Towards a Secure and Privacy-preserving Multi-service Vehicular Architecture

Nikolaos Alexiou, Stylianos Gisdakis, Marcello Laganà,
Panagiotis Papadimitratos

KTH Royal Institute of Technology
School of Electrical Engineering
Stockholm, Sweden
{alexiou, gisdakis, lagana, papadim}@kth.se

May 31, 2013

Abstract

Intensive efforts in industry, academia and standardization bodies have brought vehicular communications (VC) one step before commercial deployment. In fact, future vehicles will become significant mobile platforms, extending the digital life of individuals with an ecosystem of applications and services. To secure these services and to protect the privacy of individuals, it is necessary to revisit and extend the vehicular Public Key Infrastructure (PKI)-based approach towards a multi-service security architecture. This is exactly what this work does, providing a design and a proof-of-concept implementation. Our approach, inspired by long-standing standards, is instantiated for a specific service, the provision of short-term credentials (pseudonyms). Moreover, we elaborate on its operation across multiple VC system domains, and craft a roadmap for further developments and extensions that leverage Web-based approaches. Our current results already indicate our architecture is efficient and can scale, and thus can meet the needs of the foreseen broad gamut of applications and services, including the transportation and safety ones.

1 Introduction

The evolution of Vehicular Communications (VC) over the past years led to extended investigations on related security and privacy-enhancing schemes. A prototype for a state-of-the-art architecture is now being built by the Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) project [1], in collaboration with the Car-to-Car Communication Consortium (C2C-CC) [2] and other European projects for field operational testing [3].

Thus far, transportation safety and efficiency have been the main driving forces for VC and related research. Nonetheless, VC systems are gradually coming to the center of an ecosystem of multiple and diverse services, service providers and user-portable devices; Location Based Services (LBSs), in-car entertainment, and infotainment [4], enabled by multiple radio technologies [5]. Vehicles are emerging as a major mobile platform for the future, running a gamut of services and performing numerous transactions for their users. This transformation and the salient characteristics of VC systems (large scale, volatility, large geographical spread) call for a renewal of our building VC security architectures. Transportation safety and efficiency already raised significant challenges for security and privacy protection; e.g., high-rate safety beaconing raises both performance (processing load and communication overhead), reliability, and credential management issues [6]. The need to grant fine-grained access, across multiple domains, to the a multiplicity of diverse services increases complexity dramatically, making it hard to address with the current identity and credential management facilities alone.

Our proposal, which we term a *multi-service* security and privacy-enhancing architecture for VC, seeks to address this challenge. We leverage long-term credential and identity managing entities, expected to be deployed for VC. We extend their mandate to handle the authorization of registered vehicles for specific services. To enable access, we leverage another longer-standing concept, a *ticket*, and cater to multi- and cross-domain operation. With these design choices, while being standard-compliant [4, 7], our architecture allows efficient and fine-grained access control in a privacy-enhancing manner. At the same time, it greatly simplifies the tasks of the service providers, and it can be further extended by leveraging web services; as a result, it can facilitate deployment of services and contribute to the enrichment of VC functionality.

In the rest of the paper, Sec. 2 discusses the current status of standardization efforts for VC security and privacy. Sec. 3 elaborates on the need for renewing the VC identity and credential management. Sec. 4 presents our design to address the problem at hand, along with evaluation results for our prototype implementation. Sec. 5 explores next steps for the development of Vehicular PKIs (VPKIs) leveraging Web Services (WS)-based approaches, before we conclude.

2 Current Status

To enable transportation safety, efficiency, and other applications, Intelligent Transport Systems (ITS) rely on VC, i.e., Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication [5]. Roadside Infrastructure Units (RSUs) and service providers are considered part of the VC infrastructure. The European Telecommunications Standards Institute (ETSI) and the IEEE defined inter-operable standards for secure VC, over the 5.9 GHz wireless channel IEEE 802.11p [7, 4]. Vehicles broadcast Cooperative Awareness Messages (CAMs) and Decentralized Environmental Notification Messages (DENMs), according to the ETSI nomenclature, to enable transportation safety and efficiency. while numerous other applications [4] are being developed.

