Privacy-Enhanced Capabilities for VANETs using Direct Anonymous Attestation

Jorden Whitefield, Liqun Chen, Thanassis Giannetsos, Steve Schneider and Helen Treharne
Surrey Centre for Cyber Security, University of Surrey, United Kingdom
Email: {j.whitefield, liqun.chen, a.giannetsos, s.schneider, h.treharne}@surrey.ac.uk

***Abstract*—In this paper, we propose a novel secure and privacy-preserving solution for V2X systems leveraging widely accepted trusted computing technologies. Our approach systematically addresses all key aspects, i.e., security, privacy and accountability (revocation). By reflecting on state-of-the-art pseudonym architectures, we identify their limitations focusing on pseudonym re-usage policies and revocation mechanisms. We propose the use of Direct Anonymous Attestation (DAA) algorithms to enhance existing V2X security architectures. The novelty of our proposed solution is its decentralized approach in shifting trust from the infrastructure to vehicles. Applying DAA in V2X enables enhanced privacy protection than is possible in current architectures through user-controlled linkability. The paper presents the incorporation of DAA algorithms within V2X together with rigorous security and privacy arguments.**

***Index Terms*—Security, Privacy, Trusted Computing, Direct Anonymous Attestation, Vehicle-2-X.**

I. Introduction

The rapid growth of Intelligent Transportation Systems (ITS) has embraced a variety of services intended to maximize transport efficiency and increased safety; ranging from collision avoidance and crash notifications to traffic information and infotainment services [1] among others. Vehicular Communications (VC) play a central role in this effort: collecting and communicating large amounts of data among vehicles, road-side units, humans and the surrounding environments.

In order to provide implementations for ITS, many challenges have to be overcome with *security* and *privacy* being critical pillars [2]; especially in the context of safety applications where critical decisions are based on information collected by vehicles regarding their status (e.g., position, speed, etc.) or surrounding events (e.g., traffic jam, icy road, etc.).

Privacy requirements have been well documented in the European Telecommunications Standards Institute (ETSI) TS 102 941 [3], and IEEE Wireless Access in Vehicular Environments (WAVE) [4] standards highlighting the following properties:

- *Anonymity:* ability of a vehicle to use a resource or service without disclosing the user's identity.
- *Pseudonymity:* ability of a vehicle to use a resource or service without disclosing the user's identity while still being accountable for that action.
- *Unlinkability:* ability of a vehicle to make multiple uses of resources or services without others being able to link them together (i.e., infer mobility patterns).
- *Unobservability:* ability of a vehicle to use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

Over recent years, emphasis in secure ITS research has converged on the use of Vehicular Public Key Infrastructures (VPKIs) [5] for credential management and privacy-friendly authentication services through the use of short-term anonymous credentials, i.e., *pseudonyms*. 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. While intensive research efforts have proven the security and privacy guarantees provided in VPKIs, there are still a number of challenges to be conquered [6] [7].

Firstly, it is essential to provide efficient, reliable and in timely and privacy-preserving communications to all vehicles and their embedded sensors. The reliance on infrastructure entities within the overall architecture for such services raises questions towards a system's availability and scalability in the case of a technical fault or attack. Secondly, many researchers have demonstrated the privacy weaknesses of varying pseudonym re-usage policies; even in the case of unconditional anonymity where frequently changing pseudonyms (one per message) has been proposed for a vehicle to avoid being tracked, it has been shown to be ineffective due to the timing information of changing pseudonyms [8]. Thirdly, in the context of revocation policies for removing misbehaving nodes from the network, this can only be achieved when the employed pseudonym scheme supports the resolution of participants' long-term identities from their pseudonyms [9] [10]. In this case, information about the revocation of a vehicle's long-term credentials, is disseminated to other participants through Certificate Revocation Lists (CRLs) or other means. Besides being computationally intensive (i.e., the use of CRLs also assumes enhanced connectivity so that all vehicles can periodically retrieve any updated lists [11]), this is harmful to the protection of their privacy [12].

If we are to fruitfully benefit from the evolution of ITS, all aforementioned challenges need to be resolved while taking into consideration the key technological transformations of the automotive industry, empowered with advanced 5G capabilities [13]. Beyond the adaptation of VC design, new types of secure and privacy-preserving protocols are needed to provide the envisioned level of security and privacy while augmenting the efficiency of the current infrastructure model.

Contributions: In this paper, we propose the use of trusted computing technologies to significantly enhance the state-of-

the-art in security and privacy of V2X. As part of this novel decentralized approach, anonymous credentials are leveraged through the use of Direct Anonymous Attestation (DAA) [14] addressing all the aforementioned aspects and limitations, i.e., privacy, security and accountability (revocation). More specifically, our proposed solution (*i*) is scalable and decentralized removing the need for federated trust of the infrastructure entities in existing V2X architectures, (*ii*) is the first instance (to the best of our knowledge) that applies the DAA algorithms to provide *strong privacy protection* and *user-controlled linkability* without the limitations of current pseudonym schemes, (*iii*) proposes simplified DAA-based versions of pseudonym provision, management, and revocation only requiring a limited set of infrastructure entities, and (*iv*) efficiently removes misbehaving vehicles without revealing the vehicle's identity nor requiring the use of computationally intensive technologies (e.g., CRLs).

