

# An Interoperability System for Authentication and Authorization in VANETs

Valentina Casola<sup>1</sup>, Jesus Luna<sup>4</sup>, Antonino Mazzeo<sup>1</sup>, Manel Medina<sup>2</sup>,  
Massimiliano Rak<sup>3</sup>, and Jetzabel Serna<sup>2</sup>

<sup>1</sup> Dipartimento di Informatica e Sistemistica,  
Università degli studi di Napoli Federico II  
`{casolav,mazzeo}@unina.it`

<sup>2</sup> Computer Architecture Department,  
Technical University of Catalonia (UPC)  
`{jetzabel,medina}@ac.upc.edu`

<sup>3</sup> Dipartimento di Ingegneria dell'Informazione,  
Seconda Università di Napoli  
`massimiliano.rak@unina2.it`

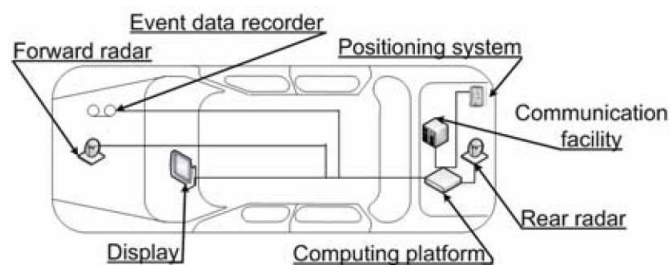
<sup>4</sup> Barcelona Digital Centre Tecnologic,  
`jluna@bdigital.org`

**Abstract.** Vehicular Ad-Hoc NETWORKS (VANETs) have evolved considerably over the last years, promising to drastically reduce the number of traffic victims by increasing the overall road safety. Despite the wide number of potential applications VANETs also raise a broad range of critical security challenges mostly related with *Privacy*, which remains as an important factor to consider for the successful deployment of these technologies. To achieve privacy it is important to enforce the concepts of authentication and authorization via well proved mechanisms, i.e. Public Key Infrastructures (PKI) relying on a large set of regional Certification Authorities (CAs) with explicit cross-certification agreements to provide interoperability for vehicles and services. To avoid the burden of managing these cross-certificates our research proposes the *Interoperability System* (IS), an architecture able to provide VANETs' nodes with a security mechanism for different and mutually untrusted domains. The IS supplies vehicles with a trusted set of authentication and authorization credentials, by implementing an OSCP-based certificate status service and a quantitative security level evaluator. This paper shows that the proposed architecture can be used to implement a Mandatory Access Control mechanism in two well known VANET scenarios, therefore enforcing driver's privacy and liability (non-repudiation) with a protocol independent of the underlying communication system.

**Keywords:** Authentication, authorization, interoperability, security, Vehicular Ad-hoc NETWORKS.

## 1 Introduction

Vehicular Ad hoc NETWORKS (VANETs) are an emerging research area and also one of the most relevant forms of mobile ad-hoc networks [1]. By the year 2010 it is expected that 40% of all vehicular components will be electronic and with this integration VANET vehicles will be capable of storing and processing great amounts of information, including a driver's personal data and geolocation information. A VANET vehicle (Figure 1) is equipped with processing, recording and positioning mechanisms with a potentially "infinite" power supply.



**Fig. 1.** New vehicles will include a central computing platform network that can provide USB, Bluetooth, IEEE 802.11 interfaces or Ethernet and may have such features as GPS, EDR -Event Data Recorder- (i.e. to store data for a vehicle's crash reconstruction) and radars.

VANETs enable car-to-car and car-to-infrastructure communication, thus communicating nodes are either vehicles or base stations that can exchange information; for the rest of this paper, these will be referred as *Car-to-Car* (C2C) and *Car-to-Service* (C2S) communications.

According to [2-4] VANETs' messages can be classified in three groups: warning -to prevent detected risky situations-, traffic management and added value -to provide Internet services-. Despite VANETs share general features with conventional ad-hoc networks, they have individual characteristics that are decisive in the design of the communication system [5] these include: (i) Dynamic topology, (ii) Mobility models, (iii) Infinite energy supply and (iv) Localization functionality.

Unfortunately, a VANETs system can be vulnerable to security attacks which may compromise the driver's privacy (i.e. disclosing his personal data) and even cause life-threatening situations (i.e. false warnings resulting in road accidents). In a VANET the network access is granted by default, so messages sent by one node are "available" to all other nodes that have joined the network thus easing packets' eavesdropping. One of the most important challenges in VANETs is related with finding proper techniques and architectural solutions to enforce *security* and *privacy*. The apparent trade offs among these two concepts have been discussed on a broader level by [6].

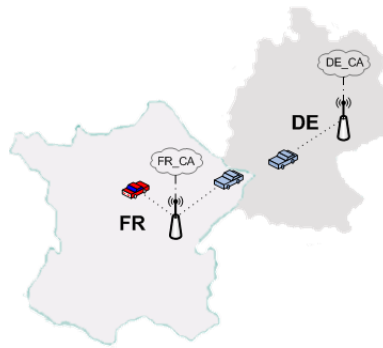
A connected vehicle is also able to run wireless cryptographic protocols [7] and to use X.509 v3 digital certificates from Public Key Infrastructures (PKI) [8]; these two features are becoming a common approach for implementing VANETs' secure access to value added services [9]. Available proposals envision a wide number of Certification Authorities (CA) (that act as Trusted Third Parties within regional scopes) and cross-certification agreements to provide interoperability among these otherwise *untrusted domains*. Unfortunately existing approaches are based on static and hard to manage trust relationships and certificates among the participants, resulting in security issues with vehicles needing to access up-to-date information about trusted CAs -authoritative for the vehicle's location- to validate messages received on the road (just as shown in Example 1).

*Example 1.* Consider the scenario depicted in Figure 2 where a vehicle with a German Electronic Licence Plate -ELP- and a digital certificate issued by  $DE_{CA}$ , travels to France and receives from another vehicle a warning message digitally signed by a certificate issued by  $FR_{CA}$ .

