VeSPA: Vehicular Security and Privacy-preserving architecture

N. Alexiou M. Laganà S. Gisdakis
M. Khodaei P. Papadimitratos

School of Electrical Engineering, KTH, Sweden
surname@kth.se

HotWiSec13'

April 19, 2013

Table of Contents

Vehicular Communications

- Vehicular Communications (VC)
- Vehicles propagate information for Safe-Driving
  - Location, Velocity, angle
  - Hazardous warnings
  - Emergency break etc.
- Cooperative awareness through beaconed status messages and event-triggered warnings
- ..Security in VC?
  - Assure legitimate vehicles propagate information
  - Secure integrity of information

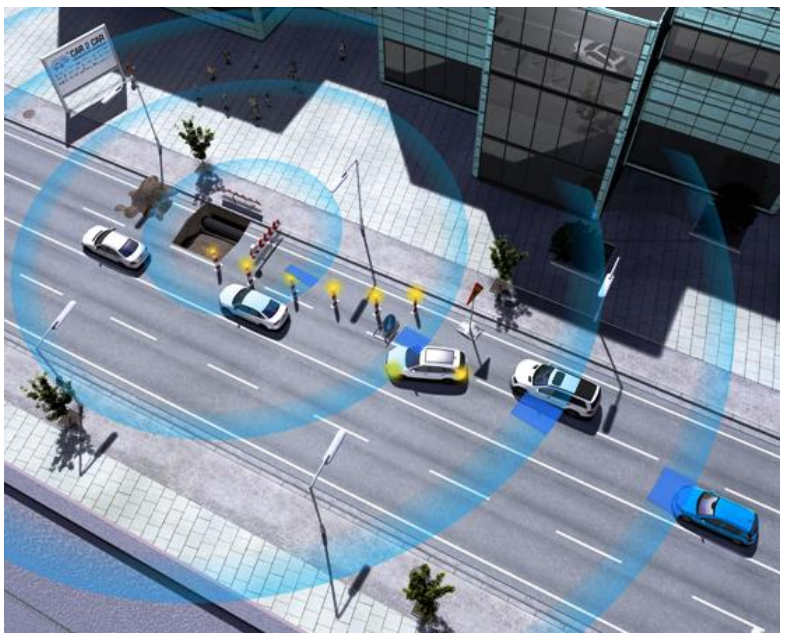


Image source: C2C-CC

Digital Signatures for VC

- Vehicles hold Private-Public Key pair
- Unique pair to each vehicle
- Digital Signature of the messages
  - Authentication
  - Integrity
  - Non-repudiation
- Vehicular Public Key Infrastructure (VPKI)
  - To assign credentials
  - Propagate trust

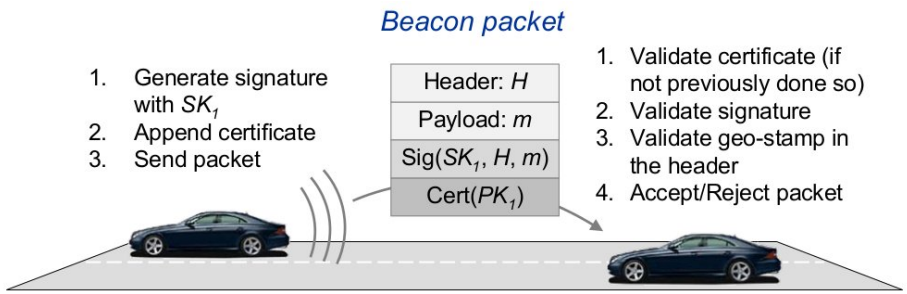
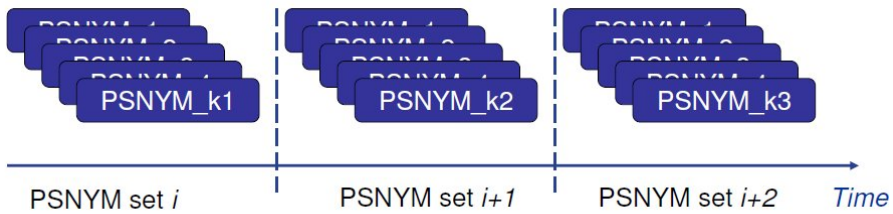
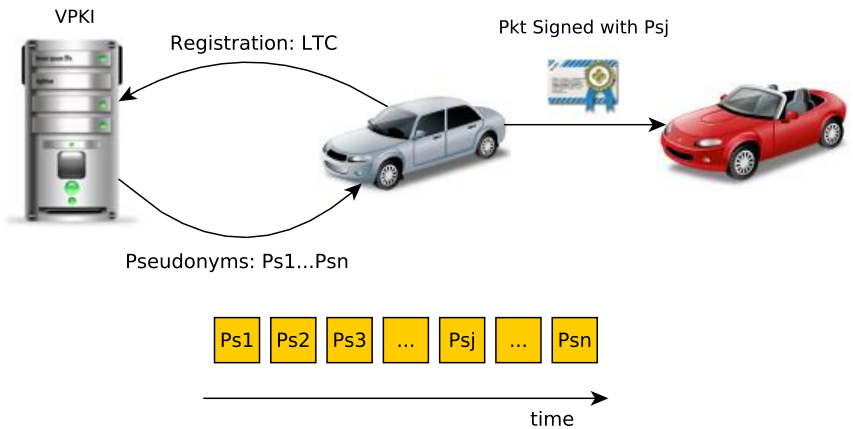


