Ad Hoc Networks xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations

A.I. González-Tablas *, A. Alcaide, J.M. de Fuentes, J. Montero

COSEC – UC3M Computer Security Lab: http://www.seg.inf.uc3m.es/, Computer Science and Engineering Department, University Carlos III of Madrid, Avda. de la Universidad, 30, 28911 Leganés, Madrid, Spain

ARTICLE INFO

Article history:
Received 15 October 2012
Received in revised form 19 April 2013
Accepted 20 May 2013
Available online xxxx

Keywords:
Traffic law enforcement
Privacy
Accountability
Vehicular mandatory authorization
Anonymous credential
Privacy attribute-based credential

ABSTRACT

Nowadays, improving road safety is one of the major challenges in developed countries and, to this regard, attaining more effectiveness in the enforcement of road safety policies has become a key target. In particular, enforcing the requirements related to the technical and administrative mandatory documentation of on-the-road motor vehicles is one of the critical issues. The use of modern technologies in the context of Intelligent Transportation Systems (ITS) could enable the design of a more convenient, frequent and effective enforcement system compared to the traditional human patrol controls. In this article we propose a novel system for the on-the-fly verification of mandatory technical and administrative documentation of motor vehicles. Vehicles not complying with the required regulations will be identified and sanctioned whereas those vehicles, observant of the mandatory regulations, will maintain anonymity and non-traceability of their whereabouts. The proposed system is based on the use of anonymous credentials which will be loaded onto the vehicle to automatically and on-the-fly prove holdership of required credentials without requiring the vehicle to stop beside the road. We also implement a prototype of the credential system and analyze the feasibility of our solution in terms of computational cost and time to perform such telematic controls.

1. Introduction

Nowadays, improving road safety is one of the major challenges in developed countries. Effectiveness of road safety policies enforcement is related to the intensity of controls and compliance with safety requirements. Regulating technical and administrative requirements on vehicles (such as registration certificates or mandatory periodic technical inspections) is part of current strategies to achieve a better road safety. Current regulations usually require a vehicle or its keeper to hold five different documents in order to assert its compliance with mandatory requirements: certificate of conformity (or technical characteristics certificate), registration certificate, valid and up-to-date technical inspection report, proofs of up-to-date motor vehicle local tax and compulsory third party insurance payment. However current situation is far away from its solution (e.g., in Spain 400.000 cars were reported of being driven without having passed the mandatory technical inspection in 2009 [1]).

The use of information and communication technologies in vehicular environments has led to a new family of advanced services that have been referred to as Intelligent Transportation Systems (ITS). In this type of systems it is assumed that vehicles count with sensing, processing, and communicating capabilities. Under this assumption, it is possible to build a more convenient, frequent and effective telematic road enforcement system while reducing the number of human patrols deployed to control road stretches. The system will be more convenient because ITS can make possible the telematic on-the-road verification of the documents – that is, without the car needing to stop

* Corresponding author. Tel.: +34 91 624 5957; fax: +34 91 624 9429.
E-mail addresses: aigonzal@inf.uc3m.es (A.I. González-Tablas), aalcaide@inf.uc3m.es (A. Alcaide), jfuentes@inf.uc3m.es (J.M. de Fuentes).

1570-8705/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2013.05.008

and presenting the documents to a traffic agent, provided that a set of equivalent electronic documents are issued. With an ITS-based road enforcement system, the frequency of document inspection can be set as a dynamically configurable parameter, and its possibilities will be mainly limited by the size and availability of the deployed road side infrastructure. The system will be more effective in two ways. Firstly, well-designed electronic credentials will be more difficult to forge than current paper-based ones. Secondly, if such credentials verification is unsatisfactory, a fine could be immediately issued by the Traffic Authority and notified to the offender [2].

Electronic License Plates (ELP) or Electronic Chasis Number (ECN) have already been suggested as long-term electronic identities for vehicles and it is assumed that vehicles will hold a public key certificate linked to that identity [3]. This credential could be understood as an electronic registration certificate.

Therefore, a first solution would consider the issuance of electronic credentials, such as attribute certificates, linked to that long-term identity, that attest each of the remaining mandatory requirements. Nodes of the road side infrastructure could require passing by vehicles to send these credentials and prove their holdership. However, creating such a system raises critical privacy concerns, as it may enable the Traffic Authority or other nearby entities to easily track vehicles and their drivers and know all attributes encoded in the credentials.

In ITS scenarios, the use of a set of pseudonyms has been devised as an alternative mechanism to authenticate vehicles. A public key certificate will be issued for each pseudonym, with a relatively short-term validity period, such as a week, and used only during a short period of time, such as a minute [4]. The certification authority issuing the certificates also serves as an identity escrow agent to satisfy the principle of accountability for malicious vehicle behaviors.

Therefore, a second solution would consider the issuance of attribute certificates linked to each of the pseudonym-based certificates a vehicle holds. Alternatively, instead of issuing attribute certificates for all the pseudonym-based certificates hold by a vehicle, only a specific subset or a separate set of certificates may be considered. However, the most convenient option under this approach would be to issue the pseudonym-based certificates with attribute extensions representing the satisfaction of the mandatory requirements. However, besides the privacy issues arising in pseudonym-based credential systems [5], the main problem of this type of solution is the credential life-cycle management (certificate issuance, revocation, refilling, etc.) of such a huge number of certificates. In the addressed scenario, this problem will be worse as the satisfaction of each mandatory requirement grants an authorization for a different validity period, starting at different times. In the more convenient pseudonym-based setting (certificates with attribute extensions), vehicles will only obtain valid credentials for the period in which all requirements are satisfied. Once the validity period of one requirement expires, vehicles will be forced to retrieve a new set of certificates. Moreover, if the verification of a set of credentials fails because the vehicle does not have valid credentials, it would not be possible to distinguish which requirement is not being fulfilled at the time of detection. Finally, public key and attribute certificates do not operate on the premises of minimal disclosure of information, i.e., when a certificate is shown, all attributes in the certificate are revealed at the same time.

By contrast, an anonymous attribute-based credential system (ABC-system) allows users authentication while guaranteeing partial information disclosure and unlinkability. Attribute-based anonymous credentials are certificates that provide the subject with a digital identity composed by a set of attributes. Users of anonymous credentials are able to prove, to a verifying entity, holdership of the credential, knowledge of all attribute values or that such values satisfy a given property (such as belonging to a range or satisfying a function). Moreover, users can choose to disclose a set of attributes while keeping others hidden (*partial disclosure of information*). Moreover, verifiers cannot link a request with a specific user or with other past requests (*unlinkability*). Finally, anonymous credential systems may allow for credential *revocation* and anonymity revocation (*de-anonymity*) ensuring accountability of misuses and misbehaviors.

Indeed, the privacy by design feature of anonymous credentials make them very attractive and highly suitable for the representation of authorizations required by regulations over motor vehicles. In this work we explore the feasibility of such an approach by proposing a privacy-preserving and accountable telematic on-the-road verification system of motor vehicle authorizations, being these authorizations represented by anonymous attribute-based credentials. To the best of our knowledge, this is the first proposal in the literature addressing this topic.

The main two technologies being currently developed for the implementation of anonymous credentials correspond to U-Prove [6–8] and Idemix [9–11] systems provided by Microsoft and IBM, respectively. Although, both systems present many core-concept similarities, they also differ on many other aspects, namely the mathematical foundations and the functionality features which have actually been implemented. Although our proposal is not based on any of these systems we briefly comment on their main characteristics. As for U-Prove, its current implementation offers the following features: (1) It allows proof of possession of the credential without disclosing the actual credential. (2) It preserves issuance-show unlinkability, this is, the authority issuing the credential cannot link the credential issued with the credential being shown to the verifying entity. (3) It allows partial information disclosure, meaning that when showing the credential, the user can disclose only some of the attributes in the credential, proving to the verifying party that those attributes were certified by the issuer without disclosing the other attributes. By contrast, it does not offer multi-show unlinkability (different uses or shows of the same credential can be linked together) and the user (credential holder) cannot prove that two of its undisclosed attributes hold the same value when being encoded into the same or into two different credentials. Due to the latter two non-implemented features we have not adopted the U-Prove technology.

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

By contrast, Idemix is a much more featured and developed system offering the following interesting functionalities: (1) It allows proof of possession of the credential, (2) it preserves issuance-show unlinkability, (3) it allows partial information disclosure, (4) multi-show unlinkability and, (5) cross-credential proving (attributes encoded in one credential can be proven to hold a =, >=, <=, >, < relation with another attribute encoded in a different credential). However, despite the extra functionalities offered by Idemix, we have not adopted this system either. The intention of this work is to promote an alternative technology to the two major systems. Our work is based on the anonymous credential system presented by Persiano and Visconti in [12], being the main reasons to adopt such an approach the following:

- Persiano et al.'s work is easy to understand and therefore easier to customize and modify.
- Similar features to those (1) to (5) of Idemix can be implemented.
- The showing credential protocol can be made non-interactive.
- Finally, as credential revocation would break the issuance-show property, it stands as the biggest challenge of anonymous credential technologies and not very practical approaches have been adopted for revocation in the two major systems. On one hand Idemix white-listing revocation process, based on accumulators [9], is not really applicable in the vehicular network scenario because of scalability reasons.
  On the other hand, revocation in U-Prove is only possible when untraceability is not a requirement, which is not our case.

The specific contributions of this work are the following ones:

1. We propose an anonymous ABC-system to represent main motor vehicle authorizations required by current regulations. The different parts of the overall system we propose are based on the anonymous credential system presented by Persiano and Visconti in [12] and the work of Camenisch and Stadler in [13]. A vehicle can prove that it holds the required credentials, all linked to the same long-term identity (license number), while guaranteeing minimal disclosure information of the private attributes encoded in the credentials and unlinkability between different credential shows. The system also uses a specific set of pseudonym-based certificates which allows for (1) the retrieval of the identity of vehicles unobservant of mandatory requirements, (2) the collection of non-repudiation evidences of such vehicles, and (3) the revocation of vehicular mandatory authorizations. The use of pseudonym-based certificates to provide these properties allows a smooth integration with current approaches in ITS [4].
2. We have adapted Persiano and Visconti anonymous credential system to make it non-interactive and to allow the validation of multiple credentials held by the same entity and encoding the same private attribute (cross-credential proving).
3. We have implemented the adapted Persiano and Visconti anonymous credential system on a standard PC platform. To the best of the authors' knowledge, it is the first implementation of such a system.
4. We provide with a comprehensive analysis of the fullfilment of the security objectives and of the performance of the proposed system, showing that it is suitable for vehicular scenarios.[1]

After presenting related work and background in Sections 2 and 3, the model of the system is described in Section 4. Next, Section 5 contains a detailed description of the proposed system. The security and performance of the system are analyzed in Sections 6 and 7. Finally, conclusions are presented in Section 8. For completness purposes, Appendix A summarizes the mathematical foundations and assumptions of this work.

2. Related work

Although there is a large body of research work related to the security and privacy in VANETs, very few of them address traffic law enforcement ([14–17]). Most of them are focused in providing privacy-preserving systems (respect to vehicle's identity and location) for Electronic Toll Pricing (ETP), speeding ticketing, and 'Pay-As-You-Drive' (PAYD) systems. But none of these systems addresses the privacy-preserving verification of motor vehicles' mandatory authorizations. Moreover, none of these proposals are based on anonymous credentials systems although [14] suggests that they would be an interesting approach to complement parts of their proposal.

On the other hand, the European Commission (EC) is working on building credentials of motor vehicles and drivers in electronic format and has suggested the use of smart cards as the physical support for driving licenses [18–20]. Such electronic formats may constitute a significant barrier against illegal credential creation and an opportunity to apply new and more efficient enforcement mechanisms. As an example, previous European research project ESCAPE has envisioned a new automated driver identification system based on an electronic driver's license [21]. In Spain, it is already enacted that the vehicle's technical inspection card will be issued in electronic format (although vehicle's owners will still receive a copy in paper format) [22]. However, the options that are being considered to represent these electronic credentials are X.509 public key certificates and plain electronic signatures (such as XMLDSig).

