Comparative Evaluation of PKI and DAA-based Architectures for V2X Communication Security

Anna Angelogianni*, Ioannis Krontiris†, Thanassis Giannetsos∓
*Department of Digital Systems, University of Piraeus, Greece
†Huawei Technologies Duesseldorf GmbH, Munich, Germany
∓Ubitech Ltd., Digital Security & Trusted Computing Group, Greece
Email: annaaggelogianni@ssl-unipi.gr, ioannis.krontiris@huawei.com, agiannetsos@ubitech.eu

***Abstract*—The emerging Cooperative Intelligent Transportation Systems (C-ITS) landscape is expanding in terms of security and trust requirements, to provide the necessary enablers for the safety of critical operations (i.e., collision avoidance). To this extend, Public Key Infrastructure (PKIs) and Direct Anonymous Attestation (DAA) schemes have been proposed by the literature, in order to provide authenticity over the exchanged messages. DAA schemes can help address several challenges of centralized PKIs by offering a more scalable solution for pseudonym certificate issuance, reloading and revocation. This paper is the first to implement a DAA-based solution and then perform a methodological comparison of the two schemes based on an experimental evaluation. The acquired results do not directly dictate one prevailing solution, but rather suggest the need for an integrated approach converging concepts from both schemes, in order to better accommodate the needs of future C-ITS systems.**

I. Introduction

Connected vehicles, as part of the emerging Cooperative Intelligent Transportation Systems (C-ITS) are positioned to transform the future of mobility. This change is enabled by the vehicle's communication with other entities (V2X). V2X communication systems are expected to greatly improve road safety and traffic control efficiency, while better supporting autonomous driving. V2X can also save lives by providing road hazard warnings to the driver, hence reduce collisions [1]. Many challenges though need to be overcome with *security* and *privacy* being at the forefront; especially in the context of safety applications where critical decisions are taken.

The use of digital certificates was suggested very early on, to authenticate messages in vehicular communications, thus prevent an attacker from injecting false messages. However, there is a need to protect privacy as well. Many V2X applications rely on broadcasting continuous and detailed location information, as for example, through Cooperative Awareness Messages (CAM), which are broadcasted unencrypted by vehicles at the (default) frequency of 10 Hz [2]. If this information is misused (by eavesdropping) this could lead to the extraction of detailed location profiles of vehicles and path tracking. Since there is usually a strong correlation between a vehicle and its owner [3], location traces of vehicles have the potential to reveal the movement and activities of their drivers. Addressing this challenge, current approaches are based on PKI-based solutions [4] with privacy-friendly authentication services through the use of short-term *pseudonyms* [5]. 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. Hence, the location privacy is protected by requiring that each vehicle uses multiple pseudonyms, that are frequently updated [4].

The use of changing pseudonyms can be considered the state-of-the-art in C-ITS privacy-enhancing technologies like the one that was recently proposed in [6]. Prominent solutions include the Security Credential Management System (SCMS) [6], which is a product of vehicle OEM consortia and the US Department of Transport (USDOT), the Cooperative-ITS Certificate Management System (CCMS) developed by the European Committee for Standardisation (CEN) and European Telecommunications Standards Institute (ETSI), with support from the European Commission [7] and the Chinese C-SCMS developed by CCSA [8]. These architectures have several inherent drawbacks, though, stemming from the fact that they are based on a complex and centralized ecosystem of PKI entities. Given that these pseudonyms, along with their certificates, must be changed periodically for privacy, vehicles need to ensure that there are always valid certificates available, which implies a need to periodically connect to the back-end and retrieve sets of valid certificates that cover the time beyond the immediate period. Nevertheless, vehicles can neither store a large number of certificates nor do they have frequent connectivity to the back-end. The big scale of C-ITS systems also make revocation schemes inefficient, for example in terms of certificate revocation list (CRL) size and distribution.

To address the aforementioned challenges of centralized PKI solutions in C-ITS, several researchers have suggested moving towards a decentralized approach, where trust is shifted from the back-end infrastructure to the vehicle itself [9]–[11]. As it has been shown by recent work, one way to do this is by leveraging the use of Direct Anonymous Attestation (DAA) and the incorporation of trusted computing technologies [9], [10], [12]. DAA, originally introduced by Brickell, Camenisch, and Chen [13], is a cryptographic protocol designed primarily to enhance user privacy within the remote attestation process of computing platforms, which has been adopted by the Trusted Computing Group (TCG) [14], in its latest specification. Applying the DAA protocols for securing V2X communication results in the removal of most of the PKI infrastructure entities,

