Secure Vehicle Communication

SEVECOM

Security aspects in C2C-CC and CALM

Antonio Kung (Trialog)
Coordinator Sevecom

TRIALOG

eSafety

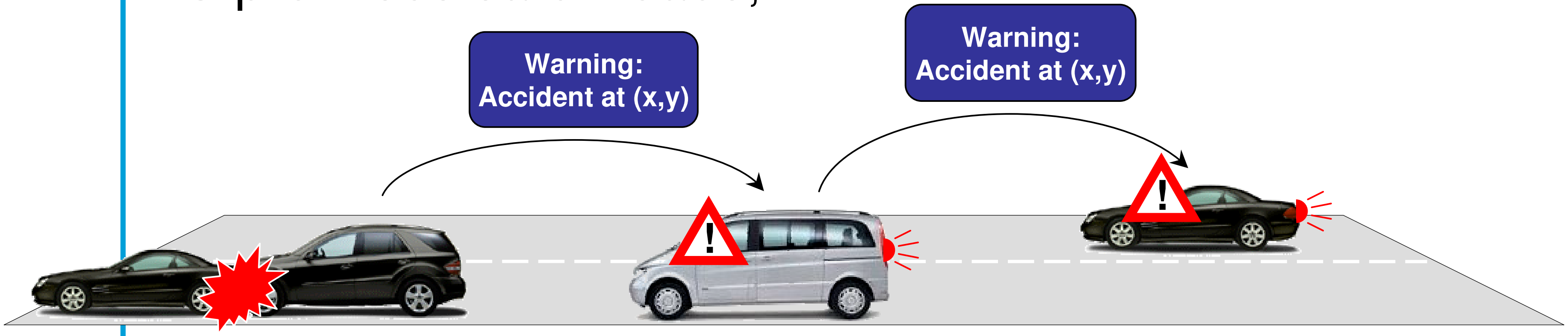
Information Society and Media

Outline

- Rationale
- Sevecom Initiative
- Baseline Architecture for Security and Privacy
- Other Working Groups

Vehicle Communication (VC)

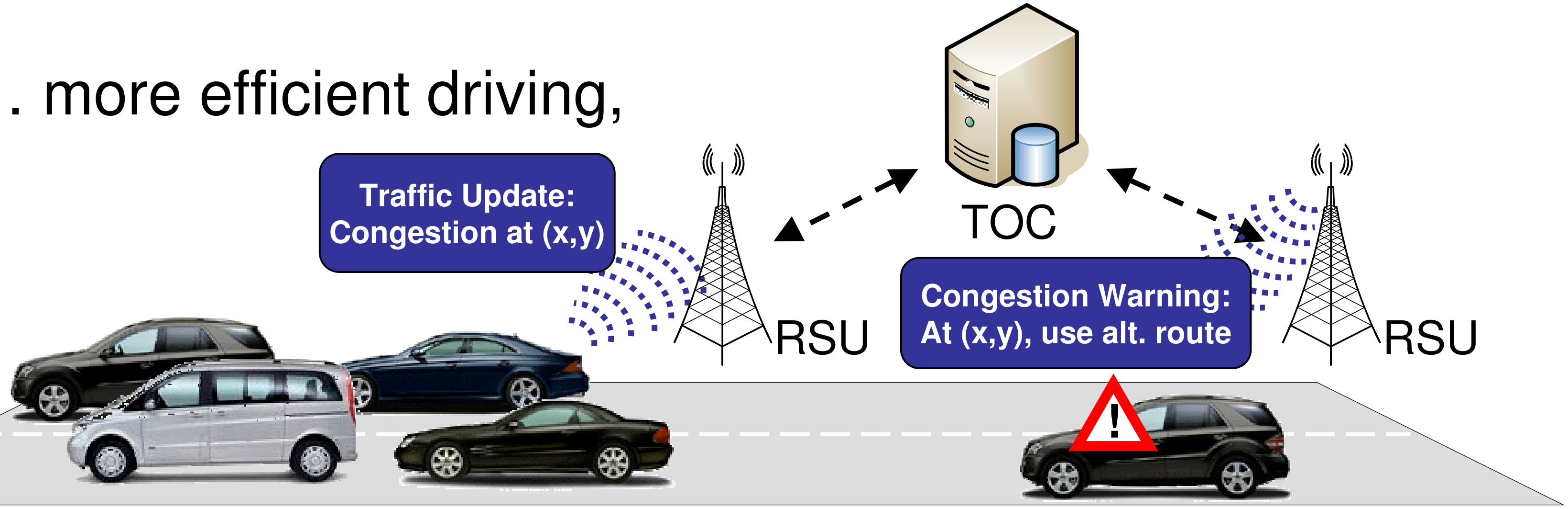
- VC promises safer roads,



Warning:
Accident at (x,y)