Finally, as one of the contributions of this paper addresses the implementation of an anonymous credential system, several representative recent developments must be considered. Idemix has been already implemented in smart cards (e.g. [23]), also including the selective disclosure feature [24]. Similarly, an implementation of U-Prove on these devices can be found at [25]. Nevertheless, to the

[1] Vehicular platforms are expected to have slightly less computational capacities than standard PCs. However, performance figures on the selected platform can be used to reasonably estimate figures on the vehicular one.

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

best to the authors' knowledge there are no implementations of Persiano and Visconti credential system.

3. Background

In this section, a short introduction to Intelligent Transportation Systems (ITS) and Vehicular Ad-hoc Networks (VANETs) is presented to the reader.

The use of information and communication technologies in vehicular environments has led to a new family of advanced services that have been referred to as Intelligent Transportation Systems (ITS). Thanks to ITSs, drivers can have more immediate and accurate information concerning the road traffic status and passengers can enjoy entertainment applications.

Given that vehicles are moving at a relatively high speed, connectivity is a critical issue in these environments. In order to promote a permanent communication to and from vehicles, a specific type of network (called Vehicular Ad-Hoc Network and usually referred to as VANET) has been proposed.

The usual elements appearing in a VANET scenario are depicted in Fig. 1. Thus, there exists a set of communication nodes placed aside the roads that are called Road-Side Units (RSUs). RSUs are assumed to have a resilient connection with other infrastructure nodes. Trusted Third Parties (TTPs), the road traffic authority or the ITS-related service providers belong to such set of infrastructure entities.

In order to exchange data to and from vehicles, they need to be equipped with specific communication and processing hardware and software. All these components are referred to as On-Board Equipment (OBE) and three main elements are usually considered [26]: first, a set of sensors that enables having a real-time vision of the vehicle status and its surroundings; second, a Hardware Security Module (HSM) which provides with secure storage, reliable time source and cryptographic capabilities; and third, an On-Board Unit (OBU) which is a communication device that enables exchanging data not only with RSUs, but also with other surrounding OBUs. System architectures, such as the one developed within the *SeVeCom* project [4,27], allow the implementation of secure vehicular communication systems.

Given the specific constraints that affect the vehicular data transmission, a new communication technology is being developed. It is commonly referred to as Dedicated Short Range Communications (DSRC) and it is specifically tailored for this context. The whole architecture of DSRC is being standardized in the IEEE 1609 family of standards [28].

4. System model

4.1. Context

We assume that there exists an architecture such as the one described in Section 3. In particular, we assume that vehicles' on-board equipment follows a design and architecture such as the one proposed in [27]. In summary, each vehicle counts with a communication unit (OBU), a hardware security module (HSM) with an internal trusted time source. The HSM stores the vehicle's cryptographic material and allows to operate with it securely.

Furthermore, we assume that vehicles have been issued several credentials as in [4]. Firstly, each vehicle U has a long-term identity ID_U (equivalent to the vehicle's license number). Each long-term identity has associated a key pair (SK_U, PK_U), generated by the HSM, and a set of attributes *atts*. A public key certificate $C_U = Cert(ID_U, PK_U, \textit{long validity period}, \textit{atts})$ is issued by a *CA*.

Secondly, vehicles also generate a set of n short-term key pairs $\left(SK_i^U, P_i^U\right)$ with i from 1 to n) which will be

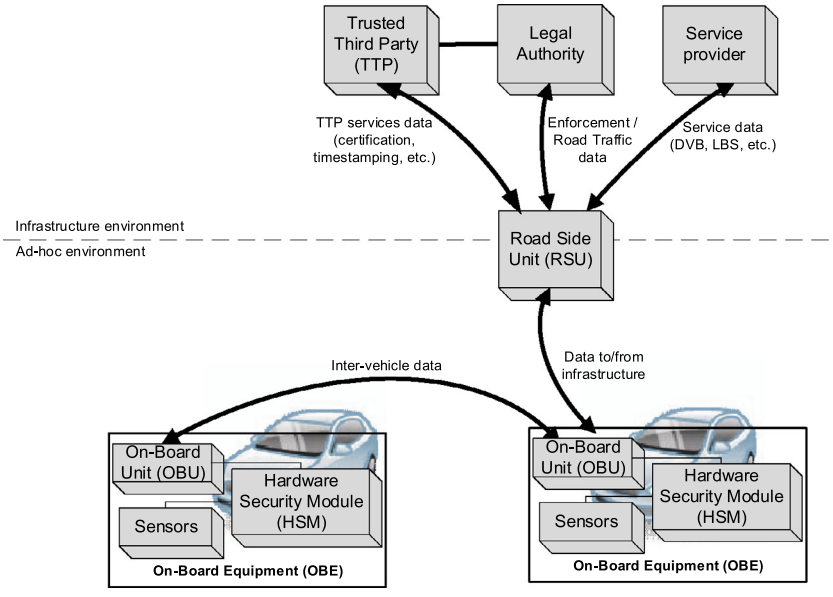

Fig. 1. Usual elements in a vehicular network scenario. (Source: adapted from [29].)

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

Table 1
Notation used in the description of our proposal.

Symbol	Meaning
d	Private RSA exponent such that $3\,d = 1 \bmod \phi(N)$
a *div* e	The whole part resulting of the division of integer a by integer e.
(e,N)	Public RSA key (N is an RSA modulus product of two safe primes)
$\mathbb{Z}_N^*$	Set of co-primes with N
$H(m)$	Result of applying a cryptographic hash function H on message m
$\in_R$	Randomly chosen
$Enc(m,x)$	Encryption of message m with key x
$Sig(m,x)$	Signature of message m with key x
(SK_U, PK_U)	Entity U's long-term key pair
(SK_U^i, PK_U^i)	The ith short-term key pair in $\mathcal{CERT}$ of entity U
$\bar{S}_U^j$	The jth pseudonym in set $\bar{\mathcal{CERT}}$ of entity U
$(\bar{SK}_U^j, \bar{PK}_U^j)$	The jth short-term key pair $\bar{\mathcal{CERT}}$ of entity U for the verification process
sk	Secret derived from entity U's SK_U
(SK_X, PK_X)	Entity X's key pair (with X being V, VC or Adj)

associated to a set of pseudonyms S_U^i. A certification authority CA_P issues a set of pseudonym-based public key certificates:

$$\mathcal{CERT} = \left\{ Cert\left(S_U^i, PK_U^i, short\ \ validity\ period\right) :\ i = 1 \ldots n \right\}$$

From time to time (e.g., a year), vehicles obtain a new set $\mathcal{CERT}$. Vehicles use these certificates to authenticate safety messages over DSRC [30]. A Revocation Authority RA_P publishes periodically Certificate Revocation Lists *CRL* that allow entities to verify the state of a pseudonym-based certificates in $\mathcal{CERT}$.

We also assume the existence of Road Side Units (RSU). RSUs also have an HSM and can communicate with service providers and authorities. We assume that RSUs have an identifier ID_V and a key pair (SK_V, PK_V) that is bound to its identifier by a public key certificate $Cert(ID_V, PK_V, validity\ period)$. Vehicles communicate with each other and with RSUs through a communication network following the IEEE 1609 Family of Standards (WAVE) [28].

Additionally to C_U (long-term public key certificate) and the set $\mathcal{CERT}$ (short-term pseudonym-based public key certificates), we assume that there also exist other agents that are in charge of issuing current motor vehicle paper-based mandatory authorizations or the equivalent (traditional) in electronic form. In particular, we assume that the Traffic Authority *TA* issues vehicle's registration certificates (and fines to misbehaving vehicles), Technical Inspector Agents issue technical inspection certificates, Tax Companies issue proof of payment of local motor vehicle tax, and Insurance Companies provide proofs of compulsory third party insurance payments.

4.2. Equivalent anonymous vehicular credentials

Within our system, equivalent anonymous attribute-based vehicular credentials are generated to substitute the paper-based or electronic non-privacy aware vehicular mandatory authorizations (the registration certificate, the technical inspection certificate, the proof of payment of local motor vehicle tax, and the proof of compulsory third party insurance payments). We denote these four anonymous credentials by AC_A, AC_B, AC_C and AC_D. There exists a Trusted Authority O, responsible for the anonymous credential system setup, and a set of Trusted Authorities O_A, O_B, O_C and O_D, dependant of O and responsible for issuing the credentials AC_A, AC_B, AC_C and AC_D to vehicles. The on-the-fly telematic verification of vehicular mandatory authorizations will consist in the showing of randomized and unlinkable versions of these four anonymous credentials. To allow for credential revocation and de-anonymization, these randomized versions are built using (and associated to) single-use pseudonym-based public key certificates.

Therefore, besides the long-term public key certificate C_U and the set $\mathcal{CERT}$ of pseudonym-based certificates, for each vehicle, an additional set $\bar{\mathcal{CERT}}$ of m pseudonym-based certificates is issued:

$$\bar{\mathcal{CERT}} = \left\{ Cert\left(\bar{S}_U^j, \bar{PK}_U^j, short\ \ validity\ period\right) :\ j = 1 \ldots m \right\}$$

A Certification Authority $\bar{CA}_P$ issues certificates in set $\bar{\mathcal{CERT}}$ and a Revocation Authority $\bar{RA}_P$ periodically publishes Certificate Revocation Lists *CRL* regarding those certificates. These certificates are used by vehicles to create evidence that will allow, if necessary, the retrieval of the vehicle's identity from the credential verification response. Using a set $\bar{\mathcal{CERT}}$, different from set $\mathcal{CERT}$, allows a vehicle to know in advance which is the pseudonym $\bar{S}_U^j$ to be used next in the pre-computation of the necessary data for the telematic verification process (this is not possible if set $\mathcal{CERT}$ is used). Each of the certificates in $\bar{\mathcal{CERT}}$ is used at most once. When they are all used or expired, a new set $\bar{\mathcal{CERT}}$ is issued. The revocation of certificates in $\bar{\mathcal{CERT}}$ conforms the revocation process of the anonymous credential AC_A. The remaining credentials do not need revocation, as explained in Section 4.4.

4.3. System overview

The specific entities that participate in the system are the following ones. Vehicles that are asked to prove their credentials will be denoted as *U*. Other vehicles (denoted by *W*) may participate in the protocol if witnesses' evidences are required. The verifier agents will be denoted by *V* and are assumed to be deployed dynamically and strategically among the set of RSUs (we do not address the details of verifier agents' deployment in this paper). Verifier agents can order an associated videocamera *VC* to take photographs to passing–by vehicles. Videocameras are assumed to be placed relatively close to the RSU where the associated verifier agent is deployed. It is assumed that a secure communication channel exists between *V* and *VC*. In the proposed system verifier agents *V* communicate telematically with specific passing–by vehicles *U* while vehicles are moving. Verification agents *V* may communicate with other entities that form part of the infrastructure. These entities are the Traffic Authority *TA*, an Adjudicator *Adj* and a public repository.

As previously described, we assume that the vehicle has been issued the long-term public key certificate C_U and the

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

set $\mathcal{CERT}$ of pseudonym-based certificates and that all these credentials and their corresponding cryptographic material have been loaded on the vehicle's HSM. Besides, we also assume that the vehicle has the vehicular mandatory authorizations, which may be in a paper-based or electronic format, and that these credentials are under the control of the vehicle's keeper.

Table 1 provides a summary of the used notation throughout the paper.

4.4. Phases

The system we propose consists on the following phases.

