We present SECMACE, a VPKI system, which is compatible with moderate overhead.

VPKI interactions, based on which and two large-scale mobility trace datasets, we evaluate the full-blown implementation of SECMACE. With very little attention on the VPKI performance, we provide a detailed description of our state-of-the-art VPKI that have reached a consensus to use Public Key Cryptography (PKC) to protect the V2V and V2I communications: 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 and subsequent projects, e.g., Crash Avoidance Metrics Partnership Vehicle Safety Consortium (CAMP VSC) and Preparing Secure Vehicle-to-X Communication Systems (PRESERVE), as well as technical standards, notably the IEEE 1609.2 WG, ETSI, and harmonization documents.

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, $k_v$, that corresponds to a currently valid pseudonym, $P_v$. 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 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 honest-but-curious (PKC) to protect the V2V and V2I communications: 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 and subsequent projects, e.g., Crash Avoidance Metrics Partnership Vehicle Safety Consortium (CAMP VSC) and Preparing Secure Vehicle-to-X Communication Systems (PRESERVE), as well as technical standards, notably the IEEE 1609.2 WG, ETSI, and harmonization documents.

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, $k_v$, that corresponds to a currently valid pseudonym, $P_v$. 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 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 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 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, and requests could act as user ‘fingerprints’. 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, 23], 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: 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, 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, 19, 20, 21, 22, 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-
TABLE I
VPKI Security Features and Properties Comparison (✓: support, ×: no support)

| Schemes | Properties | IEEE 1609.2 compliance | ETSI compliance | Long-term identifier | Multiple domains | SBID resilience | Cryptosystem | Cryptographic algorithms | Revocation | Accountability | Perfect forward secrecy | Rolling strategy | V:VPKI communication |
|---------|------------|------------------------|-----------------|----------------------|-----------------|----------------|--------------|-------------------------|------------|----------------|------------------------|-----------------|--------------------|
| Fischer et al. (SRAC) [15] | ✓ | ✓ | Certificate | ✓ | PKC | Magic-out signatures | ✓ | ✓ | On-demand | Blind signature without confidentiality | SYMREF key authentication (asymmetric key) | SECURITY VPKI S |
| Sha et al. [16] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| SeVCom [17] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| CnX: CnX pilot PKI [18] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Studer et al. (TACK) [19] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Schaub et al. (V-tokens) [20] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Dienstle et al. (VTPA) [21] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Biizerza et al. (UCPMS) [22] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Grimaldi et al. (SEROVA) [23] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| White et al. (GAMBIT) [24] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Forster et al. (PUCAS) [25] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Khoshaba et al. (SRAC) [26] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Sun et al. [27] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Guo et al. [28] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Liu et al. (GAMBIT) [29] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Zhao et al. (ECMS) [30] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Zhao et al. (ECMS) [31] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Lu et al. (ECPY) [32] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |
| Calandriello et al. [33] | ✓ | ✓ | Certificate | ✓ | PKC | GraphGID signature | ✓ | ✓ | On-demand | Secure, wireline communication | DL/ECIES over UDP | SECURITY VPKI S |

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, 25].

This naturally leads us to the protocol of a hybrid approach [18, 32, 35]. 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 assumes 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.

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) 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. 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 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 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. 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 (revo cation): 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. 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) 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.

The H-LTCA authenticates and authorizes vehicles, which authenticate the H-LTCA over a mutually authenticated Transport Layer Security (TLS) tunnel. This way the vehicle obtains a native ticket (\(n\)-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 (\(f\)-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 (\(n\)-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 \(f\)-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) and perform Online Certificate Status Protocol (OCSP) operations, authenticated with a current valid pseudonym.

#### 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].

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 requestor. 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.

Oblivious Policy (P2): The vehicle interacts with the VPKI every $\Gamma_{P2}$ seconds (determined by the PCA and fixed for all users) and it requests pseudonyms for the entire $\Gamma_{P2}$ 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.