Direct Anonymous Attestation is an anonymous digital signature mechanism, where for each signature no entity can discover the signer's identity. However, DAA still has the property that only a legitimate signer (e.g., vehicle) can create a valid signature through the use of trusted computing hardware (e.g., automotive variant of TPM [15]). Under DAA, vehicles will be responsible for generating their own pseudonyms resulting in simplified infrastructure models where there is no need for a dedicated entity to take up this role, as is the case in current VPKIs. DAA algorithms have no ability to create pseudo-linkability between changing pseudonyms making the revocation of misbehaving/malicious vehicles possible.

The remainder of this paper is organized as follows: the current status of vehicular communication systems is discussed in Section II and the primitives of DAA are presented in Section III. Section IV and V comprise the core of this work; they give an insight to the novel DAA-based architecture, the security and privacy-preserving services it offers along with a detailed presentation of all implemented components and protocols. In Section VI, we present a qualitative security and privacy analysis of our scheme and, finally, Section VII concludes the paper.

II. Vehicular Communication Background

Intensive efforts in academia, industry and standardization bodies have spurred a number of European projects. The E-Safety Vehicle Intrusion protected Applications (EVITA) project [16] developed a prototype for securing in-car networks, while the Secure Vehicle Communication (SeVeCom) [17] and Privacy Enabled Capability in Co-operative Systems and Safety Applications (PRECIOSA) [18] projects addressed the complex security and privacy challenges over the wireless channel. Most recent efforts such as the Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) and COmmunication Network VEhicle Global Extension (CONVERGE) [19] projects worked towards the design, implementation, and evaluation of a complete secure and privacy-preserving subsystem that employs a Hardware Security Module.

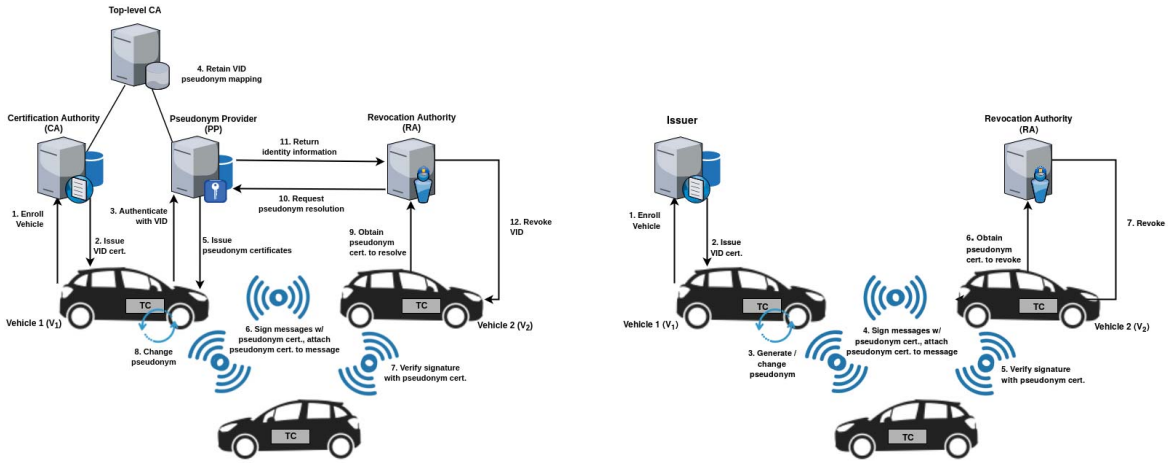
The aforementioned research efforts have proposed the use of pseudonym-based schemes as the main privacy preserving mechanism for VC [10]. The pseudonym lifecycle for existing asymmetric pseudonym protocols follows the pattern that is depicted in Figure 1a. The *infrastructure entities* in such architectures can be broadly classified as Certification Authority (CA), Pseudonym Provider (PP) and Revocation Authority (RA) which are responsible for the provision of services such as authenticated vehicle registration, pseudonym provision and vehicle credentials revocation, respectively. In a nutshell, the CA and PP issue long-term certificates and pseudonym credentials (respectively) to vehicles and implement a resolution mechanism to allow linking back pseudonyms to long-terms IDs (VID)(Steps 1-5). During communication between vehicles, they monitor each other's behaviour, using misbehaviour detection mechanisms, and may issue reports of misbehaving vehicles to the RA (Step 9). The RA, then, makes a decision on whether to revoke reported pseudonyms based on strong evidence [20] [21]. In this case, the RA coordinates with the PP, CA and Top-level CA requesting the resolution of the given pseudonym's long-term identifier (Steps 10-11) which is then disseminated to other vehicles using (for example) CRLs. However, as described in the previous section, such schemes have been shown to suffer from scalability issues [7] [9] and privacy weaknesses of varying pseudonym re-usage and revocation policies [10]; especially against scenarios where the (trusted) authorities collude with each other to link vehicles' actions or completely de-anonymize their identity.