1. *Pseudonym-based certificates issuing*. As a result of this phase, certificates of set $\mathcal{CERT}$ are issued and loaded into the vehicle's HSM. Also, the specific application software in charge of the execution of the credential verification protocol in the vehicle, is securely deployed on the vehicle's OBE.
2. *Anonymous credential system setup*. The trusted authority O executes this setup phase to generate a couple of tuples (Pub_O and $Priv_O$) holding all the public and secret global parameters used by the actors of the anonymous credential system. Trusted authorities O_A, O_B, O_C and O_D are assigned a subset of the parameters from the tuples Pub_O and $Priv_O$.
3. *Anonymous credentials issuing*. During this phase, an entity U approaches the corresponding authorities O_A, O_B, O_C and O_D to obtain the corresponding anonymous credentials AC_A, AC_B, AC_C and AC_D. Note that, although we do not address the specific logistic or operational details of how entity U initiates the anonymous credentials issuing process, we suggest that, firstly, entity U should demonstrate to be the authorized holder of the appropriate non-anonymous version of the credentials, either if they are on a paper-based format or on an electronic one. Besides, the process could be designed to be initiated by the vehicle or it could need some previous action or collaboration of the vehicle keeper. For the purposes of this work, anonymous credentials contain two private attributes denoted as x_1, equivalent to ID_U (the long-term identification of the vehicle), and x_2, a secret derived from sk (attribute x_2 is of the form g_2^{sk} where sk is SK_U, entity U's long-term private key, or a secret derived from it); credentials also contain three open-atributes α_3, α_4 and α_5, specifying the first two of them the period of validity of the credential (valid from and not valid after).[2] Note that the validity period of AC_A will be similar to $Cert(ID_U, PK_U, long\ validity\ period, atts)$ but the validity period of AC_B, AC_C and AC_D is expected to be much shorter (one year for AC_C and AC_D, and two to four years for AC_B). These credentials are loaded into the vehicle's HSM.
4. *Anonymous credentials joint proving*. This phase can be further divided in two parts: a first *offline* part and a second *online* part.
   (a) *Offline part*. In the offline part, entity U pre-computes a set of session commitments and follows the steps to construct the results of a series of four non-interactive Zero Knowledge Proof of Knowledges (ZK-PoK-1 to ZK-PoK-4)[3]. For this purpose, U choses a random factor y and uses it to produce randomized versions of each anonymous credential AC_A, AC_B, AC_C and AC_D, using the next available pseudonym S_U^j. Note that the j-th pseudonym will be used only once. The result of the pre-computation of commitments and non-interactive ZK-PoKs will serve to prove the following list of core statements:
      - *ZK-PoK-1*: That the attribute x_1 (private) is common to the four credentials, that U has the knowledge of secret sk encoded in attribute x_2 (private), that the credentials also encode the appropriate open-attributes, and that the correct pseudonym S_U^j has been used to construct the proofs.
      - *ZK-PoK-2*: That commitments are properly constructed.
      - *ZK-PoK-3*: That the credentials AC_A to AC_D encode a valid signature (i.e., authority O_A has signed AC_A and so on).
      - *ZK-PoK-4*: That the vehicle has indeed computed commitments and the previous ZK-PoKs. For this, U must prove knowledge of the random factor y.
   (b) *Online part*. In the online part, entity V selects a passing-by vehicle U which is using a pseudonym S_U^i at that moment for the authentication of DSRC messages [30]. V requests U to prove holdership of its mandatory authorizations. After receiving the request, U sends V a response message, signed with its short-term private key SK_U^j. Besides other data, the response message contains commitments of each credential, and the pre-computed non-interactive ZK-PoK-1 to ZK-PoK-4 over the randomized versions of AC_A to AC_D.

Then, V performs two sets of verifications. Firstly, V assesses the feasibility of retrieving the identity of U from the response message it has sent to V (*identity inspection feasibility*). If it is not feasible, V orders VC to take a photo of passing-by vehicle U. V collects available evidence (the photo and other collected evidence such as acknowledgements sent by surrounding vehicles W taking the approach proposed in [31]) and sends it to adjudicator Adj (so it can take a decision about calling the RSU or the vehicle to revision). Secondly, if the first set of verifications are successful, V proceeds to verify the vehicle's credentials (*credentials validity*). V verifies the revocation status of U's certificate, the correctness of open-attributes, and the four non-interactive ZK-PoKs. If these verifications fail, V

[2] The third open-attribute α_5 is not specifically used in the system proposed herein, although an immediate use would be to encode the vehicle's type, which can be used to enforce policies that restrict the type of vehicles that can be driven depending on the time of the day.

[3] For an explanation of ZK-PoK, see Appendix A.

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

collects available evidence and sends it to the Traffic Authority *TA* (so it can take a decision about a possible *U*'s unobservance and the appropriateness of fining *U*).

5. *Pseudonym-based certificates revocation*. From the set of vehicular mandatory authorizations that a vehicle must hold, we assume that only the registration certificate may need to be revoked online and without physically inspecting the vehicle (e.g., the vehicle has been stolen). It is reasonable to assume that if a technical inspection credential needs to be revoked, the vehicle will be at the inspector premises. Therefore, the corresponding anonymous credential can be deleted or updated. We assume that the proofs of payment of local motor vehicle tax and compulsory third party insurance do not need to be revoked online or offline; they just expire. The revocation of certificates in $\mathcal{CERT}$ is used herein to assess the validity of anonymous credential AC_A and can be understood as a temporal de-registration of the vehicle. Permanent de-registrations will consider the deletion of AC_A.
6. *Pseudonym-based certificates refilling and anonymous credentials update*. From time to time, vehicles will need to refill sets $\mathcal{CERT}$ and $\mathcal{CERT}$. Anonymous credential AC_A persists during the time the vehicle is registered, but anonymous credentials AC_B, AC_C and AC_D expire and need to be updated.

4.5. Security requirements

4.5.1. Correctness

The system works correctly if, when a vehicle *U* fails to prove holdership of the required credentials, its identity can be retrieved and available (and sufficient) evidence is collected in order that a third party can determine whether a fine should be issued (i.e., the vehicle is accountable for driving without appropriate credentials). The system should not be able to fine a vehicle that has correctly executed the credentials proving protocol and counts on valid and up-to-date credentials.

4.5.2. Soundness

Vehicular credentials must be non-transferable and unforgeable. Moreover, an adversary that captures transcripts of protocol executions should not be able to use them to prove holdership of valid credentials.

4.5.3. Privacy

If a vehicle proves holdership of valid and up-to-date credentials when required by a verifier agent, its identity must be preserved and it cannot be traced by the system, in particular, different executions of the protocol between the system and a vehicle cannot be linked by the system.

4.6. Threat model

We assume that the following enitites are trusted to correctly execute the proposed protocol: *TA*, *CA*, CA_P, CA_P, RA_P, RA_P, *Adj* and entity *VC*. Regarding vehicles and RSUs, their HSMs are trusted (cryptographic material cannot be transferred outside of them and it cannot be used by unathorized software). However, OBUs of vehicles and RSUs can be compromised by an adversary (messages can be captured, modified, deleted or inserted). Note that we assume that verifiers *V* do not collude with other verifiers to share transcripts of protocol executions or capture VANET messages of large areas. We also assume that vehicles *W* that act as witness of exchanged messages collaborate in the protocol and, in particular, they do not collude to not send any acknowledgement messages. We consider active adversaries that may have as main interests: (1) to successfully pass an execution of the credentials verification protocol without having valid and up-to-date credentials, (2) to avoid being caught without valid and up-to-date credentials (e.g., another vehicle is fined), and (3) to know the identity of passing-by vehicles (when it should not be disclosed, i.e., vehicle holds valid and up-to-date credentials) or link different protocol executions by the same vehicle.

5. System description

Phases 2, 3 and 4 directly related with the anonymous credential system, and briefly described in Section 4.4, are detailed next. Note that, for the sake of clarity, we describe the phases in detail using only two anonymous credentials AC_A and AC_B (this description can be easily extrapolated to the four anonymous credentials needed in the verification system).

5.1. Anonymous credential system setup

The system setup protocol is based on and inherits the instructions from the protocol `Enroll` presented in [12]. The algorithm is performed by an organization *O* which follows the steps described below.

1. *O* randomly picks two $k-bit$ long safe primes $p_1 = 2q_1 + 1$, $p_2 = 2q_2 + 1$ such that $gcd(3, \phi(p_1p_2)) = 1$, and sets $N = p_1p_2$.
2. Randomly picks $e \in \mathbb{Z}_N$ such that $gcd(e, \phi(N)) = 1$ and $gcd(3, e) = 1$.
3. Computes $d \in \mathbb{Z}_N$ such that $3d \equiv 1 (\mathrm{mod}\ \phi(N))$; (note that the private parameter *d* and public parameter *e* are **not** part of the same key pair).
4. Selects elements $g,\ c \in \mathbb{Z}_N$ of large order.
5. Randomly picks elements v_1, v_2, v_{3_A}, v_{3_B}, v_{4_A}, v_{4_B}, $v_{5_A}, v_{5_B}, v_{6_A}, v_{6_B}$, and sets $g_1 \equiv g^{v_1}, g_2 \equiv g^{v_2}$, $g_{3_A} \equiv g^{v_{3_A}}, g_{3_B} \equiv g^{v_{3_B}}$, $g_{4_A} \equiv g^{v_{4_A}}, g_{4_B} \equiv g^{v_{4_B}}$, $g_{5_A} \equiv g^{v_{5_A}}, g_{5_B} \equiv g^{v_{5_B}}, g_{6_A} \equiv g^{v_{6_A}}, g_{6_B} \equiv g^{v_{6_B}}$ (mod *N*).
6. Computes $s \equiv g^d (\mathrm{mod}\ N)$.
7. Computes a cyclic group *G* of order *N* in which computing the discrete logarithm (DL) is infeasible (e.g., *G* is computed as a subgroup of $\mathbb{Z}_q$ for a prime *q* such that $N|(q-1)$), along with six more elements h_1, h_2, h_3, h_4, h_5, $h_6 \neq 1$ of G.
8. Outputs public information

$$Pub_O = (N, e, q, g, s, c, h_1, h_2, h_3, h_4, h_5, h_6, g_1, g_2, g_{3_A}, g_{4_A}, g_{5_A}, g_{6_A}, g_{3_B}, g_{4_B}, g_{5_B}, g_{6_B})$$

9. Keeps the following private information

$$Priv_O = (p_1, p_2, d, v_1, v_2, v_{3_A}, v_{4_A}, v_{5_A}, v_{6_A}, v_{3_B}, v_{4_B}, v_{5_B}, v_{6_B})$$

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

10. Organizations O_A and O_B are given the corresponding tuples with public and private parameters:

$$Pub_A = (N, e, q, g, s, c, h_1, h_2, h_3, h_4, h_5, h_6, g_1, g_2, g_{3_A}, g_{4_A}, g_{5_A}, g_{6_A})$$

$$Priv_A = (p_1, p_2, d, v_1, v_2, v_{3_A}, v_{4_A}, v_{5_A}, v_{6_A})$$

$$Pub_B = (N, e, q, g, s, c, h_1, h_2, h_3, h_4, h_5, h_6, g_1, g_2, g_{3_B}, g_{4_B}, g_{5_B}, g_{6_B})$$

$$Priv_B = (p_1, p_2, d, v_1, v_2, v_{3_B}, v_{4_B}, v_{5_B}, v_{6_B})$$

5.2. Anonymous credential issuing

In this phase the organization O_A issues an anonymous credential AC_A and organization O_B issues an anonymous credential AC_B for an entity U, both encoding attribute x_1 such that $0 \leqslant x_1 < e$. Note that for simplicity purposes, attribute x_2 is also the same in both credentials (x_2 contains a secret *sk, such that* $0 \leqslant sk < e$, derived from SK_U), however, this secret could be different for each anonymous credential and the proof of its knowledge be performed independently from one credential to another.