Warning:
Accident at (x,y)

- … more efficient driving,

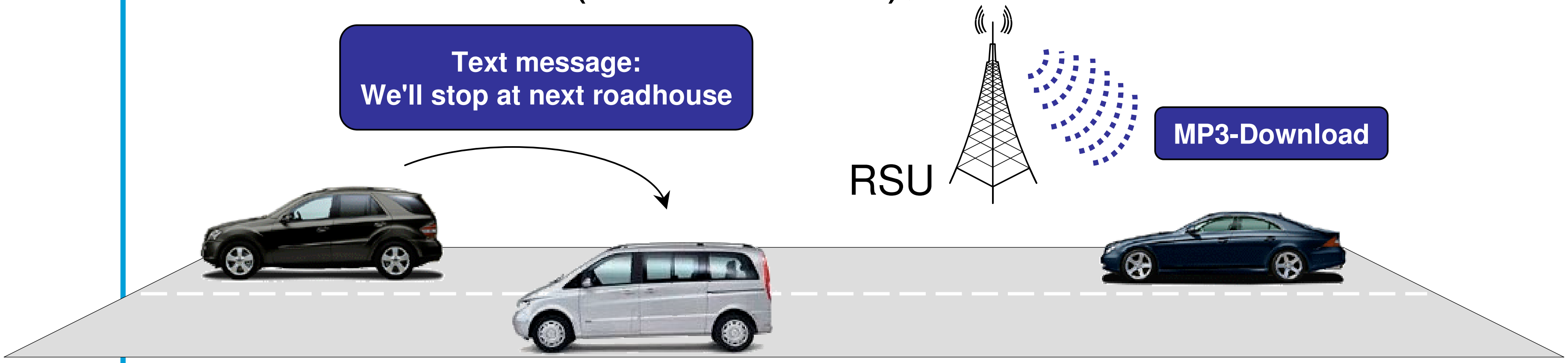


Traffic Update:
Congestion at (x,y)

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

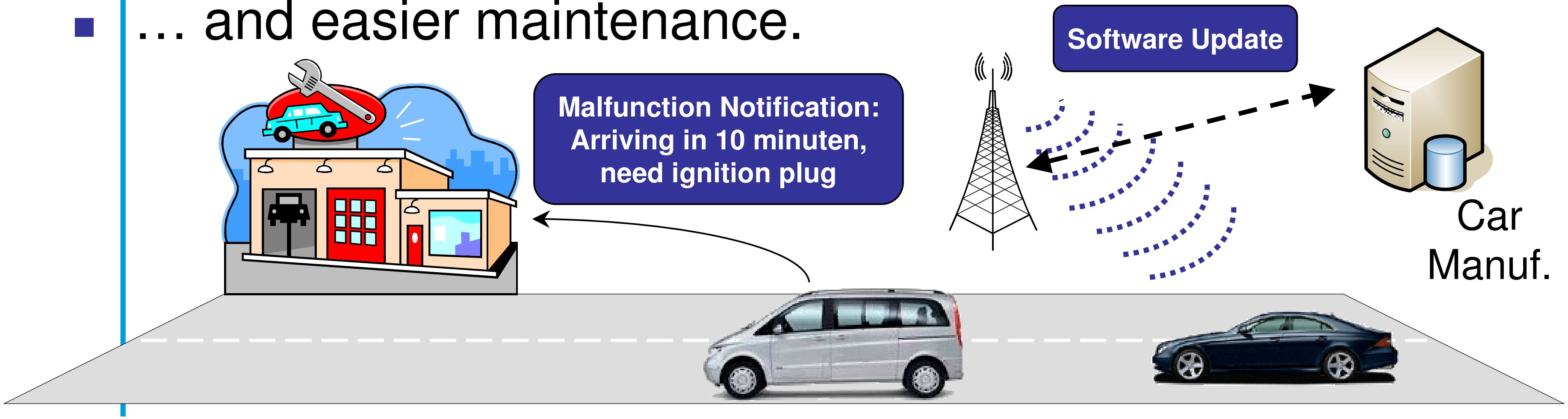
Vehicle Communication (VC)

- … more services (infotainment),



Text message:
We'll stop at next roadhouse

- … and easier maintenance.



