Secure Vehicle Communication

SEVECOM

Towards a Secure Vehicle to Vehicle and to Intrastructure Communication : the SEVECOM project

Antonio Kung (Trialog)

TRIALOG

eSafety

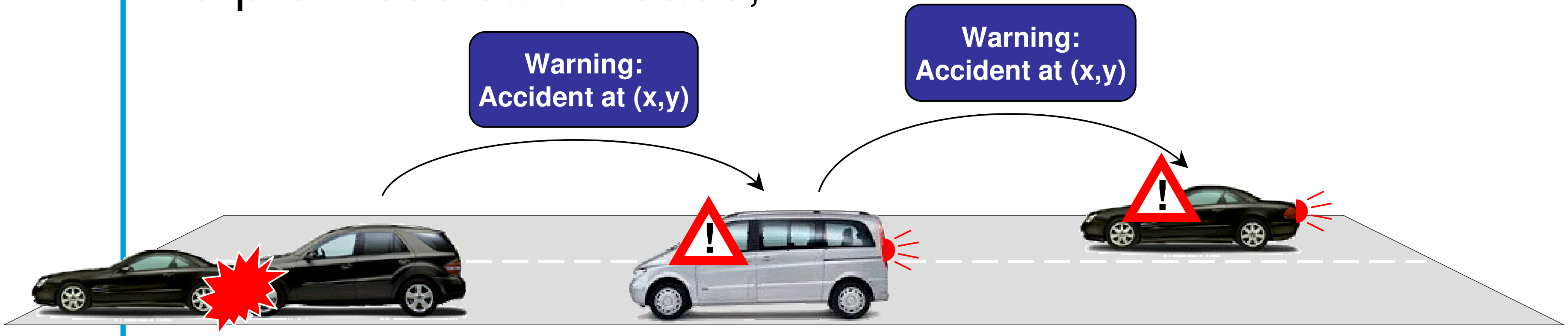
Information Society and Media

Outline

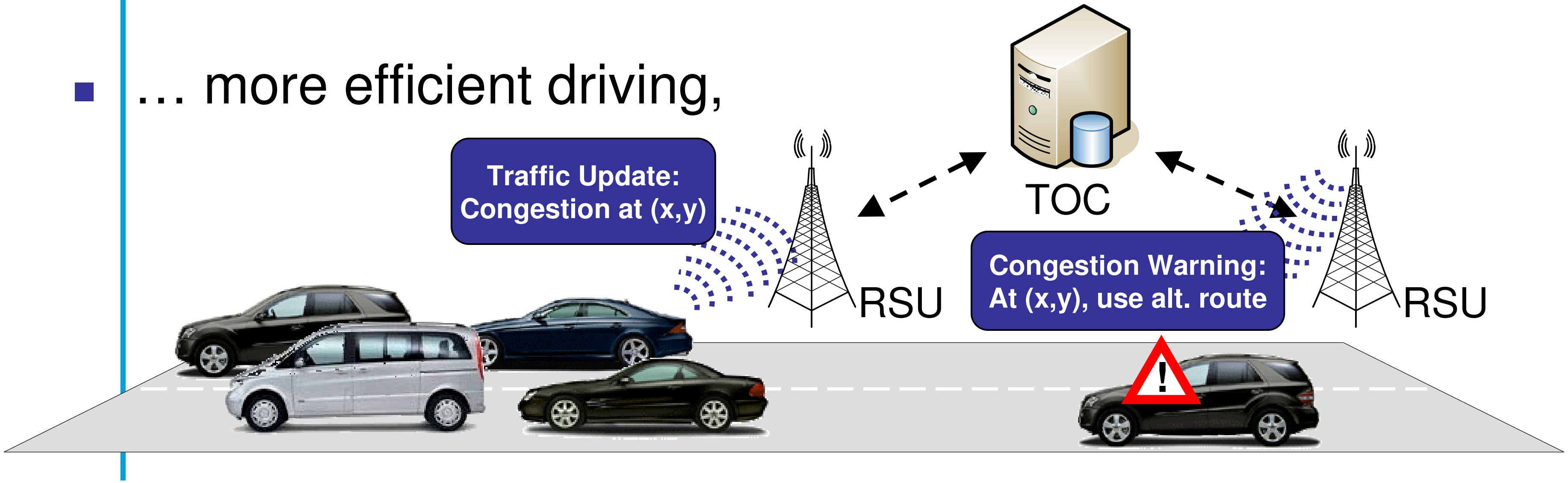
- Brief presentation of Sevecom
- Sevecom Baseline Architecture for Privacy
- Other Working Groups

Vehicle Communication (VC)

- VC promises safer roads,

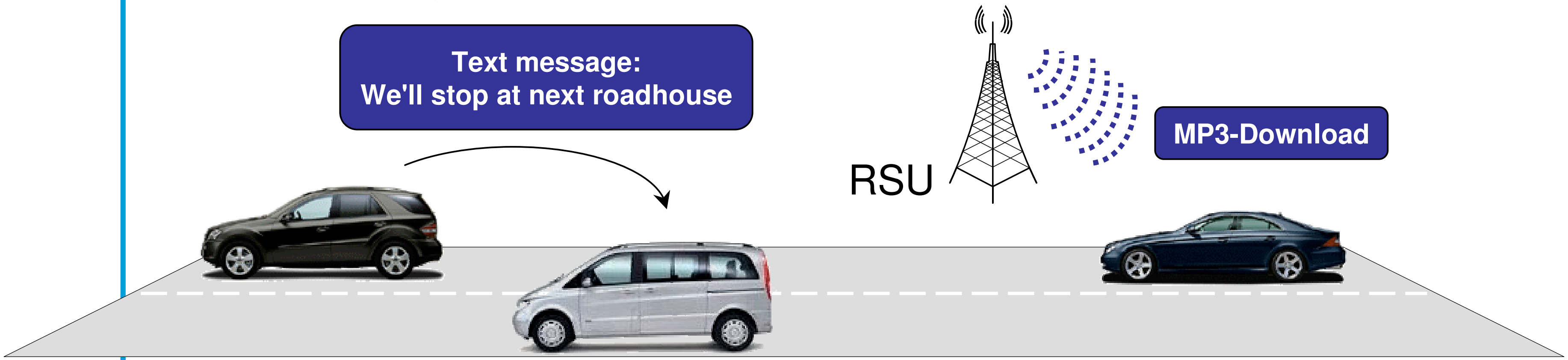


- … more efficient driving,

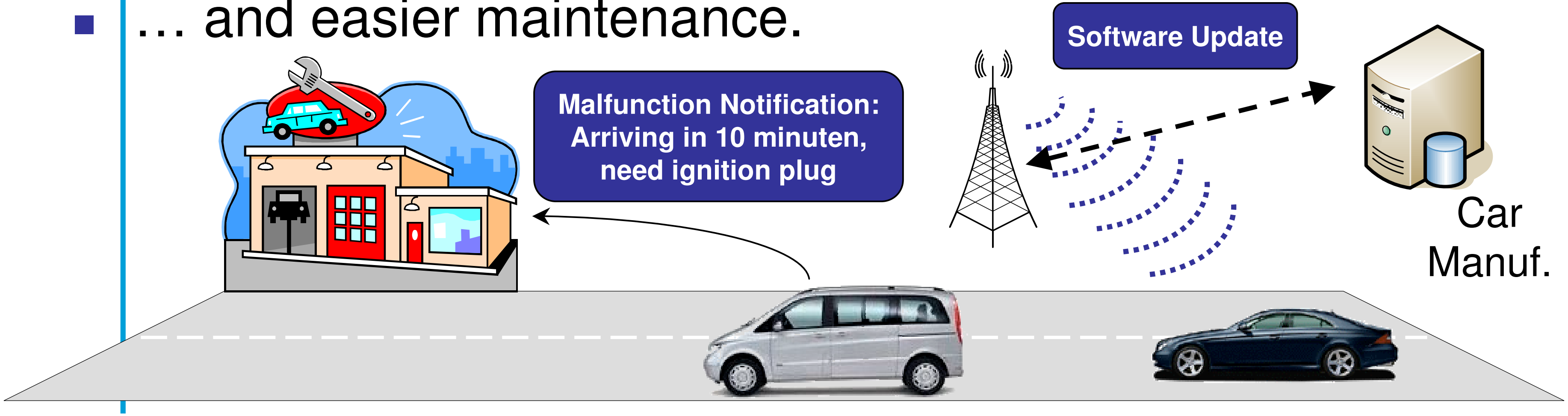


Vehicle Communication (VC)

- … more fun,



- … and easier maintenance.

