Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure

Mohammad Khodaei, Hongyu Jin, Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden
{*khodaei, hongyuj, papadim*}@kth.se

arXiv:1601.00846v1 [cs.CR] 5 Jan 2016

***Abstract*---Several years of academic and industrial research efforts have converged to a common understanding on fundamental security building blocks for the upcoming Vehicular Communication (VC) systems. There is a growing consensus towards deploying a Vehicular Public-Key Infrastructure (VPKI) enables pseudonymous authentication, with standardization efforts in that direction. However, there are still significant technical issues that remain unresolved. Existing proposals for instantiating the VPKI either need additional detailed specifications or enhanced security and privacy features. Equally important, there is limited experimental work that establishes the VPKI efficiency and scalability. In this paper, we are concerned with exactly these issues. We leverage the common VPKI approach and contribute an enhanced system with precisely defined, novel features that improve its resilience and the user privacy protection. In particular, we depart from the common assumption that the VPKI entities are fully trusted and we improve user privacy in the face of an *honest-but-curious* security infrastructure. Moreover, we fully implement our VPKI, in a standard-compliant manner, and we perform an extensive evaluation. Along with stronger protection and richer functionality, our system achieves very significant performance improvement over prior systems - contributing the most advanced VPKI towards deployment.**

I. INTRODUCTION

Vehicular Communication (VC) systems enable a multitude of applications, disseminating warnings on environmental hazards, traffic conditions and other location-relevant information [1], [2]. At the same time, the need to secure VC systems and protect their users' privacy has been long and well understood [3], and academia and industry have worked towards addressing these challenges. The common understanding is to use public key cryptography: long-term credentials (and keys) for accountable identification of the VC on-board platform (termed the vehicle for simplicity), in conjunction with short-term anonymized credentials, broadly termed *pseudonyms*, for limited unlinkability of vehicle-originating messages. Projects on both sides of the Atlantic developed systems based on this approach (Secure Vehicle Communication (SeVeCom) [4], CAMP [5], IEEE 1609.2 WG [6]), in cooperation with harmonization (Car-to-Car Communication Consortium [7], [8]) and standardization (European Telecommunications Standards Institute (ETSI) [9], [10]) bodies.

The cornerstone of all these efforts, along with continuing work towards Field Operational Testing (FOT), is a Vehicular Public-Key Infrastructure (VPKI) that comprises a set of *authorities* with distinct roles: the Long Term Certification Authority (LTCA), the Pseudonym Certification Authority (PCA), and the Resolution Authority (RA). The LTCA is responsible for issuing Long Term Certificates (LTCs), in principle one per vehicle. The PCA issues sets of pseudonyms to each vehicle registered with an LTCA. Both the LTCA and the PCA can revoke the credentials they issued. When necessary, e.g., for investigation purposes, the RA can initiate a process to reveal the long-term identity of a vehicle, based on a set of pseudonymously authenticated messages. This separation of duty provides conditional anonymity, revoked under special circumstances, while ensuring that only legitimate vehicles can obtain pseudonyms and accountably participate in the system.

Challenges and Contributions: With basic concepts understood, there are few works that crisply define VPKI components. On that front, we advance the state-of-the-art, enhancing our earlier work for a *multi-domain* VPKI [11], [12], with a more complete system. Our protocols presented here and their novel features render the VPKI more robust to misbehaving vehicles. In particular, even in a future environment with a multiplicity of LTCA and PCA servers, it is impossible for a compromised vehicle to obtain multiple credentials valid simultaneously (i.e., set the ground for Sybil-based [13] misbehavior), and thus harm the VC operations. Moreover, we propose a generic pseudonym lifetime determination approach to enhance message unlinkability, thus user privacy.

So far, it has been assumed, often implicitly, that the VPKI servers are fully trustworthy. Nonetheless, the prospect of having multiple such servers commercially deployed, in diverse environments under different regulations, makes this assumption less realistic. In fact, one cannot preclude servers that are *honest*, i.e., follow specified protocols and protect their private keys, but they may be *curious*, i.e., tempted to trace clients (vehicles) if given the opportunity. For example, to offer customized services or optimize own operations. The experience from other mobile applications and location-based services hints this is a realistic threat to user privacy. To address this challenge, we extend our adversary model by considering *honest-but-curious* servers and design our VPKI to be resilient against such behaviors.

Last but not least, very few works provided detailed experimental validation of their VPKI designs to show the performance and availability of their systems. To address this challenge, we develop a *standard-compliant* full-fledged, refined, cross-platform VPKI and present an extensive experimental evaluation. Using the similar setup as in the literature, to have a meaningful and direct comparison, we find that our system achieves very significant improvement over prior art. With contributions on these three dimensions, we advance towards a more robust and scalable concrete VPKI system.

In the rest of the paper, we describe the system and adversarial model considered (Sec. II) and move on with the design of our system (Sec. III). We then analyze the protocols (Sec. IV) and present extensive experimental evaluation (Sec. V), before related work (Sec. VI) and conclusions (Sec. VII).

II. SYSTEM & ADVERSARIAL MODEL AND OBJECTIVES

System model & assumptions: We assume a VPKI architecture with distinct entities (LTCA, PCA, and RA), and we define a *domain* as the set of vehicles registered with one LTCA, subject to the same administrative regulations and policies. We do not dwell on the formation of such domains (geographic regions, cities, states, or otherwise). We assume that the LTCA is reachable by vehicles registered with it. Furthermore, we assume multiple PCA servers, active in one or across multiple domains, which have already established trust (security associations) with the corresponding LTCA(s). Each vehicle has a unique membership, registered to one domain, its *home domain*; it can freely obtain pseudonyms from any PCA in its home or in a *foreign* domain.[1] We assume that across different domains, trust is established with the help of a higher-level authority, Root Certification Authority (RCA), or a set of such authorities and cross-certification.

