Noname manuscript No.
(will be inserted by the editor)

Assessment of attribute-based credentials for privacy-preserving road traffic services in smart cities

J. M. de Fuentes · L. González-Manzano · J. Serna-Olvera · F. Veseli

Received: date / Accepted: Feb. 7th, 2017

Post-print version. Accepted for publication in Personal and Ubiquitous Computing Journal, Special Issue on Security and Privacy for Smart Cities, 2017. The final publication is available at Springer. Please check the final version at http://www.springer.com/computer/hci/journal/779

Abstract Smart cities involve the provision of advanced services for road traffic users. Vehicular ad-hoc networks (VANETs) are a promising communication technology in this regard. Preservation of privacy is crucial in these services to foster their acceptance. Previous approaches have mainly focused on PKI-based or ID-based cryptography. However, these works have not fully addressed the *minimum information disclosure* principle. Thus, questions such as how to prove that a driver is a neighbour of a given zone, without actually disclosing his identity or real address, remain unaddressed. A set of techniques, referred to as Attribute-Based Credentials (ABCs), have been proposed to address this need in traditional computation scenarios. In this paper, we explore the use of ABCs in the vehicular context. For this purpose, we focus on a set of use cases from European Telecommunications Standards Institute (ETSI) Basic Set of Applications, specially appropriate for the early development of smart cities. We assess which ABC techniques are suitable for this scenario, focusing on three representative ones – Idemix, U-Prove and VANET-updated

J. M. de Fuentes
Computer Security Lab (COSEC). Carlos III University of Madrid (Spain)
Tel.: +34-91-624-9422
Fax: +34-91-624-9960
E-mail: jfuentes@inf.uc3m.es

· L. González-Manzano Computer Security Lab (COSEC). Carlos III University of Madrid (Spain)
J. Serna-Olvera and F. Veseli
Chair of Mobile business and multilateral security. Goethe Universitat Frankfurt am Main (Germany)

Persiano systems. Our experimental results show that they are feasible in VANETs considering state-of-the-art technologies, and that Idemix is the most promising technique for most of the considered use cases.

Keywords Smart cities · Attribute-Based Credential (ABC) · Privacy preservation · Vehicular networks · VANETs

1 Introduction

Smart cities involve the management of different infrastructures in order to provide better services to citizens. Among these services, those intended to improve road traffic play a key role in smart cities development [3]. In order to achieve this goal, Vehicular Ad-hoc Networks (VANETs) are being developed. VANETs allow the exchange of information with vehicles around and also with the traffic manager and other service providers. In this way, VANETs enable not only traffic management but also a plethora of services to enhance citizens' experience of travelling. In particular, the European Telecommunications Standards Institute (ETSI) has defined the Basic Set of Applications (BSA), which "can be deployed simultaneously at a targeted time (day 1) with the objective to serve societal and business objectives of private and public road transport stakeholders" [18]. Therefore, BSA is a stepping stone towards the development of smart cities.

However, despite their benefits, privacy is a key concern in this facet of smart cities [22]. For example, given that vehicles will be exchanging data with other entities, path tracking becomes a feasible threat. What is more, the passive collection of data will enable the attacker to keep track of driver's and/or vehicle's issues (e.g. behavior, preferences, characteristics, etc.) and their automatic analysis [17], [43], [44].

To address the privacy issue, a plethora of contributions have been proposed so far. Several approaches have mainly focused on public key cryptography based on certificates [45], or ID-based (i.e. certificateless) cryptography [8]. Traditional PKI authentication systems were not designed to provide any privacy protection [23] [22]; thus, in typical PKI approaches, the use of certificates leads to unnecessarily revealing the identity of their holders as well as other privacy-sensitive attributes [24]. In a more privacy-preserving way, the use of pseudonyms has been proposed. Pseudonyms are different identities to conceal the real one to unauthorized parties [7]. However, privacy threats are still possible when a pseudonym is used in scarce networks [22], where even small correlations of data could reveal sensitive information.

In a smart city context, when a driver or vehicle requests a resource or service using VANET communications, the provider only needs to verify if the vehicle is authorized to access the requested issue. However, revealing more information than necessary could lead to privacy risks [50]. Thus, achieving *minimum information disclosure*, that is minimizing as much as possible the disclosed information (attributes in this case) to achieve a goal, is of utmost relevance. This property contributes to avoid data inference from a service

provider or a collusion of them. Credential holders (e.g. drivers) must be able to disclose a subset of credential attributes without giving away their identity or other private information. In order to achieve this goal, Attribute-Based Credentials (ABCs) have been explored [57], [47].

ABCs are slowly gaining momentum, and yet a number of ABC theoretical approaches exist [40], [13], [39], [35]. Regardless of ABC benefits, few proposals have suggested applying them in the field of VANETs. [38] presents challenges and open issues regarding privacy and identity management in vehicular communication and point out ABCs as a potential solution for addressing privacy needs in generic scenarios; neither specific scenarios are discussed, nor an evaluation of ABCs applicability or technical feasibility is introduced. Authors in [52] introduce a conceptual framework including the use of ABCs, to provide trustworthy vehicular communications, in their work, authors highlighted the need of evaluating different ABC technologies in order to assess both: the privacy features offered by each technology and their technical feasibility for VANET environments. ABCs could enable, for instance, showing that a driver is neighbour of a given zone, without actually disclosing his identity or real address. Nevertheless, developing such an application requires a theoretical and practical analysis on the suitability of each ABC technique. This would enable to take an informed decision on the best mechanism for each VANET application.

To address this issue, this paper presents a feasibility analysis of ABC techniques for the vehicular context which, to the best of the authors' knowledge, remains unaddressed. This issue has been pointed out as a research need [52] due to the complexity of these technologies [62]. Thus, the goal of this paper is to analyze how these systems can be adapted to VANETs and to assess if such adaptation is feasible and useful for VANET use cases. The analysis is focused on a subset of the aforementioned BSA services in which we identify privacy issues. We consider two major ABC systems – Idemix [13] and U-Prove [39] – which have not been assessed yet. This analysis is completed with a third system, an updated version of Persiano's ABC system [25], as it has already been applied to the VANET context. According to existing literature [31], our selection is consistent in that it represents the two major families of ABC systems, namely those based on blind signatures (U-Prove) and those based on zero-knowledge proofs (Idemix, Persiano). Furthermore, the ABC technology introduced in [4] was afterwards discarded by the authors who developed more efficient technologies based on the specifications provided by U-Prove and Idemix, and introduced them in [34] and [59] respectively. Authors in [26] proposed an anonymous credential system which was limited in functionality, since it did not provide all privacy features offered by Idemix and U-Prove. Therefore, we stick to the aforementioned alternatives since they are more complete and count with a working implementation.

The rest of the paper is organized as follows. Section 2 describes the related work. Section 3 introduces the required background. Section 4 shows the road traffic services in smart cities that can benefit from ABCs. Section 5 focuses on how to adapt these techniques to the VANET context. Section 6 performs a

suitability assessment of the so-adapted ABC technologies. Section 7 highlights several open research directions. Finally, Section 8 draws the main conclusions of the paper.

2 Related work

Credentials are essential in identity management systems. They attest that an entity (e.g. user or vehicle) has a certain type of feature, knowledge, skill, etc. A credential can be composed of attributes with attached values, e.g. $degree =$ "*science*" or $driverLicense =$ "*yes*". In the field of VANETs, public key digital certificates [27] are one of the most used types of credentials. They attest that an entity holds a particular public key. Their use is specially associated with providing authenticated communications, as well as integrity and confidentiality in interchanged messages. By contrast, in multiple scenarios (e.g., parking payment) identity disclosure is not a mandatory requirement, since only attribute verification is needed. As a privacy-preserving solution to the problem Brands presents the concept of digital credentials [9], as an instantiation of pseudonymous systems proposed by Chaum [14]. One main point is that credentials involve attributes of an entity without including identity information which allows linking the credential to its owner. Furthermore, assuming that security and privacy are among the most relevant aspects in VANETs, the actual driver identity has to be revealed only to authorized entities, as it could be used for malicious purposes otherwise [7]. Therefore, credentials are the first step towards anonymity management.

Anonymity is the state of being not identifiable [42], which actually means much more than just identity preservation. Questions like 'why should I reveal the age of my vehicle when just the tax records are requested?' or 'why should I reveal my postal address when just the driving license is needed?' are at stake. Chaum was one of the first researchers to provide an answer to this kind of questions [14]. He envisioned anonymous credentials systems. His approach is based on a cryptographic scheme called blind signatures in which signers neither learn the signed message nor the identity of the individuals who request signatures except for uncommon occasions, e.g. a court order.

An anonymous or Attribute-Based Credential (ABC) system consists of users who obtain credentials from organizations and prove the possession of such credentials without disclosing values within them. In these systems, transactions carried out by the same user may not be linkable each other.

Several works have been developed in relation to anonymous credentials. [36] presents an attribute-based access control protocol to manage access to services. In that work anonymous credentials are used to protect vehicles' privacy but without detailing management processes. In [55] an identity-based encryption system in VANETs is proposed to achieve the privacy users desire and the traceability required by government authorities. However, the way anonymous certificates are applied is generally described but not detailed. Büttner et al. [11] propose a system in which anonymous credentials are used

to get attribute-based authorization tickets. The system is described but specifications regarding credentials management are not provided. More recently, PUCA, a pseudonym scheme with user-controlled anonymity for VANETs is presented [20]. Anonymous credentials are used for authentication purposes in car-to-X communications applying Camenisch et al. approach [13]. Chim et al. [16] propose a VANET-based secure navigation protocol which takes advantage of anonymous credentials to provide secure navigation services to drivers. In that work anonymous credentials creation and management follow Chaum's approach which was later enhanced by Brands [9] as well as Camenisch and Lysyanskaya [13]. Also looking for anonymity Raya et al. [46] present a protocol based on anonymous keys to conceal vehicles' identity. However, though anonymous keys can be compared to credentials, their management and use is analogous to that of a public key infrastructure. J. Petit et al. [41] present a survey of pseudonyms schemes in VANETs noticing that pseudonym-based credentials must be efficient to support real-time requirements in applications. It can be extrapolated to anonymous certificates as it is pointed out that anonymous credentials are one way of implementing one-time pseudonyms.

Apart from anonymous credentials theoretical approaches, two main implementations of these systems have been developed – U-Prove technology from Microsoft [39] and Idemix from IBM [13]. Some proposals have compared their developments against these technologies, e.g. [35] and [60] assess the efficiency of implementing U-Prove and Idemix in smart cards respectively. Specifically in the vehicular context, to the best of the authors' knowledge only Gonzalez-Tablas et al. [25] propose and implement an ABC system, namely a VANET-updated version of Persiano et al. scheme [40].

3 Background

This Section provides the reader with an introduction to VANETs (Section 3.1) and a brief description of the three Privacy-ABC techniques considered in this paper, namely U-Prove, Idemix and the VANET-updated version of Persiano (Section 3.2).

3.1 Vehicular Ad-hoc Networks (VANETs)

Information and communication technologies in the vehicular context encouraged the emergence of new services called Intelligent Transport Systems (ITS) [61]. ITS facilitate the presentation of immediate and accurate information concerning road traffic status or entertainment services, e.g info about nearest shopping malls or restaurants. Therefore, ITS can be seen as an instantiation of Location-Based Services (LBS) [53]. However, ITS also consider other traffic- and safety-related aspects for the service provision.

In order to realize ITS, different architectures have been proposed. Apart from regional initiatives, such as the European ITS architecture [21], standardized approaches are gaining attention. In particular, ISO 21217 standard

defines the entities at stake as well as their internal structure. Thus, the main elements are Road-Side Units (RSUs), On-Board Units (OBUs), central ITS stations and personal ITS stations. Each one is introduced below.

