to the untrusted nature of the host, it can be the case that it may not forward the revocation message to the TC for further processing. The implementation of a "heartbeat" mechanism (similar to the one used for monitoring the status of one-hop vehicular topologies) can provide protection against such malevolent actions. The RA sends out a message every cycle (which is expected to be received by TCs), either a revocation request or a signed and timestamped heartbeat message. TCs will take appropriate action if such messages are not received since this might be an indication of misbehaviour. While there is an overhead incurred by the introduction of this mechanism, it remains substantially lower than the current approaches that use pseudonym CRLs.

## 6.2 Protocol Details

Figure 2 introduces how a typical DAA pseudonym lifecycle architecture would execute. As we can see, only two trusted third-parties are required; (*i*) the Issuer who is responsible for authenticating vehicles through the Join protocol and (*ii*) the RA, as already exists in current architectures, that shuns out misbehaving vehicles from the ITS. In our context, vehicles are the combination of a *host*, that is a vehicular on-board computer "normal world", and a TC that executes in the "secure world"; together they form the platform which we refer to from this point onwards as the vehicle. We also have an additional role - this of *verifiers* which are other ITS entities, e.g., another vehicle, third-party service, etc. As depicted, the use of pseudonyms for V2X communications follows a similar pattern as in Figure 1, although they differ in the way pseudonyms are introduced and revoked. There are many similarities with the existing ITS architectures, demonstrating the feasibility of our DAA-based solution, since with limited effort it can be implemented in compliance with ETSI standards.

We have to highlight that such a solution assumes on-board TCs that support (*i*) *isolation*: separate and protected from the host in the event of compromise, (*ii*) *protected execution*: ensures the operation is executed and not interfered with, and (*ii*) *secure storage*: storage which is only accessible by the TC if the vehicle is in a "good" state.

## 7 CONCLUSIONS

We believe that sustainable evolution is the key to healthy V2X communication systems. To this end, in this paper, we presented the existing PKI-based solutions toward enhanced security, privacy and trust in V2X environments and we delved on their shortcomings. We then presented a decentralized DAA pseudonym framework for V2X, which provides clear benefits through a comprehensive set of security, privacy and accountability services to V2X systems. Leveraging widely accepted trusted computing technologies, this solution caters to the needs of vehicular users while overcoming the limitations of existing PKIs. However, there are still a number of questions to be answered since the adoption of such a (distributed) secure and privacy-preserving architecture, based on trusted computing, is not straightforward. For instance, what operational functions is it reasonable to place within the "*trusted world*" of a TC without compromising the overall performance? It is our strong belief that if these challenges are tackled now while such approaches are at an early stage, then this emerging security and privacy-preserving mechanism can reach its full potential.

## 8 ACKNOWLEDGMENT

This work was supported by the European Commission, under the ASTRID and FutureTPM projects; Grant Agreements no. 786922 and 779391, respectively.

## REFERENCES

[1] L. Chunli and T. L. Fang, "The Application Mode in Urban Transportation Management Based on Internet of Things," in *Proceedings of the 2nd International Conference on Electric Technology and Civil Engineering (ICETCE)*, May 2012.

[2] PRESERVE, "Preparing secure V2X communication systems," 2011, https://preserve-project.eu/ [Online; accessed 26-August-2017].

[3] Z. Xiong, H. Sheng, W. Rong, and D. E. Cooper, "Intelligent transportation systems for smart cities: a progress review," *Science China Information Sciences*, 2012.

[4] S. Gisdakis, T. Giannetsos, and P. Papadimitratos, "SPPEAR: Security & Privacy-preserving Architecture for Participatory-sensing Applications," in *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless &#38; Mobile Networks*, ser. WiSec '14. New York, NY, USA: ACM, 2014, pp. 39–50.

[5] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proceedings of the 7th International Conference on Pervasive Computing*, ser. Pervasive '09. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 390–397.

[6] "Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats," Technical Specification, October 2017.

[7] ETSI, "Trust and Privacy Management," 2012, http://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.01.01_60/ts_102941v010101p.pdf [Online; accessed 26-August-2017].

[8] L. Gollan and C. Meinel, "Digital Signatures For Automobiles?!" in *Proceedings of Systemics, Cybernetics and Informatics (SCI)*, July 2002, pp. 1–5.

[9] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 228–255, 2015.

[10] S. Gisdakis, M. Lagana, T. Giannetsos, and P. Papadimitratos, "SEROSA: service oriented security architecture for vehicular communications," in *VNC*. IEEE, 2013, pp. 111–118.

[11] M. Gerlach, "Assessing and Improving Privacy in VANETs," in *Proceedings of the 4th Workshop on Embedded Security in Cars (ESCAR)*, 2006.

[12] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *2013 IEEE Vehicular Networking Conference ((VNC'13)*, Dec 2013, pp. 1–8.

[13] T. Kosch, C. J. Adler, S. Eichler, C. Schroth, and M. Strassberger, "The scalability problem of vehicular ad hoc networks and how to solve it," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 22–28, October 2006.