The anonymous credential issuing protocol is based on and inherits the instructions from the algorithms `Enroll` and `IssueCred` in [12]. The algorithm is performed first by entity U with organization O_A.

1. Entity U holds two non-privacy aware certificates that share a common attribute x_1 with the same value: $Cert_1 = (x_1, \alpha_3, \alpha_4, \alpha_5)$ and $Cert_2 = (x_1, \beta_3, \beta_4, \beta_5)$. U submits $Cert_1$ together with x_2 to O_A and $Cert_2$ together with x_2 to O_B.
2. The organization O_A verifies the certificate $Cert_1$, in particular, the value of x_1. O_A also verifies that $x_2 = g_2^{sk} \bmod N$, where sk is a secret derived from the user's private key SK_U, and that U knows SK_U so it knows how to derive such a secret. We assume that such algorithm exists.
3. The organization randomly chooses α_6, x_A, such that $0 < \alpha_6 < e$, α_6 co-prime with e and not multiple of 3, and a value $x_A \in \mathbb{Z}_N^*$;
4. The organization sets and computes:
   - $a_A \equiv g_1^{x_1}\ x_2\ g_{3_A}^{\alpha_3}\ g_{4_A}^{\alpha_4}\ g_{5_A}^{\alpha_5}\ g_{6_A}^{\alpha_6} x_A^e \pmod N$
   - $b_A \equiv c \pmod N$
   - $v_A \equiv (a_A + b_A)^d \pmod N$
5. The organization O_A sends the tuple $\langle x_1, x_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, x_A, v_A \rangle$ to U;
6. The entity U verifies the signature $v_A$using the public key 3. The tuple constitutes its anonymous certificate denoted as AC_A.

Similarly, U executes the same protocol with organization O_B. In this case, U obtains from O_B the tuple $\langle x_1, x_2, \beta_3, \beta_4, \beta_5, \beta_6, x_B, v_B \rangle$ as credential AC_B.

5.3. Anonymous credential joint proving

This phase has been briefly described in Section 4.4 and consists on two parts: an *offline* part and an *online* one. For the construction and verification of ZKPoKs, the phase is based on and inherits various instructions from the protocols `ProveCred` and `VerifyCred` in [12]. Such protocols have been adjusted to the new setting (where attributes to be verified belong to two different credentials) according to the work in [13].

Description of the *offline part*:

(1) *Construct commitments.* U constructs a series of commitments in relation to the credentials and stores them in CMT.

U: CMT↤ConstructCMT

(2) *Construct ZK-PoK-1 to ZK-PoK-4.* The prover must then prove knowledge on how those commitments have been constructed. The prover A constructs four different non-interactive ZK-PoKs (*ZK-PoK-1* to *ZK-PoK-4*) and stores them in ZKPoK1, ZKPoK2, ZKPoK3, and ZKPoK4.

U: ZKPoK1↤ConstructZKPoK1
U: ZKPoK2↤ConstructZKPoK2
U: ZKPoK3↤ConstructZKPoK3
U: ZKPoK4↤ConstructZKPoK4

Description of the *online part*:

(1) *Credential proving request.* V selects a vehicle U that is using pseudonym S_U^i. V stores in EVIDV the signed beacon BEACON sent by U. Then, V sends U a request for proving holdership of its credentials and starts a timer.

$V \rightarrow U:\ Enc((cha, t_{request}), PK_U^i), S_U^i,$

$Sig((Enc((cha, t_{request}), PK_U^i), S_U^i), SK_V), Cert(ID_V, PK_V,$ *validity period*)

Other passing-by vehicles W send to V ACKs of having received the request message. V stores them in ACKREQ and adds them to EVIDV.

(2) *Credential proving response.* U stores the received message in REQ, and adds it to EVIDU. U verifies the signature and the certificate. If these verifications are succesful, U retrieves from its local storage CMT, ZKPoK1, ZKPoK2, ZKPoK3, and ZKPoK4 and concatenates all these elements in PRV. U decrypts and verifies correcteness of challenge *cha* and time $t_{request}$, if they are correct U sends back its response.

$U \rightarrow V$: PRV,α_3, α_4, α_5, β_3, β_4, β_5,

$Enc\big((cha, t_{response}, Sig((\text{PRV}, \alpha_3, \alpha_4, \alpha_5, \beta_3, \beta_4, \beta_5, cha, t_{response}), SK_U^j)..,$
$Cert\big(\bar{S}_U^j, \bar{PK}_U^j, short\ \ validity\ period\big)\big), PK_V\big)$

Other passing-by vehicles W send to U ACKs of having received the response message. U stores them in ACKRES and adds them to EVIDU.

(3) *Credential proving response verification.*

Verifications regarding the *identity inspection feasibility*.

(a) If V does not receive U's response within expected time (timer times out), V exits step 3 and executes step 4.

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

(b) *V* stores the response in RES and adds it to EVIDV.
(c) *V* decrypts the challenge, the response time, the signature and the certificate. Then, it verifies the challenge and the signature. If these verifications fail, *V* exits step 3 and executes step 4.
Verifications regarding the *credentials validity*.
(d) *V* verifies the revocation status of the certificate using the last received *CRL*. If this verification fails, *V* adds a reference of the *CRL* to EVIDV, exits step 3 and executes step 5.
(e) *V* verifies the correctnes of the open-attributes sent in the message (i.e. expiry dates). If this step fails, *V* exits step 3 and executes step 5.
(f) *V* retrieves CMT, ZKPoK1, ZKPoK2, ZKPoK3, and ZKPoK4 and performs the following verifications:

`VerifyZKPoK1`(CMT, ZKPoK1)
`VerifyZKPoK2`(CMT, ZKPoK2)
`VerifyZKPoK3`(CMT, ZKPoK3)
`VerifyZKPoK4`(CMT, ZKPoK4)

If any of these verifications fails, *V* exits step 3 and executes step 5.
(g) If previous verifications are succesful, *V* sets *Successful Verification* in Feedback and executes step 6.
(4) *Dispute resolution request*. If ACKREQ $\neq$ *null*, *V* asks *VC* (over a secure channel) to take a photograph of vehicle *U* and *VC* sends back *V* a photo encrypted with entity *Adj*'s public key PK_{Adj}. *V*, after receiving the photo, stores it in ENCPHOTO and adds it to EVIDV.

$V \Rightarrow VC:\ Take\ Photo, cha$
$VC \Rightarrow V:\ Enc(PHOTO, cha, PK_{Adj})$

V sends to *Adj* (over a secure channel) a dispute resolution request containing EVIDV. Then, *Adj* decrypts ENCPHOTO, recognizes *U*'s license number in the photo, and contacts *U* to request evidence EVIDU, if *U* has it, for a time near $t_{request}$.

$Adj \Rightarrow U:\ Evidence\ Request, t_{request}$
$U \Rightarrow Adj:$ EVIDU

Once *Adj* has all available evidence, it resolves if some of the devices need to be called for a revision or some other corrective measure (e.g., for repeated failures). Finally, *V* sets *Dispute Resolution Requested* in Feedback and executes step 6.

(5) *Fine issuance request*. *V* sends to the Traffic Authority *TA* a fine issuance request containing EVIDV. Additionally, *V* sets *Fine Issuance Requested* in Feedback and executes step 6.

$V \Rightarrow TA:\ Fine\ Issuance\ Request$, EVIDV

(6) *Feedback publication*. *V* publishes in a public repository a feedback message to vehicle *U* indicating the result of the verification. *U* may access this repository to check the result of this protocol execution.

$V \rightarrow Repository:\ t_{request}, cha, Enc((\text{Feedback}, S^i_U), PK^i_U), Sig((t_{request}, cha, Enc((\text{Feedback}, S^i_U), PK^i_U)), SK_V)$

5.3.1. Construct commitments (`ConstructCMT`)

The algorithm `ConstructCMT` consists of the following steps:

1. Entity *U* sets the following values for credential AC_A:
   - $a_A = g_1^{x_1}\ x_2\ g_{3_A}^{\alpha_3}\ g_{4_A}^{\alpha_4}\ g_{5_A}^{\alpha_5}\ g_{6_A}^{\alpha_6} x_A^e \pmod N$
   - $b_A \equiv c \bmod N$
   - $m_A \equiv (a_A + b_A) \bmod N$

   U repeats the steps for credential AC_B, obtaining values a_B, b_B and m_B.
2. Entity *U* randomizes the values just set: *U* randomly picks a value *y* such that $0 \leqslant y < e$ and computes for credential AC_A:
   - $a_A \equiv g^y\ a_A \bmod N$
   - $b_A \equiv g^y\ b_A \bmod N$
   - $m_A \equiv g^y\ m_A \bmod N$; thus we have: $m_A - a_A - b_A \equiv 0 \bmod N$
   - $v_A \equiv s^y\ v_A \bmod N$

   U repeats the steps for credential AC_B, obtaining values a_B, b_B, m_B and v_B.
3. *U* computes commitments on the values a_A, b_A and m_A: *U* randomly picks values $\{w_{1_A}, w_{2_A}, w_{3_A}\} \in_R \mathbb{Z}_N$ and computes the following values in *G*:
   - $Com(m_A) = h_1^{m_A}\ h_2^{w_{1_A}} \bmod q$
   - $Com(a_A) = h_3^{a_A}\ h_4^{w_{2_A}} \bmod q$
   - $Com(b_A) = h_5^{b_A}\ h_6^{w_{3_A}} \bmod q$
   - $Com_A = Com(m_A)\ Com(a_A)\ Com(b_A) \bmod q$

   U performs the same steps for values a_B, b_B and m_B, by randomly picking values $\{w_{1_B}, w_{2_B}, w_{3_B}\} \in_R \mathbb{Z}_N$ and computing $Com(m_B)$, $Com(a_B), Com(b_B)$, and Com_B.
4. *U* stores in CMT the values a_A and a_B, and all commitments $Com(m_A)$, $Com(a_A), Com(b_A), Com(m_B)$, $Com(a_B), Com(b_B)$, Com_A, Com_B.

5.3.2. ZK-PoK-1 (`ConstructZKPoK1` and `VerifyZKPoK1`)

Both *U* and *V* execute *ZK-PoK-1* to prove that x_1 encoded in AC_A and x_1 encoded in AC_B are equal. Additionally, the verifier receives non-interactive zero knowledge proof of knowledge that x_2 encrypts *sk* (for simplicity purposes, we assume the same *sk* in both credentials), and that the public attributes α_3, α_4, α_5 and β_3, β_4, β_5 are included in the credentials. Therefore, *U* must prove knowledge of a tuple of secrets $(y, x_1, x_2, \alpha_6, x_A)$ which computes $\hat{a}_A\ g_{3_A}^{-\alpha_3} g_{4_A}^{-\alpha_4} g_{5_A}^{-\alpha_5} \bmod N$ and the tuple of secrets $(y, x_1, x_2, \beta_6, x_B)$ which computes $\hat{a}_B\ g_{3_B}^{-\beta_3} g_{4_B}^{-\beta_4} g_{5_B}^{-\beta_5} \bmod N$. (Note that on the one hand *U* never loses control over neither the anonymous certificates encoding the attributes, nor the private attributes, but only PoKs are realized; on the other hand, the values of the *open* attributes are sent to the verifier during the execution of this protocol).

Steps of algorithm `ConstructZKPoK1` are detailed below:

1. *U* chooses random values r_y, r_1, r_{2_A}, r_{2_B}, r_{6_A}, $r_{6_B} \in_R \mathbb{Z}_e$.
2. *U* chooses random values r_A, $r_B \in_R \mathbb{Z}_N^*$.
3. *U* computes $t_A = g^{r_y}\ g_1^{r_1}\ g_2^{r_{2_A}}\ g_{6_A}^{r_{6_A}}\ r_A^e \bmod N$ and $t_B = g^{r_y}\ g_1^{r_1}\ g_2^{r_{2_B}}\ g_{6_B}^{r_{6_B}}\ r_B^e \bmod N$ as *commitments*.
4. *U* computes $t = H(t_A + S^j_U) \bmod e$ as a *challenge*, where S^j_U is the entity's current pseudonym.