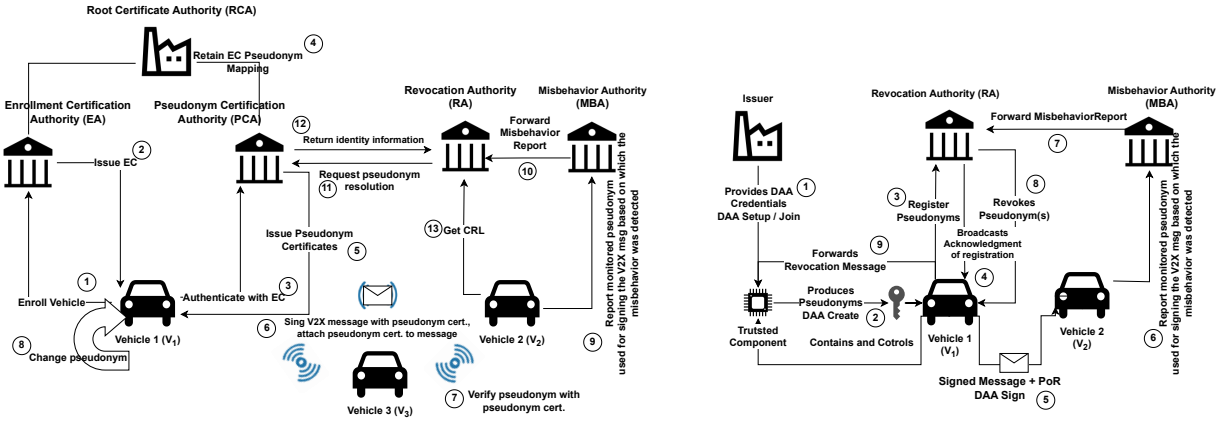

Fig. 1. V2X Security Management Systems based on (a) PKIs vs. (b) Direct Anonymous Attestation

including the pseudonym certificate authority: vehicles can now create their own pseudonym certificates using an in-vehicle trusted computing component (TC), and DAA signatures are used as credentials to create pseudonyms that are verifiable by all recipients, providing privacy too. Furthermore, a DAA-based model supports a more efficient revocation of misbehaving vehicles that does not require the use of CRLs, removing, therefore, all the computational and communication overhead that comes with it [11]. Instead, when the Revocation Authority (RA) issues a revocation request, this triggers the TC of the misbehaving vehicle to delete all of its pseudonymous certificates and cryptographic key pairs, thus, rendering the TC unable to generate new pseudonyms in the future.

However, all the above have not yet been compared through an experimental evaluation so far. From the side of PKI-based solutions, some implementations and evaluations exist, notably from the EU Project PRESERVE [15]. Kotsi et al. [16] give a thorough overview of the different C-ITS deployment projects and implementations in Europe and USA. From the side of DAA-based solutions, none has been demonstrated in the context of C-ITS so far, and their feasibility remain an open question. As a consequence, there is a lack of a comprehensive comparison of both of these approaches in order to advance the current discussions of advantages and limitations between centralized and decentralized security configurations.

Contribution: In this paper, we are the first to provide a full implementation of a DAA-based solution for safeguarding the broadcast communication of messages in the V2X realm. We leverage the detailed protocol description published previously [11], and in what follows we focus more on demonstrating its feasibility and evaluating experimentally all core DAA features and functionalities, including crtificate (pseudonym) revocation capabilities. At the same time, we put forth the first complete analysis between DAA-enabled and PKI-enabled security configurations. The findings throughout the experiments prove that our novel DAA-based architecture overcomes a series of shortcomings of the conventional centralized solutions in terms of scalability and computational footprint and suggest the need to move towards more integrated solutions converging concepts from both approaches, in order to better accommodate the needs of future C-ITS.

II. Credential Management in V2X

A. The PKI Approach

Public Key Infrastructures (PKIs) are currently the prominent solution in order to guarantee security and privacy in the overall C-ITS ecosystem, and they have been already standardized in US [6], Europe [7] and China [8]. What is common in all of these approaches is that a set of Certification Authorities (CAs) that manage the lifecycle of credentials in the system. Hammi et al. recently published a comprehensive survey of existing PKI architectures in C-ITS [17]. In the general case, there is a set of different authorities with distinct roles (see Figure 1 (a)): The Root Certification Authority (RCA) is the top main trust anchor of the PKI, responsible for issuing certificates to sub-CAs. The certificate of the RCA is self-signed, or, if multiple RCAs are used, each RCA cross certify other RCAs. The Enrolment Certification Authority (ECA) is responsible for registering vehicles and issuing long-term certificates. The Pseudonym Certification Authority (PCA) is responsible for verifying the identity of ITS stations and then issue and provide pseudonym certificates to those who have been enrolled to the ECA. Finally, the Revocation Authority (RA) is responsible for issuing revocation lists applying to various certificates when a misbehavior has been detected by the Misbehavior Authority (MBA).

While intensive research efforts have proven the security and privacy guarantees provided in such PKI-based security configurations [18], there are still a number of challenges that have not been addressed sufficiently [9].

Separation of Duties. PKI architectures envisage a technical and organizational separation of duties between different PKI authorities to cope with internal attackers, ensuring that "no single entity" in the architecture can track a vehicle across space and time, unless it colludes with one or more entities. However, since it would be a costly solution to realize this, in practice it is not precluded that multiple authorities, operating these entities, are under the same organizational

umbrella. For example, USDOT describes removal of certain separations of SCMS functions, which may now reside in the same organization, while the responsibility is passed to the SCMS Manager to decide on the rules for governance/policy of separation. However, it is clear that removing the "no single entity" constraint does weaken the privacy protection, and hence may increase the risk of vehicle tracking.