The security and the protection of users' privacy have received extensive attention in the community. Research projects such as SeVeCom [8], PRECIOSA [9], EVITA [10], and now PRESERVE [1] have investigated multiple facets of VC security and privacy. The ensemble of such efforts in Europe and those in the US have led to a convergence on a common baseline approach summarized in the the current form of standards [4, 7].

Confidentiality, integrity, and authenticity of messages, notably CAM and DENM, are protected cryptographically. Digital signatures are generated by the Elliptic Curve Digital Signature Algorithm (ECDSA), with keys generated by curves computed over primes of 224 or 256 bits, i.e., a security level comparable to an RSA 2048-bit-long key [11]; yet, with a smaller signature size, suitable for the VC constrained and mobile environment.

The ETSI Security Working Group [12] defines a Certification Authority (CA), termed the *Enrolment Authority*, that validates an ITS station and issues enrolment credentials, i.e., certificates, valid within the CA's domain. As these credentials have long-term validity, the CA is termed the **Long Term CA (LTCA)**. The private key associated with the certificate issued by the LTCA is used whenever the vehicle needs to be authenticated as a legitimate member of the network. Long-term keys and credentials can provide message integrity, sender authenticity, and non-repudiation. However, messages signed with the same key are trivially linkable (by validating the attached signature with the same public key) and the whereabouts and actions of a vehicle (and its driver and passengers) can thus be exposed.

The location privacy of drivers and passengers can be protected if exchanged messages, e.g., CAMs and DENMs, are signed using ephemeral keys and anonymized credentials, termed *pseudonyms* [8]. Changing from one pseudonym to another renders the vehicle transmissions *linkable only over a short period*, the pseudonym lifetime [13], thus enhancing location privacy, while protecting and facilitating safety applications. Another entity, the **Pseudonym CA (PCA)**, is responsible for the provision and the management of such short-term certificates. *Pseudonymity* ensures that an Intelligent Transport Systems Station (ITS-S) may communicate or use a resource or service without disclosing its identity while remaining accountable for any such action [12, 14].

The PRESERVE project is currently developing a Hardware Security Module (HSM) which accelerates cryptographic operations to facilitate the processing of VC messages but also protect the storage of long-term and short-term keys. Digital signatures are computed within the HSM so that private keys never leave these trusted modules [1].

From a security point of view, it is important that a separation of privilege approach [15] is applied when it comes to PCAs and LTCAs. This separation mitigates the potential damage of an attack against the infrastructure, and restricts the amount of knowledge of each CA on the user's behavior. Finally, **Root CA (RCA)** is responsible for establishing trust among the different entities in the system, i.e., RCA digitally signs the certificates of the LTCA(s) and the PCA(s).

The IEEE 1609 working group has taken a somewhat different approach for the CA structure [7], yet it abides to aforementioned principles. According to the standard, LTCAs and PCAs are termed Message CAs (MCAs). In addition, the standard defines that a separate authority is responsible for signing Certificate Revocation Lists (CRLs). Lastly, the IEEE 1609 Working Group introduces a Wireless Access in Vehicular Environments (WAVE) Service Advertisement CA (WSACA) in charge of informing the entities of the system about the offered services.

In some cases, the pseudo-/anonymity needs to removed or simply the credentials (long- and/or short-term) of a vehicle (or ITS-S more generally) need to be revoked. It may be necessary to prevent further abuse if the ITS-S is compromised and thus misbehaves, or for other reasons [16]. The process of revoking the pseudonymity of a vehicle is carried out by a **Resolution Authority (RA)**. Once the actual (long-term) identity has been resolved, it might be requested that the vehicle be evicted from the network. This is done with the use of CRLs that are issued by the CAs. The LTCA issues a CRL that revokes the long-term certificate of the evicted vehicle, whereas the PCA does the same to revoke pseudonyms.

Another component of the infrastructure defined in the ETSI ITS Security document [17] is the **Authorization Authority (AA)**. Its role is to issue authorization *tickets* to the ITS stations that require specific permissions within the managed enrolment domain and the authorization context. A station requests a ticket from the AA by demonstrating the ownership of its enrolment credentials; nonetheless the AA may be prevented from determining the long-term credentials of the applying ITS station. It is possible for a single authority to assume the role of both an AA and an LTCA [12].

