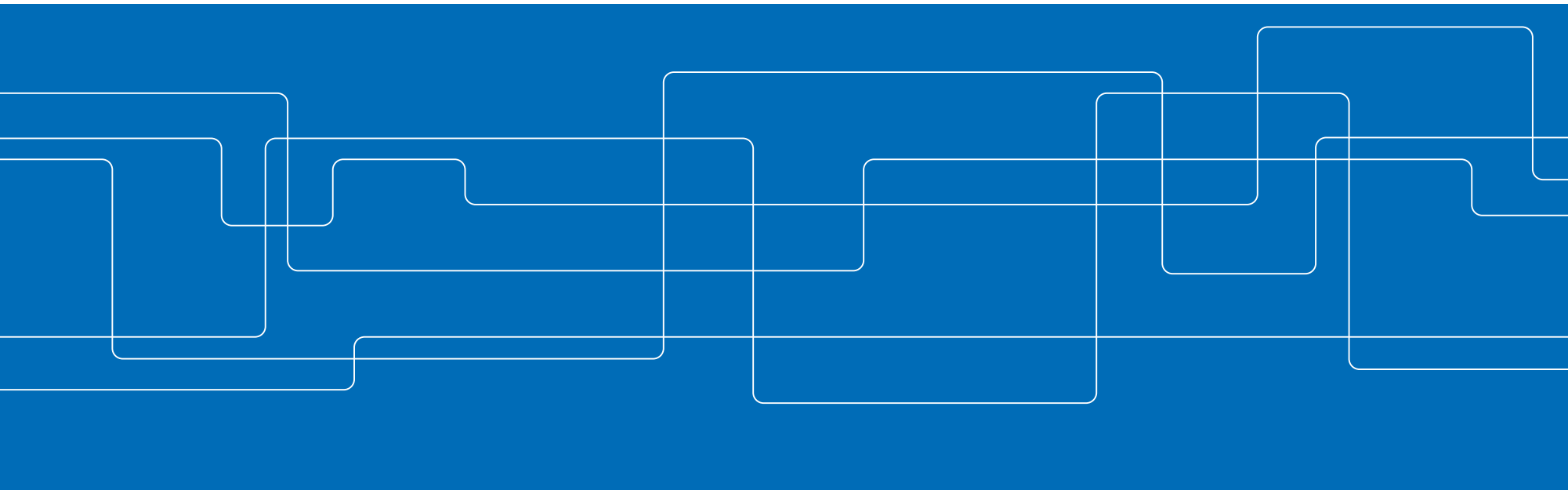
KTH ROYAL INSTITUTE
OF TECHNOLOGY

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

M. Khodaei, H. Jin and P. Papadimitratos
Networked Systems Security Group (NSS)

In IEEE Transactions on Intelligent Transportation Systems (April 2018)



Outline

Vehicular Communication (VC) Systems

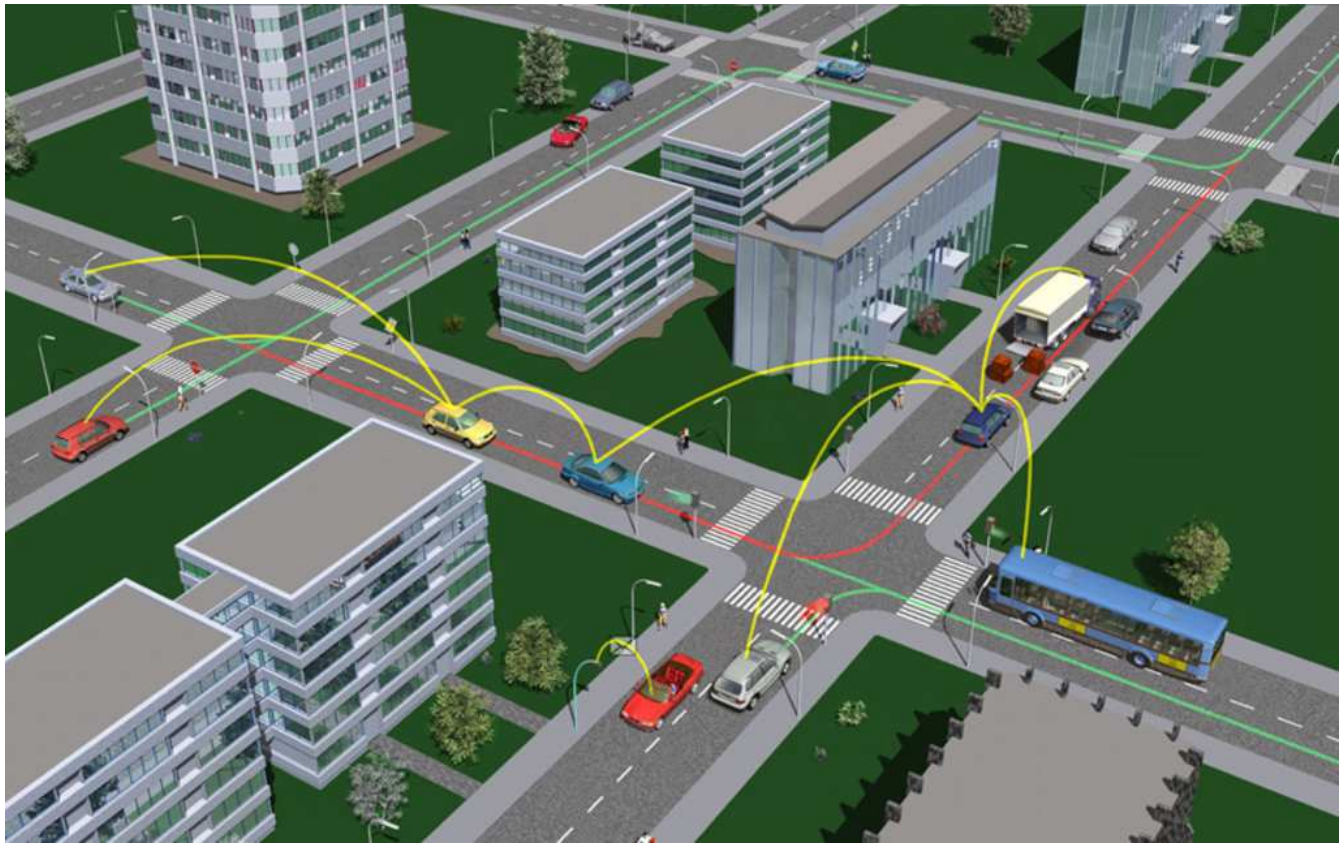
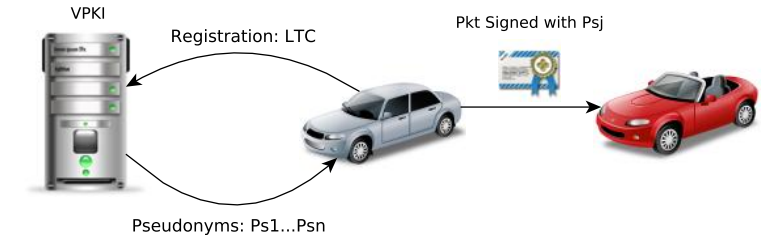


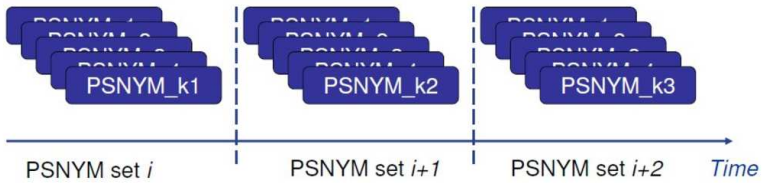
Figure: Photo Courtesy of the Car2Car Communication Consortium (C2C-CC)

Security and Privacy for VC Systems[1]

Basic Requirements

- Message authentication & integrity
- Message non-repudiation
- Access control
- Entity authentication
- Accountability
- Privacy protection



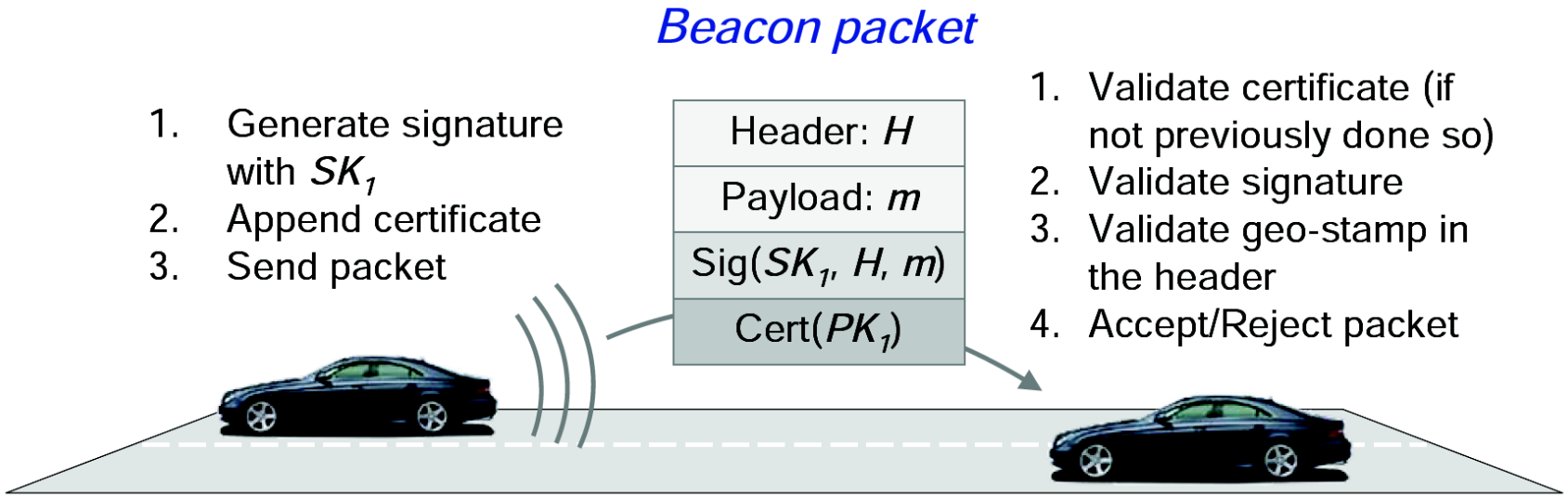


Vehicular Public-Key Infrastructure (VPKI)