Authentication in the previous example implies the following *certificate validation* process:

1. Cryptographic verifications over the Certificate Path (i.e. verifying the digital signature of each certificate),
2. Verifying each certificate's validity period,
3. Verifying that the first certificate in the chain is a Trust Anchor and,
4. Verifying the status of each certificate in the Path to ensure that it has not been revoked or suspended.

The process just described is referred as *Basic Path Validation* [8].



**Fig. 2.** In a VANET, CA information depends on the vehicle's geographical position.

Because of the regional CAs used in VANETs environments it is feasible to conclude that drivers will have a certificate issued by their own CA, therefore

conveying a big interoperability problem when interacting with services and vehicles from others CAs. Returning to the previous example: how to perform the *Basic Path Validation* process if (i) a trust anchor can not be determined ( $FR_{CA}$  is unknown to the German driver) and therefore (ii) revocation information for the French driver can not be validated? Is the originator of the warning *authorized* to generate this class of messages?

For the research presented in this paper security and privacy issues in VANETs are related with the concepts of *Authentication and Authorization*, so they will be addressed by proposing an infrastructure called the *Interoperability System* which focuses on the capability of providing reliable users' identities to the different domains through the adoption of a policy-based approach. This process, called *Extended Path Validation* [8], defines an approach that enables any Entity (service providers and vehicles) to validate in real-time a digital certificate issued by any other CA even though they do not belong to the same trusted domain.

To perform the Extended Path Validation in VANETs the following two phases are required:

1. Automatically perform the cross certification by an automatic policy mapping (i.e. comparison and evaluation of the Certificate Policies from the involved CAs ) to build a *dynamic CA Federation*;
2. Validate in near-real time a VANET certificate's status.

Furthermore, the proposed Interoperability System will act as an Attribute Authority for any Service Provider implementing an identity-based access control mechanism that takes into account the driver's privacy and liability (non-repudiation).

The reminder of this paper is organized as follows: in Section 2 related works on security architectures and solutions for VANETs are reported; in Section 3 it is presented a high-level view of an architectural solution proposed for the interoperability of different untrusted domains. In Section 4 the contributed Interoperability System is presented and the Extended Path Validation concept is widely explained. In Section 5 adoption of the proposed Interoperability System for the C2C and C2S scenarios will be demonstrated. Finally in Section 6 some conclusions are drawn and the directions of the future work are outlined.

## 2 State of the Art

VANET technology is a novel research topic, currently in standardization process and therefore works presented in this section raise mostly from academical and industrial worlds. The following paragraphs will cover the most important research related with VANETs' authentication, authorization and privacy issues.

In recent studies ([3], [10], [11] and [12]) the use of Public Key Infrastructures and digital certificates have been proposed to provide a suitable solution to the authentication and authorization challenges in VANETs. An efficient architecture for managing the whole certificate's life cycle (issue, distribution, validation and revocation) has been found to be fundamental. In [13] authors presented a

certificate validation scheme based on a distributed version of OSCP for authorization and authentication in VANETs, capable of preventing known issues like the flooding of extended revocation lists. Unfortunately, privacy issues were not taken into account.

Authors of [14] proposed a certificate revocation model consisting in a set of three protocols (Revocation using Compressed Certificate Revocation Lists (RC2RL), Revocation of the Tamper-Proof Device -RTPD- and the Distributed Revocation Protocol -DRP-), each one adapted to a specific VANET scenario. In RC2RL and RTPD revocation occurs when the CA sends a message to the “revoked vehicle”, however other relying parties (vehicles and service providers) do not receive these notifications therefore opening a security gap on the whole VANET system. In the case of the DRP protocol the possibility of collusion attacks also remains open. Obviously we have to consider that an attacker detection system, basic for the deployment of the mentioned family of protocols, has not yet been designed.

The SRAAC protocol proposed in [15] allows distribution of certificates, anonymous message authentication with quorum based blinded certificate issuance, anonymity, revocation and isolation of misbehaving vehicles. SRAAC makes use of a digital signature algorithm called Magic Ink-DSS with shared secrets, however the disadvantage of this model is that a vehicle detected as malicious will not be revoked in real time because its issued certificates (previously stored in their On Board Unit) will still be valid for some arbitrary time window.

A mechanism for access control using the Kerberos model was described in [16]. The authors proposed an authentication and authorization mechanism to access offered services according to a previous subscription (token) so afterwards the vehicle is authenticated at the highways entry points. This model is specific for highways environments, thus limiting its applicability.

From the investigation of the relevant related work it must be remarked that VANETs’ authorization research is still quite limited. In many distributed infrastructures, the adoption of a certificate delegation model is also proposed; at the state of the art proxy credentials [17] are a common technique used for delegation, where an *entity A* grants to another *entity B* the right for *B* to be authorized with others as if it were *A*. In other words, *entity B* is acting as a proxy on behalf of *entity A*. The computational Grid is the most common scenario where proxy credentials are used for security delegation [18, 19].

Apart from authentication, authorization and delegation, privacy is also an important issue for VANETs. In [20] and [11] authors gave a detailed analysis of general system attacks on Inter-Vehicle Communication (IVC) and described the main challenges in securing vehicular networks, pointing out other important system requirements (i.e. privacy). Potential implications of missing privacy are exposed in [21] and the author proposes to use centrally assigned digital pseudonyms. Authors of [22] defined a system where vehicles change pseudonyms in a certain region pointed by the system, this region being where a lot of vehicles are within the communication range [21]. A disadvantage of the latter appears when there are not enough vehicles changing pseudonyms within a re-

gion. To overcome this problem [23] proposes self assigned digital pseudonyms that take a set of measures while changing them: *(i)* synchronizing pseudonym change, *(ii)* introducing gaps (silent periods) and *(iii)* changing pseudonyms when nodes are in the region (this was also considered in [24] by defining them as mix-contexts in addition to frequently change of pseudonyms and protection of a centralized mapping that intend to increase anonymity). In [25] authors provided an improvement of mix-contexts considering anonymity over randomly changing pseudonyms in certain intervals. CARAVAN ([26], [27]) proposes a random silent period in order to hamper linkability between pseudonyms just as considered in other architectures already mentioned.