Software Update

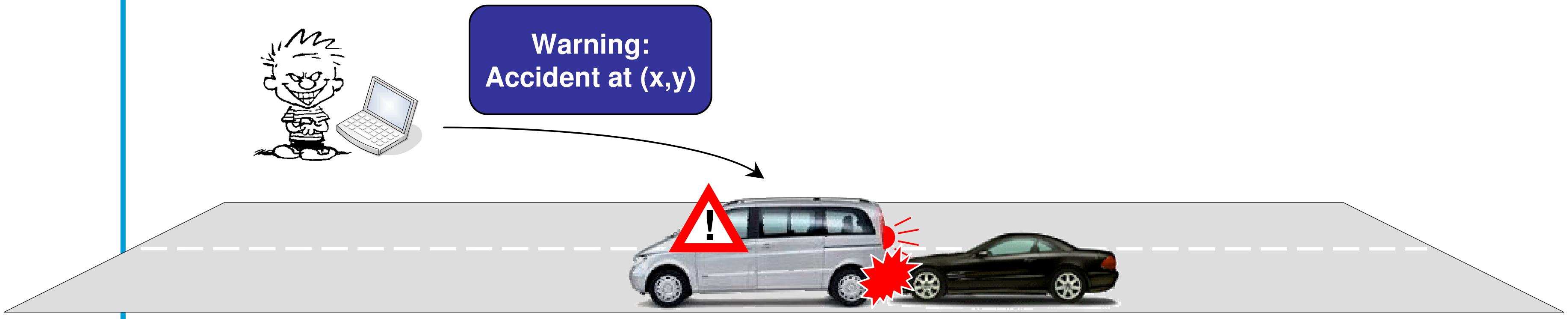
Malfunction Notification:
Arriving in 10 minuten,
need ignition plug

Sounds good

BUT …

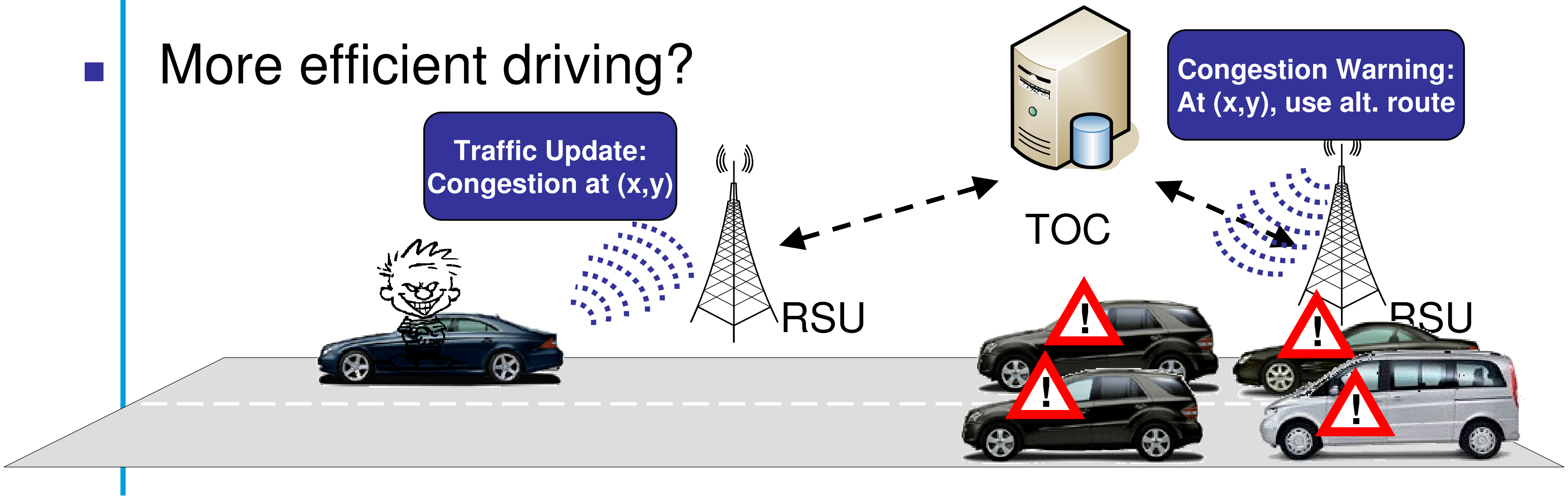
Security and Privacy???

- Safer roads?



Warning:
Accident at (x,y)

- More efficient driving?

