SeVeCom : Secure Vehicle Communication

Antonio Kung
Coordinator
Trialog
25 rue du Général Foy
75008 Paris, France
www.trialog.com

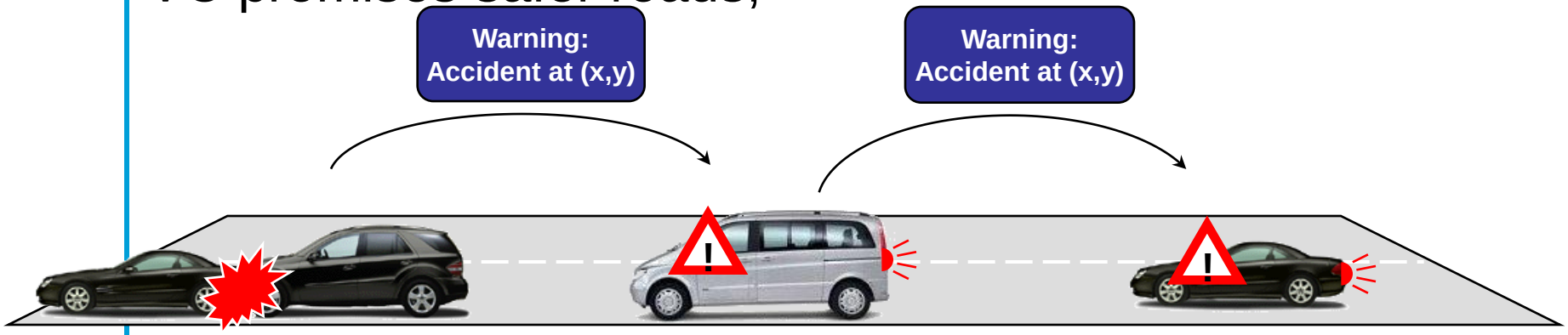
TRIALOG

Safety

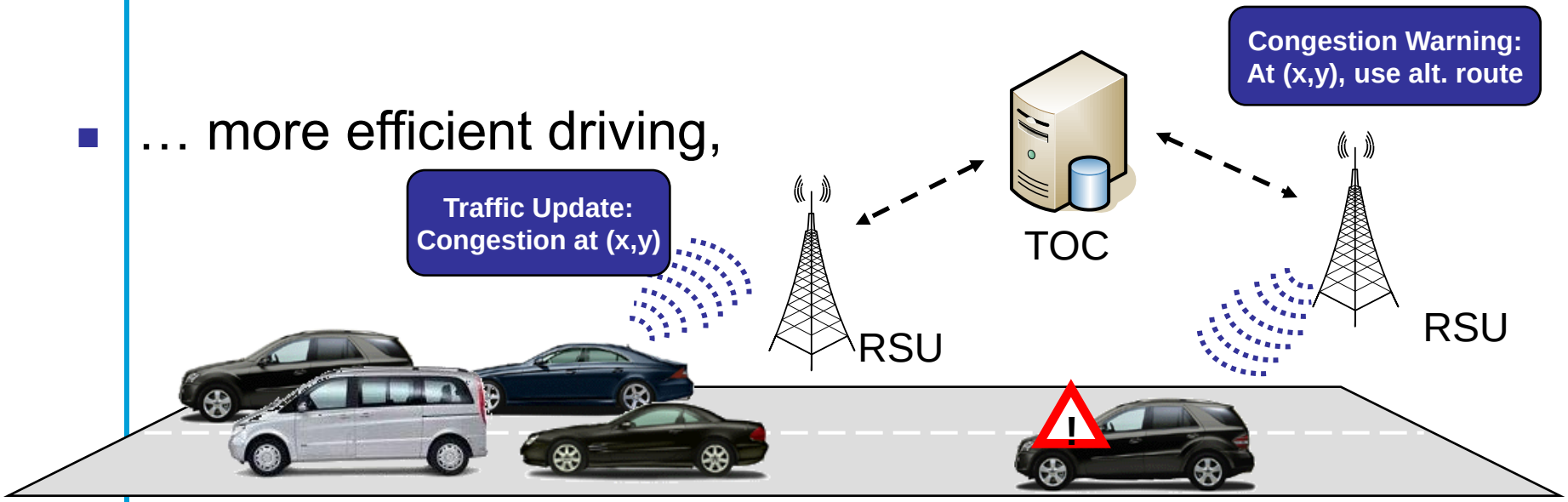
Information Society and Media

Vehicle Communication (VC)