In contrast, our distributed DAA-based approach offers strong security and privacy requirements without the need of a PP since pseudonyms are now created by the vehicles themselves. Using DAA, an in-vehicle trusted computing component (TC) is responsible for creating an unlimited amount of trusted pseudonym certificates without involving any infrastructure component. The proposed approach does not require any type of pseudonym resolution as deterministic signatures (created only by the TC) are used for self-identification by vehicles.

In this line of research, the PUCA architecture [22] was the first one to propose the use of anonymous credentials along with the REWIRE [23] protocol that focused on privacy-preserving revocation. Recent work, however, described how an adversary can intercept a REWIRE revocation message and create a valid confirmation that is sent and accepted by the RA. An enhanced variant was presented in O-TOKEN [24] where an additional key pair is embedded into pseudonym certificates that the RA can use to verify revocation confirmations. Although these works propose a (limited) security and privacy-oriented set of services leveraging trusted computing technologies, in contrast to our solution, they do not provide a comprehensive solution addressing all key VC aspects.

III. An overview of Direct Anonymous Attestation

Direct Anonymous Attestation [14] is a platform authentication mechanism that enables the provision of privacy-preserving and accountable authentication services. DAA is based on group signatures that give strong anonymity guarantees. The key



(a) Asymmetric Pseudonym scheme lifecycle. [10]

(b) DAA Pseudonym scheme lifecycle.

Fig. 1: V2X Architectures

System Actor	*Data Item*	*Description*
Issuer	$sk_I / pk_I := pk(sk_I)$	DAA key pair.
	pk_{ltk} / sk_{ltk}	Long-term key pair.
	K_I	ECC Algorithm security parameters constructed
	pk_I	from the issuers DAA public key and
	pk_{ltk}	long-term public key, hashed.
TC	DAASeed	Unique secret installed at manufacture time.
	cnt	Counter value.
	$sk_{tc} := \texttt{hash}(\texttt{DAASeed} \parallel K_I \parallel cnt)$	Secret DAA key.
	$pk_{tc} := pk(sk_{tc})$	Public DAA key.
	$sk_{ek_{tc}} / pk_{ek_{tc}} := pk(sk_{ek_{tc}})$	TC endorsement key pair.
	$sk_{ps} / pk_{ps} := pk(sk_{ps})$	Pseudonym key pair.
Host	$cre := \texttt{blindSign}(pk_{tc}, sk_I)$	Attestation Identity Credential.
	$ps_{Cert_{tc}}$	Pseudonym
	pk_{ps}	Pseudonym public key.
Verifier	pk_{ps}	A vehicle's pseudonym public key.
	$\texttt{ROGUE}_{sk_{tc}}$	Set of revoked TC keys.
RA	$sk_{ra} / pk_{ra} := pk(sk_{ra})$	RA key pair
	pk_{ps}	A vehicle's pseudonym public key RA wants to revoke.

TABLE I: DAA Security Parameters

security and privacy properties of DAA documented in [25] [26] [27] are:

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

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

In a nutshell, DAA is essentially a two-step process where, firstly, the registration of a TC executes once and during this phase the TC chooses a secret key (SETUP). This secret key is stored in secure storage so that the host cannot have access to it (as we will see in Section VI-A, we assume the possible compromise of the hosts). Next the TC talks to the issuer so that it can provide the necessary guarantees of its validity (JOIN). The issuer then places a signature on the public key, producing the Attestation Identity Credential (AIC) cre. The second step is to use this cre for anonymous attestations on the platform (SIGN), using Zero-Knowledge Proofs [28]. These proofs convince a verifier that a message is signed by some key that was certified by the issuer, without knowledge of the TC's DAA key or cre (VERIFY). Of course, the verifier has to trust that the issuer only issues cres to valid TCs.

IV. MOTIVATION AND DESIGN CHOICES

Our novel DAA solution yields many advantages over state-of-the-art asymmetric pseudonym-based V2X architectures in terms of *security*, *privacy* and *scalability*. Most notably one of the biggest advantages of such a decentralized approach is its scalability, as trust is shifted from the back end infrastructure to vehicles. Applying the DAA protocols results in the redundancy (and removal) of the PP: vehicles can now create their own pseudonyms, and DAA signatures are used to self-certify each such credential that is verifiable by all verifiers. Furthermore, vehicles have total control over their privacy, as no trusted third-party is involved in the pseudonym creation phase. This means that it is infeasible for any third-party to reveal the identity of another vehicle assuring that pseudonym resolution is not possible in 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 1a are no longer required due to the fact that trust is shifted to the edge points (vehicles).