RSUs are communication nodes placed aside roads to behave as a proxy between vehicles and infrastructure. On the other hand, OBUs are vehicle-mounted devices to allow the exchange of data with RSUs and other surrounding OBUs. These devices are resource-constrained, which poses a performance challenge when designing applications and services. Central ITS stations are infrastructure elements that provide with ITS-based services. Finally, personal ITS stations are portable devices that may offer services to its owner (say the driver or a passenger).

In order for these entities to communicate with each other, different technologies may be applied. In particular, both short-range and long-range alternatives are considered. For short range, Dedicated Short Range Communications (DSRC) are being developed following standard family IEEE 1609 [29]. DSRC is reserved for automotive traffic safety applications using Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I/I2V) communications forming Vehicular Ad-hoc Networks (VANETs). On the other hand, 3G is representative for long-range communications.

From the architectural point of view, the said entities present significant similarities. On the one hand, all of them contain a gateway if they are connected to more than one network. For example, it is the case of OBUs, since they need to share information between its network and that internal of the vehicle. Similarly, they contain a router to exchange packets with other ITS entities. Considering OBUs again, the router enables V2V or V2I/I2V communications. Furthermore, a central element called ITS-SU (ITS Station Unit) properly handles each packet by executing applications.

As ABC-related protocols can be seen as applications themselves, in the following we focus on ITS-SU composition (Figure 1). Particularly, it is organized following an ISO-layered protocol stack. Thus, the access, networking and transport, facilities and application elements offer their services by leveraging on what the immediate inferior provides. Additionally, the management and security elements offer transversal services to the said components.

The security component is specially relevant for the sake of this work. In particular, Figure 1 shows its four sub-components. A firewall and an intrusion detection system prevent network attacks such as illegal accesses. On the other hand, an authentication, authorization and profile management cares about these procedures. For this purpose, it cooperates with the Security Management Information Base (S-MIB) which manages cryptographic credentials and certificates. These elements are stored in a special device called Hardware Security Module (HSM). This module is assumed to provide with secure storage, reliable time source and cryptographic capabilities [37].

One important remark is that the security aspects are not fully refined in ISO 21217. Particularly, the definition of which of the said elements (gateway, router, ITS-SU) have to carry out each security operation has not been clarified. For the sake of simplicity and without loss of generality, in this work we

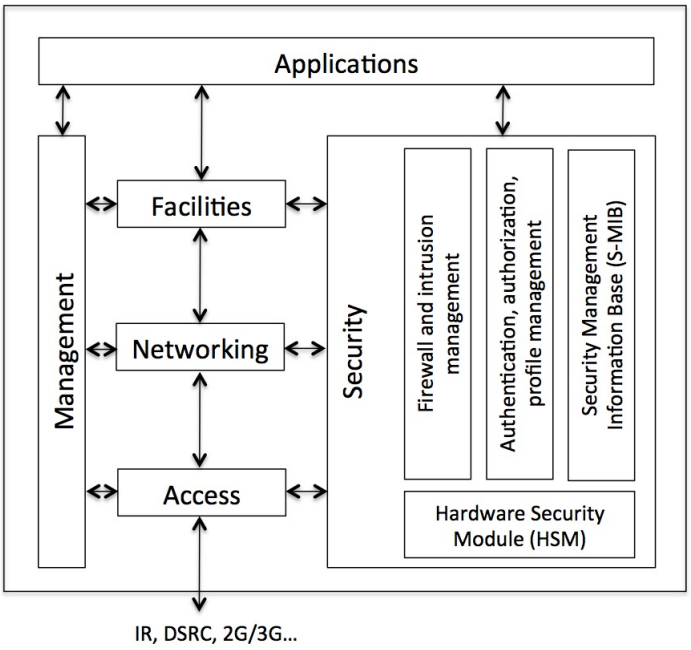

Fig. 1 ITS-SU architecture according to ISO 21217 [30]. The security entity is further decomposed

assume that ABC-related operations are carried out by the security component of ITS-SU.

3.2 Attribute-Based Credentials (ABCs). Fundamentals

Attribute-Based Credentials (ABCs) technologies have been designed to enhance users' privacy. For several years, they have been investigated as part of anonymous credential systems and group signatures [15]. ABCs are issued like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital (secret) signature key [47] – basically a PKI with privacy-enhancing features. In ABCs, the main enhancing feature is that credential's attributes could be transformed into *unlinkable* and *non-transferable* presentation tokens[1] able to protect the holder's privacy, while offering the same level of security. In the following sections participant roles and involved phases are described. The set of features provided by ABCs are presented in Section 3.4, after presenting each technique in detail.

3.2.1 Roles

Roles within a general ABC system are defined as follows:

[1] A presentation token is a digitally signed container of attribute information [48]

- Issuer: it is an infrastructure-based (trusted) identity provider also known as an attribute authority; this entity or organization is responsible of issuing credentials, that is, a certified container of attributes where an attribute has a type and a value (e.g., first name, Bob). It is also responsible for vouching for the correctness of the information contained in the credentials; therefore, the issuer might request other means of authentication prior to credential issuance.
- Users: entities to which the identity providers (issuers) will issue the ABCs. They will use these credentials to assert claims about their identity to service providers.
- Verifier: any relying party willing to protect access to resources, information or services.
- Revocation Authority: this entity is responsible for revoking issued credentials and preventing their further usage. A revocation authority is not a mandatory entity in typical ABC systems.
- Inspector: it consists of a trusted authority comprised of either a single entity or a multi-party cooperation. The inspector's role is to de-anonymize the user under specific situations (e.g., misuse or liability). The inclusion of this entity is not mandatory in traditional approaches. Ideally, the capability of inspection should be done in a distributed fashion, and it must be compliant with a policy that specifies which information should be recoverable by an inspector and under which circumstances.

3.2.2 Phases

In an ABC system the following phases are distinguished:

- Set-up: it is performed only once by each entity of the system. A trusted authority generates all public and secret global parameters used by the entities of the system. At the end of this phase, the issuer is ready to release credentials to users and the verifier is ready to validate such credentials.
- Issuance: an issuer can issue a credential without being related to any existing credential owned by the user.
- Presentation: it is one of the most important stages from the ABC lifecycle. Verifiers request a credential and users provide it (or a *presentation token* derived from it) to be later verified.
- Revocation: credentials are revoked by the revocation authority, which is also responsible for making available updated revocation information.
- Inspection: there are scenarios in which it is necessary to de-anonymize the credential holder. This is achieved by performing token inspection. Conditional anonymity is provided if and only if a token was generated in compliance with a policy specifying which information could be revealed and under which conditions. A typical example is the case of misbehaving nodes. The process of de-anonymization is restricted to authorized entities and it should ideally require a multi-party intervention.

3.3 ABC systems

This Section describes the considered ABC systems, namely Idemix [13], U-Prove [39] and the VANET-updated version of Persiano [25]. Note that the first pair of ABC technologies are jointly described due to their working similarities.

3.3.1 Idemix and U-Prove

Idemix (short for Identity Mixer) [28], developed and distributed by IBM, and U-Prove [33] of Microsoft are two examples of the most prominent ABC technologies currently available. Both technologies represent a suite of cryptographic libraries that can be combined into a functional ABC system. In terms of their construction, the main difference between the two technologies consists in the type of the digital signature scheme being used. While Idemix's main building block is the Camenisch-Lysyanskaya digital signature scheme [12], *U-Prove* [33] is based on the Brands' digital signature scheme [10] instead.

Both technologies support most of the common features of ABCs. However, there are some practical differences between them in the degree of privacy they provide (see Section 3.4), their efficiency and the methods that can be used to practically construct them. For instance, U-Prove's design allows the use of elliptic curves instead of standard subgroups, which could result in better efficiency. However, in this paper we focus on the available implementations, which are based on the latter.

Details on how both systems carry out each phase are given below (Figure 2):

- Set-up: it is performed once by each of the entities in the system except by the user. In the case of the Issuer, it generates a credential specification, issuer parameters and a secret issuance key used to issue credentials. The credential specification describes the type of attributes encoded in a credential and the corresponding encoding mechanism (e.g., cryptographic hash function). Issuer parameters are cryptographic information used by service providers to verify the authenticity of presentation tokens, i.e., Issuer's public key, identifier of a cryptographically secure hash algorithm, revocation information -if revocation process is supported, etc. The issuance key (secret key) needs to be kept secret and it is used by the Issuer to issue credentials.
- Issuance: issuance of a credential is an interactive protocol between the User and the Issuer, and works similarly for both Idemix and U-Prove. A difference in the protocol flow is the number of protocol rounds (and the corresponding number of messages during each round). In the case of Idemix, issuance of a credential is done in a single protocol round (two messages exchanged); the user first requests a credential, and if eligible, the issuer produces a credential by signing a statement containing the corresponding attributes [28]. In the case of U-Prove, it requires two rounds (four messages); the user first requests a credential, and if eligible, the

issuer generates a signature specific for the requested credential. Afterwards, the user generates a proof using the U-Prove token's public key, user and issuer parameters, on reception the issuer generates the corresponding credential. In both cases, the Issuer defines an issuance policy that describes the requirements that must be met by the User in order to get a credential, and contains the identifiers of the credential specification and the issuer parameters of the credential to be issued. The user receives the issuance policy and generates an issuance token. The issuance token contains cryptographic information required by the issuance policy, the token is generated from the token description and the proof generation (ZKProof). Upon reception, the issuer verifies the proof and generates the credential, i.e., a Zero-knowledge proof containing issuer's blind signature on the credential, the issuer-set attributes and if applicable the revocation information.

- Presentation: Idemix and U-Prove protocols work quite similar. For a particular requested policy a presentation token is delivered. The presentation policy may define the type of credential(s) that are accepted, which attributes must be disclosed, and potentially the predicates that should be used. Predicates over attributes consist of statements that allow the user proving certain property of an attribute value without disclosing the actual value (e.g., birthdate $< 1993/01/01$). The presentation token includes a cryptographic evidence for the possession of a credential by proving the knowledge of the credential secret by the User, token information such as validity period, and cryptographic commitments to the encoded attributes (a commitment is the product of generators with attributes and a secret key as their exponents). When the verifier receives the presentation token, it verifies that the statements are logically satisfied as well as the validity of the cryptographic evidence.
- Revocation: the revocation mechanism implemented for both U-Prove and Idemix, requires that both users and verifiers have the most recent revocation information from the corresponding revocation authority. There are two different settings for revocation, 1) issuer-driven revocation (global context), this approach requires that any presentation token should be proved against the most recent revocation information, which mainly requires online interaction. Additionally, nodes are responsible for updating their non-revocation evidence, which can derive potential privacy risks due to timing correlations, especially when performed at presentation time; 2) verifier-driven revocation (specific context), this approach can be done offline, it consists of a black list of attribute values managed by the verifier. It is worth mentioning that this approach will only affect the specific verifier and does not have any global effect.
- Inspection: Idemix and U-Prove share the implementation of a mechanism that only supports one inspector. This entity is able to uncover inspectable attributes which can lead to the identification of the credential owner. Note that by default Idemix and U-Prove tokens are anonymous and can only become inspectable if defined in the presentation policy.