- VC promises safer roads,

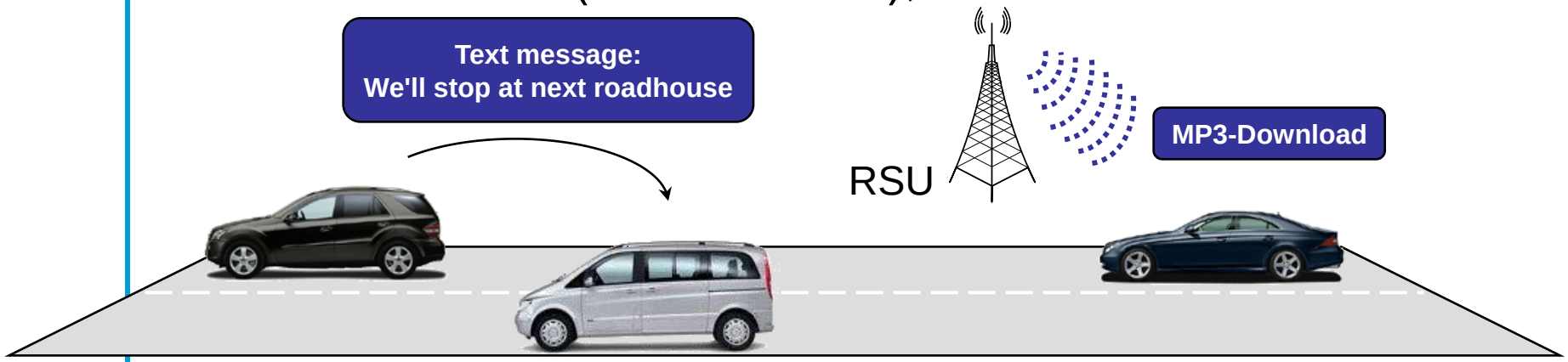


- … more efficient driving,

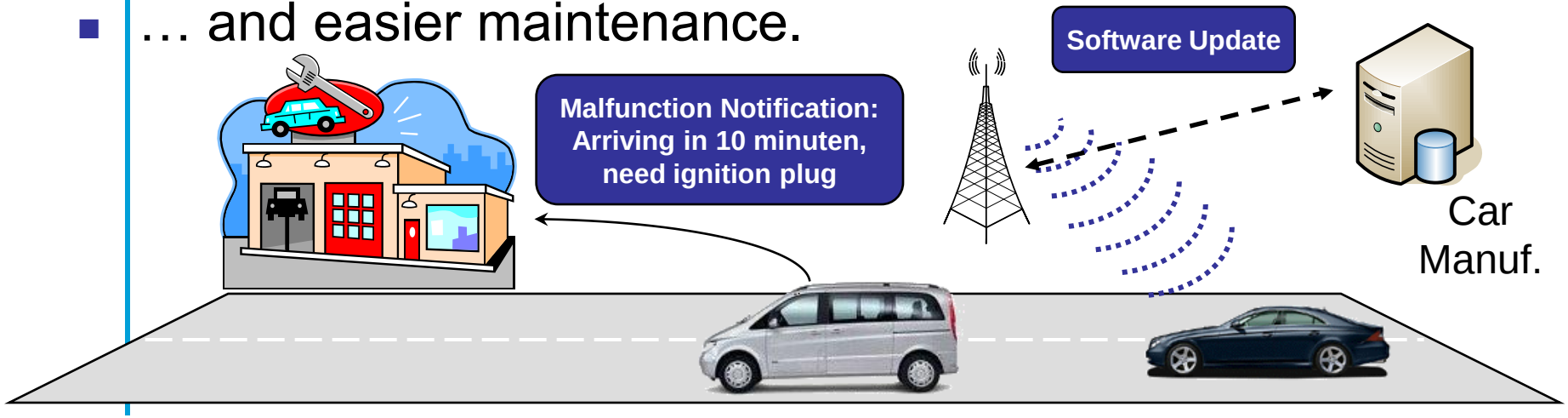


Vehicle Communication (VC)

- … more services (infotainment),



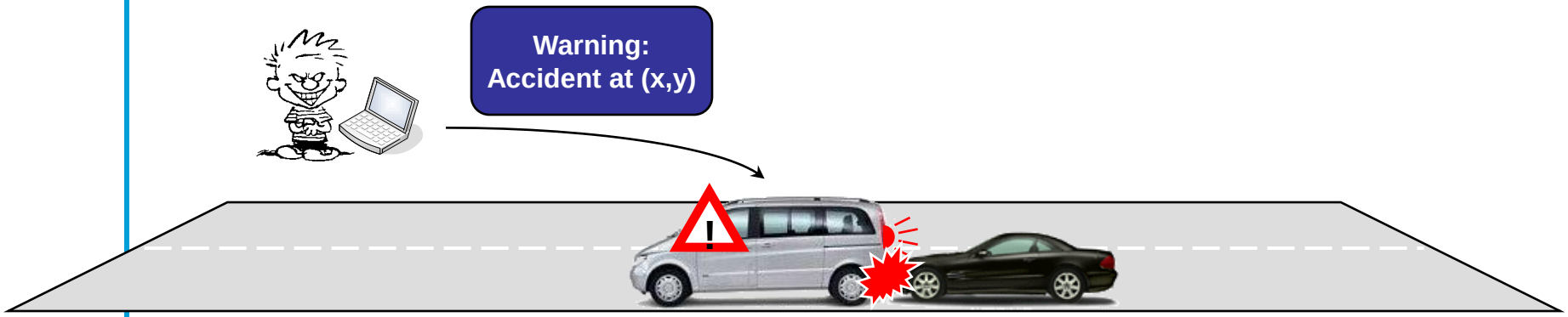
- … and easier maintenance.