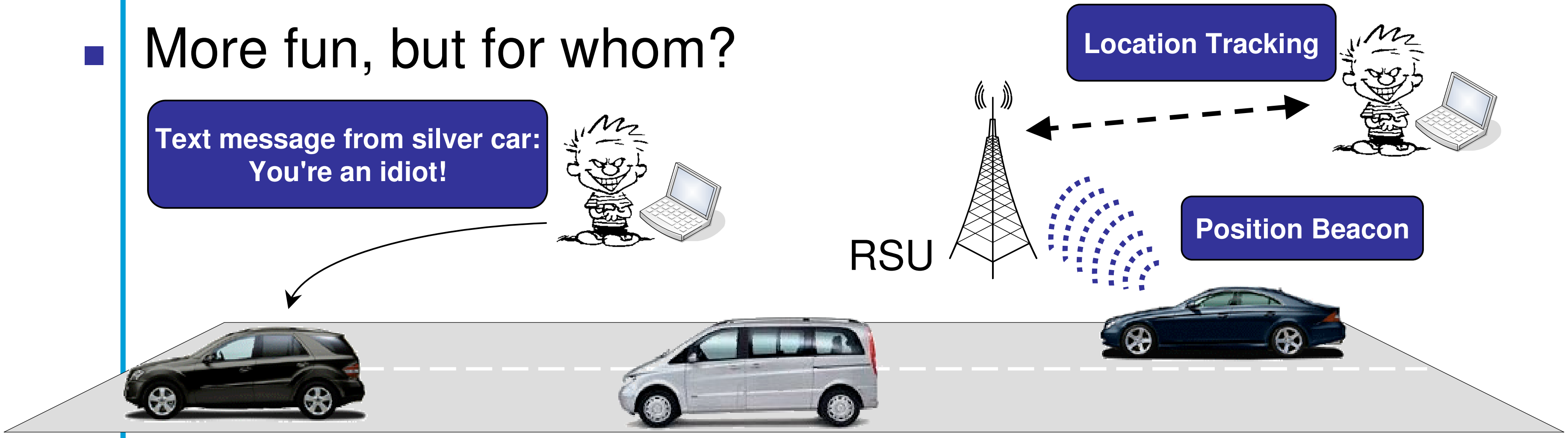


Traffic Update:
Congestion at (x,y)

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

Security and Privacy???

- More fun, but for whom?

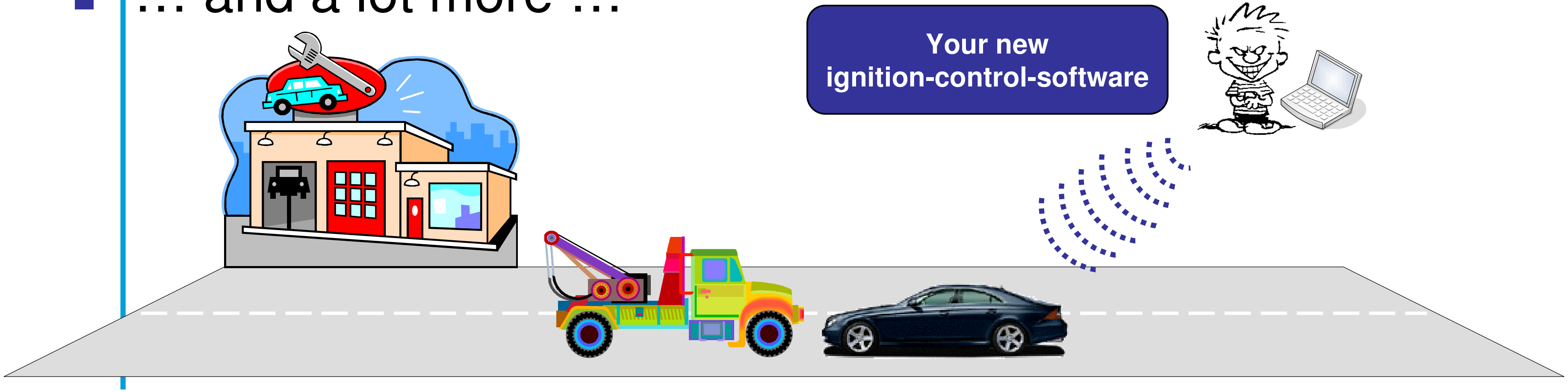


Text message from silver car: You're an idiot!