Universally Fixed Policy (P3): The H-LTCA, as the policy decision point in its domain, has predetermined universally fixed interval, $\Gamma_{P3}$, and pseudonym lifetime, $\tau_{P3}$. At the start of the trip, its vehicle requests pseudonyms for the "current" $\Gamma_{P3}$, out of which useful (non-expired) ones are actually obtained for the residual trip duration within $\Gamma_{P3}$. For the remainder of the trip, the vehicle requests pseudonyms for the entire $\Gamma_{P3}$ 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 $\Gamma_{P3}$ seconds to obtain pseudonyms. A strict limitation in using this policy is that partial pseudonym acquisition in $\Gamma_{P3}$ is not allowed, i.e., the vehicle must request pseudonyms for the entire $\Gamma_{P3}$.

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].

Ticket Acquisition (Protocol I): 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]), i.e., step 1 in Protocol I. While with P2, each vehicle requests pseudonyms for $[t_s, t_e+\Gamma_{P2}]$ (step [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 $\Gamma_{P3}$ of that specific PCA (step [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., $H(ID_{PCA}||Rnda_{n-tkt})$ (step [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 $f-tkt$ and it concatenates its targeted F-LTCA (instead of the desired PCA) and a random number. The vehicle then signs the request (step [5]) and sends it to its H-LTCA to obtain an $n-tkt$ (step [6]). Upon a successful validation of the LTC and verification of the request (step [7]), the H-LTCA generates the "ticket identifiable key" ($IK_{n-tkt}$) to bind the ticket to the LTC: $H(LTC_{n}||t_{s}||t_{e}||Rnda_{n-tkt})$ (step [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, $(n-tkt)_{\sigma_{n-tkt}}$ (step [9]). 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
Pseudonym Resolution and Revocation (Protocol 3):

\[
\begin{align*}
\text{RA} & : \zeta \leftarrow (Id_{req}, P^i) \quad (1) \\
\text{RA} & \rightarrow \text{PCA} : (\zeta)_{\sigma_{PCA}} \leftarrow \text{Sign}(Lk_{PCA}, \zeta) \quad (2) \\
\text{RA} & \rightarrow \text{PCA} : ((\zeta)_{\sigma_{PCA}}, Lk_{PCA}, N, t_{now}) \quad (3) \\
\text{PCA} & : \text{Verify}(LTC_{PCA}, (\zeta)_{\sigma_{PCA}}) \quad (4) \\
\text{PCA} & : \{n-tkt, Rnd_{IK_{P^i}}\} \leftarrow \text{Resolve}(P^i) \quad (5) \\
\text{PCA} & : \{Id_{req} \equiv \text{"revoke"}, \text{Add}(P^i, \text{CRL})\} \quad (6) \\
\text{PCA} & : \chi \leftarrow (Id_{req}, n-tkt, Rnd_{IK_{P^i}}) \quad (7) \\
\text{PCA} & : (\chi)_{\sigma_{PCA}} \leftarrow \text{Sign}(Lk_{PCA}, \chi) \quad (8) \\
\text{RA} & \rightarrow \text{PCA} : ((\chi)_{\sigma_{PCA}}, N+1, t_{now}) \quad (9) \\
\text{RA} & : \text{Verify}(LTC_{PCA}, \chi) \quad (10) \\
\text{RA} & : \{H(1K_{n-tkt}||K^i_v||t^i_e||Rnd_{IK_{P^i}}) \equiv 1K_{P^i}\} \quad (11) \\
\text{RA} & : \text{Resolve}(LT(n-tkt)) \quad (12)
\end{align*}
\]

LTC Resolution and Revocation (Protocol 4):

