SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems

Mohammad Khodaei, Hongyu Jin, and Panagiotis Papadimitratos

***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 toward deploying a special-purpose identity and credential management infrastructure, i.e., a vehicular public-key infrastructure (VPKI), enabling pseudonymous authentication, with standardization efforts toward that direction. In spite of the progress made by standardization bodies (IEEE 1609.2 and ETSI) and harmonization efforts [Car2Car Communication Consortium (C2C-CC)], significant questions remain unanswered toward deploying a VPKI. Deep understanding of the VPKI, a central building block of secure and privacy-preserving VC systems, is still lacking. This paper contributes to the closing of this gap. We present SECMACE, a VPKI system, which is compatible with the IEEE 1609.2 and ETSI standards specifications. We provide a detailed description of our state-of-the-art VPKI that improves upon existing proposals in terms of security and privacy protection, and efficiency. SECMACE facilitates multi-domain operations in the VC systems and enhances user privacy, notably preventing linking *pseudonyms* based on timing information and offering increased protection even against *honest-but-curious* VPKI entities. We propose multiple policies for the vehicle–VPKI interactions and two large-scale mobility trace data sets, based on which we evaluate the full-blown implementation of SECMACE. With very little attention on the VPKI performance thus far, our results reveal that modest computing resources can support a large area of vehicles with very few delays and the most promising policy in terms of privacy protection can be supported with moderate overhead.**

***Index Terms*— Vehicular communications, security, privacy, identity and credential management, vehicular PKI.**

I. Introduction

VEHICULAR Communication (VC) systems can generally enhance transportation safety and efficiency with a gamut of applications, ranging from collision avoidance alerts to traffic conditions updates; moreover, they can integrate and enrich Location Based Services (LBSs) [1], [2] and vehicular social networks [3], and provide infotainment services. In VC systems, vehicles are provided with On-Board Units (OBUs) to communicate with each other (Vehicle-to-Vehicle (V2V) communication), or with Roadside Units (RSUs) (Vehicle-to-Infrastructure (V2I) communication). The deployment of such a large-scale system cannot materialize unless the security and privacy of the users are safeguarded [4]. Standardization bodies (IEEE 1609.2 WG [5] and ETSI [1]) and harmonization efforts (Car2Car Communication Consortium (C2C-CC) [6]) have reached a consensus to use Public Key Cryptography (PKC) to protect the V2V and V2I communications [7]: a set of Certification Authorities (CAs), constituting the Vehicular Public-Key Infrastructure (VPKI), provide credentials to legitimate vehicles; each vehicle is provided with a Long Term Certificate (LTC) (and has the corresponding private key) to ensure accountable identification of the vehicle. To achieve unlinkability of messages originating the vehicle, a set of short-lived anonymized certificates, termed *pseudonyms*, are used, along with the corresponding short-term private keys. The system maintains a mapping of these short-term identities to the vehicle long-term identity for accountability. Such ideas were elaborated by the Secure Vehicle Communication (SeVeCom) project [7], [8] and subsequent projects, e.g., Crash Avoidance Metrics Partnership Vehicle Safety Consortium (CAMP VSC3) [9] and Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) [10], as well as technical standards, notably the IEEE 1609.2 WG [5], ETSI [1], and harmonization documents (C2C-CC [6]).

In multi-domain VC systems, each vehicle is registered with one Long Term CA (LTCA), responsible for issuing its LTC, and it is able to obtain pseudonyms from any Pseudonym CA (PCA), a pseudonym provider. Vehicles digitally sign transmitted messages, e.g., Cooperative Awareness Messages (CAMs) or Decentralized Environmental Notification Messages (DENMs), with the private key, k_v^i, that corresponds to a currently valid pseudonym, P_v^i. The pseudonym is then attached to the signed messages to facilitate verification by any recipient. Upon reception, the pseudonym is verified (presuming a trust relationship with the pseudonym provider) before the message itself (signature validation). This ensures authenticity and integrity of the message and non-repudiation. Vehicles switch from one pseudonym (and the corresponding private key) to another one (ideally, non-previously used) to ensure message unlinkability (pseudonyms per se are inherently unlinkable if they are issued appropriately as it will become clear later).

We propose SECMACE, a VPKI system compatible with standards, which improves the state-of-the-art both in terms of security and privacy protection, as well as extensive

Manuscript received May 9, 2016; revised October 20, 2016; accepted June 16, 2017. Date of publication August 17, 2017; date of current version May 2, 2018. The Associate Editor for this paper was E. Kaisar. *(Corresponding author: Mohammad Khodaei.)*

The authors are with the Networked Systems Security Group, KTH Royal Institute of Technology, Stockholm 100 44, Sweden (e-mail: khodaei@kth.se; hongyuj@kth.se; papadim@kth.se).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TITS.2017.2722688

evaluations of the system. In the following, we describe four technical aspects of our system that improves over the state-of-the-art. The VPKI entities are, often implicitly, assumed to be fully trustworthy. Given the experience from recent mobile applications, we need to extend the adversarial model from fully trustworthy to *honest-but-curious* VPKI servers: they are *honest*, i.e., thoroughly complying with the best practices, specified protocols, and system policies, but *curious*, i.e., tempted to infer sensitive user information, thus harming user privacy. In the context of VC systems, an LTCA should not know which PCA is targeted, and which pseudonyms are obtained by which vehicles, and for which period; the PCA also should not be able to identify the real identity of the vehicles, or link successive pseudonym requests to a single vehicle.

We propose a system that prevents misuse of the credentials, in particular towards a Sybil-based [11] misbehavior: the acquisition of multiple simultaneously valid pseudonyms enables an attacker to inject multiple erroneous hazard notifications as if they were originated from multiple vehicles, thus misleading the system. In the light of a multi-domain VC systems with a multiplicity of PCAs, each vehicle could obtain pseudonyms from any PCA. This enables a compromised vehicle to obtain multiple sets of pseudonyms, valid simultaneously, from different PCAs, thus operating as a Sybil node. A general remedy to mitigate such a misbehavior [12] is to issue the pseudonyms with non-overlapping lifetimes and equip the vehicles with Hardware Security Modules (HSMs), using which all outgoing signatures are guaranteed to be signed under the private key of a single valid pseudonym at any time. However, our VPKI design, per se, prevents Sybil-based misbehavior in a multi-domain VC system without presuming trusted hardware.

We further ensure that the pseudonyms themselves are not inherently linkable based on the timing information: a transcript of pseudonymously authenticated messages could be linked simply based on the pseudonym lifetime and issuance times [13], and requests could act as user *"fingerprints"* [14]. Simply put, individually determined pseudonym lifetimes allow an observer to link pseudonyms of the same vehicle only by inspecting the successive pseudonym lifetimes (without even examining the content of the message). To mitigate this threat, we propose a privacy-preserving policy so that the timing information does not harm user privacy.

We provide three generally applicable policies, including a privacy-preserving one, for vehicle-VPKI interactions with a realistic evaluation of the workload that a VPKI would face. The workload on the VPKI servers mainly depends on the frequency of vehicle-VPKI interactions and the duration for which vehicles request pseudonyms for. Towards dimensioning our VPKI, we investigate the overall effects of these policies on the actual implementation of our VPKI and we provide an extensive analysis of the suitability of different representative policies for vehicle-VPKI interactions. We demonstrate that SECMACE, as the most promising VPKI in terms of performance combined with the most promising policy in terms of privacy, introduces a very modest overhead. Eventually, any vehicle could obtain all required pseudonyms within a short delay, practically in real-time, for its participation in the system.

SECMACE, a comprehensive security and privacy-preserving architecture for VC systems, contributes a set of novel features: (i) multi-domain operation, (ii) increased user privacy protection, in the presence of honest-but-curious system entities even with limited collusion, and by eliminating pseudonym linking based on timing information, (iii) thwarting Sybil-based misbehavior, and (iv) multiple pseudonym acquisition policies. Beyond these features, we provide an extensive survey of the prior art and a detailed security and privacy analysis of our system. We further provide an extensive evaluation of the overall system performance including alternative pseudonym acquisition policies, and assessing its efficiency, scalability, and robustness based on an implementation of our VPKI and two large-scale mobility traces.

In the rest of the paper, we describe the related work (Sec. II) and the problem statement (Sec. III). We then explain our system entities and model with detailed security protocols (Sec. IV). We describe the security and privacy analysis (Sec. V), followed by the extensive experimental evaluation (Sec. VI) before the conclusion (Sec. VII).

II. Related Work

Pseudonymous authentication was elaborated by SeVeCom [7], [8], PRESERVE [10], CAMP VSC3 [9], [24], standardization bodies (IEEE 1609.2 and ETSI), and harmonization efforts (C2C-CC [6]). Several proposals follow the C2C-CC architecture, e.g., PRESERVE [10], [22], entailing direct LTCA-PCA communication during the pseudonym acquisition process. This implies that the LTCA can learn the targeted PCA. As a consequence, the LTCA can link the real identity of the vehicle with its corresponding pseudonyms based on the timing information [13]: the exact time of request could be unique, or one of few, and thus linkable by the LTCA, as it might be unlikely in a specific region to have multiple requests at a specific instance.

A ticket based approach was proposed in [20], [21], and [23]: the LTCA issues authenticated, yet anonymized, tickets for the vehicles to obtain pseudonyms from a PCA. There is no direct LTCA-PCA communication and the PCA does not learn any user-related information through the pseudonym acquisition process. However, the LTCA can still learn when and from which PCA the vehicle shall obtain pseudonyms during the ticket issuance phase, because this information will be presented (by the vehicle) and will be included in the authenticated ticket (by the LTCA). The pseudonym acquisition period can be used to infer the active vehicle operation period, and the targeting PCA could be used to infer a rough location (assuming the vehicle chooses the nearest PCA) or the affiliation (assuming the vehicle can only obtain pseudonyms from the PCA it is affiliated to, or operating in) of the vehicle.

A common issue for all schemes proposed in the literature is that the PCA can trivially link the pseudonyms issued for a vehicle as a response to a single pseudonym request [18]–[23], [25]. CAMP VSC3 [9], [24] proposes a proxy-based scheme that the registration authority (a proxy to validate, process, and forward pseudonym requests to the PCA)

aggregates and shuffles all requests within a large period of time before forwarding them to the PCA, so that the PCA cannot identify which pseudonyms belong to which vehicles. Our system can also be configured to prevent an honest-but-curious PCA from linking a set of pseudonyms issued for a vehicle (as discussed in Sec. V).

The idea of enforcing non-overlapping pseudonym lifetimes was first proposed in [12]. The motivation is to prevent an adversary from equipping itself with multiple valid identities, and thus affecting protocols of collection of multiple inputs, e.g., based on voting, by sending out redundant false, yet authenticated, information, e.g., fake traffic congestion alerts, or fake misbehavior detection votes [33]. Though this idea has been accepted, a number of proposals [20]–[23] do not prevent a vehicle from obtaining simultaneously valid pseudonyms via multiple pseudonym requests. The existence of multiple PCAs deteriorate the situation: a vehicle could request pseudonyms from multiple PCAs, e.g., by requesting multiple tickets from the LTCA or reusing a ticket, while each PCA is not aware whether pseudonyms for the same period were issued by any other PCA. Reference [19] prevents a vehicle from obtaining multiple simultaneously valid pseudonyms by enabling the PCAs communicating with each other, e.g., a distributed hash table. SECMACE (including its predecessor work [13], [14]) prevents Sybil-based misbehavior on the infrastructure side without the need for an additional entity, i.e., extra interactions or intra-VPKI communications. More specifically, it ensures that each vehicle can only have one valid pseudonym at any time in a multi-domain environment: the LTCA maintains a record of ticket acquisitions for each vehicle, thus preventing a vehicle from obtaining multiple simultaneously valid tickets.