- Pseudonymous authentication
- Trusted Third Party (TTP):
  - Certification Authority (CA)
  - Issues credentials & binds users to their pseudonyms

[1] P. Papadimitratos, et al. "Securing Vehicular Communications - Assumptions, Requirements, and Principles," in ESCAR, Berlin, Germany, pp. 5-14, Nov. 2006.
P. Papadimitratos, et al. "Secure Vehicular Communication Systems: Design and Architecture," in IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

Security and Privacy for VC Systems (cont'd)



- Sign packets with the private key, corresponding to the current valid pseudonym
- Verify packets with the valid pseudonym
- Cryptographic operations in a Hardware Security Module (HSM)

State-of-the-art

Standardization and harmonization efforts

- IEEE 1609.2 [1], ETSI [2] and C2C-CC [3]
- VC related specifications for security and privacy-preserving architectures

Projects

- SEVECOM, EVITA, PRECIOSA, OVERSEE, DRIVE-C2X, Safety Pilot, PRESERVE, CAMP-VSC3

Proposals

- V-Token, CoPRA, SCMS , SEROSA, PUCA

Outline

Problem Statement and Motivation
The design of a VPKI

- Resilience
- Stronger adversarial model (than fully-trustworthy entities)
  - User privacy protection against *"honest-but-curious"* entities
  - User privacy enhancement and service unlinkability (inference of service provider or time)
- Pseudonym acquistion policies
  - How should each vehicle interact with the VPKI, e.g., how frequently and for how long?
  - Should each vehicle itself determine the pseudonym lifetime?
- Operation across multiple domains, thus a scalable design
- Efficiency and robustness

Security and Privacy Requirements for the VPKI Protocols

- Authentication, communication integrity and confidentiality
- Authorization and access control
- Non-repudiation, accountability and eviction (revocation)
- Privacy
  - Anonymity (conditional)
  - Unlinkability
- Thwarting Sybil-based misbehavior
- Availability

Adversarial Model

External adversaries

Internal adversaries

Stronger adversarial model

Protection against *honest-but-curious* VPKI entities

- Correct execution of protocols but motivated to profile users
- Concealing pseudonym provider identity and acquisition time, and reducing pseudonyms linkability (inference based on time)

Multiple VPKI entities could collude

Outline

Secure VC System

- Root Certification Authority (RCA)
- Long Term CA (LTCA)
- Pseudonym CA (PCA)
- Resolution Authority (RA)
- Lightweight Directory Access Protocol (LDAP)
- Roadside Unit (RSU)
- Trust established with RCA, or through cross certification

