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 reloading and revocation. This paper is the first to implement a DAA-based solution and then do a methodological comparison of the two schemes side-by-side 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 critical pillars; 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 need to protect privacy as well. Many V2X applications rely on broadcasting continuous and detailed location information, as for example, through the Cooperative Awareness Messages (CAM), which are broadcasted unencrypted by vehicles at the frequency of 10 Hz. 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 [2], 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 [3] with privacy-friendly authentication services through the use of short-term *pseudonyms* [4]. 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 [3].

The 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 [5]. Prominent solutions include the Security Credential Management System (SCMS) [5], 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 [6] and the Chinese C-SCMS developed by CCSA [7]. 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, to retrieve sets of valid certificates, 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 centralised PKI solutions in C-ITS, several researchers have suggested moving towards a decentralised approach, where trust is shifted from the back-end infrastructure to the vehicle itself [8]–[10]. 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 [8], [9], [11]. DAA, originally introduced by Brickell, Camenisch, and Chen [12], 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) [13], in its latest specification. Applying the DAA protocols for securing V2X communication results in the removal of most of the PKI infrastructure entities,

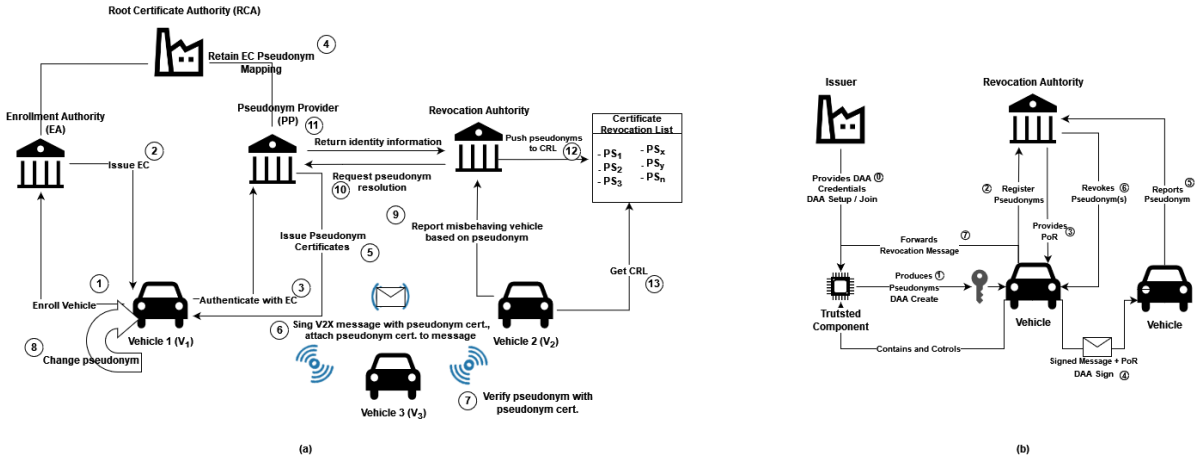

Fig. 1. V2X Security Management Systems based on (a) PKIs vs. (b) Direct Anonymous Attestation

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 don't require the use of CRLs, removing, therefore all the computational and communication overhead that comes with it. 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 be compared and elaborated by an experimental evaluation so far. From the side of PKI-based solutions, some implementations and evaluations exist, notably from the EU Project PRESERVE [14]. Kotsi et al. [15] 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 implemented and 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 (PKI and DAA) in order to advance the current discussions of advantages and limitations between centralized and decentralized security configurations.

In this paper we are the first to provide an implementation of a DAA-based solution for securing broadcast messages in V2X communication. We demonstrate its feasibility and evaluate experimentally of all core DAA features and functionalities, including revocation. At the same time we put forth the first complete analysis between DAA-enabled and PKI-enabled security solution. 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 suggests the need for integrated solutions converging concepts from both approaches, in order to better accommodate the needs of future C-ITS systems.