Location Tracking

Position Beacon

- … and a lot more …

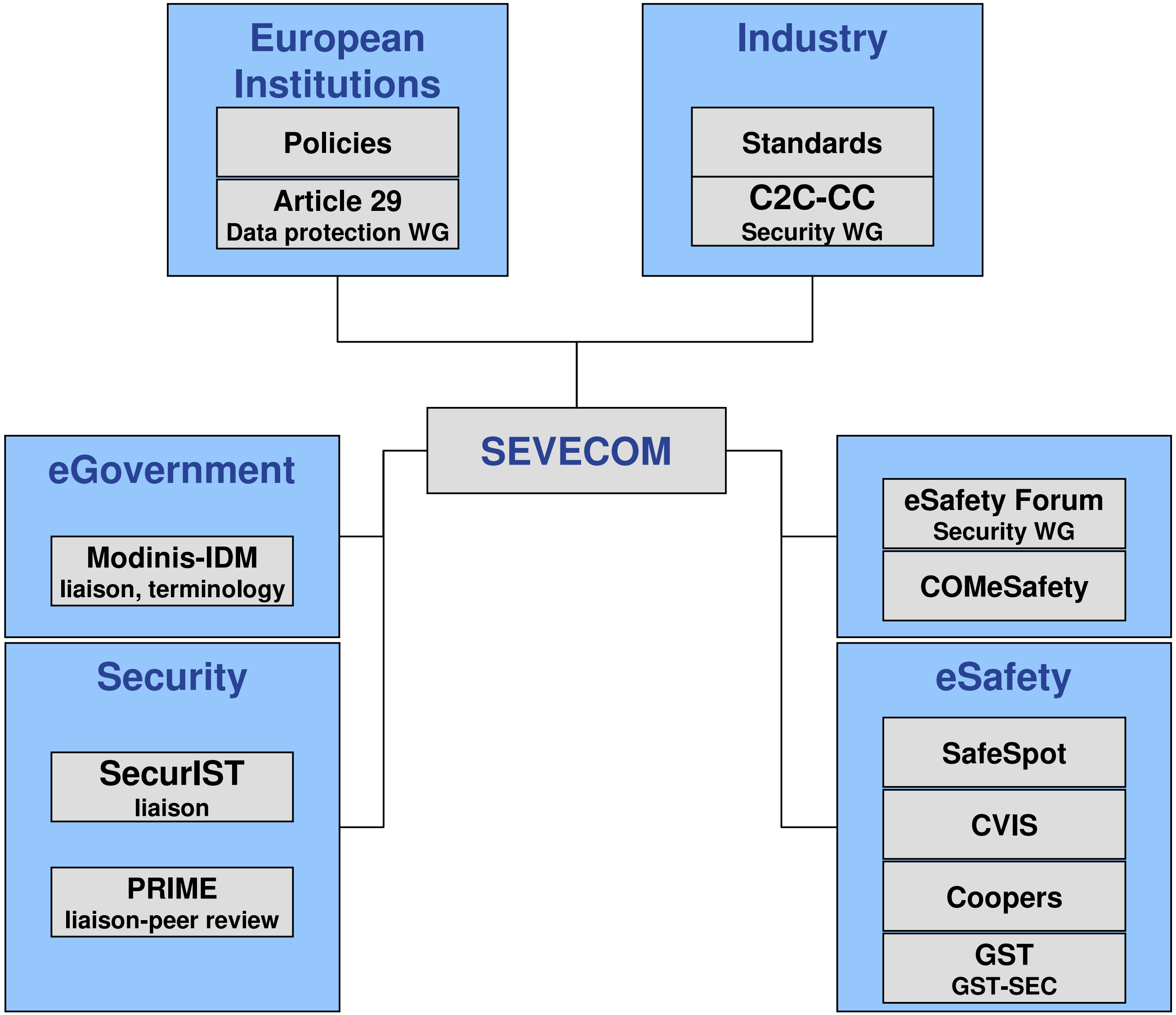


Your new ignition-control-software

SE-cure VE-hicle COM-munication

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

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

Security

SecurIST
liaison

PRIME
liaison-peer review

eSafety Forum
Security WG

COMeSafety

eSafety

SafeSpot

CVIS

Coopers

GST
GST-SEC

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	Data consistency	Investigation work
A6	**Privacy**	Fully addressed
A7	Secure positioning	Investigation work
A8	Secure user interface	Investigation work

