Secure Vehicle Communication

SEVECOM Support for Privacy

Gijs Withagen (Technolution), on behalf of
Antonio Kung (Trialog)
25 rue du Général Foy
75008 Paris, France

SE-cure VE-hicle COM-munication

SEVECOM

- Mission: future-proof solution to the problem of V2V/V2I security

- Partners
  - Trialog (Coordinator)
  - DaimlerChrysler
  - Centro Ricerche Fiat
  - Philips
  - Ecole Polytechnique Fédéral de Lausanne
  - University of Ulm
  - Budapest University of Technology and Economics

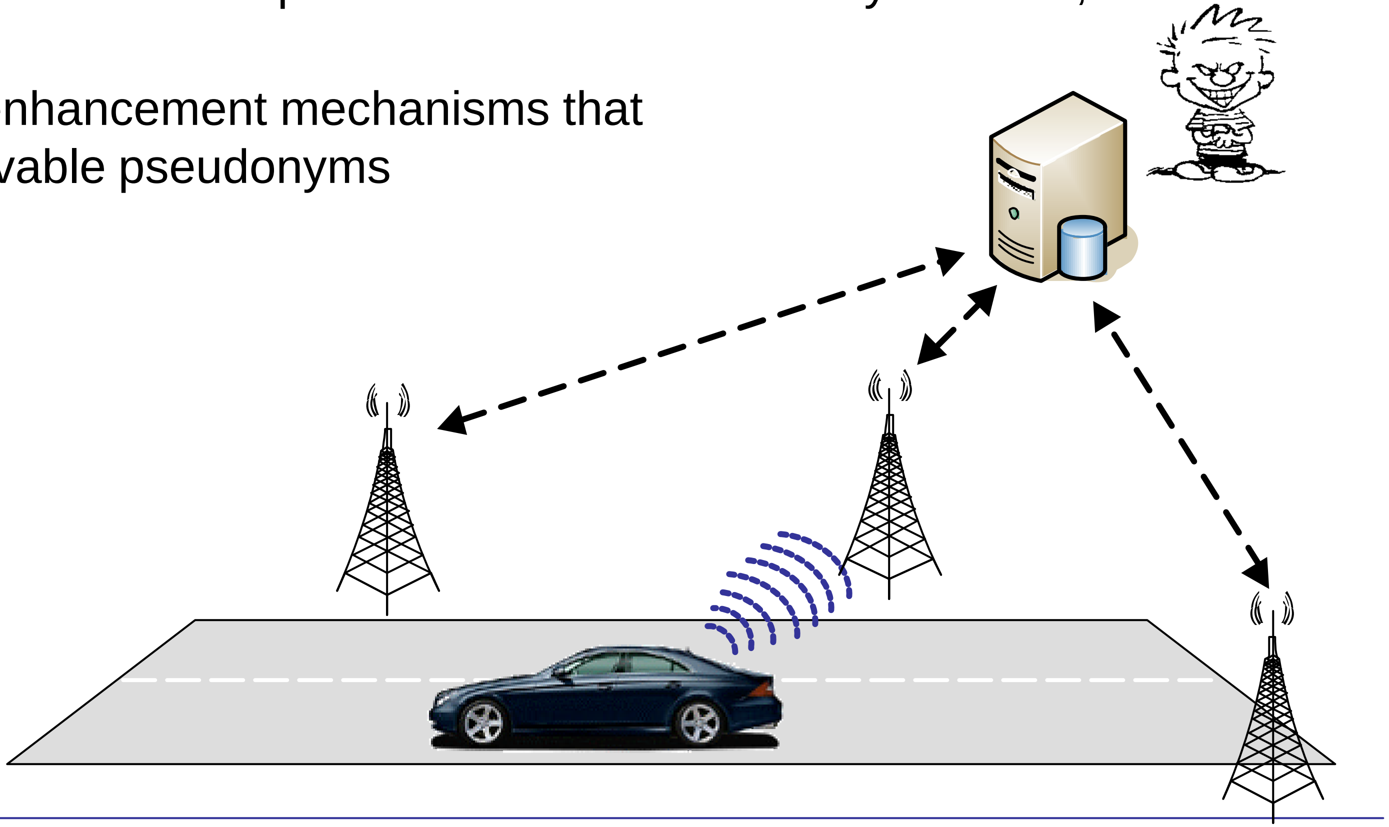
Research topics

	Topic	Scope of work
A1	**Key and identity management**	Fully addressed
A2	**Secure communication protocols (inc. secure routing)**	Fully addressed
A3	**Tamper proof device and decision on cryptosystem**	Fully addressed
A4	Intrusion Detection	Investigation work
A5	Data consistency	Investigation work
A6	**Privacy**	Fully addressed
A7	Secure positioning	Investigation work
A8	Secure user interface	Investigation work

Privacy

- V2V / V2I communication
  - should not make it easier to identify or track vehicles
  - should conform to future privacy directives
- Lack of privacy control will prevent deployment
  - safety applications require information from nearby vehicles, not their identity