Analysing the privacy requirements specified in ETSI TS 102 941 and DAA's attributes (Sections I and III, respectively),

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

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

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

Effective revocation has been identified as a challenge [10] due to the decentralized nature of vehicular networks and the various pseudonym re-usage and update policies. The revocation service in our model provides strong guarantees of successful completion when a misbehaviour has been identified and reported correctly using existing protocols [20, 21]. This is mainly due to the presence of the TC who is responsible for executing the revocation command, thus, not allowing to be circumvented by a (compromised) vehicle. Secondly, through the use of DAA deterministic signatures and link tokens, revocation under changing pseudonyms is still possible and the RA can verify revocation messages without compromising the vehicles' privacy. Additionally, as demonstrated in REWIRE [23] and O-TOKEN [24], CRLs are not required. This is also true for our architecture since the revocation mechanism triggers the TC to delete all of its secrets, thus, not allowing any subsequent (authorized) communication from the misbehaving vehicle. We have to note, however, that due to the untrusted nature of the host, it can be the case that it may not forward the revocation message to the TC for further processing. As we will elaborate in Section VI-B, the implementation of a "heartbeat" mechanism (similar to the one used for monitoring the status of one-hop vehicular topologies [29]) can provide protection against such malevolent actions. The RA sends out a message every cycle (which is expected to be received by TCs), either a revocation request or a signed and timestamped heartbeat message. TCs will take appropriate action if such messages are not received since this might be an indication of misbehaviour. While there is an overhead incurred by the introduction of this mechanism, it remains substantially lower than the current approaches that use pseudonym CRLs.

V. DAA PSEUDONYM SCHEME

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

We have to highlight that our proposed solution assumes on-board TCs that support (*i*) *isolation*: separate and protected from the host in the event of compromise, (*ii*) *protected execution*: ensures the operation is executed and not interfered with, and (*ii*) *secure storage*: storage which is only accessible by the TC if the vehicle is in a "good" state. Examples of TCs include TPM [15], Intel SGX [30] and ARM TZ [31]. In this paper we do not build our solution around a specific type of TC and we leave this as an implementation detail. For the DAA-based scheme, vehicles are required to have a TC and support the specified functionalities. Furthermore, as an additional implementation detail, we recommend the use of the ECC-based DAA protocol, as this scheme is included in ISO/IEC 20008-2 2:2013 [32]. ECC is more efficient for low-end devices which is appropriate for VCs.

Figure 2 defines the implementation of our DAA protocols. We describe each protocol execution by defining the responsibility of all system actors and separate the roles of the TC and host. This allows us to better reason against the required functionality of a TC. The reader is referred to Table I for fully expanded explanations of the notations contained below.

A. Vehicle Registration

The first step for a vehicle acquiring its certificates consists of two phases: SETUP for generation of keys and the enrollment phase to an Issuer (JOIN). We assume that during manufacture time, the TC will have a unique `DAASeed` installed, a non-monotonic counter cnt, and the hardware will be endorsed by the manufacturer through means of burning the endorsement key pair: $sk_{ek_{tc}}$ / $pk_{ek_{tc}}$ into the TC. For the SETUP phase the