In [28] authors proposed a system to balance auditability and privacy in VANETs based on symmetric cryptographic primitives and two different sorts of pseudonyms (short and long term). A study of practicability in pseudonymity deployment and implementation was done in [29], where possible solutions were represented as a combination of existing pseudonymity algorithms.

In [30] authors defined a protocol for conditional privacy preservation by proposing short-time anonymous key generation in order to minimize their number and ease their management. RSUs (Road Side Units) are in charge of generating the short-time keys and above these entities is found the TA (Trusted Authority), ultimate responsible for issuing RSUs' certificates. In [30] a mechanism based on different levels of privacy is also presented; it is based on a combination of levels of authentication, anonymity and unlinkability that are a very interesting approach to cope with the privacy issues found by our research.

In summary, most of the research and proposed solutions for privacy mainly focus on the use of pseudonyms and algorithms for changing them. Because of the common belief that pseudonyms are important for VANETs' overall security and are quite beneficial for protecting users' identity, the architecture to be introduced in Section 3 is fully compatible with these solutions.

### 3 Architecture of a Security Framework for VANETs

Despite its importance, at the state of the art there is no real architecture or standard for solving VANETs' security issues mentioned in previous sections. In this paper we propose a framework that can be adopted by any car to implement interoperable and secure authentication mechanisms in VANETs.

The contributed framework uses a PKI infrastructure, but allows final users (vehicles into the VANET) to perform authentication in any untrusted domain by dynamically enabling interoperability among different CAs without explicit agreements (i.e. cross certification). Such a model will be called a *CA Federation*. To illustrate our proposal we will refer to two use cases introduced in Section 1: the *Car to Service Communication (C2S)* and, the *Car to Car Communication (C2C)*. Even though the protocols, data and security features of the reference scenarios are quite different from an architectural point of view, we will manage them in a very similar way: in both cases we propose the introduction of an *Interoperability System (IS)* acting as a trusted third party and, able to au-

thenticate digital certificates by providing access credentials that will be used afterwards for authorization purposes. The IS solves the problem of managing explicit trust relationships by enabling a dynamic trust establishment through the evaluation of a digital certificate's security level. The rest of this paper will further detail the IS architecture and the security evaluation methodology being used.

Because a VANET Service Provider needs to protect the access to its services, we can talk about authorization decisions based on access control policies defined by commercial aspects. On the other hand a car does not offer a service, but still has to share information for other VANET's nodes therefore requiring the protection of the driver's private information. To face the latter problem we propose the implementation of a Mandatory Access Control (MAC) mechanism [31] on the vehicle by assigning security labels to the personal data that is being managed: the access will be granted if the security level of the requestor is equal or higher than the security level denoted by the data's label. This feature will be further explained in Section 5.2.

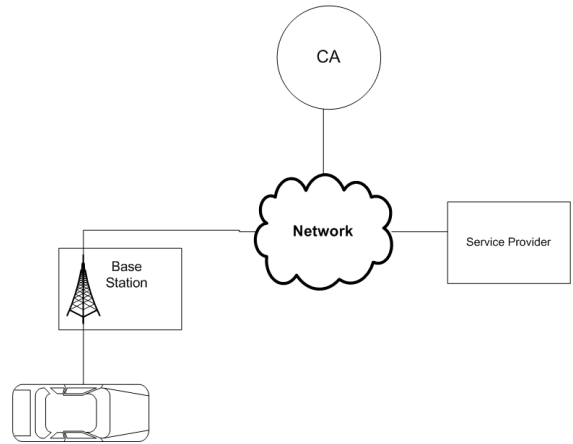
### 3.1 Use cases

In the C2S scenario (Figure 3) a vehicle needs to be able to access any authorized service available on the road, even in "untrusted" domains –those being serviced under a different Certification Authority–. As shown in figure 3 the vehicle uses the *base stations* (i.e stations along the road that offers a wireless network access to the car) to access external services offered by service providers hosted by infrastructure nodes. The problems to address in this scenario are:

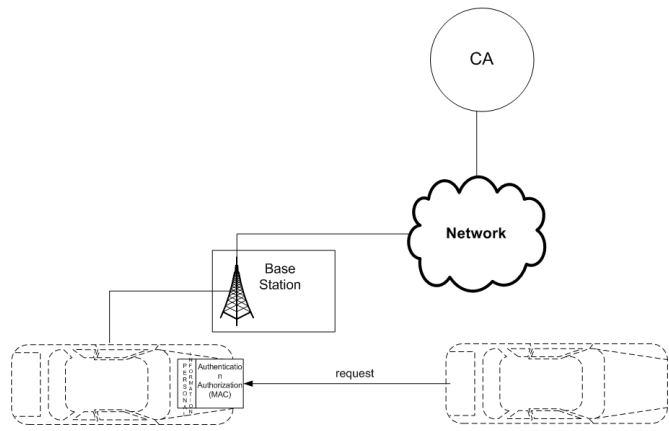
1. How does the service authenticate the car?
2. How does the car authenticate the service?
3. Which service can the car access (service authorization)?
4. Which driver's data the service can access (car authorization)?
5. What happens when the connections are lost (car are in fast movement, therefore connection cannot be considered stable)?
6. How to perform authentication and authorization when a car moves between two different domains?

A VANET's vehicle is able to request any available infrastructure service, but also can offer "services" to other vehicles: for example a police car requesting a vehicle's driver information and current speed. In these C2C scenarios (Figure 4) a vehicle will need to authorize other vehicles to access its information (including the driver's private data). To achieve this goal, a driver can decide which personal information can be accessible and the minimum required security level to do this. A brief summary of the problems to solve are:

1. How can the cars authenticate each other?
2. Which data can be shared among vehicles?
3. What happens when communication is lost?



**Fig. 3.** C2S Components



**Fig. 4.** c2c components

4. How to perform authentication and authorization when cars belong to two different domains?

Both cases put in evidence that the VANET infrastructure can be seen as two different networks: *(i)* a peer-to-peer network of cars made of unreliable and dynamic connections and, *(ii)* the network's infrastructure offering services to the cars. The C2S scenario models the communication between these two networks, while the C2C scenario represents peer-to-peer communication.