➔ Privacy-enhancement mechanisms that use resolvable pseudonyms

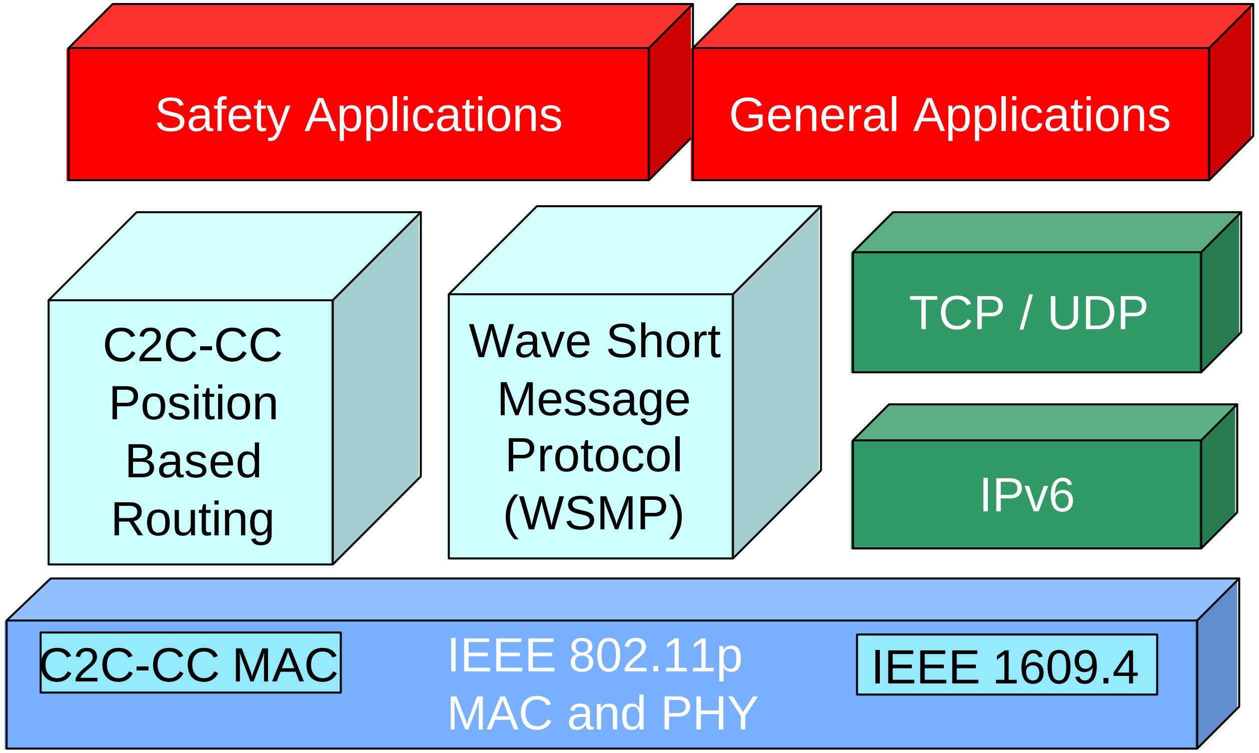


Security Baseline Architecture (cont'd)

- Objectives
  - Focus on communication
  - Baseline Privacy Enhancing Technology (PET)
  - Future dynamic deployment of stronger PETs
    - Analogy: switching from 8 to 10 digit telephone numbers
- Baseline solution design approach
  - Standardized cryptographic primitives
  - Easy-to-implement
  - Low overhead
  - Adaptable protection