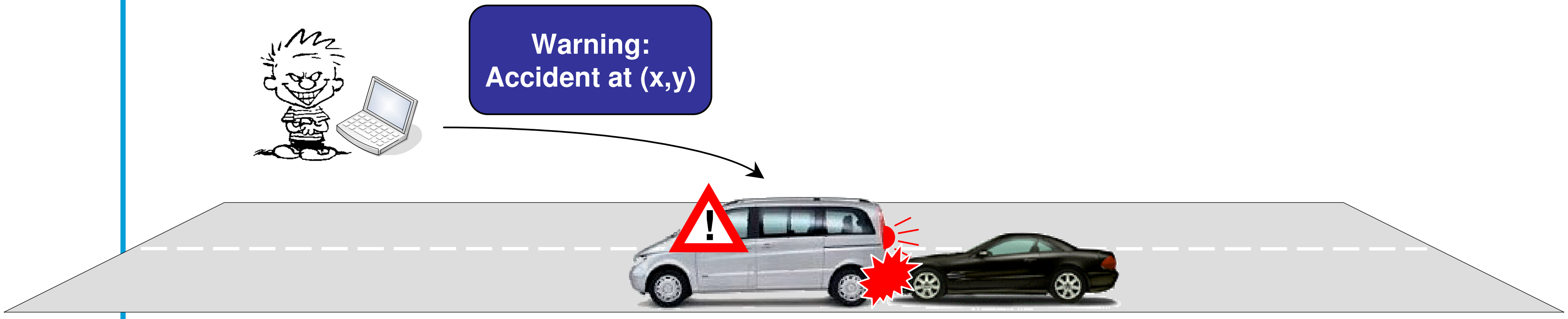


Sounds good

BUT ...

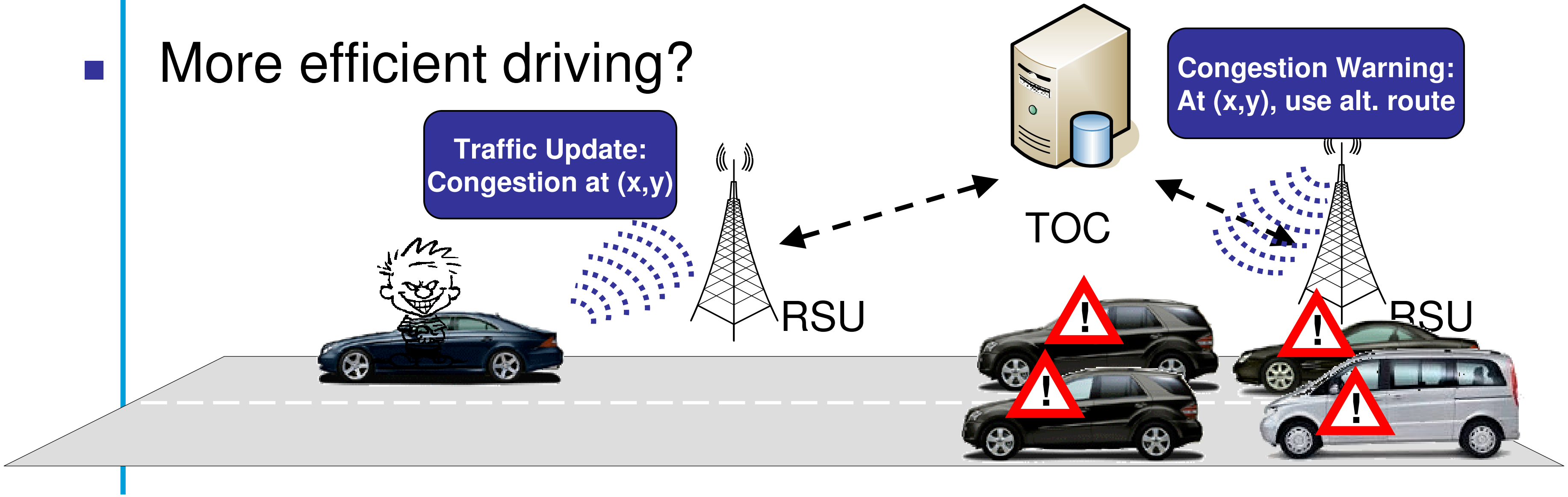
Security and Privacy???

- Safer roads?



Warning:
Accident at (x,y)

- More efficient driving?

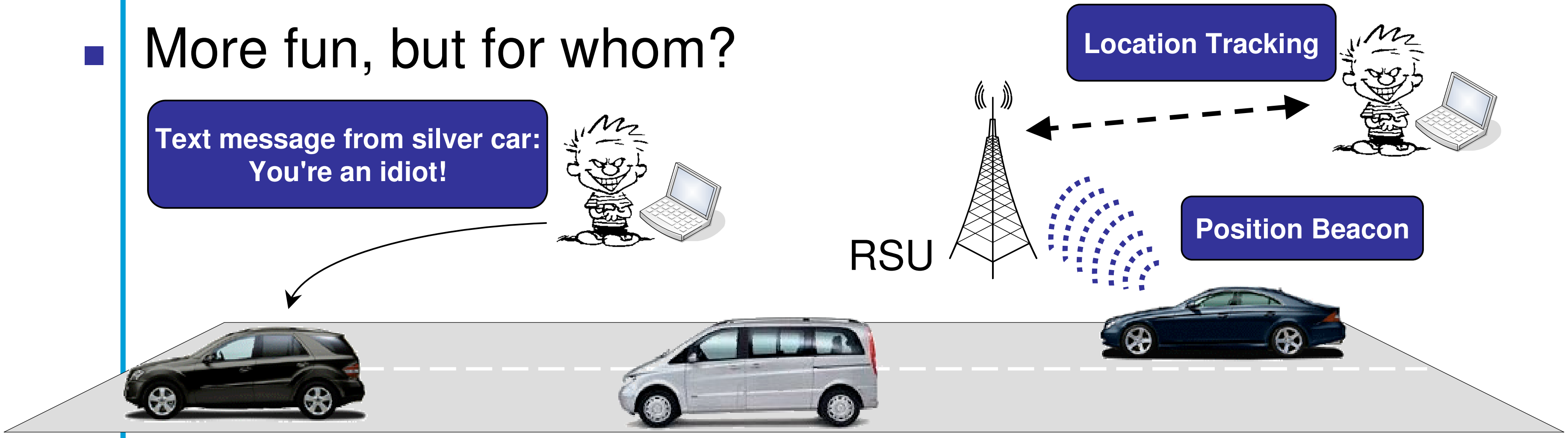


Traffic Update:
Congestion at (x,y)

Congestion Warning:
At (x,y), use alt. route

Security and Privacy???

- More fun, but for whom?