Beyond the standards specifications (classic PKC), there have been proposals to use anonymous authentication by leveraging Group Signatures (GS) [34], [35]. Each group member is equipped with a group public key, common to all the group members, and a distinct group signing key. Group signing keys can be used to sign messages and these signatures can be verified with the group public key. The signer is kept anonymous as its signatures (even the signatures of two identical messages) cannot be linked. A group signing key itself can be used to sign outgoing messages [28]. However, GS themselves exhibit high computational delay to sign VC messages [32]. For example, the signing delay with Group Signatures with Verifier Local Revocation (GS-VLR) [34] is around 67 times higher than that with the Elliptic Curve Digital Signature Algorithm (ECDSA)-256, and the verification delay with the former one is around 11 times higher than that of the latter (for the same security level, i.e., 128 bits) [32]. Reference [25] proposes a fully anonymous scheme using Zero Knowledge Proofs (ZKPs) for the vehicle-PCA authentication with the consequence that compromised OBUs can be revoked only *"manually"* with involvement of the owners.

This naturally leads us to the protocol of a hybrid approach [18], [32], [36]. In [32], a vehicle generates public/private key pairs and *"self-certifies"* the public keys on-the-fly with its own group signing key to be used as the pseudonyms. Such schemes eliminate the need to request pseudonyms from the VPKI repeatedly. Upon reception of messages signed under a new pseudonym, the GS and the pseudonym are verified before the message itself (signature validation); if the pseudonym is cached, only the signatures of the messages need to be verified. Performance improvement relies on the lifetime of each pseudonym: the longer the pseudonym lifetime is, the less frequent pseudonym verifications are needed. However, this trades off the linkability of the messages that are signed under the same pseudonym. Moreover, allowing a vehicle to generate its own pseudonyms also makes Sybil-based misbehavior possible. In [18], a vehicle requests a new pseudonym every time it enters a new region. A pseudonym request is signed with the group signing key of the vehicle, thus it is kept anonymous. Sybil-based misbehavior is prevented by fixing the random number (which is changed periodically) that used for GS generations. Therefore, a vehicle cannot request two pseudonyms through two pseudonym requests with the same random number. However, it presumes that the random number should be negotiated and bound to the vehicle before requesting pseudonyms, while it is unclear how this can be done without disclosing the vehicle identity.

Table I shows a comparison of all, to the best of our knowledge, existing proposals for a VPKI or its main building blocks with respect to their security properties. Only a few of the works evaluated the performance of their implementation while in the light of the VC large-scale multi-domain environment, the efficiency and scalability of a VPKI should be extensively evaluated. In this paper, we extensively evaluate the performance of the full-blown implementation of our VPKI. Beyond the scope of this paper, SECMACE can be highly beneficial in other application domains, e.g., secure and privacy-preserving LBS provision [37].

III. Problem Statement

A. System Model and Assumptions

We assume that a VPKI consists of a set of authorities with distinct roles: the Root CA (RCA), the highest-level authority, certifies other lower-level authorities; the LTCA is responsible for the vehicle registration and the LTC issuance; the PCA issues pseudonyms for the registered vehicles; and the Resolution Authority (RA) is able to initiate a process to resolve a pseudonym, thus identifying the long-term identity of a (misbehaving, malfunctioning, or outdated [38]) vehicle, i.e., the pseudonym owner. We further assume that each vehicle is only registered to its *Home-LTCA (H-LTCA)*, the *policy decision and enforcement point*, and is reachable by the registered vehicles in its *domain*. A *domain* is defined as a set of vehicles, registered with their H-LTCA, subject to the same administrative regulations and policies [39]. Each domain is governed by only one H-LTCA, while there are several PCAs active in one or multiple domains. Each vehicle, depending on the policies and rules, can cross to *foreign* domains and communicate with the *Foreign-LTCA (F-LTCA)* towards obtaining pseudonyms. Trust between two domains can be established with the help of an RCA, or through cross certification between them. All vehicles registered in the system are provided with HSMs, ensuring that private keys never leave the HSM. We assume that the certificates

TABLE I
VPKI SECURITY FEATURES AND PROPERTIES COMPARISON (✓: SUPPORT, ×: NO SUPPORT)

Properties / Schemes	IEEE 1609.2 compliance	ETSI compliance	Long-term identifier	Multiple domain	Sybil resilience	Cryptosystem	Cryptographic algorithms	Revocation	Accountability	Perfect forward privacy	Refilling strategy	V↔VPKI communication
Fischer et al. (SRAAC) [15]	×	×	Certificate	×	×	PKC	Magic-ink signature with DSS	✓	✓	×	On-demand	Blind signature without confidentiality
Sha et al. [16]	×	×	Certificate	✓	×	PKC	ECC public key cryptography and RSA	✓	✓	—	On-demand	Symmetric-key cryptography (session key)
SeVeCom [7, 17]	×	×	Certificate	×	✓	PKC	ECDSA	✓	✓	×	Preloading	Secure wireline communication
C2C-CC pilot PKI [6]	✓	✓	Certificate	✓	×	PKC	ECDSA	×	✓	×	Preloading	DL/ECIES over UDP
Studer et al. (TACK) [18]	×	×	Group user key	✓	✓	GS/PKC	ECDSA and VLR GS	✓	✓	✓	On-demand	GS without confidentiality
Schaub et al. (V-tokens) [19]	×	×	Certificate	✓	✓	PKC	—	×	✓	—	On-demand	Blind signature scheme & anonymous communication channel (e.g., onion routing)
Alexiou et al. (VeSPA) [20, 21]	✓	×	Certificate	✓	×	PKC	ECDSA	✓	✓	×	On-demand	SSL/TLS
PRESERVE [10]	✓	✓	Certificate	×	×	PKC	ECDSA	✓	✓	×	Preloading	DL/ECIES over UDP
Bißmeyer et al. (CoPRA) [22]	✓	✓	Certificate	✓	×	PKC	ECDSA & ECIES	×	✓	×	On-demand	DL/ECIES over UDP
Gisdakis et al. (SEROSA) [23]	✓	×	Certificate	✓	×	PKC	ECDSA	✓	✓	×	On-demand	SSL/TLS
Whyte et al. (CAMP VSC3) [9, 24]	✓	×	Certificate	✓	×	PKC	Butterfly key expansion cryptography	✓	✓	✓	Preloading	Asymmetric cryptography over UDP
Förster et al. (PUCA) [25]	×	×	Certificate	✓	✓	ZKP/PKC	ECDSA, Dynamic accumulator and CL signature	×	×	×	On-demand	SSL/TLS over Tor
Khodaei et al. (SECMACE)	✓	×	Certificate	✓	✓	PKC	ECDSA	✓	✓	✓	On-demand	SSL/TLS
Sun et al. [26]	×	×	Group user key	×	×	GS	Short GS with provably-secure ID-based signature scheme	✓	✓	✓	On-demand	—
Guo et al. [27]	×	×	Group user key	✓	×	GS	Short GS with optimization: probabilistic verification of signatures	✓	✓	✓	Annual preloading	Off-line annual renewal keys
Lin et al. (GSIS) [28]	×	×	Group user key	✓	×	GS	GS and ID-based signature	✓	✓	✓	On-demand	—
Wasef et al. (ECMV) [29]	×	×	Group user key	✓	×	GS	Bilinear & ID-based cryptography	✓	✓	✓	On-demand	Encrypted tunnel leveraging asymmetric cryptography
Wasef et al. (PPGCV) [30]	×	×	Group user key	×	×	GS	Group key cryptography	✓	✓	✓	On-demand	—
Lu et al. (ECPP) [31]	×	×	Group user key	✓	×	GS	GS & bilinear pairing-based cryptography	✓	✓	✓	On-demand	Non-secure 5.9 GHz DSRC
Calandriello et al. [32]	×	×	Group user key	×	✓	Hybrid	ECDSA and VLR GS	✓	✓	✓	On-demand	SSL/TLS

of higher-level authorities are installed on the OBUs, which are loosely synchronized with the VPKI servers.

B. Adversarial Model

We adhere to the assumed adversarial behavior defined in the literature [4] and in this paper, we are primarily concerned with adversaries that seek to abuse the VPKI. Nonetheless, we consider a stronger adversarial model: rather than assuming fully trustworthy VPKI entities, we consider them to be *honest-but-curious*. Such servers correctly execute the security protocols, but the servers function towards collecting or inferring user sensitive information based on the execution of the protocols. Such honest-but-curious VPKI servers could link pseudonym sets provided to the users, through the VPKI operations, e.g., pseudonyms issuance, thus, tracing vehicle activities. Our adversarial model considers multiple VPKI servers collude, i.e., share information that each of them individually infers with the others, to harm user privacy. The nature of collusion can vary, e.g., depending on who is the owner or administrator of any two or more colluding servers. We analyze the effects of collusion by different VPKI entities in Sec. V-A.

In a multi-PCA environment, *internal adversaries*, i.e., malicious (compromised) clients, raise two challenges. First, they could obtain multiple simultaneously valid pseudonyms, thus misbehaving each as multiple registered legitimate-looking vehicles. Second, they can degrade the operations of the system by mounting a clogging Denial of Service (DoS) attack against the VPKI servers. *External adversaries*, i.e. unauthorized entities, can try to harm the system operations by launching a DoS (or a Distributed Denial of Service (DDoS)), thus degrading the availability of the system. But they are unable to successfully forge messages or 'crack' the employed cryptosystems and cryptographic primitives.

C. Security and Privacy Requirements

The security and privacy requirements for the V2V and V2I (V2X) communications are described in the literature [4]. Here, we only focus on the security and privacy requirements on vehicle-VPKI interactions, intra-VPKI actions, and relevant requirements in the face of honest-but-curious VPKI entities.

- *R1. Authentication and communication integrity, and confidentiality:* All vehicle-VPKI interactions should be authenticated, i.e., both interacting entities should corroborate the sender of a message and the liveness of the sender. We further need to ensure the communication integrity, i.e., exchanged messages should be protected from any alternation. To provide confidentiality, the content of sensitive information, e.g., exchanged messages between a vehicle and a VPKI entity to obtain pseudonyms, should be kept secret from other entities.
- *R2. Authorization and access control:* Only legitimate, i.e., registered, and authenticated vehicles should be able to be serviced by the VPKI, notably obtain pseudonyms. Moreover, vehicles should interact with the VPKI entities according to the system protocols and policies, and domain regulations.
- *R3. Non-repudiation, accountability and eviction (revocation):* All relevant operation and interactions with the VPKI entities should be non-repudiable, i.e., no entity should be able to deny having sent a message. Moreover, all legitimate system entities, i.e., registered vehicles and

VPKI entities, should be accountable for their actions that could interrupt the operation of the VPKI or harm the vehicles. In case of any deviation from system policies, the misbehaving entities should be evicted from the system.