### 3.2 An architectural model for VANET Security

Current state of the art authentication and authorization mechanisms for VANETs have been derived from traditional ones (as PKI for authentication and policy based access control mechanisms for authorization), however many particular problems remain open: *(i)* issues with unreliable communications and brief connections require a special care, *(ii)* cross certification agreements between untrusted domains are hard to manage in VANETs. The former problem relates with the VANETs' nature itself: interleaves of "communication silent" due to infrastructure's failures are likely to occur along with very short connections with other cars or infrastructures because of the car's speed. A well-designed VANET protocol should implement *optimized* messages where security (i.e. digital signature mechanism and cryptosystem being used) and performance (i.e. signature size and encryption time) are balanced to cope with these unreliable and short connections.

The protocols we propose are designed in order to take into account the VANET requirements (i.e. unreliable and short connections) at design level and independently from the (proprietary) technology involved. As a consequence, the solution we propose has been designed with a performance-oriented approach just as illustrated in Section 5.

On the other hand, the problem of cross certification agreements is due to the future deployment of VANETs which will result in the creation of several PKIs, each one usually installing its own Certification Authority and thus giving birth to a large set of different and untrusted security domains (based on the authors' experience at least one-per Member State in the EU). This represents one of the biggest interoperability problems that could arise among all VANETs users and therefore, one of the major security challenges to be faced before building this wide distributed infrastructure. In other words, this problem is related to the definition of a trusted PKI-infrastructure able to guarantee a secure degree of interoperability among all the involved VANETs' Certification Authorities. In practice there are two commonly accepted approaches that provide interoperability between different security domains based on PKI technology:

1. Involved CAs explicitly build a trusted domain by defining a new CA hierarchy through cross certification techniques. In this case each CA explicitly trusts the others and therefore is able to accept their certificates.
2. Involved CAs do not build an explicit trusted domain, but interoperate through a "federation": any CA belonging to the federation implicitly trusts

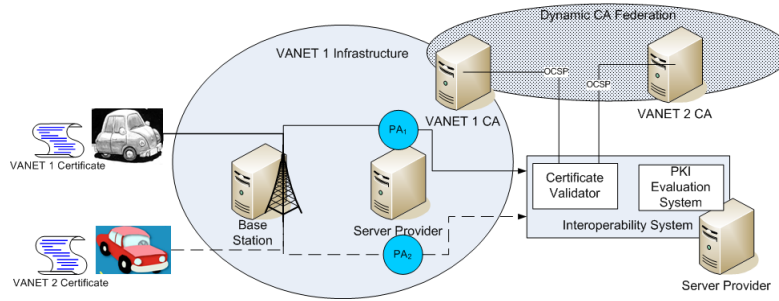
the others thanks to the definition of a well-established policy-based framework.

Even if the explicit trusted domain (first approach) is an attractive solution, it is not always possible to implement in practice because of the required agreements between the involved organizations, along with administrative overheads and technical problems that arise.

Previous issues should be addressed by VANET's protocols, but at the state of the art they are not. For this reason we have proposed an *Interoperability System for VANETs* able to work in these networks with independence of the underlying protocols thanks to the use of a *Personal Agent* -PA- software associated to each car. With this contribution we are able to cope with both of the problems mentioned at the beginning on this section: short connections and complex elaborations are managed via a PA acting *on behalf* of the car that created it by means of a delegation model. A car's PA *activates* to interact with the Interoperability System in the "wired" network and to keep the car and session status. If the car disconnects for any reason before receiving a response from the infrastructure, then as soon as it reconnects and re-authenticates to the IS its PA returns along with the validation reply.

To cope with cross-certification issues the proposed IS implements the concept of *CA Federations*. In a CA Federation the members agree on a minimum set of security requirements that must be fulfilled by all of them to interoperate. These minimum requirements are usually a subset of the CA's Certificate Policy and can be audited at any time by the other members of the same Federation. If a new CA wants to participate in the Federation, then its CP must pass through an "accreditation" process to ensure compliance with the minimum requirements or, in other case, to assess the candidate in which provisions (individual rules from the CP) should be improved to become a member. Once the accreditation process has been passed the new member CA's root certificate is added to a trusted repository (usually hosted by the Federation itself like in [32]). Instead of distributing new sets of cross-certificates to all the VANET's nodes it is only necessary to let them know how to access the CA Federation's repository in order to update their local copies of trusted CAs.

Figure 5 shows that a VANET can be modeled as a distributed system composed by *Base Stations* offering wireless connection to cars, a *Certificate Authority* and a set of *Server Providers* hosting the VANET services. It is worth to notice that cars belonging to different domains also must have certificates issued by different CAs. As shown in Figure 5 the model we propose creates a PA for each car and uses the IS as an intermediary between the certificate verifiers (vehicles and service providers) and the issuing CAs, by managing (retrieving, elaborating and updating) the information needed to create a *dynamic CA Federation*. As mentioned before the IS is independent from the underlying VANETs' communication protocols.



**Fig. 5.** The proposed Security Architecture for VANETs.

## 4 The Interoperability System

The goal of the Interoperability System is to build a dynamic federation of CAs by evaluating their Certificate Policies, thus enabling the Extended Path Validation of digital certificates from mutually untrusted domains. The IS must perform two main tasks:

1. Online validation of the certificates' status,
2. Evaluation of the issuing CA's security level.

To achieve its goal the IS should be comprised of:

- A *Certificate Validator* to verify the certificate's status in near real-time.
- A *PKI evaluation system* to obtain the security level provided by a Certification Authority.

The Certificate Validator uses a high-level *OCSP Responder* [33] to provide in near-real time the status information of certificates issued by any member of the CA Federation. Trust issues with these OCSP servers are solved considering the use of *Authorized Responders* digitally signing the OCSP Responses with a certificate from the same PKI hierarchy of the OCSP client (i.e. the driver's CA). OCSP is a request-response protocol that greatly benefits the performance of VANET-like systems, just as shown by European Projects like CertiVeR [34].