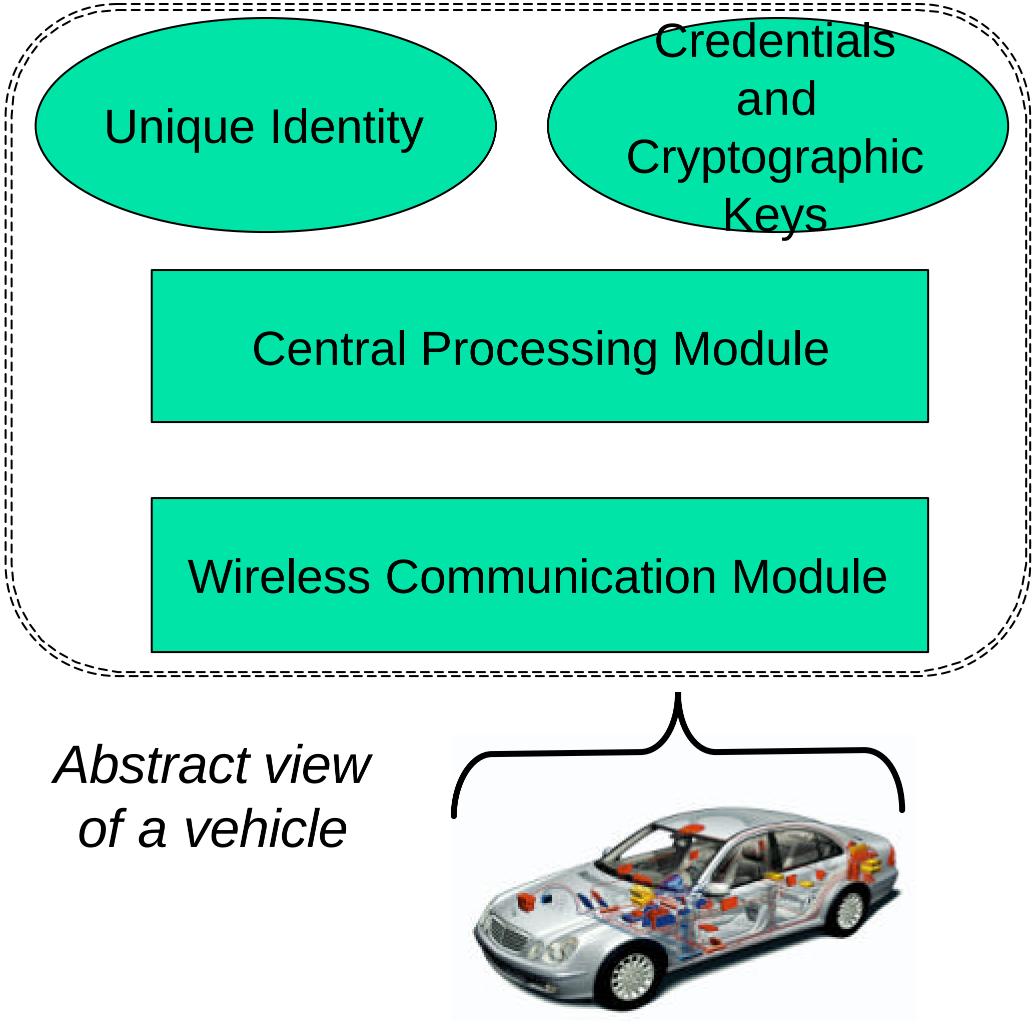
Security Baseline Architecture (cont'd)

- Challenges
  - High rate broadcast communication
  - VANET-only (e.g., safety) and TCP/IP communication



Security Baseline Architecture (cont'd)

- Basic ideas

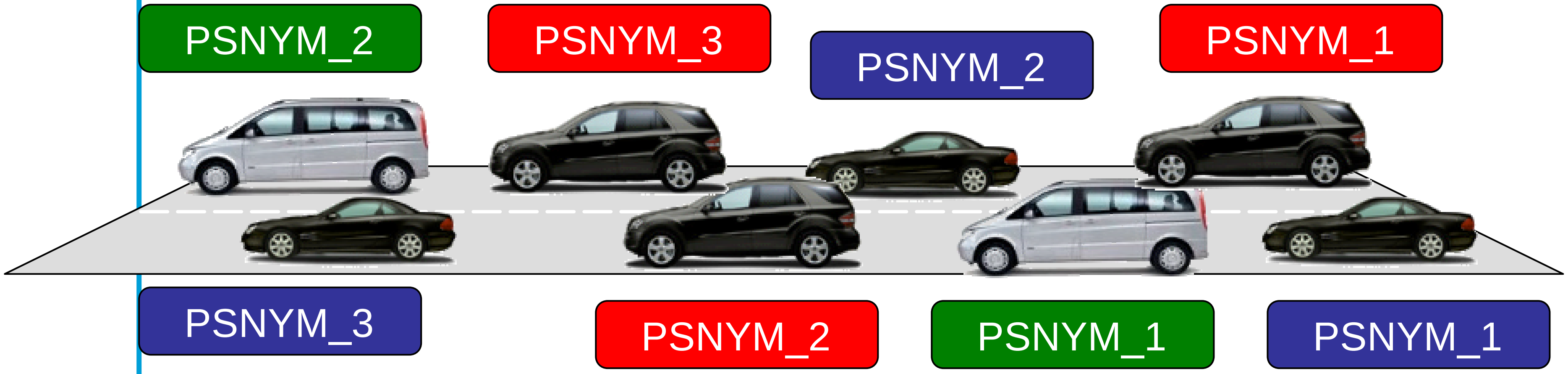

Unique Identity
Credentials and Cryptographic Keys
Central Processing Module
Wireless Communication Module

- **Long-term identity**
- **Public key crypto**
  - *EC-DSA, RSA*
- **Certificates**

Abstract view of a vehicle

Security Baseline Architecture (cont'd)

- Basic ideas (cont'd)
  - **Pseudonym**: Remove all identifying information from certificate
  - Equip vehicles with **multiple** pseudonyms
    - Alternate among pseudonyms over time (and space)
    - Sign message with the private key corresponding to pseudonym
    - Append current pseudonym to signed message