Certificate Reloading. A fundamental restriction of PKIs for C-ITS stems from the fact that vehicles need to acquire pseudonym certificates by connecting to the back-end. On one side, connectivity cannot always be assumed and on the other side, under no circumstances should a vehicle run out of valid certificates, preventing it from sending messages altogether. So the solution is to store larger sets of certificates in advance. For example SCMS [6] and the 5GCAR D4.1 document [19] describe the idea of storing 3-years worth of certificates up front. However longer term storage of certificates complicates things in terms of memory storage but also in terms of revocation of vehicles from the system. Assuming more frequent connectivity, one could reduce this period to, e.g., few weeks and reload the next set of certificates well before the currently stored sets are exhausted. However, the trade-offs still remain and there is still not a clear way to manage the certificates usage period, change rules, and reloading mechanisms.

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 (emphrequiring pseudonym resolution), which would increase the bandwidth requirement to a non-practical level.

More specifically, when it comes to revocation of pseudonym certificates, the CCMS [7] follows a passive approach and simply denies further allocation of certificates to a revoked vehicle at the time when the vehicle attempts to obtain additional ones from the certificate management system. This allows evicted vehicles to continue communication as long as their pool of certificates is not exhausted (which can be weeks or even months). The SCMS [6] supports active revocation of pseudonym certificates. Active revocation means that the certificate management system revokes the pseudonym certificates of a vehicle by issuing a Certificate Revocation List (CRL). Considering the drawbacks of CRL in an ITS environment, linkage-based revocation is adopted by the USDOT ITS standard to reduce the CRL size to just one key size for each vehicle in CRL. However, it is still far from ideal due to the volume of registered vehicles, the strict restrictions on signature processing [20] and efficient CRL distribution [18].

B. The DAA Approach: Converting Vehicles into Security-Hardened Platforms

In order to address these shortcomings, there is an increasing effort by researchers to explore decentralized solutions, capable of shifting trust from the back-end infrastructure to the edge (i.e., vehicles), in order to reduce the vector of entities for which we want to make sound statements in terms of their configuration, security settings and trustworthiness. For example, there are well known solutions based on privacy Attribute Based Credentials (Privacy-ABCs) adjusted to the C-ITS case, e.g. [21], [22]. More recent work started investigating the use of trusted computing to transfer the root of trust inside the vehicle and also leverage the power of anonymous credentials through the use of advanced cryptographic primitives such as Direct Anonymous Attestation (DAA) [10], [23].

DAA [23] is a platform authentication mechanism that enables the provision of privacy-preserving and accountable authentication services. It is based on group signatures that give strong anonymity guarantees. Whitefield et al. [10] first applied this attestation enabler to the V2X case and showed how to enable vehicles to manage their own pseudonym certificates. Larsen et al further enhanced DAA for V2X in terms of *security, privacy, scalability* and *revocation* capabilities [11]. Most notably, one of the biggest advantages of applying the DAA protocol is the redundancy (and removal) of a number of authorities, such as the Pseudonym Certification Authority; vehicles can now create their own pseudonyms, and DAA signatures are used to self-certify each such credential. This allows vehicles to have better control over their privacy, since no trusted third-party is involved in the pseudonym creation phase. It also reduces the communication overhead and connectivity dependencies, since there is no need for frequent communication with the back-end for renewing certificates.

Figure 1 (b) depicts the underpinnings of the DAA pseudonym lifecycle architecture. As we can see, only two trusted third-parties are introduced; (*i*) the Issuer that is responsible for authenticating vehicles through the JOIN protocol, and (*ii*) the RA that shuns out misbehaving vehicles from the ITS. In our implementation, vehicles are the combination of a *host*, which is a vehicular on-board computer "normal world", and a Trusted Component (TC)[1] that operates in the "secure world"; together they form the vehicle platform.

Using DAA, the TC in the vehicle is responsible for creating the pseudonym certificates without involving any infrastructure component from the back-end (Step 1 - DAA CREATE), thus, overcoming limitations of PKI-based solutions as it pertains to *pseudonym provision and reloading*. Only the Issuer knows the identity of a vehicle which is the equivalent of the RCA. During the DAA SETUP and JOIN phases, the Issuer verifies that the TC is valid and provides credentials that can be later used for creating either linked or unlinked pseudonyms; this is decided by the vehicle itself (DAA CREATE phase). Unlinkable pseudonyms enable the provision of *unconditional*

[1]In our current protocol instantiation, we have considered the use of a Trusted Platform module (TPM) as the underlying RoT

anonymity, a property that is not provided by other proposed decentralized security management frameworks [12]. The credentials do not contain any personal identifying information. The signing key of the underlying TC is not linked to the vehicle, and it is certified blindly by the Issuer making it infeasible for any verifying vehicle to link the pseudonym back to the identity of the TC and, thus, the vehicle's long-term EC.