Adversary model: We adhere to the assumed adversarial behavior defined in the literature [3] and we are primarily concerned with adversaries that seek to abuse the VPKI. With the multi-domain, thus multi-PCA, environment, internal adversaries raise a specific challenge: they could seek to obtain multiple pseudonyms valid simultaneously over the same period of time. This would allow them to act as multiple legitimate vehicles at the same time, e.g., injecting multiple bogus messages and possibly control the outcome of specific protocols, e.g., involving voting [15]. In addition, we care about external adversaries that may mount a clogging Denial of Service (DoS) attack against the VPKI servers.

We are further concerned with VPKI servers that are *honest-but-curious*. A VPKI server could have access to eavesdropped vehicle communications, that is transcripts of anonymized signed messages. Then, with knowledge obtained from the VPKI operations, if it is able to link pseudonym sets provided to the same vehicle, it could create traces of vehicle activities, thus perform a sort of user profiling. In the worst case, multiple servers could *collude*, i.e., share knowledge.

Objectives: We seek to improve the protection achieved by strengthening the robustness of the VPKI to adversarial attacks, notably in the light of a multi-domain setup. Moreover, we seek to improve the VPKI in rendering it more resilient to *honest-but-curious* servers. The motivation for the latter stems from experience in other areas of mobile computing: service providers tend to amass information in an attempt to profile clients. Although recent VPKI proposals separate duties among servers [11], [16], no design explicitly sought to prevent such tracking. We wish to maintain standard-compliant functionalities, but at the same time protect privacy. Last but not least, we wish to significantly improve the efficiency of the VPKI demonstrated through detailed experimental evaluations, towards scalable VC system deployment.

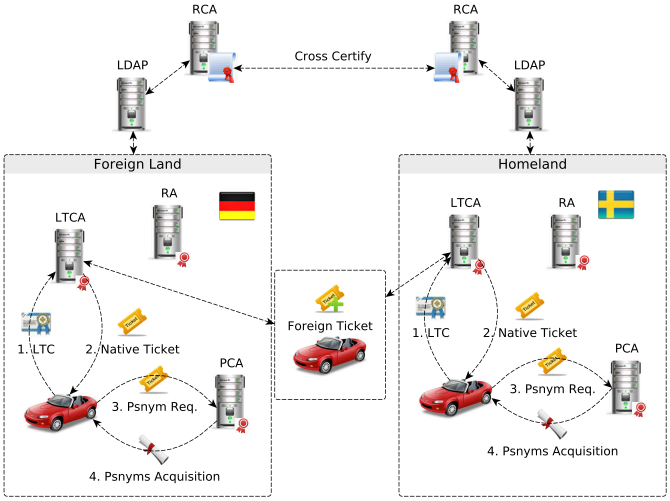


Fig. 1. System Overview

III. OUR SOLUTION

A. System Overview

Fig. 1 illustrates our proposed VPKI with two domains. The LTCA *registers* vehicles and maintains their long-term identities. It then authenticates registered vehicles and grants them access to credential management services, prominently to *obtain pseudonyms*. To do so, the vehicle obtains a *native ticket* from its home LTCA (H-LTCA) and it presents it to any PCA of its choice (e.g., one easily accessible, available, mandated, or simply preferred). The tickets are anonymized, in order not to reveal the vehicle identity to the PCA. At the same time, the *ticket issuance* protocol does not reveal to the LTCA the targeted PCA or the actual pseudonym acquisition period.

If the vehicle moves to another domain, say from Sweden to Germany, it can request from its home LTCA to obtain a *foreign ticket* without revealing the targeted foreign LTCA (F-LTCA). It then presents the foreign ticket to the German LTCA, to obtain a ticket to present to any associated PCA.[2] This way, the PCA in the German domain (in our example) will not be able to classify its requester separately from other *local* German vehicles. This is further analyzed in Sec. IV.

---

[1] In the context of VC systems, the notion of a foreign certificate was first introduced in [14].

[2] The notions of native and foreign tickets are transparent to the home LTCA based on the protocol design.

TABLE I
NOTATION USED IN THE PROTOCOLS

Lk	*Long-term Private Key*
LK	*Long-term Public Key*
k_v^i	*Pseudonymous Private Key*
K_v^i	*Pseudonymous Public Key*
P_v^i	*Pseudonymous Certificate*
CA_{id}	*Certification Authority Unique Identifier*
LTC	*Long Term Certificate*
$Cert(LTC, msg)$	*Processing of Signing on msg*
σ_{CA}	*Signature of Certification Authority*
t	*Timestamp*
N	*Nonce*
t_s	*Starting Timestamp*
t_e	*Ending Timestamp*
SN	*Serial Number*
$H()$	*Hash Function*
tkt_{expiry}	*Ticket Expiration Time*

The vehicle interacts with any PCA to obtain new pseudonyms, fetch Certificate Revocation Lists (CRLs) [14], [17], or validate pseudonym revocation status using the Online Certificate Status Protocol (OCSP) [18]. OCSP requests are authenticated with a current valid pseudonym. The overall multi-domain operations (e.g., ticket and pseudonym acquisition in a foreign domain) are assisted by directory services (Lightweight Directory Access Protocol (LDAP)). In case of misbehavior (e.g., detected locally by vehicles [19] or for other reasons [20]), the RA is able to resolve a pseudonym and possibly revoke the pseudonyms and the LTC of the misbehaving vehicle. We assume that the certificates of RCAs are pre-installed to On-Board Units (OBUs) (referred to as the vehicle for simplicity) and that the VPKI servers and the vehicles are *loosely synchronized*. All protocols are run over Transport Layer Security (TLS), with mutual authentication for obtaining tickets, and with unidirectional (server-only) authentication for obtaining pseudonyms and for LDAP queries. Table I summarizes notation used in the constituent protocols. Within a domain, the issuance of pseudonyms is regulated by the same policy, further explained in Sec. IV.