- *R4. Anonymity (conditional):* Vehicles should participate in the VC system *anonymously*, i.e., vehicles should communicate with others without revealing their long-term identifiers and credentials. Anonymity is conditional in the sense that the corresponding long-term identity can be retrieved by the VPKI entities, and accordingly revoked, if a vehicle deviates from system policies, e.g., submitting faulty information.
- *R5. Unlinkability:* In order to achieve *unlinkability*, the real identity of a vehicle should not be linked to its corresponding pseudonyms; in other words, the LTCA, should know neither the targeted PCA nor the actual pseudonym acquisition periods, nor the credentials themselves. Moreover, successive pseudonym requests should not be linked to the same requester and to each other. The PCA should not be able to retrieve the long-term identity of any requester, or link multiple pseudonym requests (of the same requester). Furthermore, an external observer should not be able to link pseudonyms of a specific vehicle based on information they carry, notably their timing information.[1] In order to achieve *full unlinkability*, which results in perfect forward privacy, no single entity (even the PCA) should be able to link a set of pseudonyms issued for a vehicle as a response to a single request.
  The level of anonymity and unlinkability is highly dependent on the *anonymity set*, i.e., the number of active participants and the resultant number of requests to obtain pseudonyms, e.g., all vehicles serviced by one PCA; because pseudonyms carry the issuer information, the VPKI should enhance user privacy by rendering any inference (towards linking, thus tracking, vehicles) hard.
- *R6. Thwarting Sybil-based attacks:* The VPKI should not issue multiple simultaneously valid pseudonyms for any vehicle.
- *R7. Availability:* The VPKI should remain operational in the presence of benign failures (system faults or crashes) and be resilient to resource depletion attacks, e.g., DDoS attack.

IV. Security System Entities and Design

A. System Overview

Fig. 1 illustrates our VPKI assuming two distinct domains: the home domain (A) and a foreign domain (B). In the registration phase, each H-LTCA registers vehicles within its domain and maintains their long-term identities. At the bootstrapping phase, each vehicle needs to discover the VPKI-related information, e.g., the available PCAs in its home domain, or the desired F-LTCA and PCAs in a foreign domain, along with their corresponding certificates. To facilitate the overall intra-domain and multi-domain operations, a vehicle first finds such information from a Lightweight Directory Access Protocol (LDAP) [40] server. This is carried out without disclosing the real identity of the vehicle. The vehicle, i.e., the OBU, *"decides"* when to trigger the pseudonym acquisition process based on different parameters, e.g., the number of remaining valid pseudonyms, the residual trip duration, and the networking connectivity. We presume connectivity to the VPKI, e.g., via RSUs; should the connectivity be intermittent, the OBU could initiate pseudonym provisioning proactively when there is connectivity.

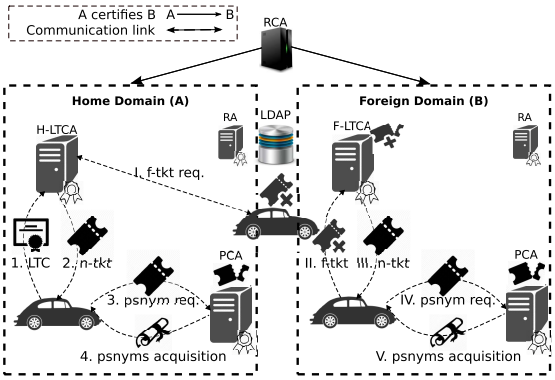


Fig. 1. Pseudonym acquisition overview in the home and foreign domains.

The H-LTCA authenticates and authorizes vehicles, which authenticate the H-LTCA over a mutually authenticated Transport Layer Security (TLS) [41] tunnel. This way the vehicle obtains a *native ticket* ($n\text{-}tkt$) from its H-LTCA while the targeted PCA or the actual pseudonym acquisition period is hidden from the H-LTCA; the ticket is anonymized and it does not reveal its owner's identity (Protocol 1). The ticket is then presented to the intended PCA, over a unidirectional (server-only) authenticated TLS, for the vehicle to obtain pseudonyms (Protocol 2).

When the vehicle travels in a foreign domain, it should obtain new pseudonyms from a PCA operating in that domain; otherwise, the vehicle would stand out with pseudonyms from another PCA. The vehicle first requests a *foreign ticket* ($f\text{-}tkt$) from its H-LTCA (without revealing its targeted F-LTCA) so that the vehicle can be authenticated and authorized by the F-LTCA. In turn, the F-LTCA provides the vehicle with a new ticket ($n\text{-}tkt$), which is native within the domain of the F-LTCA to be used for pseudonym acquisition in that (foreign) domain. The vehicle then interacts with its desired PCA to obtain pseudonyms. Obtaining an $f\text{-}tkt$ is transparent to the H-LTCA: the H-LTCA cannot distinguish between native and foreign ticket requests. This way, the PCA in the foreign domain cannot distinguish native requesters from the foreign ones. For liability attribution, our scheme enables the RA, with the help of the PCA and the LTCA, to initiate a resolution process, i.e., to resolve a pseudonym to its long-term identity. Each vehicle can interact with any PCA, within its home or a foreign domain, to fetch the Certificate Revocation List (CRL) [42] and perform Online Certificate Status Protocol (OCSP) [43] operations, authenticated with a current valid pseudonym.

[1]This does not relate to location information that vehicular communication messages, time- and geo-stamped signed under specific pseudonyms, carry.

Protocol 1 Ticket Provisioning From the H-LTCA

$$V: \textbf{P1: } (t_s, t_e) \leftarrow (t_s, t_e) \quad (1)$$

$$\textbf{P2: } (t_s, t_e) \leftarrow (t_s, \Gamma_{P2}) \quad (2)$$

$$\textbf{P3: } (t_s, t_e) \leftarrow (t_{date} + \Gamma^{i}_{P3}, t_{date} + \Gamma^{i+1}_{P3}) \quad (3)$$

$$V: \zeta \leftarrow (Id_{req}, H(Id_{pca} \| Rnd_{n\text{-}tkt}), t_s, t_e) \quad (4)$$

$$V: (\zeta)_{\sigma_v} \leftarrow Sign(Lk_v, \zeta) \quad (5)$$

$$V \rightarrow H\text{-}LTCA: ((\zeta)_{\sigma_v}, LTC_v, N, t_{now}) \quad (6)$$

$$H\text{-}LTCA: \text{Verify}(LTC_v, (\zeta)_{\sigma_v}) \quad (7)$$

$$H\text{-}LTCA: IK_{n\text{-}tkt} \leftarrow H(LTC_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}}) \quad (8)$$

$$H\text{-}LTCA: \chi \leftarrow (H(Id_{pca} \| Rnd_{n\text{-}tkt}), IK_{n\text{-}tkt}, t_s, t_e) \quad (9)$$

$$H\text{-}LTCA: (n\text{-}tkt)_{\sigma_{h\text{-}ltca}} \leftarrow Sign(Lk_{h\text{-}ltca}, \chi) \quad (10)$$

$$V \leftarrow H\text{-}LTCA: (Id_{res}, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}, Rnd_{IK_{n\text{-}tkt}}, N{+}1, t_{now}) \quad (11)$$

$$V: \text{Verify}(LTC_{h\text{-}ltca}, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}) \quad (12)$$

$$V: H(LTC_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}}) \stackrel{?}{=} IK_{n\text{-}tkt} \quad (13)$$

Protocol 2 Pseudonym Provisioning From the PCA

$$V: \zeta \leftarrow (Id_{req}, Rnd_{n\text{-}tkt}, t'_s, t'_e, (n\text{-}tkt)_{\sigma_{h\text{-}ltca}}, \{(K^1_v)_{\sigma_{k^1_v}}, \ldots, (K^n_v)_{\sigma_{k^n_v}}\}, N, t_{now}) \quad (1)$$

$$V \rightarrow PCA: (\zeta) \quad (2)$$

$$PCA: \text{Verify}(LTC_{ltca}, (n\text{-}tkt)_{\sigma_{ltca}}) \quad (3)$$

$$PCA: H(Id_{this\text{-}pca} \| Rnd_{n\text{-}tkt}) \stackrel{?}{=} H(Id_{pca} \| Rnd_{n\text{-}tkt}) \quad (4)$$

$$PCA: \textbf{P1 or P2: } [t'_s,\ t'_e] \stackrel{?}{\subseteq} ([t_s, t_e])_{n\text{-}tkt} \quad (5)$$

$$\textbf{P3: } [t'_s,\ t'_e] \stackrel{?}{=} ([t_s, t_e])_{n\text{-}tkt} \quad (6)$$

$$PCA: \textbf{for } \mathrm{i} \leftarrow 1, n \textbf{ do} \quad (7)$$

$$PCA: \quad \text{Verify}(K^i_v, (K^i_v)_{\sigma_{k^i_v}}) \quad (8)$$

$$PCA: \quad IK_{P^i_v} \leftarrow H(IK_{n\text{-}tkt} || K^i_v || t^i_s || t^i_e || Rnd_{IK_{P^i_v}}) \quad (9)$$

$$PCA: \quad \xi \leftarrow (K^i_v, IK_{P^i_v}, t^i_s, t^i_e) \quad (10)$$

$$PCA: \quad (P^i_v)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \xi) \quad (11)$$

$$PCA: \textbf{end for} \quad (12)$$

$$V \leftarrow PCA: (Id_{res}, \{(P^1_v)_{\sigma_{pca}}, \ldots, (P^n_v)_{\sigma_{pca}}\}, \{Rnd_{IK_{P^1_v}}, \ldots, Rnd_{IK_{P^n_v}}\}, N{+}1, t_{now}) \quad (13)$$

$$V: \textbf{for } \mathrm{i} \leftarrow 1, n \textbf{ do} \quad (14)$$

$$V: \quad \text{Verify}(LTC_{pca}, P^i_v) \quad (15)$$

$$V: \quad H(IK_{n\text{-}tkt} || K^i_v || t^i_s || t^i_e || Rnd_{IK_{P^i_v}}) \stackrel{?}{=} IK_{P^i_v} \quad (16)$$

$$V: \textbf{end for} \quad (17)$$

B. Pseudonym Acquisition Policies

The choice of policy for obtaining pseudonyms has diverse ramifications: on the VPKI performance as well as the user privacy. The policy determines the volume of the workload (pseudonym requests and related computation and communication latencies) imposed to the VPKI. The timing of requests can reveal information that could allow linking pseudonyms. To systematically investigate the effect of diverse on-demand pseudonym acquisition methods, here we define three specific representatives, first proposed in [14].

1) User-controlled (User-defined) Policy (P1): A vehicle requests pseudonyms for its residual (ideally entire) trip duration at the start of trip. We presume each vehicle *precisely estimates* the trip duration in advance, e.g., based on automotive navigation systems, previous trips, or user input. The PCA determines the pseudonym lifetime, either fixed for all vehicles or flexible for each requester. Additional pseudonyms should be requested if the actual trip duration exceeds the estimated one, to ensure that the vehicle is always equipped with enough valid pseudonyms throughout the entire trip.

2) Oblivious Policy (P2): The vehicle interacts with the VPKI every Γ_{P2} seconds (determined by the PCA and fixed for all users) and it requests pseudonyms for the entire Γ_{P2} time interval; this continues until the vehicle reaches its destination. This results in over-provisioning of pseudonyms only during the last iteration. The difference, in comparison to P1, is that either the vehicle does not know the exact trip duration, or, it does not attempt to estimate, or possibly, overestimate it; thus, P2 is oblivious to the trip duration.