II. Credential Management in V2X

A. The PKI Approach

PKI is the trusted third-party that guarantees security and privacy for the overall C-ITS ecosystem by managing digital certificates (for vehicle authentication) and cryptographic keys (for data protection through the support of anonymous signatures). Broadly speaking, pseudonym-based schemes are the main privacy preserving mechanism for V2X. In this context, PKIs support two types of certificates: *long-term* (called Enrollment Credentials - EC) and *short-term* pseudonymous credentials (PS_i). A vehicle typically has one EC for authentication to the PKI entities and many pseudonyms (ATs) for signing V2X messages. As mentioned previously, vehicles frequently change of ATs to help against tracking and tracing from both *outsider* and *insider* adversaries and other "honest-but-curious" entities [3].

PKI-based architectures for C-ITS have already been standardized in US [5], Europe [6] and China [7]. What is common in all of these approaches is that a set of Certification Authorities (CAs) provide credentials to the vehicles. In the general case, there is a set of different authorities with distinct roles (see Figure 1 (a)): The Root Certificate Authority (RCA) is the 'trust anchor' of the PKI, responsible for issuing certificates to sub-CAs. The certificate of the RCA is self-signed. The Enrolment Authority (EA) is responsible for registering vehicles and issuing long-term certificates. The Pseudonym Provider (PP) is responsible for issuing certificates that do not contain any identifying information. Finally, the Revocation Authority is responsible for issuing revocation lists applying to various certificates when a misbehavior has been detected.

While intensive research efforts have proven the security and privacy guarantees provided in such PKI-based security configurations [16], there are still a number of challenges that have not been addressed sufficiently [8].

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 that vehicle from sending messages altogether. So the solution is to store larger sets of certificates in advance. For example SCMS [5] and the 5GCAR D4.1 document [17] 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, the CCMS 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 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 [18] and efficient CRL distribution [16].

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

In order to address these shortcomings of PKI-based solutions, there is an increasing effort by researchers to apply trusted computing for self-issuing anonymous credentials as a solution for privacy-respecting V2X communication. Towards this direction, one key argument is that this pressing need for establishing federated trust between services and devices cannot be solely secured with common centralized solutions. 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 (DAA) [9], [19].

1) DAA For Inter-Trustability of V2X Systems with Strong Revocation Capabilities: DAA [19] 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. [9] first applied this attestation enabler to the V2X case and showed how to enable vehicles to manage their own pseudonym certificates. Extending this design, our DAA implementation yields many advantages over state-of-the-art asymmetric pseudonym-based V2X architectures in terms of *security, privacy, scalability* and *revocation* capabilities [10]. Most notably, for the first three properties, one of the biggest advantages of applying the DAA protocol is the redundancy (and removal) of a number of authorities such as the PP; vehicles can now create their own pseudonyms, and DAA signatures are used to self-certify each such credential. 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 our solution. This property also simplifies the message exchange in the context of V2X services as Steps 3, 4, 5, 10 and 11 of Figure 1 (a) are no longer required due to the fact that trust is shifted to the edge points (vehicles).

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 who is responsible for authenticating vehicles through the JOIN pro-

tocol, and (*ii*) the RA, as already exists in current architectures, that shuns out misbehaving vehicles from the ITS. In our implementation, vehicles are the combination of a *host*, that is a vehicular on-board computer "normal world", and a TC[1] that executes in the "secure world"; together they form the vehicle platform. As depicted, the use of pseudonyms for V2X communications follows a similar pattern as in PKI-based architectures, although they differ in the way pseudonyms are introduced and revoked. There are many similarities, demonstrating the feasibility and applicability of such advanced decentralized solutions that can be implemented in compliance to the existing ETSI standards for supporting VC-related specifications for multi-channel wireless and TCP-based communication profiles and V2X message formats and certificates (based on the 1609.2 specification) (Section III-A).

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 anonymity*, a property that is not provided by other proposed decentralized security management frameworks [11]. 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 differentiator 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 due to their size and infrastructure dependencies (need for continuous connectivity). Soft revocation follows the more passive approach where only the reported pseudonym is revoked while hard revocation leads to more active measures of revoking all pseudonyms and keys associated with a specific vehicle. These two variants essentially reflect the current need for *message-based* and *identity-based* revocation [11]: The first scenario might be triggered when revocation needs to occur due to a technical defect of a vehicle; i.e., malfunctioning sensor (thus, we want to temporarily revoke his ability to participate in the system by not allowing it to re-use this specific pseudonym). The second case mainly deals with malicious attackers who need to be banned from any subsequent communication.