3 Problem Statement

A *large-scale* deployment of VC systems is expected, with numerous LTCAs, PCAs, RAs, and AAs. This deployment can be pretty *diverse*; these entities could be instantiated by state authorities, local governments, counties, cantons, metropolitan areas, cities, constituting a forest of hierarchies. At the same time, car manufacturers or any other private party (e.g., the same way that certification authorities are

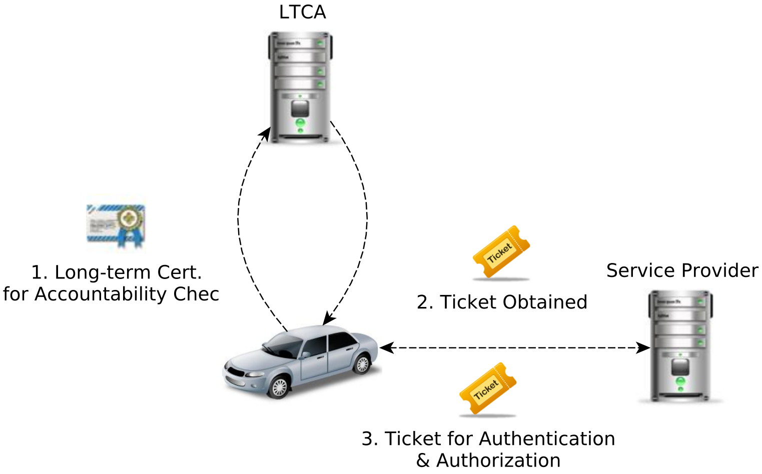

Figure 1: VeSPA: Granting access to a service

run in the traditional wire-line Internet) could instantiate them. For simplicity, let us term a subset of such entities and the registered with them vehicles as a VC system *domain*.

At the same time, scores of new services are expected, along with increased connectivity of the vehicle to the (rest of) the Internet. The diversity of these services will be much higher than that of the VC system security entities: potentially anyone could offer any service to an Internet-enabled vehicle, equipped with multiple radios. Of course, the main stake-holders (car manufacturers, transportation authorities, cities, telecommunication providers) are expected to provide a plethora of VC-specific services. Similar services could be addressed to users within a specific or across domains; each vehicle could access any set of services; Service Providers (SPs) active in different domains could have service agreements for their users. The question rises naturally: *In this VC landscape, how can a vehicle access efficiently and effectively any service it is entitled to, within any domain?*

A straightforward answer can be that each SP authenticates each vehicle and grants access. This would incur high complexity for the SPs, while identity and credential management facilities are already planned for VCs. It would then be natural to leverage these facilities: a vehicle could be authenticated and granted access based on its long-term keys and credentials. Nonetheless, this would imply loss of privacy, as all accesses would be linkable. The alternative would be to use short-term keys and credentials. This would be accountable yet only allow coarse-grained access control: for example, any pseudonym from a PCA provides access to a said service. But this would go against the provision of differentiated services to users.

What we are after: (i) fine-grained access control, (ii) privacy-preserving and (iii) accountable service access, (iv) flexible, interoperable, scalable multi-domain operation, (v) reuse of existing VPKIs and the achieved protection, and (vi) standard compliance. Moreover, we want a solution that does not add complexity on the SPs, to facilitate deployment of the foreseen multiplicity of services.

4 VeSPA: A Kerberized VPKI

To address the requirements outlined in Sec. 3 and move towards a *multi-service* architecture for secure VC, we make the following basic design choices. We de-couple the system entity responsible for access control decisions, the Policy Decision Point (PDP), from the Policy Enforcement Point (PEP) [18], the entity that enforces policy decisions. In the context of a VPKI, the PDP is the LTCA and the PEP is the PCA [17]. Then, we use the long-known concept of a *ticket* as an enabler of access, inspired by the *Kerberos* protocol [19].