3) Universally Fixed Policy (P3): The H-LTCA, as the policy decision point in its domain, has predetermined universally fixed interval, Γ_{P3}, and pseudonym lifetime, τ_P. At the start of its trip, a vehicle requests pseudonyms for the *"current"* Γ_{P3}, out of which useful (non-expired) ones are actually obtained for the residual trip duration within Γ_{P3}. For the remainder of the trip, the vehicle requests pseudonyms for the entire Γ_{P3} at each time. This policy issues time-aligned pseudonyms for all vehicles; thus, timing information does not harm user privacy. With P3, if the vehicle can *estimate* the trip duration, it can obtain all required pseudonyms at the start of its trip by interacting with the VPKI multiple times. However, if the vehicle does not attempt to estimate the trip duration, it should interact with the VPKI servers every Γ_{P3} seconds to obtain pseudonyms. A strict limitation in using this policy is that partial pseudonym acquisition in Γ^i_{P3} is not allowed, i.e., the vehicle must request pseudonyms for the entire Γ^i_{P3}. The reasons are twofold: (i) the PCA should not distinguish among different requests, and (ii) if the vehicle needs more pseudonyms during the same Γ^i_{P3}, it cannot request yet another ticket because the H-LTCA only issues one ticket for a single vehicle for each Γ^i_{P3}.

TABLE II
NOTATION USED IN THE PROTOCOLS

$(P_v^i)_{pca}$, P_v^i	a pseudonym signed by the PCA
(LK_v, Lk_v)	long-term public/private key pairs
(K_v^i, k_v^i)	pseudonymous public/private key pairs, corresponding to current valid pseudonym
Id_{req}, Id_{res}	request/response identifiers
Id_{ca}	Certification Authority unique identifier
LTC	Long Term Certificate
$(msg)_{\sigma_v}$	a signed message with the vehicle's private key
N, Rnd	nonce, a random number
t_{now}, t_s, t_e	fresh/current, starting, and ending timestamps
t_{date}	timestamp of a specific day
$n\text{-}tkt$, $(n\text{-}tkt)_{ltca}$	native ticket
$f\text{-}tkt$, $(f\text{-}tkt)_{ltca}$	foreign ticket
$H()$	hash function
$Sign(Lk, msg)$	signing a message with the private key (Lk)
$Verify(LTC, msg)$	verifying a message with the public key (in the LTC)
τ_P	pseudonym lifetime
Γ_{Px}	interacting period/interval with the VPKI for policy x
IK	identifiable key
V	vehicle
ζ, χ, ξ	temporary variables

C. VPKI Services and Security Protocols

In this section, we provide the detailed description of the protocols using the notation in Table II. For Unified Modeling Language (UML) diagrams of the security and privacy protocols, we refer the reader to our prior work [13].

1) Ticket Acquisition (Protocol 1): Assume the OBU decides to obtain pseudonyms from a specific PCA. If the relevant policy is P1, each vehicle *estimates* the trip duration $[t_s,\ t_e]$ (step 1.1, i.e., step 1 in Protocol 1). While with P2, each vehicle requests pseudonyms for $[t_s,\ t_s + \Gamma_{P2}]$ (step 1.2). If the relevant policy is P3, the vehicle calculates the trip duration based on the date of travel, t_{date}, and the actual time of travel corresponding to the universally fixed interval Γ_{P3} of that specific PCA (step 1.3). Then, the vehicle prepares a request and calculates the hash value of the concatenation of its desired PCA identity and a random number, i.e., $H(Id_{pca} \| Rnd_{n\text{-}tkt})$ (step 1.4). This conceals the targeted PCA, the actual pseudonym acquisition periods, and the choice of policy from the LTCA. In case of cross-domain operation, the vehicle interacts with the H-LTCA to obtain an $f\text{-}tkt$ and it concatenates its targeted F-LTCA (instead of the desired PCA) and a random number. The vehicle then signs the request (step 1.5) and sends it to its H-LTCA to obtain an $n\text{-}tkt$ (step 1.6). Upon a successful validation of the LTC and verification of the request (step 1.7), the H-LTCA generates the *"ticket identifiable key"* ($IK_{n\text{-}tkt}$) to bind the ticket to the LTC: $H(LTC_v || t_s || t_e || Rnd_{IK_{n\text{-}tkt}})$ (steps 1.8); this prevents the H-LTCA from mapping the ticket to a different LTC during resolution process. The H-LTCA then issues an *anonymous* ticket, $(n\text{-}tkt)_{\sigma_{h\text{-}ltca}}$ (step 1.9-1.10). The ticket is anonymous in the sense it does not reveal the actual identity of its owner, i.e., the H-LTCA issues tickets without the provided ticket revealing the actual identity of the requester. Thus, the PCA cannot infer the actual identity of the ticket owner, or distinguish between two tickets, even if the two tickets come from the same vehicle. Next, the H-LTCA delivers the ticket to the vehicle (step 1.11). Finally, the vehicle verifies the ticket and $IK_{n\text{-}tkt}$ (steps 1.12-1.13). In case of cross-domain operation, the vehicle interacts with the F-LTCA and presents the $f\text{-}tkt$ to obtain an $n\text{-}tkt$ in the foreign domain. Thus, it can interact with the PCAs within the foreign domain as a *"local"* vehicle.

2) Pseudonym Acquisition (Protocol 2): With an $n\text{-}tkt$ at hand, the vehicle interacts with the targeted PCA to obtain pseudonyms. The vehicle initiates a protocol to generate the required ECDSA public/private key pairs (which could be generated off-line) and sends a request to the PCA (steps 2.1-2.2). Upon reception and successful ticket verification (step 2.3), the PCA verifies the targeted PCA (step 2.4), and whether or not the actual period of requested pseudonyms (i.e., $[t'_s,\ t'_e]$) falls within the period specified in the ticket (i.e., $[t_s, t_e]$): $[t'_s,\ t'_e] \subseteq ([t_s, t_e])_{n\text{-}tkt}$ for P1 or P2, or $[t'_s,\ t'_e] = ([t_s, t_e])_{n\text{-}tkt}$ for P3 (steps 2.5-2.6). Then, the PCA initiates a proof-of-possession protocol to verify the ownership of the corresponding private keys, k_v^i.[2] The PCA generates the *"pseudonym identifiable key"* ($IK_{P_v^i}$) to bind the pseudonyms to the ticket; this prevents the compromised (malicious) PCA from mapping the pseudonyms to a different ticket during the resolution process. It then issues the pseudonyms (steps 2.7-2.12), and delivers the response (step 2.13). Finally, the vehicle verifies the pseudonyms and $IK_{P_v^i}$ (steps 2.14-2.17).

Protocol 3 Pseudonym Resolution and Revocation

$$RA : \zeta \leftarrow (Id_{req}, P_v^i) \quad (1)$$

$$RA : (\zeta)_{\sigma_{ra}} \leftarrow Sign(Lk_{ra}, \zeta) \quad (2)$$

$$RA \rightarrow PCA : ((\zeta)_{\sigma_{ra}}, LTC_{ra}, N, t_{now}) \quad (3)$$

$$PCA : \text{Verify}(LTC_{ra}, (\zeta)_{\sigma_{ra}}) \quad (4)$$

$$PCA : \{n\text{-}tkt, Rnd_{IK_{P_v^i}}\} \leftarrow \text{Resolve}(P_v^i) \quad (5)$$

$$PCA : Id_{req} \stackrel{?}{=} \text{'revoke':}\ \text{Add}(P_v^i,\ \text{CRL}) \quad (6)$$

$$PCA : \chi \leftarrow (Id_{res}, n\text{-}tkt, Rnd_{IK_{P_v^i}}) \quad (7)$$

$$PCA : (\chi)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \chi) \quad (8)$$

$$RA \leftarrow PCA : ((\chi)_{\sigma_{pca}}, N{+}1, t_{now}) \quad (9)$$

$$RA : \text{Verify}(LTC_{pca}, \chi) \quad (10)$$

$$RA : H(IK_{n\text{-}tkt} || K_v^i || t_s^i || t_e^i || Rnd_{IK_{P_v^i}}) \stackrel{?}{=} IK_{P_v^i} \quad (11)$$

$$RA : \text{ResolveLTC}(n\text{-}tkt) \quad (12)$$

3) Pseudonym Resolution and Revocation (Protocol 3): The RA requests the PCA to map the pseudonym to the corresponding ticket, i.e., $n\text{-}tkt$, which the PCA has stored (steps 3.1-3.3). The PCA verifies the request and maps the pseudonym to the corresponding $n\text{-}tkt$ (steps 3.4-3.5). If needed, the PCA includes all the valid (non-expired)

[2] As an optimization, the PCA can probabilistically verify $(K_v^i)_{\sigma_{k_v^i}}$.

pseudonyms, issued for this ticket, to the CRL, thus evicting the misbehaving vehicle from the system (step 3.6). Then, it sends the *n-tkt* to the RA (steps 3.7-3.9). The RA verifies the response and calculates the $IK_{P_v^i}$ to confirm that the PCA has correctly resolved the pseudonym to the corresponding *n-tkt* (steps 3.10-3.11). The output of this process is the *n-tkt*; in case of a cross-domain resolution, one additional interaction is needed to resolve the foreign ticket, the *f-tkt*. As a continuation, the RA resolves the ticket with the help of the corresponding H-LTCA (step 3.12, detailed in Protocol 4).

Protocol 4 LTC Resolution and Revocation

$$RA : \zeta \leftarrow (Id_{req}, n/f\text{-}tkt, N, t_{now}) \quad (13)$$

$$RA : (\zeta)_{\sigma_{ra}} \leftarrow Sign(Lk_{ra}, \zeta) \quad (14)$$

$$RA \rightarrow H\text{-}LTCA : ((\zeta)_{\sigma_{ra}}, LTC_{ra}) \quad (15)$$

$$H\text{-}LTCA : \text{Verify}(LTC_{ra}, (\zeta)_{\sigma_{ra}}) \quad (16)$$

$$H\text{-}LTCA : \{LTC_v, Rnd_{IK_{n\text{-}tkt}}\} \leftarrow \text{Resolve}(n/f\text{-}tkt) \quad (17)$$

$$H\text{-}LTCA : Id_{req} \stackrel{?}{=} \text{'revoke':}\ \text{Add}(LTC_v,\ \text{CRL}) \quad (18)$$

$$H\text{-}LTCA : \chi \leftarrow (Id_{res}, LTC_v, Rnd_{IK_{n\text{-}tkt}}, N{+}1, t_{now}) \quad (19)$$

$$H\text{-}LTCA : (\chi)_{\sigma_{h\text{-}ltca}} \leftarrow Sign(Lk_{h\text{-}ltca}, \chi) \quad (20)$$

$$RA \leftarrow H\text{-}LTCA : (\chi)_{\sigma_{h\text{-}ltca}} \quad (21)$$

$$RA : \text{Verify}(LTC_{h\text{-}ltca}, \chi) \quad (22)$$

$$RA : H(LTC_v||t_s||t_e||Rnd_{IK_{n\text{-}tkt}}) \stackrel{?}{=} IK_{n/f\text{-}tkt} \quad (23)$$

4) LTC Resolution and Revocation (Protocol 4): The RA queries the corresponding H-LTCA to have the vehicle identified, i.e., resolving the LTC of the vehicle. The RA prepares a request and sends the ticket serial number to H-LTCA (steps 4.13-4.15). Upon the request verification, the H-LTCA resolves, and possibly revokes, the LTC corresponding to the *n-tkt* (steps 4.16-4.18). The H-LTCA delivers the response back to the RA (steps 4.19-4.21). Upon reception of the response, the RA verifies the signature and confirms if the H-LTCA has mapped the correct LTC_v by validating the IK (steps 4.22-4.23).