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

5. U computes the following responses:
   - $\rho_y = t\ y + r_y \bmod e$
   - $\rho_1 = t\ x_1 + r_1 \bmod e$
   - $\rho_{2_A} = t\ sk + r_{2_A} \bmod e$
   - $\rho_{6_A} = t\ \alpha_6 + r_{6_A} \bmod e$
   - $\rho_A = g^{(ty+r_y)dive}\ g_1^{(tx_1+r_1)dive} g_{2_A}^{(t\ sk+r_{2_A})dive}\ g_{6_A}^{(t\alpha_6+r_{6_A})dive}\ (x_A)^t r_A \bmod N$

Similarly, U computes the responses ρ_{2_B}, ρ_{6_B} and ρ_B.

6. U stores in ZKPoK1 the responses ρ_y, ρ_1, ρ_{2_A}, ρ_{2_B}, ρ_{6_A}, ρ_{6_B}, ρ_A, ρ_B and the values of t_A and t_B.

When the verifier executes algorithm `VerifyZKPoK1`(CMT, ZKPoK1), it will accept the proof if and only if:
$\left((\hat{a}_A\ g_{3_A}^{-\alpha_3}\ g_{4_A}^{-\alpha_4}\ g_{5_A}^{-\alpha_5})^t\ t_A = g^{\rho_y}\ g_1^{\rho_1}\ g_2^{\rho_{2_A}}\ g_{6_A}^{\rho_{6_A}}\ \rho_A^e\right) \wedge$
$\left((\hat{a}_B\ g_{3_B}^{-\beta_3}\ g_{4_B}^{-\beta_4}\ g_{5_B}^{-\beta_5})^t\ t_B = g^{\rho_y}\ g_1^{\rho_1}\ g_2^{\rho_{2_B}}\ g_{6_B}^{\rho_{6_B}}\ \rho_B^e\right) \bmod N$

5.3.3. ZK-PoK-2(`ConstructZKPoK2` and `VerifyZKPoK2`)

Both entities, U and V, perform the zero knowledge proof of knowledge ZK-PoK-2 to prove that commitments Com_A and Com_B are properly constructed. For this, U must prove, in a zero knowledge fashion, knowledge of the tuple $(m_A, w_{1_A}, a_A, w_{2_A}, b_A, w_{3_A})$, which is a $(G, h_1, h_2, h_3, h_4, h_5, h_6)$-DL representation of Com_A such that $m_A = a_A + b_A$. Similarly, U must prove, in a zero knowledge fashion, knowledge of a the tuple $(m_B, w_{1_B}, a_B, w_{2_B}, b_B, w_{3_B})$, which is a $(G, h_1, h_2, h_3, h_4, h_5, h_6)$-DL representation of Com_B such that $m_B = a_B + b_B$.

The following theorem will mathematically transform the specified proofs into different ones of less complexity:

Theorem 1 (*PoK- 2*). *Proving knowledge of the tuple $(m_A, w_{1_A}, a_A, w_{2_A}, b_A, w_{3_A})$, which is a $(G, h_1, h_2, h_3, h_4, h_5, h_6)$-DL representation of Com_A such that $m_A = a_A + b_A$, is equivalent to proving knowledge of the tuple $(b_A, w_{1_A}, w_{2_A}, w_{3_A})$, which is a $(G, (h_1\ h_5), h_2, h_4, h_6)$-DL representation of $Com_A\ (h_1\ h_3)^{-a_A}$.*

Proof.

$$\left.\begin{array}{l} w_{1_A}, w_{2_A}, w_{3_A} \in_R \mathbb{Z}_N \\ Com_A \stackrel{def}{=} Com(m_A)\ Com(a_A)\ Com(b_A) \\ \quad = h_1^{m_A} h_2^{w_{1_A}}\ h_3^{a_A} h_4^{w_{2_A}}\ h_5^{b_A} h_6^{w_{3_A}} \bmod q \\ m_A = a_A + b_A \end{array}\right\} \Longleftrightarrow$$

$$Com_A = h_1^{a_A+b_A}\ h_2^{w_{1_A}}\ h_3^{a_A}\ h_4^{w_{2_A}}\ h_5^{b_A}\ h_6^{w_{3_A}} \bmod q \Longleftrightarrow$$
$$Com_A\ (h_1\ h_3)^{-a_A} = (h_1\ h_5)^{b_A}\ h_2^{w_{1_A}}\ h_4^{w_{2_A}}\ h_6^{w_{3_A}} \bmod q$$

□

***

Two remarks: (1) Theorem 1 also applies to Com_B and (2) Theorem 1 dictates that to carry out *ZK-PoK-2* the prover U must prove to the verifier V knowledge of a DL-Representation of $Com_A\ (h_1 h_3)^{-a_A}$ and knowledge of a DL-Representation of $Com_B\ (h_1 h_3)^{-a_B}$.

Steps of algorithm `ConstructZKPoK2` are detailed below:

1. U generates $(r_{b_A}, r_{1_A}, r_{2_A}, r_{3_A}) \in_R \mathbb{Z}_q$ for some prime field $\mathbb{Z}_q$
2. U generates $(r_{b_B}, r_{1_B}, r_{2_B}, r_{3_B}) \in_R \mathbb{Z}_q$ for some prime field $\mathbb{Z}_q$
3. U computes $t_A = (h_1\ h_5)^{r_{b_A}}\ h_2^{r_{1_A}}\ h_4^{r_{2_A}}\ h_6^{r_{3_A}} \bmod q$ as a *commitment*.
4. U computes $t_B = (h_1\ h_5)^{r_{b_B}}\ h_2^{r_{1_B}}\ h_4^{r_{2_B}}\ h_6^{r_{3_B}} \bmod q$ as a *commitment*.
5. U computes $h = H(t_A + \bar{S}_U^j)$ as a *challenge*, where $\bar{S}_U^j$ is the entity's current pseudonym.
6. U computes the following responses:
   - $\rho_{b_A} = h\ b_A + r_{b_A}$
   - $\rho_{1_A} = h\ w_{1_A} + r_{1_A}$
   - $\rho_{2_A} = h\ w_{2_A} + r_{2_A}$
   - $\rho_{3_A} = h\ w_{3_A} + r_{3_A}$

Similarly, U computes the responses ρ_{b_B}, ρ_{1_B}, ρ_{2_B} and ρ_{3_B}.

7. U stores in ZKPoK2 the responses ρ_{b_A}, ρ_{1_A}, ρ_{2_A}, ρ_{3_A}, ρ_{b_B}, ρ_{1_B}, ρ_{2_B}, ρ_{3_B}, and the values of t_A and t_B.

When the verifier executes algorithm `VerifyZKPoK2` (CMT, ZKPoK2), it will accept if the following statement holds true:

$$\left(\left(Com_A\ (h_1\ h_3)^{-a_A}\right)^h\right.$$
$$\left. t_A = (h_1\ h_5)^{\rho_{b_A}}\ h_2^{\rho_{1_A}}\ h_4^{\rho_{2_A}}\ h_6^{\rho_{3_A}} \bmod N\right) \wedge$$
$$\left(\left(Com_B\ (h_1\ h_3)^{-a_B}\right)^h\right.\ t_B =$$
$$\left.(h_1\ h_5)^{\rho_{b_B}}\ h_2^{\rho_{1_B}}\ h_4^{\rho_{2_B}}\ h_6^{\rho_{3_B}} \bmod N\right)$$

5.3.4. ZK-PoK-3 (`ConstructZKPoK3` and `VerifyZKPoK3`)

Signatures v_A and v_B of credentials AC_A and AC_B respectively must also be verified from the verifier's viewpoint. As in previous proofs, entity U must demonstrate knowledge of v_A and v_B as a valid signature without disclosing its real value. In particular, U gives a zero knowledge proofs of knowledge of the $(\mathbb{Z}_N^*, 3)$-root of the h_1-part of the (G, h_1, h_2)-DL representation of $Com(m_A)$ as well as of the $(\mathbb{Z}_N^*, 3)$-root of the h_1-part of the (G, h_1, h_2)-DL representation of $Com(m_B)$. In other words, U must prove that v_A is the third root of m_A and that v_B is the third root of m_B.

Steps of algorithm `ConstructZKPoK3` are detailed below:

- U chooses $r_{1_A}, r_{2_A}, r_{1_B}, r_{2_B} \in \mathbb{Z}_N$
- U computes $t_A = h_1^{r_{1_A}^3} h_2^{r_{2_A}} \bmod q$ and $t_B = h_1^{r_{1_B}^3} h_2^{r_{2_B}} \bmod q$.
- U computes $h = H(t_A + \bar{S}_U^j)$ and stores the first l most significant bits.
- For each *bit* of the l most significant bits of h:
  - If $bit = 0$ then: $\rho_{1_A} = r_{1_A}$, $\rho_{1_B} = r_{1_B}$, $\rho_{2_A} = r_{2_A}$, $\rho_{2_B} = r_{2_B}$
  - If $bit = 1$ then: $\rho_{1_A} = r_{1_A} v_A^{-1} \bmod N$, $\rho_{1_B} = r_{1_B} v_B^{-1} \bmod N$, $\rho_{2_A} = r_{2_A} - \omega_{1_A} (r_{1_A} v_A^{-1})^3 \bmod N$, $\rho_{2_B} = r_{2_B} - \omega_{1_B} (r_{1_B} v_B^{-1})^3 \bmod N$
- U stores in ZKPoK3 the responses ρ_{1_A}, ρ_{2_A}, ρ_{1_B}, ρ_{2_B} and the values of t_A and t_B.

When the verifier executes algorithm `VerifyZKPoK3` (CMT, ZKPoK3), it will accept if and only if the following statement holds true:

$$if bit = 0 \Rightarrow (t_A = h_1^{\rho_{1_A}^3}\ h_2^{\rho_{2_A}} \bmod q) \wedge (t_B = h_1^{\rho_{1_B}^3}\ h_2^{\rho_{2_B}} \bmod q)$$

$ifbit = 1 \Rightarrow (t_A = m_A^{\rho_{1_A}^3} h_2^{\rho_{2_A}} \bmod q \wedge (t_B = m_B^{\rho_{1_B}^3} h_2^{\rho_{2_B}} \bmod q)$.

5.3.5. ZK-PoK-4 (`ConstructZKPoK4` and `VerifyZKPoK4`)

Value y serves to blind the values a_A, b_A, m_A, v_A, a_B, b_B, m_B and v_B to prevent linkage between different instances of the anonymous credential joint proving protocol. If y was obtained by a malicious entity it may be possible to obtain the values for a_A, b_A, m_A, v_A, a_B, b_B, m_B and v_B and therefore credential shows becomes linkable to each other or to the specific user. Thus, entity U must give zero knowledge proof of knowledge of the discrete logarithm y to the base g of the h_5-part of the (G,h_5,h_6)-DL representation of $Com_A(b_A)^{c^{-1}}$ to the bases h_5, h_6, as well as, U must give zero knowledge proof of knowledge of the discrete logarithm y to the base g of the h_5-part of the (G,h_5,h_6)-DL representation of $Com_B(b_B)^{c^{-1}}$ to the bases h_5, h_6.

Notice that: $Com_A(b_A) = h_5^{b_A} h_6^{w_{3_A}}$ and that $b_A \equiv g^y b_A \equiv g^y c \bmod N$, and that $Com_B(b_B) = h_5^{b_B} h_6^{w_{3_B}}$ and that $b_B \equiv g^y\ b_B \equiv g^y\ c \bmod N$.