\[
\begin{align*}
\text{RA} & : \zeta \leftarrow (Id_{req}, n/f-tkt, N, t_{now}) \quad (13) \\
\text{RA} & : (\zeta)_{\sigma_{RA}} \leftarrow \text{Sign}(Lk_{RA}, \zeta) \quad (14) \\
\text{RA} & \rightarrow \text{H-LTCA} : ((\zeta)_{\sigma_{RA}}, LTC_{req}) \quad (15) \\
\text{H-LTCA} & : \text{Verify}(LTC_{req}, (\zeta)_{\sigma_{RA}}) \quad (16) \\
\text{H-LTCA} & : \{LTC_{req}, Rnd_{IK_{n-tkt}}\} \leftarrow \text{Resolve}(n/f-tkt) \quad (17) \\
\text{H-LTCA} & : \{Id_{req} \equiv \text{"revoke"}, \text{Add}(LTC_{req}, \text{CRL})\} \quad (18) \\
\text{H-LTCA} & : \chi \leftarrow (Id_{req}, LTC_{req}, Rnd_{IK_{n-tkt}}, N+1, t_{now}) \quad (19) \\
\text{H-LTCA} & : (\chi)_{\sigma_{ltca}} \leftarrow \text{Sign}(Lk_{hLTCA}, \chi) \quad (20) \\
\text{RA} & \rightarrow \text{H-LTCA} : (\chi)_{\sigma_{ltca}} \quad (21) \\
\text{RA} & : \text{Verify}(LTC_{hLTCA}, \chi) \quad (22) \\
\text{RA} & : \{H(LTC_{req}||t_{req}||Rnd_{IK_{n-tkt}}) \equiv 1K_{n/f-tkt}\} \quad (23)
\end{align*}
\]

Pseudonym Acquisition (Protocol 2): With an n-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., \(t_{req}^u, t_{req}^d\)) falls within the period specified in the ticket (i.e., \(t_{req}^u, t_{req}^d\)): \(t_{req}^u, t_{req}^d \subseteq (t_{req}^u, t_{req}^d)_{n-tkt}\) for P1 or P2, or \(t_{req}^u, t_{req}^d = (t_{req}^u, t_{req}^d)_{n-tkt}\) 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, \(K^v_i\). The PCA generates the “pseudonym identifiable key” (IK\(_{P^i}\)) 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\(_{P^i}\) (steps 2.14-2.17).

Pseudonym Resolution and Revocation (Protocol 3): The 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 11). Finally, the vehicle verifies the ticket and IK\(_{P^i}\) (steps 12-13). In case of cross-domain operation, the vehicle interacts with the F-LTCA and presents the f-tkt to obtain an n-tkt in the foreign domain. Thus, it can interact with the PCAs within the foreign domain as a “local” vehicle.

As an optimization, the PCA can probabilistically verify \((K^v_i)_{\sigma_{PCA}}\).
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 $H(Id_{pca}||R_{id_{pca,tkt}})$, and the targeted 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 $\Gamma_{P3}$ (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. VI-B. Moreover, the separation of duties between the LTCA and the PCA provides conditional anonymity, but revolved 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 requestor 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-B5.

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 $\Gamma_{P3}$ is equal to $\tau_{P}$, 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-B5.

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

| Honest-but-curious (colluding) Entities | Information Leaked | Security and Privacy Implications |
|----------------------------------------|--------------------|----------------------------------|
| H-LTCA                                | $id_{pca}$, $t_{s}$, $t_{e}$ | An H-LTCA knows during when the registered vehicles wish to obtain pseudonyms. |
| H-LTCA, F-LTCA                         | $id_{pca}$, $id_{pca}$, $id_{pca}$ | Collision among LTCA from different domains does not reveal additional information. |
| PCA$_{H}$, PCA$_{F}$                   | $t_{s}$, $t_{e}$, $P_{H}$, $P_{F}$ | Collision among PCAs from different domains does not reveal additional information. |

| H-LTCA, F-LTCA, PCA$_{H}$, PCA$_{F}$ | $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$ | The pseudonyms they issued can be linked but the real identities of the vehicles cannot be derived. |
| H-LTCA, F-LTCA, PCA$_{H}$, PCA$_{F}$ | $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$ | The pseudonyms they issued can be linked but the real identities of the vehicles cannot be derived. |
| H-LTCA, F-LTCA, PCA$_{H}$, PCA$_{F}$ | $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$ | The pseudonyms they issued can be linked but the real identities of the vehicles if the PCA$_{H}$ is the issuer of the pseudonyms. |

| H-LTCA, F-LTCA, PCA$_{H}$, PCA$_{F}$ | $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$ | The pseudonyms they issued can be linked but the real identities of the vehicles if the PCA$_{H}$ and PCA$_{F}$ are the issuers of the pseudonyms. |

| H-LTCA, F-LTCA, PCA$_{H}$, PCA$_{F}$ | $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$ | The pseudonyms they issued can be linked but the real identities of the vehicles if the PCA$_{H}$ and PCA$_{F}$ are the issuers of the pseudonyms. |

| H-LTCA, F-LTCA, PCA$_{H}$, PCA$_{F}$ | $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$, $id_{pca}$ | The pseudonyms they issued can be linked but the real identities of the vehicles if the PCA$_{H}$ and PCA$_{F}$ are the issuers of the pseudonyms. |