Image Source: Secure Vehicular Communication Systems: Design and Architecture, P. Papadimitratos et al

Privacy in VC

- Packets signed using same credentials can be trivially linked
- Solution:
  - Offer multiple short-lived credentials (Pseudonyms (PS))
  - Pseudonyms valid for unique time periods
  - Sign packets with valid pseudonyms
  - Cryptographic operations in a Hardware Security Module
- Extend the VPKI to support Pseudonyms





Current Status: Overview

- Credential management in Vehicular Communications (VC)
  - Long-term Credentials for accountability and Authentication
  - Short-lived Pseudonyms for anonymity and Location Privacy
  - A VPKI to support credential management
- VPKI Architecture:
  - **LTCA:** Issuer of Long-term Credentials
  - **PCA:** Issuer of Pseudonymous Credentials
  - **RA:** Resolution Authority
- VPKI Protocols:
  - Pseudonym provision: Refresh pool of pseudonyms
  - Pseudonym Resolution: De-anonymize misbehaving vehicles
    - Car accident, violation of traffic regulation, police request
  - Pseudonym revocation: Revoke the misbehaving pseudonyms
- Main Suspects: SEVECOM, C2C-CC, PRESERVE, 1609 family of standards WAVE, ETSI

Table of Contents

Future Challenges for VC

- Implement an efficient VPKI prototype according to the standard
- How to enhance privacy towards the infrastructure
- Envision support for future vehicular services
  - Safety as a service, not the target application
  - Location based services, Pay-as-you-drive systems
  - Enhance current VPKI to support vehicular services
  - AAA solution with current VPKI architecture as the starting point
    - **Authentication:** Legitimate part of the system
    - **Authorization:** Right to access a service
    - **Accountability:** Track of consumption