Steps of algorithm `ConstructZKPoK4` are detailed below:

- U chooses $r_{1_A}, r_{2_A}, r_{1_B}, r_{2_B} \in \mathbb{Z}_N$
- U computes $t_A = h_5^{g^{r_{1_A}}} h_6^{r_{2_A}} \bmod q$ and $t_B = h_5^{g^{r_{1_B}}} h_6^{r_{2_B}} \bmod q$.
- U computes $h = H(t_A + \bar{S}_U^j)$ and stores the first l most significant bits.
- For each bit of the l most significant bits of h:
  - If $bit = 0$ then: $\rho_{1_A} = r_{1_A}$, $\rho_{1_B} = r_{1_B}$, $\rho_{2_A} = r_{2_A}$, $\rho_{2_B} = r_{2_B}$
  - If $bit = 1$ then: $\rho_{1_A} = r_{1_A} - y$, $\rho_{1_B} = r_{1_B} - y$, $\rho_{2_A} = r_{2_A} - w_{3_A}\ c^{-1}\ g^{\rho_{1_A}} \bmod N$, $\rho_{2_B} = r_{2_B} - w_{3_B}\ c^{-1}\ g^{\rho_{1_B}} \bmod N$
- U stores in ZKPoK4 the responses ρ_{1_A}, ρ_{2_A}, ρ_{1_B}, ρ_{2_B} and the values of t_A and t_B.

When the verifier executes algorithm `VerifyZKPoK4`(CMT, ZKPoK4), it will accept if and only if the following statement holds true:

$ifbit = 0 \Rightarrow (t_A = h_5^{g^{\rho_{1_A}}} h_6^{\rho_{2_A}} \bmod q) \wedge \left(t_B = h_5^{g^{\rho_{1_B}}} h_6^{\rho_{2_B}} \bmod q\right)$

$ifbit = 1 \Rightarrow (t_A = (Com_A(b_A)^{c^{-1}})^{g^{\rho_{1_A}}} h_6^{\rho_{2_A}} \bmod q \wedge (t_B = (Com_B(b_B)^{c^{-1}})^{g^{\rho_{1_B}}} h_6^{\rho_{2_B}})$.

6. Security analysis

In the proposed system, motor vehicle mandatory authorizations are represented by the certificate $\bar{Cert}(ID_U, PK_U, long\ validity\ period)$, the set $\mathcal{CERT}$ of pseudonym-based certificates and four anonymous credentials AC_A, AC_B, AC_C and AC_D.

Authenticity of all these credentials is guaranteed by the signature of the trusted certification authorities CA, $\bar{CA}_P$, O_A, O_B, O_C and O_D, respectively. Furthermore, the private keys associated with the certificates are generated and exclusively used within vehicle U's HSM, so they cannot be transferred to other vehicle Z, and anonymous credentials are treated as cryptographic material that cannot be transferred outside of the HSM once they have been loaded in such device. Moreover, anonymous credentials contain a secret derived from entity U's long term private key SK_U, so in order to prove holdership of any of them, a vehicle must prove knowledge of that secret, hence providing unforgeability and non-transferability of those credentials.

Regarding reply attacks, another vehicle Z cannot successfully use captured response messages sent by a vehicle U to prove holdership of the required credentials, as Z will not be able to sign a fresh response message using private key $\bar{SK}_U^j$. Recall that such key will only be used once.

ZKPoKs, by definition, do not transfer any information to verifiers that has not been provided by the prover and, also by definition, different executions of the ZKPoKs are unlinkable [12]. Moreover, note that in our protocol, non-interactive ZKPoKs are used, therefore verifiers are *truly-honest* (they cannot select challenges to get additional information about the prover's credentials).

Some previous works have demonstrated that it is possible to trace vehicles that authenticate VANET messages with single-use pseudonym-based certificates [5]. However, although elements cha and $t_{request}$ are used to link a request with a response but they are not transmitted in clear, and we restrict the use of pseudonyms $\bar{S}_U^j$ to a single response, pseudonym-based certificates in $\mathcal{CERT}$ cannot be traced. An adversary capturing traffic near the verifier V only learns that one of the vehicles currently circulating at that point has answered the request, but it does not know which one.

Verifier V is the only one that is able to link both pseudonyms $\bar{S}_U^i$ and $\bar{S}_U^j$ (except in very sparse traffic conditions). However, note that we assume that verifiers do not collude with other verifiers to share transcripts of protocol executions or capture VANET messages for a large area in order to perform attacks such as the described in [5]. Additionally, as elements cha and $t_{request}$ within the request and response messages are encrypted with different public keys they cannot be used to link those messages.

Also, if a vehicle does not hold up-to-date certificates or the anonymous credentials are not valid, V will detect that certificate $\bar{Cert}(\bar{S}_U^j, \bar{PK}_U^j, short\ validity\ period)$ is revoked and V will reject the ZKPoKs, respectively. Otherwise, the non-interactive ZKPoKs sent by U do not leak any information about U (i.e., they could have been generated by V as well) but as they are signed by U, using its short-term private key $\bar{SK}_U^j$, they constitute a non-repudiation evidence of U's participation in the protocol and the status of its credentials.

In some cases, an adversary may delete request messages sent by a verifier or disable the vehicle's OBU with the intention of evading the proving request. However, as the verifier may count on acknowledgement messages sent by surrounding vehicles W, this information may be presented to the adjudicator Adj so it can call the vehicle for revision (e.g., if it happens certain number of times). A similar situation happens if an adversary prevents a vehicle, that holds the required credentials, from sending correct response messages through its OBU (before being sent), with the consequence of vehicle being called for a revision (after several occurrences).

Moreover, an external adversary may try to delete or modify messages sent by vehicle U (holding valid creden-

Table 2
Computational cost of the anonymous credential system setup phase and anonymous credential issuing phase for a single *AC*.

Phase	Average time (ms)
System setup	40,695
Anonymous credential issuing	188

tials) and received by the verifier *V*'s communication device with the intention of vehicle *U* being called for revision. However, if the adversary has not jammed all the communications, *U* may count on acknowledgement messages of *U*'s response message sent by surrounding vehicles *W*, and present them to *Adj* with the rest of elements stored by *U* as evidence. With this information, *Adj* may decide to send a technician to revise the RSU where that verifier agent *V* has been deployed. At the end, even if a vehicle is called to a revision while holding the required credentials, verifier *V* or an external adversary will not be able to learn *U*'s identity and *U* will not be incorrectly fined as it may even be able to prove holdership of credentials to *Adj* if required to.

7. Performance analysis

In this Section, we will explore and describe the feasibility of our proposal in terms of the time and computational effort for a passing-by vehicle to complete the telematic proof of observance, of the mandatory regulations regarding the technical and administrative on-the-road motor vehicle authorizations. Firstly, we present results of the implementation of algorithms directly related to the anonymous credential system and, secondly, we analyze results of the *Anonymous Credentials Joint Proving Phase* (Phase 4) taking into account all the steps (other computations, message exchanges) that take place in the online part of this phase.

7.1. Algorithms of the anonymous credential system

The anonymous credential system was prototyped on a PC platform Java 7 (update 3) and the experiments were conducted on a machine with an AMD Athlon (tm) 64 X2 Dual Core Processor 4200 2.21 GHz. All computations are for a total of five attributes in each credential (two *private*-attributes and three *open*-attributes).

According to the different phases described in Section 4.4, in Table 2 we show the computational cost of the *Anonymous Credential System SetUp Phase* (Phase 2) and of the *Anonymous Credentials Issuing Phase* for a single *AC* (Phase 3). Furthermore in Table 3 we show the computational cost of the algorithms `ConstructCMT`, `ConstructZKPoK-` (for ZKPoK-1 to ZKPoK-4) and `VerifyZKPoK-` (for ZKPoK-1 to ZKPoK-4) used in the *Anonymous Credentials Joint Proving Phase* (Phase 4). The times are the average out of 50 runs.

Furthermore, Table 4 summarizes the information shown in Table 3. It shows the overall execution time for the Joint Anonymous Credential Proving phase, for four credentials (AC_A,AC_B,AC_C and AC_D) each with five attributes, disclosing three of those attributes, and for different values of the security parameter *l*. The total average time to construct the commitments and the ZKPoKs represents the total pre-computational time a vehicle *U* needs to be ready to respond to the next credential verification request. The total average time to verify the ZKPoKs represents only the total time a verifier needs to verify those ZKPoKs received from *U*. Parameter *l* is the security parameter and it represents the number of times the ZKPOK3-4 are executed. As we can see, with the maximum level of security

Table 3
Computational cost of each of the algorithms used in our proposal in terms of the average time consumed.

Algorithms of the anonymous credential joint proving phase			
Algorithm		Average computation time (ms)	
		Construct	VerifyZKPoK-(CMT, ZKPoK −)
CMT		1584	–
ZKPOK1		848	726
ZKPOK2		500	1004
ZKPOK3	Length of challenge $l = 16$	3908	3386
	Length of challenge $l = 22$	5496	5474
	Length of challenge $l = 28$	6982	6956
	Length of challenge $l = 34$	8684	8610
	Length of challenge $l = 40$	10,290	10,268
	Length of challenge $l = 46$	11,692	11,598
	Length of challenge $l = 52$	13,180	13,102
	Length of challenge $l = 64$	16,680	16,520
ZKPOK4	Length of challenge $l = 16$	6954	6984
	Length of challenge $l = 22$	9502	9532
	Length of challenge $l = 28$	12,184	12,226
	Length of challenge $l = 34$	15,136	15,190
	Length of challenge $l = 40$	17,834	17,864
	Length of challenge $l = 46$	20,318	20,334
	Length of challenge $l = 52$	22,912	22,928
	Length of challenge $l = 64$	29,000	29,056

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

Table 4
Total computational cost of the algorithms executed by prover and verifier in terms of the average time consumed.

Algorithms of the anonymous credential joint proving phase								
	Total average computation time (ms)							
Length of challenge	$l = 16$	$l = 22$	$l = 28$	$l = 34$	$l = 40$	$l = 46$	$l = 52$	$l = 64$
Prover	13,794	17,930	22,098	26,752	31,056	34,942	39,024	48,612
Verifier	12,100	16,736	20,912	25,530	29,862	33,662	37,760	47,306

Table 5
Size of data elements in PRV, constructed for the anonymous verification of credentials AC_A, AC_B, AC_C and AC_D.

Algorithms of the anonymous credential joint proving phase			
Element	Size of data elements result of the algorithms (bits) Items	Length of Each item	Total length
CMT	$\widehat{a_A}$, $\widehat{a_B}$, $\widehat{a_C}$, $\widehat{a_D}$	length (N)	4∗length (N)
	$Com(\widehat{m_A}), Com(\widehat{a_A}), Com(\widehat{b_A})$ $Com(\widehat{m_B}), Com(\widehat{a_B}), Com(\widehat{b_B})$ $Com(\widehat{m_C}), Com(\widehat{a_C}), Com(\widehat{b_C})$ $Com(\widehat{m_D}), Com(\widehat{a_D}), Com(\widehat{b_D})$ Com_A, Com_B, Com_C, Com_D	Length (q)	16∗length (q)
ZKPoK1	ρ_y, ρ_1, ρ_{2_A}, ρ_{2_B}, ρ_{6_A}, ρ_{6_B} ρ_{2_C}, ρ_{2_D}, ρ_{6_C}, ρ_{6_D}	Length (e)	10∗length (e)
	ρ_A, ρ_B, ρ_C, ρ_D, t_A, t_B, t_C, t_D	length (N)	8∗length (N)
ZKPoK2	ρ_{b_A}, ρ_{1_A}, ρ_{2_A}, ρ_{3_A}, ρ_{b_B}, ρ_{1_B}, ρ_{2_B}, ρ_{3_B} ρ_{b_C}, ρ_{1_C}, ρ_{2_C}, ρ_{3_C}, ρ_{b_D}, ρ_{1_D}, ρ_{2_D}, ρ_{3_D} t_A, t_B, t_C, t_D	length (q)	20∗length (q)
ZKPoK3	ρ_{1_A}, ρ_{2_A}, ρ_{1_B}, ρ_{2_B}, ρ_{1_C}, ρ_{2_C} ρ_{1_D}, ρ_{2_D}	Length (N)	8∗length (N)
	t_A, t_B, t_C, t_D	length (q)	4∗length (q)
ZKPoK4	ρ_{1_A}, ρ_{2_A}, ρ_{1_B}, ρ_{2_B}, ρ_{1_C}, ρ_{2_C}, ρ_{1_D}, ρ_{2_D}	Length (N)	8∗length (N)
	t_A, t_B, t_C, t_D	length (q)	4∗length (q)
PRV	28∗length (N)+44∗length (q)+10 ∗length (e)		

(parameter $l = 64$) the total average times spent by a prover and a verifier are respectively less than 49 s and less than 48 s, whereas for the minimum level of certainty about the verification of the ZKPOK3 and ZKPOK4 (parameter $l = 14$), the total average times consumed by a prover and a verifier are respectively less than 14 s and less than 13 s.