We extend our Vehicular Security and Privacy-preserving Architecture (VeSPA), a VPKI architecture that uses *tickets* for Authentication Authorization and Access Control (AAA) and combines VC standards [7] and current prototypes [1] into a unified design. Extending [20], we present how VeSPA can treat multiple services and support them across different domains. VeSPA handles vehicles as clients who hold authorization tickets, in a similar manner to Kerberos. VeSPA achieves (i) *Authentication* of each vehicle to the infrastructure, (ii) *Authorization* of the vehicle to access the offered services, and (iii) *Accountability* of the vehicle for the accessed services, using the tickets and the long term credentials of the vehicles. Finally, VeSPA achieves enhanced privacy protection against the infrastructure by making any two service requests of the same vehicle unlinkable by the SP (e.g., the PCA). For the description of the protocols that follow, we assume that all communications take place over a secure TLS channel.

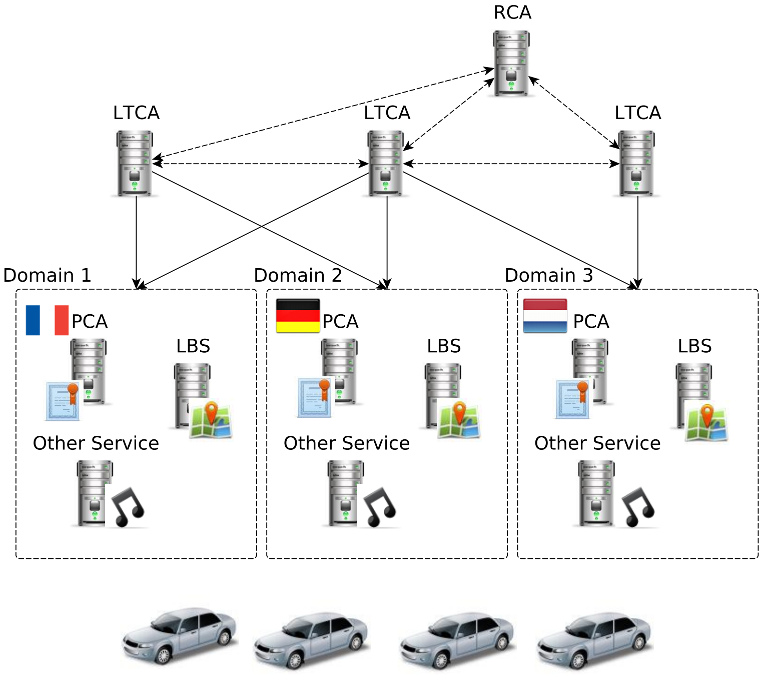

Figure 2: Multi-Domain & Multi-Service Architecture

4.1 Obtaining Tickets

To access a service, vehicles have to obtain a valid ticket first. The vehicle establishes a secure communication channel with the LTCA, which acts as the authentication and authorization point of the VPKI and, therefore, the issuer of the tickets. Vehicles are authenticated using their long-term certificates in order to provide accountability for the services. Each *ticket request* includes the list of services the vehicle wishes to access.

The LTCA is responsible for verifying the ticket request, by checking whether the vehicle should be given access to services included in the request. Reasons to reject a ticket request include an unpaid subscription to services, an invalid vehicle digital signature, or an already issued ticket for a requested service.

Tickets are digitally signed by the LTCA. The lifetime of a ticket is defined by the LTCA in the ticket itself. The ticket format is:

$$tkt = Sig_{\mathrm{LTCA}}(t_e, \{S_1\}, \dots, \{S_n\}),$$

where t_e is the ticket's expiration time and S_i is a generic service identifier. By ensuring that t_e does not exceed the subscription expiration time for any of the S_i in tkt, the LTCA can guarantee that service subscription periods are not violated. A ticket request can be made for each of the services that the vehicle subscribes to, or alternatively for a set of those, depending on the preferred level of anonymity. Separate ticket per service can enhance privacy, as Service Providers cannot learn user profiles.