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

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

The proposed evaluation scheme examines the effectiveness of the core functionalities supported by both PKI and DAA schemes and offers the benchmarking for their systematic evaluation. It is worth mentioning that the operations that constitute a functionality (i.e., sign), can be divided to *online* and *offline*. The first case, which is our main focus, signifies the execution of operations, in real-time, either on the vehicle's host or the TC (i.e., in DAA), while the second case is linked to pre-computed operations or functionalities that do not need to be executed on real-time. The properties [P] of interest that we are interested, along with their metrics [M], are summarized in the following categories:

[P1] The creation, signature, verification and secure management of V2X messages This is one of the most crucial properties when using short-range broadcast technology, since the secure and privacy-preserving transmission of those messages is the core enabler of the safety-critical applications. To provide this security enablers, messages should be signed. However, this addition could potentially have an effect on the operation and decision process of other safety related CAM services, running in the vehicle. For instance, in collision avoidance scenarios, messages should be verified. 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 security (integrity) enablers do not affect the safety logic of the C-ITS. The standards, including ETSI and the SCMS, have identified specific values regarding how many crypto operations a vehicle should be able to perform, so as to not affect the safety profile of the vehicle [20]. To further examine the impact of possible delays, created by the underlying network and its constrains, the ***end-to-end (E2E) latency*** **[M2]** is considered. That is, we measure the total time needed from the point that a message is generated at the vehicle until it is processed and verified at the receiving vehicle. This includes the time needed for the transmission and any delays occurred by e.g. queuing messages because of the low transmission rate.

[P2] Pseudonym Reloading Pseudonyms need to be frequently updated and hence in the case of PKI, a Pseudonym Provider (PP) should be able to handle a great number of

requests per second from vehicles that need to reload their pseudonym certificates. To evaluate this, we first measure the time required to serve a single request under a varying numbers of pseudonym certificates and then study the overall time needed to handle multiple concurrent requests. The time to handle one request includes the steps: (1) the vehicle contacts the PP and receives the authentication request, (2) authenticates itself to the EA, (3) provides the assertion back to the PP and, finally, (4) sends the pseudonym signing request and receives the new pseudonyms. 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 pseudonym credentials The last property includes the actual revocation mechanism of the vehicle's pseudonym credentials. Here the focus is on the time spent by the PP, the EA, and the RA for a single pseudonym resolution and its revocation, with respect to the number of already revoked pseudonyms. Consequently the important metric here is the ***revocation time*** **[M4]**.

A. Messages Exchanged and Testbed Setup

The testbed considers a V2X environment, containing 10 vehicles, which is mapped to 10 NexCom boxes, 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 *centralized* experiment (PKI), the NexCom boxes leveraged OpenSSL crypto library to support crypto operations, such as ECDSA signatures, while for the *decentralized* part of the evaluation (DAA), NexCom boxes equipped with a TC were employed, to support crypto operations, thus achieve a hardware Root of Trust. To capture the same perception requirements as in the context of an actual CAM service, we have opted to use an actual V2X Communication Stack, following the 802.11p short term wireless protocol standard, as done in PRESERVE [14]. This Communication Stack offers access to the actual *structure of the messages* as defined by ETSI, (i.e., CAM and DENM messages), as well as the actual *bandwidth usage*. The *pseudonym communication profile* for the PKI of our testbed, 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, to produce a realistic setup, thus provide pragmatic measurements regarding the network *overhead*, apart from metrics for a single vehicle, the testbed has provisioned a road segment containing *multiple vehicles* (i.e., 1, 5 and 15) and a receiving vehicle, represented by the NexCom boxes, in order to emulate different massage rates. In this way we investigate whether a certain volume of messages has an impact on the critical operations of the system. The *incoming load* of the receiver is tested for 5, 50, 100 and 500 msg/s respectively, while the messages are broadcasted at a frequency of 1, 10, 20 and 100Hz.

B. Experimental Results

This section presents the experimental results from both PKI and DAA implementations in the NexCom testbed.

1) Results of the PKI implementation: The PKI approach leverages the OpenSSL library and the ECDSA scheme.