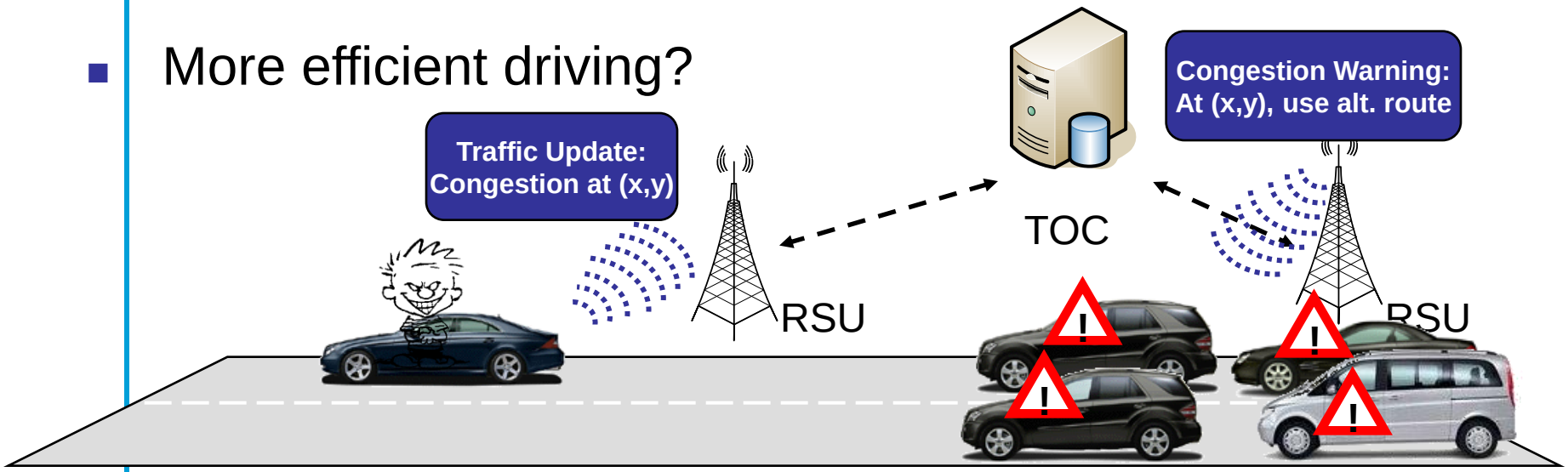

Sounds good
BUT ...

Security and Privacy???

- Safer roads?

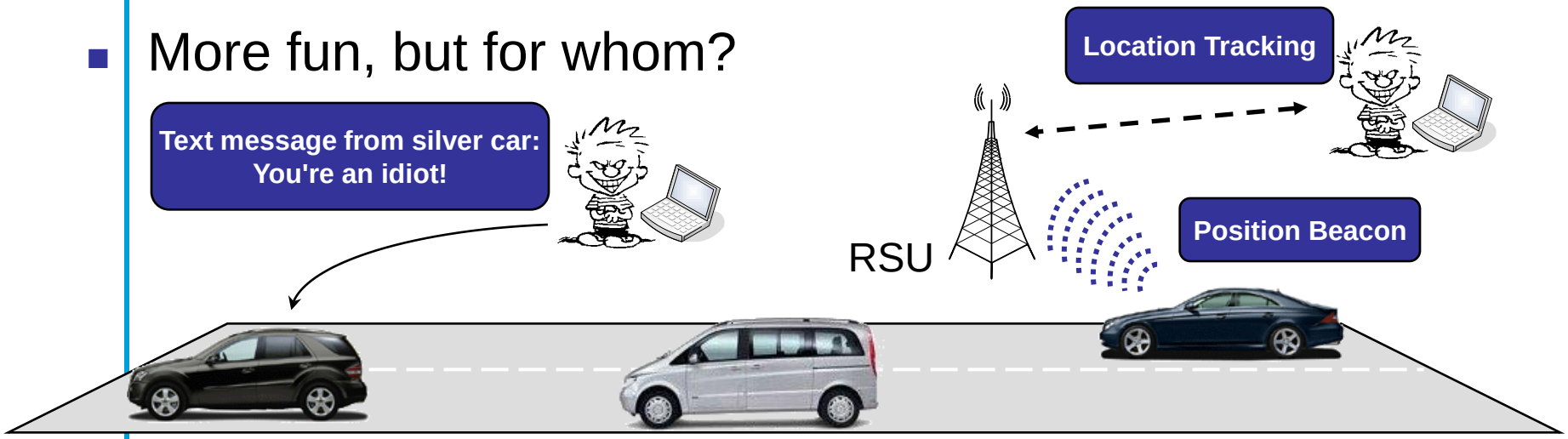


- More efficient driving?

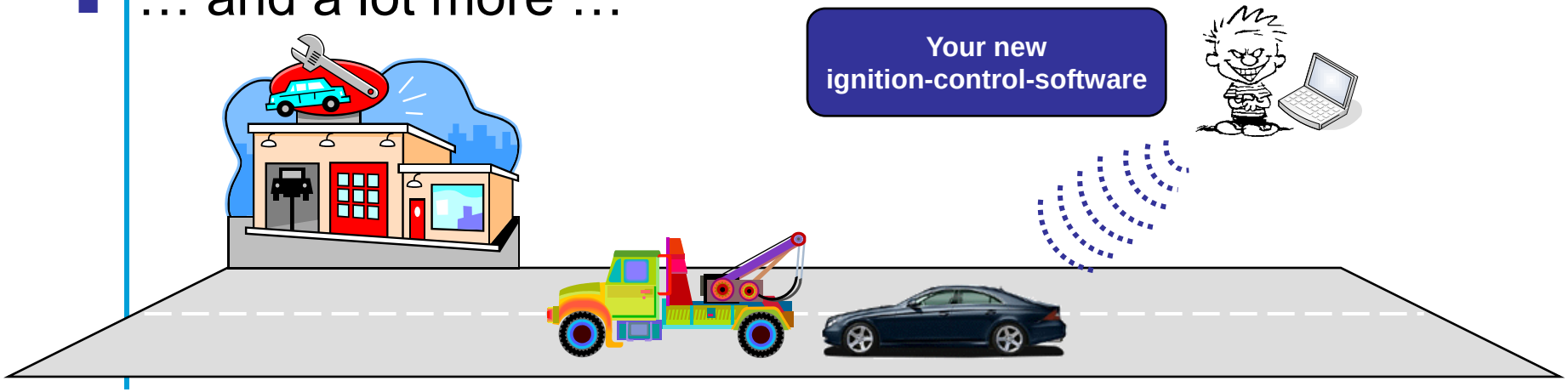


Security and Privacy???