### Table IV

| Notation Used in Security & Privacy Analysis |
|---------------------------------------------|
| $PCA_{H}$                                  | PCA$_{H}$, in the home domain         |
| $PCA_{F}$                                  | a set of PCAs in the home domain    |
| $PCA_{F}$                                  | a set of PCAs in the foreign domain |
| $id_{pca}$                                 | identities of the vehicles in the home domain |
| $id_{pca}$                                 | identities of the vehicles in the foreign domain |
| $P_{H}$                                    | pseudonyms issued by the PCAs in the home domain |

|PCAs in the home domain | PCAs in the foreign domain | identities of the vehicles in the home domain | identities of the vehicles in the foreign domain | pseudonyms issued by the PCAs in the home domain |...|
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_H/tkt, IK_F/tkt, or IK_P2, respectively.

B. Ticket and Pseudonym Lifetime Policies

Fig. 2 displays a transcript of eavesdropped pseudonyms for different pseudonym acquisition policies (Γ = 15 min, τP = 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. 2a and 2b), 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. 2a, 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. 2b, the second pseudonym in row 8 (colored in magenta) is the last pseudonym issued for the first iteration of ΓF, which expires at system time 15. The only pseudonym starting from 15 in the second iteration of ΓF is the second pseudonym in row 2 (with a repeated asterisk pattern colored in magenta).

This vulnerability is thwarted by P3 (Fig. 2c): the requesting intervals fall within “universally” fixed interval (ΓP3) 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

VPKI Testbed and Detailed Implementation: We allocate Virtual Machines (VMs) for distinct VPKI servers. Table I 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 deserializing 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 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.

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.

Choice of Parameter: The choice of parameter for $\Gamma_{p_2/p_3}$ and $\tau_p$ 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. 3a 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. 3b 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 of Protocol [1] till the successful completion of Protocol [2]. 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

3The processing time to generate the key pairs is not considered here as the OBU can generate them off-line.
acquisition policies. With P1 (Figs. 4a and 4b), each vehicle requests all required pseudonyms at once. With \( \tau =1 \text{ min} \), 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. 4b: 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.

With P2 (Figs. 4c and 4d), vehicles request a fixed amount of pseudonyms every time (for a duration of \( \tau_{P2}=10 \text{ min} \)), 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 (\( \tau_{P2}=1 \text{ min} \)) 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. 4e and 4f), the system enforces synchronized batch arrivals to obtain pseudonyms: each vehicle requests pseudonyms for the entire \( \tau_{P3} \), 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 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 \( \tau_{P}=60 \text{ sec} \) 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’’ \( \tau_{P3} \); 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 \( \tau_{P2} \), 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 \( \tau_{P2}=\tau_{P3} \)).

3) Fully-unlinkable Pseudonym Provisioning: Table IX details the latency statistics to obtain pseudonyms with P3 (\( \tau_{P3}=\tau_{P}=1 \text{ min} \)). The cumulative probability of end-to-end latency for Tapas and LuST datasets is: \( Pr\{t \leq 86\text{ms}\} = 0.99 \), and \( Pr\{t \leq 54\text{ms}\} = 0.99 \) 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.