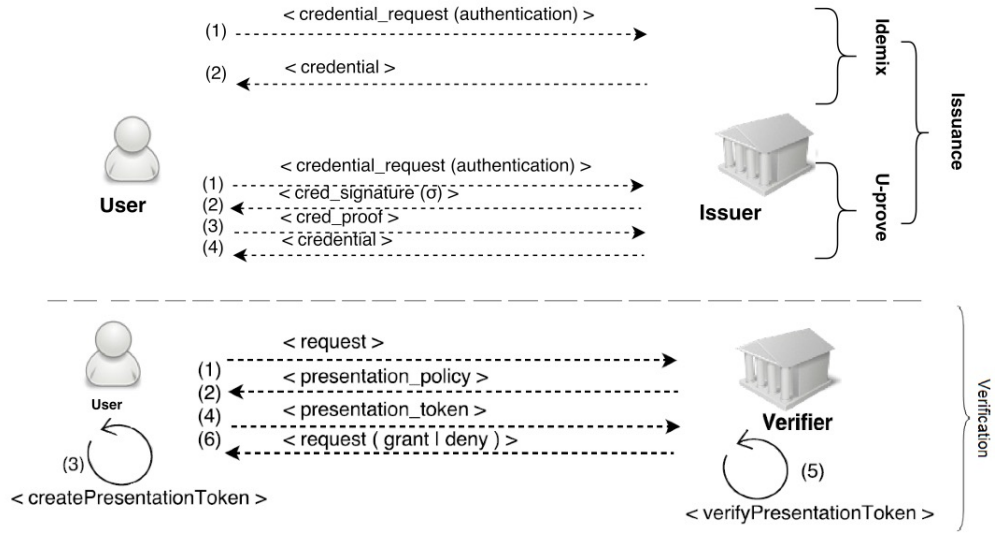

Fig. 2 Idemix & U-Prove protocol. Issuance and verification phases

3.3.2 VANET-updated Persiano

This technology is based on the use of anonymous credentials to prove their on-the-fly holdership in the context of VANETs for motor vehicles. Its phases work as follows (Figure 3):

- Set-up: as in previous techniques, public and secret parameters are established. In this updated version, each user receives a set of single-use certificates each of them linked to a pseudonym ($\overline{CERT}$).
- Issuance: the user requests a credential and demonstrates the possession of certain attributes (in a non-anonymous fashion). Once the proof is successful the issuer provides a signed credential whose signature is finally verified.
- Verification: the user and the verifier enrol in a credential joint proving process, comprised of an offline and an online part. In the former part the user creates a set of commitments and proves their ownership constructing four Zero Knowledge Proof of Knowledge (ZK-PoKs). In the online part, the verifier requests a presentation token (called proof) and the user provides the computed ZK-PoKs (and one certificate of the set $\overline{CERT}$). Finally, when the verification is performed the result is published in a public repository which is later accessed by the user. This allows the user having feedback, which is specially useful when failing this verification involves sanctions.
- Revocation: the certificate of the set $\overline{CERT}$, involved in the creation of the presentation token, can be revoked. This action can be seen as a temporal

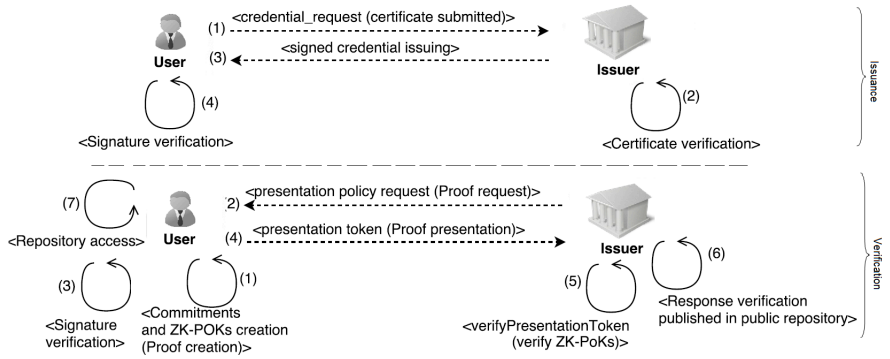

Fig. 3 VANET-updated Persiano protocol. Issuance and verification phases

de-registration of the vehicle (e.g. after verification, driving taxes are found to be unpaid).
- Inspection: certificates within the set $\overline{CERT}$ allow the retrieval of the user's identity for the authorized entity (i.e. traffic agency). In this way, it is possible to de-anonymize a given credential holder when needed.

3.4 Privacy features. Analysis per mechanism

This section introduces the most relevant features provided by ABC techniques and compares them against each mechanism. Eleven privacy features can be identified:

- Issuance unlinkability: the issuer cannot link an issued credential to the presentation of such credential.
- Multi-show unlinkability: a credential can be used multiple times without the resulting evidence becoming linkable.
- Selective disclosure of attributes: allows users to prove only a subset of attributes to a verifier.
- Predicate proof: it consists of statements that allow to prove a property of an attribute without disclosing its actual value. Example of these statements are the logical operators $>$ or $<$.
- Proof of holdership: a cryptographic evidence for proving ownership or possession of a credential without disclosing the attributes contained in that credential.
- Non-transferability: key binding can be used to bind one or more credentials of the a user to the same secret and discourage users to perform credential pooling.
- Scope-exclusive pseudonyms: a certified pseudonym unique for a specific scope and secret key, i.e. a single pseudonym can be created for each credential.

- Carry-over attributes: it relies on the assumption that the user already possesses a credential, from which a given attribute can be carried over into the new credential without disclosing the attribute value to the Issuer.
- Cross-credential proofs: it allows users to prove relations between attributes from two or more credentials without revealing them to the verifier. For instance, that the name contained on a credit card and on a passport match.
- De-anonymization: it is an optional feature that allows an authority (either alone or in cooperation with other entities) to reveal the identity of users in cases of accountability and non-repudiation.
- Revocation: in case of misuse, it allows the revocation of issued credentials to (misbehaving) users. Thus, revoked credentials cannot longer be used to generate presentation tokens.

Based on the aforementioned features, the chosen mechanisms are compared in terms of their supported privacy and privacy-influencing features. Table 1 summarizes the main results, where $\surd$, P and $-$ respectively denote that a feature is completely, partially or not provided.

Table 1 ABC features comparison

	Persiano updated	Idemix	U-Prove
ABC privacy-influencing features			
Issuance show unlinkability	$\surd$	$\surd$	$\surd$
Multi-show unlinkability	$\surd$	$\surd$	$-$
Selective disclosure	$\surd$	$\surd$	$\surd$
Predicates proof	$\surd$	$\surd$	$\surd$
Proof of holdership	$\surd$	$\surd$	$\surd$
Non-transferability	$\surd$	$\surd$	$\surd$
Scope-exclusive pseudonyms	$-$	$\surd$	$\surd$
Carry-over attributes	$-$	$\surd$	$\surd$
Cross-credential proving	$\surd$	$\surd$	$\surd$
De-anonymization	P	$\surd$	$\surd$
Revocation	$\surd$	$\surd$	$\surd$

All three given technologies provide Issuance unlinkability, while only Idemix and VANET-updated Persiano provide natively the functionality of multi-show unlinkability. In the case of U-Prove, to be able to guarantee unlinkability, the use of the same token in two different transactions must be avoided.

The three technologies enable attribute hiding, selective disclosure of attributes, and use of predicates over certain attributes, which make them suitable for scenarios where minimal information disclosure must be guaranteed.

Also, all three technologies support anonymous proof of possession of a credential, which allows users to prove holdership of a credential without disclosing the credential, as well as the non-transferability of credentials, aimed at discouraging users to perform credential pooling and at the same time enforcing non-repudiation.

Limited usage of credential and scope-based pseudonymity are both supported by U-Prove and Idemix, this is particularly useful in scenarios where users are restricted to a single pseudonym for a given scope, e.g. for accessing a certain website where multiple votes from the same user should be avoided.

Carry-over attributes is a feature that is supported by Idemix and U-Prove, while cross-credential proofs are supported by the three ABC schemes. The latter is a highly relevant feature in scenarios where the user is offered to access either joint services or a single service that requires to prove holdership of two or more credentials e.g., a service related credential, and an authority based credential. Finally, in cases of user misbehavior, both revocation and de-anonymization are supported by the three schemes, providing in this way the possibility of accountability. However, Persiano offers de-anonymization in a more constrained way than the other mechanisms, since it does not involve multi-party cooperation to reveal the identity.

4 Road traffic services benefiting from ABCs

After presenting the background on VANETs and ABCs, this Section focuses on motivating why applying the latter to the former. In recent years, smart city services built on top of VANETs are being proposed. Among them, ETSI TR 102 638 [18] points out a set of them to be available in the "day 1", thus being specially relevant for the early development of smart cities. This set is referred to as Basic Set of Applications (BSA). In this Section, the subset of applications of BSA that can benefit from ABC is identified, along with their related use cases. After analysing their privacy needs and considering the privacy features per ABC technique already introduced, this Section finishes with the election of the most theoretically suitable technique for each use case.

4.1 Applications and use cases

In BSA, four classes of applications are distinguished, namely Active road safety, Cooperative traffic efficiency, Cooperative local services and Global internet services. For each class different set of applications, use cases and attributes are distinguished. Among the 7 applications and 33 use cases of BSA, Table 2 depicts in bold those applications and uses cases that can leverage ABCs. For each one, the set of attributes at stake is identified, clarifying if they may be jointly proved (marked with J) or independently (I). Besides the applied communication protocol is also specified in Table 2. This may be an Internet connection through IPv6 or RSU communication through DSRC.

In the following, the use of ABCs in BSA applications is described, particularized per use case:

– **Enhanced route guidance and navigation**: RSU provides passing-by vehicles with travel itinerary information downloaded from servers based on

Table 2 Road traffic services for smart cities benefiting from ABCs. Legend: (J) joint proving, (I) single proving.

Applications Class	Application	Use case	Attributes	Com. protocol
Active road safety	Driving assistance - Co-operative awareness	-	-	-
	Driving assistance - Road Danger Warning	-	-	-
	Speed management	-	-	-
Cooperative traffic efficiency	**Cooperative navigation**	Enhanced route guidance and navigation	Positive current account (J), Already paid (I), Discount (J)	IPv6
		Limited access warning and detour notification	Reserved parking place X (J), Vehicle's owner lives in area X (J)	DSRC
Cooperative local services	**Location based services**	Automatic access control and parking management	Reserved parking number (J), Discount (J), Already paid (J), Positive current account (J)	DSRC
		ITS local electronic commerce	Positive current account (J), Already paid (I), Discount (J)	DSRC
		Media downloading	Positive current account (J), Already paid (I), Discount (J), Client of service X (J)	IPv6
Global internet services	**Communities services**	Insurance and financial services	Positive current account (J), Already paid (I), Discount (J)	IPv6
		Fleet management	Involved in fleet X (I)	IPv6
		Loading zone management	Vehicle type (I)	DSRC
	ITS station life cycle management	-	-	-

particular requirements. However, the interaction between vehicles and internet servers may involve some transactions. They may affect privacy due to requested data. For instance, to download an itinerary vehicles may have to attest that they have paid some fee. However, it has to be done anonymously, without disclosing any information of the vehicle or the driver. Anonymous credentials may attest a fee paid, the positive current account or the existence of a discount without disclosing further information.

– **Limited access warning and detour notification**: vehicles are warned of some road limit access, restriction or access control need. Other itinerary may be recommended to avoid a restricted area. Limitations may be related to the type of vehicle or, in general, it may be necessary to provide some information to gain access. For instance, a road that goes to a particular city district is closed to everybody except for those that attest they have a parking place in it. ABCs avoid showing the exact parking place of a vehicle but they allow attesting vehicles can park in a particular city district.
– **Automatic access control and parking management**: accessing or leaving a controlled area, e.g. a parking, requires the entitled vehicle to supply its identity. However, privacy is a key security issue in this regard. Providing information, such as having paid the monthly fee, having a particular parking place reserved, have a discount or a positive current account have to be carried out anonymously without disclosing vehicle's owner data and without being able to link multiple parking transactions of a given car.