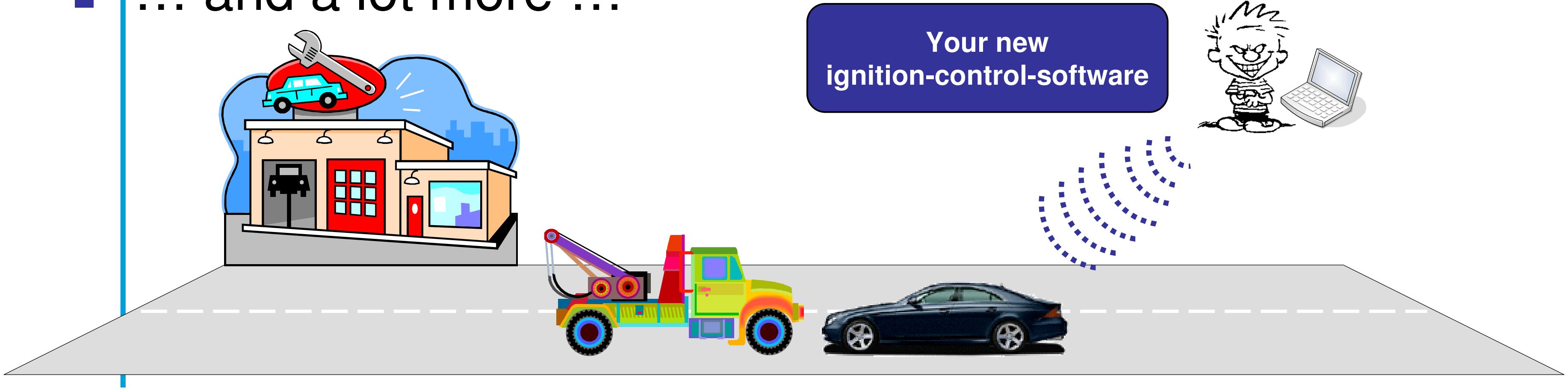


Text message from silver car: You're an idiot!