Another key difference with traditional PKI-based solutions is the provision of a more efficient revocation process beyond the use of CRLs. The vehicle cannot use pseudonyms unless they have been registered with the RA (Step 2 - DAA JOIN). The registration consists of providing the RA with unique values that can be used later to either revoke the key or the self-issued short-term anonymous credential keys (DAA SETUP). These values are shared as *revocation hashes* so as to ensure that the RA cannot breach the vehicle's unlinkability when different pseudonyms are used for signing V2X messages. These hashes only represent the configuration registers of the underlying TC where the respective pseudonyms are been stored and act as a *key restriction usage policy*: The TC will not allow the use of a pseudonym key unless it has been activated (Proof of Registration has been received by the RA - Step 3) and has not been revoked (configuration registers hold the activation or revocation hash of each pseudonym). This allows for both *soft* and *hard* revocation without the need to completely de-anonymize the target vehicle and without the limitations of CRL distribution. Soft revocation follows the more passive approach where only the reported pseudonym is revoked while hard revocation leads to more active measures including the revocation of all pseudonyms and keys associated with a specific vehicle [12].

III. On the Performance Evaluation of Vehicular PKI- & DAA-based Solutions

The followed evaluation methodology focuses on the experimental evaluation of the computational complexity and analyze the timings of the core phases of both approaches, as described in the previous sections. We divide the operations into two classes - (1) *offline* and *online*. All operations which can be either pre-computed or not need to be executed in real-time are classified as offline; i.e., the key creation and pseudonym self-issuance in the DAA scheme or the pseudonym acquisition in the context of a PKI-based security configuration. The operations which need to be performed in real-time are classified as online. These include computations that may affect the host vehicle's operational profile including all crypto calculations (i.e., sign, verify) that take place either at the host level of the vehicle or by the underlying TC (for also supporting revocation activities when needed). The endmost goal is to determine how computationally expensive each of these sets of offline and online operations is and analyze their impact on the overall resources of a vehicle. The properties [P] of interest, along with their metrics [M], are summarized as:

[P1] The creation, signature, verification and secure management of V2X messages. This is one of the most crucial properties when using short-range broadcast technologies for enabling the secure enactment of safety-critical applications without breaching the privacy of the vehicles and subsequently their drivers. To provide this security enabler, messages need to be signed by leveraging crypto primitives that can safeguard their anonymity, unlinkability and untraceability. However, the verification of such complex signatures can also have an effect on the computational profile of the receiving vehicle and, thus, in the operation and decision process of on-boarded safety-critical CCAM services. To study the impact of this type of crypto operations, we have employed the ***number of signatures and verifications that can be performed, per second*** **[M1]**, so that these integrity safeguards do not affect the safety logic of the overall C-ITS. The standards (including ETSI) have identified specific values regarding the desired number of crypto operations that a vehicle should be able to perform, so as to not affect the safety profile of the vehicle [24]. Towards this direction and to further examine the impact of possible hurdles and delays, created by the underlying network and its constrains, the ***end-to-end (E2E) latency*** **[M2]** is also considered. That is, we measure the total time needed from the point that a message is generated (at the message vhicle source tranmission) until it is processed and verified at the receiving vehicle. This includes the time needed for the transmission and any delays occurred by (for instance) queuing messages because of the low transmission rate.

[P2] Pseudonym Reloading. Pseudonyms need to be frequently updated which, in the case of a PKI-based solution, dictates the need for the PCA to be able to handle a large number of (concurrent) requests per second so as to ensure that all requesting vehicles have access to valid pseudonyms at any point in time. To evaluate this functionality, we first measure the time required to serve a single request for a varying number of pseudonyms and then study the overall time needed for handling multiple pseudonym issuances. The time to handle one operation includes the following steps: (1) the vehicle first contacts the PCA and receives an authentication request; (2) it then authenticates itself to the ECA and receives and anonymized authentication token (Step 2 in Fig. 1 (a)); (3) it provides this *anonymous* assertion back to the PCA (Step 3) and; finally, (4) sends the pseudonym signing request and acquires the new pseudonymous certificates from the PCA (Step 5). So the overhead is measured in terms of the overall time needed to respond to a ***pseudonym request*** **[M3]**.

[P3] The revocation of a vehicle's pseudonymous credentials. The last property of interest includes the evaluation of the actual revocation mechanism of the vehicle's pseudonyms. Here the focus is on the timing measurements of the operations executed by the PCA, the ECA, and the RA for a single *pseudonym resolution and revocation*, with respect to the number of already revoked pseudonyms. Consequently, the important metric here is the ***revocation execution time*** **[M4]**.

A. Messages Exchanged and Testbed Setup

All experiments were conducted in a testbed, considering a realistic V2X environment, emulating a high number of

vehicles. Each vehicle was simulated by a NexCom box (currently used as an in-vehicle computing unit in various deployments) with the following characteristics: OS: Voyage Linux; Processor Type: Intel Atom D510; Processor Speed: 1660 MHz; Physical Cores: 2; Memory Type: DDR2 667/800. In terms of the experimental evaluation of PKI-related operations, the NexCom boxes were loaded with the OpenSSL crypto library to support crypto operations, such as ECDSA signatures, while for the enactment of the DAA-based security solution, NexCom boxes were equipped with a Trusted Platform Module (TPM) as the underlying Root-of-Trust.

