VPKIaaS: Towards Scaling Pseudonymous Authentication for Large Mobile Systems

Hamid Noroozi, Mohammad Khodaei, and Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology, Sweden
www.ee.kth.se/nss

Vehicular Communication (VC) System

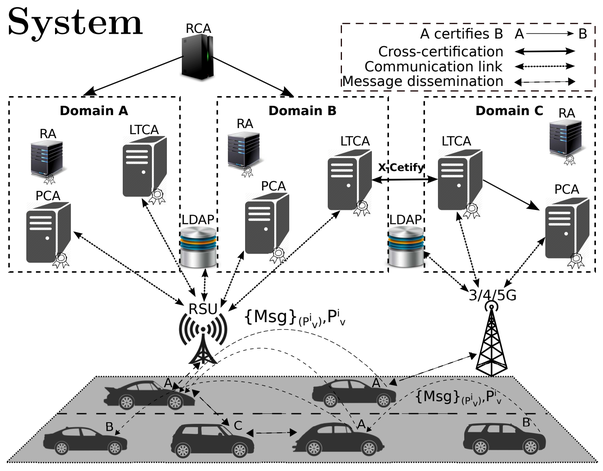


Figure 1: Vehicular Public-Key Infrastructure (VPKI) Architecture [4, 6, 8].

Identity and credential management challenges:

- Security and privacy protection, with emphasis on efficiency and scalability
- Multi-domain organization
- Cross-domain operations and service discovery
- Preventing linkability based on timing information
- ***"Honest-but-curious"*** VPKI entities

Security System Entities

- Vehicles registered with one **Long Term Certification Authority (LTCA)** (home domain)
- **Pseudonym Certification Authority (PCA)** servers in one or multiple domains
- Vehicles can obtain pseudonyms from any **PCA** (in home or foreign domains)
- Trust across domains with the help of a **Root CA (RCA)** or cross-certification

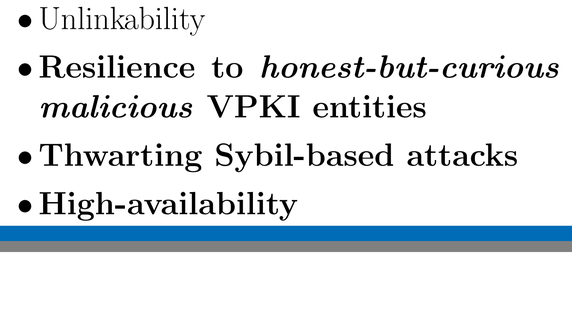


Figure 2: Hierarchical Organization of the VC Security Infrastructure [7].

Security & Privacy Requirements

- Authentication and communication integrity, and confidentiality
- Authorization and access control
- Non-repudiation, accountability and eviction
- Anonymity (conditional)
- Unlinkability
- **Resilience to *honest-but-curious* and *malicious* VPKI entities**
- **Thwarting Sybil-based attacks**
- **High-availability**

SECMACE Overview

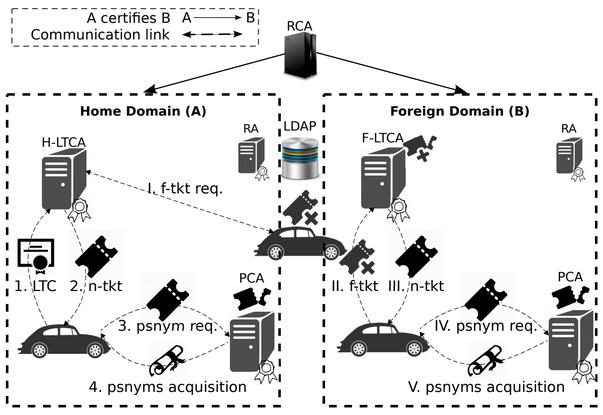


Figure 3: Pseudonym Acquisition Overview in Home and Foreign Domains [4, 8].