- **ITS local electronic commerce**: RSUs signal some service, i.e. point of interest or location based service, which requires local payment for reservation and/or purchasing. Vehicles have to pay accordingly but without disclosing any private information. They may use anonymous credentials to attest that they have some kind of discount or prove they have paid it in advance.
- **Media downloading**: RSUs provide multimedia to passengers with or without internet access. Downloading can be conditioned by a commercial transaction. Therefore, multimedia access may depend on provided data, e.g. downloading a film has some cost, whose delivery should prevent privacy issues. The use of anonymous credentials to attest, e.g. after having paid a fee, owning a voucher to access free content or being client of the downloading service, avoids privacy data disclosures.
- **Insurance and financial services**: on demand and real time interaction to a financial or insurance service, e.g. pay as you drive. As in other applications the use of anonymous credentials for committing to a payment and for being authenticated preserves privacy avoiding the disclosure of more information than the one needed.
- **Fleet management**: RSUs provide and collect data from vehicles fleet management data. Vehicles can, for instance, apply anonymous credentials to attest their private involvement in a particular fleet. Thus, e.g., a bus of a given company entering a parking lot just requires a credential attesting the relationship between the bus (driver) and the company without disclosing any identifying information.
- **Loading zone management**: drivers, fleet managers and road operators need support regarding booking, monitoring and management of the urban parking zones. They have the possibility to book in advance an urban loading bay specifying the delivery mission, the planned delivery time frame, the loading/unloading time required, the vehicle type and the estimated time to reach the parking zone. Anonymous credentials can be used to provide information preserving privacy, e.g. without disclosing vehicle's owner identity when just the vehicle type is required.

Without ABCs, a naive provision of these applications involves the excessive disclosure of information, thus threatening users' privacy. For example, in case of economic transactions users have to provide their credit card information which discloses, among other issues, their names and surnames. Other examples are related to the vehicle's type and the parking place. In the former case vehicles' logbook shows vehicles' type and other data such as the vehicles' identity number or where/who sold them. In the latter case, the parking place can be attested showing drivers' identity card but it shows the exact location of drivers' home together with additional data like drivers' birth date.

4.2 Privacy requirements per use case

The set of identified use cases need privacy preservation to some extent. This Section explores which requirements are present for each one. Tables 3 and 4 summarize the analysis presented herein, where $\surd$ means needed, $\surd*$ desirable and $-$ not required.

A total of 12 general VANET privacy requirements have been identified across works by different authors [50], [17], [45], [20], [19]. One important remark is that most of them are the same than the identified ABC features. This aspect is relevant to decide which ABC technique to apply for each VANET use case. This issue is studied in Section 4.3.

Among these 12 requirements, 6 of them are privacy needs (Table 3) whereas the remaining 6 are privacy-related ones (Table 4). With respect to the first group, the first requirement is *minimal information disclosure*, by which vehicles and drivers may disclose a set of attributes while keeping others hidden [48]. This need is present in all use cases, as it means to minimize the data leakage to the remaining entities.

On the other hand, *conditional anonymity* allows drivers and vehicles to be de-anonymized in cases of liability (e.g. due to offences) [45]. This action must be restricted to authorized entities and under certain circumstances. This is also needed in all use cases as this deters misbehavior.

A related requirement is having *distributed (multi-party) inspection*, by which de-anonymization is carried out by cooperation of several entities to prevent abuses. This is required in some applications, such as ITS local electronic commerce. In this use case, the bank together with the particular electronic service should cooperate to de-anonymize. On the contrary, this is not needed in fleet management and loading zone management. In the former use case the fleet service is the only one interested in the inspection process and similarly, in the latter the loading entity/ manager is the only one who wants to perform the inspection process. Then, in both cases abuses are not a concern.

Regarding privacy-preservation by continuous observation of a given vehicle, *unlinkability* comes into play[2]. This prevents two different transactions performed by the same vehicle to be linked. There are two variants of this requirement, namely *issuance-show* and *multi-show* unlinkability. In the former, the authority issuing a credential cannot link the credential with the presentation tokens being shown to a service provider. Thus, it is not needed in use cases in which the issuing authority is the same that checks the credentials or belongs to the public domain, such as limited access warning and detour notification. The remaining applications have this requirement. Consider ITS electronic commerce, the credential attesting having a positive account balance can be provided by a bank authority and verified by a given service provider.

With respect to multi-show unlinkability, it allows drivers and vehicles to prove possession of credentials (i.e. present tokens) multiple times without

[2] It is worth to mention that untraceability is considered an inherent characteristic of unlinkability - if some entities are unlinkable, then they are untraceable.

being linkable across different sessions, transactions or domains. This is needed in all identified use cases except for media downloading and fleet management. In both use cases this requirement is desirable because even users are linked between different uses of a credential, they do not involve high privacy risk, in contrast to others like limited access warning and detour notification which, i.e., allow users tracking.

Another requirement is *perfect forward privacy* [50]. It states that the de-anonymization of one credential should only reveal information associated to such credential, and should not reveal any information that could decrease the unlikability of other credentials of the same user. This requirement is present in all use cases to prevent abuses by collusion of different service providers. Otherwise, de-anonymizing a misbehaving driver of the access control use case could lead to guess that she was the same buying a given service through ITS electronic commerce.

Concerning privacy-related requirements, the first one is *proof of holdership*. Thanks to this, vehicles and drivers have the ability to prove holdership of a credential to a verifier without disclosing the actual credential. As in the previous case, this is critical for all use cases because all of them need to verify the possession before granting the service.

On the other hand, *non-transferability* prevents credential pooling by binding a set of credentials to a user's (e.g. vehicle owner or driver) secret key. In this way, several users cannot collude to get a service that would be unattainable for them separately. Remarkably, this need is not present in fleet management, since a vehicle belonging to a company's fleet may be driven by any employee, so the credential must be transferable between drivers.

The *revocation* requirement allows invalidating a credential when needed. This may be because of compromise (e.g. stolen vehicle) or due to credential refreshing (e.g. a vehicle's owner changing his parking place). These two reasons may be present in all use cases, thus motivating this need for all of them.

Some use cases also require *scope-exclusive pseudonyms*. These pseudonyms are unique for a specific scope or application. This allows the provider to profile drivers and/or vehicles by ensuring that a single pseudonym is created from a corresponding credential. Four use cases have this requirement, namely enhanced route guidance and navigation, ITS local electronic commerce, media downloading and fleet management. The first three applications may involve belonging to a particular service, thus owning a credential regarding the use of such service. Additionally, fleet management involves attributes related to membership of a fleet which are limited to this scope. This requirement is desirable in all cases but not mandatory because, among other issues, these credentials are not expected to be used in other scenarios. Likewise, even these credentials were used in different scopes, these use cases do not involve high privacy risk by just avoiding the satisfaction of this requirement.

In scenarios in which service providers need to verify different credentials from a given user, *cross-credential proving* may appear. Thanks to this, multiple credentials from the same or different issuers can be jointly proven in

the same presentation token; with this feature vehicles and drivers are able to access joint services offered by different providers. This is the case of all applications except for fleet management and loading zone management. Credentials can be provided by, for instance, bank authorities, e.g. to attest positive balance; web services, e.g. to attest users membership; or council authorities, e.g. to attest the ownership of a parking place in a concrete area. For example, in Media downloading it may be needed to proof membership and a positive balance in the bank account. Conversely regarding fleet management and loading zone management, the use of a single credential is identified and thus, this property does not apply.

Last but not least, *carry-over attributes* allow that newly issued credentials may contain attribute values from other credentials without the issuer learning them. This feature is specially relevant in VANETs since some current credentials (e.g. taxes, licenses, etc.) are periodically renewed. It may be relevant to accumulate the seniority. It is a desirable property in all use cases except for fleet management and loading zone management as the credentials at stake are not likely to be renewable.

Table 3 Summary of privacy properties needed for each application.

	Minimal information disclosure	Cond. Anonymity	Issuance show unlinkability	Multi-show unlinkability	Distributed (multi-party) inspection	Perfect forward privacy
Enhanced route guidance and navigation	√	√	√	√	√	√
Limited access warning and detour notification	√	√	-	√	√	√
Automatic access control and parking management	√	√	√	√	√	√
ITS local electronic commerce	√	√	√	√	√	√
Media downloading	√	√	√	√*	√	√
Insurance and financial services	√	√	√	√	√	√
Fleet management	√	√	√	√*	-	√
Loading zone management	√	√	√	√	-	√

Table 4 Summary of privacy-related properties needed for each application.

	Proof of holdership	Non - transferability	Revocation	Scope-exclusive pseudonymity	Cross-credential proving	Carry-over attributes
Enhanced route guidance and navigation	√	√	√	√*	√	√*
Limited access warning and detour notification	√	√	√	-	√	√*
Automatic access control and parking management	√	√	√	-	√	√*
ITS local electronic commerce	√	√	√	√*	√	√*
Media downloading	√	√	√	√*	√	√*
Insurance and financial services	√	√	√	-	√	√*
Fleet management	√	-	√	√*	-	-
Loading zone management	√	√	√	-	-	-

4.3 ABC techniques per use case. Theoretical analysis

Once the analysis of privacy features per VANET use case has been presented, a theoretical selection of the most suitable ABC technique is presented herein.

In particular, recalling that each technique provides with a different set of privacy properties (recall Section 3.4), it is possible to determine which technique best fits for each use case.

In order to address this issue, it is necessary to clarify how ABC features and VANET requirements match. Particularly, it is noticeable that *Selective disclosure of attributes* and *Predicate proofs* Privacy-ABC features, are related to *Minimal information disclosure* in VANETs. Similarly, *Deanonymization* Privacy-ABC feature leads to *Conditional anonymity* and *Distributed inspection* VANETs properties. Moreover, *Perfect forward privacy* appears as a VANET privacy property which has not been currently implemented in Privacy-ABC.

Table 5 Analysis of ABC technique suitable for each use case.

	Idemix	**U-Prove**	**VANET-updated Persiano**
Enhanced route guidance and navigation	√	-	-
Limited access warning and detour notification	√	-	-
Automatic access control and parking management	√	-	-
ITS local electronic commerce	√	-	-
Media downloading	√	√*	√*
Insurance and financial services	√	-	-
Fleet management	√	√*	-
Loading zone management	√	-	-

Table 5 presents results of the analysis where √ means suitable, − the contrary and √* partially suitable. Concerning studied use cases, it is noteworthy that all of them can leverage Idemix since it provides with all privacy and privacy-related features.

On the other hand, media downloading can be addressed by all techniques though under several premises. U-Prove can be applied if multi-show unlinkability is avoided and Persiano updated can be used when scope-exclusive and carry-over attributes are not an issue. Besides, fleet management application can be applied by Idemix in any circumstances and by U-Prove as long as multi-show unlinkability is not at stake.

5 Tailoring ABCs to VANETs

Section 4 has shown different road traffic services for smart cities that could benefit from ABCs. Nevertheless, one open issue is how to adapt these mechanisms to vehicular networks. This section focuses on this matter. For this purpose, the VANET architecture presented in Section 3.1 is considered. Section 5.1 describes how each ABC role is taken by each VANET entity. Afterwards, Section 5.2 addresses how each phase is carried out in these networks.

5.1 Distribution of roles

This Section describes how each ABC role may be implemented in the VANET context.

- Issuer: this role can be taken by a regional vehicular registration authority, the vehicle manufacturer, public administration entities, or any service provider, such as telecommunication operators. The particular entity at stake depends on the considered ITS service. In any case, all of them are realized in a Central ITS station. In particular, there are two components of its ITS-SU at stake. The Applications one contains the issuance policy and the credential creation procedure itself. On the other hand, the Security one (and, in particular, its S-MIB and the HSM) is in charge of creating the credentials and storing the materials needed for future verification.
- Users: this role is represented by vehicles and drivers. In the case of vehicles, ABCs will be bound to the owner of the vehicle (e.g., individual or a company). This decision is in line with current laws in several countries in which the owner is liable for traffic offences until the driver gets identified (e.g. United Kingdom, [1]). Thus, the OBU-internal ITS-SU comes into play. Particularly, the Applications element dictates when authentication is required, whereas the Authentication module of the Security element carries out the related cryptographic processes. For this purpose, again the S-MIB and HSM will cooperate.
  In the case of the driver, it is her personal ITS station which participates in the process. The elements at stake are the same than in the vehicle case.
- Verifier: as it happened with the issuer role, different entities may be verifiers according to the service or application at stake. Thus, RSUs, other vehicles, public administration authorities (e.g., police, traffic authorities, etc.), and service providers (e.g., emergency services, location-based commercial services, etc.) may take this role. Therefore, this role may be performed through Road-side ITS stations, Central ITS stations or OBU stations. In all cases, the components at stake are Applications and Security in the same terms as in the issuance.
- Revocation authority and Inspector: revocation is a requirement to prevent misbehaving or faulty vehicles to communicate and threat the proper operation of the network. To this extent, the Inspector becomes active in cases of accountability. These roles are mainly taken by the regional vehicular registration authority. Vehicle manufacturers and service providers may also take these roles in particular cases such as misuse. As in the previous cases, Central ITS stations are at stake, particularly their Applications and Security components.