To capture the same connectivity profiles, as in the context of an actual CCAM service, we opted to use an actual *V2X Communication Stack*, following the 802.11p short term wireless protocol standard, as implemented by the EU PRESERVE project [15]. This Communication Stack offers access to the standardized *structure of V2X messages* as defined by ETSI, (i.e., CAM and DENM messages), as well as the actual *bandwidth usage* (i.e., number of bytes allocated to each part of the payload including those for the security headers). The *pseudonym communication profile* considered, is also aligned with ETSI standards, which propose: (i) the TIG profile which is TCP over IPv6 over G5 and (ii) the TI3G profile which is again TCP over IPv6 but over GN6ASL over GN over G5. We have employed the first profile for our experiments.

Furthermore, in order to validate realistic scenarios, thus, providing pragmatic timing measurements considering also *network delays* that might occur, apart from metrics for a single vehicles' operations and calculations, the testbed was also configured to emulate a road segment comprising *multiple transmitting vehicles* (i.e., 1, 5 and 15) and a receiving vehicle. Set of vehicles was simulated by the NexCom boxes, in order to emulate different message rates. To better evaluate the scalability of both (PKI and DAA) approaches, each NexCom box was bootstrapping multiple instances of the V2X Communication stack, thus, simulating a high volume of message transmissions originating from different (simulated) message transmission sources. This enabled the experimentation with more that 10 (simulated) vehicles and yielded results on how varying message rates can impact the critical operations of the overall C-ITS. The *incoming load* of each receiver was set at 5, 50, 100 and 500 msg/s respectively, while the messages were broadcasted at a frequency of 1, 10, 20 and 100Hz, focusing the evaluation on both the default rate as defined in standards (i.e., 10 Hz as defined in [2]) and beyond.

B. Experimental Results

*1) **M1**:* Regarding metric **[M1]**, the PKI approach leverages the OpenSSL library and the ECDSA scheme, to evaluate the time needed for executing the sign and verify operations. Measurements were collected for both 32-bit and 64-bit systems, leveraging the pseudonyms (i.e., ephemeral keys) retrieved by a vehicle from the PCA. For the DAA approach, which is based on the use of ECC, focus was placed on the time needed to perform crypto operations by the underlying TPM once pseudonyms were self-issued. The extracted results are summarized in Table I: Overall, as can be seen, both *sign* and *verify* calculations are rather fast in PKI-based approaches, consuming less than 10 ms, hence allowing for a high number of verifications per second (close to what the OEMs require). This is to be expected as all calculations are performed in software executed by the vehicle's on-board unit, thus, enabling fast executions in systems with available resources. For instance, the time consumed in 64-bit architectures is even less (3.9 ms). It should be noted, though, that these results demonstrate a single signature and verification without taking into consideration possible delays that can be imposed by the communication protocol itself. To also capture this scenario, a vehicle's behavior when receiving varying number of messages (from different sources) was also considered so as to better evaluate the impact of the V2X communication stack in the overall process. As depicted in Figure 2, for high message rates ($> 50msg/sec$), the internal queuing message of the V2X Communication stack adds a significant burden which negates the performance benefits of SW-executed crypto operations, thus, leading to comparable results with the DAA approach with more resource-intensive crypto operations.

TABLE I
SIGN AND VERIFY TIME IN PKI AND DAA WITH ECDSA AND ECC [M1]

Setup #	(ms)	SD
PKI OpenSSL (32bit) Sign	7.1	0.01
PKI OpenSSL (64bit) Sign	3.9	0.01
PKI OpenSSL (32bit) Verify	7.9	0.01
PKI OpenSSL (64bit) Verify	2.8	0.01
DAA Sign	177.3	20.0
DAA Verify AK Credential	155.2	15.5
DAA Verify Signature	**185.1**	17.8

For the DAA, at a first glance, one may deduce that sign and verify operations are significantly more time-consuming (i.e., 177.3 ms for sign and 185.1 ms for verify). Nevertheless, it should be clarified, that our experiment considers the use of a different pseudonym for each signing operation which, in turn, requires the continuous scrutiny (by the TPM) of each key (i.e., pseudonym) against the defined key restriction usage policies so as to make sure that the target pseudonym has not been revoked. This means that the pseudonym is validated, locally, before each sign operation. During *verification*, the message sent to the receiving node includes the signature (constructed under the used pseudonym) along with the (anonymized) DAA credential for enhancing the vehicles' privacy. Thus, to correctly verify the received message integrity, one has to consider both the verification of the signature but also of the associated credential so as to make sure that the pseudonym used also belongs to the same vehicle as the one created the DAA credential. This adds to the complexity of the verification process with one additional integrity check (Table I).