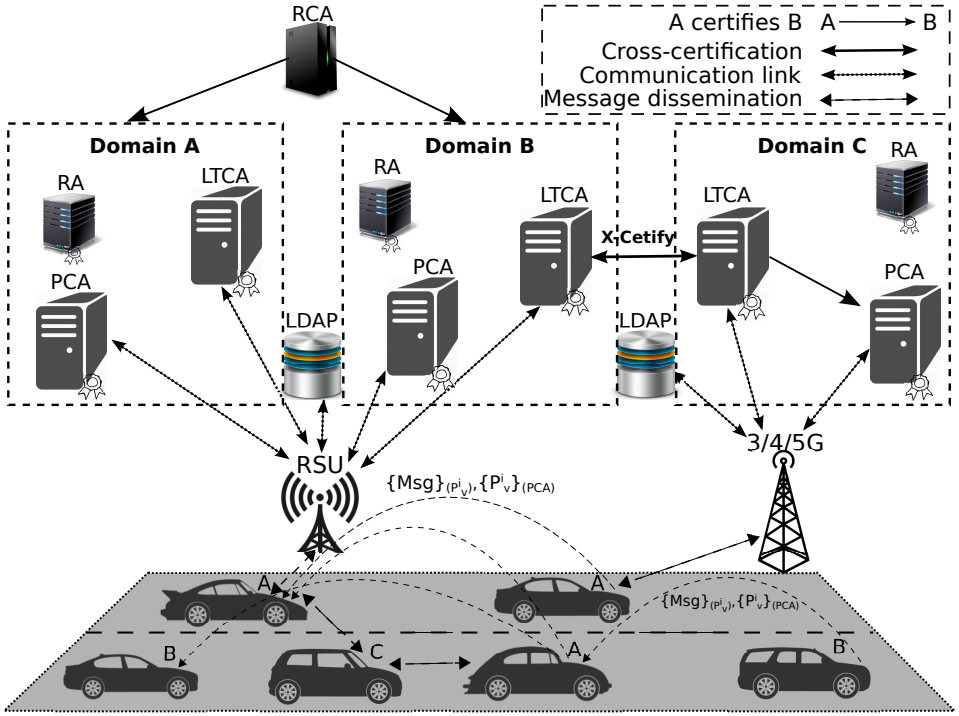


Figure: VPKI Overview

System Model

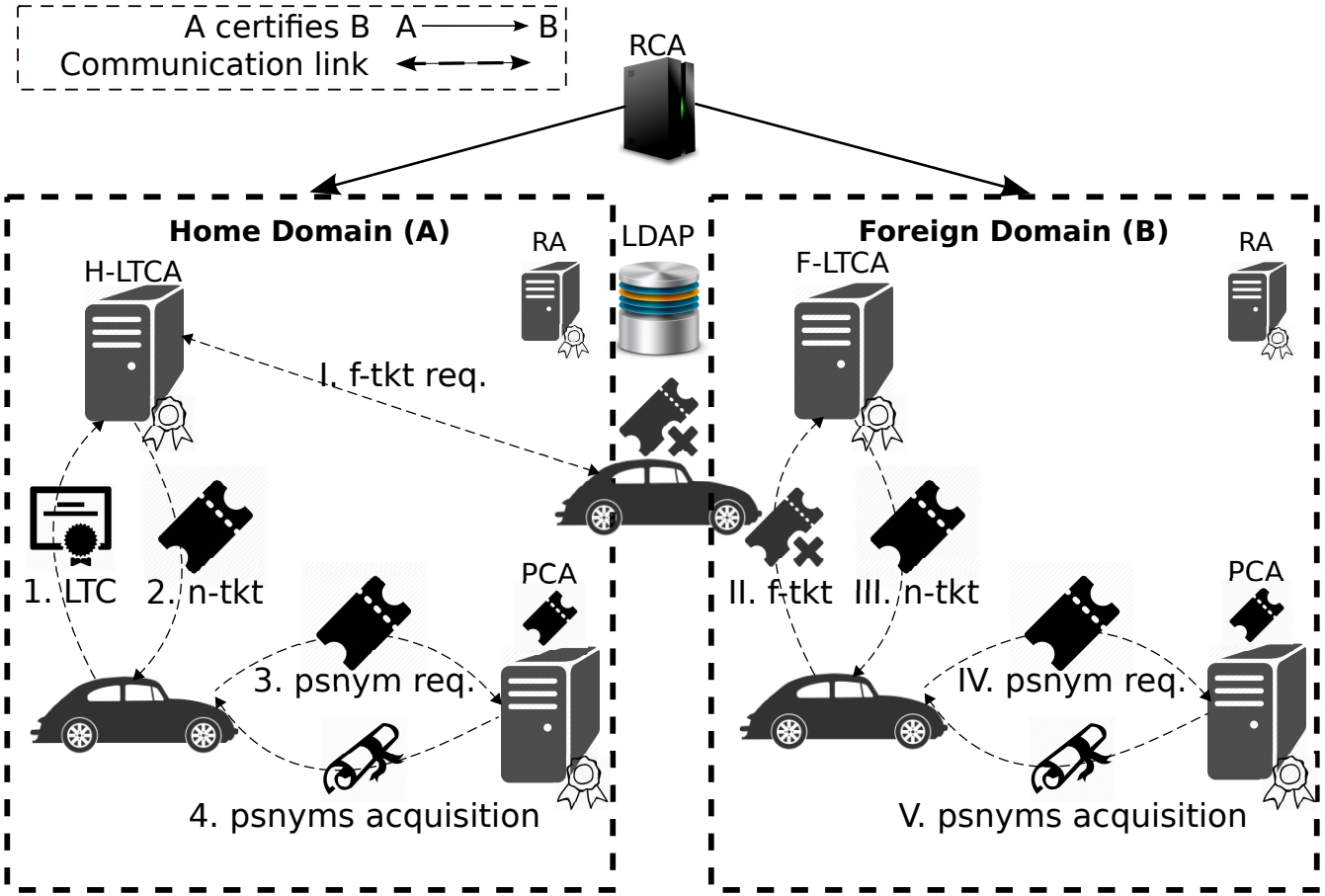


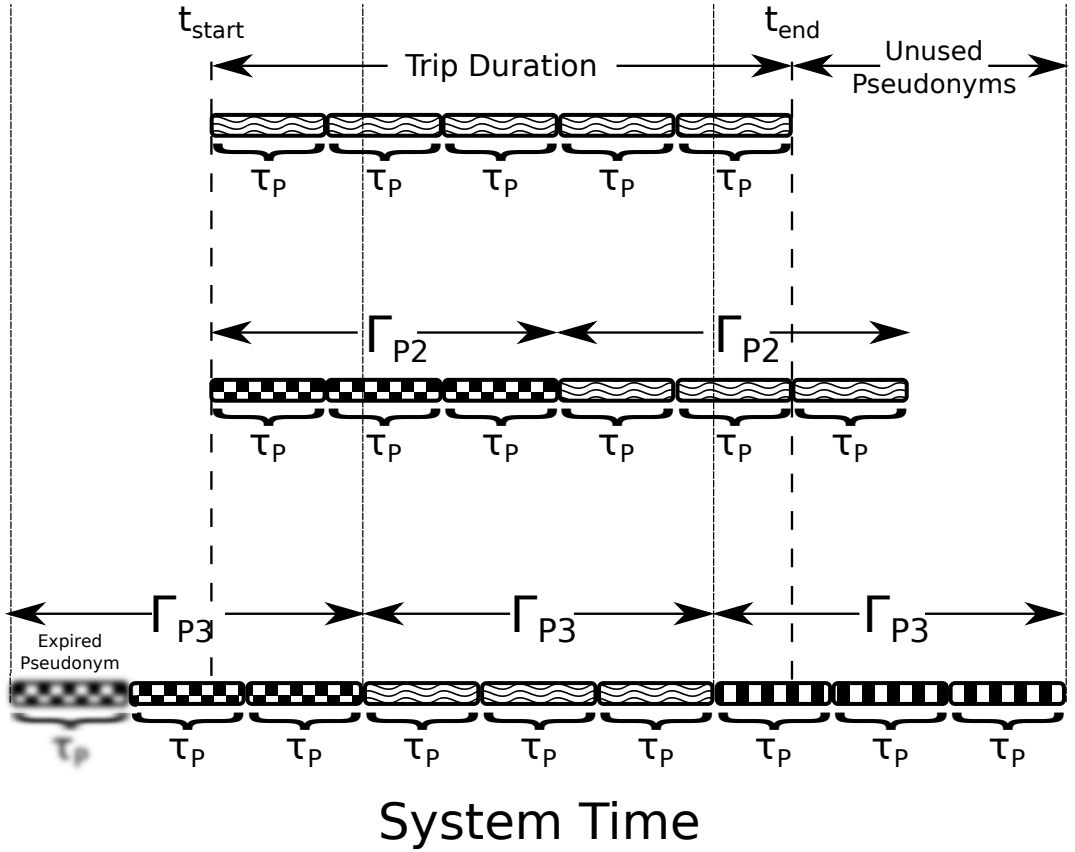
Figure: VPKI Architecture

Pseudonym Acquisition Policies

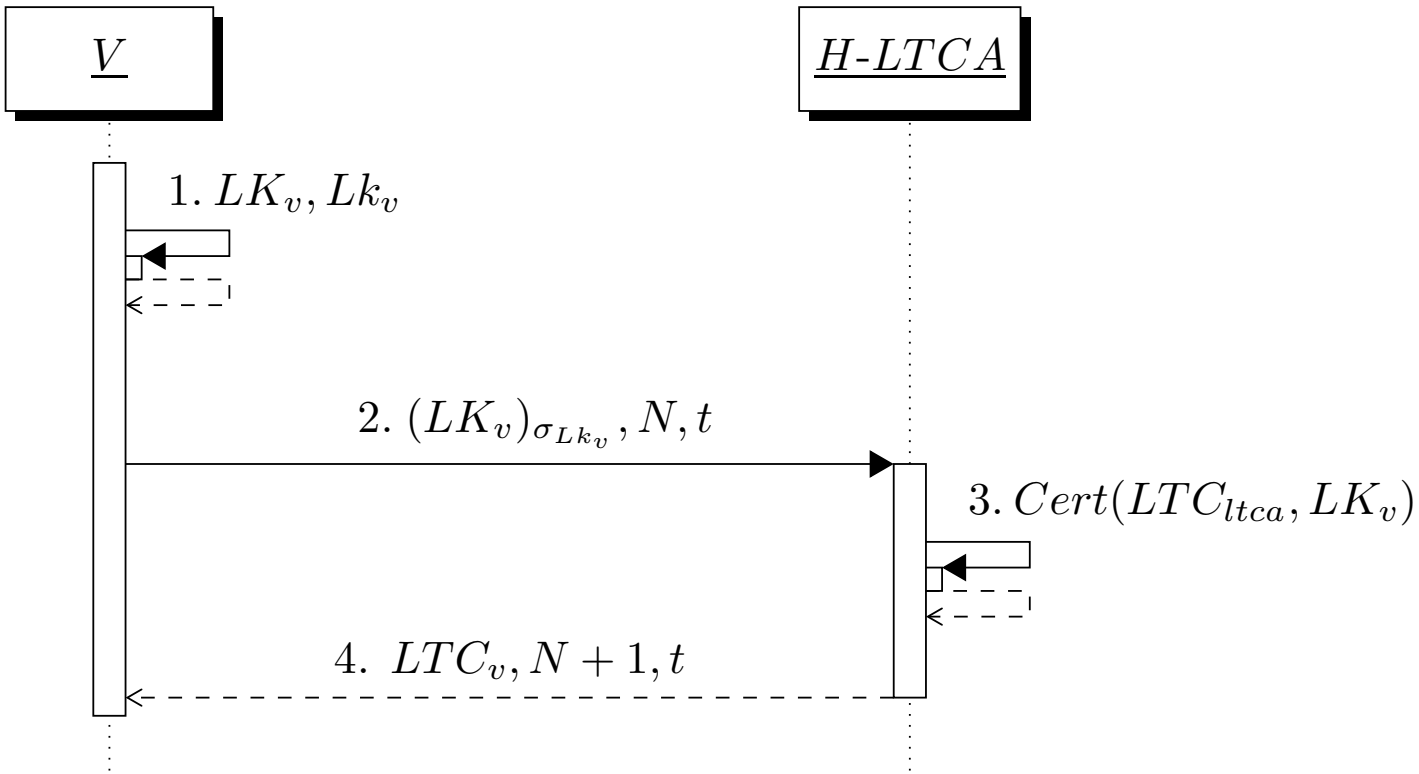
User-controlled policy (P1)

Oblivious policy (P2)

Universally fixed policy (P3)



Vehicle Registration and Long Term Certificate (LTC) Update



Ticket Acquisition Protocols

Protocol 1 Ticket Request (from the LTCA)

1: **procedure** REQTICKET($P_x, \Gamma_{Px}, t_s, t_e, t_{date}$)
2: **if** $P_x = P1$ **then**
3: $(t_s, t_e) \leftarrow (t_s, t_e)$
4: **else if** $P_x = P2$ **then**
5: $(t_s, t_e) \leftarrow (t_s, t_s + \Gamma_{P2})$
6: **else if** $P_x = P3$ **then**
7: $(t_s, t_e) \leftarrow (t_{date} + \Gamma^{i}_{P3}), t_{date} + \Gamma^{i+1}_{P3})$
8: **end if**
9: $\zeta \leftarrow (Id_{tkt\text{-}req}, H(Id_{PCA} || Rnd_{tkt}), t_s, t_e)$
10: $(\zeta)_{\sigma_v} \leftarrow Sign(Lk_v, \zeta)$
11: **return** $((\zeta)_{\sigma_v}, \text{LTC}_v, N, t_{now})$
12: **end procedure**

- Run over Transport Layer Security (TLS) with mutual authentication

Protocol 2 Issuing a Ticket (by the LTCA)

1: **procedure** ISSUETICKET($(msg)_{\sigma_v}, \text{LTC}_v, N, t_{now}$)
2: Verify($\text{LTC}_v, (msg)_{\sigma_v}$)
3: $IK_{tkt} \leftarrow H(\text{LTC}_v || t_s || t_e || Rnd_{IK_{tkt}})$
4: $\zeta \leftarrow (SN, H(Id_{PCA} || Rnd_{tkt}), IK_{tkt}, Rnd_{IK_{tkt}}, t_s, t_e, Exp_{tkt})$
5: $(tkt)_{\sigma_{ltca}} \leftarrow Sign(Lk_{ltca}, \zeta)$
6: **return** $((tkt)_{\sigma_{ltca}}, N + 1, t_{now})$
7: **end procedure**