Protocol 1 allows the vehicle to obtain tickets from the LTCA:

$$V \longrightarrow LTCA : Sig_{k_v}(t_1, S_1 ... S_i) \parallel LT_v \tag{1a}$$

$$LTCA \longrightarrow V : tkt \tag{1b}$$

4.2 Accessing the Service

Having obtained the ticket, the vehicle holds a (reusable) proof of access rights to a list of services (in the ticket signed by the LTCA). For example, consider a vehicle requesting access to an LBS. The ticket request contains the identity of the LBS (Steps 1a and 1b). The LTCA verifies the requesting vehicle does not already hold a valid ticket for the specific LBS, to avoid sybil attacks against service providers. If vehicles obtained and hold tickets from earlier executions of Protocol 1, they can directly get authorized to the LBS and skip the ticket obtaining phase.

Eventually, the ticket will be presented to the LBS provider by the vehicle, both as a proof of a successful authentication and authorization to the infrastructure. The LBS server checks the validity of the ticket by verifying the LTCA's signature, the ticket's lifetime, and if the LBS service is listed in the ticket. The overview of an access request to a vehicular service is given in Fig. 1. Communication with the SP is done over a TLS tunnel, using one-way, server to vehicle authentication.

4.3 Multi-Domain Architecture

A VPKI is expected to cover a domain, thus an LTCA should support thousands of registered vehicles. However, vehicles cannot be geographically restricted and services should be supported across multiple domains. Fig. 2 shows a case of different VPKI domains in three countries, with multiple services offered within each domain. A French car registered to a French VPKI, may travel to an area corresponding to the German domain, but still request access to services offered on a global scale; for example a LBS service that delivers real-time data to the vehicles. Even if the same service is offered across multiple domains, it might be subject to different conditions in each domain, e.g., an increased commission for services outside the native (home) domain or different policies altogether.

VeSPA can support vehicular applications in multiple domains using the tickets as anonymous proofs of access rights across federations of VPKIs. As shown in Protocol 2, the vehicle first obtains a native ticket from $LTCA_A$ in its *native* VPKI domain. By leveraging on the trust association between $LTCA_A$ and $LTCA_B$, the native ticket can then be exchanged for a new one, obtained from the *foreign* domain's $LTCA_B$, in a similar approach to multi-realm Kerberos.

Continuing the previous example, the French car should first obtain a valid ticket from the French domain, if it doesn't already have a valid one. The German domain can then verify the validity of the ticket

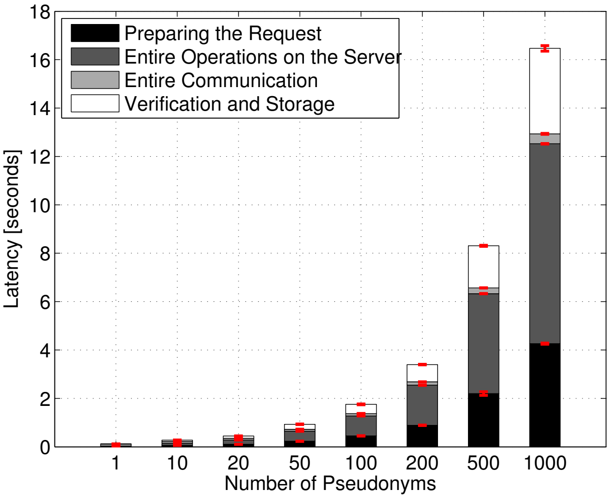

Figure 3: VeSPA: Latency in obtaining pseudonyms

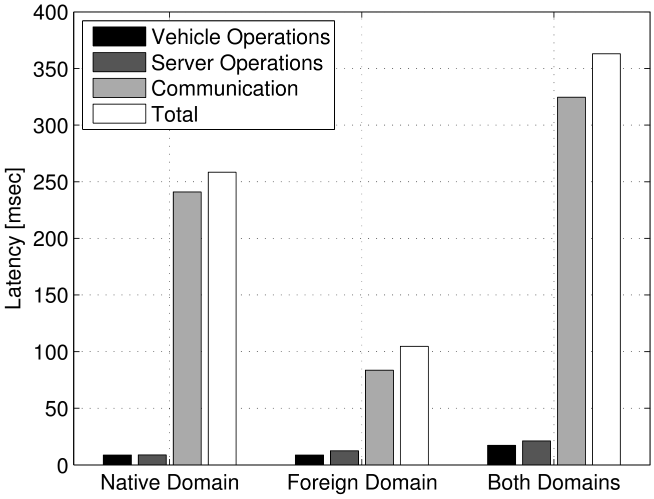

Figure 4: Performance of the Multi-Domain AAA Protocol

presented by the French car (e.g., if the requested service is offered in its own domain) and eventually apply its own policies regarding the requested service. Finally, a new ticket is issued by the German domain and sent to the French car, which can now continue accessing the service in the German domain. This way, VeSPA can support vehicular applications with multi-domain AAA, while employing *domain-specific* policies for each service (by including those in the ticket).