*2) **M2**:* Metric **[M2]** is evaluated considering an environment with a single receiver and multiple senders (i.e., 5 senders), transmitting at different rates (i.e., 5, 50, 100 and 500 msg/s). The time needed to verify all signatures from the neighbouring vehicles is assessed in the receiver's side, to discover the possible delays caused by the receiver's load. The results for both the PKI and DAA approaches are depicted in

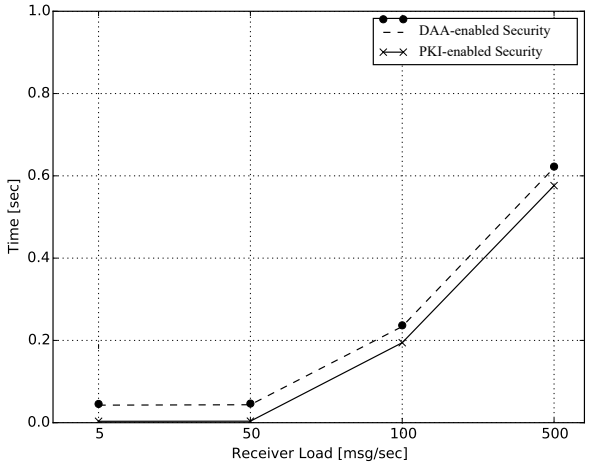

Fig. 2. E2E Network Latency [M2]

Figure 2: The E2E network latency introduced by the DAA scheme is slightly higher compared to the one introduced by the PKI. However, what becomes evident is the convergence of the latency values as a result of the constraints posed by the V2X Communication Stack in the rate that it can process transmitted messages. Hence, the design choice to integrate an actual V2X Communication Stack in order to better evaluate the impact of both the network processing and crypto operations on the overall decision process. Both schemes almost require the same amount of time for the support of the respective crypto operations as additional evidence on the applicability of the DAA scheme compared to the currently standardized PKI approach.

*3) **M3**:* Metric **[M3]** is evaluated for PKIs based on a request to the PCA to issue a number N of new pseudonym certificates. This number is explored for 1000, 2000, 3000, 4000, 5000, 6000, 7000, 8000, 9000 and 10000 pseudonyms, to observe the time consumption. The time is measured not only for the creation of the pseudonyms, but also for the authentication of the vehicle, in order to request pseudonym issuance. PKI adheres to a linear trajectory regarding the number of pseudonyms certificates that can be exported by the PCA, in a single request, as illustrated in Figure 3.

The results depicting the DAA related timings for performing the *DAA Pseudonym Creation* are presented in Table II. As we can see, the *Pseudonym Creation* includes both the construction and validation of the DAA Key (with the Issuer), under which the pseudonym leaf keys are generated. This DAA Key is created by executing the *DAA JOIN* and the *DAA CREATE* phases. The *DAA JOIN* certifies and activates the TPM with the Issuer (TPM receives valid Endorsement Credential) so that it can then successfully create the ECC-based DAA Key (DAA CREATE). Most of the time consumed in this process is for the calculation of the appropriate pairings (as part of ECC) and their subsequent communication and validation with the Issuer. However, this operation is executed only once (*offline* operation), during the first activation of

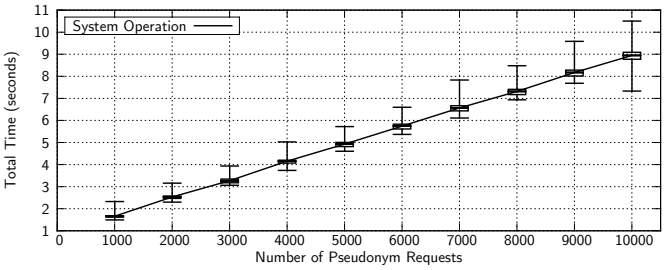

Fig. 3. PKI - Overall time for PCA to respond to a single request [M3]

the vehicle's TC. Consecutive to the creation of the DAA Key, are the *Pseudonym Creation* and *Pseudonym Activation* phases: The focus here is placed on the self-issuance of pseudonyms (by the TPM) as leaf keys of the ECC-based DAA Key so as to provide anonymity and unlikability, as well as, on the registration of pseudonyms with the RA for later usage. The latter allows the RA to keep appropriate records of the pseudonyms, intended for employment in the event of prospective revocation [11]. The *Pseudonyms Activation*, which consumes approximately 6 sec, is referred for contracting 2^{63} pseudonyms, which surpasses by far the requirements of the existing standards and the SCMS. In the same amount of time, the PCA in the PKI system would generate 6000 pseudonyms including the time required for the the processing of the respective request. However, the communication channel remains the bottleneck here, since it wouldn't be possible to transfer all these pseudonyms back to the vehicle in one chunk. This points back to the scalability problem of the centralized approach of PKI, as we pointed out earlier.

*4) **M4**:* Metric **[M4]** focuses on evaluating the time needed for the revocation, including also the time for pseudonym resolution consumed by the PKI entities (i.e., PCA, ECA and RA). During the resolution phase, the entire bunch of pseudonyms, that match the one used to sign the misbehavior report, are acquired and revoked, by adding them in the Certificate Revocation List. According to the protocol's structure, the Revocation List must be signed by both the RA and the PCA, which ultimately breaks the unlinkability dimension of using such short-term anonymous credentials. Furthermore, it is obvious that in PKIs, vehicles should frequently communicate with the RA so as to have an up-to-date Certificate Revocation List. The experiments show that the resolution time reached 320ms per pseudonym, while for the revocation, it reached 550ms per pseudonym (see Table III).