Location Tracking

Position Beacon

- … and a lot more …



Your new ignition-control-software

SE-cure VE-hicle COM-munication

- 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

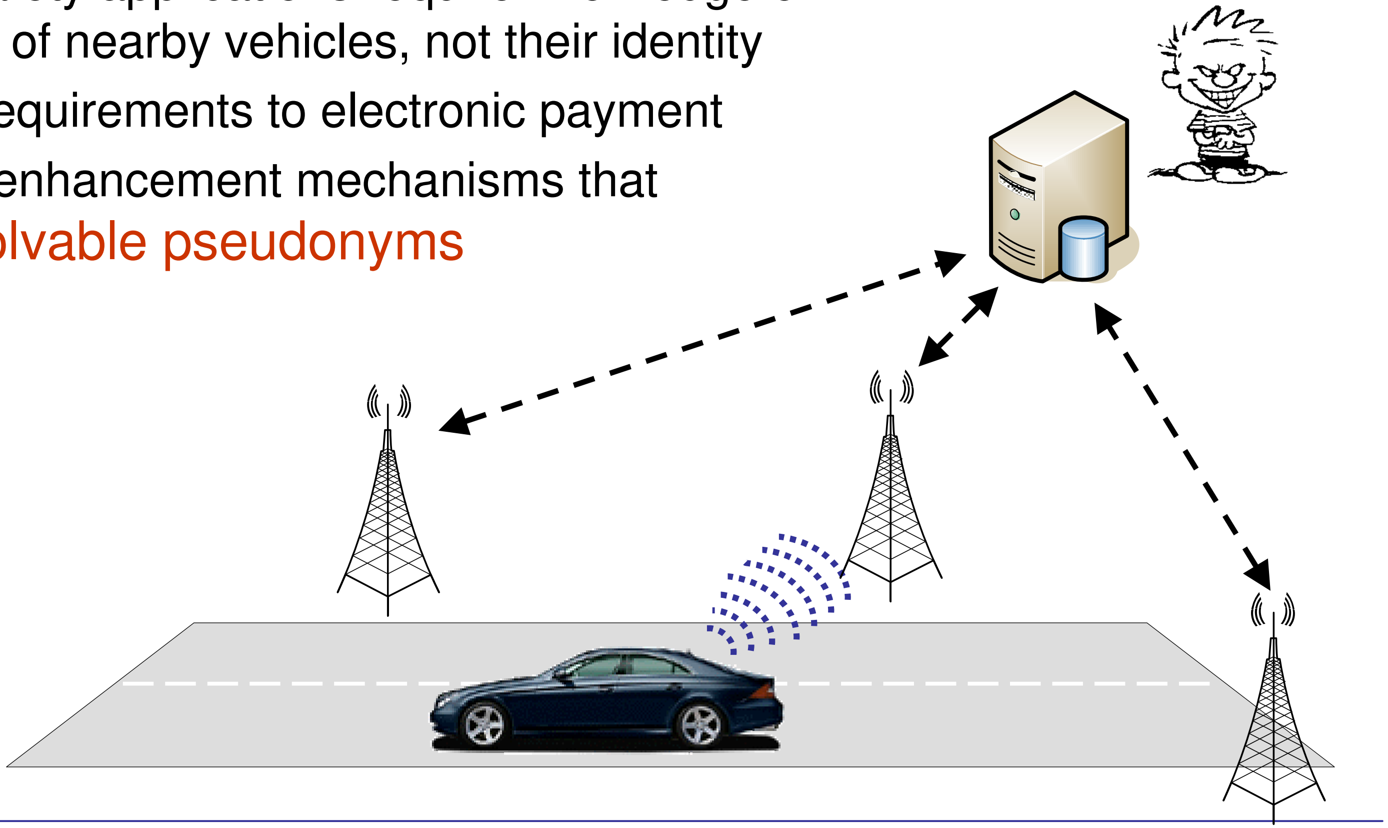
Research topics

	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

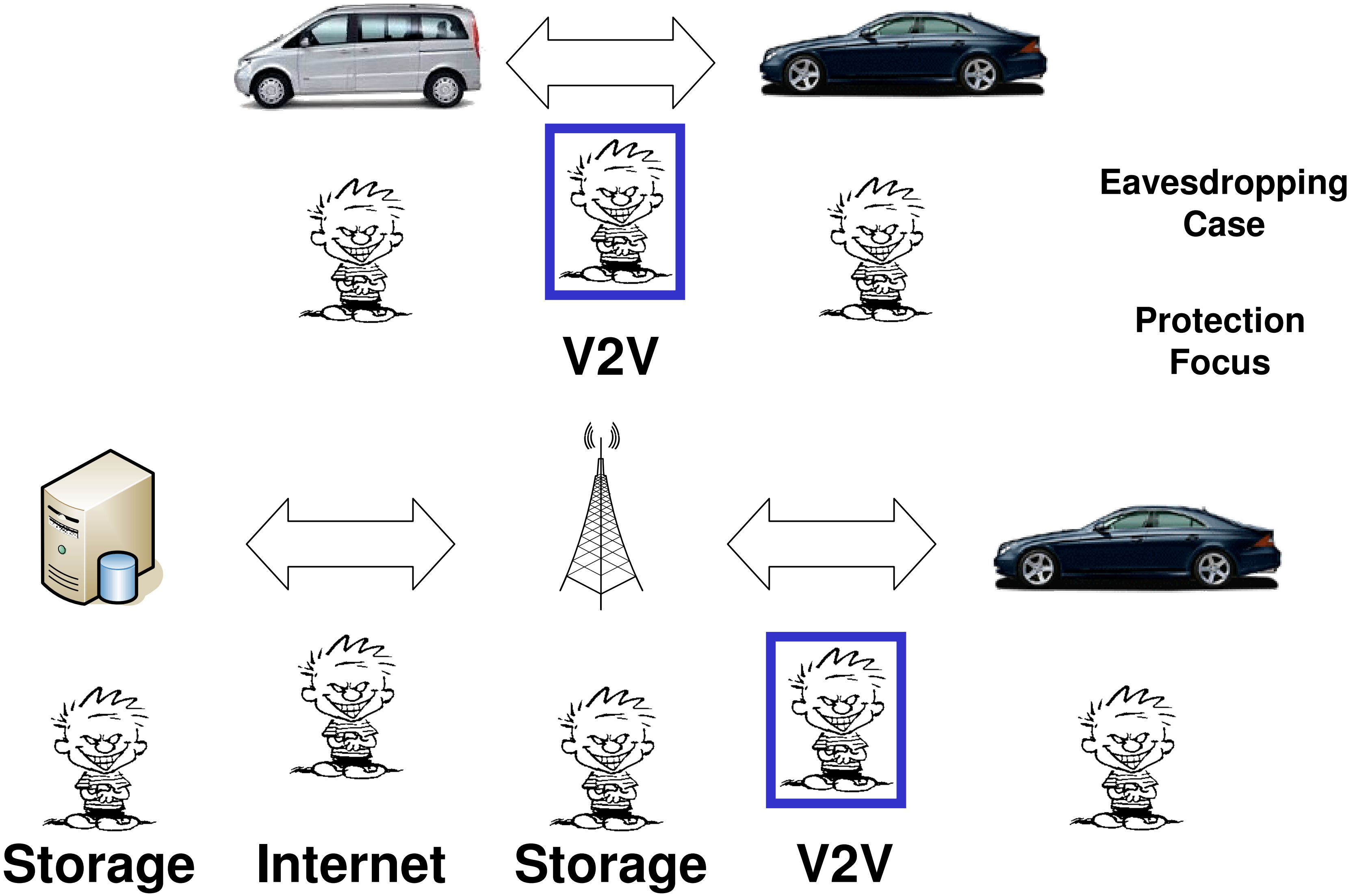
Privacy

- 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
  - Active safety applications require knowledge on activities of nearby vehicles, not their identity
  - Similar requirements to electronic payment