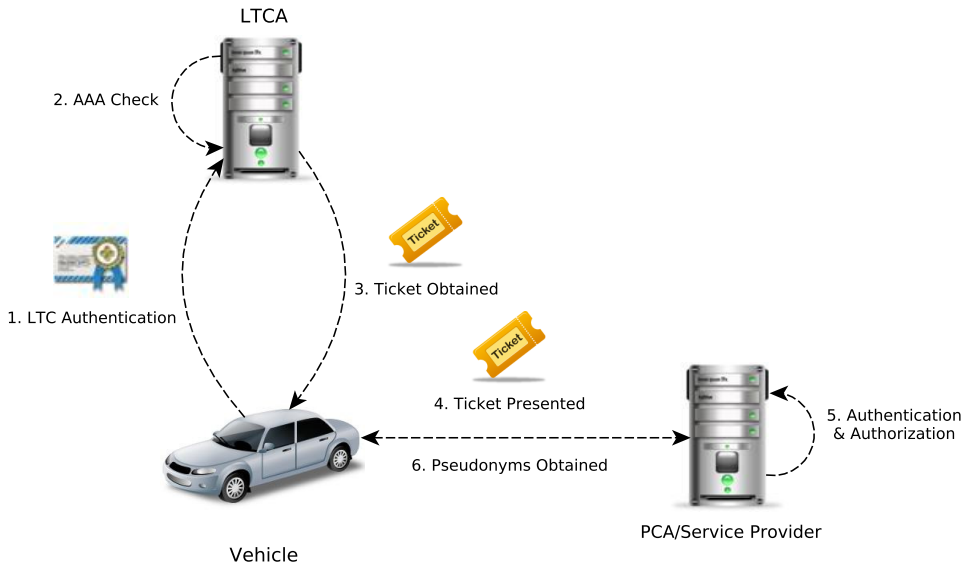
Table of Contents

VeSPA: Vehicular Security and Privacy-preserving Architecture

- *"Kerberized"* version of a VPKI
  - Efficient VPKI Credential Management Architecture
  - Enhanced VPKI design with respect to privacy
  - Cryptographic **tickets** to support AAA
- Tickets:
  - $tkt = Sig_{\mathrm{LTCA}}([t_e], \{S_1\}, \ldots, \{S_n\})$
  - Carrier of service subscription information
  - Anonymous proof of access to obtain pseudonyms
  - Authorization and Authentication to the PCA
  - Limited lifetime dependent on vehicle subscription to the service
  - Revocable upon misbehavior

VeSPA: Operation

- AAA check at LTCA
  - LTCA issues ticket
  - $73,5 msec$/ticket
- Ticket per service/access
  - Increased anonymity set
  - Low overhead introduced
- Ticket received
  - Request for new pseudonyms
- Communication over TLS (one-way authentication)



VeSPA: Protocols

Pseudonym Provision:

- $V \longrightarrow LTCA$: $Sig_{k_v}(t_1, \text{Request}) \parallel LT_v$
- $LTCA \longrightarrow V$: tkt
- $V \longrightarrow PCA$: $t_3, tkt, \{K_v^1, \ldots, K_v^n\}$
- $PCA \longrightarrow V$: $t_4, \{Ps_v^1, \ldots, Ps_v^n\}$

Resolution Protocol:

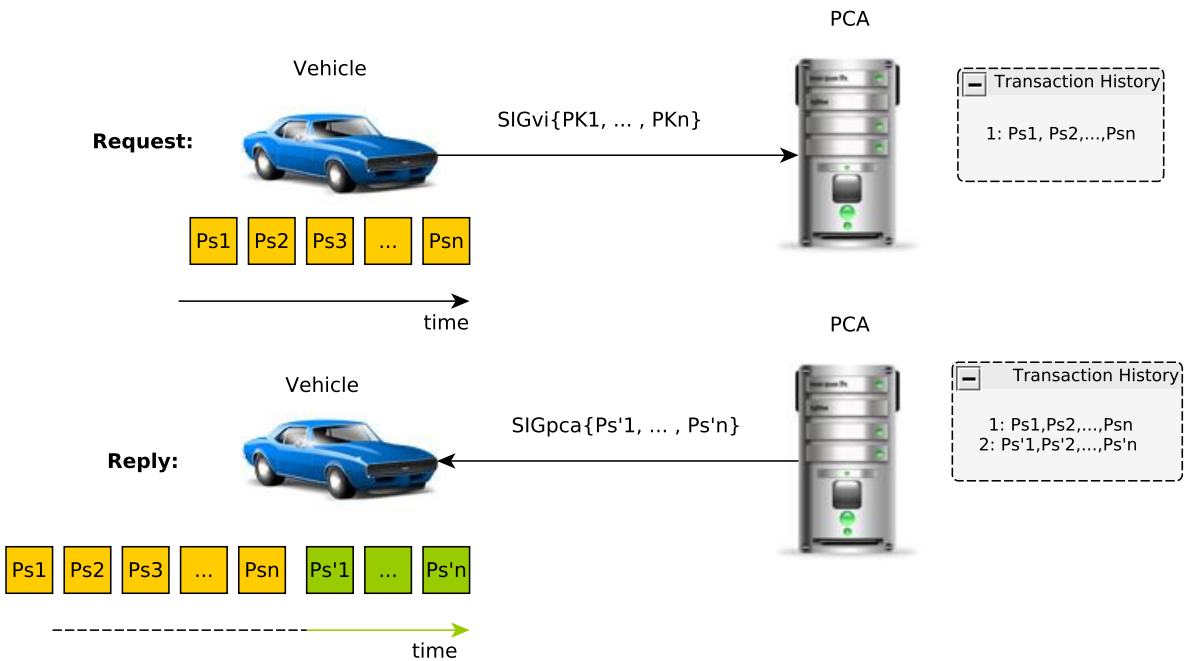
- $RA \longrightarrow PCA$: $Sig_{\text{RA}}(P_v^i, t_1)$
- $PCA \longrightarrow RA$: $Sig_{\text{PCA}}(tkt, t_2)$
- $RA \longrightarrow LTCA$: $Sig_{\text{RA}}(tkt, t_3)$
- $LTCA \longrightarrow RA$: $Sig_{\text{LTCA}}(LT_v, t_4)$