B. VPKI Services and Protocols

Vehicle Registration and LTC Update (Fig. 2): Each vehicle is registered to its home LTCA and it is issued an LTC. The vehicle generates a pair of public and private keys, LK_v and Lk_v. The prepared Certificate Signing Request (CSR) [21] is sent to the home LTCA.

Pseudonym Provision (Fig. 3): The vehicle, *V*, calculates the hash value of the concatenation of the desired PCA_{id} and a 256-bits random number; it chooses the desired time interval, $[t_s,\, t_e]$ for which it will request pseudonyms, and appends its LTC$_v$ to the *ticket provisioning request*. The protocol to obtain a ticket is:

$$\text{V} \longrightarrow LTCA : H(PCA_{id} \| Rnd_{256}), t_s, t_e, \text{LTC}_v, N, t$$
$$\text{LTCA} \longrightarrow V : tkt, N+1, t$$

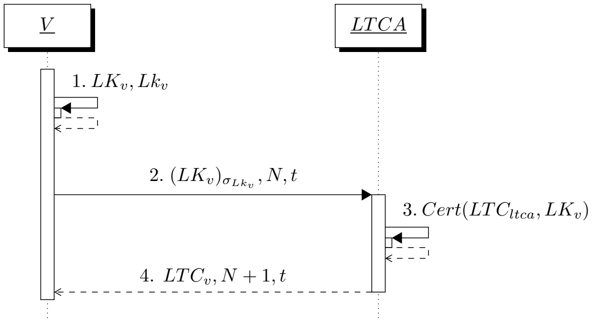


Fig. 2. Vehicle Registration and LTC Update

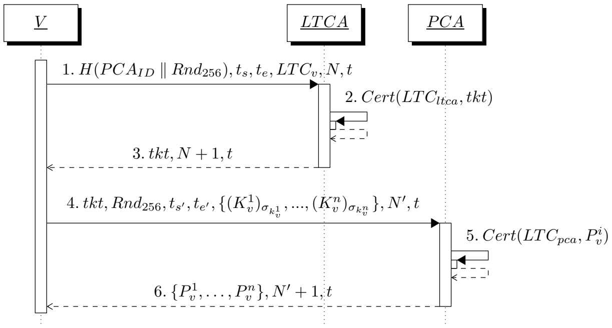


Fig. 3. Ticket and Pseudonym Acquisitions

The format of a ticket, signed by the LTCA, is:

$$tkt = \{SN, H(PCA_{id} \| Rnd_{256}), t_s, t_e, tkt_{expiry}\}_{\sigma_{\text{LTCA}}}$$

With the ticket obtained, the vehicle initiates the protocol to obtain pseudonyms:

$$\text{V} \longrightarrow PCA : Rnd_{256}, t'_s, t'_e, tkt, \{(K_v^1)_{\sigma_{k_v^1}}, ..., (K_v^n)_{\sigma_{k_v^n}}\}, N', t$$
$$\text{PCA} \longrightarrow V : \{P_v^1, \ldots, P_v^n\}, N'+1, t$$

The PCA verifies the hash value in the ticket by hashing the concatenation of its own identity and the provided random number. This ensures the ticket was issued for this PCA for the exact said time interval. A CSR, $(K_v^i)_{\sigma_{k_v^i}}$, is the signed public key generated by the vehicle. The period of requested pseudonyms, t'_s and t'_e, fall within the period of the ticket, $[t_s,\ t_e]$. Each pseudonym, signed by the PCA, is:

$$P_v^i = \{SN, K_v^i, [t_s^i, t_e^i]\}_{\sigma_{\text{PCA}}}$$

Each CSR includes the proof of possession of the corresponding private key, k_v^i [22]. Otherwise, the PCA does not issue pseudonyms for the requester. If the proof of possession on a K_v^i fails, the PCA assumes a fault; it issues pseudonyms for the correctly signed K_v^i and replies with an appropriate error message for the invalid signature. However, if the number of invalid proofs of possessions reaches a threshold, the PCA deems the requester malicious and aborts.

Foreign Domain Pseudonym Acquisition (Fig. 4 and 5): A vehicle crossing into a foreign domain obtains a *foreign ticket* (*f-tkt*) issued by its home LTCA without disclosing the targeted domain. To obtain an *f-tkt* from H-LTCA:

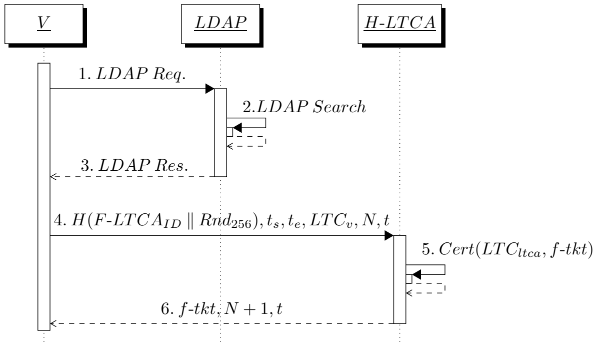


Fig. 4. Roaming User: Foreign Ticket Authentication

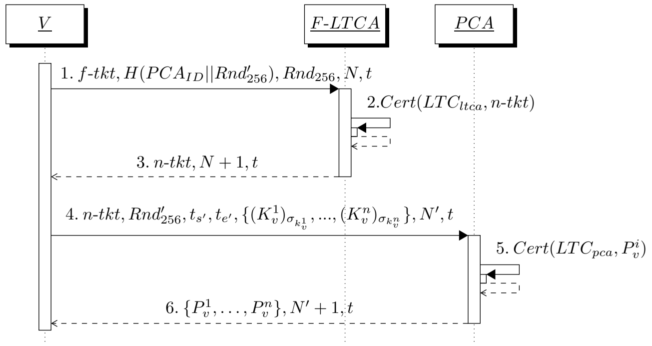


Fig. 5. Native Ticket and Pseudonym Acquisition in the Foreign Domain

$$\text{V} \longrightarrow H\text{-LTCA} : H(F\text{-}LTCA_{id} \| Rnd_{256}), t_s, t_e, \text{LTC}_v, N, t$$
$$H\text{-LTCA} \longrightarrow \text{V} : f\text{-}tkt, N+1, t$$

To obtain a *native ticket* (*n-tkt*) in the foreign domain, the vehicle sends its foreign ticket (instead of its LTC_v) to the LTCA in the foreign domain, after finding its certificate with the help of an LDAP server (similar to Fig. 3).