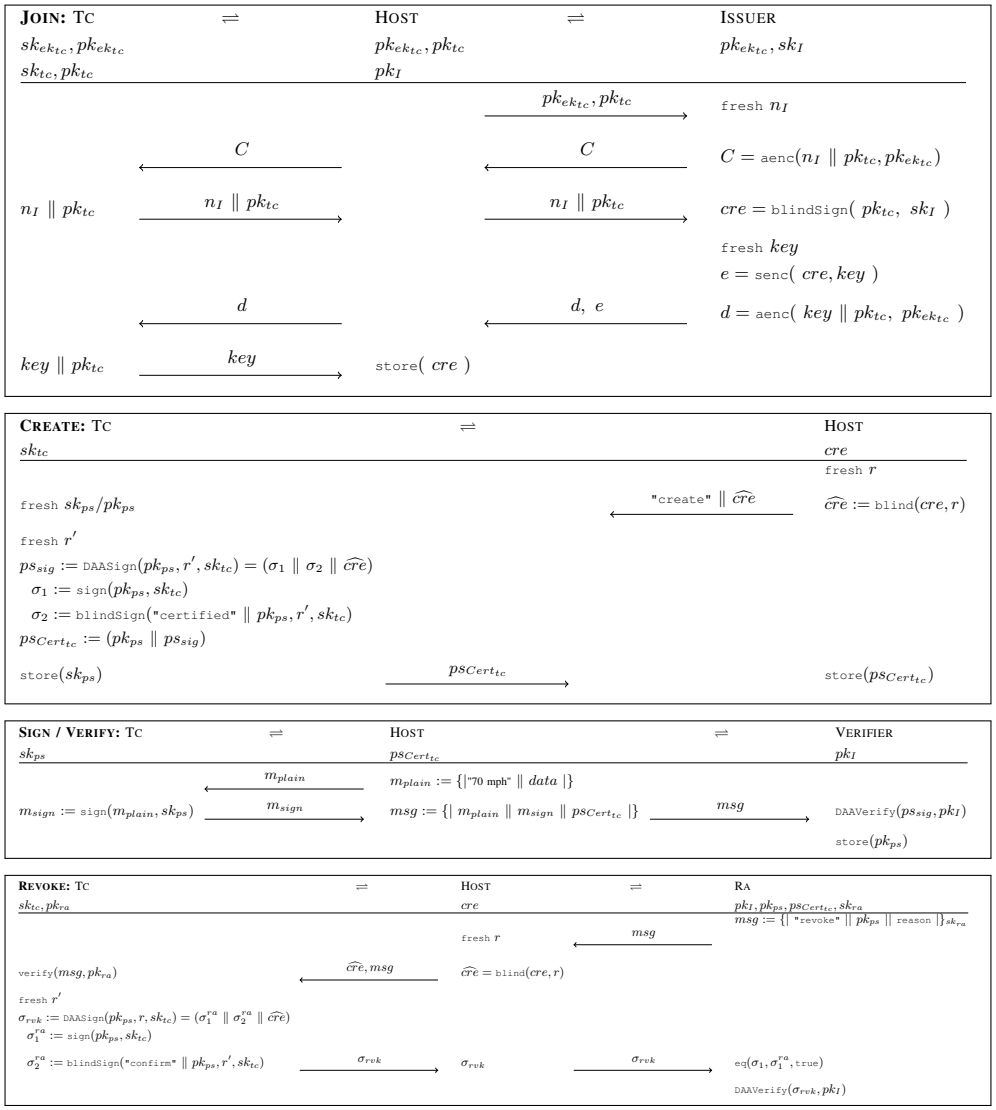


Fig. 2: High-level overview of the V2X DAA protocol interfaces.

issuer publishes its public key pk_I and the security parameters K_I. A vehicle's TC generates a DAA key pair: sk_{tc} / pk_{tc} using K_I, and publishes its public key pk_{tc}. The TC then releases the public keys $pk_{ek_{tc}}$ and pk_{tc} to the vehicle.

The details of the JOIN protocol are shown in Figure 2. By the end of the protocol the vehicle (platform) will have acquired a VID Certificate (cre) certifying that the vehicle has a valid TC which has been enrolled with the Issuer via Steps 1 and 2 of Figure 1b. To initiate the JOIN protocol a vehicle sends the Issuer its public key indicating it wants to join the network (Step 1). The Issuer responds to the vehicle with a fresh challenge C which only the valid TC can open. The vehicle then forwards C to its TC via a secure I/O (Step 2). The TC opens the challenge, confirms its validity, and sends the response to the host vehicle, which in turn, responds to the Issuer with the recovered data items (Step 3). The Issuer verifies the received response, confirming that the vehicle possesses a valid TC. Following this verification, the Issuer creates the credential cre, and a fresh symmetric session key. The credential cre, encrypted with the session key, is sent to the vehicle, along with an encryption of key intended for the TC, as e and d respectively in Step 4. Finally, the vehicle uses the TC to decrypt d, recovering the key. The TC verifies the validity of d and then releases key to the vehicle (step 5). The vehicle can then decrypt e (using key) to recover the certificate cre. Finally, it verifies cre using pk_I and stores it for future use.

By the end of this protocol, if successful, the vehicle is an authenticated and legitimate member of the ITS, and ready to register to any of the ITS' provided services including V2X communication.

B. Pseudonym Creation

The creation of pseudonyms (CREATE in Figure 2) lies within the vehicles, allowing the shift of trust from a third party to locally within the end-points. This is made possible

by all vehicles being equipped with a TC, that is responsible for generating the pseudonyms in an environment that enables protected execution, isolation and secure storage. From Figure 1b we focus on Step 3 of how pseudonyms are created locally exploiting the use of the on-board TC.

Creating new pseudonyms for a vehicle does not require any external network communication, and all message exchanges in the CREATE protocol take place over secure I/O between the host and TC. To initiate the creation process the host blinds the cre with freshly generated random nonces, and sends a "create" request to the TC with $\widehat{cre}$. Alternatively, the vehicle can choose not to "blind" its credential and create pseudonyms which are linkable. While this is bad practice, it does demonstrate that anonymity, pseudonymity, unlinkability and unobservability are under the control of the vehicle. Upon receipt of the pseudonym creation request, the TC creates a fresh pseudonym key pair sk_{ps}/pk_{ps} and fresh random r. Using the `DAASign` algorithm the TC creates two signatures: σ_1 - the public pseudonym key signed with the DAA secret key sk_{tc}, and σ_2 - a blind signature of the certified pk_{ps} key; ensuring the generated pseudonyms are not linkable. σ_1 is a "link token" which is created for the purpose of revocation, discussed in Section V-D. Once the pseudonym signature is produced, ps_{sig}, the pseudonym certificate, $ps_{Cert_{tc}}$, is produced that is constructed from the public pseudonym key pk_{ps} and the pseudonym signature. The TC concludes by storing the generated pseudonym secret key sk_{ps} and returns the pseudonym certificate to the host for use in V2X communication.

By the end of this protocol a vehicle can use its pseudonyms to communicate with the ITS's various services, such that the use of services are anonymous, unlinkable and unobserverable; whilst still being held accountable for its use of the services.

C. V2X Communication

Through the use of DAA SIGN / VERIFY phases, Steps 4, 5 and 6 (from Figure 1b) are achieved by using the already generated pseudonyms. The following protocol details how authenticated message exchanges between ITS services and V2X communication occurs.