[14] T. Lee, C. Pappas, P. Szalachowski, and A. Perrig, "Towards Sustainable Evolution for the TLS Public-Key Infrastructure," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18, 2018, pp. 637–649.

[15] 5GPPP, "5g Automotive Vision," 2015.

[16] J. Whitefield, L. Chen, T. Giannetsos, S. Schneider, and H. Treharne, "Privacy-enhanced capabilities for VANETs using direct anonymous attestation," in *2017 IEEE Vehicular Networking Conference (VNC)*, Nov 2017, pp. 123–130.

[17] E. F. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation," in *ACM Conference on Computer and Communications Security, CCS*, 2004.

[18] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on Intersection Collision Avoidance systems," in *2013 IEEE Vehicular Networking Conference*, Dec 2013, pp. 71–78.

[19] "Processing personal data in the context of C-ITS," Document, March 2017.

[20] "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility," COM(2016) 766 final, November 2016.

[21] "Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS)," Document, October 2017.

[22] F. Schaub, Z. Ma, and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," in *2009 International Conference on Computational Science and Engineering*, vol. 3, Aug 2009, pp. 139–145.

[23] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems, First International Workshop, IPTPS*, 2002.

[24] M. Khodaei and P. Papadimitratos, "The key to intelligent transportation: Identity and credential management in vehicular communication systems," *IEEE Vehicular Technology Magazine*, vol. 10, no. 4, pp. 63–69, Dec 2015.

[25] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J. Hubaux, "Secure vehicular communication systems: design and architecture," *IEEE Communications Magazine*, vol. 46, no. 11, 2008.

[26] B. Weyl, O. Henniger, A. Ruddle, H. Seudié, M. Wolf, and T. Wollinger, "Securing vehicular on-board IT systems: The EVITA Project," in *proceedings of the 25th Joint VDI/VW Automotive Security Conference*, Ingolstadt, Germany, Oct. 2009.

[27] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for Secure and Private Vehicular Communications," in *IEEE International Conference on ITS Telecommunications (ITST)*, Sophia Antipolis, France, June 2007, pp. 1–6.

[28] PRECIOSA, "PRivacy Enabled Capability In Cooperative Systems and Safety Applications - D1," Nov. 2009. [Online]. Available: http://www.preciosa-project.org/

[29] "Security requirements of vehicle security architecture," Tech. Rep., June 2011.

[30] M. Wolf and T. Gendrullis, "Design, implementation, and evaluation of a vehicular hardware security module," in *Proceedings of the 14th International Conference on Information Security and Cryptology*, ser. ICISC'11, 2012, pp. 302–318.

[31] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.

[32] "Intelligent Transport Systems (ITS); Security; Security Services and Architecture," Technical Specification, September 2010.

[33] M. Moser, D. Estor, M. Minzlaff, A. Weimerskirch, and L. Wolleschensky, "Operating a Car-to-X PKI - Challenges for Security and Privacy," in *FISITA World Automotive Congress*, June 2014.

[34] S. S. Wu, R. V. Sabett, D. S. Chokhani, D. W. S. Ford, and C. C. R. Merrill, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," RFC 3647, Nov. 2003.

[35] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough," in *Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, Feb 2010, pp. 176–183.

[36] M. E. Nowatkowski, J. E. Wolfgang, C. McManus, and H. L. Owen, "The effects of limited lifetime pseudonyms on certificate revocation list size in VANETS," in *Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon)*, March 2010, pp. 380–383.

[37] M. Zhao, J. Walker, and C.-C. Wang, "Security challenges for the intelligent transportation system," in *Security of Internet of Things*, ser. SecurIT '12, 2012.

[38] B. Edelman, "Adverse Selection in Online 'Trust' Certifications and Search Results," in *Electronic Commerce Research and Applications 10*, 2011, pp. 17–25.

[39] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, "Efficient certificate revocation list organization and distribution," *IEEE J.Sel. A. Commun.*, vol. 29, no. 3, pp. 595–604, Mar. 2011.

[40] Trusted Computing Group, "Trusted Platform Module (TPM) | Trusted Computing Group (TPM)," https://trustedcomputinggroup.org/work-groups/trusted-platform-module/ [Online; accessed 26-August-2017].

[41] J. Winter, "Trusted Computing Building Blocks for Embedded Linux-based ARM Trustzone Platforms," in *Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing*, ser. STC '08, 2008, pp. 21–30.

[42] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*. Springer Publishing Company, Incorporated, 2013.

[43] J. Camenisch, M. Drijvers, and A. Lehmann, "Anonymous Attestation with Subverted TPMs," in *Advances in Cryptology - CRYPTO 2017*, 2017, pp. 427–461.

[44] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on computing*, 1989.

[45] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl, "REWIRE – Revocation Without Resolution: A Privacy-Friendly Revocation Mechanism for Vehicular Ad-Hoc Networks," in *Trust and Trustworthy Computing*, 2015.