  ➔ Privacy-enhancement mechanisms that use resolvable pseudonyms



Sevecom Privacy focus



V2V

Eavesdropping Case

Protection Focus

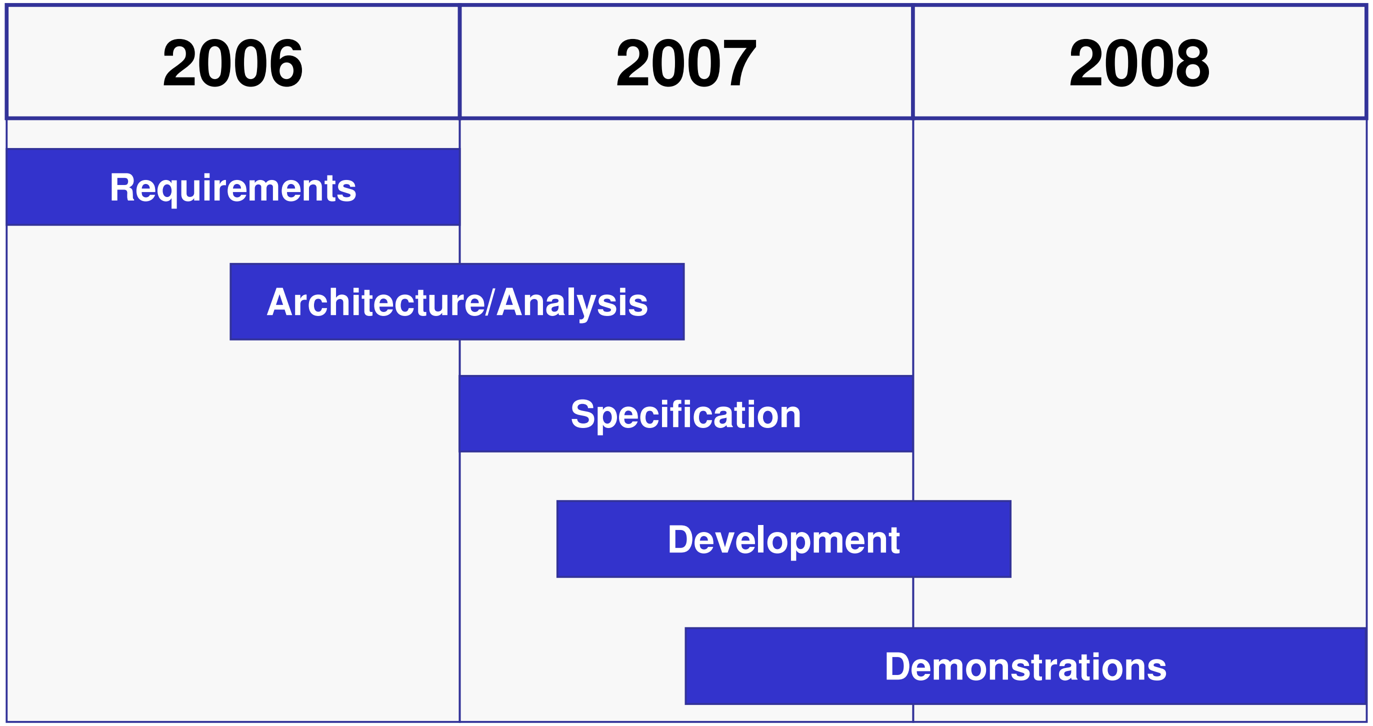
Storage

Internet

Storage

V2V

Timetable



2006

2007

2008

Requirements

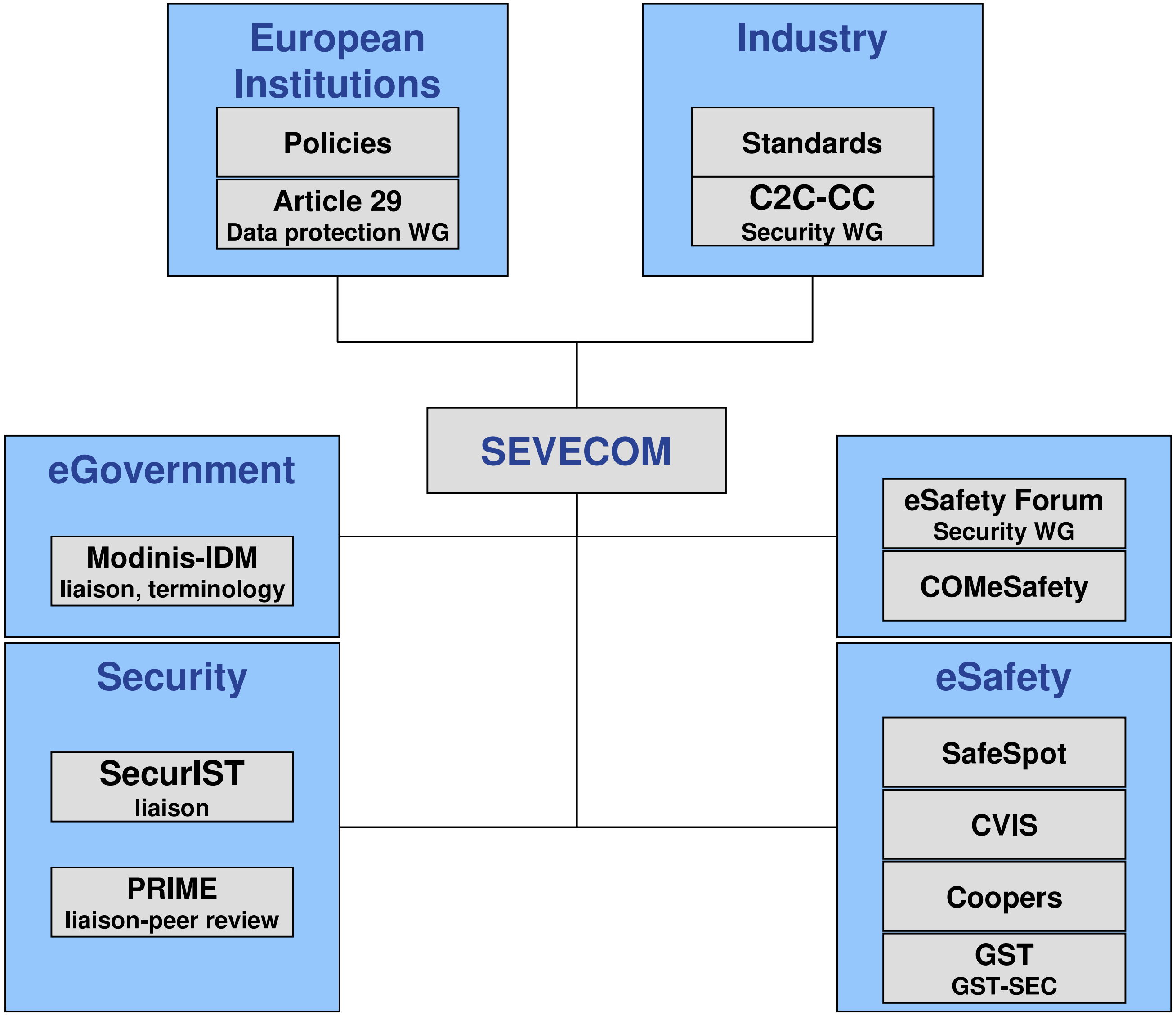
Architecture/Analysis

Specification

Development

Demonstrations

SEVECOM is a Transversal Project



European Institutions

Policies

Article 29
Data protection WG

Industry

Standards

C2C-CC
Security WG

SEVECOM

eGovernment

Modinis-IDM
liaison, terminology

eSafety Forum
Security WG

COMeSafety

Security

SecurIST
liaison

PRIME
liaison-peer review

eSafety

SafeSpot

CVIS

Coopers

GST
GST-SEC

Security Baseline Architecture

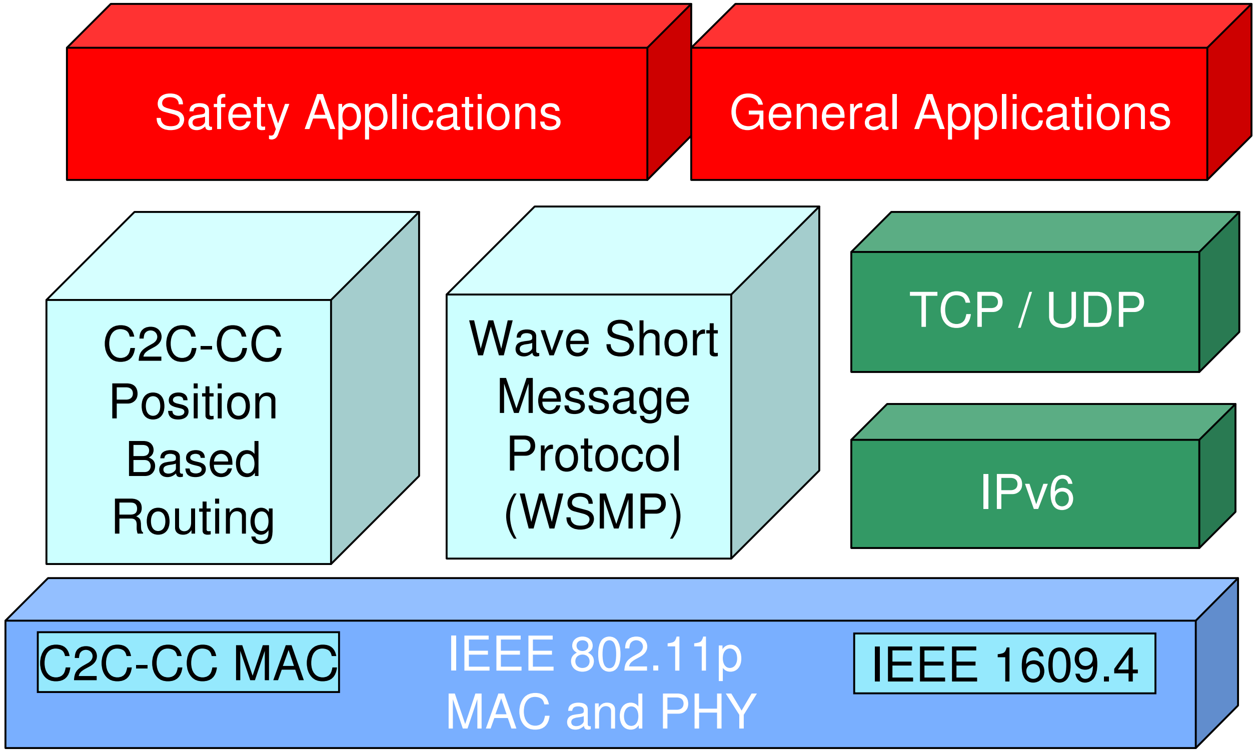
- Requirements
  - Authentication, Integrity, Non-repudiation, Access control, Confidentiality
  - Availability
  - Privacy
  - Liability identification

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)

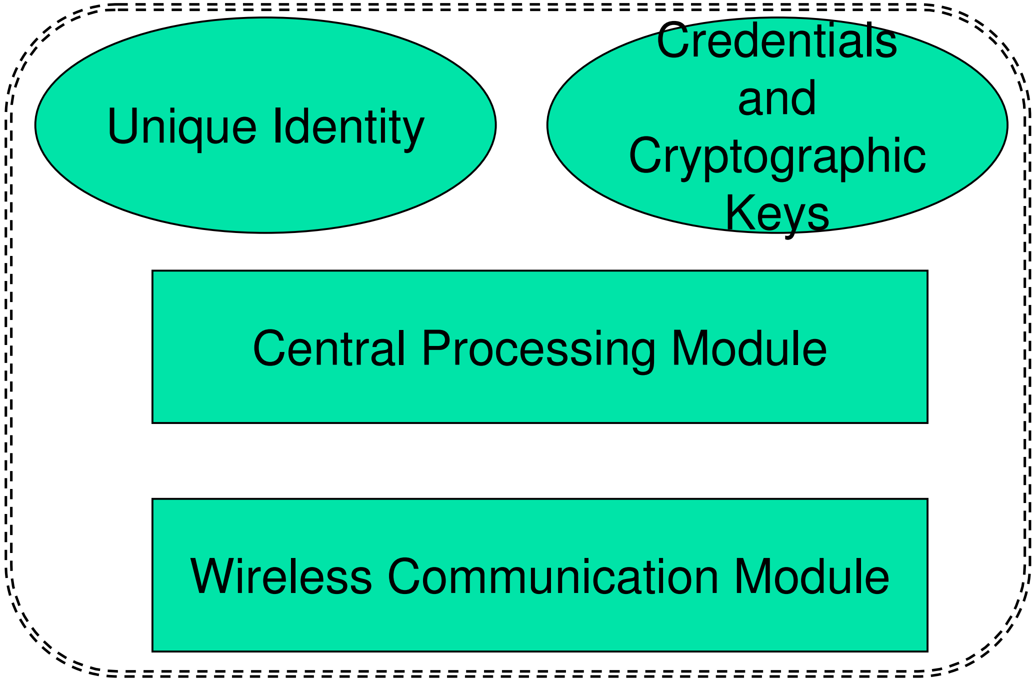
- Challenges
  - High rate broadcast communication
  - VANET-only (e.g., safety) and TCP/IP communication



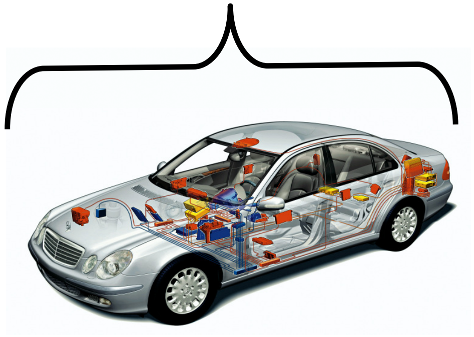
Security Baseline Architecture (cont'd)