- *"ticket identifiable key"* (IK_{tkt}) binds a ticket to the corresponding LTC
- Preventing a compromised LTCA from mapping a different LTC during resolution process

Pseudonyms Acquisition Protocols

Protocol 3 Pseudonym Request (from the PCA)

1: **procedure** REQPSNYMS($t_s, t_e, (tkt)_{\sigma_{ltca}}$)
2: **for** i:=1 to **n do**
3: **Begin**
4: Generate(K_v^i, k_v^i)
5: $(K_v^i)_{\sigma_{k_v^i}} \leftarrow$ Sign(k_v^i, K_v^i)
6: **End**
7: $psnymReq \leftarrow (Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, ..., (K_v^n)_{\sigma_{k_v^n}}\}, N, t_{now})$
8: **return** *psnymReq*
9: **end procedure**

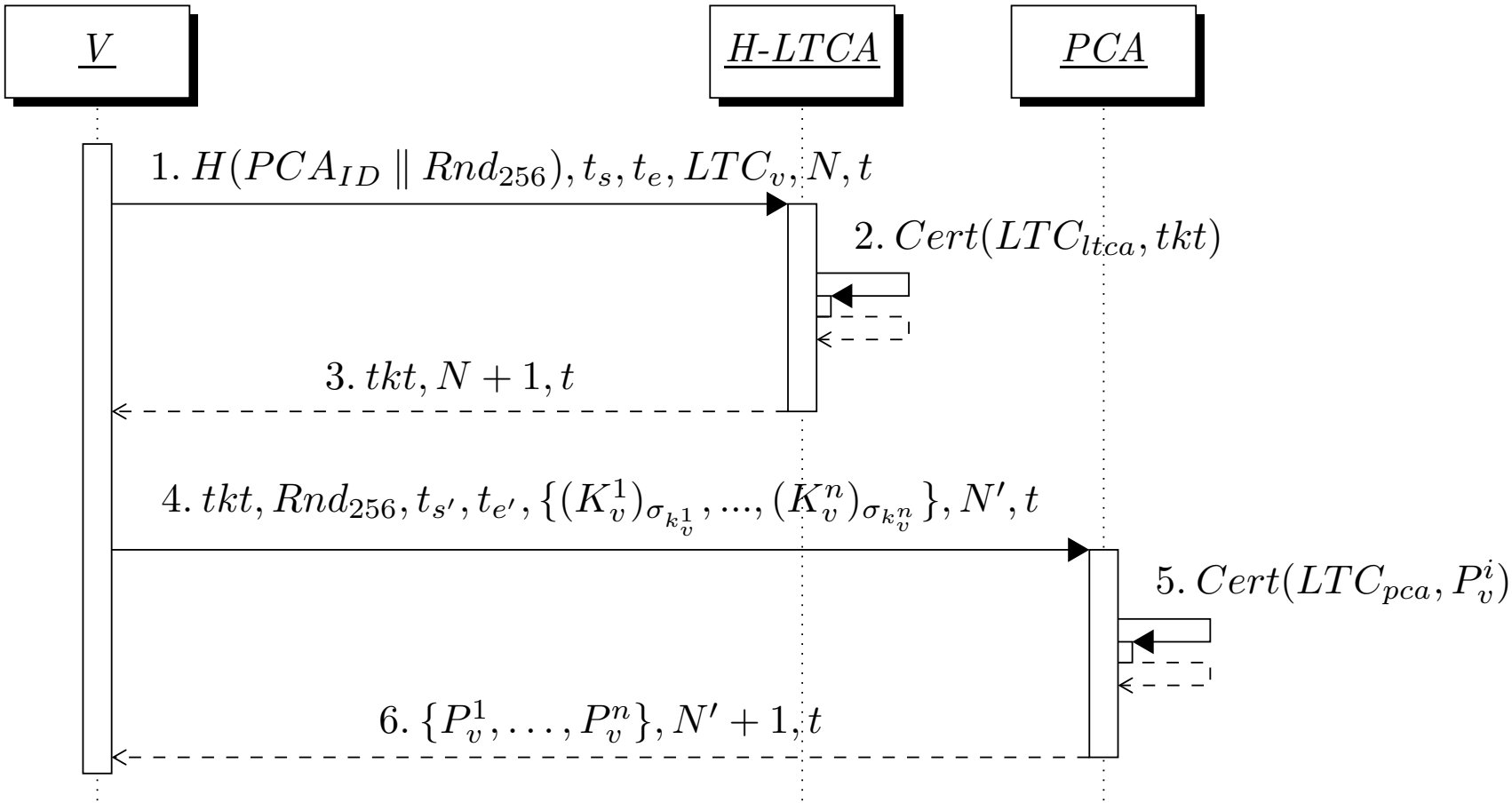
- Run over TLS with unidirectional (server-only) authentication

Protocol 4 Issuing Pseudonyms (by the PCA)

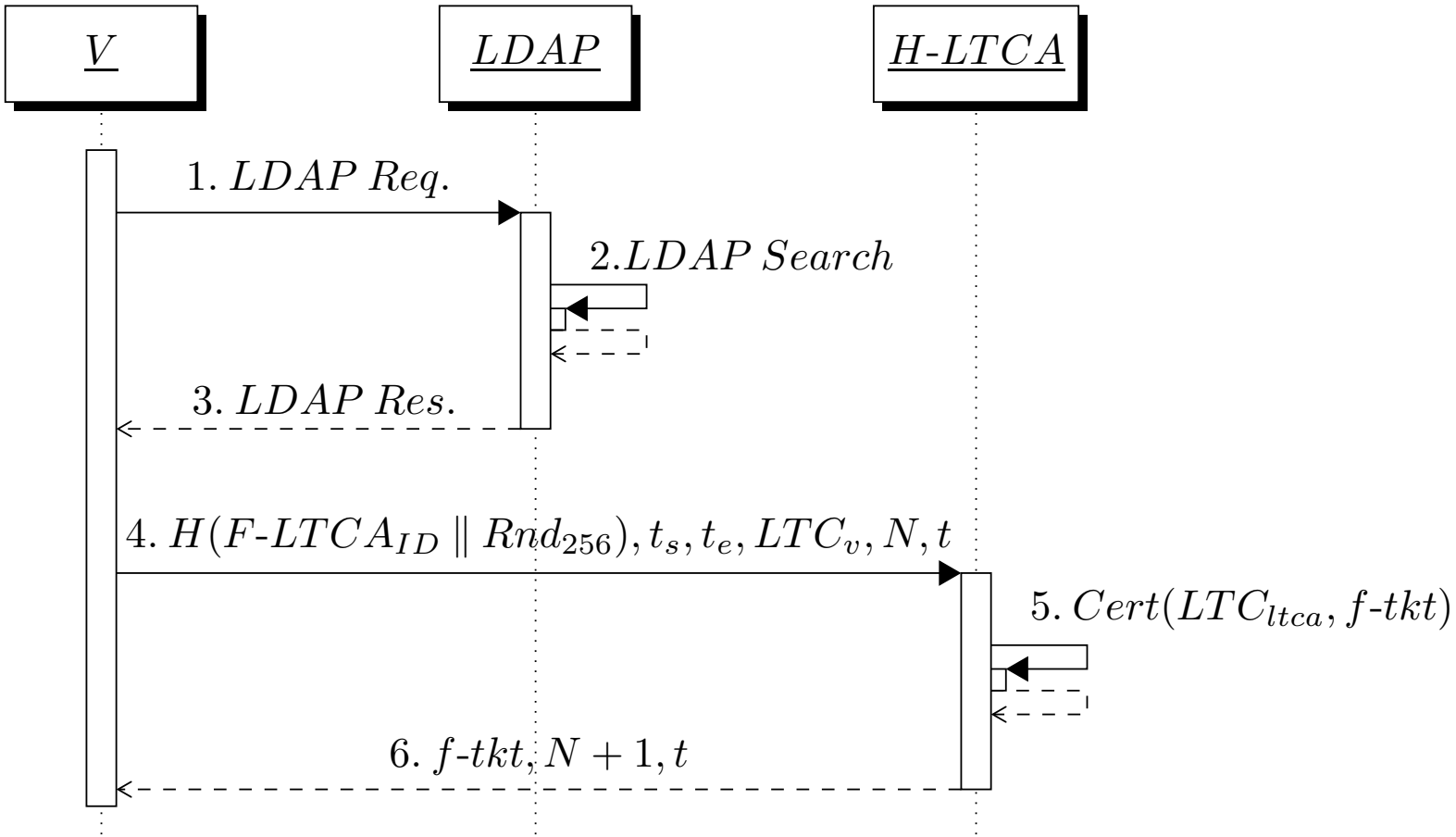
1: **procedure** ISSUEPSNYMS(*psnymReq*)
2: $psnymReq \rightarrow (Id_{req}, Rnd_{tkt}, t_s, t_e, (tkt)_{\sigma_{ltca}}, \{(K_v^1)_{\sigma_{k_v^1}}, ..., (K_v^n)_{\sigma_{k_v^n}}\}, N, t_{now})$
3: Verify($LTC_{ltca}, (tkt)_{\sigma_{ltca}}$)
4: $H(Id_{this\text{-}PCA} || Rnd_{tkt}) \stackrel{?}{=} H(Id_{PCA} || Rnd_{tkt})$
5: $[t_s,\ t_e] \stackrel{?}{=} ([t_s, t_e])_{tkt}$
6: **for** i:=1 to **n do**
7: **Begin**
8: Verify($K_v^i, (K_v^i)_{\sigma_{k_v^i}}$)
9: $IK_{P^i} \leftarrow H(IK_{tkt} || K_v^i || t_s^i || t_e^i || Rnd_{IK_v^i})$
10: $\zeta \leftarrow (SN^i, K_v^i, IK_{P^i}, Rnd_{IK_v^i}, t_s^i, t_e^i)$
11: $(P_v^i)_{\sigma_{pca}} \leftarrow Sign(Lk_{pca}, \zeta)$
12: **End**
13: **return** $(\{(P_v^1)_{\sigma_{pca}}, \ldots, (P_v^n)_{\sigma_{pca}}\}, N{+}1, t_{now})$
14: **end procedure**