About the second component, the *PKI evaluation system*, we have adopted the Reference Evaluation Model (REM) for evaluating a CA's security level (*GSL* Global Security Level- in REMs terminology) as illustrated in Section 4.1. This approach is based on the formalization of a Certificate Policy to: *i*) determine if the corresponding CA is compliant with the federation's minimal security requirements and *ii*) to quantitatively evaluate its particular Security Level. In this way it is possible for the proposed IS to dynamically build a CA federation for VANETs. As mentioned before, the CA's Security Level can be used afterwards to enforce privacy by performing authorization decisions based on a Mandatory Access Control model just as illustrated in Section 5.2. As

introduced in Section 4 a final component of the proposed architecture, the *Personal Agent* (PA), is co-located with each relying party (vehicle or service provider) to perform authentication and authorization decisions even in presence of communication failures.

Section 5 explains in further detail how the different elements of the proposed architecture interoperate in order to perform the *Extended Path Validation* in both, the C2S and the C2C scenarios.

#### 4.1 Dynamic CA Federation using the REM

The Interoperability System helps building dynamic CA federations because it allows a client to evaluate “on-the-fly” a Certificate Policy from an unknown Certification Authority, thus establishing if its security level corresponds to the requested security features.

The methodology used to evaluate the security level provided by a Certification Authority and decide to create a dynamic trust relationship with it, is the Reference Evaluation Model (REM) [35]. Its main goal is to provide an automatic mean to state the security level provided by an infrastructure; REM has been widely adopted in the past to dynamically build CA Federations [36, 19]. The methodology defines (i) how to express in a rigorous way a security policy (a Certification Policy in our particular case), (ii) how to evaluate a formalized policy and, (iii) how to state the provided security level. With REM any policy is represented through an XML tree containing all its provisions as intermediate nodes and leaves.

In Figure 6 the three phases of the REM methodology are shown: **Policy Structuring**, **Policy Formalization** and **Policy Evaluation**:

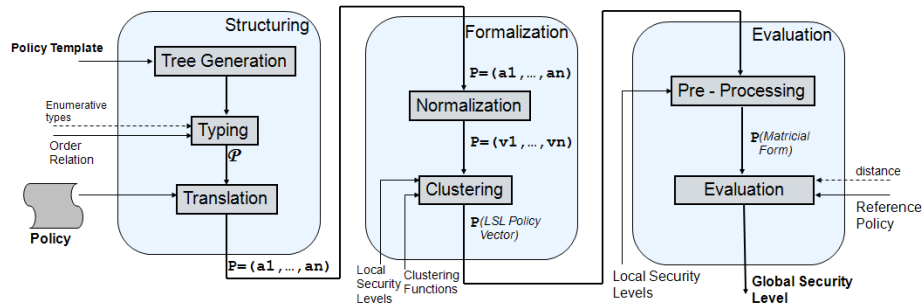


Fig. 6. Phases of the evaluation methodology

1. The goal of the **Structuring** phase is to associate an enumerative and ordered data type  $K_i$  to the  $n$  leave-provisions of the policy. A policy space “ $P$ ” is defined as  $P = K_1 \times K_2 \times \dots \times K_n$ , i.e. the vectorial product of the

$n$  provisions  $K_i$ . For example, the provision *KeyLength* can assume the following ordered values: {128bits, 512bits, 1024bits, 2048bits }. The space is defined according to a policy template that strongly depends on the application context.

2. The main goal of the **Formalization** phase is to turn the policy space “ $P$ ” into an homogeneous space “ $PS$ ”. This transformation is accomplished by a normalization and clusterization process which allows to associate a Local Security Level (LSL) to each provision. For example if a policy has a KeyLength of 512bits, it will be associated to the LSL=2 and the normalized vector is (1,1,0,0). After that the provisions may be compared by comparing their LSLs.
3. The main goal of the **Evaluation** phase is to pre-process the “ $PS$ ” vector of LSLs in order to represent it by a  $n \times l$  matrix whose rows are the single provisions  $K_i$  and the number of columns is the chosen number of LSLs for each provision. For example, if the number of LSL is four and the LSL associated to a provision is  $l_2$ , the row in the matrix associated to the provision in the matrix will be: (1,1,0,0). Finally, a distance criteria for the definition of a metric space is applied. REM adopts the Euclidean distance among matrices:

$$d(A, B) = \sqrt{(\sigma(A - B, A - B))}$$

where  $\sigma(A - B, A - B) = Trace((A - B)(A - B)^T)$

To define the Global Security Level (GSL)  $L_{P_x}$  associated to the policy  $P_x$ , must be introduced some reference levels according to the following metric function:

$$L_{P_x} = \begin{cases} L_0 & \text{iff } d_{x0} \leq d_{10} \\ L_1 & \text{iff } d_{10} < d_{x0} < d_{20} \\ L_2 & \text{iff } d_{20} < d_{x0} < d_{30} \\ L_3 & \text{iff } d_{30} < d_{x0} < d_{40} \\ L_4 & \text{iff } d_{40} \leq d_{x0} \end{cases}$$

where  $d_{i,0}$  are the distances among the references and the origin of the metric space (denoted as  $\emptyset$ ). *This function gives a numerical value to the security level.*

In summary, REM’s goal is to evaluate the GSL or security level associated with a CA through the evaluation of its Certificate Policy so trust decisions can be taken.

## 5 Authentication and Authorization in VANETs

The Interoperability System can offer its services in any distributed infrastructure, nevertheless its implementation should deal with the failures of the communication layers and in particular with the inherent VANET’s mobility. Let us take for example a vehicle that moves from one base station to another, the management of secure messages is still required to preserve the privacy and keep the status of a service request (even if the communication is lost). These issues are addressed by assuming that the communication between vehicles and infrastructure are asynchronous and a *Personal Agent* is associated to each car.

The *Personal Agent* (PA) works on behalf of a car in the infrastructure, any car creates and delegates its own PA to authenticate and authorize any request and to preserve its status in case of network disconnections. Furthermore it is responsible to communicate with the proposed Interoperability System to validate digital certificates by performing the Extended Path Validation.

In the next subsections we will illustrate how the PA and the IS are adopted to authenticate and authorize drivers to access a service provider (C2S scenario, Section 5.1) and, how to authenticate and authorize drivers to access other car's data while preserving driver's privacy (C2C scenario, Section 5.2).