VPKI as a Service (VPKIaaS)

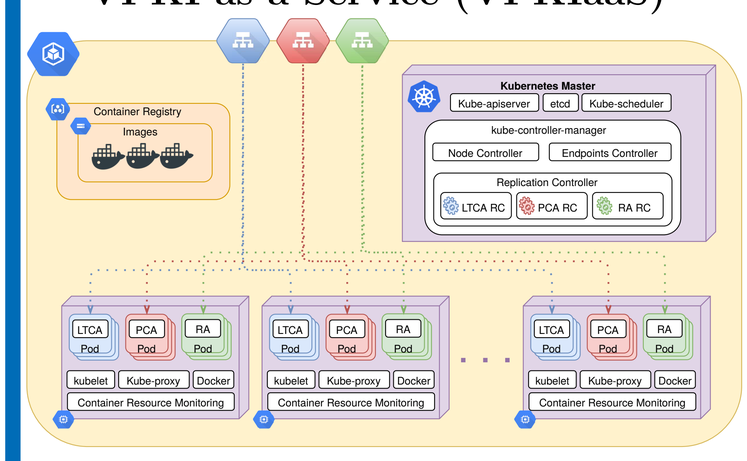
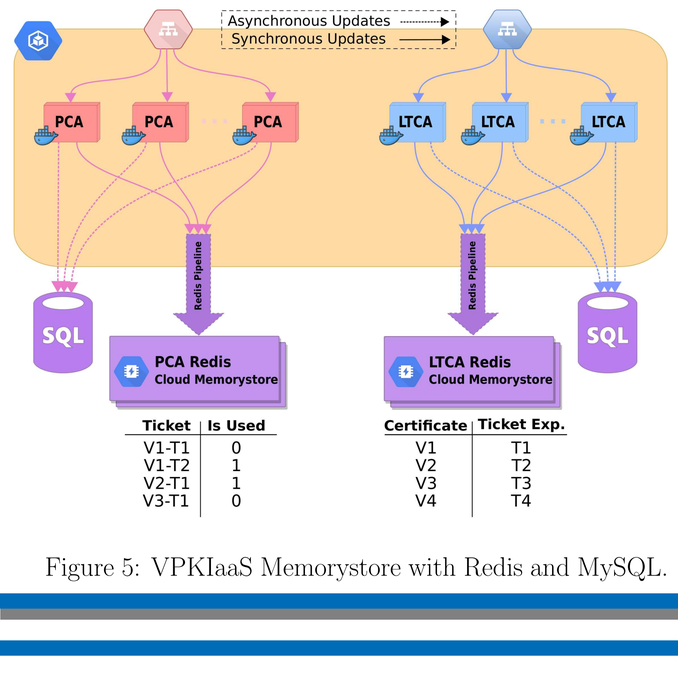


Figure 4: A High-level VPKIaaS Architecture.

VPKIaaS Memorystore



Ticket	Is Used
V1-T1	0
V1-T2	1
V2-T1	1
V3-T1	0

Certificate	Ticket Exp.
V1	T1
V2	T2
V3	T3
V4	T4

Figure 5: VPKIaaS Memorystore with Redis and MySQL.

Experimental Setup

- Nexcom boxes: Dual-core 1.66 GHz, 1GB memory, which support IEEE 802.11p
- Google Kubernetes Engine (GKE) v1.10.11: A cluster of five VMs (n1-highcpu-32), each with 32 vCPUs and 28.8GB of memory
- Implementation in C++, OpenSSL for cryptographic protocols & primitives, TLS and ECDSA-256
- **Config-1:** Normal vehicle arrival rate; every 1-5 sec, a new vehicle joins the system, requesting 100-500 pseudonyms
- **Config-2:** Flash crowd scenario; on top of Config-1, 100 new vehicles join the system every 1-5 sec, requesting 100-200 pseudonyms