SEVECOM

- Basic ideas


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

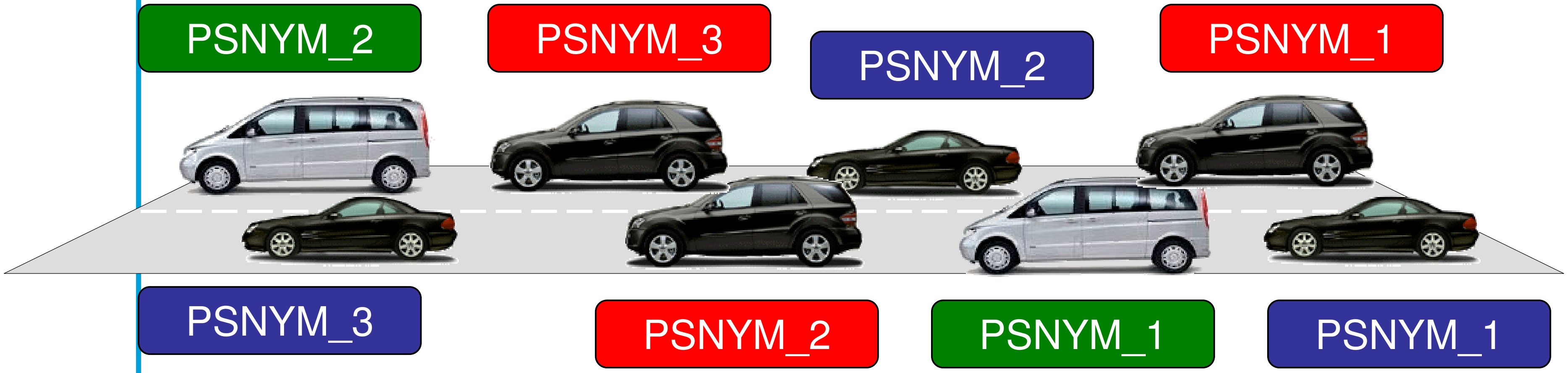
- **Long-term identity**
- **Public key crypto**
  - *EC-DSA, RSA*
- **Certificates**



Abstract view of a vehicle

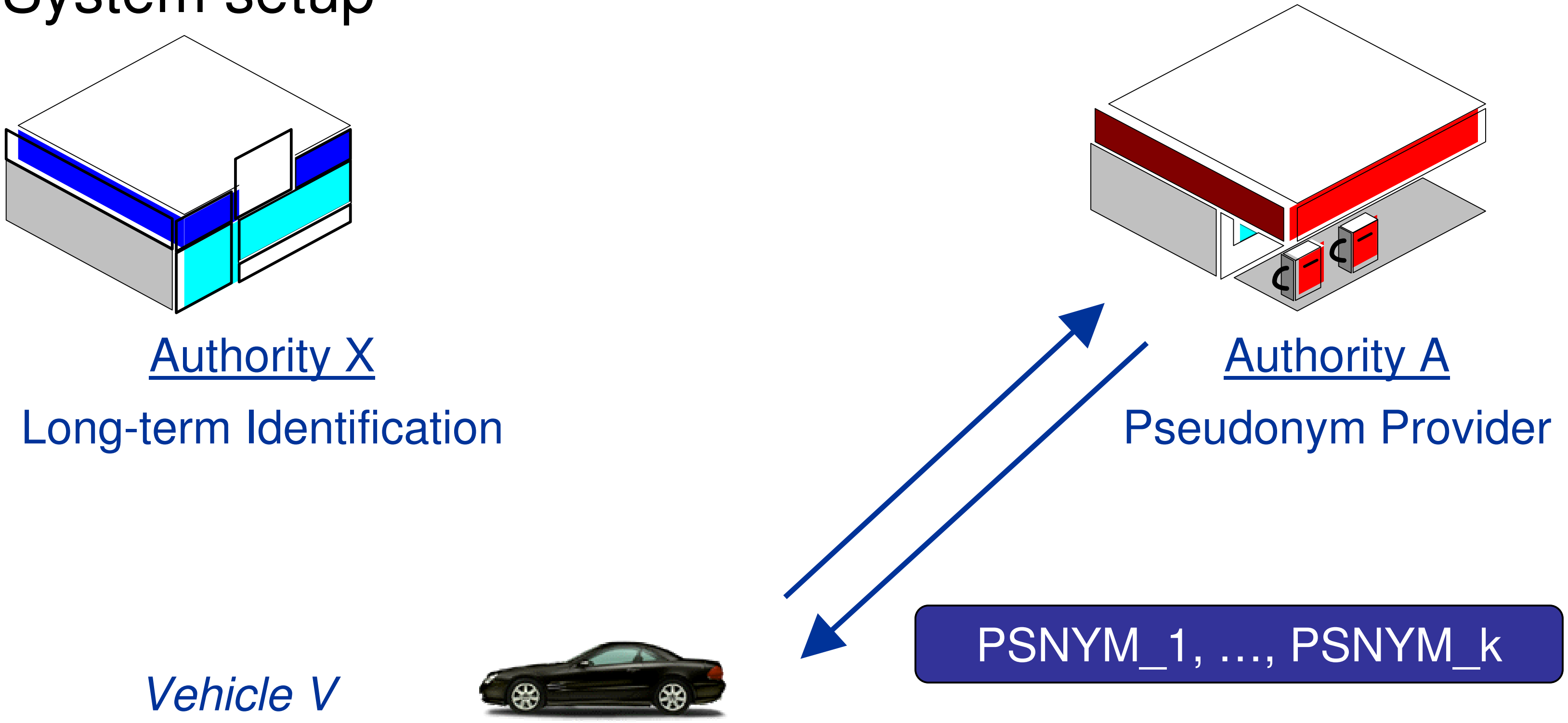
Security Baseline Architecture (cont'd)

- 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)