In DAA, the *revocation phase* consists of the vehicle's local operation to verify the status of the reported pseudonym based on the revocation message broadcasted by the RA. This status could be "active" or "revoked". Consequently, a single message is enough for DAA to revoke a pseudonym. In parallel, as aforementioned, in this scheme, two revocation options are proposed: the Soft and the Hard. The first signifies that if a pseudonym is revoked, the de-anonymisation of the rest pseudonyms is not needed, while in the latter, if one pseudonym is revoked, then the rest pseudonyms should also be revoked (Table II). Overall, it can be seen that the

TABLE II
DAA OPERATIONS [M3][M4]

Activity	Mean (HW-TPM)	± (95% CI)
DAA Join	605.70 ms	0.37/0.83 ms
DAA Key Creation	226.23 ms	0.23/0.07 ms
Pseudonym Creation	**8383.50** ms	0.58/0.31 ms
Pseudonym Activation	5951.99 ms	8.38/4.33 ms
Soft (S) Revocation	817.05 ms	0.24/0.10 ms
Hard (H) Revocation	812.25 ms	0.45/0.14 ms

Revocation in DAA is a less time consuming task (approx. 810 ms) compared to PKI (i.e., 550 ms for one pseudonym), since the DAA revokes all vehicle's pseudonyms in a single request, while the pseudonym resolution step is not needed.

IV. Bridging Privacy Management with Trusted Computing to Transform Future V2X

Seeking to improve the secure and privacy-preserving architectures of C-ITS, one has to cater for the open challenges we discussed in the previous sections. A security solution in the C-ITS standards solely based on PKIs may not be adequate for overcoming all of them. This is apparent from the detailed evaluation and computational complexity description, between PKI- and DAA-based security configurations, put forth in Section III and summarized in Table III.

Scalability: The reliance of PKI-based architectures 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 (future) involved stake-holders (e.g., VRUs, MEC as V2X-equipped actors that will play a more "active" role) in automotive applications, this needs for a scalable Web of Trust which can be better supported through a DAA-based architecture. This also reduces the costs for operating (OPEX) the infrastructure.

Trust: The integration of trusted computing technologies, such as the DAA protocol, 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. Analysing the privacy requirements specified in ETSI TS 102 941 and DAA's attributes, 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 and 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.

Efficient Revocation: The revocation service in the DAA-based solution provides strong guarantees of successful completion when a misbehaviour has been identified and reported correctly. 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 with better efficiency - Table II) and the RA can verify revocation messages without compromising the vehicles' privacy. Overall, such a DAA-based configuration avoids several of the shortcomings of the revocation solutions in PKI systems [4], [5], [25].

Furthermore, each vehicle can create pseudonyms on its own and there is no need to communicate with the back end infrastructure. Traditional (centralized) V2X PKI systems like SCMS have limited capacity of supporting up to 300 billion certificates per year for 300 million vehicles. In a decentralized, distributed solution like DAA, there is no upper limit: **Creating pseudonyms is local and very fast and requires no communication overhead.** Even considering the complex revocation process the use of the hard-revocation hash represents a command that sets the hard revocation bit and any other unique combination of bits in the index, allowing for the management of 2^{63} pseudonyms with a unique hard-revocation index; for a single RA domain. To support multiple RA domains in a single index, the number of linked pseudonyms is limited to 2^n where $n$represents the available bit space for each pseudonym set. As the TPM is limited in its internal storage to a minimum of 1600 bytes (for automotive), out of which 12800 bits can be used for managing pseudonyms, considerations should be made to reduce the number of indexes used.

Sybil Attacks: In PKI-based security configurations, vehicles can have multiple certificates valid simultaneously for longer time periods, which enables a malicious node to create multiple fake identities and launch the so-called Sybil attack [6]. There are some proposed detection solutions in the bibliography but they cannot be deployed in current C-ITS.

V. Conclusions

Leveraging widely accepted trusted computing technologies, our solution caters to the needs of vehicular users while overcoming the limitations of existing VPKIs. Applying the DAA protocols for securing V2X communication minimized bandwidth and connectivity requirements due to the redundancy (and removal) of most of the PKI infrastructure entities, including the pseudonym certificate authority: vehicles can now create their own pseudonym certificates using an in-vehicle trusted computing component (TC), and DAA signatures are used to self-certify each such credential that is verifiable by all recipients. Furthermore, a DAA-based model supports a more efficient revocation of misbehaving vehicles that don't require the use of CRLs, removing, therefore all the