Pseudonym Resolution & Revocation (Fig. 6): The Resolution Authority (RA), in case of misbehavior, can resolve a pseudonym with the help of the PCA and the LTCA. The RA first asks the PCA to map the transcript pseudonyms to the corresponding ticket (which the PCA returns). Then, the RA queries the LTCA to have the vehicle identified (as the LTCA can map the ticket to the long-term credentials of the vehicle). In case of a cross-domain resolution, one additional step, involving the foreign LTCA makes the link to the H-LTCA, is needed. Steps 1, 2 and 3 in Fig. 6 show the process to resolve a ticket and possibly revoke the pseudonyms. The PCA adds all the valid pseudonyms, issued for the ticket, to the CRL. Steps 4, 5 and 6 show the process to identify the vehicle and revoke its LTC.

IV. SECURITY ANALYSIS

Our primary concern is to analyze the achieved security and privacy considering the honest-but-curious VPKI servers. We present these findings in Sec. IV-A. Then, in Sec. IV-B, we explain how arbitrary pseudonym request times along with pseudonym lifetimes can provide significant information to any adversary (eavesdropper) to link pseudonyms and thus messages. Accordingly, we explain how our policy, enforced at PCAs, can mitigate this threat. Table II summarizes notation used in the security analysis.

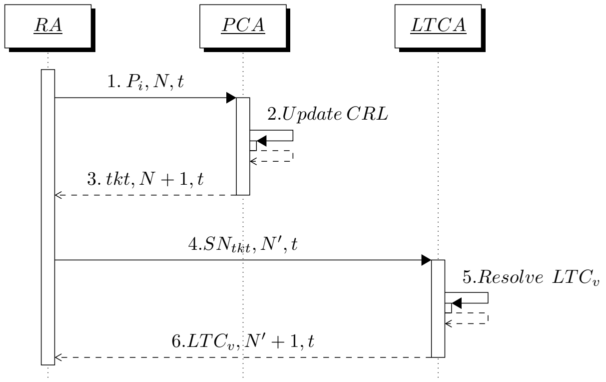


Fig. 6. Pseudonym Resolution and Revocation

TABLE II
NOTATION USED IN SECURITY ANALYSIS

$LTCA_A$	*LTCA of domain A*
PCA_{A_i}	PCA_i *in domain A*
PCA_A	*A set of PCAs in domain A*
id_A	*Identities of the vehicles in domain A*
P_A	*Pseudonyms issued by the PCAs in domain A*

Communication integrity, confidentiality, non-repudiation: This is achieved thanks to the use of secure channels (TLS) for vehicle to VPKI communication, while security associations allow any server to authenticate messages generated by any other server (notably, tickets). Digital signatures and certificates ensure non-repudiation.

Authentication and authorization: The LTCA makes the appropriate decisions, based on the registration of the vehicle, its status (revoked or not), and the use of its long-term credentials. The PCA grants the service, the pseudonyms, by validating the LTCA signature, based on their prior trust establishment. Trust associations of PCAs and LTCAs are made known to vehicles through LDAP services.

Thwarting Sybil-based misbehavior: The LTCA keeps the records of the issued tickets. Upon receiving a request, the LTCA checks whether a ticket was issued to the vehicle for that period. This ensures that no vehicle can request more than one ticket for any period. As a ticket is bound to a specific PCA and the PCA keeps records of ticket usage, a ticket cannot be reused for other PCAs. This implies that at any point in time, the vehicle cannot obtain more than one pseudonym sets (thus pseudonyms) valid simultaneously. This means that one cannot act as more than one entity.

Concealing pseudonym providers, foreign identity providers and actual pseudonym acquisition period: By sending $H(PCA_{id} \| Rnd_{256})$, t_s, t_e, LTC_v to the LTCA, the vehicle reveals its long-term identity, LTC_v, but it hides the targeted PCA$_{id}$ (and the targeted LTCA$_{id}$ in case of foreign ticket request) and the actual requested interval, $[t'_s, t'_e]$. The

TABLE III
INFORMATION HELD BY HONEST-BUT-CURIOUS ENTITIES

Honest-but-curious (colluding) Entities	**Information**	**Privacy Implications**
$LTCA_A$	id_A, t_s, t_e	An LTCA knows during when the registered vehicles wish to obtain pseudonyms.
PCA_{A_i}	t_s, t_e, P_{A_i}	A PCA can link the pseudonyms it issued for a same request, but cannot link those for different requests.
$LTCA_A$, PCA_A	id_A, t_s, t_e, P_A	The pseudonyms they issued can be linked and the vehicle identities within the same domain can be derived.
$LTCA_A$, $LTCA_B$	id_A, id_B, t_s, t_e	Collusion among LTCAs from different domains does not reveal additional information.
PCA_A, PCA_B	t_s, t_e, P_A, P_B	Collusion among PCAs from different domains does not reveal additional information.
$LTCA_A$, $LTCA_B$, PCA_A, PCA_B	$id_A, id_B, t_s, t_e, P_A, P_B$	Colluding LTCAs and PCAs can link the pseudonyms they issued. The vehicle identities can be derived, as long as the issuers of the pseudonyms and the corresponding tickets collude.