V. Security and Privacy Analysis

We analyze the achieved security and privacy of our VPKI with respect to the requirements presented in Sec. III-C. All the communication runs over secure channels, i.e., TLS with uni- or bidirectional authentication, thus we achieve *authentication, communication integrity* and *confidentiality* (R1). The H-LTCA authenticates and authorizes the vehicles based on the registration and their revocation status, and makes appropriate decisions. It grants a *service-granting ticket*, thus enabling the vehicles to request pseudonyms from any PCA by presenting its anonymous ticket. The PCA then grants the service, based on prior established trust, by validating the ticket (R2). Given the ticket acquisition request is signed with the private key corresponding to the vehicle's LTC and pseudonym acquisition entails a valid ticket, the system provides *non-repudiation and accountability* (R3). Moreover, the LTCA and the PCA calculate ticket and pseudonym identifiable keys (IK_{tkt} and IK_P) to bind them to the corresponding LTC and ticket respectively (R3).

According to the protocol design, the vehicle conceals the identity of its targeted PCA with $H(Id_{pca}||Rnd_{n\text{-}tkt})$, and the targeted F-LTCA when operating in a foreign domain. With P1 and P2, the vehicle hides the actual pseudonym acquisition periods, i.e. $[t_s', t_e']$, while only $[t_s, t_e]$ is revealed to the LTCA. With P3, requesting intervals fall within the *"universally"* fixed Γ_{P3} (along with aligned pseudonyms lifetimes); thus timing information cannot be used to link two successive pseudonyms as they are time-aligned with those of all other active vehicles that obtain pseudonyms by the same PCA (R4, R5). This is further discussed in Sec. V-B. Moreover, the separation of duties between the LTCA and the PCA provides *conditional anonymity*, but revoked under special circumstances, e.g., misbehavior (R3).

The H-LTCA enforces a policy that each vehicle cannot obtain tickets with overlapping lifetime: upon receiving a request, the H-LTCA checks if a ticket was issued for the requester during that period. This ensures that no vehicle can obtain more than a single valid ticket to request multiple simultaneously valid pseudonyms. Moreover, a ticket is implicitly bound to a specific PCA; thus, it cannot be used more than once or be reused for other PCAs. The PCA also issues the pseudonyms with non-overlapping lifetimes; all in all, no vehicle can be provided with more than one valid pseudonym at any time; thus, Sybil-based misbehavior is thoroughly thwarted within a multi-domain VC environment (R6). We achieve availability in the face of a crash failure by mandating load-balancers and server redundancy [13]; in case of a DDoS attack, we use a puzzle technique as a mitigation approach (R7), further discussed in Sec. VI-B.5.

The OBU could request pseudonyms for a period depending on the policy, determined by the user (P1) or fixed by the VPKI (P2 and P3). Based on the policy and the pseudonym lifetime, the OBU automatically calculates the number of pseudonyms to obtain. Clearly, there is a trade off: the longer the pseudonym refill interval is, i.e., the higher the number of pseudonyms in a single request is, the less frequent vehicle-VPKI interactions are. But the higher the chance for a PCA to trivially link the issued pseudonyms for the same vehicle as a response to a single request. With our scheme, we can configure the system to reduce the number of pseudonyms per request to one to achieve *full unlinkability*, thus enhancing user privacy. To do so, we configure the system with P3 so that Γ_{P3} is equal to τ_P, and have each vehicle requesting pseudonyms for a duration of $[t_s, t_s + \tau_P]$, i.e., obtaining a single pseudonym with a different ticket. This implies that a PCA cannot link any two pseudonyms issued for a single vehicle. But this configuration increases the frequency of vehicle-VPKI interactions. The performance of our VPKI to issue fully-unlinkable pseudonyms is evaluated in Sec. VI-B.3.

TABLE III
INFORMATION HELD BY HONEST-BUT-CURIOUS ENTITIES

Honest-but-curious (colluding) Entities	Information Leaked	Security and Privacy Implications
H-$LTCA$	id_H, t_s, t_e	An H-LTCA knows during when the registered vehicles wish to obtain pseudonyms.
PCA_{H_i}	t_s, t_e, P_{H_i}	A PCA in the home domain can link the pseudonyms it issued for a same request, but it cannot link those for different requests.
H-$LTCA$, F-$LTCA$	id_H, id_F, t_s, t_e	Collusion among LTCAs from different domains does not reveal additional information.
PCA_H, PCA_F	t_s, t_e, P_H, P_F	Collusion among PCAs from different domains does not reveal additional information.
H-$LTCA$, PCA_H	id_H, t_s, t_e, P_H	The pseudonyms they issued can be linked and the vehicle identities within the same domain can be derived.
F-$LTCA$, PCA_F	id_F, t_s, t_e, P_F	The pseudonyms they issued can be linked but the real identities of the vehicles cannot be derived.
H-$LTCA$, F-$LTCA$, PCA_F	$id_H, id_F, t_s, t_e, P_F$	Colluding H-LTCAs, F-LTCA and PCA$_F$ can link the pseudonyms issued in the foreign domain with the real identities of the vehicles if the PCA_F is the issuer of the pseudonyms.
H-$LTCA$, F-$LTCA$, PCA_F, PCA_F	$id_H, id_F, t_s, t_e, P_H, P_F$	Colluding H-LTCAs, F-LTCA, PCA$_H$ and PCA$_F$ can link the pseudonyms issued in the home and foreign domains with the real identities of the vehicles if the PCA_H and PCA_F are the issuers of the pseudonyms.
V, H-$LTCA$, F-$LTCA$, PCA_F, PCA_F	$id_H, id_F, t_s, t_e, P_H, P_F$	Colluding vehicle, H-LTCA, F-LTCA, PCA$_H$, and PCA$_F$ could result in generating invalid $IK_{n/f\text{-}tkt}$, $IK_{n\text{-}tkt}$, or IK_{P_v}, respectively.

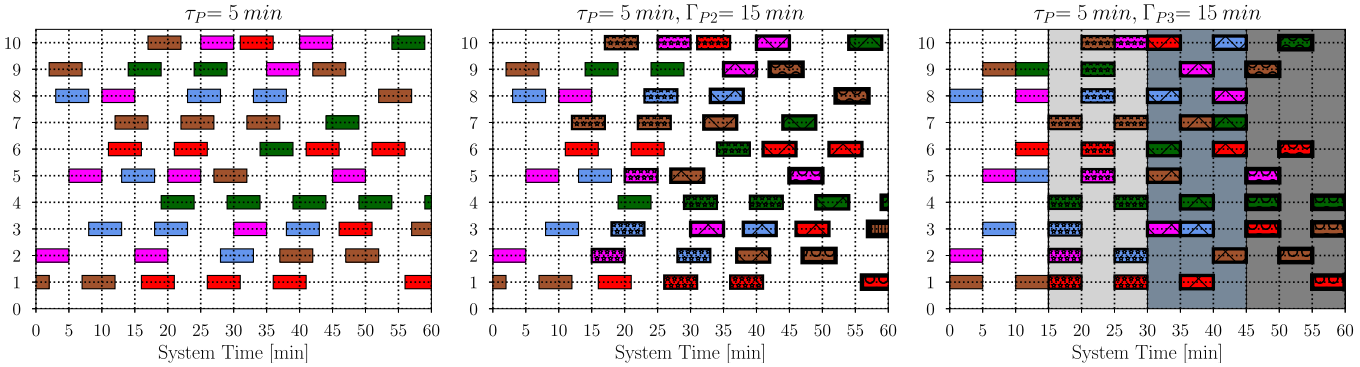


Fig. 2. Pseudonym acquisition policies (Each color shows the non-overlapping pseudonym lifetime). (a) P1: User-controlled policy. (b) P2: Oblivious policy. (c) P3: Universally fixed policy.

TABLE IV
NOTATION USED IN SECURITY & PRIVACY ANALYSIS

PCA_{H_i}	PCA_i in the home domain
PCA_H	a set of PCAs in the home domain
PCA_F	a set of PCAs in the foreign domain
id_H	identities of the vehicles in the home domain
id_F	identities of the vehicles in the foreign domain
P_H	pseudonyms issued by the PCAs in the home domain

A. Honest-But-Curious VPKI Servers

We further consider the privacy sensitive information that can be inferred by colluding VPKI servers within the home or across domains. Table III presents this information and the privacy implications when different honest-but-curious VPKI entities collude, based on notation summarized in Table IV. A single entity cannot fully de-anonymize a user due to the separation of duties in our design. Collusion by H-LTCA and F-LTCAs, or PCA_H and PCA_F from the same or different domains, do not reveal any useful information to link the user identities with their pseudonyms. However, collusion by H-LTCA and the PCA_H enables them to link the vehicle identities with their pseudonyms. Collusion by the F-LTCA and the PCA_F does not reveal the real identities of the vehicles, but their pseudonyms and the foreign domain identifier. Collusion by H-LTCA, F-LTCA and PCA_F enables them to link the issued pseudonyms with their long term identifiers. Additionally, collusion by H-LTCA, F-LTCA, PCA_H, and PCA_F results in linking the vehicle identities and their corresponding pseudonyms in the home and foreign domains. Finally, collusion of a vehicle and the H-LTCA, the F-LTCA, or the PCA, could yield invalid $IK_{n/f\text{-}tkt}$, $IK_{n\text{-}tkt}$, or $IK_{P_v^i}$, respectively.

B. Ticket and Pseudonym Lifetime Policies

Fig. 2 displays a transcript of eavesdropped pseudonyms for different pseudonym acquisition policies ($\Gamma = 15$ min, $\tau_P = 5$ min). We assume an LTCA, a PCA, or an external observer attempts to link pseudonyms of the same vehicle based on the timing information of the credentials. With P1 and P2 (Fig. 2.a and 2.b), requests could act as user *"fingerprints"*: the exact time of requests and all subsequent requests until the end of trip could be unique, or one of few, and thus linkable even by an external observer as it might be unlikely in a specific region to have multiple requests at a unique instance. In Fig. 2.a, the pseudonym (colored in magenta) in row 2 expires at system time 5 while the only pseudonym valid at time 5 is located in row 5. Thus, an external observer could simply link these two pseudonyms based on the pseudonym lifetimes. With P2, not only an external observer could link two successive pseudonyms of the same vehicle, but also a PCA could link two sets of pseudonyms for the same requester based on the timing information: in Fig. 2.b, the second pseudonym in row 8 (colored in magenta) is the last pseudonym issued for the first iteration of Γ_{P2}, which expires at system time 15. The only pseudonym starting from 15 in the second iteration of Γ_{P2} is the second pseudonym in row 2 (with a repeated asterisk pattern colored in magenta).