Security Baseline Architecture

- 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

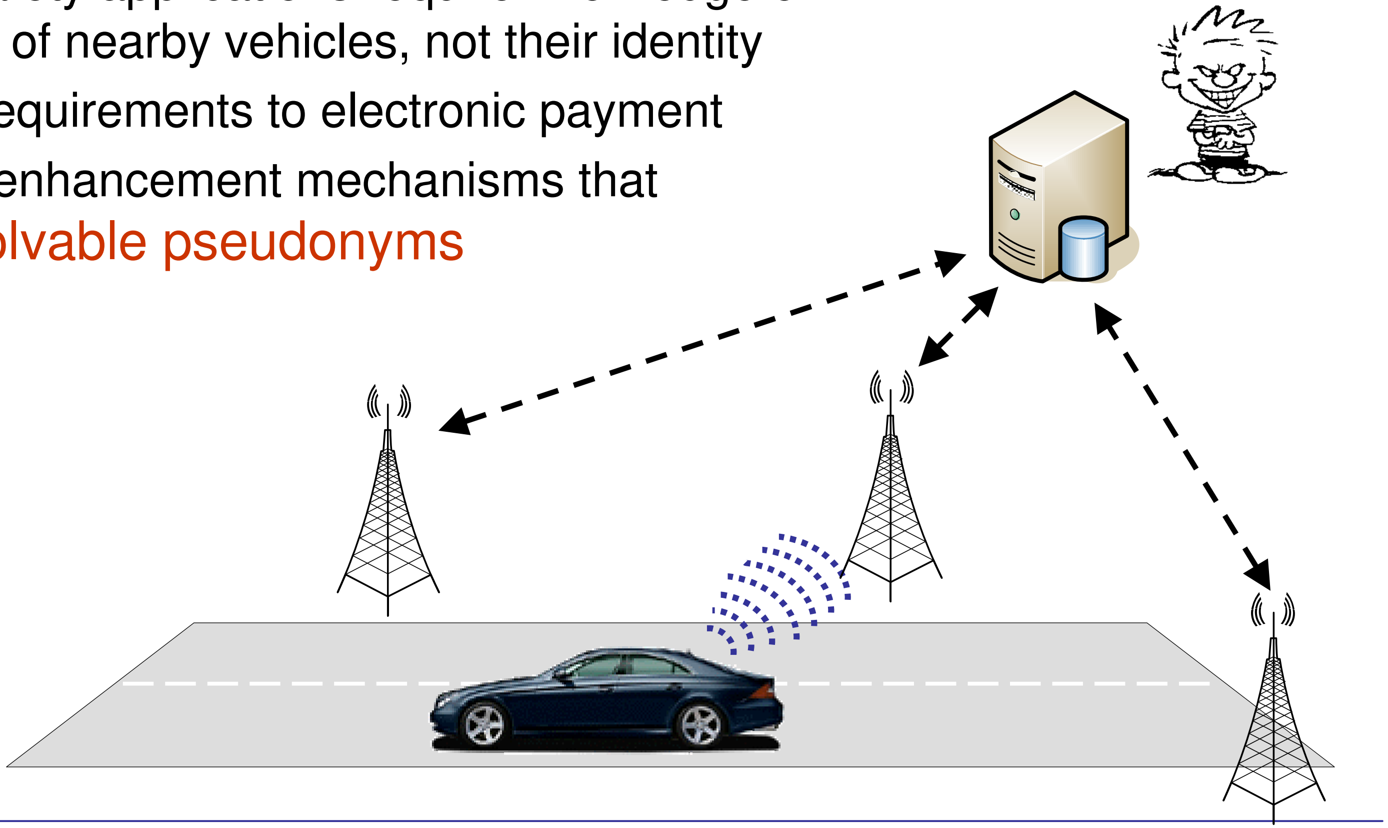
Security Baseline Architecture

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

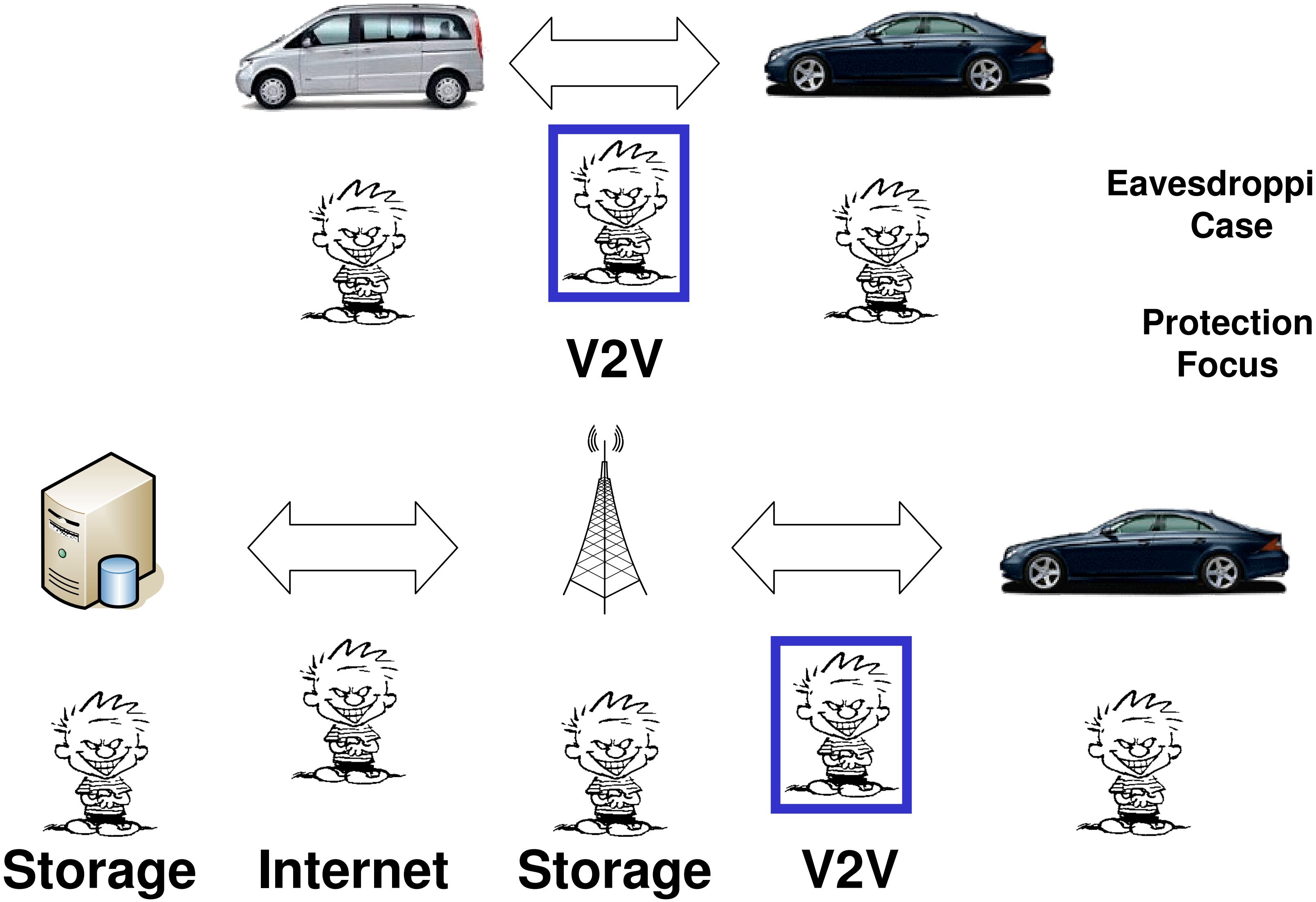