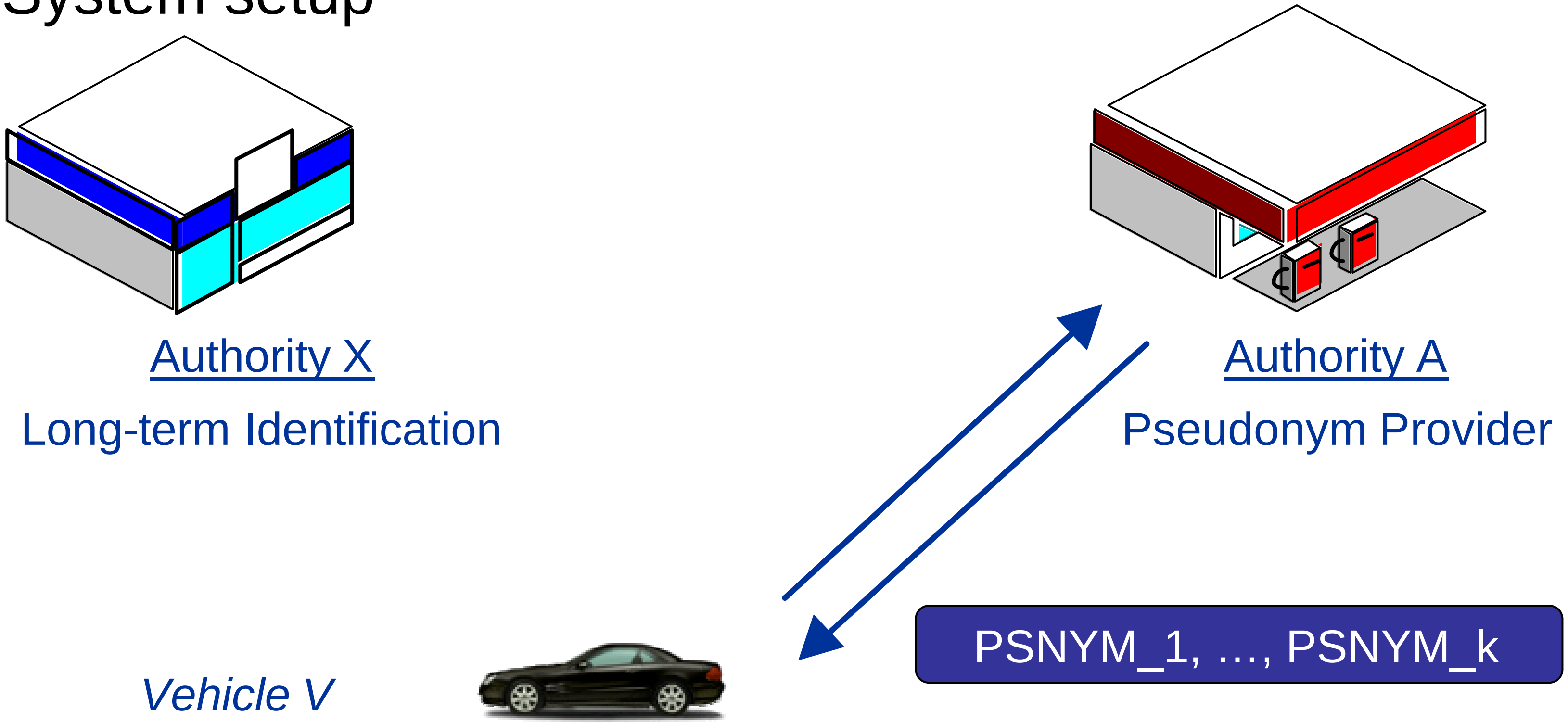


Security Baseline Architecture (cont’d)

- Pseudonym changes over space/time (« region »)
  - identity of a vehicle in a region unknown
  - space size/time duration is a parameter
  - cannot track a vehicle from one region to another
- Service providers can still track a given customer
  - e.g. through a fixed IP V6 address
  - secure tunnel on top of changing pseudonyms and addresses

Security Baseline Architecture (cont’d)