Regarding metric **[M1]**, the results we got are summarized on Table I. Measurements were collected for 32bit and 64bit systems, executing the basic sign and verify operations based on the pseudonyms retrieved by a vehicle from the PP. Overall, both operations are rather rapid, consuming less than 10 ms, hence allowing for a number of verifications per second close to what the OEMs require, while the time consumed in 64bit architectures is even less, as expected. It should be noted though, that these results demonstrate a single signature and verification. The vehicle's response for multiple senders was further investigated, excluding the network overhead, to study the impact caused by the increase of participating vehicles. The retrieved results yielded a linear growth, in terms of time consumed for the signature verification, as a result of the increased number of senders and the frequency of the message exchange rate (i.e., 1, 10, 20, 100Hz).

Metric **[M2]** is evaluated considering an environment with a single receiver and multiple senders (i.e., 5 senders), transmitting at a different rate (i.e., 5, 50, 100 and 500 msg/s). More specifically, the time needed to verify all signatures from the neighboring vehicles is assessed in the receiver's side, to discover the possible delays caused by the receiver's load, as described in Figure 2.

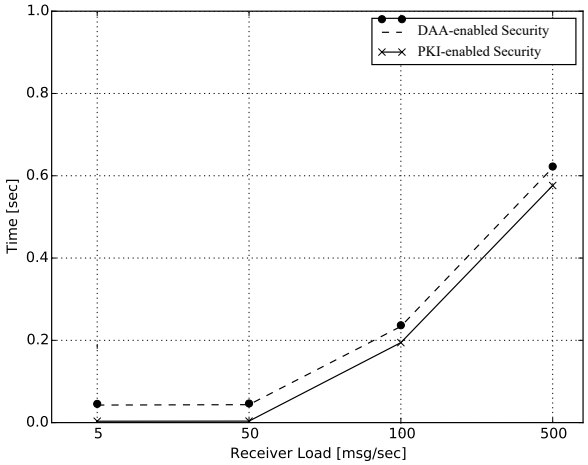

Fig. 2. E2E Network Latency [M2]

Metric **[M3]** is evaluated for a request to the PP for a number of new pseudonym certificates, where we increase the number of requested pseudonyms. We measure the time not only for the creation of the pseudonyms, but also for the authentication of the vehicle in order to request the pseudonyms. The results show that the E2E latency grows linearly with the number of pseudonyms contained in a single request, as illustrated on Figure 3.

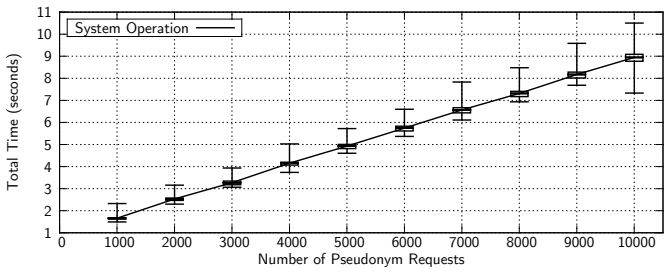

Fig. 3. Pseudonyms in a single request [M3]

Lastly, metric **[M4]** is investigated, to discover the time consumed by the PKI entities (i.e., PP, EA and RA) for a single pseudonym resolution, followed by its revocation. During the resolution phase, the whole bunch of pseudonyms, that match the one used to 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 IdP and the PCA, breaking the unlinkability factor. Obviously, in PKI, vehicles should frequently communicate with the Revocation Authority to request the Certificate Revocation List. The experiments show that the resolution time reached 320ms per pseudonym, while the revocation, reached 550ms.

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	711.35	0.55
DAA Verify AK Credential	155.2	15.5
DAA Verify Signature	185.1	17.8

2) Results of the DAA implementation: To evaluate the DAA-based scheme, focus was placed on: (i) the time needed to perform operations within the TC (i.e. the host platform) and how this affected **[M1],[M3], and [M4]**, and (ii) the E2E network latency **[M2]**.

As it appears on Table I, the *signing* operation **[M1]** in DAA is time consuming. It should be stated though, that our experiment considers the use of a different pseudonym for each signing operation, and the enforcement of key restriction usage policies by the TC, which validate locally the pseudonym before each usage to ensure that it has not been revoked. The *verification* message sent to the receiving node, includes signature with the pseudonym along with the DAA anonymised certificate to verify that the pseudonym is correctly signed with the DAA credential, thus that the DAA credential used originates from a valid TC **[M1]**.