- More fun, but for whom?



- … and a lot more …

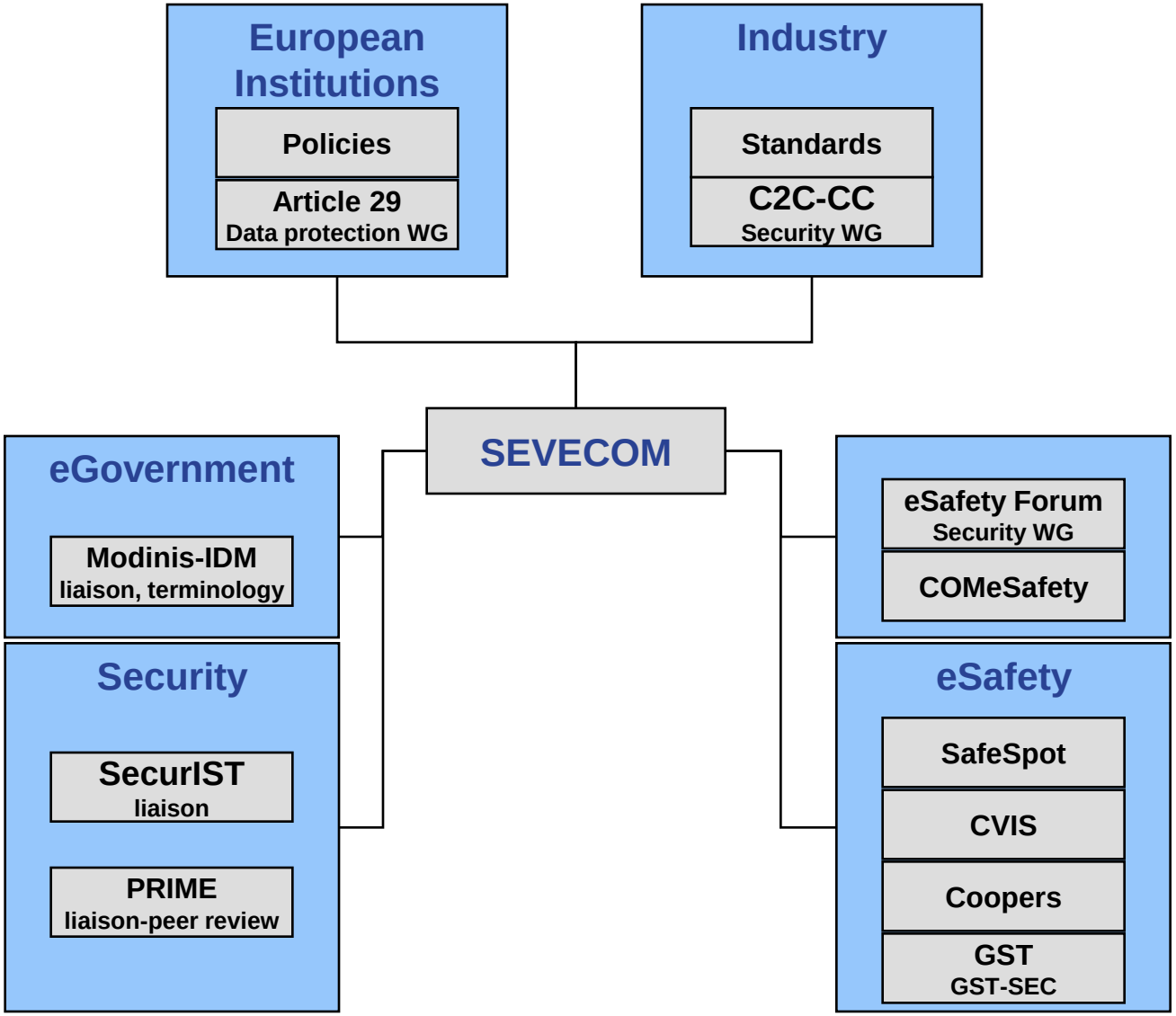


SE-cure VE-hicle COM-munication

SEVECOM

- Mission: future-proof solution to the problem of V2V/V2I security
- Partners
  - Trialog (Coordinator)
  - DaimlerChrysler
  - Centro Ricerche Fiat
  - Bosch
  - KU Leuven
  - Ecole Polytechnique Fédéral de Lausanne
  - University of Ulm
  - Budapest University of Technology and Economics