- System setup



Authority X

Long-term Identification

Authority A

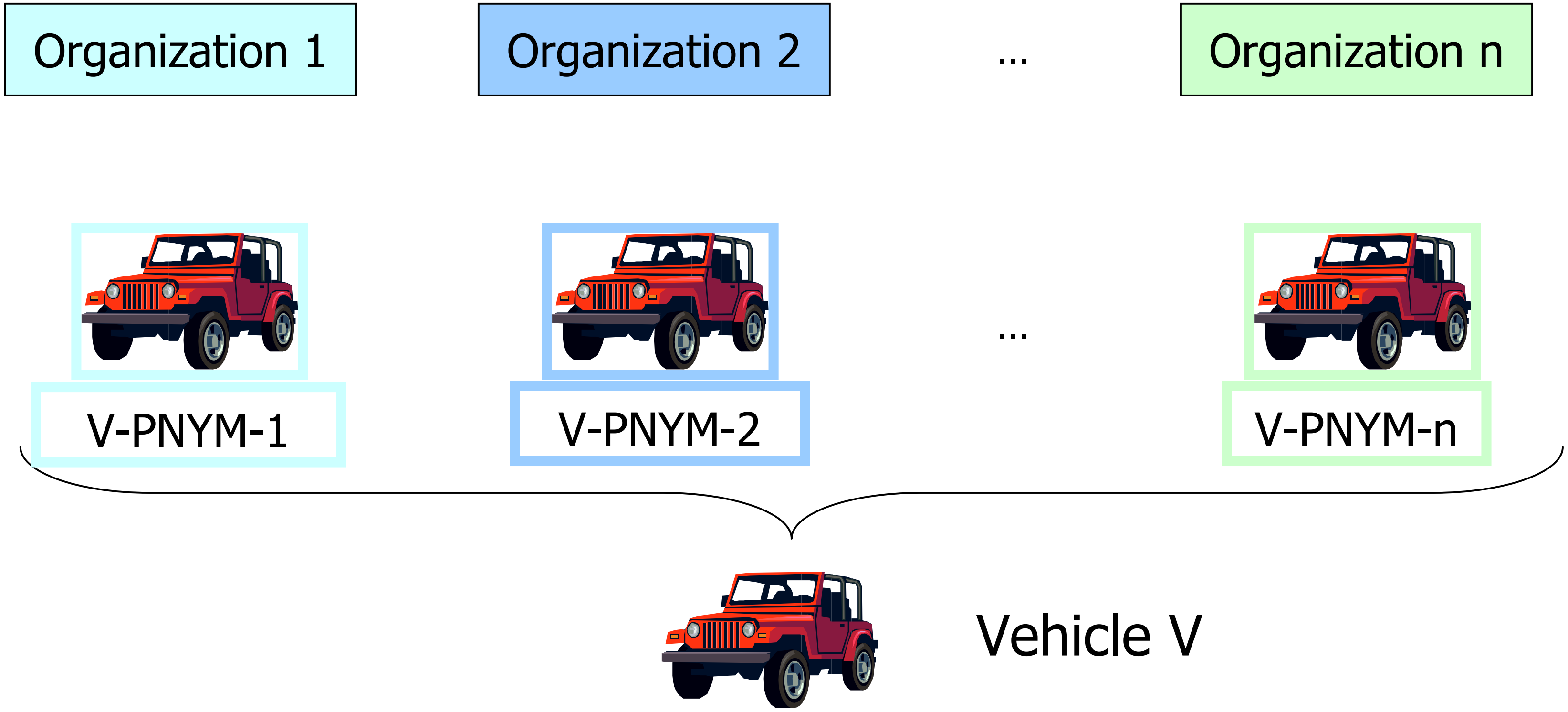
Pseudonym Provider

Vehicle V

PSNYM_1, …, PSNYM_k

Security Baseline Architecture (cont'd)

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

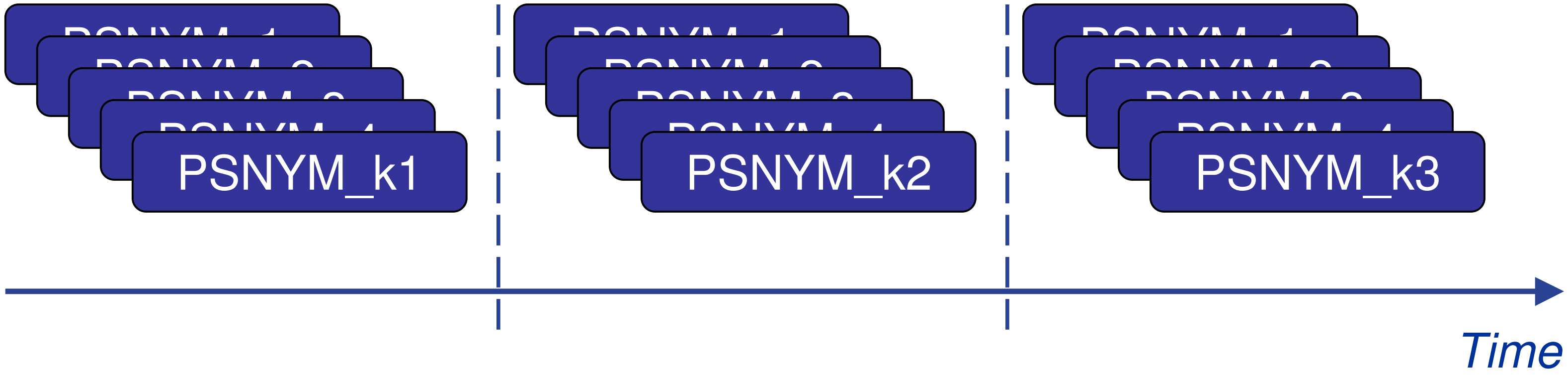


Security Baseline Architecture (cont'd)

- Pseudonym format

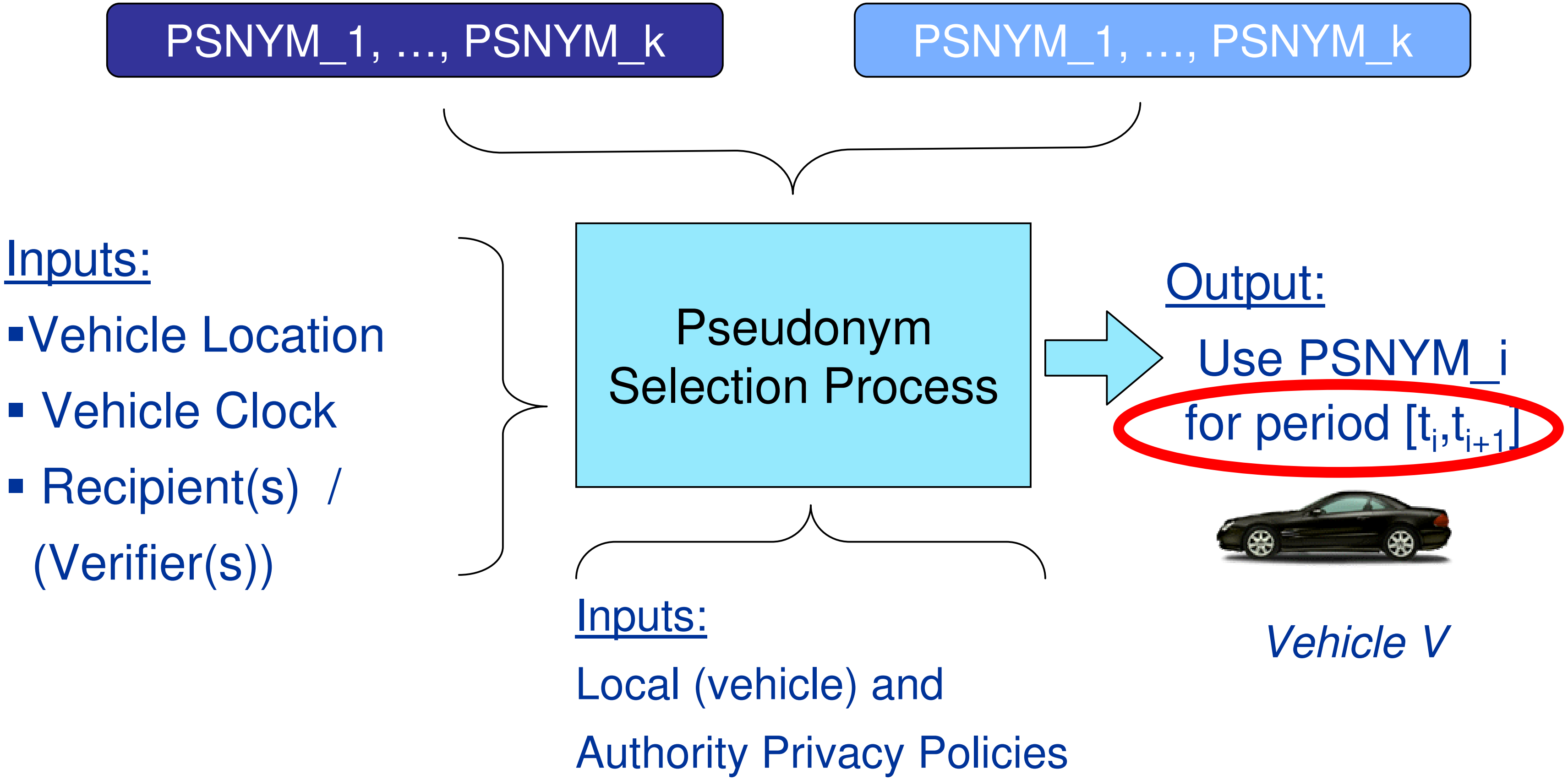
<table>
<tr><td>PSNYM-Provider ID</td><td>PSNYM Lifetime</td></tr>
<tr><td colspan="2">Public Key</td></tr>
<tr><td colspan="2">PSNYM-Provider Signature</td></tr>
</table>