PCA, then, verifies if $[t'_s, t'_e] \subseteq [t_s, t_e]$ and grants pseudonyms accordingly.

A. Honest-but-curious Authorities

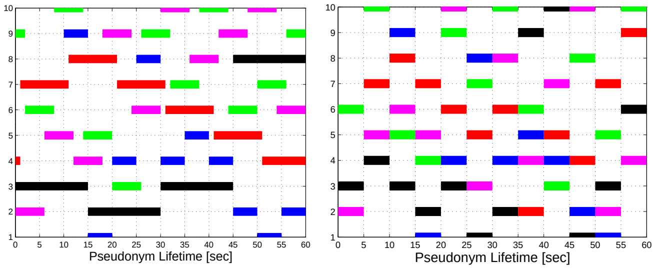
Table III outlines the information held by honest-but-curious, possibly colluding, authorities within the same domain or across domains. We do not consider the RA because it does not hold information on unresolved pseudonyms. Of course, a malicious (but, not honest-but-curious) RA could unnecessarily initiate resolutions. Collusion among the LTCA and the PCAs from the same domain enables them to link vehicle identities to issued pseudonyms. Moreover, collusion among LTCAs and PCAs from different domains further enables them to link vehicle identities to pseudonyms issued for foreign tickets.

B. Tickets and Pseudonym Lifetime Policies

Consider a set of vehicles and their pseudonyms issued in a fully flexible, on-demand manner, with a policy allowing pseudonyms with any lifetime. A transcript of pseudonymously authenticated messages can lead to linked pseudonyms simply by inspecting their (successive) lifetimes. In Fig. 7.a, the first pseudonym in row 7 is the only one valid at time 1, with lifetime 10; and then there is a single pseudonym (in row 8, from the same vehicle) valid at time 11, thus making the linking of the two trivial.

In contrast, Fig. 7.b illustrates how one can mitigate this vulnerability: the vehicle can request pseudonyms at any point in time, but the PCA must, according to the domain policy, issue all its pseudonyms according to fixed lifetimes, equal for all requesting vehicles. With the additional requirement to ensure that there is no backward overlap, by controlling the request interval, the PCA aligns all pseudonym lifetimes. This removes any distinction among different sets, resulting in an anonymity set equal to the number of (active) requests. A similar policy should also be applied to ticket acquisition. Although $[t_s, t_e]$ is protocol selectable, the LTCA fixes this to be the same for all tickets; this prevents a PCA that serves successive requests from linking tickets (similarly to the flexible pseudonym lifetime case). Of course, the actual request from the vehicle to the PCA can be any sub-interval of $[t_s, t_e]$.

Clearly, there is a trade-off in this approach: the longer the interval to obtain pseudonyms (or the ticket validity), the less frequent the vehicle-VPKI communication, but the higher the chance to overprovision a vehicle (e.g., if the period includes no movement), and vice-versa. Further discussion on an optimal choice and implementation considerations (e.g., connection to the vehicle mobility, level of unlinkability and thus pseudonym lifetime) are out of the scope of this paper.



(a) Flexible lifetimes (b) Fixed lifetimes

Fig. 7. Pseudonym lifetime policy (Each color shows the non-overlapping pseudonym lifetimes for a vehicle.)

V. EVALUATION

We are primarily interested in assessing the efficiency of the full-blown implementation of our VPKI, notably measuring the **performance** both on the client (vehicle) and the server sides. We capture this by measuring *protocol execution delays* experienced on the vehicle side, as well as measuring delays for individual protocol steps. To gauge the **availability** of the system, its ability to remain operational in the face of failures, we perform two experiments: (i) a *crash* failure of one PCA, and (ii) a Distributed Denial of Service (DDoS) of increasing intensity against a PCA and an LTCA.

Summary of findings: We demonstrate a highly efficient VPKI system, comparing its performance to the state-of-the-art for the similar experimental setup. In particular, we have a *four-fold* acceleration compared to the best previous results. Essentially, the more efficient the VPKI and the lower the overhead/cost for the vehicles, the higher the scalability of the system (being able to service more vehicles per deployed processing power unit). At the same time, the more effective and easier the vehicle-VPKI interactions are. Finally, as expected, back-up processing power renders the system dependable.

A. Experimental Setup

We allocate resources to distinct VPKI servers and we emulate the VC system, notably, the population of registered vehicles. We carry out the experiments in a controlled virtualized environment, with servers and vehicles running on Virtual Machines (VMs). This essentially eliminates network

TABLE IV
SYSTEM SETUP AND POLICIES

Type of Experiments	Pseudonyms	Execution Time	Frequency	Number of Vehicles
Ticket & Pseudonym Acquisition (Fig. 8)	1-1K	50 times	-	-
Pseudonym Acquisition (Fig. 9 & 10.a)	100	1h	6/h	10K
Pseudonym Acquisition (Fig. 10.b)	10-200	1h	10/h	10K
DDoS Attacks (Fig. 11)	100	1h	6/h (Attackers: 360/h)	10K (Attackers: 0-20K)
Fetching CRL (Fig. 12.a)	1K-100K (Revoked)	1h	6/h	10K
OCSP Operations (Fig. 12.b)	0.5K-4K (Revoked)	1h	6/h	10K
Pseudonym Resolution (Fig. 13)	1	50 times	-	-

TABLE V
SERVERS AND CLIENTS SPECIFICATIONS

	LTCA	PCA	RA	Clients
VM Number	2	5	1	25
Dual-core CPU (Ghz)	2.0	2.0	2.0	2.0
BogoMips	4000	4000	4000	4000
Memory	2GB	2GB	1GB	1GB
Database	MySQL	MySQL	MySQL	MySQL
Web Server	Apache	Apache	Apache	-
Load Balancer	Apache	Apache	-	-
Emulated Threads	-	-	-	400