Finally, Table 5 shows the total size (number of bits) of the different data elements that entity U has to store in PRV, to sign (along with other data elements) and finally to send to V. These calculations allow us to estimate, for a modulo $length(N) = 1024$, $length(e) = 448$ and, $length(q) = 448$ bits, a final size of PRV of $length(\text{PRV}) = 52{,}864$ bits (6.608 Kbytes).

7.2. Online part of the anonymous credential joint proving phase

In this subsection, the computational and transmission costs produced in the online phase of the anonymous credential joint proving are analyzed. For this purpose, the computational capabilities of vehicular communication networks and computational devices will be assumed. Concerning the communication network, it will be based on Dedicated Short Range Communications (DSRC) technology, which has a bandwidth of 6 Mbit/s [32]. With respect to the computational devices, performance figures provided by CycurV2X[4]'s manufacturer will be considered.

In this part of the process, the main computational tasks are related to encryption and digital signatures. The aforementioned device takes 27.938 ms. for encryption and 21.26 ms. for decryption. Digital signatures are computed in 7.156 ms. and verified in 27.114 ms. The aforementioned figures are the result of applying ECIES encryption and ECDSA signatures over 16 bytes of data. Such algorithms are chosen in compliance with IEEE 1609.2 standard [30]. Note that while the performance of ECDSA is not significantly affected by the message length (as it starts by applying a hash over the message), ECIES performance grows accordingly. As its foundations lie on a symmetric encryption algorithm, it will be assumed that the encryption time grows linearly with respect to the message length.

In order to calculate the costs of this phase it is necessary to determine the message length. For this purpose, *cha*, open-attributes (α_i, β_i, γ_i and δ_i for $i = 3 \ldots 5$) and the time marks $t_{request}$ and $t_{response}$ are assumed to be 4 bytes length. Public key certificates are 125 bytes and digital sig-

[4] https://www.escrypt.com.

Table 6
Size of messages exchanged between *U* and *V* during the online part of the *Anonymous credential joint proving phase*.

Online part of the anonymous credential joint proving phase		
Message	Size of exchanged messages (bytes) Size of each element in message	Total size
REQ	4 + 4+4 + 56 + 125	193
RES	6608 + 48 + 8+56 + 125	6845

natures are 56 bytes in size, according to SAE J2735 standard [33]. The remaining data elements' sizes are shown in Table 5. Size of exchanged messages is shown in Table 6.

Taking these elements into account, consumed times in steps `Cred. Prov. Request`, `Cred. Prov. Response`, and `Cred. Prov. Response Verification` of the online part of the *Anonymous Credential Joint Proving Phase* are shown in Table 7.

The request step takes 21.124 ms. of computation for *V*, and 0.26 ms. of transmission. Concerning the response step, it takes 85.976 ms. of computation time for *U*, and 9.126 ms. of transmission. The set of sub-steps regarding the verification of the identity inspection feasibility, within the response verification step, takes 278.106 ms. The set of sub-steps regarding the credentials validity verification, also within the response verification step, takes 47,306.00 ms. It should be noted that computation times should be enlarged with the cost of verifying the status of public key certificates (for which no reference performance figures exist in this environment). On the other hand, even if *V* computational capabilities would be higher than those available for *U*, these calculations enable having a worst-case analysis. One important issue is to determine the feasibility of this part of the process in a realistic driving environment. Particularly, it is critical to assess whether it can be performed between a vehicle and a single *V* (i.e. a single Road-Side Unit), or it is necessary to perform a hand-over between different verifiers. In a real driving environment, the maximum (legal) speed is usually 120 km/h. Given that DSRC coverage area is 1 km., a vehicle remains 30,000 ms. within a single *V*'s range. At the light of the previous results, it may be seen that the steps of the process that need *U* being in the range of *V* (`Cred. Prov. Request`, `Cred. Prov. Respose` and steps (a) to (c) of `Cred. Prov. Response Verification`) can be performed within the 30 s. time frame. As a consequence, the online part may be performed between a vehicle (*U*) and a single RSU (*V*). Moreover, the total amount of time taken before *V* starts the credentials validity verification, i.e., before *V* must decide if it is necessary to take a photo to vehicle *U*, is 394.592 ms. In this time, a vehicle at a speed of 120 km/h will cover 13.15 m., that is a distance short enough to have the assurance that videocamera *VC* is going to take a photo of the right vehicle.

8. Conclusions

Nowadays, the verification of the status of road traffic credentials incurs in a significant cost due to the required manpower. Moreover, it introduces a privacy threat as the credentials' content have to be fully shown to the verifier, enabling the chance of tracking. To contribute on this issue, in this work a novel privacy-preserving and accountable verification system for vehicular mandatory authorizations has been proposed. The process is designed to be performed electronically on-the-road. For this purpose, a set of anonymous credentials, based on existing driving authorizations, has been designed. In order to prove such credentials, several proof-of-knowledge cryptographic mechanisms have been adapted.

The system ensures that vehicles with valid credentials remain anonymous, no matter the amount of verifications performed. On the contrary, vehicles without valid credentials will have their identity revealed. In this way, the proposed approach constitutes a suitable tradeoff between privacy preservation and offenders' accountability. Experimental results show that the system is suitable for vehicular scenarios, considering both the limitation of available computational resources and the unreliability of communication networks.

Future work will be focused on three main issues. On the one hand, the system will be expanded to cope with more specific, fine-grained verification of authorizations, such as particular driving regulations for heavyweight vehicles. On the other hand, driver's credentials will be also considered, enabling further verifications such as ensuring that the driver is entitled to drive a given vehicle. Finally, the anonymous credential system will be evolved to comply with the architecture for attribute-based technology specified within the *ABC4Trust* project [34]. Additionally, it would be interesting to design similar systems to the one proposed herein but based on U-Prove and Idemix.

Table 7
Time consumed in the main steps of the online part of the *Anonymous credential joint proving phase*.

Online part of the anonymous credential joint proving phase				
Step	Consumed time (ms) Computation time *U*	Transmission time *V*	Total time $U \leftrightarrow V$	
`Cred. prov. request`		21.124	0.26	21.384
`Cred. prov. response`	85.976		9.126	95.102
`Cred. prov. response verification`				
Identity inspection feasibility		278.106	–	47,584.106
Credentials validity		47,306.00	–	

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

Acknowledgements

This work has been funded by Grant CCG10-UC3M/TIC-5174 (Project PRECIOUS) and partially by Grant TIN2009-13461 (Project E-SAVE).

Appendix A. Mathematical foundations and assumptions

The system heavily relies on zero knowledge proofs of knowledge and commitments. In this section, we offer the highlights of such constructions.

A.1. Zero Knowledge Proofs of Knowledge and Σ-protocols

A Zero Knowledge Proof of Knowledge (ZK-PoK) makes reference to an algorithm between two different entities, a *Prover* and a *Verifier*. Such proofs must satisfy the properties of completeness, soundness and zero knowledge. Loosely speaking, a ZK-PoK states that the prover can convince the verifier of the knowledge of a secret if and only if the prover knows the secret and the verifier learns nothing more about the secret than what he already knew about it before the proof. The most common version for this type of construction is based on the so called Σ-protocols which can be generalized (in the interactive form) as a three move protocol in the following definition.

Definition 1 (*Σ-protocols*). A protocol between a prover A and a verifier B is called a Σ-protocol, with challenge set $\mathcal{C}$, predicate $\mathcal{P}$ and a (secret) *witness* x of a public parameter y, if it satisfies the following conditions:

1. A sends a *commitment* t to a verifier B.
2. B sends a *random challenge* $c \in \mathcal{C}$ to A.
3. A computes a *response* $\rho(c;x)$ and sends $\rho(c;x)$ to B, keeping value x as the secret *witness*.
4. B accepts A has knowledge of the secret x if and only if predicate $\mathcal{P}(t;c;\rho;y)$ holds true; otherwise he rejects.

The result of taking a Σ-protocol and making the challenge the output of a hash function over the commitment, is a *non-interactive* ZK-PoK, hence reducing the interaction necessary between prover and verifier.

A.2. Commitments

In our system, the commitments, based on Pedersen et al. work ([35]), are composed together with the ZK-PoK in the following manner:

1. *Setup phase*: The verifier obtains from the system public parameters a large prime q and a cyclic group G of order N (a product of two safe primes), which is a subgroup of Z_q. It also obtains a public parameter $h = g^a mod\ q$. The values q, N, g, h are also public for the prover.
2. *Commit phase*: The prover wants to commit to some $x \in G$. The prover chooses random $r \in G$ and sends $c = g^x * h^r\ mod\ q$ to the verifier. This is simply $g^x * (g^a)^r = g^{x+ar}\ mod\ q$.
3. *Proof phase*: The prover realizes a noninteractive ZK-PoK over the tuple of secrets (x,r).

A.3. Σ-protocols Used in the Proposed System

The different parts of the overall system we propose are based on the anonymous credential system presented by Persiano and Visconti in [12], which is itself based on the following mathematical blocks.

A.3.1. DL and RSA representations

Definition 2 (*Discrete Logarithm Representation (DL-REP)*). Let G be a group of order N and let y, $g_1, \ldots, g_m \neq 1$ be elements of G. A $(G,g_1,\ldots,g_m)$-DL representation (DL-REP) of y is a tuple $(x_1,\ldots,x_m)$ such that $\forall i = \{1,\ldots,m\}$, $0 \leqslant x_i \leqslant N-1$ and $y = g_1^{x_1} * \ldots * g_m^{x_m}$. Moreover, for $i = 1,\ldots,m$, we call x_i the g_i-part of the $(G,g_1,\ldots,g_m)$-DL representation $(x_1,\ldots,x_m)$ of y.

Definition 3 (*RSA Representation (RSA-REP)*). Let $e \in \mathbb{Z}_N^*$ be co-prime with $\phi(N)$ and let $y, g_1, \ldots, g_m \neq 1$ be elements of $\mathbb{Z}_N^*$. A $(\mathbb{Z}_N^*, e, g_1, \ldots, g_m)$-RSA representation (RSA-REP) of y is a tuple $(x_1,\ldots,x_m,x)$ such that $y \equiv g_1^{x_1} * \ldots * g_m^{x_m} * x^e \bmod N$, $0 \leqslant x_i < e$ for $i = 1,\ldots,m$ and $x \in \mathbb{Z}_N^*$.

Definition 4 (*$(\mathbb{Z}_N^*, e)$-root of an element*). Let e be an element of $\mathbb{Z}_N^*$ co-prime with $\phi(N)$. A $(\mathbb{Z}_N^*, e)$-root of $y \in \mathbb{Z}_N^*$ is an element $x \in \mathbb{Z}_N^*$ such that $x^e \equiv y \bmod N$.