Privacy

- 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

Storage

Internet

Storage

V2V

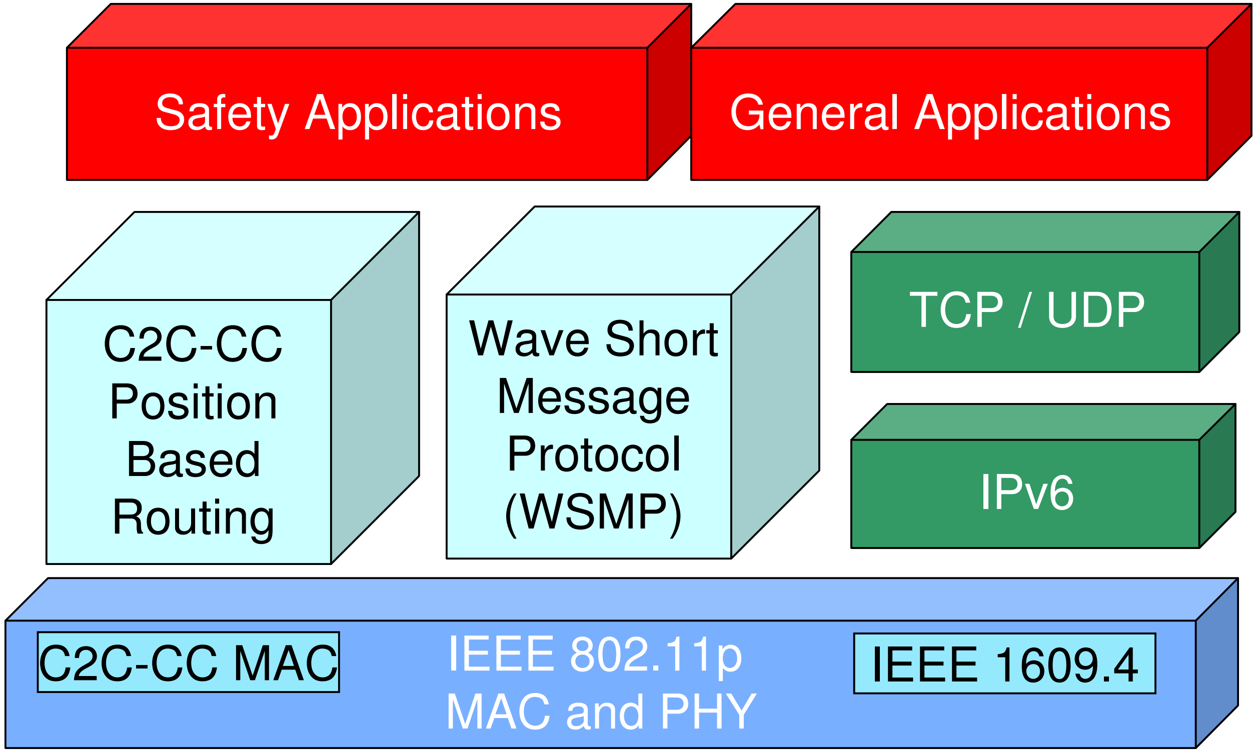
Eavesdropping Case

Protection Focus

Security Baseline Architecture (cont'd)