- *"pseudonym identifiable key"* (IK_{P^i}) binds a pseudonym to the corresponding ticket
- Preventing a compromised PCA from mapping a different ticket during resolution process

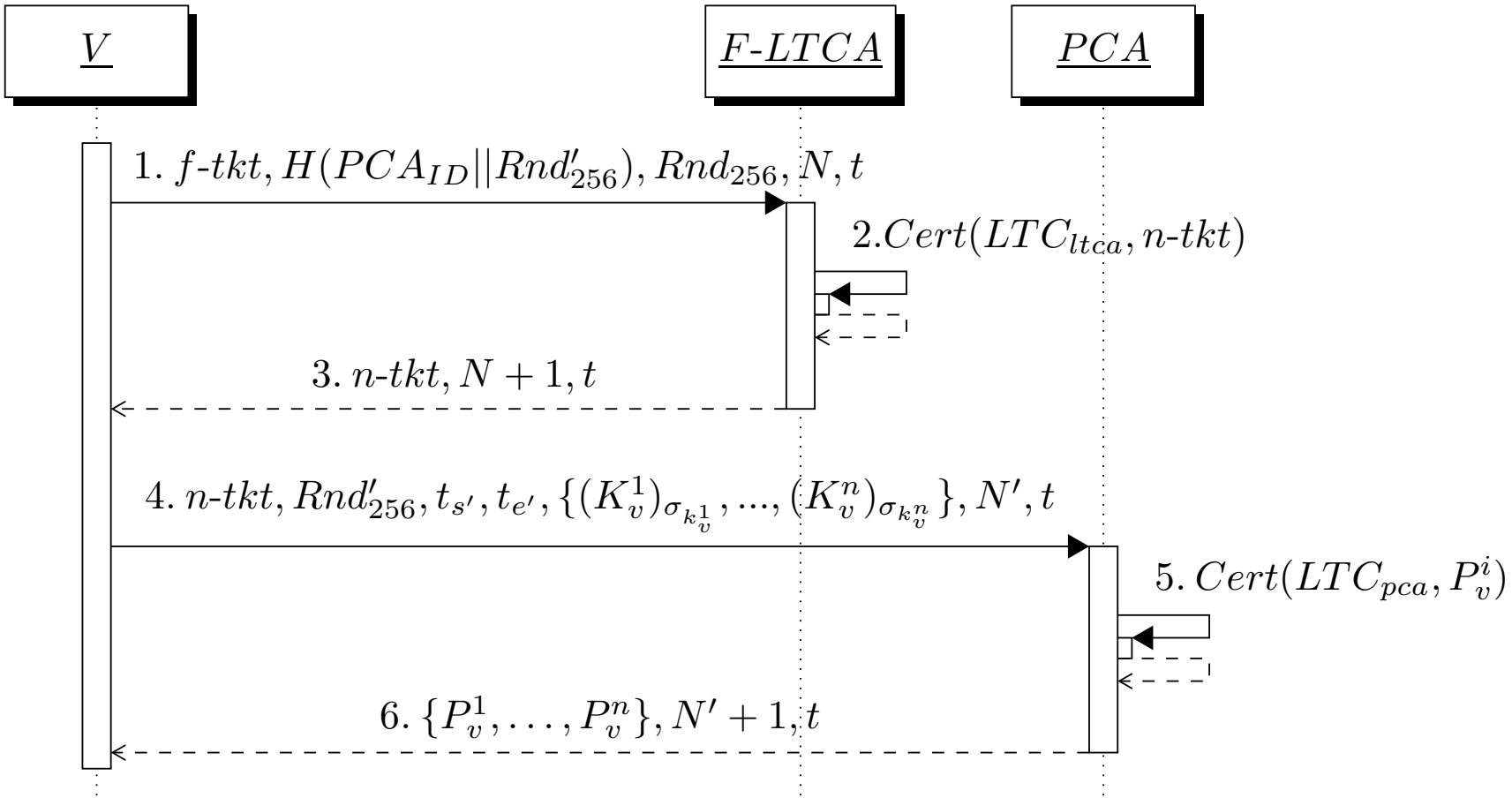
Ticket and Pseudonym Acquisition



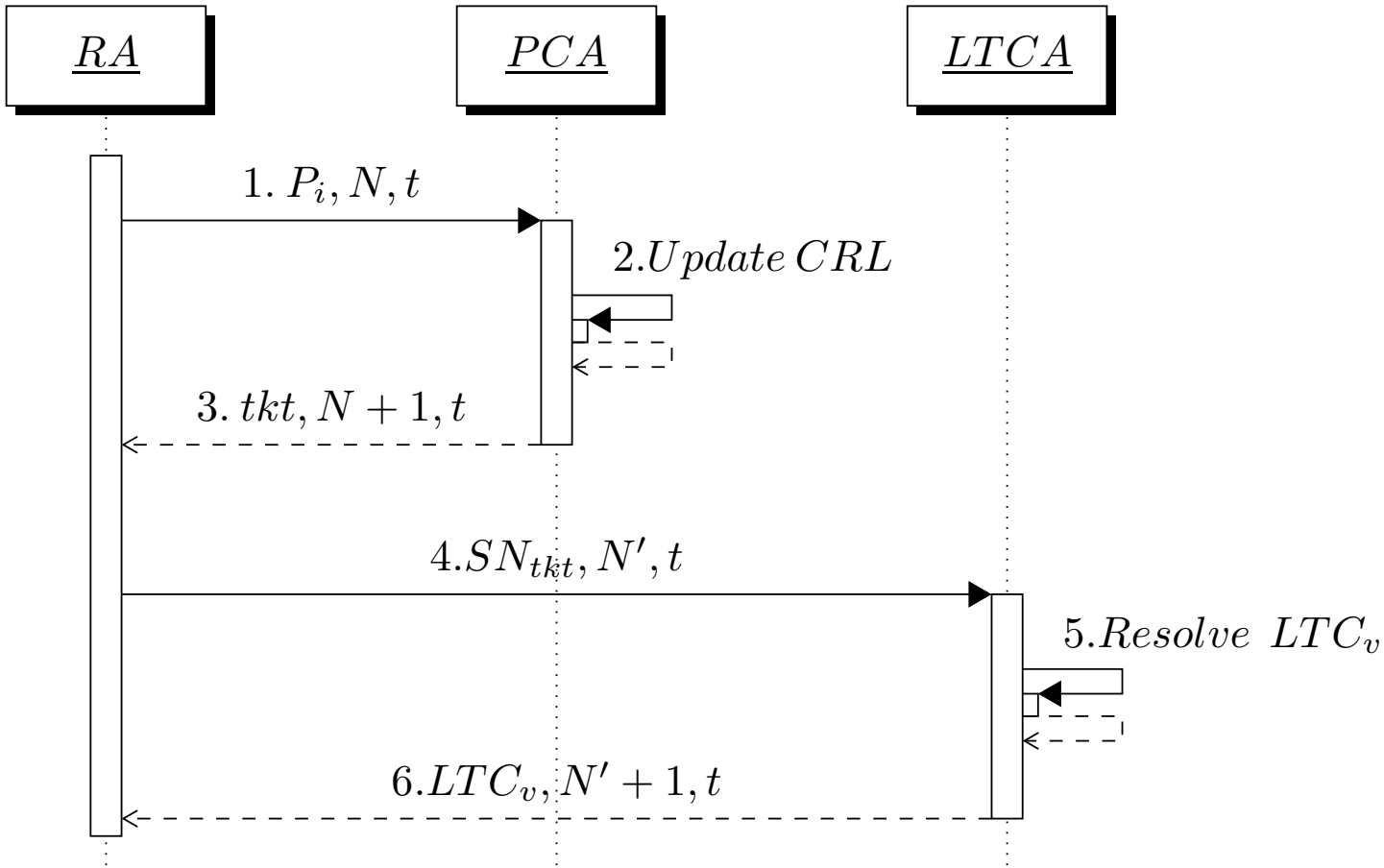
Roaming User: Foreign Ticket Authentication