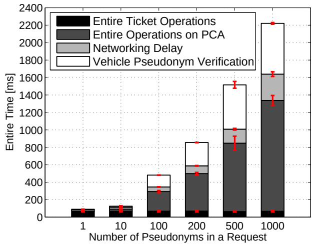


Fig. 8. Client processing time

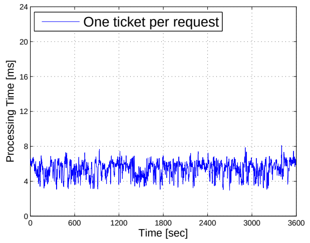
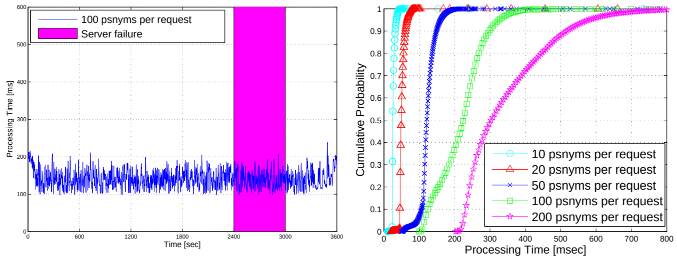


Fig. 9. LTCA performance



(a) Issuing 100 pseudonyms per request

(b) Performance under different configurations

Fig. 10. PCA processing delay

propagation delays, which would vary greatly based on the vehicle-VPKI connectivity, thus allowing us to isolate the effect of our protocols. Tables IV and V show the system setup and the servers and clients specifications respectively. We consider large sets of clients, 10K threads on 25 VMs, executing protocols with (sending requests to) the VPKI servers. We experiment under various conditions (configurations, parameters and policies). We gradually increase the load to investigate the behavior of the VPKI servers. Our implementation is in C++ and we use OpenSSL for cryptographic operations and algorithms, including: Elliptic Curve Digital Signature Algorithm (ECDSA) and TLS. As ETSI and IEEE 1609.2 propose, the ECDSA key size is 256 bits [2], [6], although other key sizes are also acceptable. It is important to note that the emulated vehicle resources are modest, much lower than the anticipated cryptographic processing power in ongoing FOTs (e.g., [23]). Thus, one can expect even better results overall.

B. Results & Analysis

1) Ticket & Pseudonym Provisioning: Fig. 8 shows the delay to obtain pseudonyms for each component, ticket provisioning, pseudonym verification, the PCA processing delay and network transmission delay.[3] The processing time to generate public/private keys is not considered here, as they can be generated off-line on the vehicle. For example, the delay to obtain 100 pseudonyms is around 500 ms. Fig. 9 shows the average response time for the LTCA to issue a ticket, approximately 5 ms (including request decapsulation, verification of the LTC, ticket issuance and response encapsulation).

Fig. 10.a shows the average response time of the PCAs for issuing 100 pseudonyms (request decapsulation, ticket certificate chain verification, verification of proof of possessions for each public key, issuance of pseudonyms and encapsulation of the response). The system configuration here requests from the PCAs to issue 100 pseudonyms every 100 minutes per vehicle. The shadowed area shows the period during which one of the servers instantiating the PCAs was forced to crash. We see that the responsiveness of the PCA remains unscathed.

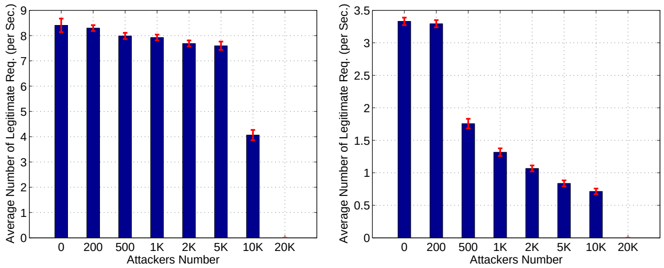
Fig. 10.b shows the performance of the PCAs issuing different numbers of pseudonyms. For example, the cumulative probability of delays for obtaining 200 pseudonyms is: $F_x(t = 500) = 0.9$, or $Pr\{t \leq 500\} = 0.9$. This confirms the system can scale: obtaining more than 120 pseudonyms every 10 minutes (pseudonym lifetime of 5 sec.) is considered as a quite demanding case, considering current expectations that one pseudonym per day or per trip is used [7]. Of course, this is a function of the number of registered vehicles and the PCA processing power. But we see that a modest machine can serve thousands of demanding vehicles.

DDoS Attack: External adversaries could clog the LTCA or the PCA with spurious, bogus requests.[4] They can send requests to the LTCA with fake certificates, or to the PCA with

---

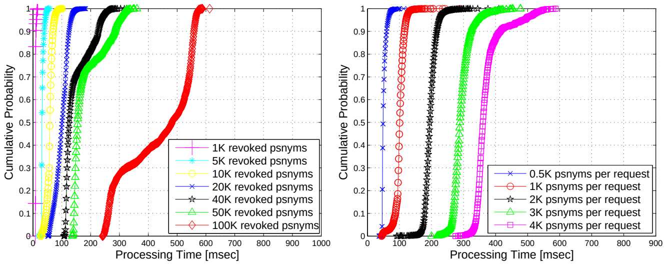
[3] Again, the lab environment dwarfs this, but it is deliberate to factor this out as it is orthogonal to our design. It was also done so in the works we compare to. A separate investigation taking into account the access networks is interesting future work.

[4] Similarly for the RA, but as it is less critical for the real-time operations of the VC system, we do not investigate here.