Table of Contents

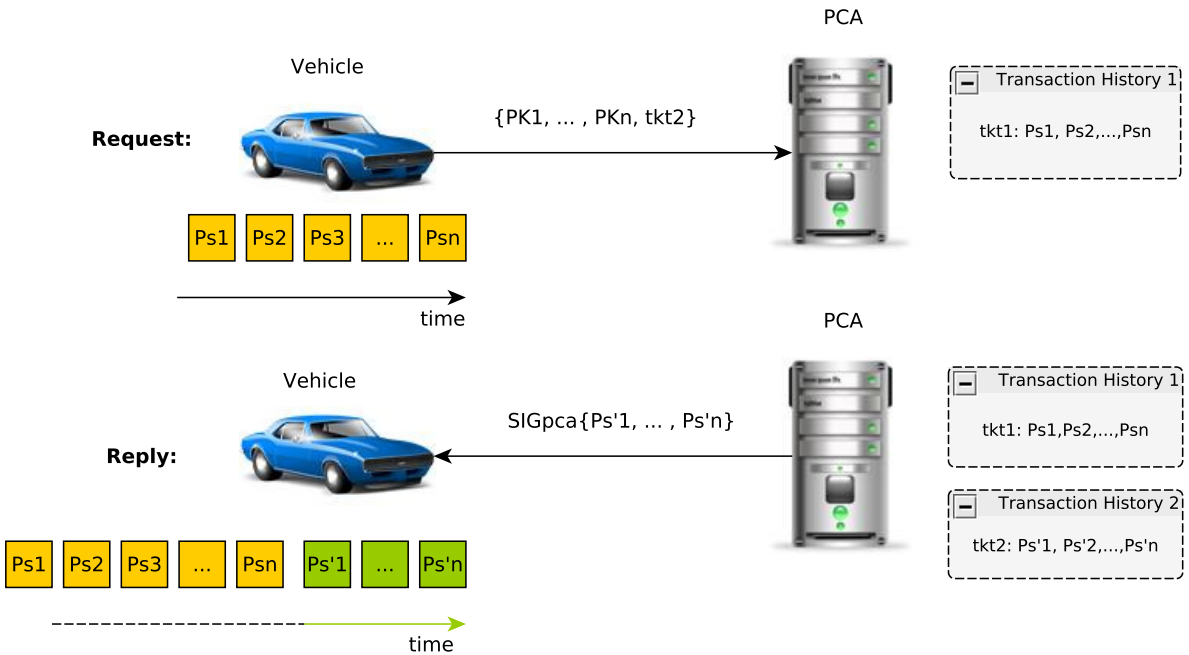
Implementation Details

- OpenCA for cryptographic operations
- ECC-256 keys for digital certificates
- 1609.2 standard compatible
- Separate machines for each entity:
  - Intel Xeon 3.4 GHz, 8 GB RAM
  - System scales up with more machines or..
  - stronger equipment
- Communications over encrypted TLS channel (one-way authentication)
  - Authentication of server
  - Confidentiality