TABLE V
SERVERS AND CLIENTS SPECIFICATIONS

	LTCA	PCA	RA	Client
Number of entities	1	1	1	1
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

TABLE VI
MOBILITY TRACES INFORMATION

	Tapas-Cologne	LuST
Number of vehicles	75,576	138,259
Number of trips	75,576	287,939
Duration of snapshot (hour)	24	24
Available duration of snapshot (hour)	2 (6-8 AM)	24
Average trip duration (sec)	590.49	692.81

This vulnerability is thwarted by P3 (Fig. 2.c): the requesting intervals fall within *"universally"* fixed interval (Γ_{P3}) and the issued pseudonyms are aligned with global system time (PCA clock); thus, at any point in time all vehicles in a given domain will be transmitting under pseudonyms which are indistinguishable based on timing information alone. This results in eliminating any distinction among pseudonym sets, i.e., an anonymity set equal to the number of active requests. Hence, not only an external observer, but also the PCA could not distinguish among pseudonyms sets, thus, protecting user privacy. The same policy should be applied for the ticket acquisition, during which the H-LTCA fixes the timing interval to be the same for all requesters; thus preventing an LTCA from linking successive requests from a vehicle.

VI. PERFORMANCE EVALUATION

Without a large-scale deployment of VC systems, we resort to realistic large-scale mobility traces. Based on these, we determine the period the vehicles need pseudonyms. We extract two features of interest from the mobility traces, i.e., the departure time and the trip duration for each vehicle, and we apply policies described in Sec. IV-B to create the workload for the VPKI to assess the performance, i.e., scalability, efficiency, and robustness, of the full-blown implementation of our VPKI for a large-scale deployment. We evaluate performance with two mobility traces and we only plot the results for both traces and policies if they are significantly different than each other. The main functionality of interest are: ticket and pseudonym acquisition, CRL update, pseudonyms validation with OCSP, and pseudonym resolution. The main metric is the *end-to-end pseudonym acquisition latency*, i.e., the delay from the initialization of protocol 1 till the successful completion of protocol 2, measured at the vehicle.

A. Experimental Setup

1) VPKI Testbed and Detailed Implementation: We allocate Virtual Machines (VMs) for distinct VPKI servers. Table V details the specification of the distinct servers and the clients. Our full-blown implementation is in C++ and we use FastCGI [44] to interface Apache web-server. We use XML-RPC [45] to execute a remote procedure call on the servers. Our VPKI interface is language-neutral and platform-neutral as we use Protocol Buffers [46] for serializing and de-serializing structured data. For the cryptographic protocols and primitives (ECDSA and TLS), we use OpenSSL with ECDSA-256 public/private key pairs according to the standards [1], [5]; other algorithms and key sizes are compatible for our implementation. We run our experiments in a testbed

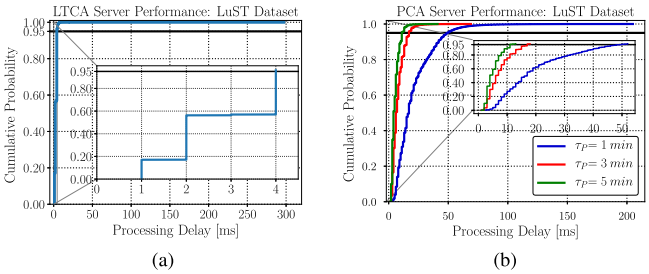


Fig. 3. CDF of server processing delay for P1, LuST dataset. (a) Issuing a ticket. (b) Issuing pseudonyms.

with both servers and clients (emulating OBUs) running on the VMs: this essentially eliminates the network propagation delays of the vehicle-VPKI connectivity. As such a connectivity would vary greatly based on the actual vehicle-VPKI connectivity, we do not consider it here.

2) Mobility Traces: We use two microscopic vehicle mobility datasets: Tapas-Cologne [47] and Luxembourg SUMO Traffic (LuST) [48]. The former one represents the traffic demand information across the Cologne urban area (available only for 2 hours, 6-8 AM), while the latter presents a full-day realistic mobility pattern in the city of Luxembourg. Table VI shows the mobility traces information for the two datasets.

3) Choice of Parameter: The choice of parameter for $\Gamma_{P2/P3}$ and τ_P mainly determines the frequency of interaction with the VPKI and the volume of workload imposed to the PCA: the shorter the pseudonym lifetimes are, the greater number of pseudonyms will be requested, thus a higher workload is imposed on the PCA. We evaluate the overall performance of the VPKI servers to issue pseudonyms with short lifetimes, e.g., 60 sec, to investigate the behavior of the servers under a high-workload condition.

B. VPKI Server Performance

1) Ticket and Pseudonym Provisioning: Fig. 3.a illustrates the CDF of a single ticket issuance processing delay for the Tapas dataset. For example, $F_x(t = 4\ ms) = 0.95$, or $Pr\{t \leq 4\ ms\} = 0.95$. Fig. 3.b shows the processing delay for issuing pseudonyms with different lifetimes for Tapas dataset. As illustrated, with $\tau_P = 1$ min, around 95% of requesters are served less than 52 ms: $F_x(t = 52\,ms) = 0.95$, i.e., $Pr\{t \leq 52\,ms\} = 0.95$. The results confirm the efficiency and scalability of our system.

2) End-to-End Latency: We are primarily concerned with the *end-to-end latency*, i.e., the delay for pseudonym acquisition, measured at the vehicle, calculated from the initialization

TABLE VII

END-TO-END LATENCY STATISTICS ($\Gamma = 10$ Min, $\tau_P = 1$ Min)

	Tapas-P1	Tapas-P2	Tapas-P3	LuST-P1	LuST-P2	LuST-P3
Maximum (ms)	296	320	5,168	3,062	248	5,545
Minimum (ms)	19	26	18	18	26	18
Average (ms)	50.29	45.56	42.76	51.78	47.58	43.10
Std. Deviation	16.26	12.10	26.19	35.40	11.72	23.53
Variance	264.35	146.5	685.83	1253.22	137.25	553.84
Pr{t ≤ x (ms)} = 0.99	102	83	69	110	80	70

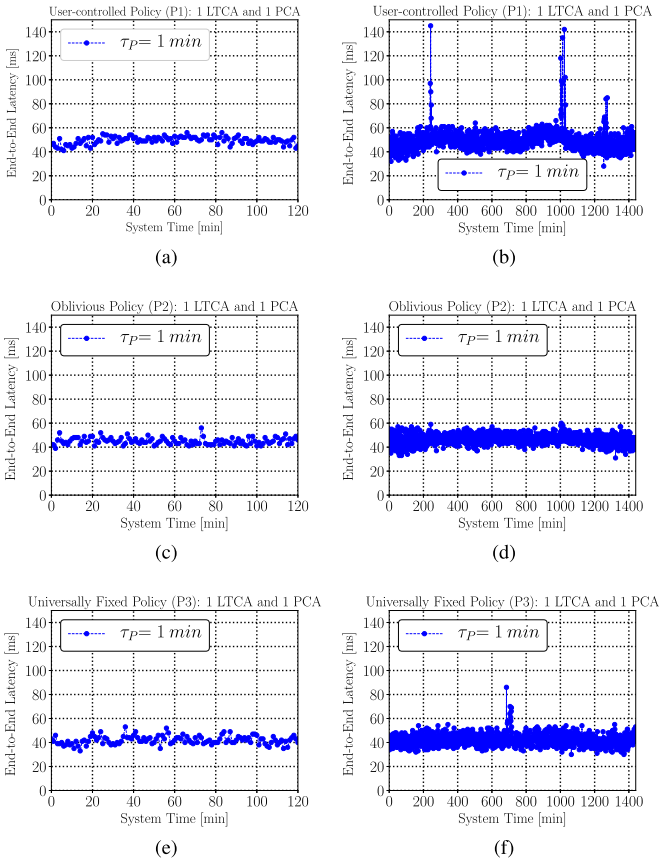


Fig. 4. Average end-to-end latency for different policies ($\Gamma = 10$ min, $\tau_P = 1$ min). The first row (a, b), the second row (c, d), and the third row (e, f) show the average end-to-end latency for user-controlled policy (P1), oblivious policy (P2), and universally fixed policy (P3), respectively. The first column represents the delays for Tapas dataset while the second one shows the delay for LuST dataset. (a) Tapas dataset. (b) LuST dataset. (c) Tapas dataset. (d) LuST dataset. (e) Tapas dataset. (f) LuST dataset.

of Protocol 1 till the successful completion of Protocol 2.[3] Table VII details the latency statistics to obtain pseudonyms with different policies for the two datasets. Figs. 4 show the average latency for the vehicles with different pseudonym acquisition policies. With P1 (Figs. 4.a and 4.b), each vehicle requests all required pseudonyms at once. With $\tau = 1$ min, 99% of the requesters for the Tapas and LuST datasets are served within less than 102 ms and 110 ms respectively. As we see, there are some sudden jumps in Fig. 4.b: the principal reason is that P1 allows vehicles to request pseudonyms for any trip duration; thus, long trip durations result in requesting more pseudonyms at once.

[3]The processing time to generate the key pairs is not considered here as the OBU can generate them off-line.

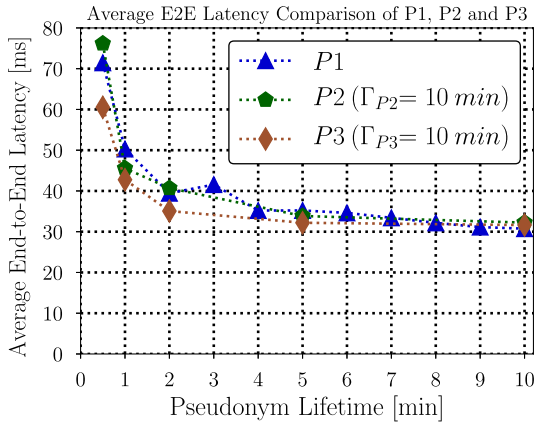


Fig. 5. End-to-end latency comparison for different policies (Tapas dataset).

With P2 (Figs. 4.c and 4.d), vehicles request a fixed amount of pseudonyms every time (for a duration of $\Gamma_{P2} = 10$ min), thus never overloading the PCA server with a large amount of pseudonyms in a single request; this results in low standard deviation and variance, and a smoother average delay in comparison to P1. The average end-to-end latency for Tapas and LuST datasets ($\tau_P = 1$ min) is 46 ms and 48 ms respectively; accordingly, 99% of vehicles are served within less than 83 ms and 80 ms respectively.

With P3 (Fig. 4.e and 4.f), the system enforces synchronized batch arrivals to obtain pseudonyms: each vehicle requests pseudonyms for the entire Γ_{P3}, timely aligned with the rest. 99% of the vehicles for the two datasets are served within less than 69 ms and 70 ms respectively. This confirms that the most promising policy in terms of privacy protection incurs even lower overhead in compare to other policies. All in all, our secure and privacy preserving scheme efficiently issues pseudonyms for the requesters and an OBU can initiate a request for pseudonyms within the lifetime of the last single valid pseudonym.

Fig. 5 and Table VIII show a comparison of the average end-to-end latency for different pseudonym acquisition policies. P3 incurs the lowest delay among the three policies: for example, the average end-to-end latency for P1, P2, and P3, with $\tau_P = 60$ sec is 50, 46, and 43 ms respectively. With P1, each vehicle requests all the required pseudonyms at once, which results in a higher workload on the PCA, thus higher latency. In other words, for P2 and P3, a request with large number of pseudonyms is split into multiple requests, each with fewer pseudonyms, thus achieving better performance due to the parallelization in multi-core processors.