Native Ticket and Pseudonym Acquisition in the Foreign Domain



Pseudonym Revocation and Resolution

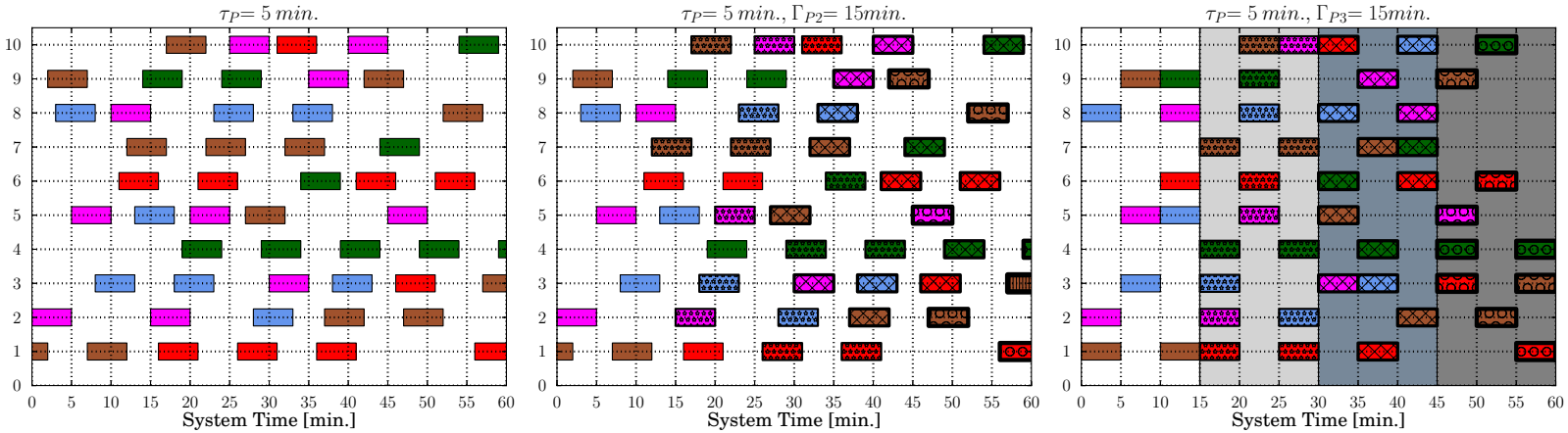


Outline

Security and Privacy Analysis

- Communication integrity, confidentiality, and non-repudiation
  - Certificates, TLS and digital signatures
- Authentication, authorization and access control
  - LTCA is the *policy decision and enforcement point*
  - PCA grants the service
  - Security association discovery through LDAP
- Concealing PCAs, F-LTCA, actual pseudonym acquisition period
  - Sending $H(PCA_{id} \| Rnd_{256})$, t_s, t_e, LTC_v to the H-LTCA
  - PCA verifies if $[t'_s,\ t'_e] \subseteq [t_s,\ t_e]$
- Thwarting Sybil-based misbehavior
  - LTCA never issues valid tickets with overlapping lifetime (for a given domain)
  - A ticket is bound to a specific PCA
  - PCA keeps records of ticket usage

Linkability based on Timing Information of Credentials



(a) P1: User-controlled policy (b) P2: Oblivious policy (c) P3: Universally fixed policy

- Non-overlapping pseudonym lifetimes from eavesdroppers' perspective
- P1 & P2: Distinct lifetimes per vehicle make linkability easier (requests/pseudonyms could act as user *'fingerprints'*)
- P3: Uniform pseudonym lifetime results in no distinction

Outline

Experimental Setup

- **VPKI testbed**
  - Implementation in C++
  - OpenSSL: TLS and Elliptic Curve Digital Signature Algorithm (ECDSA)-256 according to the standard [1]
- **Network connectivity**
  - Varies depending on the actual OBU-VPKI connectivity
  - Reliable connectivity to the VPKI (e.g., RSU, Cellular, opportunistic WiFi)

Table: Servers and Clients Specifications

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

- **Use cases**
  - Pseudonym provision
  - Performing a DDoS attack

Experimental Setup (cont'd)

Table: Mobility Traces Information

	TAPASCologne	LuST [5]
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
Total trip duration (sec.)	44,655,579	102,766,924

- **Main metric**
  - End-to-end pseudonym acquisition latency from the initialization of ticket acquisition protocol till successful completion of pseudonym acquisition protocol

Table: Servers & Clients Specifications

	LTCA	PCA	Client
Number of entities	1	1	1
Dual-core CPU (Ghz)	2.0	2.0	2.0
BogoMips	4000	4000	4000
Memory	2GB	2GB	1GB
Database	MySQL	MySQL	MySQL

- N.B. PRESERVE Nexcom boxes specs: dual-core 1.66 GHz, 2GB Memory

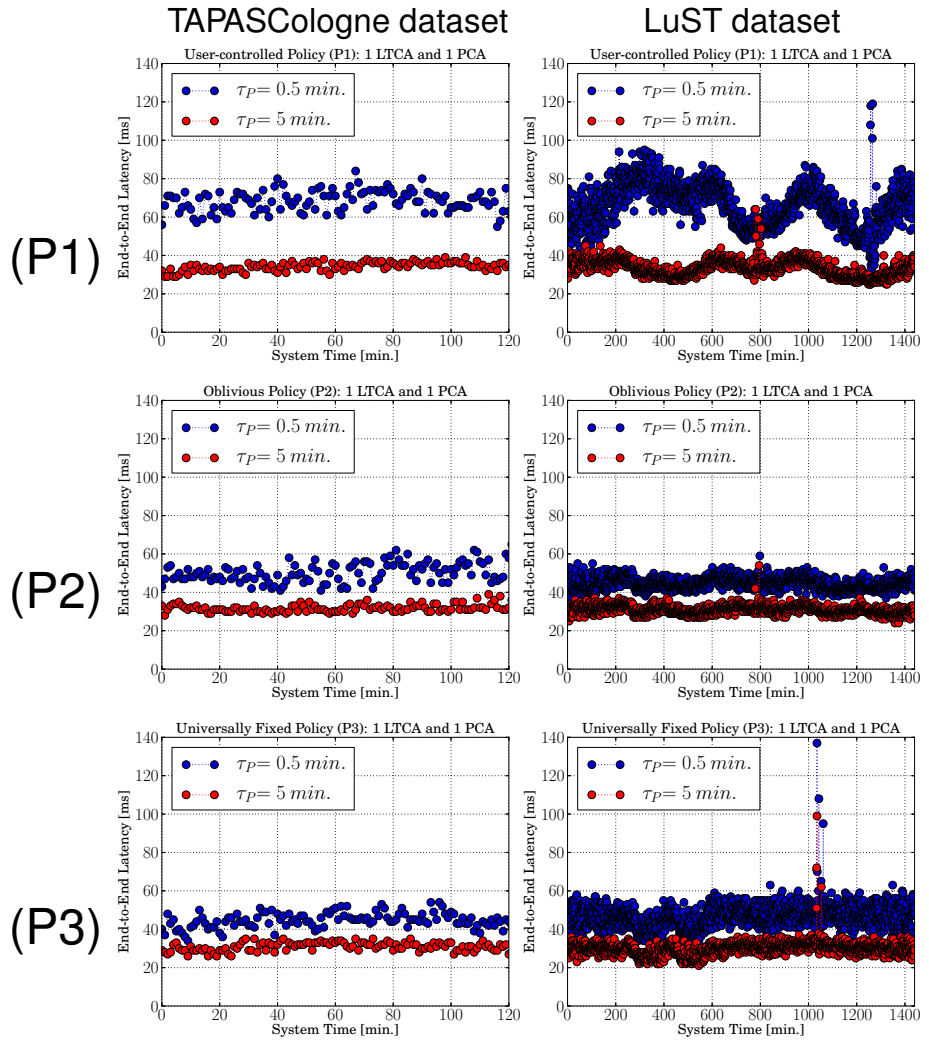
End-to-end Latency for P1, P2, and P3

Choice of parameters:

- Frequency of interaction and volume of workload to a PCA
- Γ=5 min., τ_P=0.5 min., 5 min.