TABLE III
COMPARATIVE TABLE OF PKI AND DAA

		PKI	**DAA**
Infrastructure	Required Entities	6 infrastructure entities	2 Infrastructure entities
Signature	Crypto Algorithms	RSA and ECDSA	ECC
	Credential & Signature Size	Signature: 385 bytes Credential: 193 bytes	Signature: 958 bytes (same bsn), 758 (different bsn) Credential: 479 bytes
	Signature Benchmark [M1]	Sign: 7.1 ms (no Pseudonym Validity Check)	DAA SIGN: 177.3 ms (including also Pseudonym Validity Check)
	Signature Verification benchmark [M1]	7.9 ms	10 ms
	Pseudonym Certificate Verification [M3]	55 ms	184 ms
V2X Communication	V2X message Latency [M2]	0.0108 sec (50 msg/sec) 0.594 sec (500 msg/sec)	0.0204 (50 msg/sec) 0.635 (500 msg/sec)
Issuance	Issuance of new Pseudonyms	Remote request (refill) from the PP	Local (self-issuance)
	Pseudonym Key Restriction	Software-based keys	Hardware-based keys
	Size and Issuance Time of new Pseudonyms per Batch [M3]	9 sec (10000 pseudonyms) Increases linearly to the number of pseudonyms	8.3 sec (2^{63} pseudonyms) Constant self-issuance time
Revocation [M4]	Use and distribution of CRLs	Yes	No
	Pseudonym resolution	320 ms (per pseudonym)	No resolution needed
	Support of privacy-preserving revocation for specific certificates	No	Yes
	Vehicle revocation time [M4]	550 ms (per pseudonym) Increases linearly to the number of pseudonyms	approx. 810 ms for both *hard* and *soft* revocation

computational and communication overhead that comes with it. Instead, when the Revocation Authority issues a revocation request, this triggers the TC of the misbehaving vehicle to delete all of its pseudonymous certificates and cryptographic key pairs, thus, rendering the TC unable to generate new pseudonyms in the future.

ACKNOWLEDGMENT

This research has received funding from the European Union's Horizon 2020 EU Research & Innovation program under Grant Agreement No 101069688 (H2020-EU CONNECT).

REFERENCES

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

[2] ETSI, "Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service," EN 302 637-2, September 2014.

[3] P. Golle and K. Partridge, "On the anonymity of home/work location pairs," in *Proc. of the 7th Int. Conf. on Pervasive Computing*, 2009.

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

[5] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Comm. Surveys Tutorials*, 2015.

[6] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A Security Credential Management System for V2X Communications," *IEEE Trans. on Int. Transp. Systems*, 2018.

[7] EU Commission, "Certificate Policy for Deployment and Operation of EU Cooperative Intelligent Transport Systems (C-ITS)," June 2018.

[8] China Communications Standards Association (CCSA), "Technical Requirement of Security Certificate Management System for LTE-based Vehicular Communication," http://www.ccsa.org.cn.

[9] T. Giannetsos and I. Krontiris, "Securing V2X Communications for the Future: Can PKI Systems Offer the Answer?" in *Proc. of the 14th Int. Conf. on Availability, Reliability and Security (ARES '19)*, 2019.

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

[11] B. Larsen, T. Giannetsos, I. Krontiris, and K. Goldman, "Direct Anonymous Attestation on the Road: Efficient and Privacy-Preserving Revocation in C-ITS," in *Proc. of the 14th ACM WiSec)*, 2021.

[12] C. Hicks and F. D. Garcia, "A vehicular DAA scheme for Unlinkable ECDSA pseudonyms in V2X," in *2020 IEEE EuroS&P*, 2020.

[13] E. Brickell, J. Camenisch, and L. Chen, "Direct Anonymous Attestation," in *In Proc. of the 11th ACM CCS*, 2004, p. 132–145.

[14] Trusted Computing Group, "Trusted Computing Platform Alliance (TCPA) main specification," http://www.trustedcomputinggroup.org.

[15] The PRESERVE Consortium, "Deliverable 5.3 - Deployment Issues Report V3," 2013.

[16] A. Kotsi, E. Mitsakis, and D. Tzanis, "Overview of C-ITS Deployment Projects in Europe and USA," in *2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC)*, 2020.

[17] B. Hammi, J.-P. Monteuuis, and J. Petit, "PKIs in C-ITS: Security Functions, Architectures and Projects: A Survey," *Vehicular Communications*, vol. 38, no. C, 2022.

[18] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A survey of security and privacy issues in v2x communication systems," *ACM Comput. Surv.*, 2023.

[19] M. Condoluci, L. Gallo, L. Mussot, A. Kousaridas, P. Spapis, M. Mahlouji, and T. Mahmoodi, "5G V2X System-Level Architecture of 5GCAR Project," *Future Internet*, vol. 11, no. 10, 2019.

[20] E. Verheul, C. Hicks, and F. D. Garcia, "Ifal: Issue first activate later certificates for v2x," in *IEEE EuroS&P*, 2019.

[21] G. Neven, G. Baldini, J. Camenisch, and R. Neisse, "Privacy-Preserving Attribute-Based Credentials in Cooperative Intelligent Transport Systems," in *2017 IEEE VNC*, 2017, pp. 131–138.

[22] A. Singh and H. C. Fhom, "Restricted Usage of Anonymous Credentials in Vehicular Ad Hoc Networks for Misbehavior Detection," *International Journal of Information Security*, vol. 16, no. 2, p. 195–211, April 2017.

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

[24] ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," Technical Specification TS 102 941, June 2012.

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