| TABLE VIII |
|-------------|
| **LATENCY STATISTICS FOR DIFFERENT POLICIES, TAPAS DATASET (\( \Gamma =10 \text{ min} \))** |
| | **P1** | **P2** | **P3** |
| | **Metrics** | Avg. E2E latency (ms) | Avg. no. of pseudonyms | Total no. of pseudonyms | Avg. E2E latency (ms) | Avg. no. of pseudonyms | Total no. of pseudonyms | Avg. E2E latency (ms) | Avg. no. of pseudonyms | Total no. of pseudonyms |
| | \( \tau_{P}=30 \text{ (sec)} \) | 75.65 | 20.17 | 1,524,227 | 74.17 | 20 | 2,226,560 | 60.51 | 14.63 | 2,196,277 |
| | \( \tau_{P}=60 \text{ (sec)} \) | 50.20 | 10.33 | 781,060 | 45.56 | 10 | 1,113,280 | 42.76 | 7.47 | 995,291 |
| | \( \tau_{P}=120 \text{ (sec)} \) | 44.26 | 5.42 | 409,355 | 40.70 | 5 | 556,640 | 35.07 | 3.85 | 578,099 |
| | \( \tau_{P}=180 \text{ (sec)} \) | 41.56 | 3.77 | 285,359 | —— | —— | —— | —— | —— | —— |
| | \( \tau_{P}=240 \text{ (sec)} \) | 35.20 | 2.96 | 223,578 | —— | —— | —— | —— | —— | —— |
| | \( \tau_{P}=300 \text{ (sec)} \) | 35.21 | 2.46 | 186,116 | 33.86 | 2 | 222,656 | 32.19 | 1.70 | 255,384 |
| | \( \tau_{P}=360 \text{ (sec)} \) | 34.62 | 2.13 | 161,211 | —— | —— | —— | —— | —— | —— |
| | \( \tau_{P}=420 \text{ (sec)} \) | 33.40 | 1.90 | 143,498 | —— | —— | —— | —— | —— | —— |
| | \( \tau_{P}=480 \text{ (sec)} \) | 32.17 | 1.72 | 125,074 | —— | —— | —— | —— | —— | —— |
| | \( \tau_{P}=540 \text{ (sec)} \) | 31.74 | 1.58 | 119,481 | —— | —— | —— | —— | —— | —— |
| | \( \tau_{P}=600 \text{ (sec)} \) | 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 (\( \Gamma_{P3}=1 \text{ min} \), \( \tau_{P}=1 \text{ min} \))** |
| | Minimum ms | Maximum ms | Average ms | Std. Deviation | Variance | \( Pr\{t \leq x \text{ (ms)}\} \) |
| Tapas | End-to-end latency | Tapas | | End-to-end latency | Tapas | | |
| LuST | 74.17 | 155,071 | 75.65 | 1,524,227 | 74.17 | 2,226,560 | 75.65 | 2,196,277 | 0.99 |

Fig. 5. End-to-end latency comparison for different policies (Tapas dataset).
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 \( \Gamma \), i.e., \( \Gamma_{P2/P3} \), and the shorter pseudonym lifetime \( \tau_P \), the less frequent the vehicle-VPKI interactions but the higher the chance to over-provision a vehicle. In other words, the longer the \( \Gamma \) intervals and the \( \tau_P \) 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 \( \Gamma = 5 \text{ min} \) and \( \tau_P = 30 \text{ sec} \), 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 \( \tau = 5 \text{ min} \). 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, 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. 9a) and across domains (Fig. 9b). 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 demonstrates the latency for issuing 100 pseudonyms (without communication delay).

| Scheme                        | Delay (ms) | CPU (GHz) |
|-------------------------------|------------|-----------|
| VeSPA [21]                    | 817        | 3.4       |
| SEROSA [23]                   | 650        | 2.0       |
| PUCA [23]                     | 1,000      | 2.53      |
| PRESERVE PKI (Fraunhofer SIT) | ≈ 4,000    | N/A       |
| C2C-CC PKI (ESCRYPT) [5]      | 393        | N/A       |
| SECMACE                       | 260        | 2.0       |

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 [21-25]. 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 [23].

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.