(a) LTCA performance (b) PCA performance

Fig. 11. VPKI servers under a DDoS attack



(a) Obtaining a CRL (b) OCSP validation

Fig. 12. Obtaining a CRL or performing OCSP validation

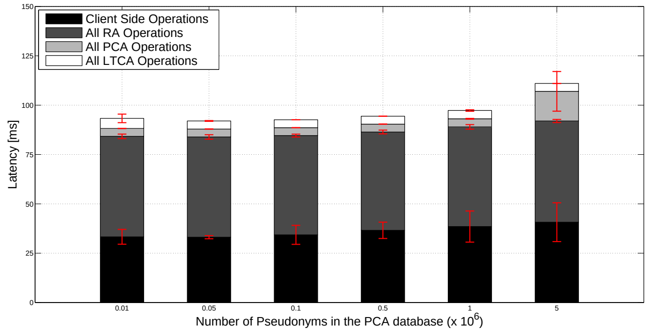


Fig. 13. Response Time to Resolve & Revoke a Pseudonym

fake tickets. We set a high request frequency, on the average once per 10 seconds, increasing the number of adversarial nodes acting this way up to 20K. Fig. 11 shows the responsiveness of an LTCA and a PCA under DDoS. The average number of legitimate serviced requests per second for the LTCA drops by half for 10K attackers. While the same happens for the PCA only for 500 attackers. This is naturally so, because both servers have the same resources, but the overhead for providing pseudonyms is much higher than that for providing a ticket. One can suggest allocating higher resources to the PCA, or employing DDoS mitigation techniques appropriate for the limited client (vehicle) resources, e.g., puzzles [24].

2) Revocation: Fig. 12.a illustrates performance when 10K vehicles query the PCAs, once every 10 minutes on average, to fetch the CRL; with different numbers of revoked pseudonyms, from one to one-hundred thousand (1K to 100K). For example, for a CRL with 50K revoked pseudonyms, $F_x(t = 280) = 0.9$, or $Pr\{t \leq 280\} = 0.9$. Fig. 12.b shows the performance when the same client population checks the revocation status of 500 to 4,000 different pseudonyms. We reckon that OCSP would not be used for such high numbers of pseudonyms. Still, the system can comfortably handle such demanding load.

3) Pseudonym Resolution: Fig. 13 shows the delay to resolve and revoke a pseudonym. As PCA databases could be gigantic, we evaluate resolution for 10,000 to 5 million pseudonyms. Pseudonym resolution and revocation is comfortably handled, in around 100 ms.

4) Performance Comparison: We compared the relevant results[5] directly to the performance results presented in [11], [12], [16], exactly because we use very similar setup. We see we achieve significant improvements in terms of efficiency and performance. The main reasons for such significant improvements, given protocols of very similar message complexity, are: multi-threading implementation and use of database, code and memory usage optimization techniques. The result of these can be a 4-fold improvement, e.g., the processing delay to issue 10 pseudonyms for the PCA for SEROSA [16] is around 100 ms, while it is approx. 26 ms in our system.

VI. RELATED WORK

The SeVeCom project [25], and its continuation, Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) [26], have led to a VPKI instantiation compliant to the Car2Car Communication Consortium (C2C-CC) framework. Because of direct PCA - LTCA communication at the time of pseudonym provision, the LTCA knows the pseudonym providing PCA, thus it can easily link messages. Similarly, the Security Credential Management System (SCMS) [5] requires that the identity provider forwards requests to PCAs, thus being prone to the same inference.[6] The linking of the pseudonym request (and thus long-term identity) to a specific PCA and the request timing (and thus an easy to guess set of pseudonyms and signed messages) is possible for VeSPA and its extension [11], [12]: they leverage an anonymized ticket but the LTCA still knows *when* the ticket will be used to obtain pseudonyms and from *which* PCAs. Our VPKI addresses this concern, providing improved security. We also achieve significant improvement in performance. For example, to obtain 10 pseudonyms, the processing delays of the PCAs in VeSPA and our scheme are 300 ms and 26 ms, respectively.

Concerning pseudonym resolution, the V-token scheme [27] mandates a random checking of V-tokens to prevent vehicles from binding false identities to pseudonyms. However, an honest-but-curious LTCA would learn which vehicles the randomly checked V-tokens belong to. Having this information, it can link the (eavesdropped) pseudonyms to the

---

[5] CRL and OCSP operations and resiliency to DDoS attacks were not considered in related works.

[6] Unlike the PRESERVE system, SCMS allows multiple simultaneously valid pseudonyms held by the vehicle, thus not being concerned with Sybil-based misbehavior.

vehicle identities by looking at the V-tokens included in the pseudonyms. CoPRA [28] stores resolution IDs, the hash of each short-term public key and a random number, at both the LTCA and the PCA; the honest-but-curious LTCA can easily calculate hashes of any public key from (eavesdropped) pseudonyms and link them to the identity of the vehicle. Our proposal is more general and more robust, further analyzed, and with detailed experimental evaluation.

SEROSA [16] proposed a general service-oriented security architecture seeking to bridge Internet and the VC domains. However, the identity provider can still infer the identity of the service provider based on the protocol design. Moreover, the multi-domain environment explicitly addressed by SEROSA (as was the case for VeSPA, and not elaborated in other proposals) leaves space for Sybil-based misbehavior. The infrastructure cannot prevent multiple spurious requests to different PCAs. Of course, an Hardware Security Module (HSM) (ensuring all signatures are generated under a single valid pseudonym at any time) can be a general remedy to the problem [29]. Our VPKI alone prevents Sybil-based misbehavior without trusted hardware and it is significantly more efficient in terms of performance.

Last but not least, an issue relevant to all systems with non-overlapping pseudonym lifetimes: while seeking to prevent Sybil-based misbehavior even without trusted hardware (as long as the misbehaving client cannot requests to multiple PCAs serviced), linkability could remain easy (Sec. IV). This was not identified before and our VPKI hints how to address it through its pseudonym lifetime and ticket validity policy.