SEVECOM is a Transversal Project



Research topics

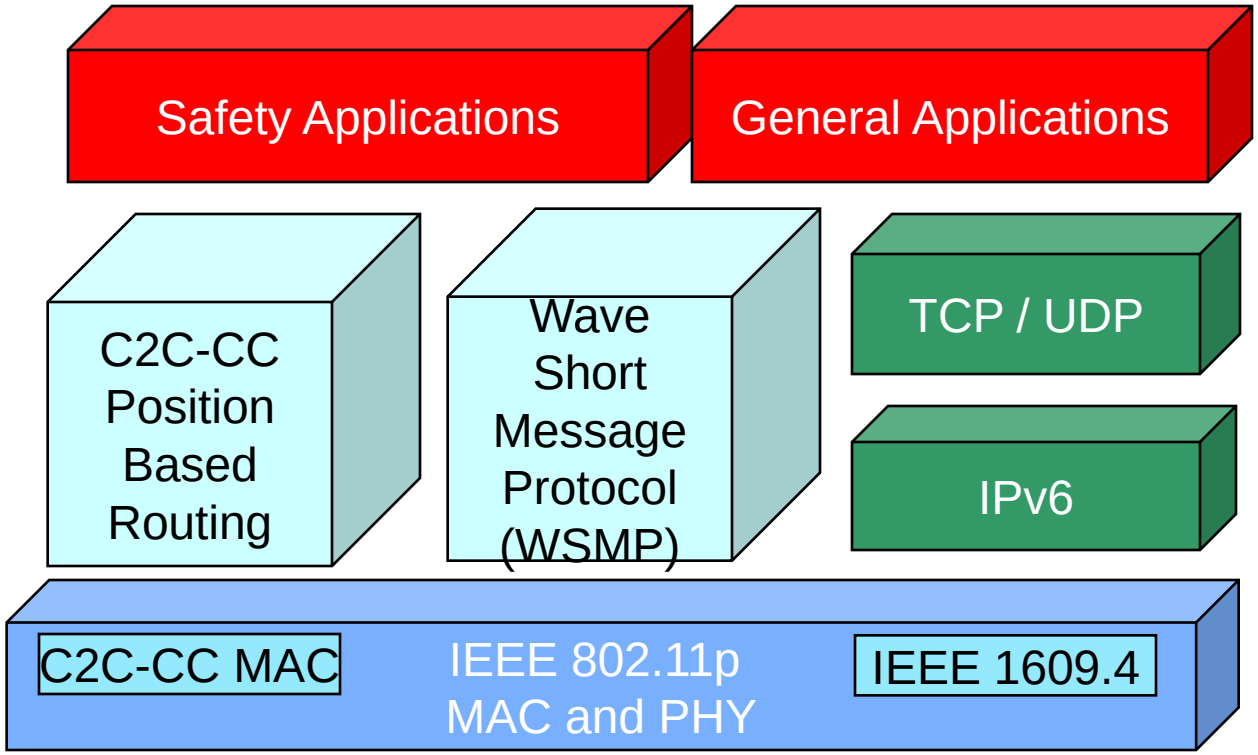
	Topic	Scope of work
A1	**Key and identity management**	Fully addressed
A2	Secure communication protocols (inc. secure routing)	Fully addressed
A3	Tamper proof device and decision on cryptosystem	Fully addressed
A4	Vehicle Intrusion	Investigation work
A5	Mulfunction detection and Data consistency	Investigation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

Security Baseline Architecture

SEVECOM

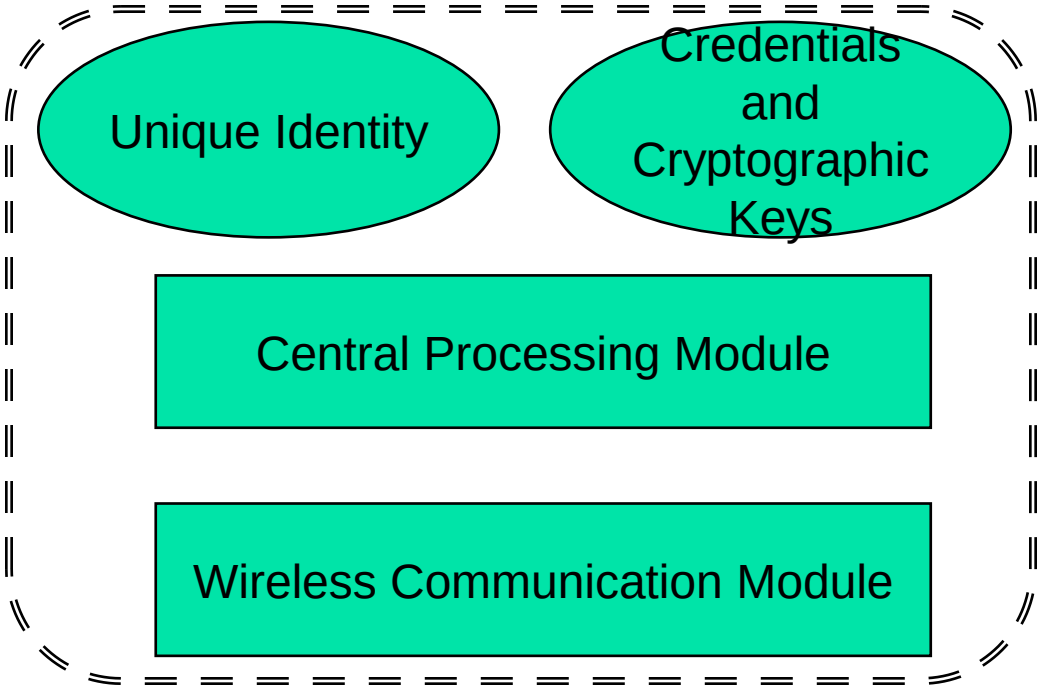
- Objectives
  - Focus on communication
  - Baseline Privacy Enhancing Technology (PET)
  - Future dynamic deployment of stronger PETs
    - Analogy: switching from 8 to 10 digit telephone numbers
- Baseline solution design approach
  - Standardized cryptographic primitives
  - Easy-to-implement
  -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

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



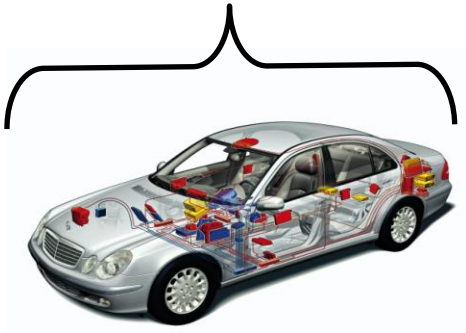
Security Baseline Architecture (cont'd)