To initiate a communication, the vehicle creates a safety message that wants to broadcast to other system participants. In our example, the vehicle creates a plain unsigned message, m_{plain}, stating its speed is "70 mph" and includes binary data information. The TC is given m_{plain} and signs it using the current pseudonym secret key, and responds to the vehicle with a valid signature for m_{plain}. The vehicle then constructs the complete message, msg, to broadcast to its surrounding vehicles. msg is constructed from the plain message, the message signature and the current pseudonym certificate $ps_{Cert_{tc}}$. The surrounding vehicles (VERIFIER) receive msg, and first verify that the contained $ps_{Cert_{tc}}$ was created by a valid TC that has been authorised by the Issuer. To achieve this the verifying vehicle extracts ps_{sig} from the received $ps_{Cert_{tc}}$, and uses `DAAVerify` and the Issuers public key pk_I to confirm the pseudonym was created by a valid TC. The vehicle stores pk_{ps} which uses it to verify that the safety message was signed.

D. Revocation

As aforementioned, one of the most critical services in an ITS is revocation. In our protocol (REVOKE in Figure 2), we demonstrate how this is achieved, using DAA, whilst preserving privacy, and confirmation that the vehicle was revoked. Revocation messages have linkable signatures to guarantee the correct reception of a revocation command by the vehicle in question. Prior to the execution of this protocol, we assume a number of reports containing a misbehaving vehicle's pseudonym have been issued to the RA, and the decision to revoke the vehicle has been made based on strong evidence. Therefore, it is reasonable to assume that before the revocation protocol executes, the RA has knowledge of the Issuer's public key pk_I, the misbehaving vehicles pseudonym $ps_{Cert_{tc}}$ and its public key pk_{ps}.

The RA initiates the REVOKE protocol by creating a signed revocation message msg using its secret key sk_{ra}. It broadcasts msg containing the public pseudonym key, pk_{ps}, that needs to be revoked. All vehicles receive the revocation message since the hosts are required to forward them to their TCs (Section VI-B), and furthermore they generate fresh random nonces and blind the credential producing $\widehat{cre}$ which is again forwarded to their TCs. The TC recognises this message as a revocation request, and verifies that the pseudonym public key was generated by the TC and prepares to respond to the RA. The TC generates some fresh random r, and uses the `DAASign` algorithm to produce the revocation confirmation signatures σ_1^{ra} and σ_2^{ra}. σ_1^{ra} is a deterministic signature that is linkable with σ_1 confirming the revocation is designated for this vehicle. Then, σ_2^{ra} is a signed commitment to confirm that the pseudonym was revoked. As a consequence of σ_{ra} being produced, the TC deletes all pseudonyms and its DAA key pair sk_{tc}/pk_{tc}. The TC responds to the vehicle with the revocation confirmation σ_{rvk}, which is then sent to the RA. Upon reception of the revocation confirmation, the RA verifies that σ_1^{ra} is the same signature as σ_1 from the pseudonym certificate implying that the correct vehicle has revoked itself. The entire signature σ_{rvk} can be verified using `DAAVerify` as being signed by the TC that belongs to the misbehaving vehicle.

By the end of this protocol, there are strong guarantees that the vehicle in question has been revoked without the need of any pseudonym resolution. The RA has verifiable evidence, from the vehicle, that it has performed the revocation enforced by the TC. In the event of a vehicle revocation, it has to re-run the JOIN protocol before being able to re-join the ITS and acquire new credentials.

VI. SECURITY MODEL

In this section, we discuss the proposed DAA-based solution with respect to the achieved security and privacy properties. We consider the following roles within the scope of our analysis to be Vehicles (Users is also considered here), TCs, Verifiers, Issuer and RA.

A. Threat and Adversary Model

Vehicular Communication systems are susceptible to both *outsider* and *insider* adversaries [9] [33]. The former are unauthorized entities (i.e., no credentials or trust relationships with other system entities) that seek to compromise the system and disrupt its operation. In contrast, the primary goal of an insider attacker would be to intercept, block or modify network communications or impersonate a legitimate vehicle (Sybil attack [34]). Assuming that it is impractical to break the cryptographic protocols, the remaining attack vector would be to try and obtain a vehicle's DAA credentials in order to perform a malicious action. An adversary armed with such credentials may also try to extract the identity of the host vehicle. For instance, signatures produced by the compromised DAA credentials could be used to track the vehicle, thus, breaching its privacy, unlinkability and untraceability.

Furthermore, in our context, we are also considering *Honest-But-Curious* (HBC) [12] adversaries who represent legitimate participants (i.e., infrastructure entities and/or vehicles). Their goal is not to disrupt the functionality of the network but to breach a vehicle's privacy. The HBC does not deviate from the defined protocol rules but possibly learns information from legitimate message exchange and information monitoring.

B. Security Analysis

The security assurances rest on the TCs within the vehicles to provide the security guarantees, in particular their possession of an endorsement key embedded at manufacture which only a genuine TC can have. We consider the following key properties.

User-controlled anonymity: The identity of a vehicle (user), using the credentials provided by the CREATE protocol, is not disclosed unless this is dictated by the vehicle itself. In particular, the credentials do not contain any personal identifying information. The signing key of the TC is not linked to the vehicle, and it is certified blindly by the Issuer. Extracting to whom the pseudonym corresponds to is infeasible because the identity of the TC (and hence that of the vehicle) is not linked to its signing key.