- System setup



Authority X

Long-term Identification

Authority A

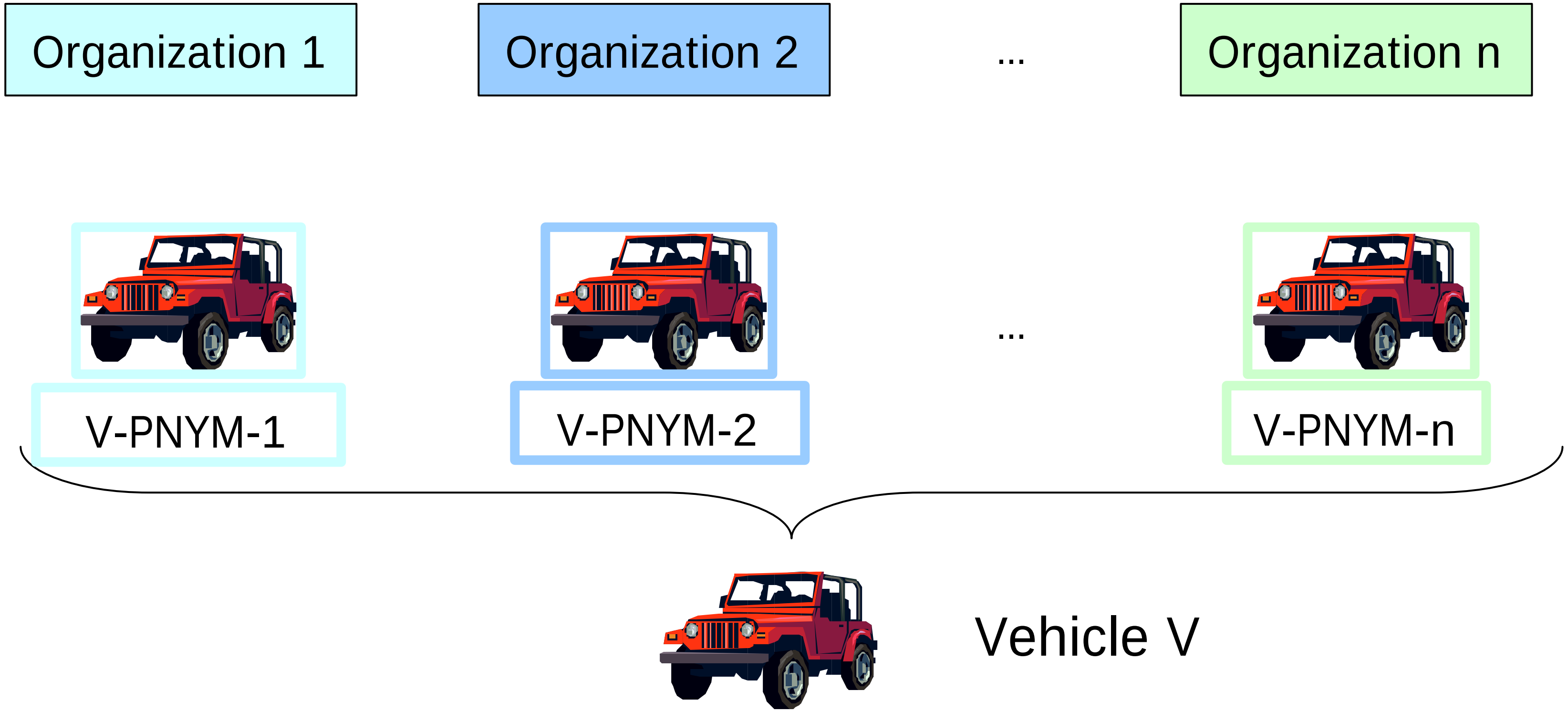
Pseudonym Provider

Vehicle V

PSNYM_1, …, PSNYM_k

Security Baseline Architecture (cont'd)

- System setup (cont'd)
  - Multiple pseudonym providers

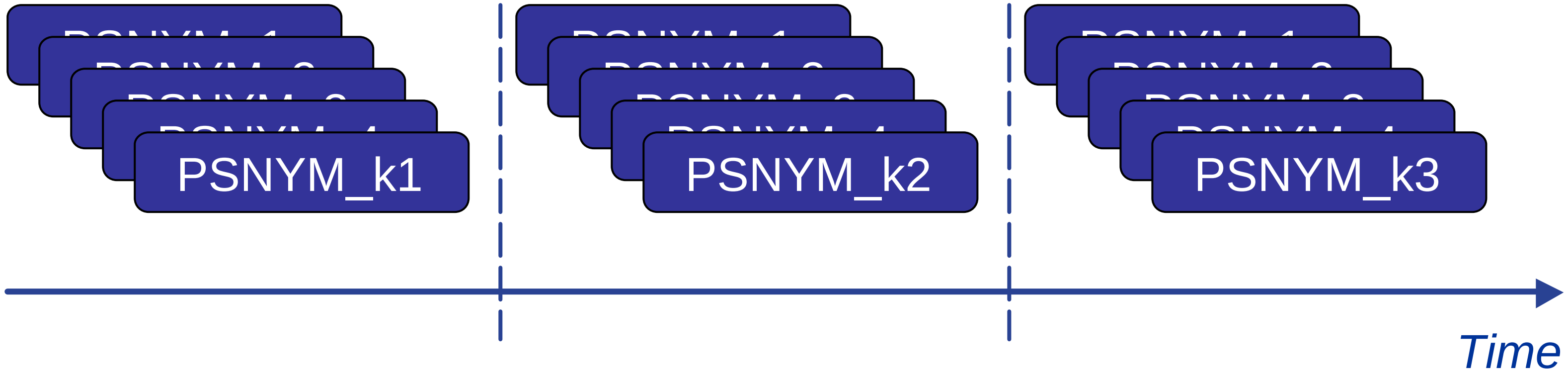


Security Baseline Architecture (cont'd)