- 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

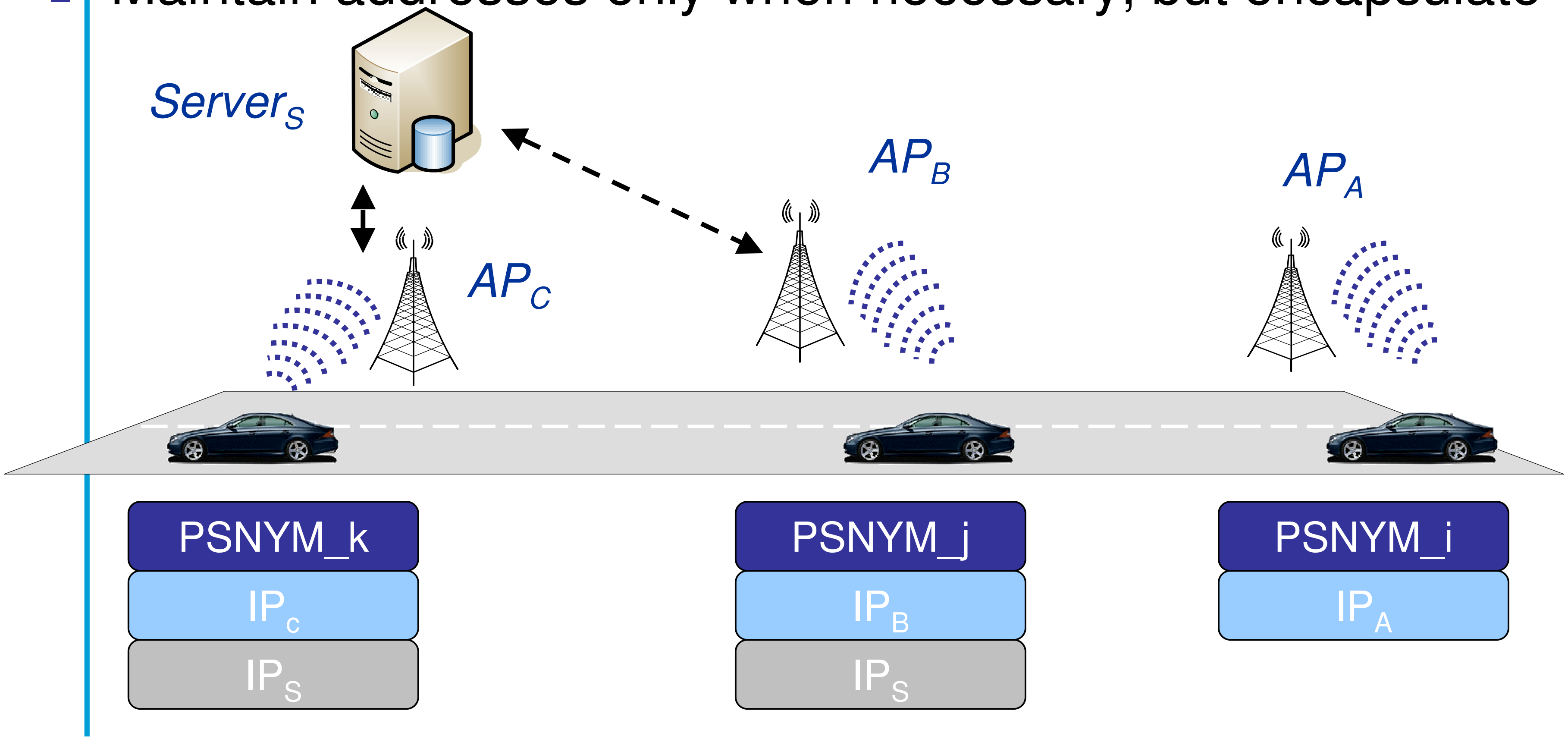
Inputs:

Local (vehicle) and Authority Privacy Policies

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

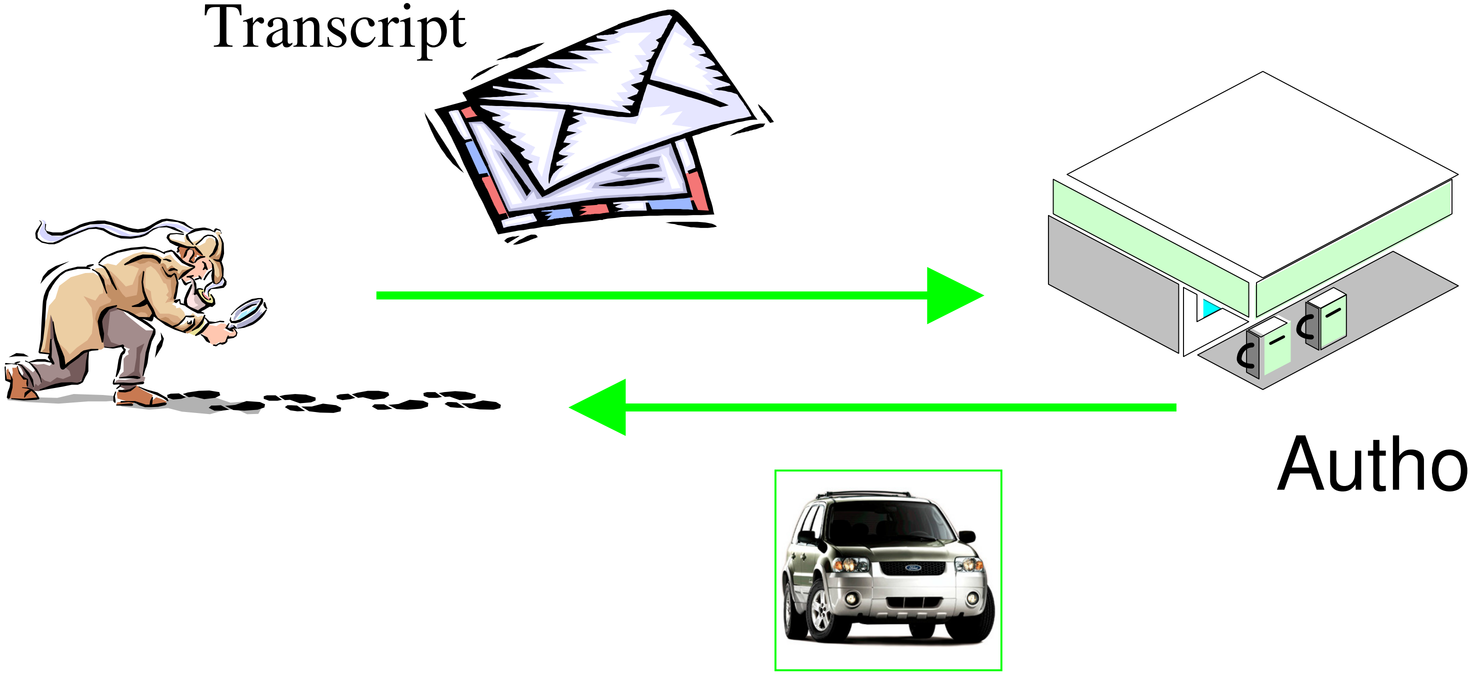
Privacy Baseline Architecture (cont'd)

- 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

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

eSecurity WG

- Working group of the eSafety forum
  - Co chairs : Antonio Kung. Trialog, Christoph Ruland. University of Siegen
- Motivation
  - Support of the reliability of eSafety
  - Protection of eSafety functions
  - Prevention of critical road safety effects which result from electronic vehicle systems
  - Preventing of misuse or malpractice, including **privacy infringement**
  - Establishment of new R&D fields
  - Providing **recommendations, code of practice, standardisation**
  - Transparency of implemented safety and security functions
  - New fields of business

eSecurity WG

- Focus
  - Data protection.
  - Intrusion
- Activities
  - A1 State of the art (Claude Daulaud)
  - A2 Stakeholders and role (Nol Venema)
  - A3 Threats (Nol Venema)
  - A4 Security Requirements (Frank Kargl)
  - A5 Organisational Requirements (OEM)
  - A6 Regulation requirements (OEM)
  - A7 Research requirements (Chair)
  - A8 Results (Chair)
- Coordination
  - Article 29
  - C2C Sec WG
- Timetable
  - Kickoff meeting April 3rd
  - Next Meeting June 25th, 2007

Thank You

www.sevecom.org