5.2 Implementation of phases

This Section shows how the general ABC phases (recall Section 3.2.2) are implemented in VANETs. Each one is studied below. We omit the sequence

diagram for the Revocation phase since it is an internal process carried out by the credential issuer.

- Set-up: all entities have to be equipped with required cryptographic materials. Importantly, credentials issued by a trusted CA (regional vehicular authority) are stored in the HSM of the ITS entity at stake (Roadside ITS station, OBU ITS station, Personal ITS station). The procedure is shown in messages 1-11 of Figure 4. Management and distribution of the credential specification and issuer parameters can be done either leveraging on regular vehicular processes (e.g. yearly inspection, tax renewal, etc.) or using Over-The-Air (OTA) updates managed by the Security component. It must be noted that secure OTA software updates have already been considered for vehicular platforms [51].
- Issuance: this phase is shown in messages 12-27 of Figure 4. At first, the vehicle will provide either the CertID or the full certificate to the issuer (msg. 12). Such certificate could also consist of a short-term certificate based on an underlying pseudonym solution. The vehicle may provide with the requested proofs as introduced in Section 3.3. On successful validation, the Issuer will then prepare the corresponding ABCs (msgs. 13-19). Simple issuance in VANET will include key binding (i.e. making two or more credentials bind to the same key). This will discourage users in VANETs to give away their credentials. Moreover, service providers may request users to prove that they are authorized to communicate in the VANET system, and at the same time authorized to access their resources. Thus, a proof of holdership of multiple credentials bound to the same key (i.e. cross-credential proving, recall Section 3.4) is needed. Carry-over credentials may also be issued, as a means of adding new properties to existing credentials (e.g. extensions to the insurance policy). Once created, these materials are sent to the OBU HSM (msgs 20-27).
- Presentation: this phase starts by creating the commitments that will be at stake to anonymously prove one or more attributes. The procedure is shown on Figure 5. For the sake of simplicity, the message in which the prover asks for credentials is omitted from Figure 5. Thus, after the said creation (messages 1-10), the verifier asks for the required proof considering a given policy (msg. 11). The Application component of the OBU collaborates with the Security MIB and the HSM to build up the presentation token according to the specified policy (msgs. 12-24). The Application at the verifier then checks the token validity and the commitment correctness (msgs. 25-39). It must be noted that for this purpose its Security MIB and HSM are involved.
- Revocation: there can be many reasons for revoking a credential, e.g., a malicious attacker sending spoofed or forged information that might jeopardize the security and safety of vehicles in the network. This process is carried out by the authority, being this information spread to all VANET entities to ensure a proper exclusion of revoked parties.

– Inspection: this task has to be done by an authorized entity. In the VANET context, the traffic authority is the ideal holder of this matter. Other trusted service providers (e.g. technical inspection facilities) may take this role as well. The process is shown on Figure 6. In this case, the central ITS station's HSM is used to open the commitment (msgs. 1-5). This leads to obtaining the pseudonym under which the vehicle is operating. Based on this information, the Security MIB reveals which is the real identity of the misbehaving vehicle (msgs. 6-9).

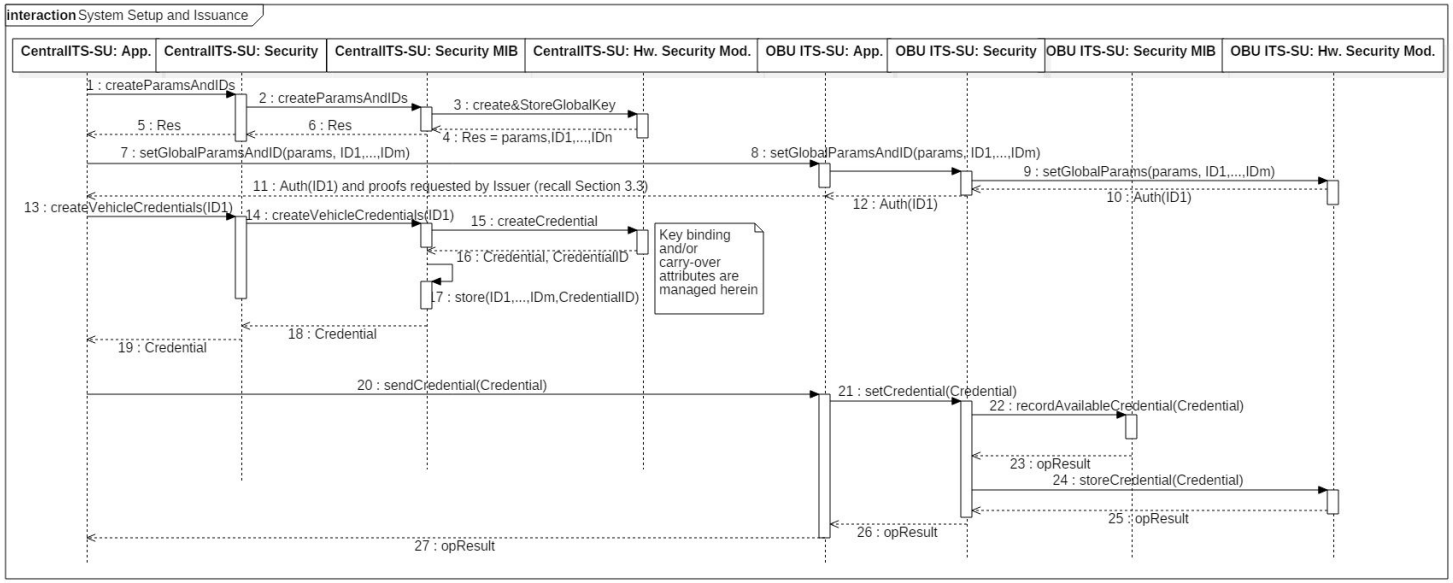

Fig. 4 Setup and issuance phases of ABC according to VANET architecture

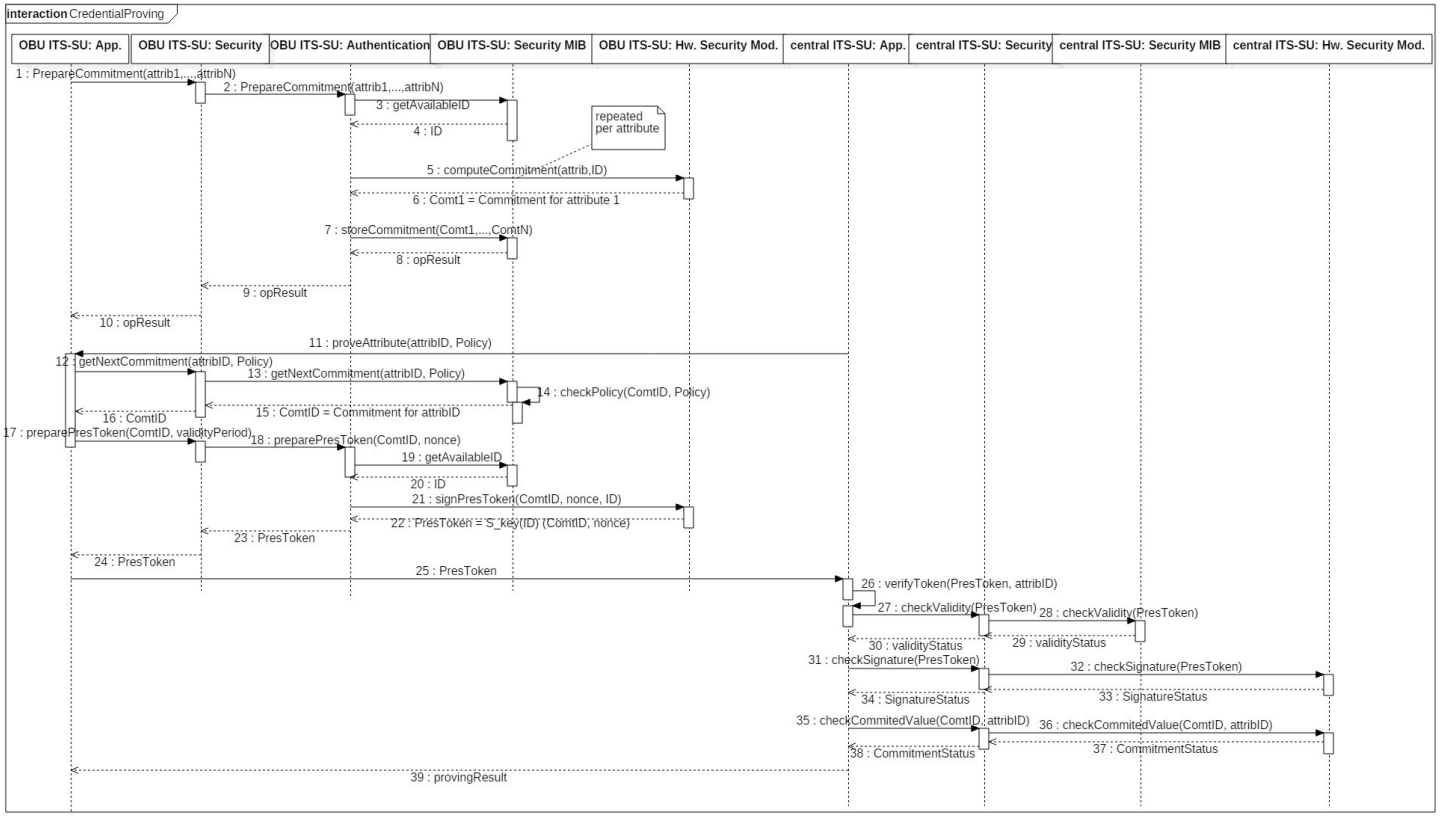

Fig. 5 Presentation phase of ABC according to VANET architecture

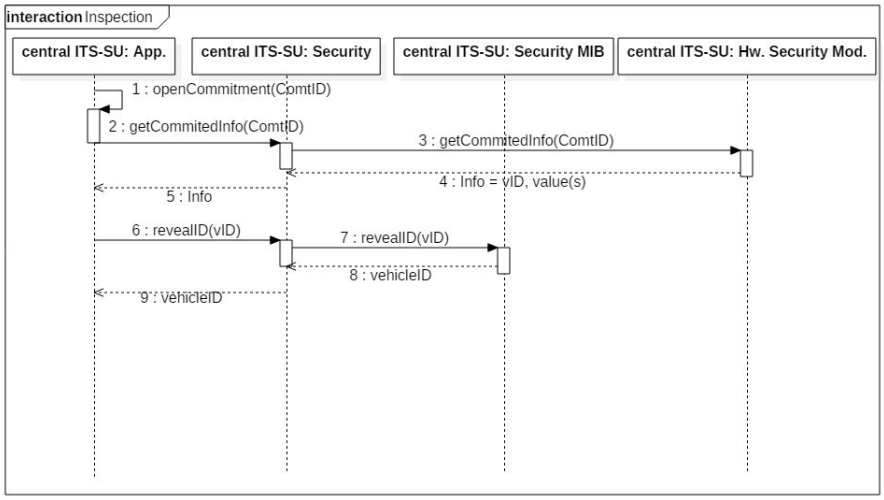

Fig. 6 Credential inspection phase of ABC according to VANET architecture

6 Performance assessment

While the previous Section focused on how ABCs may be integrated into VANETs, this Section assesses the suitability of the said integration. Particularly, a performance comparison between Idemix, U-Prove and VANET-updated Persiano is presented. Considering this aspect as well as the provision of privacy properties (recall Section 3.4), Section 6.3 discusses the feasibility of each ABC technique in the considered use cases.