User-controlled unlinkability: Unlinkability depicts that linking of subsequent communications (or service requests) originating from the same vehicle is infeasible. In this context, if a vehicle wishes for two communications to be unlinkable then it can do so by using different pseudonyms (hence "user controlled"). The certificate $ps_{Cert_{tc}}$ in the two cases cannot be linked as being associated to the same TC since: (*i*) the public key pk_{ps} is fresh and could have been generated by any TC in each case, (*ii*) the credential $\widehat{cre}$ is freshly blinded in each case, (*iii*) σ_1 by itself is not a verifiable signature, and does not reveal which sk_{tc} was used, or relate to a particular pk_{tc}, and similarly (*iv*) the signatures in σ_2 are blinded.

Non-frameability: This property states that communications from a vehicle cannot be faked or generated by some attacker (or even the Issuer) without the involvement of the vehicle's TC. This is achieved as any message m_{plain} issued by a vehicle is signed by the TC in the $SIGN/VERIFY$ protocol. The signature on m is assured by the credential cre signed by the Issuer (together with $ps_{Cert_{tc}}$) and, therefore, it can only be generated from the associated TC.

Assurance of revocation requests: A TC should only accept genuine revocation requests so as to ensure that attackers cannot arbitrarily revoke vehicles. This property is achieved by including the RA's signature on any revocation message, so that it will not be accepted by the TC as a valid revocation unless the signature is present. Since msg includes the public key of the pseudonym to be revoked, it cannot be reused by an attacker to revoke any other pseudonym.

Assurance of revocation confirmation: A key requirement of the revocation mechanism is to provide strong guarantees that when an RA has initiated and run the protocol to completion, then the associated TC must have been involved in the protocol instance and correctly received the revocation request. It is the TC, as the trusted platform, who is responsible for deleting the pseudonym certificates and no longer using them. In particular, the RA should not reach the point of believing that the revocation has taken place when in fact the TC is unaware of it. This assurance is provided by the TC signing the confirmation against the pseudonym public key pk_{ps} whose revocation is requested, and the RA can verify the TC's signature on that. No other party can create this signature, and TC will only create this confirmation when pk_{ps} is being revoked. Hence, no revocation confirmation can be used by an attacker to spoof a confirmation of any other revocation request.

Assurance of revocation: If a revocation request reaches the TC then it will trigger the process of deleting all generated pseudonym certificates. However, the attacker model also allows a vehicle to block messages intended for the TC, including revocation requests (note that this is also an issue for REWIRE [23] and O-TOKEN [24]). In order for revocation to take effect in this case, the TC needs to detect that this has occurred. This can be achieved by a *heartbeat* mechanism, such that the TC periodically expects either a revocation message or a heartbeat (which may be a revocation intended for some other TC, or else a timed message). Revocation messages and heartbeats include information about the period they are intended for, thus, a heartbeat for one period cannot be used at a different time. They are signed by the RA so they cannot be tampered with or spoofed, and only one message is generated by the RA for each time period. Failure to receive a heartbeat message (or a series of messages so as to allow possible limited connectivity) can act as indication for potential misbehaviour that can also trigger revocation by the TC. In order to improve the safety level provided, this mechanism can make use of the types of heartbeat messages already provided for monitoring the status of one-hop vehicular topologies so as to produce indistinguishable communications and diminish the revocation vulnerability window existing in conventional CRLs [11].

These security arguments with respect to the required properties will benefit from formal modelling and analysis. Work is currently underway formulating the protocols in the TAMARIN protocol verification tool [35], in which properties can be captured as lemmas on the model. Furthermore, a full

blown implementation and evaluation of the system is ongoing to demonstrate its efficiency, practicality and scalability. Various properties are of interest with a particular focus on *pseudonym generation*, *revocation* and *network latency*; the latter can be induced by vehicular mobility so as to better assess the revocation protocol under volatile network connectivity. The goal is to provide strong evidence on the efficient provision of security-related services in vehicular networking environments against existing architectures [9] [36].

VII. Conclusions and Future Work

In this paper, we presented our novel (distributed) DAA pseudonym framework for VC, which provides a comprehensive set of security, privacy and accountability services to V2X systems. Leveraging widely accepted trusted computing technologies, our solution caters to the needs of vehicular users while overcoming the limitations of existing VPKIs. However, there are still a number of questions to be answered since the adoption of such a (distributed) secure and privacy-preserving architecture, based on trusted computing, is not straightforward. For instance, what operational functions is it reasonable to place within the "*trusted world*" of a TC without compromising the overall performance? The same question can be reversed for the context of the "*untrusted world*" provided by a host: what types of services can be placed in this model without compromising the overall security and privacy? These are interesting challenges for future work, where implementation and experimentation will be performed to evaluate the feasibility of the DAA solution, and identify a TC capable of performing the required functionality.

Acknowledgments

Jorden Whitefield is funded by the EPSRC iCASE studentship 15220193 through Thales UK. Thanks also to Adrian Waller and Thales eSecurity Cambridge for detailed feedback, and to the reviewers for their constructive comments.

References

[1] M. Gerla and L. Kleinrock. "Vehicular Networks and the Future of the Mobile Internet". In: *Computer Networks* (2011).

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

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

[4] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Multi-Channel Operation". In: *IEEE Std 1609.4-2016 (Revision of IEEE Std 1609.4-2010)* (2016). DOI: 10.1109/IEEESTD.2016.7435228.