$$V \longrightarrow LTCA_A : Sig_{k_v}(t_1, S_1 ... S_i, Dom_B) \parallel LT_v \tag{2a}$$
$$LTCA_A \longrightarrow V : tkt_A \tag{2b}$$
$$V \longrightarrow LTCA_B : t_2, tkt \tag{2c}$$
$$LTCA_B \longrightarrow V : tkt_B \tag{2d}$$

4.4 Efficiency Analysis

We use the same experimental setup as in [20]. The average time for a vehicle to obtain one ticket containing a single service identifier from the LTCA is 100.95 msec. This low latency indicates that VeSPA can efficiently facilitate operations with *one ticket per service*, an approach for enhanced privacy protection. Moreover, VeSPA supports all the currently proposed VPKI protocols for certificate management, such as pseudonym acquisition and CRL distribution.

The pseudonym acquisition protocol incurs significant overhead; the higher the sought unlinkability, the higher the number of pseudonyms needed. Fig. 3, shows the latency for each vehicle to obtain a certain amount of pseudonyms. Acquisition of 1000 pseudonyms has an average latency of 16.46 sec. The number of requested pseudonyms depends on desired location privacy and the PCA policy. Nevertheless, 1000 pseudonyms are considered sufficient by the VC community for a period of one day, either by using equal validity time per pseudonym, or shorter pseudonym lifetime for *high mobility* hours and longer pseudonym lifetime for *low mobility* hours.

The pseudonym resolution adds very low latency to the VPKI operation: for the resolution of 200 pseudonyms, the PCA and the LTCA need 922 msec and 55 msec respectively. Furthermore, the Multi-Domain operation protocol also incurs low latency. The vehicle has to establish a secure connection with its distant native LTCA server while in a foreign domain; this communication has the dominant latency. For our experiments, we measured the latency to establish a TLS connection with a server that is 1300 km away. The total communication costs are 258.4 msec for the native domain and 104 msec for the foreign domain. The foreign LTCA has the additional overhead of verifying and handling the ticket presented by the vehicle, compared to the computational cost for the native LTCA, which only has to issue the ticket. Overall, the multi-domain protocol has a latency of 363 msec, which shows its efficiency and applicability for future VCs systems.

5 Future Directions for VPKIs

There are alternative ways of performing identity management, leveraging well-defined open standards and solutions currently in use for traditional networks. More specifically, we are developing an instantiation of an architecture structured around the Web-Services paradigm, where the LTCA serves as the Identity Provider (IdP) and the PCA as a SP. This way we treat the provision of pseudonyms, and consequently privacy, as a service.

5.1 Identity Management in a Web Services-based VPKI

In a Service-oriented-Approach (SoA), an IdP is responsible for operations such as user registration, issuance of long-term certificates, user revocation and enforcement of security policies (i.e., authorization and access control). By following a WS approach, in the context of VC, the LTCA becomes an IdP, and as a result, all of the aforementioned services can be transparently offered to any SP, including the PCA.

The merging of WS with VC can yield numerous benefits, especially in the context of trust-establishment. More specifically, to establish trust between the IdP and the SPs a WS-Metadata exchange needs to take place. In principle, metadata are Extensible Markup Language (XML) based entity descriptors. They contain various pieces of information, such as authentication requirements, the Uniform Resource Identifiers (URIs) of the VPKI entities, protocol bindings and most importantly, digital certificates. For example, referring to Figure 2, each SP may opt to establish trust relations with multiple IdPs. An SP can exchange metadata with multiple IdPs and vice versa. This approach could allow the construction of a complex Web of Trust (WoT) in a manner that satisfies policies and trust relationships without the need for RCAs. Unlike traditional PKI cross-certification schemes, WS trust configurations can be easily automated. Moreover, WS facilitate the use of technologies such as proxies, load balancers, and deployment over redundant computer clusters, thus leading to highly dependable infrastructures.