Furthermore, the average end-to-end latency with P3 is lower than that with P2: the reason is that, with P3, each vehicle requests pseudonyms only for the *"current"* Γ_{P3}; this results in the acquisition of only non-expired pseudonyms for the residual trip duration; while, with P2, each vehicle requests pseudonyms for an entire Γ_{P2}, out of which all pseudonyms are actually obtained. This is why the average end-to-end latency with P3 is lower than that with P2 (assuming $\Gamma_{P2} = \Gamma_{P3}$).

TABLE VIII
LATENCY STATISTICS FOR DIFFERENT POLICIES, TAPAS DATASET ($\Gamma = 10$ Min)

Policy	P1			P2			P3		
Metrics	**Avg. E2E latency (ms)**	**Avg. no. of psnyms**	**Total no. of psnyms**	**Avg. E2E latency (ms)**	**Avg. no. of psnyms**	**Total no. of psnyms**	**Avg. E2E latency (ms)**	**Avg. no. of psnyms**	**Total no. of psnyms**
τ_P**=30 (sec)**	75.65	20.17	1,524,227	74.17	20	2,226,560	60.51	14.63	2,196,277
τ_P**=60 (sec)**	50.29	10.33	781,060	45.56	10	1,113,280	42.76	7.47	995,291
τ_P**=120 (sec)**	44.26	5.42	409,355	40.70	5	556,640	35.07	3.85	578,099
τ_P**=180 (sec)**	41.56	3.77	285,359	——	——	——	——	——	——
τ_P**=240 (sec)**	35.20	2.96	223,578	——	——	——	——	——	——
τ_P**=300 (sec)**	35.21	2.46	186,116	33.86	2	222,656	32.19	1.70	255,384
τ_P**=360 (sec)**	34.62	2.13	161,211	——	——	——	——	——	——
τ_P**=420 (sec)**	33.40	1.90	143,498	——	——	——	——	——	——
τ_P**=480 (sec)**	32.17	1.72	125,074	——	——	——	——	——	——
τ_P**=540 (sec)**	31.74	1.58	119,481	——	——	——	——	——	——
τ_P**=600 (sec)**	31.63	1.47	111,237	32.23	1	111,328	31.63	1	150,071

TABLE IX
END-TO-END LATENCY STATISTICS
WITH P3 ($\Gamma_{P3} = 1$ Min, $\tau_P = 1$ Min)

	Maximum (ms)	Minimum (ms)	Average (ms)	Std. Deviation	Variance	$Pr\{t \leq x\,(ms)\} = 0.99$
Tapas	6,462	17	34.72	24.69	609.39	86
LuST	5,043	19	34.72	21.52	462.92	54

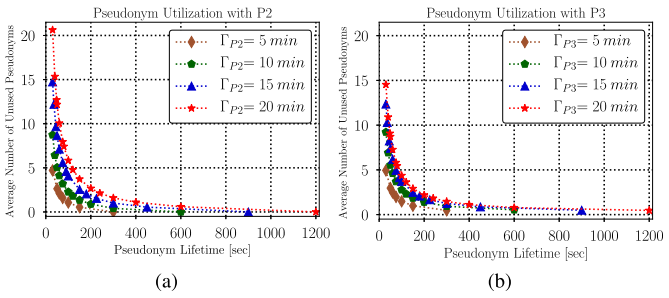


Fig. 6. Pseudonym utilization, LuST dataset for P2 and P3. (a) P2. (b) P3

3) Fully-Unlinkable Pseudonym Provisioning: Table IX details the latency statistics to obtain pseudonyms with P3 ($\Gamma_{P3} = \tau_P = 1$ min). The cumulative probability of end-to-end latency for Tapas and LuST datasets is: $Pr\{t \leq 86\,ms\} = 0.99$, and $Pr\{t \leq 54\ ms\} = 0.99$ respectively. With this probability, one can be fairly assured that even under this seemingly extreme configuration, the system is workable, i.e., the servers can issue fully unlinkable pseudonyms for the requesters. Nonetheless, there are rare events where the latency jumps; this indicates that either we need to enhance servers processing power, or trade it off by requesting small sets of linkable pseudonyms.

4) Optimal Pseudonym Utilization: Using P1, each vehicle interacts with the VPKI servers once to obtain the necessary pseudonyms for the entire trip duration (ideally without over-provisioning). However, according to P2 and P3, vehicles could be potentially equipped with more pseudonyms than necessary, i.e., the PCA might issue pseudonyms that the vehicle will not use them. Fig. 6 shows the average number of unused pseudonyms for LuST datasets with P2 and P3. In general, the longer the pseudonym refill interval Γ, i.e., $\Gamma_{P2/P3}$, and the shorter pseudonym lifetime (τ_P) are, the less frequent the vehicle-VPKI interactions but the higher the chance to overprovision a vehicle. In other words, the longer the Γ intervals and the τ_P are, the less the average number of unused pseudonyms is, thus the higher pseudonym utilization. For example, the average number of unused pseudonyms with P2 and P3, when Γ is 5 min and τ_P is 30 sec, is 4.7 and 4.9 respectively; this implies that under these configurations, each vehicle on average is issued approximately 5 unused pseudonyms. The flip side is that this would allow the PCA to have each set of pseudonyms (as a result of each request) trivially linked.

5) DDoS Attack: Internal adversaries could mount a clogging DoS attack. A rate limiting mechanism prevents internal adversaries from affecting the system performance; moreover, the system flags the legitimate but misbehaving users, thus evicting them from the system. External adversaries could launch a DDoS attack by clogging the LTCA with faked certificates, or the PCA with bogus tickets.

To gauge the availability of the system, we evaluate the average system latency to issue pseudonyms under a DDoS attack. We performed the experiments for different policies with various pseudonym lifetimes for the two datasets; we realized that the choice of policy, pseudonym lifetime, or dataset do not have a direct effect on the results; thus, we show the results for the LuST dataset, as it represents a full-day scenario, with P1 and $\tau = 5$ min. We increase the rate of adversarial requests up to 1,000 req/sec. As illustrated in Fig. 7, the average latency rapidly increases when the faked requests reach 1,000 req/sec. We use the guided tour puzzle [49] with difficulty level (L) 5 as a DDoS mitigation technique to prevent the external adversaries from overflowing the servers with spurious requests. Using this mechanism, the power of an attacker is degraded to the power of a legitimate client; thus, an attacker cannot send high-rate spurious requests to the servers. Therefore, the attack is mitigated while the overhead to obtain pseudonyms for the legitimate vehicles increases only by approximately 50 ms.

C. Revocation Update

Fig. 8 shows the CDF of latencies for obtaining a CRL and the average latency to perform OCSP validation for the LuST dataset. With a modest VM dedicated for the PCA server,

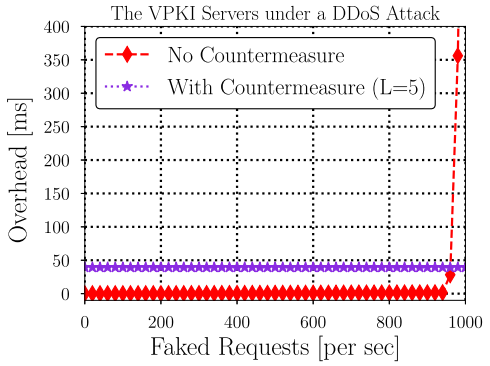
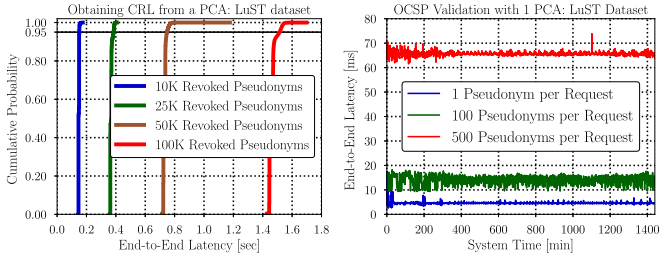
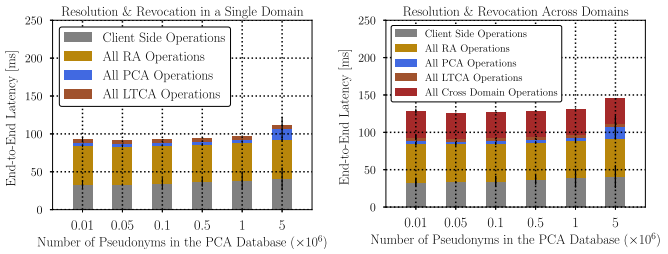


Fig. 7. The VPKI servers are under a DDoS attack: overhead to obtain pseudonyms for LuST dataset with P1 (difficulty level: L=5, $\tau_P = 5$ min).



(a) (b)

Fig. 8. End-to-end latency for revocation update (LuST dataset). (a) CRL acquisition. (b) OCSP validation.



(a) (b)

Fig. 9. End-to-end latency to resolve and revoke a pseudonym. (a) Single domain. (b) Across domains.

the results confirm the scalability of our system: 95% of the requesters to fetch a CRL with 100,000 revoked pseudonym are served within less than 1,500 ms, and the latencies for OCSP validation with 500 pseudonyms never exceeds 75 ms.

D. Pseudonym Revocation and Resolution

Fig. 9 shows the latency for each system component to resolve and revoke a pseudonym within a single domain (Fig. 9.a) and across domains (Fig. 9.b). We evaluate resolution with different number of pseudonyms in the PCA database (from 10,000 to 5,000,000 pseudonyms). Unlike another scheme [22] in which the performance is affected by increasing the number of revoked pseudonyms, our implementation is not. Our scheme outperforms other schemes, e.g., resolving and revoking a pseudonym in [23] takes more than 2 sec while with the same system configuration, it takes approximately 100 ms in our implementation.

TABLE X

LATENCY FOR ISSUING 100 PSEUDONYMS (WITHOUT COMMUNICATION DELAY)

	$Delay_{pca}$	CPU_{pca}
VeSPA [21]	817 ms	3.4 GHz (dual-core)
SEROSA [23]	650 ms	2.0 GHz (dual-core)
PUCA [25]	1,000 ms	2.53 GHz (dual-core)
PRESERVE PKI (Fraunhofer SIT) [10]	≈ 4,000 ms	N/A
C2C-CC PKI (ESCRYPT) [6]	393 ms	N/A
SECMACE	260 ms	2.0 GHz (dual-core)

E. Comparison With Other Implementations

There are a few schemes with performance evaluation of their implementations. A direct comparison among these schemes based on the available information is not straightforward. However, to highlight the essential need to the experimental validation and to ensure the viability as the system scales up, Table X demonstrates the latency for issuing 100 pseudonyms in different schemes.[4] The results confirm a significant performance improvement of our scheme over prior works: a 3-fold improvement over VeSPA [21], a 2.5-fold improvement over SEROSA [23] and a 4-fold improvement over PUCA [25].