[5] IEEE 1609 WG. *Family of Standards for WAVE*. 2009.

[6] M. Zhao, J. Walker, and C.-C. Wang. "Security Challenges for the Intelligent Transportation System". In: *Security of Internet of Things*. SecurIT '12. 2012.

[7] M. Feiri, J. Petit, and F. Kargl. "Formal model of certificate omission schemes in VANET". In: *IEEE VNC*. 2014.

[8] M. Gerlach and F. Guttler. "Privacy in VANETs using Changing Pseudonyms - Ideal and Real". In: *IEEE Vehicular Technology Conference*. 2007.

[9] S. Gisdakis, M. Lagana, T. Giannetsos, and P. Papadimitratos. "SEROSA: SERvice Oriented Security Architecture for Vehicular Communications". In: *IEEE Vehicular Networking Conference, 2013*.

[10] J. Petit, F. Schaub, M. Feiri, and F. Kargl. "Pseudonym Schemes in Vehicular Networks: A Survey". In: *IEEE Communications Surveys and Tutorials* (2015).

[11] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux. "Efficient Certificate Revocation List Organization and Distribution". In: *IEEE J.Sel. A. Commun.* 29.3 (Mar. 2011), pp. 595–604.

[12] S. Gisdakis, T. Giannetsos, and P. Papadimitratos. "SPPEAR: Security & Privacy-preserving Architecture for Participatory-sensing Applications". In: *ACM*. WiSec '14.

[13] 5GPPP. "5G Automotive Vision". In: *Available online at https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf* (2015).

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

[15] Trusted Computing Group. "Library profile for automotive thin specification, version 1.0". In: *Available online at http://www.trustedcomputinggroup.org/resources/tcg tpm 2.0 library profile for automotivethin* (2015).

[16] B. Weyl et al. "Securing vehicular on-board IT systems: The EVITA Project". In: *VDI/VW Automotive Security Conference*. 2009. URL: http://www.evita-project.org/.

[17] P. Papadimitratos et al. "Architecture for Secure and Private Vehicular Communications". In: *IEEE International Conference on ITS Telecommunications (ITST)*. 2007.

[18] PRECIOSA. *PRivacy Enabled Capability In Cooperative Systems and Safety Applications - D1*. 2009. URL: http://www.preciosa-project.org/.

[19] PRESERVE Project. *Security Requirements of Vehicle Security Architecture*. 2011. URL: http://preserve-project.eu/.

[20] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic. "On Data-Centric Misbehavior Detection in VANETs". In: *2011 IEEE Vehicular Technology Conference (VTC Fall)*. Sept. 2011, pp. 1–5.

[21] R. van der Heijden, S. Dietzel, and F. Kargl. "Misbehavior detection in vehicular ad-hoc networks". In: *Inter-Vehicle Communication (FG-IVC 2013)*. CCS-2013-0. University of Innsbruck, Feb. 2013.

[22] D. Förster, F. Kargl, and H. Löhr. "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks". In: *Ad Hoc Networks* (2016).

[23] 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 2015*.

[24] J. Whitefield et al. "Formal Analysis of V2X Revocation Protocols". In: *Security and Trust Management - 13th International Workshop, STM*. Vol. 10547. Oslo, Norway: Springer, 2017.

[25] E. Brickell, L. Chen, and J. Li. "Simplified security notions of direct anonymous attestation and a concrete scheme from pairings". In: *Int. J. Inf. Sec.* (2009).

[26] J. Camenisch et al. "One TPM to Bind Them All: Fixing TPM 2.0 for Provably Secure Anonymous Attestation". In: *2017 IEEE Symposium on Security and Privacy, SP*.

[27] J. "Camenisch, M. Drijvers, and A. Lehmann. "Anonymous Attestation with Subverted TPMs". In: *"Advances in Cryptology - CRYPTO 2017"*.

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

[29] R. Chen, W. Jin, and A. Regan. "Broadcasting safety information in vehicular networks: issues and approaches". In: *IEEE Network* (2010).

[30] F. McKeen et al. "Innovative instructions and software model for isolated execution". In: *Hardware and Architectural Support for Security and Privacy HASP*. 2013.

[31] ARM. *TrustZone - ARM*. https://www.arm.com/products/security-on-arm/trustzone [Online; accessed 26-August-2017].

[32] ISO. *Information technology – Security techniques – Anonymous digital signatures – Part 2: Mechanisms using a group public key*. ISO 20008-2 2:2013. Int. Organization for Standardization, 2013.

[33] T. Abera et al. "Things, trouble, trust: on building trust in IoT systems". In: *Design Automation Conference, DAC 2016*.

[34] J. R. Douceur. "The Sybil Attack". In: *Peer-to-Peer Systems, First International Workshop, IPTPS*. 2002.

[35] S. Meier, B. Schmidt, C. Cremers, and D. A. Basin. "The TAMARIN Prover for the Symbolic Analysis of Security Protocols". In: *Computer Aided Verification, CAV 2013*.

[36] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. "How to Win the Clonewars: Efficient Periodic N-times Anonymous Authentication". In: CCS '06. ACM, pp. 201–210.