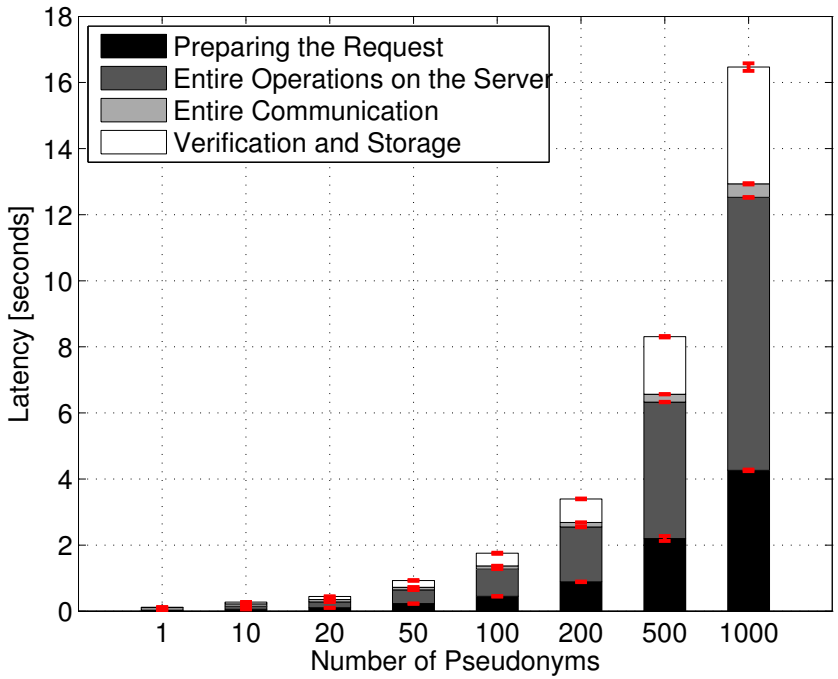
Increased Privacy against the VPKI



Privacy against the Infrastructure

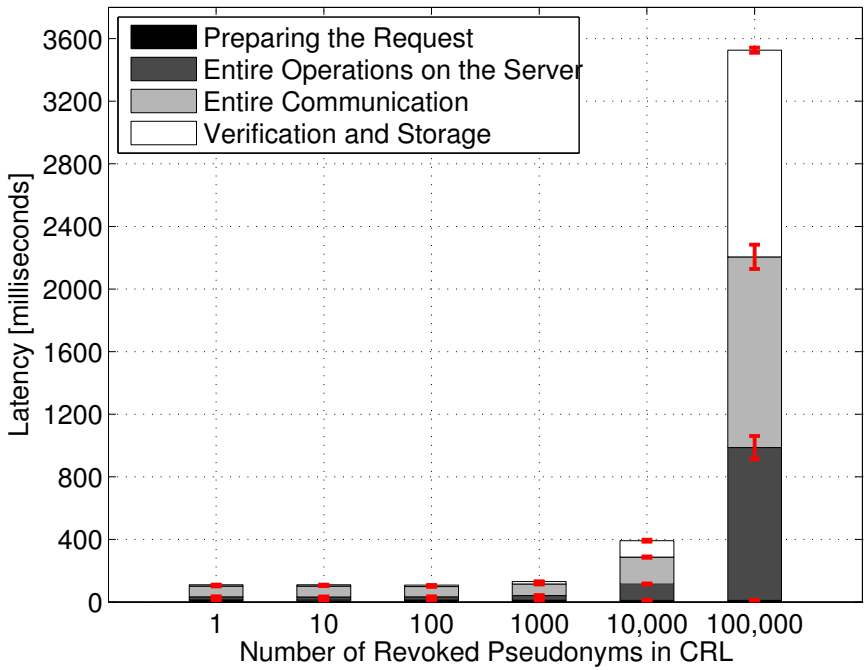


Pseudonym Provision Efficiency



Infrastructure, Vehicle, Communications Efficiency vs number of requested pseudonyms

Pseudonym Revocation Efficiency



Infrastructure, Vehicle, Communications Efficiency vs number of revoked pseudonyms

Table of Contents

Overview & Future Work

VeSPA:

- Efficient VPKI Prototype according to the standards
- Increased Privacy to towards the infrastructure
- Enhanced VPKI with AAA capabilities
- A VPKI able to support vehicular services

Ongoing Work:

- Integration of Anonymous Authentication Mechanisms
- Extensions to support multi-Domain VPKI architectures