For this assessment, we have adopted the framework for evaluation of Privacy-ABC technologies proposed in [58]. We enhance this framework by considering additional criteria particularly useful for understanding the potential of ABCs in VANETs. Accordingly, we show empirical results obtained from a quantitative analysis focused on latency. We have used the ABC4Trust reference implementation [6] of a unified architecture for ABC technologies, which currently integrates Idemix and U-Prove technologies, and the implementation of VANET-updated Persiano introduced in [25].

For the sake of simplicity, we did not use all of the criteria described in [58], but only those elements that were common for the three technologies and which we considered to be suitable for the scenarios we have chosen. Particularly, we evaluated the time taken for system *setup*, *issuance*, as well as time to do a *presentation*, which is split into two parts, namely *proving*, which happens at the User side (in our case, on the vehicle), and *verification*, which is done by the Verifier (in our case, by the Central ITS Station). For all these phases, this assessment focuses on the computational time taken on same machine configurations. It must be noted that this time is independent of the particular road traffic scenario. Thus, network-related incidental factors

such as the road design (which may affect coverage range) or vehicular density (which may alter channel availability) are left out of the analysis. Therefore, our analysis shows an unavoidable, lower-bound time taken to carry out these computations.

6.1 Experimental setup

We have considered different setups for the different entities, namely the Central ITS station and the OBU. In order to provide a modest setup for the Central ITS Station, we used a machine with an 8-core i7 CPU of 2.3 GHz and 8 GB of RAM. Regarding the OBU, we simulated the experiments on a less powerful machine with a 3-core CPU of 460 Mhz and 256 MB of RAM, comparable to state-of-the-art devices, such as the OBU-201U[3]. Thus, each of these machines carry out the steps and operations that correspond to its entity in every ABC technique.

We have performed a number of simulations using varying parameters, such as the number of attributes in a credential, disclosing (hiding) attributes, and increasing the key size for the crypto operations. For the sake of clarity, the performance of each phase for the three technologies is discussed separately. Each experiment has been run 50 times, showing the average herein. We assume credentials with 2, 5 and 10 attributes and key sizes 1024 and 2048 bits. We believe these values are representative, and appropriate from the security point of view [56]. Appendix I presents the main data obtained from experiments, which are discussed herein.

6.2 Performance results

Regarding system setup (Figure 7), all steps to generate the necessary cryptographic materials, including the public-private key pairs of the Issuer and Verifier, are measured. The most efficient technology regarding this phase is U-Prove, which completes the system setup in 2.5 s and 24.3 s for key sizes 1024 bits and 2048 bits respectively, followed by VANET-updated Persiano with 5.6 s and 38.5 s and U-Prove with 14.8 s and 58.5 s for key sizes 1024 bits and 2048 bits respectively. Results show a significant increase for 2048 bits key, being specially remarkable in U-Prove whose suffers an increment of 1200%.

With respect to issuance (Figure 7), a credential with 5 attributes using a 1024 bits key with VANET-updated Persiano takes on average 0.09 s, with U-Prove 2.1 s, whereas with Idemix 2.8 s For 2048 bits key, though the increase of VANET-updated Persiano is the highest one, it continues being the technology which produces the lowest impact in the issuance phase, it takes 0.6 s in comparison with U-Prove and Idemix which take 5.5 s and 3.4 s respectively. According to Section 3 these results are expected because U-Prove requires two

[3] http://unex.com.tw/v2x/obu-201u, last accessed January 2017.

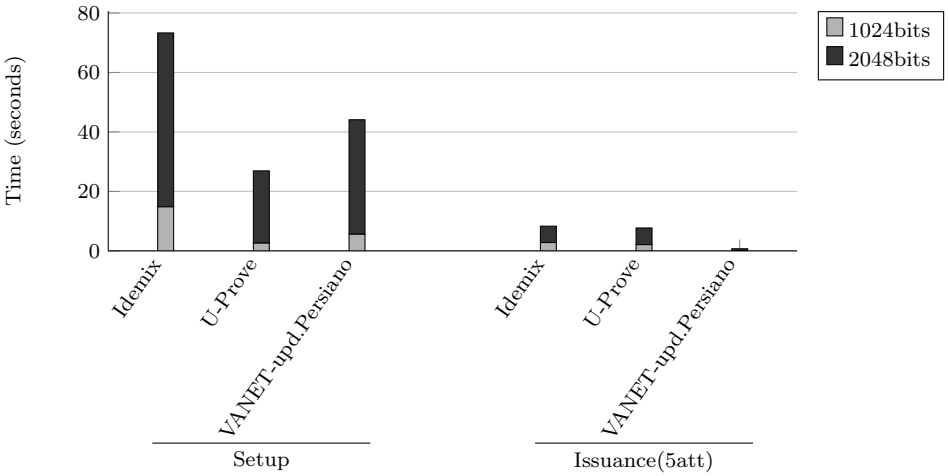

Fig. 7 Evaluation for the impact of setup and issuance for all three technologies.

rounds to complete the issuance while Idemix requires one. Likewise, VANET-updated Persiano needs to demonstrate the possession of attributes in an non-anonymous fashion. Note that, according to our experiments, issuance time is independent of the number of attributes and thus we have chosen 5 attributes as a representative value.

Certainly, the most relevant results for the use of these techniques while driving are those related to the presentation of Privacy-ABCs. In particular, proving possession of credentials (by the OBU) and verification of such proofs (by the Central ITS) are at stake. We have studied the performance for the three technologies using a cryptographic key size of 1024 bits when presenting a credential with 5 attributes and iteratively disclosing attributes (Figure 8). It is identified that Idemix is the best choice, as it presents the lowest time either for proving or verification, while U-Prove and VANET-updated Persiano are comparable. Moreover, the number of disclosed attributes does not significantly affect computation time.

Similarly, Figure 9 shows results for the same configuration but doubling the key size to 2048 bits. Though time increases in all technologies, the high computation time required in the proving phase is particularly remarkable in VANET-updated Persiano. Indeed, in this last technology credential proving requires the computation of ZK-POKs which are highly affected by the key size [25].

Finally, the impact of the number of attributes on the presentation time for all three technologies is assessed (Figure 10). Here, each technology is assessed when presenting (proving and verifying) credentials with respectively 2, 5, and 10 attributes using a key size of 1024 bits (2048 key size is not studied because VANET-updated Persiano produces very high impact, e.g. computation time for proving higher than 22s.). It is identified that Idemix continues being the best alternative considering computation time and, though VANET-updated

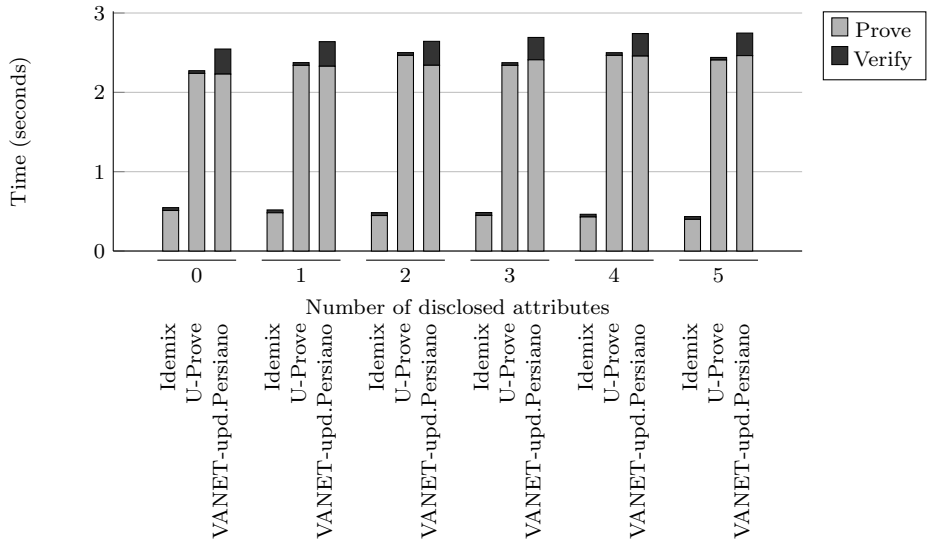

Fig. 8 Evaluation for the impact of the selective disclosure on the time efficiency of presentation. Results based on the key size of 1024 bits and a credential with 5 attributes for all three technologies.

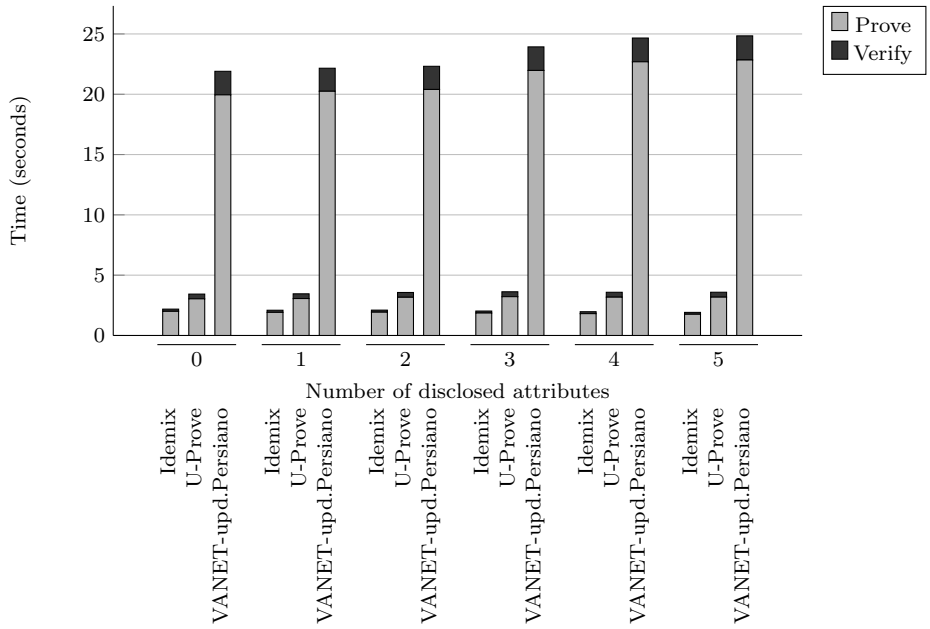

Fig. 9 Evaluation for the impact of the selective disclosure on the time efficiency of presentation. Results based on the key size of 2048 bits and a credential with 5 attributes for all three technologies.

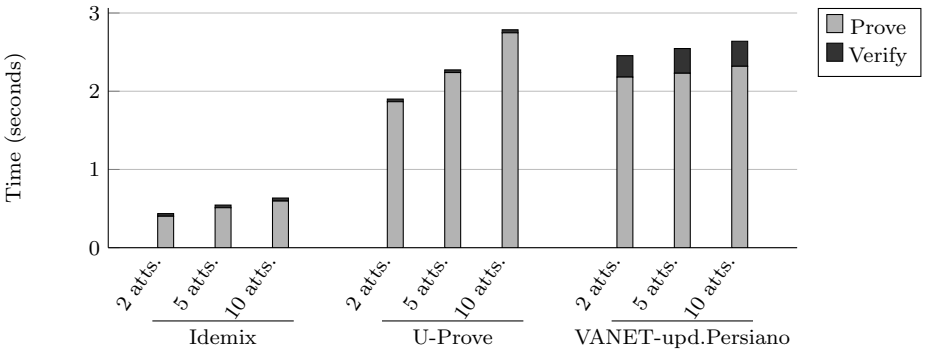

Fig. 10 Evaluation for the impact of the total number of attributes in a credential on the time efficiency of presentation. Results based on the key size of 1024 bits and no disclosed attributes for all three technologies.

Persiano is worse at verification, it is comparable with U-Prove at proving and even better when 10 attributes are at stake.

6.3 Feasibility analysis and discussion

Given the different nature of the use cases at stake, the time constraints can be determinant to adopt or reject ABC techniques. To this extent, in this Section the time taken to carry out each phase is studied.