LuST dataset ($\tau_P = 0.5\ min$):

- P1: $F_x(t = 167\ ms) = 0.99$
- P2: $F_x(t = 80\ ms) = 0.99$
- P3: $F_x(t = 74\ ms) = 0.99$



Latency Comparison for Different Policies

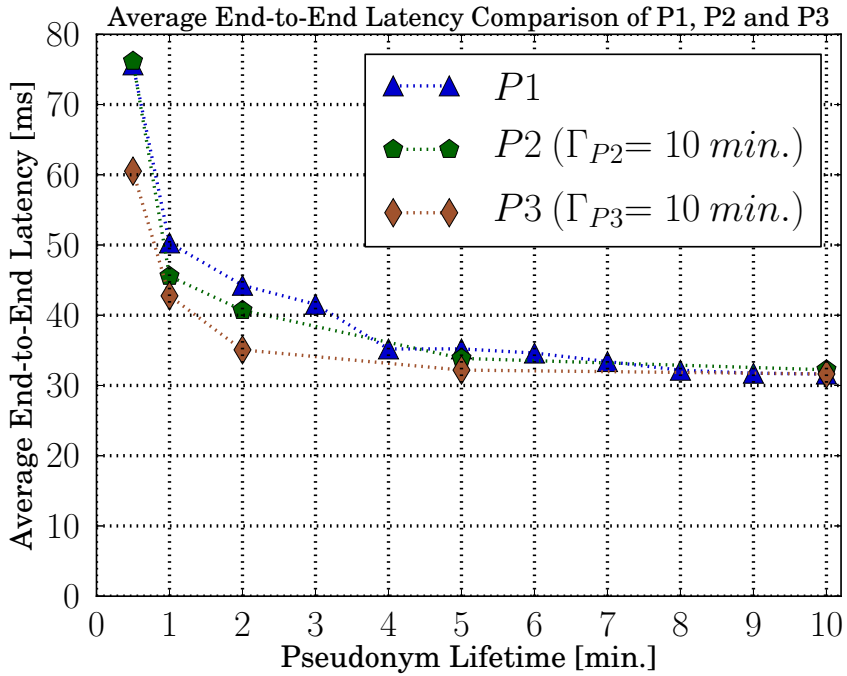
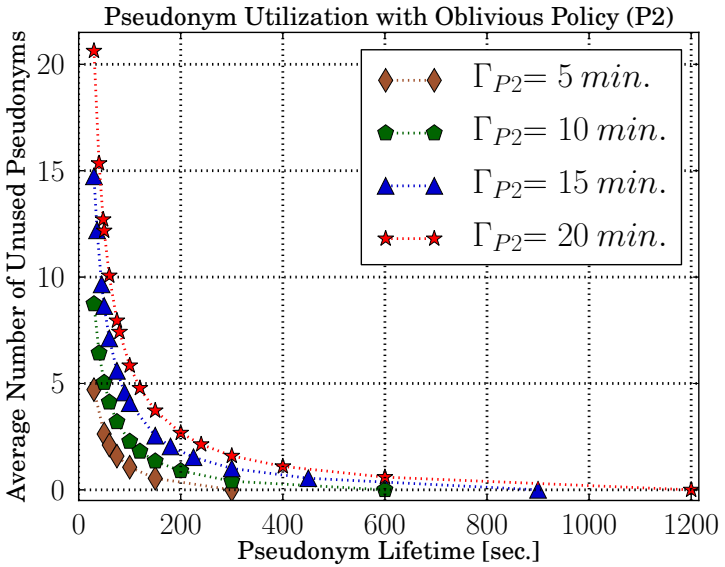
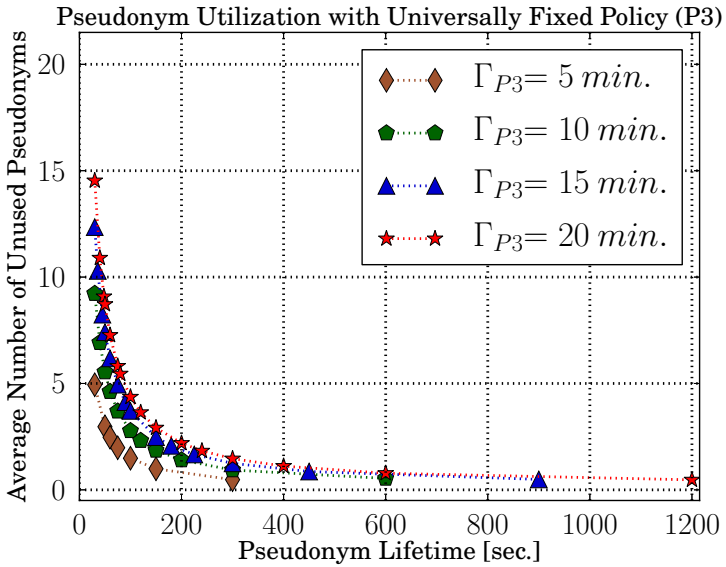


Figure: End-to-end latency comparison for different policies (Tapas Dataset)

Pseudonym Utilization, LuST Dataset for P2 & P3



P2: Oblivious Policy



P3: Universally Fixed Policy

The VPKI Servers under a DDoS Attack

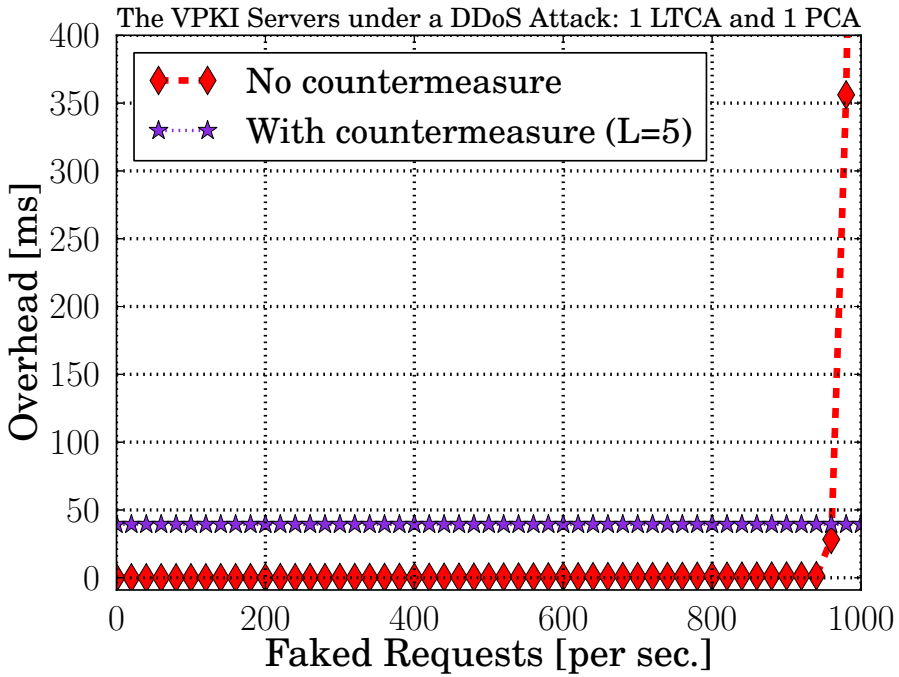
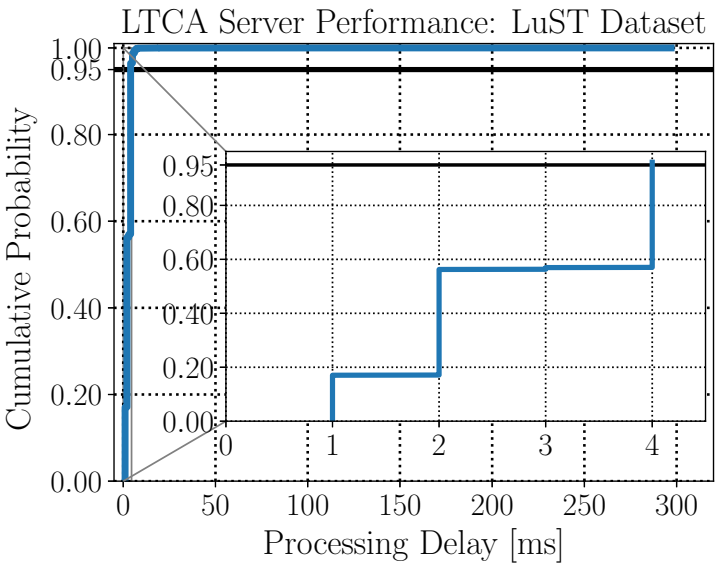
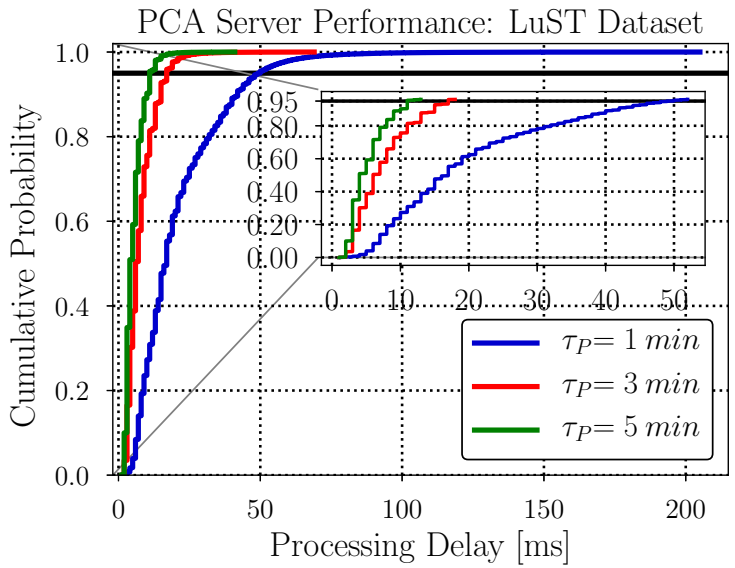


Figure: Overhead to obtain pseudonyms, LuST dataset with P1 (τ_P = 5 min.)