### 5.1 Car to Service Provider secure access

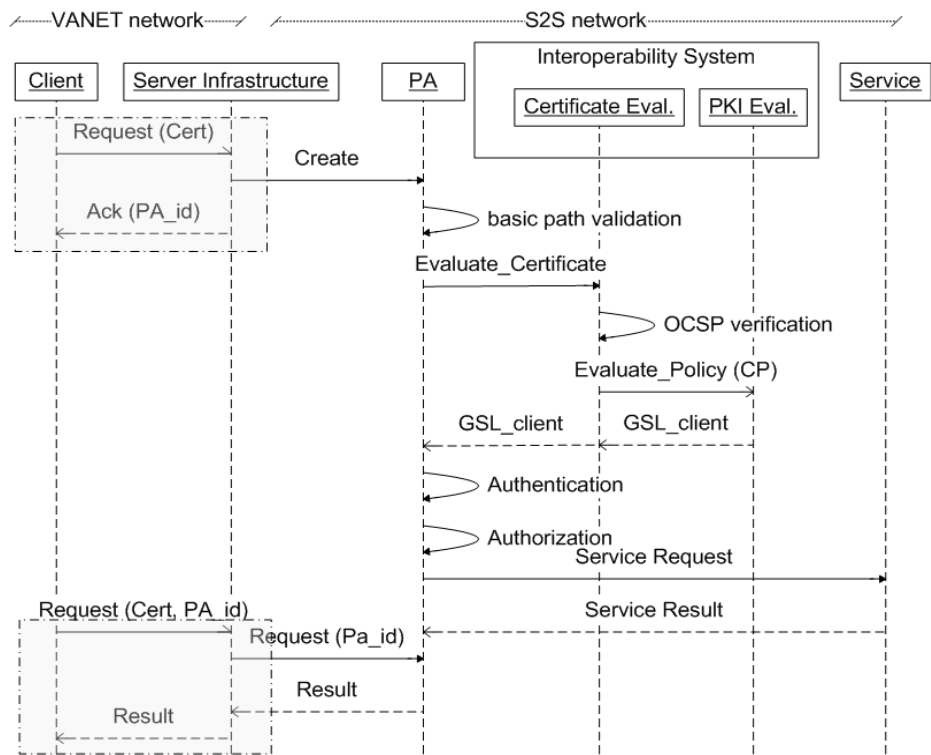
To implement the asynchronous protocol introduced in previous sections, we have proposed an approach based on agents that are able to keep the status associated to a session/request even when the connection is lost.

The proposed protocol is depicted in Figure 7. There is a special *Server Infrastructure* (it is assumed to be offered by the road infrastructure) whose aim is to accept vehicle's signed requests towards a specific *Service* being offered and, to create a *Personal Agent* associated to each request. When a Personal Agent is created, its identification number ( $PA_{id}$ ) is returned to the vehicle to acknowledge the request and to let it know how to manage a disconnection due to a communication failure. A final acknowledge message closes the previous asynchronous exchange. From this point on, the Personal Agent will work on the infrastructure on behalf of the vehicle that requested the service. The first time a car requests a service, the Personal Agent will do the following:

1. Perform the basic path validation and invoke the Interoperability Service to get the  $GSL_{client}$ ;
2. Compare the GSL of the driver ( $GSL_{client}$ ) against the GSL of the requested service ( $GSL_{server}$ ) to complete the authentication step through an Extended Path Validation;
3. Enforce the authorization mechanism (authorization handler) with the GSL and the service access control policies;
4. Forward the Car Client request to the Service Provider after authentication and authorization;
5. Store the results that will be forwarded to the Car Client even if it has lost the connection.

For the subsequent requests the vehicle will sign them and enclose its  $PA_{id}$ , which is then verified by the Server Infrastructure to return the respective stored results.

One of the requirements addressed by this protocol is that connections must be short and only few message should be exchanged. We are able to meet this by adopting an asynchronous approach: messages exchanged inside the VANET network, i.e. between the car and the server infrastructure (grey boxes in figure 7), are short and never require a complex behavior. The personal Agent (PA),

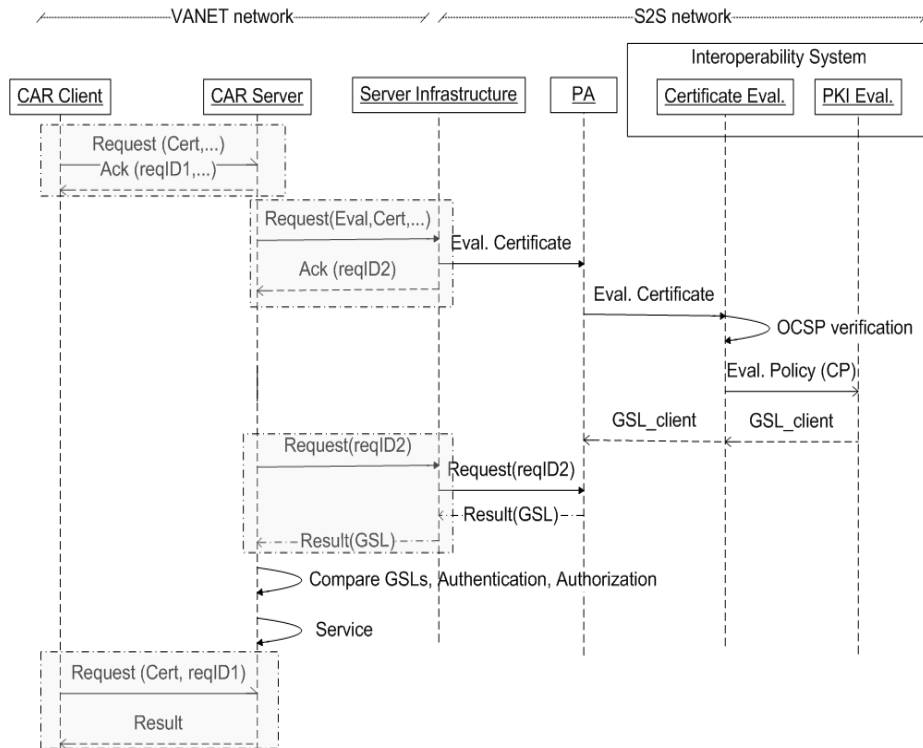


**Fig. 7.** Asynchronous Car to Service Provider communication protocol.

which resides on the server and communicates with other components using the S2S (Service to Service) network, has the role of managing the complex elaborations. To complete the exchange a car sends the *Request* message by attaching its  $PA_{id}$ . In this case, security is granted due to the certificate delegation model between the car and the PA. Following the asynchronous approach, if the client sends a Request before the result is available, the server simply will not return any result.