VPKIaaS Performance under Normal Situation

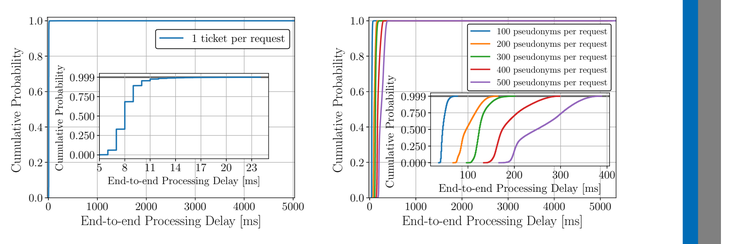


Figure 6: (a) CDF of E2E latency to issue a ticket. (b) CDF of E2E processing delay to issue pseudonyms.

VPKIaaS System Performance with Flash Crowd Load Pattern

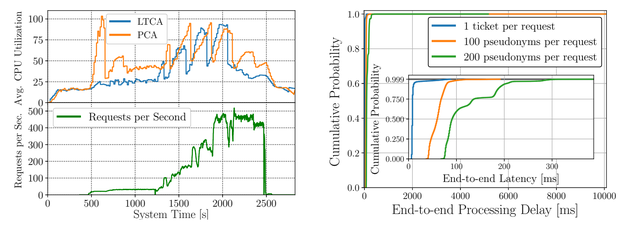


Figure 7: (a) CPU utilization with number of requests. (b) CDF of processing latency to issue tickets and pseudonyms.

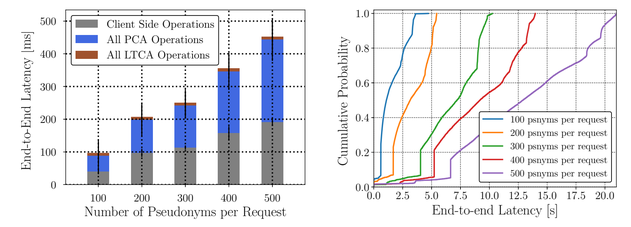


Figure 8: (a) Average E2E latency to obtain pseudonyms. (b) CDF of E2E latency, observed by clients.

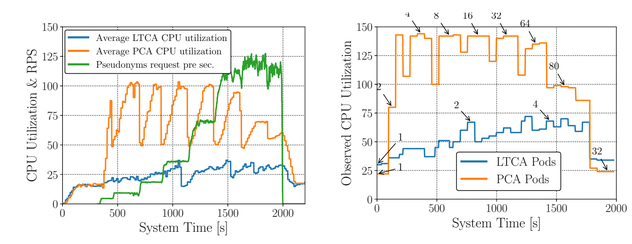


Figure 9: (a) Number of active vehicles and CPU utilization. (b) Dynamic scalability of the VPKIaaS system.

References

[1] M. Khodaei, H. Noroozi, and P. Papadimitratos, **"Scaling Pseudonymous Authentication for Large Mobile Systems,"** in ACM WiSec, Miami, FL, USA, May 2019.

[2] H. Noroozi, M. Khodaei, and P. Papadimitratos, **"DEMO: VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure,"** in ACM WiSec, Stockholm, Sweden, June 2018, pp. 302–304.

[3] M. Khodaei, H. Noroozi, and P. Papadimitratos, **"POSTER: Privacy Preservation through Uniformity,"** in ACM WiSec, Stockholm, Sweden, June 2018, pp. 279–280.

[4] M. Khodaei, H. Jin, and P. Papadimitratos, **"SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,"** in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, 1430–1444, May 2018.

[5] M. Khodaei, A. Messing, and P. Papadimitratos. 2017. **"RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd,"** in IEEE Vehicular Networking Conference (VNC), Torino, Italy, Nov. 2017.

[6] 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.

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

[8] M. Khodaei, H. Jin, and P. Papadimitratos. **"Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,"** in IEEE Vehicular Networking Conference (VNC), Paderborn, Germany, Dec. 2014.

Swedish Foundation *for* Strategic Research