The first point to consider is the high impact of 2048 bits key specially for VANET-updated Persiano. The use of this technology and key size is not recommendable for use cases when significant immediacy is demanding, e.g. automatic access control. This result may be produced by the fact that while U-Prove and Idemix have tested and well-known implementations, VANET-updated Persiano implementation has not reached such a high level of maturity.

Regarding setup and issuance, both phases are computed by trusted authorities which are assumed to have stronger computational capabilities. Furthermore, involved communication is not an issue since they may take place in controlled scenarios (e.g. technical inspection).

The proving and verification steps of the presentation phase are the main challenge to address. Although the use cases at stake are not safety-related, a practical feasibility threshold exists. In case that a given ABC mechanisms takes too long to execute, the vehicle may be far away from its original location when the protocol started. This renders some use cases impractical. For example, the *limited access warning* use case is intended to warn approaching vehicles. If ABCs involve a huge time for execution, the vehicle may have passed through the controlled area. Similarly, the *access control and parking* use case cannot wait for a long time in practice – the vehicle must be authorized prior to area entrance (for security) and it cannot be stuck for a long time

before leaving (for practical reasons). It must be recalled that this situation may get worse in geographically harsh scenarios or roads with high density, as the packet delivery ratio (which indicates the proportion of correctly received packets) decreases dramatically [2]. In such situation, re-transmission costs increase the mechanism latency. However, for the sake of consistency, in the following we leave networking aspects out of the discussion.

Considering these issues, our feasibility analysis concentrates on the distance traveled by the vehicle while computing the proving and verification phases in each ABC mechanism. Thus, considering 42 m/s (i.e. around 150 km/h) as driving speed, 1024 bits for key sizes and 5 disclosed attributes, the vehicle will be moving for 115.1 meters in VANET-updated Persiano, 102.5 meters in U-Prove and 18.1 meters in Idemix. If 2048 bits were considered, results would be affected specially in VANET-updated Persiano, requiring 1043.3 meters to complete.

Combining the previous results with the theoretical suitability of ABC mechanisms per VANET use case (recall Section 4.3), an overall suitability can be concluded. Thus, Idemix is the most suitable technique since except for the issuance phase, it offers the best performance results. The reduced driving distance is specially relevant for uses cases in which DSRC communications technology comes into play. Recalling Table 2, it happens in the *limited access warning*, *automatic access control*, *ITS e-commerce* and *loading zone management* use cases. According to our findings, data transmission has to be carried out in 300 - 18.1 = 281.9 meters driving distance for these use cases to be feasible, if 300 meters is taken as the effective communication range [2] and no geonetworking or RSU handover is considered. Of course, this threshold can be raised by relaxing any of the previous conditions.

On the other hand, *media downloading* is also feasible by using U-Prove or VANET-updated Persiano. Nevertheless, U-Prove is dramatically more efficient than VANET-updated Persiano. Particularly, as 4 attributes are at stake in this use case (recall Table 2), U-Prove is almost three times faster than VANET-updated Persiano. This difference is relevant if the anonymous authentication is to be carried out periodically (e.g. after each downloaded chunk), as the shorter the process takes, the faster the download is completed.

Finally, recalling that both Idemix and U-Prove can be applied in the *fleet management* use case, Idemix is the most suitable choice for performance issues and the only one if multi-show unlinkability is needed.

7 Open Research Issues

The use of ABCs into smart city services built on top of VANETs opens the door to three main research directions, namely the real-world implementation and assessment of this technology, the extension to other use cases and the improvement of the cryptographic primitives at stake.

Concerning the real-world assessment, the networking aspect of ABC is a critical factor. Our results support the computational feasibility of ABCs

in vehicular environments. Thus, they enable carrying out another step of experiments, which consider the impact of channel reliability. In particular, as vehicular density affects to the packet delivery ratio, it is important to assess the suitability of every ITS use case design in different road traffic scenarios, ranging from rural areas (with sparse RSU coverage and low traffic) to urban settings (with high RSU coverage and high density of vehicles).

Regarding the extension to other use cases, the following list may serve as a starting point for designing promising smart city services in which ABCs may be at stake:

- **Parking meter**: modern cities usually have parking meters spread around them. Parking cost is dependent on factors like the type or the age of the vehicle to park. Some parking meters require the user to type the vehicle's license plate. However, this enables a potential "big brother" effect by Authorities. Thus, parking meter tickets have to be delivered just taking into account particular factors.
- **Start the vehicle**: from the development of traditional keys to start vehicles until present time many techniques have emerged. Smart-keys are challenging developments in this regard which are applied by multiple carmakers [49]. These keys may have the look and feel of a card or just a small rectangular box. The point is that some vehicles may be driven by people who share some common features. For instance, bus drivers of company A are allowed to drive all buses of this company, thus each of them needs a personal key that attests their link with the company and can be used in all coaches. Furthermore, to avoid excessive surveillance, the actual identity of the driver should only be disclosed under particular circumstances (e.g. traffic offences).
- **Incentives for users profiling**: in VANETs content dissemination scenarios, users and service providers may find a privacy-preserving tradeoff – service providers will be able to build profiles from anonymized users and deliver personalized services, while users might receive other incentives in exchange of disclosing their attributes, such as, special offers or discount coupons [32]. It must be noted that users must be able to control the amount and linkability of the information disclosed.

Implementation issues of ABCs have to be considered as well. In particular, improving HSM native support for ABCs could dramatically improve the overall performance. On the other hand, the development of Proofs of Knowledge (PoK) based on lightweight cryptography would be also beneficial. As OBUs are resource-constrained devices, leveraging on cryptography for similar environments (such as Internet of Things [5] or smart health [54]) is a promising approach.

8 Conclusions

Road traffic services are essential in the future development of smart cities. They can be designed on top of the upcoming vehicular ad-hoc networks

(VANETs). However, privacy aspects in this scenario must be addressed prior to their deployment. Multiple cryptographic approaches have been developed in this regard, particularly those focused on traditional PKI systems. However, in many situations too much unnecessary data is delivered in contrast to the principle of *minimum information disclosure*. Attribute Based Credentials (ABCs) help to address this issue by allowing the disclosure of only the necessary data. In this paper, the suitability of three prominent ABC techniques (U-Prove, Idemix and VANET-updated Persiano) to VANETs has been studied. A set of smart city services, chosen from ETSI's Basic Set of Applications, has been considered for the analysis. Our results show that they are feasible according to current state-of-the-art devices and that they can be applied taking into account the standard vehicular architecture. Moreover, Idemix is the most promising approach for this scenario both in terms of performance and the set of smart city road traffic services that could adopt it.

Acknowledgements This work was supported by the MINECO grant TIN2013-46469-R (SPINY: Security and Privacy in the Internet of You); the CAM grant S2013/ICE-3095 (CIBER- DINE: Cybersecurity, Data, and Risks) and by the MINECO grant TIN2016-79095-C2-2-R (SMOG-DEV - Security mechanisms for fog computing: advanced security for devices). Jose Maria de Fuentes and Lorena Gonzalez were also supported by the Programa de Ayudas para la Movilidad of Carlos III University of Madrid. Authors would like to thank Prof. Kai Rannenberg for his comments on the earlier versions of this paper. Furthermore, Prof. Alejandro Calderon also gave us useful advices for the experiments. We also thank Dr. Hans-Joachim Fischer for his collaboration regarding ISO 21217 aspects. Finally, we thank the anonymous reviewers for their comments.

References

1. Lowe's Transport Manager's and Operator's Handbook 2016. KoganPage (2016)
2. Bai, F., Krishnan, H.: Reliability analysis of dsrc wireless communication for vehicle safety applications. In: Intelligent Transportation Systems Conference, 2006. ITSC '06. IEEE, pp. 355–362 (2006). DOI 10.1109/ITSC.2006.1706767
3. Barba, C.T., Mateos, M.A., Soto, P.R., Mezher, A.M., Igartua, M.A.: Smart city for vanets using warning messages, traffic statistics and intelligent traffic lights. In: Intelligent Vehicles Symposium (IV), 2012 IEEE, pp. 902–907. IEEE (2012)
4. Batina, L., Hoepman, J., Jacobs, B., Mostowski, W., Vullers, P.: Developing efficient blinded attribute certificates on smart cards via pairings. In: D. Gollmann, J. Lanet, J. Iguchi-Cartigny (eds.) Smart Card Research and Advanced Application, 9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010, Passau, Germany, April 14-16, 2010. Proceedings, *Lecture Notes in Computer Science*, vol. 6035, pp. 209–222. Springer (2010). DOI 10.1007/978-3-642-12510-2_15. URL http://dx.doi.org/10.1007/978-3-642-12510-2_15
5. Bertino, E., Choo, K.K.R., Georgakopolous, D., Nepal, S.: Internet of things (iot): Smart and secure service delivery. ACM Transactions on Internet Technology (TOIT) **16**(4), 22 (2016)
6. Bichsel, P., Camenisch, J., Dubovitskaya, M., Enderlein, R., Krenn, S., Krontiris, I., Lehmann, A., Neven, G., Nielsen, J.D., Paquin, C., Preiss, F.S., Rannenberg, K., Sabouri, A., Stausholm, M.: D2.2 Architecture for Attribute-based Credential Technologies - Final Version. *ABC4TRUST* project deliverable (2014). Available online at https://abc4trust.eu/index.php/pub
7. Biswas, S., Haque, M.M., Misic, J.V.: Privacy and anonymity in vanets: A contemporary study. Ad Hoc & Sensor Wireless Networks **10**(2-3), 177–192 (2010)

8. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003)
9. Brands, S.A.: Privacy-protected transfer of electronic information. Tech. rep. (1996)
10. Brands, S.A.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge, MA, USA (2000)
11. Büttner, C., Huss, S.A.: Anonymous credentials and attribute-based authorization tickets in car-to-x communication. Fachgespräch Inter-Vehicle Communication p. 9 (2014)
12. Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: Advances in Cryptology.EUROCRYPT 2001, pp. 93–118. Springer (2001)
13. Camenisch, J., Van Herreweghen, E.: Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACM conference on Computer and communications security, pp. 21–30. ACM (2002)
14. Chaum, D.: Blind signatures for untraceable payments. In: Advances in cryptology, pp. 199–203. Springer (1983)
15. Chaum, D.: Security without identification: Transaction systems to make big brother obsolete. Commun. ACM **28**(10), 1030–1044 (1985). DOI 10.1145/4372.4373. URL http://doi.acm.org/10.1145/4372.4373
16. Chim, T.W., Yiu, S.M., Hui, L.C., Li, V.O.: Vspn: Vanet-based secure and privacy-preserving navigation. Computers, IEEE Transactions on **63**(2), 510–524 (2014)
17. Doetzer, F.: Privacy issues in vehicular ad hoc networks. In: G. Danezis, D. Martin (eds.) Privacy Enhancing Technologies, *Lecture Notes in Computer Science*, vol. 3856, pp. 197–209. Springer Berlin Heidelberg (2006). DOI 10.1007/11767831_13. URL http://dx.doi.org/10.1007/11767831_13
18. ETSI: Etsi tr 102 638 v1.1.1. intelligent transport systems (its); vehicular communications; basic set of applications; definitions. Tech. rep., ETSI (2009)
19. Feiri, M., Petit, J., Kargl, F.: Real world privacy expectations in vanets real world privacy expectations in vanets. In: 2nd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication, FG-IVC 2014, vol. TR-SnT-2014-4, pp. 30–32. Vehicular Lab, University of Luxembourg, Luxembourg City, Luxembourg (2014). URL http://doc.utwente.nl/93395/
20. Forster, D., Kargl, F., Lohr, H.: Puca: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (vanet). In: Vehicular Networking Conference (VNC), 2014 IEEE, pp. 25–32. IEEE (2014)
21. FRAME: European intelligent transport systems (its) framework architecture. Tech. rep., FRAME Forum (2011). URL http://frame-online.eu/
22. de Fuentes, J.M., Gonzalez-Manzano, L., Gonzalez-Tablas, A.I., Blasco, J.: Security models in vehicular ad-hoc networks: A survey. pp. 47–64 (2014). DOI 10.1080/02564602.2014.890844
23. Gerlach, M.: Assessing and improving privacy in vanets. In: 4th Workshop on Embedded Security in Cars (ESCAR 2006), pp. 1–11 (2006)
24. Gerlach, M., Gattler, F.: Privacy in vanets using changing pseudonyms - ideal and real. In: VTC Spring, pp. 2521–2525. IEEE (2007). URL http://dblp.uni-trier.de/db/conf/vtc/vtc2007s.html
25. González-Tablas, A.I., Alcaide, A., de Fuentes, J.M., Montero, J.: Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations. Ad hoc networks **11**(8), 2693–2709 (2013)
26. Hajny, J., Malina, L.: Unlinkable attribute-based credentials with practical revocation on smart-cards. In: S. Mangard (ed.) Smart Card Research and Advanced Applications - 11th International Conference, CARDIS 2012, Graz, Austria, November 28-30, 2012, Revised Selected Papers, *Lecture Notes in Computer Science*, vol. 7771, pp. 62–76. Springer (2012). DOI 10.1007/978-3-642-37288-9_5. URL http://dx.doi.org/10.1007/978-3-642-37288-9_5
27. Housley, R., et al.: Internet x.509 public key infrastructure certificate and crl profile. Tech. rep., Internet Engineering Task Force (1999). URL https://www.ietf.org/rfc/rfc2459
28. IBM Research Zurich: Identity mixer. http://www.zurich.ibm.com/idemix/downloads.html (2015)