- Basic ideas

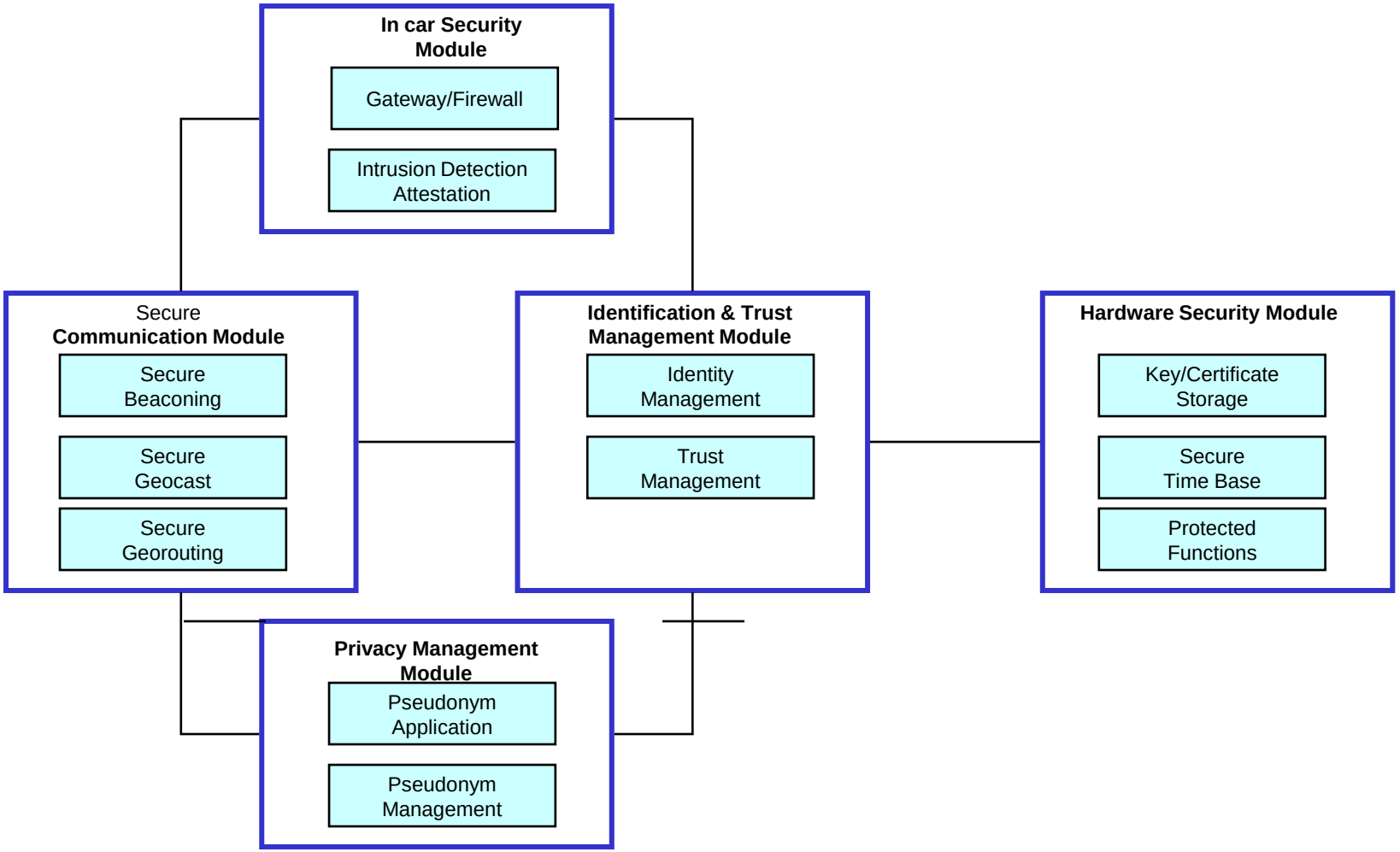


- **Long-term identity**
- **Public key crypto**
  - *EC-DSA, RSA*
- **Certificates**