## 5.2 Car to Car secure access

In the asynchronous C2C scenario (Figure 8) the message originator is the *Car Client*, while the message's target becomes another vehicle (the *Car Server*). The latter can delegate its operations to its own Personal Agent (just like the one used by the Server Infrastructure explained in Section 5.1). Notice that in Figure 8 we assume that the Car Server has already created its own Personal Agent to keep the state of the Car Client's request even if the communication link among them is lost.



**Fig. 8.** Asynchronous Car to Car communication protocol.

In this scenario the following interactions occur:

1. The Car Client sends a message to the Car Server (i.e. asking for road conditions) and receives a *RequestID*.
2. The Car Server sends a request to its Personal Agent to validate the Car Client certificate.
3. The Car Server's Personal Agent performs the Extended Path Validation of the Car Client's certificate ( $Cert_{client}$ ), evaluates its GSL ( $GSL_{client}$ ) and locally stores it.
4. The Car Server requests the results of the Certificate Evaluation ( $GSL_{client}$ ). On the basis of this GSL and on a Mandatory Access Control mechanisms, it can authorize the access to the service and if granted, it will prepare and keep the service's results.
5. In the last part of the protocol the Car Client requests the service's results.

As in the previous case, the asynchronous approach helps us to face the VANET performance requirements: all messages exchanged inside the VANET network (between any car and the server infrastructure) are short and never imply complex elaborations (see grey boxes in Figure 8). From this design phase we can also note that to improve overall performance, the GSL comparison and authorization processes (currently taking place inside the Car Server) can be delegated to the Personal Agent if few resources are available. Furthermore, the Personal Agent can also cache the policy evaluation's result and associate it to a known CA, thus avoiding the re-evaluation of a known policy in the future.

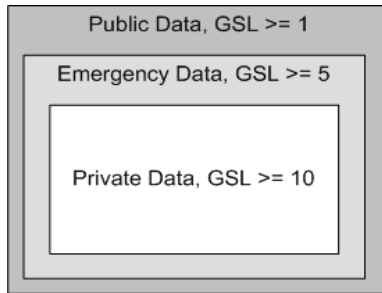
When a Car Server receives the Car Client's GSL ( $GSL_{client}$ ) a Mandatory Access Control (MAC) is applied over the driver's personal data. This authorization model is based on two basic rules [31]:

1. The *Simple Security Property* states that a subject at a given security level may not read an object at a higher security level (no read-up).
2. The *\*-Property* (read star-property) states that a subject at a given security level must not write to any object at a lower security level (no write-down) and, may only append new data to any object at a higher security level.

As introduced in Section 3 the basic idea behind the proposed authorization mechanism is to assign a *security label* to each data of the driver's personal information. This label will represent the *minimum GSL* required to enforce MAC's Simple Security Property, just as shown in the following example.

*Example 2.* Let us suppose a Car Server which driver's personal data has been assigned the security labels (GSLs) shown in Figure 9. If a Car Client's  $GSL_{client} = 5$ , then it will be able to access both, the Car Server's Public ( $GSL_{client} > GSL_{public}$ ) and Emergency data ( $GSL_{client} = GSL_{emergency}$ ), but not its Private one ( $GSL_{client} < GSL_{private}$ ).

Finally it is worth to highlight, that the drivers' real identity is not further compromised with our proposal because Personal Agents can be created according to the pseudo-identification mechanism used by the VANET (i.e. pseudonyms).



**Fig. 9.** In the proposed authorization mechanism, driver’s personal data is labeled with a minimum required security level (GSL).

## 6 Conclusions

In this paper we have presented a framework and its corresponding architecture to cope with security and interoperability problems appearing in VANET environments requiring the use of multiple regional Certification Authorities. The first part of this research has analyzed how important the concept of interoperability is for VANET’s authentication and authorization, which ultimately translates into potential risks for the overall security and privacy.

The second part of this research introduced the Interoperability System (IS) in charge of validating in near real-time the driver’s certificate via the Online Certificate Status Protocol (OCSP) and, quantitatively evaluating its security level through a technique known as the Reference Evaluation Methodology (REM). The latter value can be used to enforce a Mandatory Access Control model proposed to protect the driver’s personal data, which has been previously labeled with the minimum security level required to access it. The process just described was named Extended Path Validation and in this paper we have proposed a protocol to implement it in two widely-used VANET scenarios: car-to-car (C2C) and car-to-service providers (C2S) communication. Thanks to the use of a Personal Agent component in each node, it is possible for the proposed mechanisms to be independent of the VANET’s underlying communication protocols and to keep the state of a vehicle’s request, therefore avoiding communication problems caused by mobile nodes disconnecting from the network by any reason.

Future work will be aimed at doing the required simulations to evaluate and analyze the performance and costs of using the proposed protocol into a VANET environment, using for example an underlying routing protocol like VITP [37]. Even though in this paper we have commented the basics about using the IS for enforcing VANET’s privacy, our future work also will focus in providing a more in-depth study of this feature by comparing it versus other Privacy Enhancing Mechanisms. Finally we would like to begin extrapolating the proposed architecture and protocol to other MANET environments with analogous privacy requirements, i.e. Smartphone-to-Smartphone communication.