Performance Evaluation for Ticket and Pseudonym Acquisition



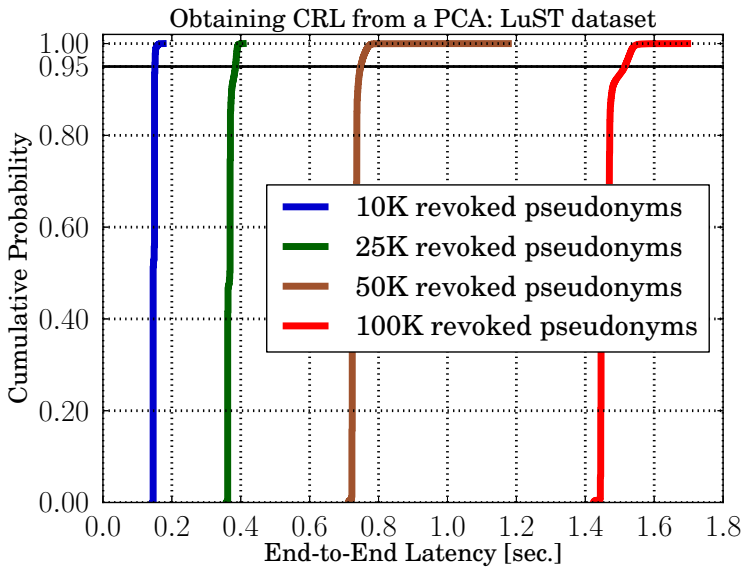
Obtaining a Certificate Revocation List (CRL)

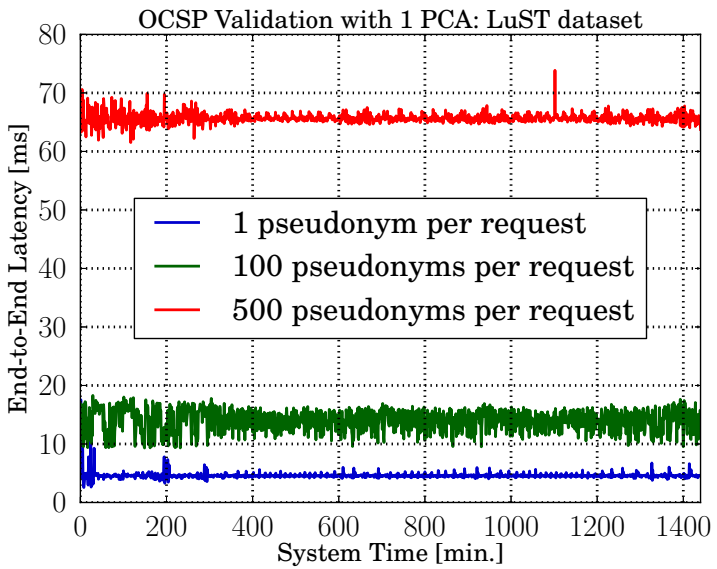


Online Certificate Status Protocol (OCSP) validation

- Ticket Acquisition: F_x(t=4ms)=0.95 or Pr{t$\leq$4ms}=0.95.
- Pseudonym Acquisition: F_x(t=52ms)=0.95 or Pr{t$\leq$52}=0.95.

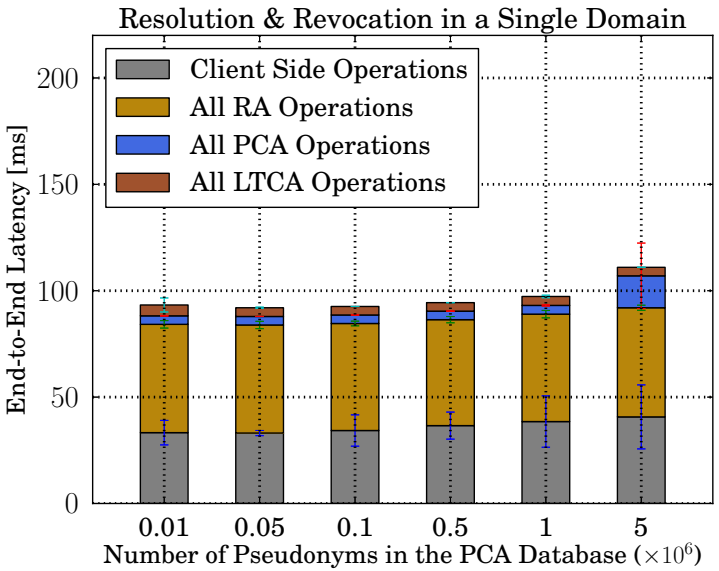
Performance Evaluation for Pseudonym Revocation (CRL or OCSP)



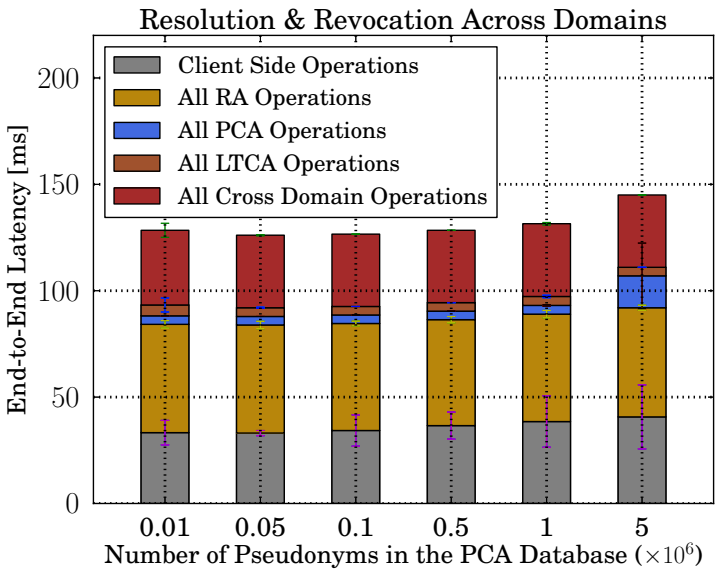


Obtaining a CRL OCSP validation

Entities Response Time to Resolve & Revoke a Pseudonym



Single Domain Operation



Across Domains Operation

- On average 100 ms to resolve & revoke a pseudonym

Comparison with Other Implementations

Table: Latency for issuing 100 pseudonyms (without communication delay)

	$Delay_{PCA}$	CPU_{PCA}
VeSPA [6]	817 ms	3.4 GHz
SEROSA [7]	650 ms	2.0 GHz
PUCA [8]	1000 ms	2.53 GHz
PRESERVE PKI (Fraunhofer SIT) [9]	$\approx$ 4000 ms	N/A
C2C-CC PKI (ESCRYPT) [3]	393 ms	N/A
SECMACE	260 ms	2.0 GHz

Outline

Summary of Contributions

1. Facilitating multi-domain operation
2. Offering increased user privacy protection
   - Honest-but-curious system entities
   - Eliminating pseudonym linking based on timing information
3. Eradication of Sybil-based misbehavior
4. Proposing multiple generally applicable pseudonym acquisition policies
5. Detailed analysis of security and privacy protocols
6. Extensive experimental evaluation
   - Efficiency, scalability, and robustness
   - Achieving significant performance improvement
   - Modest VMs can serve sizable areas or domain

Future Steps

VPKI enhancements

- Evaluation of the level of privacy, i.e., unlinkability, based on the timing information of the pseudonyms for each policy
- Evaluation of actual networking latency, e.g., OBU-RSU
- Rigorous analysis of the security and privacy protocols

Efficient distribution of revocation information

- *How to disseminate pseudonyms validity information without interfering with vehicles operations?*

Bibliography I

[1] "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.

[2] T. ETSI, "ETSI TS 103 097 v1. 1.1-Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats, Standard, TC ITS," Apr. 2013.

[3] Car-to-Car Communication Consortium (C2C-CC), June 2013. [Online]. Available: http://www.car-2-car.org/

[4] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A Security Credential Management System for V2V Communications," in *IEEE VNC*, Boston, MA, pp. 1–8, Dec. 2013.

[5] L. Codeca, R. Frank, and T. Engel, "Luxembourg Sumo Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research," in *IEEE VNC*, Kyoto, Japan, pp. 1–8, Dec. 2015.

Bibliography II

[6] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, “VeSPA: Vehicular Security and Privacy-preserving Architecture,” in *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*, Budapest, Hungary, pp. 19–24, Apr. 2013.

[7] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, “SEROSA: SERvice Oriented Security Architecture for Vehicular Communications,” in *IEEE VNC*, Boston, MA, USA, Dec. 2013.

[8] D. Förster, H. Löhr, and F. Kargl, “PUCA: A Pseudonym Scheme with User-Controlled Anonymity for Vehicular Ad-Hoc Networks (VANET),” in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[9] “Preparing Secure Vehicle-to-X Communication Systems - PRESERVE.” [Online]. Available: http://www.preserve-project.eu/

[10] M. Khodaei, “Secure Vehicular Communication Systems: Design and Implementation of a Vehicular PKI (VPKI),” Master’s thesis, Lab of Communication Networks (LCN), KTH University, Oct. 2012.

Bibliography III

[11] 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, pp. 33–40, Dec. 2014.

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

[13] ——, “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.

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

M. Khodaei, H.Jin, and P. Papadimitratos
Networked Systems Security Group (NSS)
www.ee.kth.se/nss

In IEEE Transactions on
Intelligent Transportation Systems
(April 2018)