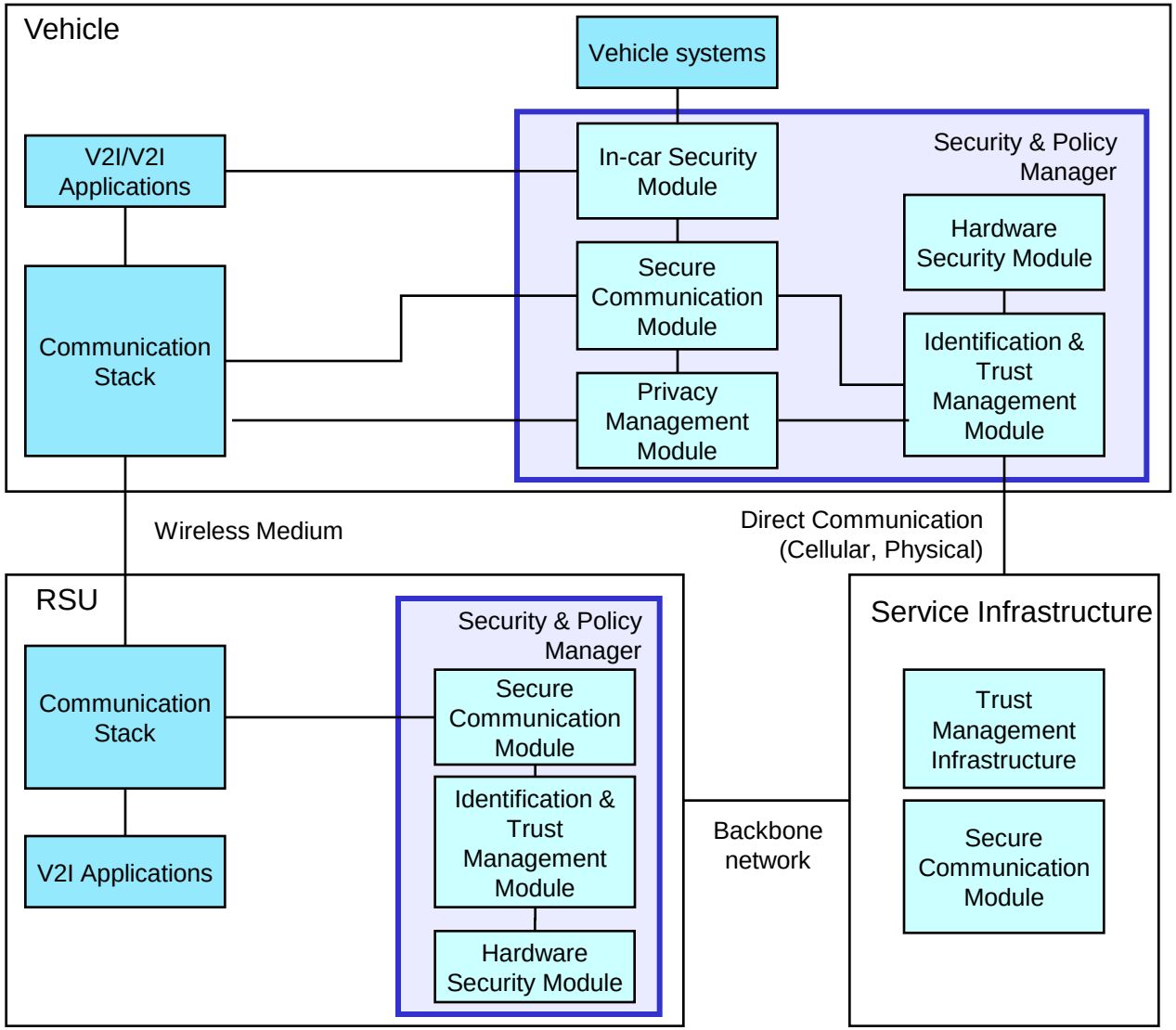
Abstract view of a vehicle



Building Blocks in Baseline Architecture



Deployment


Vehicle
Vehicle systems
V2I/V2I Applications
In-car Security Module
Security & Policy Manager
Hardware Security Module
Secure Communication Module
Communication Stack
Identification & Trust Management Module
Privacy Management Module
Wireless Medium
Direct Communication (Cellular, Physical)
RSU
Security & Policy Manager
Service Infrastructure
Communication Stack
Secure Communication Module
Trust Management Infrastructure
Identification & Trust Management Module
Backbone network
V2I Applications
Secure Communication Module
Hardware Security Module