Mixing anonymous authentication with classic public key cryptography was proposed: e.g., in [30] group signatures allow pseudonym self-generation on-the-fly; or, in [31] group keys are used as long-term credentials instead of certificates. Standardization bodies have not yet embraced such approaches. Moreover, performance evaluation results are available for Vehicle-to-Vehicle (V2V) communication [30], [32], but not for a full-blown credential management system.

VII. Conclusions

Our results primarily show that our VPKI strengthens security and privacy protection, extends functionality, and outperforms (in response delays) prior proposals. These contributions lead us closer to a robust and scalable VPKI.

References

[1] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, ‘‘Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation,’’ *IEEE Communications Magazine*, 2009.

[2] ETSI TR 102 638, ‘‘Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions,’’ Jun. 2009.

[3] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, ‘‘Securing vehicular communications-assumptions, requirements, and principles,’’ in *ESCAR*, Berlin, Germany, Nov. 2006.

[4] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, ‘‘Secure vehicular communication systems: Design and architecture,’’ *IEEE Communications Magazine*, Nov. 2008.

[5] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, ‘‘A security credential management system for V2V communications,’’ in *IEEE VNC*, Boston, MA, Dec. 2013.

[6] IEEE P1609.2/D12, ‘‘Draft Standard for Wireless Access in Vehicular Environments,’’ Jan. 2012.

[7] Car-to-Car Communication Consortium (C2C-CC). [Online]. Available: http://www.car-2-car.org/

[8] N. Bißmeyer, H. Stubing, E. Schoch, S. Gotz, J. P. Stotz, and B. Lonc, ‘‘A generic public key infrastructure for securing car-to-x communication,’’ in *ITS World Congress*, Orlando, Florida, USA, Oct. 2011.

[9] ETSI TR 102 731, ‘‘Intelligent transport systems (ITS); security; security services and architecture,’’ Sep. 2009.

[10] ETSI TR 102 941, ‘‘Intelligent transport systems (ITS); security; trust and privacy management,’’ Jun. 2012.

[11] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, ‘‘Vespa: Vehicular security and privacy-preserving architecture,’’ in *ACM HotWiSec*, Budapest, Hungary, Apr. 2013.

[12] N. Alexiou, S. Gisdakis, M. Lagan, and P. Papadimitratos, ‘‘Towards a secure and privacy-preserving multi-service vehicular architecture,’’ in *D-SPAN*, Madrid, Spain, Jun. 2013.

[13] J. R. Douceur, ‘‘The sybil attack,’’ in *ACM Peer-to-peer Systems*, London, UK, Mar. 2002.

[14] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, ‘‘Certificate revocation list distribution in vehicular communication systems,’’ in *ACM VANET*, San Francisco, CA, Sep. 2008.

[15] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, ‘‘Eviction of misbehaving and faulty nodes in vehicular networks,’’ *IEEE Journal on Selected Areas in Communications*, Oct. 2007.

[16] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, ‘‘SEROSA: Service oriented security architecture for vehicular communications,’’ Boston, MA, USA, Dec. 2013.

[17] D. Solo, R. Housley, and W. Ford, ‘‘Internet x. 509 public key infrastructure certificate and certificate revocation list profile,’’ 2002.

[18] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, ‘‘X. 509 internet public key infrastructure online certificate status protocol-ocsp,’’ RFC 2560, Tech. Rep., 1999.

[19] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, ‘‘Fast exclusion of errant devices from vehicular networks,’’ in *IEEE SECON*, San Francisco, CA, Jun. 2008.

[20] P. Papadimitratos, ‘‘”On the road” - Reflections on the Security of Vehicular Communication Systems,’’ in *IEEE ICVES*, Columbus, OH, USA, Sep. 2008.

[21] D. Cooper, ‘‘Internet x. 509 public key infrastructure certificate and certificate revocation list profile,’’ 2008.

[22] M. Myers, C. Adams, D. Solo, and D. Kemp, ‘‘Internet x. 509 certificate request message format,’’ RFC 2511, March, Tech. Rep., 1999.

[23] ‘‘Preparing secure vehicle-to-x communication systems - PRESERVE.’’ [Online]. Available: http://www.preserve-project.eu/

[24] T. Aura, P. Nikander, and J. Leiwo, ‘‘DoS-resistant authentication with client puzzles,’’ in *Proceedings of Security Protocols Workshop*, New York, USA, 2001.

[25] A. Kung, ‘‘Security architecture and mechanisms for V2V/V2I, SeVeCom - Deliverable 2.1,’’ Feb. 2008.

[26] J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, and C. Schleiffer, ‘‘Security requirements of vehicle security architecture, PRESERVE - Deliverable 1.1,’’ Jun. 2011. [Online]. Available: http://www.preserve-project.eu/

[27] F. Schaub, F. Kargl, Z. Ma, and M. Weber, ‘‘V-tokens for conditional pseudonymity in vanets,’’ in *IEEE WCNC*, NJ, USA, Apr. 2010.

[28] N. Bißmeyer, J. Petit, and K. M. Bayarou, ‘‘Copra: Conditional pseudonym resolution algorithm in vanets,’’ in *IEEE WONS*, Banff, Canada, Mar. 2013.

[29] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, ‘‘Architecture for secure and private vehicular communications,’’ in *IEEE ITST*, Sophia Antipolis, 2007.

[30] P. Papadimitratos, G. Calandriello, A. Lioy, and J.-P. Hubaux, ‘‘Impact of Vehicular Communication Security on Transportation Safety,’’ in *IEEE INFOCOM MOVE*, Phoenix, AZ, USA, Apr. 2008.

[31] A. Studer, E. Shi, F. Bai, and A. Perrig, ‘‘Tacking together efficient authentication, revocation, and privacy in vanets,’’ in *IEEE SECON*, Rome, Italy, 2009.

[32] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, ‘‘On the performance of secure vehicular communication systems,’’ *IEEE TDSC*, vol. 8, no. 6, pp. 898–912, Nov. 2011.