REFERENCES

1. European Telecommunications Standards Institute, “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions,” ETSI Tech. TR-102-638, Jun. 2009.
2. 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, 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. Taylor & Francis Group, 2016.
4. P. Papadimitratos, V. Gligor, and J.-P. Hubaux, “Securing Vehicular Communications-Assumptions, Requirements, and Principles,” in ESCAR, Berlin, Germany, pp. 5–14, Nov. 2006.
5. “IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages.” IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013), Mar. 2016.
6. Car-to-Car Communication Consortium (C2C-CC), Accessed Date: 9-May-2016. [Online]. Available: http://www.car-2-car.org/
7. P. Papadimitratos, L. Buttyan, T. Holezer, E. Schoch, F. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure Vehicular Communication Systems: Design and Architecture,” IEEE Communications Magazine, vol. 46, no. 11, pp. 100–109, Nov. 2008.
8. T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, “SEVECOM-Secure Vehicle Communication,” in Proceedings of IST Mobile Summit, Myconos, Greece, June 2006.
9. W. Whyte, A. Weimerskirch, V. Kumar, and T. Hahn, “A Security Credential Management System for V2V Communications,” in IEEE VNC, Boston, MA, USA, pp. 1–8, Dec. 2013.
10. “Preparing Secure Vehicle-to-X Communication Systems - PRESERVE,” Accessed Date: 9-May-2016. [Online]. Available: http://www.preserve-project.eu/
11. J. R. Douceur, “The Sybil Attack,” in ACM Peer-to-peer Systems, London, UK, Mar. 2002.
12. 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, Jun. 2007.
13. M. Khodaei, H. Jin, and P. Papadimitratos, “Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,” in IEEE VNC, Paderborn, Germany, Dec. 2014.
14. M. Khodaei and P. Papadimitratos, “Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,” in Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet, Paderborn, Germany, pp. 7–12, July 2016.
15. L. Fischer, A. Aijaz, C. Eckert, and D. Vogt, “Secure Revocable Anonymous Authenticated Inter-vehicle Communication (SRAAC),” in ESCAR, Berlin, Germany, Nov. 2006.
16. K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang, “Adaptive Privacy-Preserving Authentication in Vehicular Networks,” in ChinaCom., Beijing, China, pp. 1–8, Oct. 2006.
17. F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiederheim, T.-V. Thong, G. Calandrieri, A. Held, and A. Kung, “Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges,” IEEE Communications Magazine, 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 IEEE SECON, Rome, Italy, pp. 1–9, Jun. 2009.
19. F. Schaub, F. Kargl, Z. Ma, and M. Weber, “V-tokens for Conditional Pseudonymity in VANETs,” in IEEE WCNC, Sydney, Australia, pp. 1–6, Apr. 2010.
20. M. Khodaei, “Secure Vehicular Communication Systems: Design and Implementation of a Vehicular PKI (VPKI),” Master’s thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, Oct. 2012.

We would like to show our gratitude to Sebastian Mauthofer (Fraunhofer SIT) and Daniel Estor (Escript) to provide us the processing delays of their systems. We would like to thank Assoc. Prof. Tomas Olofsson (Chalmers University of Technology) for his helpful comments on an earlier version of the manuscript.
[21] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, “VeSPA: Vehicular Security and Privacy-preserving Architecture,” in *ACM HotWise*, Budapest, Hungary, Apr. 2013.

[22] N. Billmeyer, J. Petri, and K. M. Bayarou, “CoPRA: Conditional Pseudonym Resolution Algorithm in VANETS,” in *IEEE WONS*, Banff, Canada, pp. 9–16, Mar. 2013.

[23] L. Codeca, O. Trullols-Cruces, and M. Fiore, “SecureVehicular: User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET),” in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[24] X. Lin, X. Sun, and P.-H. Ho, “Secure Vehicular Communications based on Group Signature and ID-based Signature Scheme,” in *IEEE ICC*, Glasgow, Scotland, Jun. 2007.

[25] J. Guo, J. P. Baugh, and S. Wang, “A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework,” *Mobile Networking for Vehicular Environments*, pp. 103–108, May 2007.

[26] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications,” *IEEE Transactions on Vehicular Technology*, Nov. 2007.

[27] A. Wasef, Y. Jiang, and X. S. Shen, “ECMV: Efficient Certificate Management Scheme for Vehicular Networks,” in *IEEE GLOBECOM*, New Orleans, LO, USA, Dec. 2008.