6 Conclusions

In this paper, we presented key challenges for identity management in VC, and proposed design directions of future VPKIs. We presented our Kerberized, standard-compliant VPKI prototype called VeSPA. Our ticket-based multi-service architecture can satisfy security and privacy needs of an emerging ecosystem of vehicular applications. Additionally, we realize that VPKI architectures can leverage well-defined open standards for Identity Management as in WS. The merging of VC and web technologies can yield numerous advantages. We are investigating further how to instantiate WS-based VPKIs.

References

[1] J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, and C. Schleiffer. *Security Requirements of Vehicle Security Architecture, PRESERVE - Deliverable 1.1.* Version 1.1. June 2011. URL: `http://www.preserve-project.eu/`.

[2] Car-to-Car Communication Consortium (C2C-CC). URL: `http://www.car-2-car.org/`.

[3] *Field Operational Testing Network.* Version 1.1. Jan. 2011. URL: `http://http://wiki.fot-net.eu`.

[4] ETSI TR 102 638. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions.* June 2009.

[5] P. Papadimitratos, A. De La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza. 'Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation'. In: *IEEE Communications Magazine* Vol. 47.11 (Nov. 2009), pp. 84–95.

[6] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. 'On the Performance of Secure Vehicular Communication Systems'. In: *IEEE Transactions on Dependable and Secure Computing* Vol. 8.6 (Nov. 2011), pp. 898–912.

[7] IEEE P1609.2/D12. *Draft Standard for Wireless Access in Vehicular Environments (WAVE). Security Services for Applications and Management Messages.* Jan. 2012.

[8] A. Kung. *Security Architecture and Mechanisms for V2V/V2I, SeVeCom - Deliverable 2.1.* Version 3.0. Feb. 2008.

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

[10] B. Weyl, O. Henniger, A. Ruddle, H. Seudié, M. Wolf, and T. Wollinger. 'Securing vehicular on-board IT systems: The EVITA Project'. In: *Proceedings of 25th Joint VDI/VW Automotive Security Conference.* Ingolstadt, Germany, Oct. 2009. URL: `http://www.evita-project.org/`.

[11] S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, and B. Moeller. *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS).* RFC 4492 (Informational). Internet Engineering Task Force, May 2006.

[12] ETSI TR 102 941. *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management.* June 2012.

[13] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. 'Securing Vehicular Communications - Assumptions, Requirements, and Principles'. In: *Workshop on Embedded Security in Cars (ESCAR).* Berlin, Germany, Nov. 2006.

[14] S. Park, H. Park, Y. Won, J. Lee, and S. Kent. *Traceable Anonymous Certificate.* RFC 5636 (Experimental). Internet Engineering Task Force, Aug. 2009.

[15] N. Provos, M. Friedl, and P. Honeyman. 'Preventing privilege escalation'. In: *Proceedings of the 12th conference on USENIX Security Symposium.* Vol. 12. Washington, DC, USA, Aug. 2003.

[16] P. Papadimitratos. 'On the Road - Reflections on the security of Vehicular communication systems'. In: *IEEE International Conference on Vehicular Electronics and Safety (IEEE ICVES).* Columbus, OH, USA, Sept. 2008.

[17] ETSI TR 102 731. *Intelligent Transport Systems (ITS); Security; Security Services and Architecture.* Sept. 2009.

[18] R. Yavatkar, D. Pendarakis, and R. Guerin. *A Framework for Policy-based Admission Control.* RFC 2753 (Informational). Internet Engineering Task Force, Jan. 2000.

[19] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. *The Kerberos Network Authentication Service (V5).* RFC 4120 (Proposed Standard). Updated by RFCs 4537, 5021, 5896, 6111, 6112, 6113, 6649, 6806. Internet Engineering Task Force, July 2005.

[20] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos. 'VeSPA: Vehicular Security and Privacy-preserving Architecture'. In: *Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy.* Budapest, Hungary, Apr. 2013.