- Pseudonym format

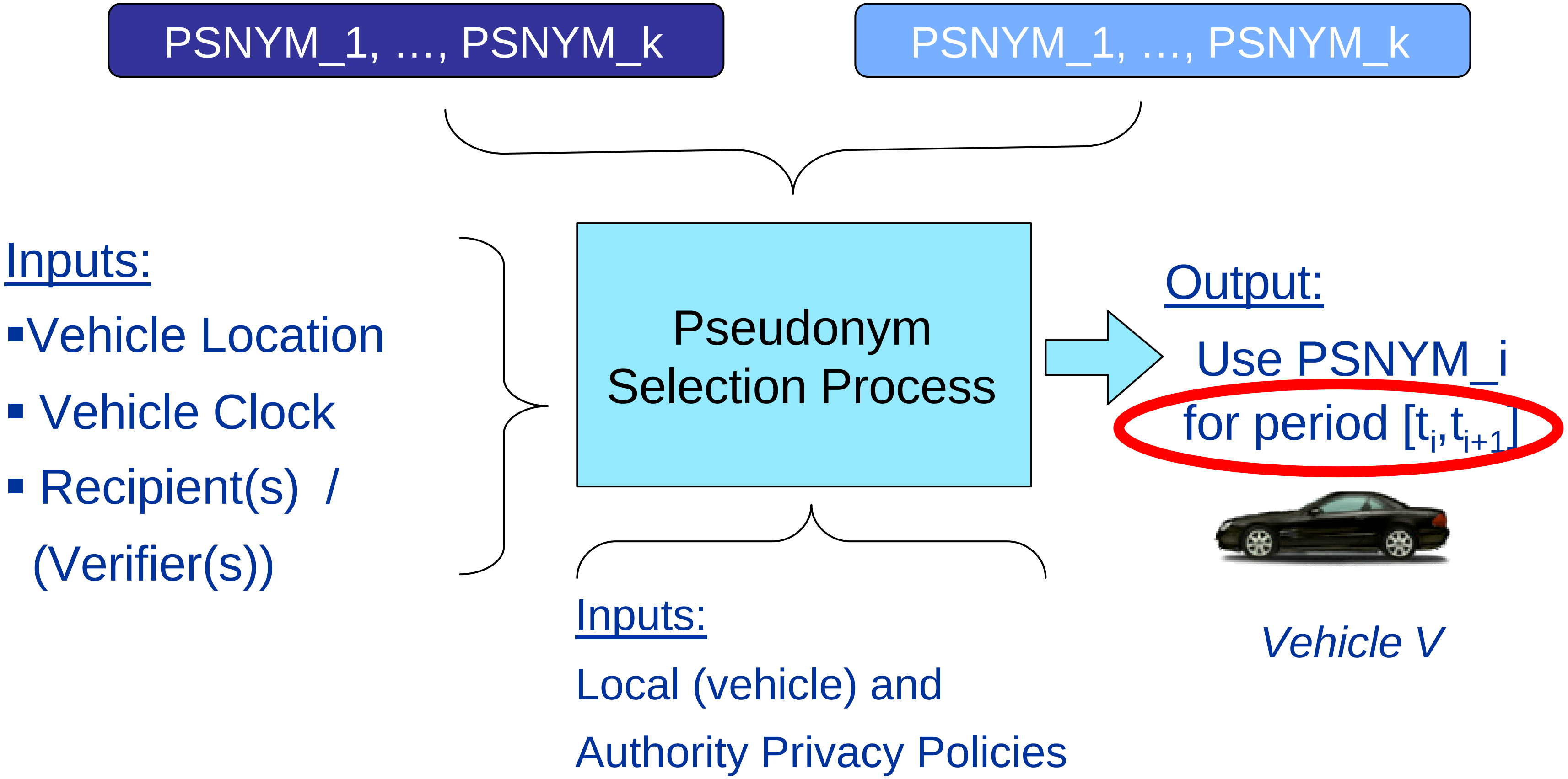
<table>
<tr><td>PSNYM-Provider ID</td><td>PSNYM Lifetime</td></tr>
<tr><td colspan="2">Public Key</td></tr>
<tr><td colspan="2">PSNYM-Provider Signature</td></tr>
</table>

- Supplying vehicles with pseudonyms
  - Sufficient in number
  - Periodic 'refills'



Privacy Baseline Architecture (cont'd)

- Pseudonym Change Mechanism



PSNYM_1, …, PSNYM_k

PSNYM_1, …, PSNYM_k

Inputs:

- Vehicle Location
- Vehicle Clock
- Recipient(s) / (Verifier(s))

Pseudonym Selection Process

Output:

Use PSNYM_i for period $[t_i, t_{i+1}]$

Vehicle V

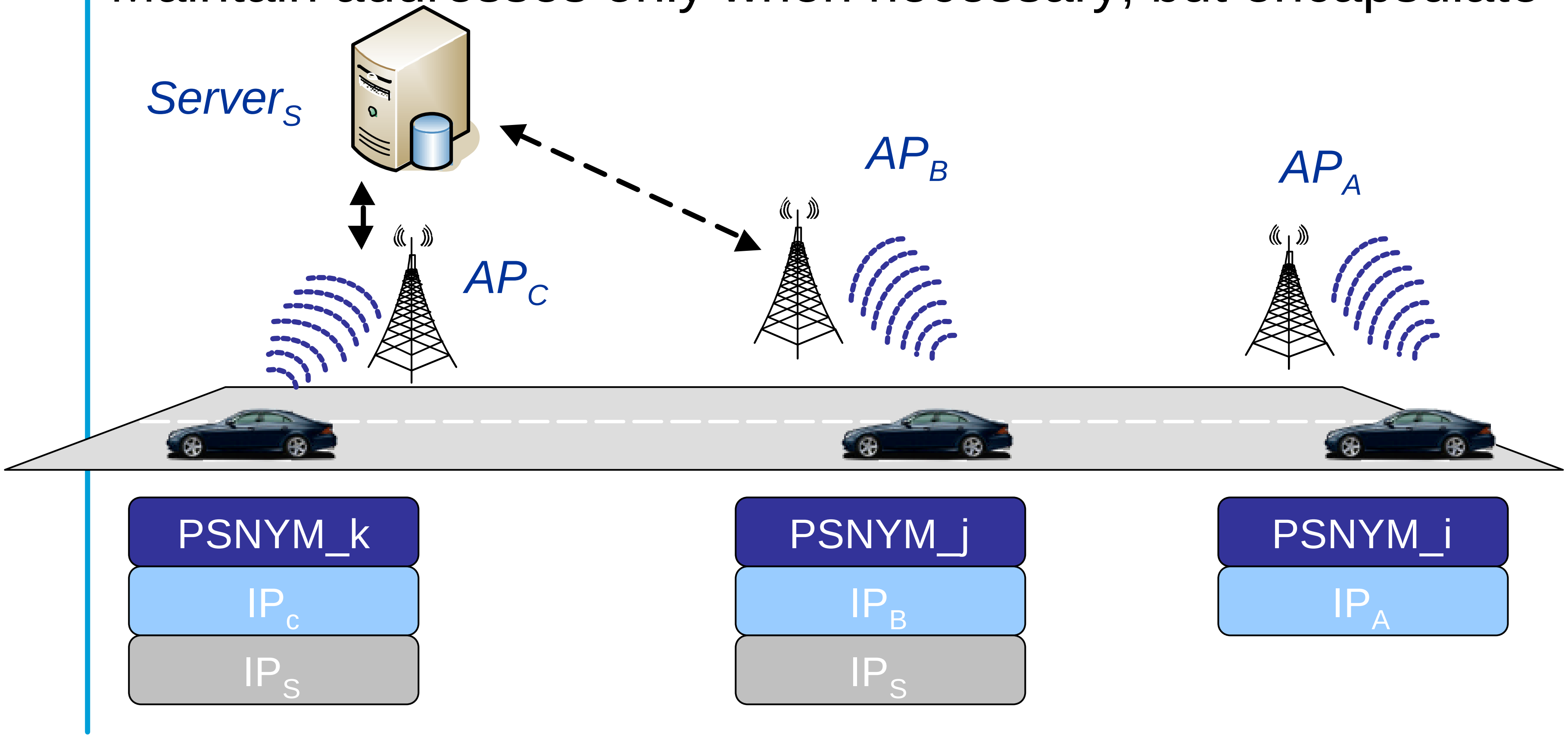
Inputs:

Local (vehicle) and Authority Privacy Policies

- *One pseudonym per day (?)*
- *One per transaction (?)*

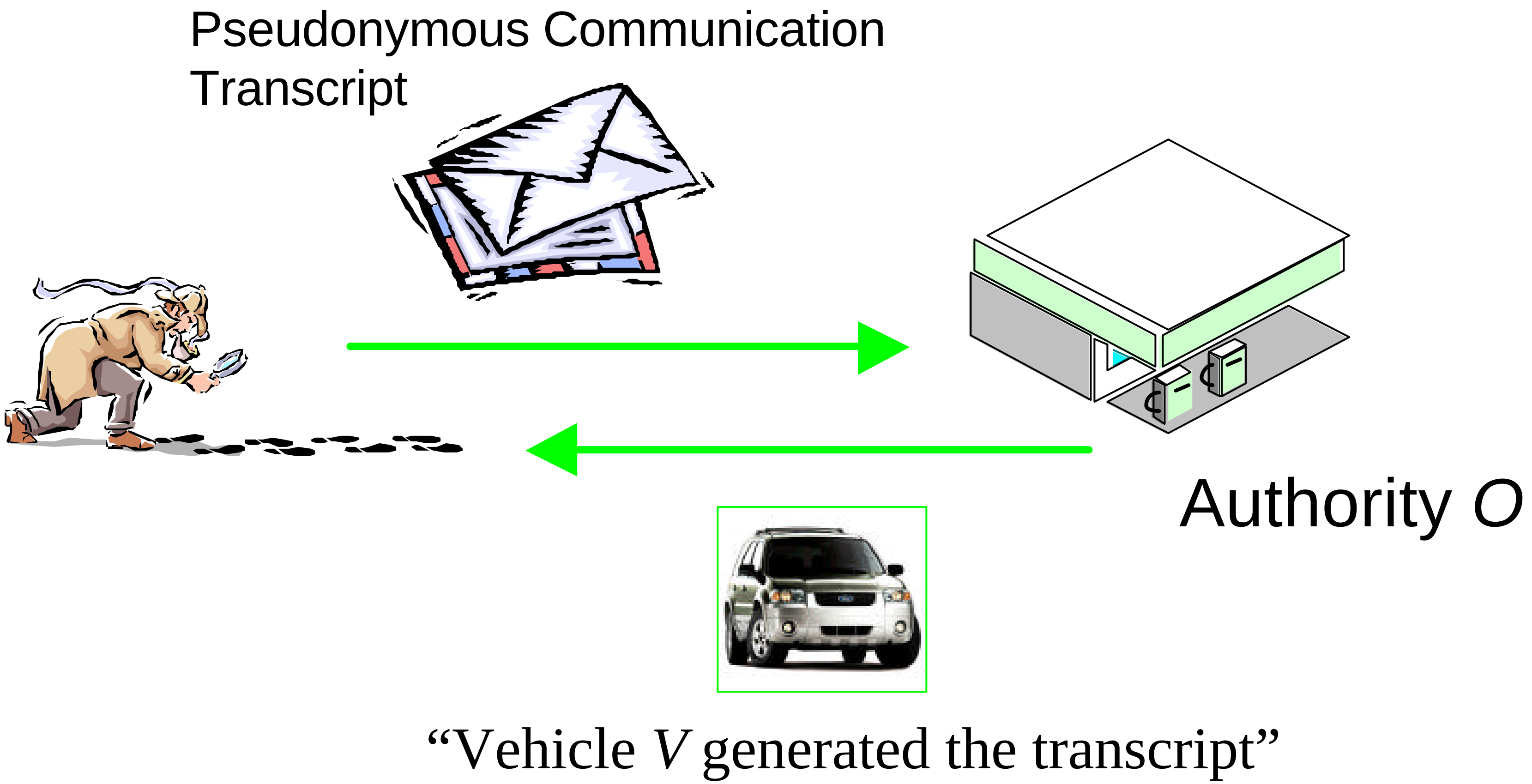
Privacy Baseline Architecture (cont'd)

- Other vehicle network identifiers: e.g., IP and MAC addresses
- Change addresses along with pseudonyms
- Maintain addresses only when necessary, but encapsulate



Privacy Baseline Architecture (cont'd)

- Pseudonym resolution



Pseudonymous Communication Transcript

Authority *O*

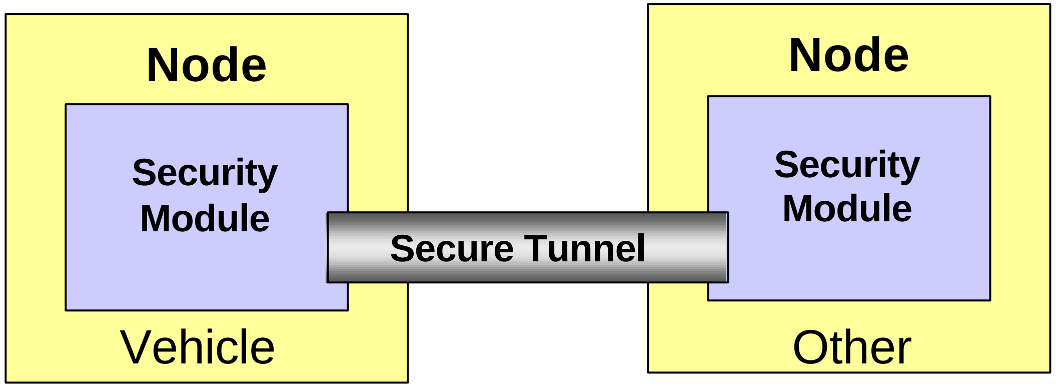
"Vehicle *V* generated the transcript"

Privacy Baseline Architecture (cont'd)

- Baseline Solution
  - Well-accepted building blocks (e.g., cryptographic primitives) and concepts (e.g., anonymized certificates/pseudonyms)
  - Adaptation to enhance protection
- Investigation of alternative techniques
  - 'Newer' cryptography
- Flexible Security Architecture
  - Plug-in stronger privacy enhancing technology

Coordination and Implementation

- Discussion with CVIS
  - Psnym change management specification
  - Need for meeting
- Reuse of CVIS reference platform
  - Need for contact point
- Reuse of GST SEC Secure communication engine
  - secure tunnels
    - Insecure
    - Authenticated
    - Confidential
    - Secure
  - security modules



Security Working Groups

- C2C Security Working Group
  - Dr H.J Voegel, BMW

White Paper
Baseline Architecture

- COMeSafety IST project
  - Dr T.Kosch, BMW

Impact of Security to eSafety Architecture

- eSafety forum Security WG
  - Antonio Kung, Trialog
  - Prof. Ruland, Siegen U.

Code of Practice for Data Protection Recommendations

Secure Vehicle Communication

SEVECOM

Thank You

www.sevecom.org