The results depicting the DAA related timings for performing the DAA Pseudonym Creation and the Revocation are presented on Table II. As part of the Pseudonym Creation what needs to be executed is the creation of the DAA Master key, under which the pseudonym leaf keys will be created. This DAA key is created executing the *DAA Join* and the *DAA Key Creation* phase. The *DAA Join* is the first operation executed, taking place in order to certify and activate the TC with the issuer, thus creating the ECC-based DAA Key. Most of the time here is consumed on calculating the pairings in the Elliptic Curve as well as on the communication with the Issuer. Nevertheless, this operation is executed only once during the first activation of the vehicle's TC. The *DAA Key Creation* is a less time consuming task than the DAA Join, while the most time, in this process, is consumed on verifying with the Issuer the correct creation of key, per the existing policies. Furthermore, in the *Pseudonym Creation* and the *Pseudonym Activation* the focus is placed on the creation of the pseudonyms, as leaf keys of the ECC-based DAA Key, to provide anonymity and unlikability, and their registration to the Revocation Authority, so that the latter can keep the appropriate hashes of these pseudonyms, representing the revocation bits to the host vehicle that can be used in the case of future revocation [10]. Note that the Pseudonyms Activation which consumes approximately 6 sec is referred to 2^{63}, which surpasses the requirements of the existing standards. It is evident that significantly more time may be consumed than in the rest DAA operations **[M3]**.

The *revocation phase* is comprised of the vehicle's operation in order to verify with the Revocation Authority the local bits, that represent the state of the pseudonyms (i.e., active or revoked) is correct **[M4]**. In DAA a single message is enough to revoke a pseudonym. In parallel, it must be clarified that, in this scheme, two revocations 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.

Lastly, the E2E latency **[M2]** is evaluated under the same characteristics as in PKI, with a single receiver and multiple senders (i.e., 5 senders), transmitting at a different rate (i.e., 5,50, 100 and 500 msg/s). The goal is to observe the possible delays caused by the receiver's load, as described in Figure 2.

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
Revocation	2037.45 ms	0.73/0.25 ms
Soft (S) Revocation	817.05 ms	0.24/0.10 ms
Hard (H) Revocation	812.25 ms	0.45/0.14 ms

IV. BRIDGING PRIVACY MANAGEMENT WITH TRUSTED COMPUTING TO TRANSFORM FUTURE V2X

Seeking to design successful and secure and privacy-preserving architectures for V2X communication networks, one has to cater for the open challenges we discussed in the previous sections. The issues and gaps we identified, in the context of PKI-based solutions, stem from conflicting and undefined specifications in the standards especially with

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: 185 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 to be revoked	approx. 810 ms for both hard revocation (all vehicle's pseudonyms) and soft revocation (specific set of pseudonyms)

relation to certification management for all comprised entities and stakeholders; i.e., certificate usage period, change rules and reloading mechanisms. System level aspects need further definition, e.g., interworking and trust establishment between multiple authorities and management systems across varying jurisdictions. The security management of new actors including both pedestrians and road-users (VRUs) as well as the addition of localized computational infrastructure entities, represented by the Multi-Access Edge Computing (MEC) layer which envisions to transform V2X into C-V2X (Cellular Vehicle-to-Anything) enabling further the vision of a *service-oriented* vehicular ecosystem, requires strategic rethinking of scalability policies and processes in the context of cyber-security, privacy and trust establishment.

Thus, a security solution in the ITS standards solely based on PKIs may not be adequate for overcoming all the security and privacy challenges of the foreseeable evolution of smart-mobility infrastructures. 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 [3], [4], [21].

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 [5]. There are some proposed detection solutions in the bibliography but they cannot be deployed in current C-ITS systems.

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 DAAbased model supports a more efficient revocation of misbehaving vehicles that don't require the use of CRLs, removing, therefore all the 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 International Conference on Electric Technology and Civil Engineering (ICETCE)*, May 2012.

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

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

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

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

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

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

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

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

[10] 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.

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

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

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

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

[15] 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.

[16] 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.

[17] 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.

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

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

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

[21] 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.