VII. CONCLUSION

Paving the way for the deployment of a secure and privacy-preserving VC system has been started; standardization bodies and harmonization efforts have consensus towards deploying a special-purpose identity and credential management system. However, its success requires effective security and privacy-preserving protocols to guarantee the operations of the VC systems. To address the existing challenges, we proposed SECMACE, a novel VPKI that improves upon prior art in terms of security and privacy protection, and efficiency, and it provides solid evidence through a detailed implementation; we proposed three pseudonym acquisition policies, one of which protects user privacy to a greater extent while the timing information cannot harm user privacy. We further provide a full-blown implementation of our system and we evaluated our scheme with real mobility traces to confirm its efficiency, scalability, and robustness. Through extensive experimental evaluation, we demonstrated that modest VMs dedicated for the servers can serve on-demand requests with very low delay, and the most promising policy in terms of privacy protection incurs moderate overhead. This supports that the deployment of VPKI facilities can be cost-effective.

ACKNOWLEDGMENT

The authors would like to express their gratitude to Sebastian Mauthofer (Fraunhofer SIT) and Daniel Estor (Escrypt) for providing the processing delays of their systems. The authors would like to thank Assoc. Prof. Tomas Olovsson (Chalmers University of Technology) for his helpful comments on an earlier version of the manuscript.

[4]We emphasize that the results of the PRESERVE PKI are for VMs with shared resources. Thus, the latency should not be directly compared to that for other systems. We include it here only for completeness.

REFERENCES

[1] "Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions," Eur. Telecommun. Standards Inst., Sophia Antipolis, France, Tech. Rep. TR-102-638, Jun. 2009.

[2] 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," *IEEE Commun. Mag.*, vol. 47, no. 11, pp. 84–95, Nov. 2009.

[3] H. Jin, M. Khodaei, and P. Papadimitratos, "Security and privacy in vehicular social networks," in *Vehicular Social Networks*. New York, NY, USA: Taylor & Francis, 2016.

[4] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, "Securing vehicular communications—Assumptions, requirements, and principles," in *Proc. ESCAR*, Berlin, Germany, Nov. 2006, pp. 5–14.

[5] *IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*, IEEE Standards 1609.2-2016, Mar. 2016.

[6] *Car-to-Car Communication Consortium (C2C-CC)*, accessed on May 9, 2016. [Online]. Available: http://www.car-2-car.org/

[7] P. Papadimitratos *et al.*, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[8] T. Leinmüller *et al.*, "SEVECOM-secure vehicle communication," in *Proc. IST Mobile Summit*, Myconos, Greece, Jun. 2006.

[9] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications," in *Proc. IEEE VNC*, Boston, MA, USA, Dec. 2013, pp. 1–8.

[10] *Preparing Secure Vehicle-to-X Communication Systems—PRESERVE*, accessed on May 9, 2016. [Online]. Available: http://www.preserve-project.eu/

[11] J. R. Douceur, "The sybil attack," in *Proc. ACM 1st Int. Workshop Peer-to-Peer Syst.*, London, U.K., Mar. 2002, pp. 251–260.

[12] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications," in *Proc. IEEE ITST*, Sophia Antipolis, France, Jun. 2007, pp. 1–6.

[13] M. Khodaei, H. Jin, and P. Papadimitratos, "Towards deploying a scalable & robust vehicular identity and credential management infrastructure," in *Proc. IEEE VNC*, Paderborn, Germany, Dec. 2014, pp. 33–40.

[14] M. Khodaei and P. Papadimitratos, "Evaluating on-demand pseudonym acquisition policies in vehicular communication systems," in *Proc. 1st Int. Workshop Internet Veh. Veh. Internet*, Paderborn, Germany, Jul. 2016, pp. 7–12.

[15] L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, "Secure revocable anonymous authenticated inter-vehicle communication (SRAAC)," in *Proc. ESCAR*, Berlin, Germany, Nov. 2006, pp. 1–9.

[16] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, "Adaptive privacy-preserving authentication in vehicular networks," in *Proc. IEEE ChinaCom*, Beijing, China, Oct. 2006, pp. 1–8.

[17] F. Kargl *et al.*, "Secure vehicular communication systems: Implementation, performance, and research challenges," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 110–118, Nov. 2008.

[18] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. IEEE SECON*, Rome, Italy, Jun. 2009, pp. 1–9.

[19] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in VANETs," in *Proc. IEEE WCNC*, Sydney, NSW, Australia, Apr. 2010, pp. 1–6.

[20] M. Khodaei, "Secure vehicular communication systems: Design and implementation of a vehicular PKI (VPKI)," M.S. thesis, Royal Inst. Technol., Stockholm, Sweden, Oct. 2012.

[21] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, "VeSPA: Vehicular security and privacy-preserving architecture," in *Proc. ACM HotWiSec*, Budapest, Hungary, Apr. 2013, pp. 19–24.

[22] N. Bißmeyer, J. Petit, and K. M. Bayarou, "CoPRA: Conditional pseudonym resolution algorithm in VANETs," in *Prcc. IEEE WONS*, Banff, Canada, Mar. 2013, pp. 9–16.

[23] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, "SEROSA: SERvice oriented security architecture for vehicular communications," in *Proc. IEEE VNC*, Boston, MA, USA, Dec. 2013, pp. 111–118.

[24] (Jul. 2016). *Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System*. [Online]. Available: https://www.regulations.gov/document?D=NHTSA-2015-0060-0004

[25] D. Förster, H. Löhr, and F. Kargl, "PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET)," in *Proc. IEEE VNC*, Paderborn, Germany, Dec. 2014, pp. 25–32.

[26] X. Sun, X. Lin, and P.-H. Ho, "Secure vehicular communications based on group signature and ID-based signature scheme," in *Proc. IEEE ICC*, Glasgow, U.K., Jun. 2007, pp. 1539–1545.

[27] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Netw. Veh. Environ.*, May 2007, pp. 103–108.

[28] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[29] A. Wasef, Y. Jiang, and X. Shen, "ECMV: Efficient certificate management scheme for vehicular networks," in *Proc. IEEE GLOBECOM*, New Orleans, LO, USA, Dec. 2008, pp. 1–5.

[30] A. Wasef and X. Shen, "PPGCV: Privacy preserving group communications protocol for vehicular ad hoc networks," in *Proc. IEEE ICC*, Beijing, China, May 2008, pp. 1458–1463.

[31] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 1903–1911.

[32] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "On the performance of secure vehicular communication systems," *IEEE Trans. Depend. Sec. Comput.*, vol. 8, no. 6, pp. 898–912, Nov./Dec. 2011.

[33] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 8, pp. 1557–1568, Oct. 2007.

[34] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, Washington, DC, USA, Oct. 2004, pp. 168–177.

[35] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Proc. 24th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, Aug. 2004, pp. 41–55.

[36] P. Papadimitratos, G. Calandriello, A. Lioy, and J.-P. Hubaux, "Impact of vehicular communications security on transportation safety," in *Proc. IEEE INFOCOM MOVE*, Phoenix, AZ, USA, Apr. 2008, pp. 1–6.

[37] H. Jin and P. Papadimitratos, "Resilient privacy protection for location-based services through decentralization," in *Proc. ACM WiSec*, Boston, MA, USA, Jul. 2017, pp. 1–6.

[38] P. Papadimitratos, "'On the road'—Reflections on the security of vehicular communication systems," in *Proc. IEEE ICVES*, Columbus, OH, USA, pp. 359–363, Sep. 2008.

[39] M. Khodaei and P. Papadimitratos, "The key to intelligent transportation: Identity and credential management in vehicular communication systems," *IEEE Veh. Technol. Mag.*, vol. 10, no. 4, pp. 63–69, Dec. 2015.

[40] J. Sermersheim, "Lightweight directory access protocol (LDAP): The protocol," Tech. Rep., Jun. 2006.

[41] T. Dierks, "The transport layer security (TLS) protocol version 1.2," Tech. Rep., Aug. 2008.

[42] D. Solo, R. Housley, and W. Ford, "Internet X. 509 public key infrastructure certificate and certificate revocation list (CRL) profile," Tech. Rep., Apr. 2002.

[43] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams, "X. 509 Internet public key infrastructure online certificate status protocol—OCSP," Tech. Rep., Jun. 2013.

[44] P. Heinlein, "FastCGI: Persistent applications for your Web server," *Linux J.*, vol. 1998, no. 55es, p. 1, Nov. 1998. [Online]. Available: http://www.linuxjournal.com/article/2607

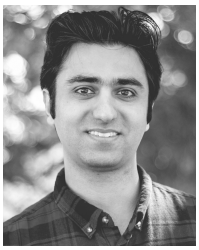
[45] *XML-RPC for C and C++*, accessed on May 9, 2016. [Online]. Available: http://xmlrpc-c.sourceforge.net/

[46] *Google Protocol Buffer*, accessed on May 9, 2016. [Online]. Available: https://developers.google.com/protocol-buffers/

[47] S. Uppoor, O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, "Generation and analysis of a large-scale urban vehicular mobility dataset," *IEEE Trans. Mobile Comput.*, vol. 13, no. 5, pp. 1061–1075, May 2014.

[48] L. Codeca, R. Frank, and T. Engel, "Luxembourg SUMO traffic (LuST) Scenario: 24 Hours of mobility for vehicular networking research," in *Proc. IEEE VNC*, Kyoto, Japan, Dec. 2015, pp. 1–8.

[49] M. Abliz and T. Znati, "A guided tour puzzle for denial of service prevention," in *Proc. IEEE Comput. Secur. Appl. Conf. (ACSAC)*, Honolulu, HI, USA, Dec. 2009, pp. 279–288.



Mohammad Khodaei received the Diploma degree in software engineering from Azad University of Najafabad, Isfahan, Iran, in 2006 and the M.S. degree in information and communication systems security from KTH Royal Institute of Technology, Stockholm, Sweden, in 2012, where he is currently working toward the Ph.D. degree with the Networked Systems Security Group, under the supervision of Prof. P. Papadimitratos. His research interests include security and privacy in vehicular ad hoc networks, smart cities, and Internet of Things.

Hongyu Jin is working toward the Ph.D. degree with the Networked Systems Security Group, KTH Royal Institute of Technology, supervised by Prof. P. Papadimitratos. His research interests are in security and privacy in vehicular communication systems and location-based services.

Panagiotis (Panos) Papadimitratos received the Ph.D. degree from Cornell University, Ithaca, NY, USA, in 2005. He then held positions at Virginia Tech, École Polytechnique Fédérale de Lausanne, and Politecnico di Torino. He is currently a tenured Professor with KTH Royal Institute of Technology, Stockholm, Sweden, where he leads the Networked Systems Security Group. His research agenda includes a gamut of security and privacy problems, with an emphasis on wireless networks. He is a member of the Young Academy of Europe. At KTH, he is affiliated with the ACCESS Center, leading its Security, Privacy, and Trust Thematic Area, as well as the ICES Center, leading its Industrial Competence Group on Security. He is a Knut and Alice Wallenberg Academy Fellow and he received the Swedish Science Foundation Young Researcher Award. He has delivered numerous invited talks, keynotes, and panel addresses, as well as tutorials in flagship conferences. He currently serves as an Associate Editor of IEEE TRANSACTIONS ON MOBILE COMPUTING, *ACM Transactions on Networking*, and IEEE TRANSACTIONS ON NETWORKING. He has served in numerous program committees, with leading roles in numerous occasions, and in 2016 he was the Program Co-Chair of the ACM WiSec and the TRUST conferences, and he serves as the General Chair of the ACM WISec (2018) and PETS (2019) conferences.