29. IEEE: IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE). Tech. rep., IEEE (2006). URL https://www.standards.its.dot.gov/factsheets/factsheet/80
30. ISO: Iso 21217:2014. intelligent transport systems – communications access for land mobiles (calm) – architecture. Tech. rep. (2014)
31. Lapon, J.: Anonymous credential systems: From theory towards practice. Katholieke Universiteit Leuven (Ph.D. thesis) (2012)
32. Li, Z., Liu, C., Chigan, C.: On secure vanet-based ad dissemination with pragmatic cost and effect control. Intelligent Transportation Systems, IEEE Transactions on **14**(1), 124–135 (2013)
33. Microsoft Research: U-prove. http://research.microsoft.com/en-us/projects/u-prove/ (2013)
34. Mostowski, W., Vullers, P.: Efficient u-prove implementation for anonymous credentials on smart cards. In: M. Rajarajan, F. Piper, H. Wang, G. Kesidis (eds.) Security and Privacy in Communication Networks - 7th International ICST Conference, SecureComm 2011, London, UK, September 7-9, 2011, Revised Selected Papers, *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 96, pp. 243–260. Springer (2011). DOI 10.1007/978-3-642-31909-9_14. URL http://dx.doi.org/10.1007/978-3-642-31909-9_14
35. Mostowski, W., Vullers, P.: Efficient u-prove implementation for anonymous credentials on smart cards. In: Security and Privacy in Communication Networks, pp. 243–260. Springer (2012)
36. Nkenyereye, L., Tama, B.A., Park, Y., Rhee, K.H.: A fine-grained privacy preserving protocol over attribute based access control for vanets. J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl **6**(2), 98–112 (2015)
37. Papadimitratos, P., Buttyan, L., Holczer, T.S., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., Hubaux, J.P.: Secure vehicular communication systems: design and architecture. Communications Magazine, IEEE **46**(11), 100–109 (2008)
38. Papadimitratos, P., Kung, A., Hubaux, J.P., Kargl, F.: Privacy and Identity Management for Vehicular Communication Systems: a Position Paper. In: Workshop on Standards for Privacy in User-Centric Identity Management, pp. 1–11 (2006)
39. Paquin, C., Zaverucha, G.: U-prove cryptographic specification v1. 1. Tech. rep., Microsoft Technical Report, http://connect. microsoft. com/site1188 (2011)
40. Persiano, G., Visconti, I.: An efficient and usable multi-show non-transferable anonymous credential system. In: Financial Cryptography, pp. 196–211. Springer (2004)
41. Petit, J., Schaub, F., Feiri, M., Kargl, F.: Pseudonym schemes in vehicular networks: a survey. Communications Surveys & Tutorials, IEEE **17**(1), 228–255 (2015)
42. Pfitzmann, A., Hansen, M.: Anonymity, unlinkability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology. Tech. rep., TU Dresden (2005)
43. Quick, D., Choo, K.K.R.: Digital forensic intelligence: Data subsets and open source intelligence (dfintosint): A timely and cohesive mix. Future Generation Computer Systems pp. – (2016). DOI http://dx.doi.org/10.1016/j.future.2016.12.032. URL //www.sciencedirect.com/science/article/pii/S0167739X16308639
44. Quick, D., Choo, K.K.R.: Pervasive social networking forensics: Intelligence and evidence from mobile device extracts. Journal of Network and Computer Applications pp. – (2016)
45. Raya, M., pierre Hubaux, J.: The security of vanets. In: In VANET05, September 2, pp. 93–94 (2005)
46. Raya, M., Hubaux, J.P.: Securing vehicular ad hoc networks. Journal of Computer Security **15**(1), 39–68 (2007)
47. Sabouri, A., Krontiris, I., Rannenberg, K.: Attribute-based credentials for trust (abc4trust). In: Trust, Privacy and Security in Digital Business - 9th International Conference, TrustBus 2012, Vienna, Austria, September 3-7, 2012. Proceedings, pp. 218–219 (2012). DOI 10.1007/978-3-642-32287-7_21. URL http://dx.doi.org/10.1007/978-3-642-32287-7_21
48. Sabouri, A., Krontiris, I., Rannenberg, K.: Attribute-based credentials for Trust (ABC4Trust). Springer (2012)

49. SBD Secure Car research: What makes a good smart key system? Tech. rep., SBD Secure Car research (2010)
50. Schaub, F., Ma, Z., Kargl, F.: Privacy requirements in vehicular communication systems. In: Proceedings of the 12th IEEE International Conference on Computational Science and Engineering, CSE 2009, Vancouver, BC, Canada, August 29-31, 2009, pp. 139–145 (2009). DOI 10.1109/CSE.2009.135. URL http://dx.doi.org/10.1109/CSE.2009.135
51. Scheibert, K., Klimke, M.: Secure and seamless integration of software over the air (sota) update in modern car board net architectures. In: Embedded Security in Cars Conference (ESCAR) (2015)
52. Serna, J., Morales, R., Medina, M., Luna, J.: Trustworthy communications in vehicular ad hoc networks. In: WF-IoT, pp. 247–252 (2014). DOI 10.1109/WF-IoT.2014.6803167. URL http://dx.doi.org/10.1109/WF-IoT.2014.6803167
53. Solanas, A., Martínez-Ballesté, A.: Privacy protection in location-based services through a public-key privacy homomorphism. In: European Public Key Infrastructure Workshop, pp. 362–368. Springer (2007)
54. Solanas, A., Patsakis, C., Conti, M., Vlachos, I.S., Ramos, V., Falcone, F., Postolache, O., Pérez-Martínez, P.A., Di Pietro, R., Perrea, D.N., et al.: Smart health: a context-aware health paradigm within smart cities. IEEE Communications Magazine **52**(8), 74–81 (2014)
55. Sun, J., Zhang, C., Zhang, Y., Fang, Y.: An identity-based security system for user privacy in vehicular ad hoc networks. Parallel and Distributed Systems, IEEE Transactions on **21**(9), 1227–1239 (2010)
56. *ed.*, N.: D.SPA.20 ECRYPT II yearly report on algorithms and keysizes (2011-2012). Tech. rep., European Network of Excellence in Cryptology II (2012)
57. Turner, S., Housley, R., et al.: An internet attribute certificate profile for authorization. Tech. rep., Internet Engineering Task Force (2010). URL http://tools.ietf.org/html/rfc5755
58. Veseli, F., Vateva-Gurova, T., Krontiris, I., Rannenberg, K., Suri, N.: Towards a framework for benchmarking privacy-abc technologies. In: ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings, pp. 197–204 (2014)
59. Vullers, P., Alpár, G.: Efficient selective disclosure on smart cards using idemix. In: S. Fischer-Hübner, E. de Leeuw, C. Mitchell (eds.) Policies and Research in Identity Management - Third IFIP WG 11.6 Working Conference, IDMAN 2013, London, UK, April 8-9, 2013. Proceedings, *IFIP Advances in Information and Communication Technology*, vol. 396, pp. 53–67. Springer (2013). DOI 10.1007/978-3-642-37282-7_5. URL http://dx.doi.org/10.1007/978-3-642-37282-7_5
60. Vullers, P., Alpár, G.: Efficient selective disclosure on smart cards using idemix. In: Policies and Research in Identity Management, pp. 53–67. Springer (2013)
61. Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (vanets): status, results, and challenges. Telecommunication Systems **50**(4), 217–241 (2012)
62. Zhang, L., Wu, Q., Qin, B., Domingo-Ferrer, J., Liu, B.: Practical secure and privacy-preserving scheme for value-added applications in {VANETs}. Computer Communications pp. – (2015). DOI http://dx.doi.org/10.1016/j.comcom.2015.08.005. URL http://www.sciencedirect.com/science/article/pii/S014036641500290X

Appendix I. Performance results

In the following, Tables 6, 7 and 8 present complete results of the experimental study.

Table 6 Evaluation of the impact of setup and issuance. Time in miliseconds for key sizes 1024 and 2048.

1024 bits					
VANET-upd. Persiano		**Idemix**		**U-Prove**	
Setup	**Issuance**	**Setup**	**Issuance**	**Setup**	**Issuance**
5615	97	14829	2873	2563	2182
2048 bits					
38500	649	58522	3402	24351	5579

Table 7 Evaluation of the impact of proving and verification. Time in miliseconds for key size 1024, having 2,5 and 10 attributes, disclosing different number of attributes.

# Disclosed attributes	**Proving**	**Verification**	**Proving**	**Verification**	**Proving**	**Verification**
	2 attributes		**5 attributes**		**10 attributes**	
	VANET-upd. Persiano					
0	2181	274	2230	316	2319	320
1	2346	262	2329	310	2235	315
2	2375	263	2341	302	2440	304
3			2410	282	2508	264
4			2457	284	2544	257
5			2463	284	2588	258
6					2562	261
7					2692	262
8					2603	265
9					2635	268
10					2660	283
	Idemix					
0	402	34	511	34	596	39
1	389	33	482	35	578	38
2	374	31	447	35	566	38
3			449	34	530	38
4			429	34	510	38
5			399	33	501	36
6					498	37
7					495	36
8					488	36
9					465	35
10					425	37
	U-Prove					
0	1866	34	2239	34	2747	39
1	1848	33	2340	35	2954	38
2	1878	31	2466	35	2764	37
3			2340	34	3062	38
4			2466	34	3046	38
5			2407	33	3185	38
6					3310	36
7					3373	37
8					3590	36
9					3412	36
10					3392	35

Table 8 Evaluation of the impact of proving and verification. Time in miliseconds for key sizes 1024 and 2048, having 5 attributes and disclosing different number of attributes.

# Disclosed attributes	VANET-upd. Persiano		Idemix		U-Prove	
	Proving	Verification	Proving	Verification	Proving	Verification
	1024 bits					
0	2230	316	511	34	2239	34
1	2329	310	482	35	2340	35
2	2341	302	447	35	2466	35
3	2410	282	449	34	2340	34
4	2457	284	429	34	2466	34
5	2463	284	399	33	2407	33
	2048 bits					
0	19950	1953	2003	182	3038	393
1	20248	1910	1916	177	3062	392
2	20398	1920	1931	171	3167	398
3	21974	1954	1861	165	3217	406
4	22691	1971	1810	160	3176	406
5	22841	2001	1759	155	3178	407