Several years of academic and industrial research efforts have converged to a common understanding on fundamental security building blocks for the upcoming Vehicle Communication (VC) systems. There is a growing consensus towards deploying a special-purpose identity and credential management infrastructure with standardization efforts towards that direction. The central building block of secure and privacy-preserving VC systems is a Vehicular Public-Key Infrastructure (VPKI), e.g., [1, 2, 3, 4], which provides vehicles with multiple anonymized credentials, termed pseudonyms. These pseudonyms are used to ensure message authenticity and integrity while preserving vehicle (thus passenger) privacy. Vehicles switch from one pseudonym to a non-previous used one towards message unlinkability, as pseudonyms are per se inherently unlinkable. Pseudonymity is conditional, in the sense that the corresponding long-term vehicle identity can be retrieved by the VPKI when needed, e.g., if vehicles deviating from system policies. In the light of emerging large-scale multi-domain VC environments [5], the efficiency of the VPKI and, more broadly, its scalability are paramount. By the same token, preventing misuse of the credentials, in particular, Sybil-based misbehavior, and managing “honest-but-curious” [5] insiders are other facets of a challenging problem.

Deploying a VPKI differs from a traditional PKI, e.g., [6, 7, 8]. One of the most important factors is the PKI dimension, i.e., the number of registered users (vehicles) and the multiplicity of certificates per user. According to the US Department of Transportation (DoT), a VPKI should be able to issue pseudonyms for more that 350 million vehicles across the Nation [9]. Considering the average daily commute time to be 1 hour [9] and a pseudonym lifetime of 5 minutes, the VPKI should be able to issue at least $1.5 \times 10^{12}$ pseudonyms per year, i.e., 5 orders of magnitude more than the number of credentials the largest current PKI issues (10M per year [1]).

In this poster, we leverage and enhance a state-of-the-art VPKI, and propose a VPKI as a Service (VPKIaaS) [10, 11] system towards a highly-available, dynamically-scalable, and fault-tolerant design, ensuring the system remains operational in the presence of benign failures or any resource depletion attack (clogging a Denial of Service (DoS) attack). Moreover, our scheme eradicates Sybil-based misbehavior when deploying such a system on the cloud with multiple replicas of a micro-service without diminishing the pseudonym acquisition efficiency. All procedures of deployment and migration to the cloud, e.g., bootstrapping phase, initializing the micro-services, pseudonym acquisition process, monitoring health and load metrics, etc., are fully automated. Through extensive experimental evaluation, we show that the VPKIaaS system could dynamically scale out, or possibly scale in\(^1\), based on the VPKIaaS system workload and the requests’ arrival rate, so that it can comfortably handle unexpected demanding loads while being cost-effective by systematically allocating and deallocating resources. Our experimental evaluation shows a 36-fold improvement over prior work [12]: the processing delay to issue 100 pseudonyms for [12] is 2010 ms, while it is approx. 56 ms in our system. Moreover, the performance of [4] drastically decreases when there is a surge in the pseudonym request arrival rates; on the contrary, our VPKIaaS system can comfortably handle demanding loads request while efficiently issuing batches of pseudonyms.

\section*{References}
\begin{itemize}
\end{itemize}

\(^1\)In cloud terminology, scaling in/out (horizontal scaling), refers to replicating a new instance of a service, while scaling up/down (vertical scaling), refers to allocating/deallocating resources for an instance of a given service.