A.3.2. ZK-PoK of DL and RSA representations

A *ZK-PoK of a DL-representation* makes reference to a Σ-protocol between two different entities, a prover and a verifier, in which the prover has to prove, in a zero knowledge fashion, knowledge of a tuple of witnesses values $(x_1,\ldots,x_m)$ of a public parameter $y = g_1^{x_1} * \ldots * g_m^{x_m}$.

In a similar way, a *ZK-PoK of a RSA-representation* makes reference to an Σ-protocol between two different entities, a prover and a verifier, in which the prover has to prove, in a zero knowledge fashion, knowledge of a tuple of witnesses values $(x_1,\ldots,x_m,x)$ of a public parameter $y = g_1^{x_1} * \ldots * g_m^{x_m} * x^e$.

Also, a *ZK-PoK of the ith part of a DL-representation* makes reference to an algorithm between two different entities, a prover and a verifier, in which the prover has to prove, in a zero knowledge fashion, knowledge of a witness value (x_i) of a public parameter $y = g_1^{x_1} * \ldots * g_m^{x_m}$.

Finally, a *ZK-PoK of the eth root of an element* makes reference to an algorithm between two different entities, a prover and a verifier, in which the prover has to prove, in a zero knowledge fashion, knowledge of a witness value x of a public parameter y such that $x^e \equiv y \bmod N$.

In [36], the details of two interactive Σ-protocols can be found for ZK-PoKs of DL and RSA representations. The author also provides formal proofs of the completeness, soundness and zero-knowledge properties of the proofs,

as well as of the of existence of such proofs when the secret tuple of secrets $(x_1,\ldots,x_m)$ satisfies a certain boolean formula $\Phi(x_1,\ldots,x_m)$. The Σ-protocols for ZK-PoKs of DL and RSA representations used in this proposal are based on those proposed in [36]. Such schemes have been modified to make them non-interactive and, a new Σ-protocol is defined to proof knowledge of a Boolean composition of two RSA-representations with one shared secret. In [12,13], algorithms are depicted to carry out ZK-PoKs of a part of a DL-representation and, ZK-PoKs of the e-th root of a part of a DL-representation, respectively. Similarly, those algorithms have been modified to be non-interactive and adapted to the scenario in hand.

A.4. Computational assumptions

The computational assumptions can be summarized as follows:

Lemma 1. *On input an integer N, such that $N = p_1{}^*p_2$ where p_1 and p_2 are primes of the same length, an integer e such that $gcd(e,\phi(N)) = 1$ and $a, c \in \mathbb{Z}_N$, it is hard to find in probabilistic polynomial time a pair (v,x) such that $v^e = a^*x + c \ (modN)$ ([12]).*

Lemma 2. *Let G be a group of prime order q, and let $\{g_1,\ldots,g_m\}$ be random elements of G. Assuming the discrete logarithm assumption in G, it holds that no probabilistic polynomial-time algorithm can output, with non-negligible probability, an element $h \in G$ and two different representations of h with respect to some of the g_i's ([37]).*

References

[1] Spanish National Association of Breakdown Service Businesses (ANEAC). La caducidad de la ITV no será motivo para quitar el carné. <http://www.aneac.com/index.php/2010/04/la-caducidad-de-la-itv-no-sera-motivo-para-quitar-el-carne/> (accessed 10.12).
[2] J. de Fuentes, A. González-Tablas, J. Hernández-Ardieta, A. Ribagorda, Towards an automatic enforcement for speeding: enhanced model and intelligent transportation systems realisation, Intelligent Transport Systems, IET 6 (3) (2012) 270–281.
[3] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J. Hubaux, Securing vehicular ad hoc networks, Journal of Computer Security 15 (1/2007) (2008) 39–68.
[4] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J. Hubaux, Secure vehicular communication systems: design and architecture, IEEE Communications Magazine 46 (11) (2008) 100–109.
[5] B. Wiedersheim, Z. Ma, F. Kargl, P. Papadimitratos, Privacy in inter-vehicular networks: why simple pseudonym change is not enough, in: 2010 Seventh Intl. Conf. on Wireless On-demand Network Systems and Services (WONS), IEEE Computer Society Press, 2010, pp. 176–183.
[6] C. Paquin, G. Zaverucha, U-Prove Cryptographic Specification v1.1 Draft Revision 2, Tech. Rep., Microsoft Corporation, April 2013.
[7] C. Paquin, U-Prove Technology Overview v1.1 Draft Revision 2, Tech. Rep., Microsoft Corporation, April 2013.
[8] S.A. Brands, Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy, MIT Press, 2000.**
[9] C.S.D. Security Team, Specification of the Identity Mixer Cryptographic Library Version 2.3.1, Tech. Rep. Research Report RZ 3730, IBM Research Zurich, December 2010.
[10] J. Camenisch, E. Van Herreweghen, Design and implementation of the idemix anonymous credential system, in: Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS '02, ACM, 2002, pp. 21–30.
[11] J. Camenisch, A. Lysyanskaya, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: Proc. of the Int. Conf. on the Theory and Application of Cryptographic Techniques (EUROCRYPT '01), Springer-Verlag, London, UK, 2001, pp. 93–118.
[12] G. Persiano, I. Visconti, An efficient and usable multi-show non-transferable anonymous credential system, in: Financial Cryptography, Lecture Notes in Computer Science, vol. 3110, 2004, pp. 196–211.
[13] J. Camenisch, M. Stadler, Efficient group signature schemes for large groups, in: Proc. of the Advances in Cryptology (CRYPTO'97), 1997.
[14] A. Blumberg, L. Keeler, A. Shelat, Automated traffic enforcement which respects driver privacy, in: Proceedings of the IEEE International Conference on Intelligent Transportation Systems (ITSC), IEEE, 2005, pp. 941–946.***
[15] R. Popa, H. Balakrishnan, A. Blumberg, VPriv: protecting privacy in location-based vehicular services, in: Proceedings of the 18th Conference on USENIX Security Symposium, USENIX Association, 2009, pp. 335–350.
[16] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, C. Geuens, PrETP: privacy-preserving electronic toll pricing, in: Proceedings of the 19th USENIX Conference on Security, USENIX Association, 2010, pp. 5–5.
[17] C. Troncoso, G. Danezis, E. Kosta, B. Preneel, PriPAYD: privacy friendly pay-as-you-drive insurance, in: Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, ACM, 2007, pp. 99–107.
[18] Commission Directive 2003/127/EC of 23 December 2003 amending Council Directive 1999/37/EC on the registration documents for vehicles, in: Official Journal of the European Union, vol. 10, 2004, pp. 29–53.
[19] Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licenses, in: Official Journal of the European Union, vol. 403, 2006, pp. 18–60.
[20] Directive 2007/46/EC of 5 September 2007 establishing a framework for the approval of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, Official Journal of the European Union 263 (2007) 1–160.**
[21] F. Sagberg. Automatic enforcement technologies and systems. Working paper 7 of the ESCAPE project, May 2000. <http://virtual.vtt.fi/virtual/proj6/escape/escape_wp7.pdf> (Last accessed on July 2013).
[22] Orden ITC/2536/2006, de 26 de julio, por la que se regula el soporte electrónico para la tarjeta ITV y (..), in: Boletín Oficial del Estado, vol. 184, 2006, pp. 28994–28994.
[23] P. Bichsel, J. Camenisch, T. Groß, V. Shoup, Anonymous credentials on a standard java card, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09, ACM, 2009, pp. 600–610. doi:10.1145/1653662.1653734.
[24] P. Vullers, G. Alpár, Efficient selective disclosure on smart cards using idemix, in: Proceedings of the 3rd IFIP WG 11.6 Working Conference on Policies & Research in Identity Management (IFIP IDMAN), IEEE, 2013.***
[25] W. Mostowski, P. Vullers, Efficient u-prove implementation for anonymous credentials on smart cards, in: Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 96, Springer, Berlin Heidelberg, 2012, pp. 243–260.
[26] Trial-Use Standard for Wireless Access in Vehicular Environments (Wave) – Resource Manager, IEEE Std. 1609.1-2006 (2006) 1–71. doi:10.1109/IEEESTD.2006.246485.
[27] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, J.-P. Hubaux, Secure vehicular communication systems: implementation, performance, and research challenges, Communications Magazine, IEEE 46 (11) (2008) 110–118. doi:10.1109/MCOM.2008.4689253.**
[28] IEEE 1609 Working Group, IEEE 1609 Working Group Public Site (Last accessed on April 2013). <http://vii.path.berkeley.edu/1609_wave/>.
[29] J.M. de Fuentes, A. Gonzlez-Tablas, A. Ribagorda, Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts, IGI Global, 2011, Ch. Overview of Security Issues in Vehicular Ad-hoc Networks, pp. 894–911.
[30] IEEE P1609.2 Security Profile for Specific Use Cases, Tech. Rep., IEEE, 2012.
[31] J.M. de Fuentes, A.I. González-Tablas, J. Blasco, L. González-Manzano, Protocol for behavior-describing evidence generation and verification in vehicular environments, Journal of Systems Architecture 2013, in press.

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008

[32] J. Kenney, Dedicated short-range communications (DSRC) standards in the United States, Proceedings of the IEEE 99 (7) (2011) 1162–1182.
[33] SAE J2735 DSRC Message Set Dictionary, Tech. Rep., Society of Automotive Engineers, 2009.
[34] J. Camenisch, I. Krontiris, A. Lehmann, G. Neven, C. Paquin, K. Rannenberg, H. Zwingelberg, D2. 1 Architecture for Attribute-based Credential Technologies-Version, Tech. Rep., Technical Report, ABC4Trust Consortium, December 2011. <https://abc4trust.eu/index.php/pub/107-d21architecturev1>.
[35] T.P. Pedersen, Non-interactive and information-theoretic secure verifiable secret sharing, in: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '91, 1992, pp. 129–140.
[36] S. Brands, Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy, MIT Press, 2000.
[37] E. Bresson, J. Stern, Proofs of knowledge for non-monotone discrete-log formulae and applications, in: Proceedings of the 5th International Conference on Information Security, ISC '02, 2002, pp. 272–288.

Ana Isabel González-Tablas is associate professor in the Computer Science and Engineering Department at University Carlos III of Madrid. She is Telecommunications Engineering by the Polytechnic University of Madrid, Spain, since 1999 and received her Ph.D. degree in Computer Science from University Carlos III of Madrid, Spain, in 2005. Her main research interests are security and privacy for Intelligent Transportation Systems and Location Based Services. She has published numerous articles in national and international journals and conferences. She has been the principal researcher of project PRECIOUS and is part of the research team of project E-SAVE.

Almudena Alcaide, PhD. is assistant professor at the Information Security Group of the Computer Science Department of Carlos III University of Madrid. She has a B.Sc. in Mathematics by Complutense University of Madrid, a M.Sc. in Advanced Computing by King's College of London and a PhD. in Computer Science by Carlos III University of Madrid. Her research is focused on formal methods applied to the design and analysis of cryptographic protocols and more recently on privacy and cryptography applied to computer security and network security. She is part of the research team of projects PRECIOUS and E-SAVE.

José María de Fuentes, Ph.D. is teaching assistant in the Computer Science and Engineering Department at University Carlos III of Madrid (Spain). His main research interests are digital evidences management, non-repudiation issues and secure message distribution in vehicular environments. He has published several articles in international conferences and journals. He is part of the research team of projects PRECIOUS and E-SAVE.

José Montero, is Ph.D. candidate in the Computer Science and Engineering Department at University Carlos III of Madrid (Spain). He is currently working at company brain-tec AG. His main research interests are privacy and anonymity in distributed contexts, as well as cooperation in ad hoc environments.

Please cite this article in press as: A.I. González-Tablas et al., Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.05.008