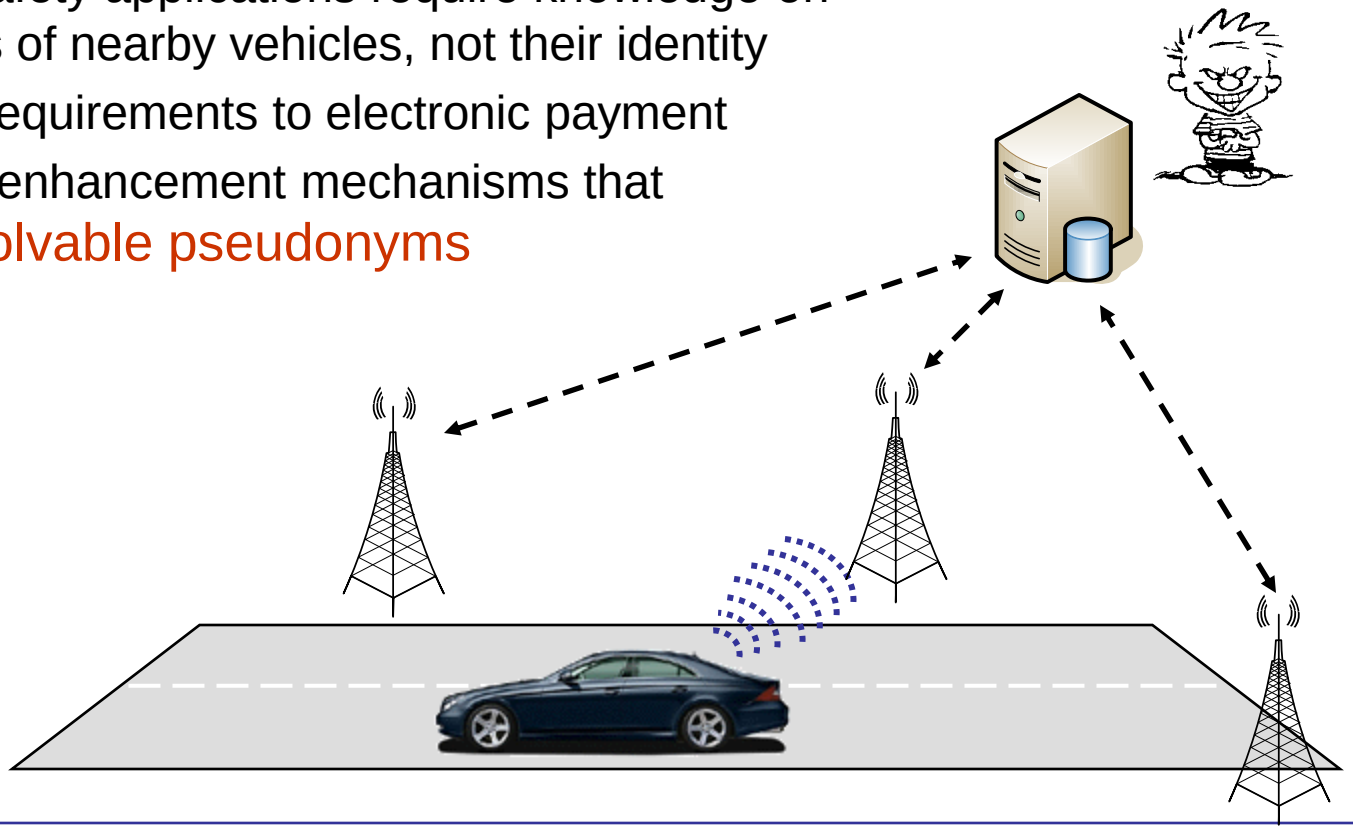
Sevecom Privacy focus

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

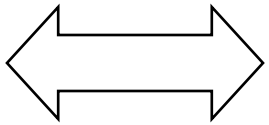
Sevecom Privacy focus

- 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

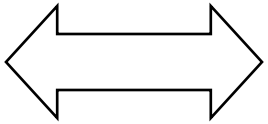
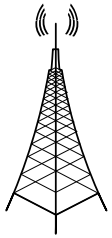
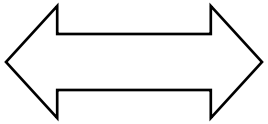





V2V

Eavesdropping Case

Protection Focus

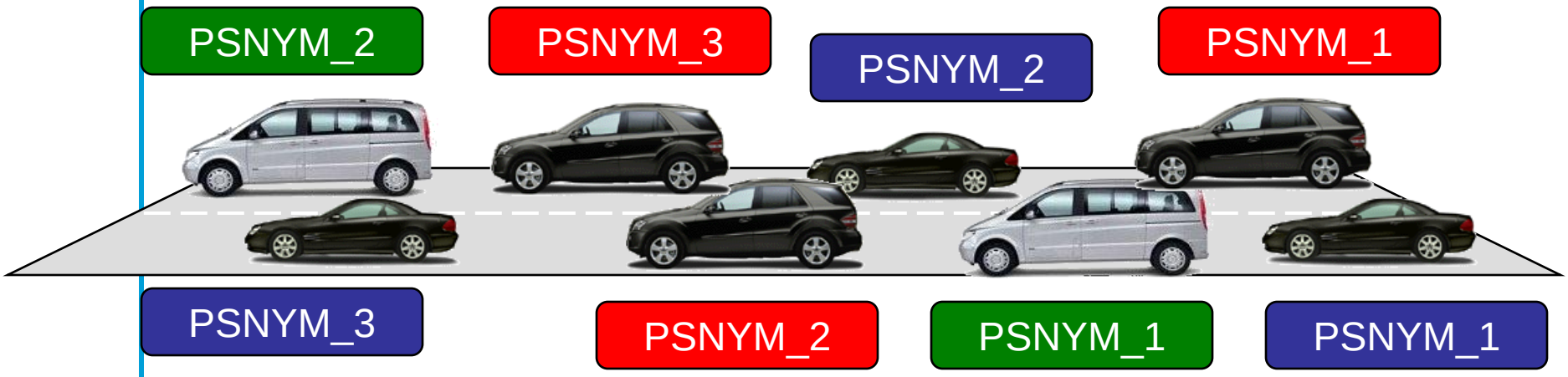




Storage **Internet** **Storage** **V2V**

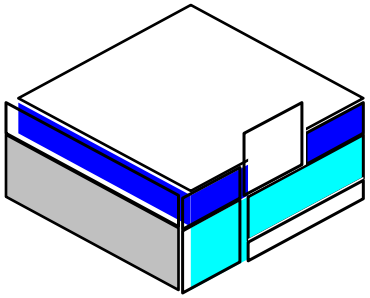
Security Baseline Architecture (cont'd)

- 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



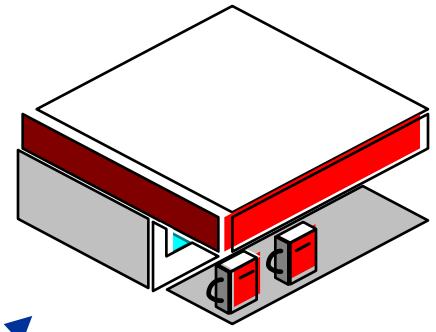
Security Baseline Architecture (cont'd)

- System setup



Authority X

Long-term Identification



Authority A

Pseudonym Provider

Vehicle V

PSNYM_1, …, PSNYM_k

Security Working Groups

- C2C Security Working Group
  - Dr H.J Voegel, BMW
- COMeSafety IST project
  - Dr T.Kosch, BMW
- eSafety forum Security WG
  - Antonio Kung, Trialog
  - Prof. Ruland, Siegen U.

White Paper
Baseline Architecture

Impact of Security to eSafety Architecture

Recommendations

In-vehicle Communication,
Telematics and Co-operative systems
Workshop on security and privacy issues
Brussels, 27 May 2008

Thank You

www.sevecom.org