[28] A. Wasef and X. S. Shen, “PPGCV: Privacy Preserving Group Communications Protocol for Vehicular Ad Hoc Networks,” in *IEEE ICC*, Beijing, China, May 2008.

[29] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications,” in *IEEE INFOCOM*, Phoenix, AZ, USA, pp. 1903–1911, Apr. 2008.

[30] 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.

[31] 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*, pp. 1557–1568, Oct. 2007.

[32] D. Boneh and H. Shacham, “Group Signatures with Verifier-Local Revocation,” in *Proceedings of the 11th ACM conference on Computer and communications security*, Washington, DC, USA, Oct. 2004.

[33] D. Boneh, X. Boyen, and H. Shacham, “Short Group Signatures,” in *Proceedings of 24th Annual International Cryptology Conference*, Santa Barbara, California, USA, Aug. 2004.

[34] 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.

[35] H. Jin and P. Papadimitratos, “Resilient Privacy Protection for Location-Based Services Through Decentralization,” in *ACM WiSec*, Boston, MA, USA, July 2017.

[36] M. Khodaei and P. Papadimitratos, “The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,” *IEEE VTC Magazine*, vol. 10, no. 4, pp. 63–69, Dec. 2015.

[37] J. Sermersheim, “Lightweight Directory Access Protocol (LDAP): The Protocol,” Jun. 2006.

[38] T. Dierks, “The transport layer security (TLS) protocol version 1.2,” Aug. 2008.

[39] S. Antonsen, 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.

[40] P. Heinlein, “FastCGI,” *Linux Journal*, vol. 1998, no. 55es, p. 1, Nov. 1998.

[41] D. Boneh, “XML-RPC for C and C++,” Accessed Date: 9-May-2016. [Online]. Available: http://xmlrpc-c.sourceforge.net/

[42] C. 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.

[43] M. Khodaei, O. Trullols-Cruces, M. Fiore, and J. M. Barcelo-Ordinas, “Generation and Analysis of a Large-scale Urban Vehicular Mobility Dataset,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 5, pp. 1061–1075, May 2014.

[44] L. Codeca, O. Trullols-Cruces, and M. Fiore, “Luxembourg Sumo Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research,” in *IEEE VNC*, Kyoto, Japan, pp. 1–8, Dec. 2015.

[45] Mohammad Khodaei earned his diploma in software engineering from Azad University of Najafabad in Isfahan, Iran, in 2006 and his M.S. degree in information and communication systems security from KTH Royal Institute of Technology, Stockholm, Sweden, in 2012. He is currently pursuing his Ph.D. degree at the Networked Systems Security Group, KTH, under the supervision of Prof. Panos Papadimitratos. His research interests lie in security and privacy in vehicular ad hoc networks, smart cities, and the Internet of Things.

[46] Hongyu Jin is currently a Ph.D student at KTH Royal Institute of Technology in Networked Systems Security Group, supervised by Prof. Panos Papadimitratos. His research interests lie in security and privacy in Vehicular Communication systems and Location-based Services.

[47] Panagiotis (Panos) Papadimitratos earned his Ph.D. degree from Cornell University, Ithaca, NY, in 2005. He then held positions at Virginia Tech, Ecole Polytechnique Federale de Lausanne and Politecnico of Torino. Panos is currently a tenured Professor at KTH, Stockholm, Sweden, where he leads the Networked Systems Security group. His research agenda includes a gamut of security and privacy problems, with emphasis on wireless networks. 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. Panos is a Knut and Alice Wallenberg Academy Fellow and he received a Swedish Science Foundation Young Researcher Award. He has delivered numerous invited talks, keynotes, and panel addresses, as well as tutorials in flagship conferences. Panos currently serves as an Associate Editor of the IEEE Transactions on Mobile Computing and the ACM/IEEE Transactions on Networking. He has served in numerous program committees, with leading roles in numerous occasions; recently, in 2016, as the program co-chair for the ACM WiSec and the TRUST conferences; he serves as the general chair of the ACM WiSec (2018) and PETS (2019) conferences. Panos is a member of the Young Academy of Europe. His group webpage is: www.ee.kth.se/nss.