## References

1. Fonseca, E., Festag, A.: A survey of existing approaches for secure ad hoc routing and their applicability to vanets. Technical Report NLE-PR-2006-19, NEC Deutschland GmbH, NEC Network Laboratories (2006)
2. Raya, M., Hubaux, J.P.: The security of vehicular ad hoc networks. In: SASN '05, New York, NY, USA, ACM (2005) 11–21
3. Plossl, K., Nowey, T., Mletzko, C.: Towards a security architecture for vehicular ad hoc networks. ARES '06 (20-22 April 2006) 8
4. Prevent-project <http://www.prevent-ip.org/> (2008)
5. Zanella, A., Fasolo, E.: Inter-vehicular communication networks: a survey. In: 2nd Internal NEWCOM Workshop. (2006)
6. Security vs. privacy. [http://www.schneier.com/blog/archives/2008/01/security\\_vs\\_pri.html](http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html) (2008)
7. Hubaux, J., Capkun, S., Luo, J.: The security and privacy of smart vehicles. Security and Privacy, IEEE **02**(3) (May-June 2004) 49–55
8. Internet X.509 Public Key Infrastructure (PKI) – Proxy Certificate Profile (2002)
9. Ieee p1609.2 version 1 - standard for wireless access in vehicular environments - security services for applications and management messages (2006) Work in Progress.
10. Liu, X., Fang, Z., Shi, L.: Securing vehicular ad hoc networks. Pervasive Computing and Applications, 2007. ICPCA 2007. 2nd International Conference on (26-27 July 2007) 424–429
11. Parno, B., Perrig, A.: Challenges in securing vehicular networks. Workshop on Hot Topics in Networks (HotNets-IV) (2005)
12. Papadimitratos, P., Buttyan, L., Hubaux, J.P., Kargl, F., Kung, A., Raya, M.: Architecture for secure and private vehicular communications. Telecommunications, 2007. ITST '07. 7th International Conference on ITS (6-8 June 2007) 1–6
13. Papapanagiotou, K., Marias, G.F., Georgiadis, P.: A certificate validation protocol for vanets. Globecom Workshops, 2007 IEEE (Nov. 2007) 1–9
14. Raya, M., Jungels, D., Papadimitratos, P., Aad, I., Hubaux, J.: Certificate revocation in vehicular networks. Technical Report LCA-REPORT-2006-006, EPFL (2006)
15. Fischer, L., Aijaz, A., Eckert, C., Vogt, D.: Secure revocable anonymous authenticated inter-vehicle communication (sraac). In: 4th Workshop on Embedded Security in Cars (ESCAR 2006). (2006)
16. Moustafa, H., Bourdon, G., Gourhant, Y.: Providing authentication and access control in vehicular network environment. In Fischer-Hübner, S., Rannenber, K., Yngström, L., Lindskog, S., eds.: SEC. Volume 201 of IFIP., Springer (2006) 62–73
17. Neman, B.C.: Proxy-based authorization and accounting for distributed systems. In: Proceedings of the 13th International Conference on Distributed Computing Systems. (1993) 283–291
18. R., H., et al.: Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile (2004)
19. Casola, V., J.Luna, Oscar, M., Mazzocca, N., m. Medina, Rak, M.: Interoperable grid pkis among untrusted domains: Architectural proposal, Springer-Verlag, Lecture Notes in Computer Science (2007)
20. Aijaz, A., Bochow, B., Dtzer, F., Festag, A., Gerlach, M., Kroh, R., Leinmller, T.: Attacks on inter-vehicle communication systems - an analysis. In: 3rd International Workshop on Intelligent Transportation (WIT 2006). (2006)

21. Dötzer, F.: Privacy issues in vehicular ad hoc networks. In: Privacy Enhancing Technologies. (2005) 197–209
22. Beresford, A.R., Stajano, F.: Mix zones: User privacy in location-aware services. In: PERCOMW '04: Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, Washington, DC, USA, IEEE Computer Society (2004)
23. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in vanets. In: VANET '04: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, New York, NY, USA, ACM (2004) 29–37
24. Gerlach, M.: Assessing and improving privacy in vanets. In: 4th Workshop on Embedded Security in Cars (ESCAR 2006). (2006)
25. Gerlach, M., Güttler, F.: Privacy in vanets using changing pseudonyms - ideal and real. In: VTC Spring, IEEE (2007) 2521–2525
26. Gerlach, M.: Trust for vehicular applications. Autonomous Decentralized Systems, 2007. ISADS '07. Eighth International Symposium on (21-23 March 2007) 295–304
27. Sampigethaya, K., Huangy, L., Li, M., Poovendran, R., Matsuuray, K., Sezaki, K.: Caravan: Providing location privacy for vanet. In: 3rd Workshop on Embedded Security in Cars (ESCAR). (2005)
28. Choi, J.Y., Jakobsson, M., Wetzel, S.: Balancing auditability and privacy in vehicular networks. In: Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, New York, NY, USA, ACM (2005) 79–87
29. Fonseca, E., Festag, A., Baldessari, R., Aguiar, R.: Support of anonymity in vanets - putting pseudonymity into practice. Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE (11-15 March 2007) 3400–3405
30. Lu, R., Lin, X., Zhu, H., Ho, P.H., Shen, X.: Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications. INFOCOM 2008. The 27th Conference on Computer Communications. IEEE (April 2008) 1229–1237
31. Bell, D.E.: Looking back at the bell-la padula model. In: ACSAC '05, Washington, DC, USA, IEEE Computer Society (2005) 337–351
32. The international grid trust federation. <http://www.gridpma.org/> (2008)
33. M., M., et al.: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol (1999)
34. Certiver project. <http://www.certiver.com/> (2005)
35. Casola, V., Mazzeo, A., Mazzocca, N., Vittorini, V.: A security metric for public key infrastructures. Journal of Computer Security (February 2007)
36. Casola, V., J.Luna, Oscar, M., Mazzocca, N., m. Medina, Rak, M.: Static evaluation of certificate policies for grid pkis interoperability. In: Proc. of the 2nd International conference of Availability, Reliability and Security, IEEE Computer Society (2007)
37. Dikaiakos, M., Florides, A., Nadeem, T., Iftode, L.: Location-aware services over vehicular ad-hoc networks using car-to-car communication. Selected Areas in Communications, IEEE Journal on **25**(8) (Oct. 2007) 1590–1602