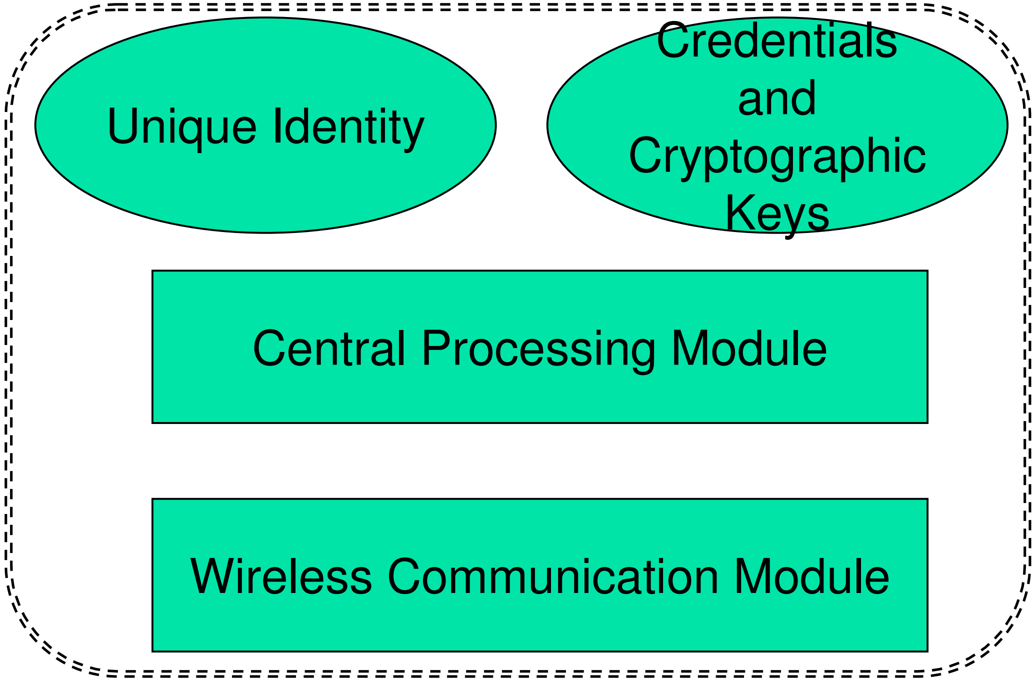
SEVECOM

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



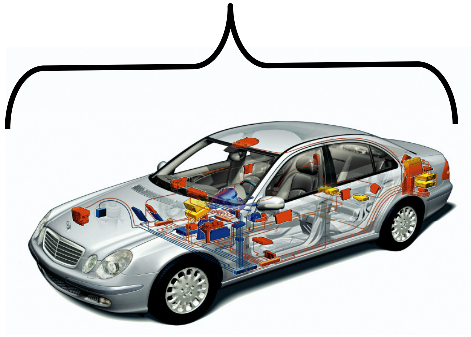
Security Baseline Architecture (cont'd)

- Basic ideas


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

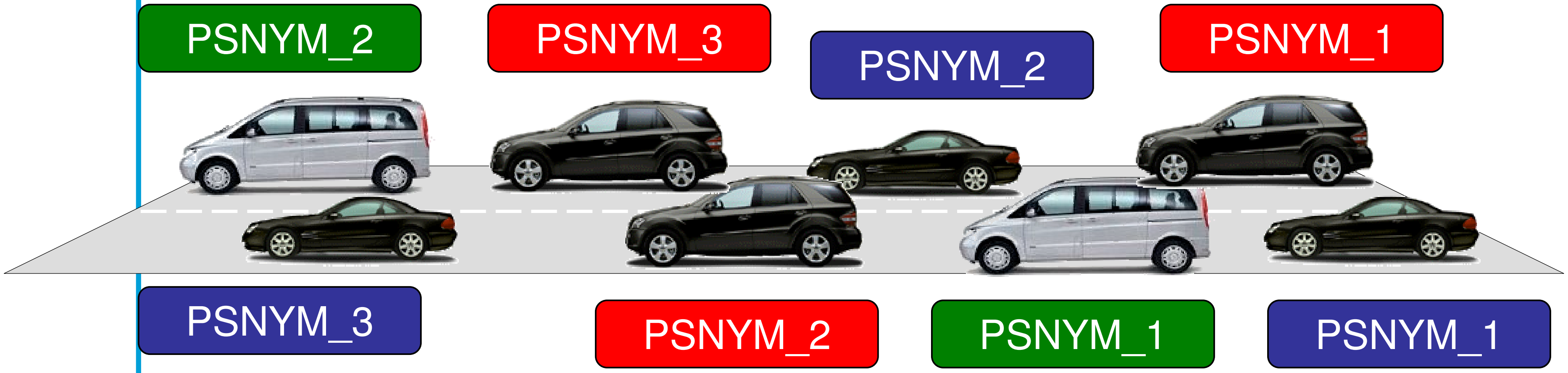
- **Long-term identity**
- **Public key crypto**
  - *EC-DSA, RSA*
- **Certificates**

Abstract view of a vehicle



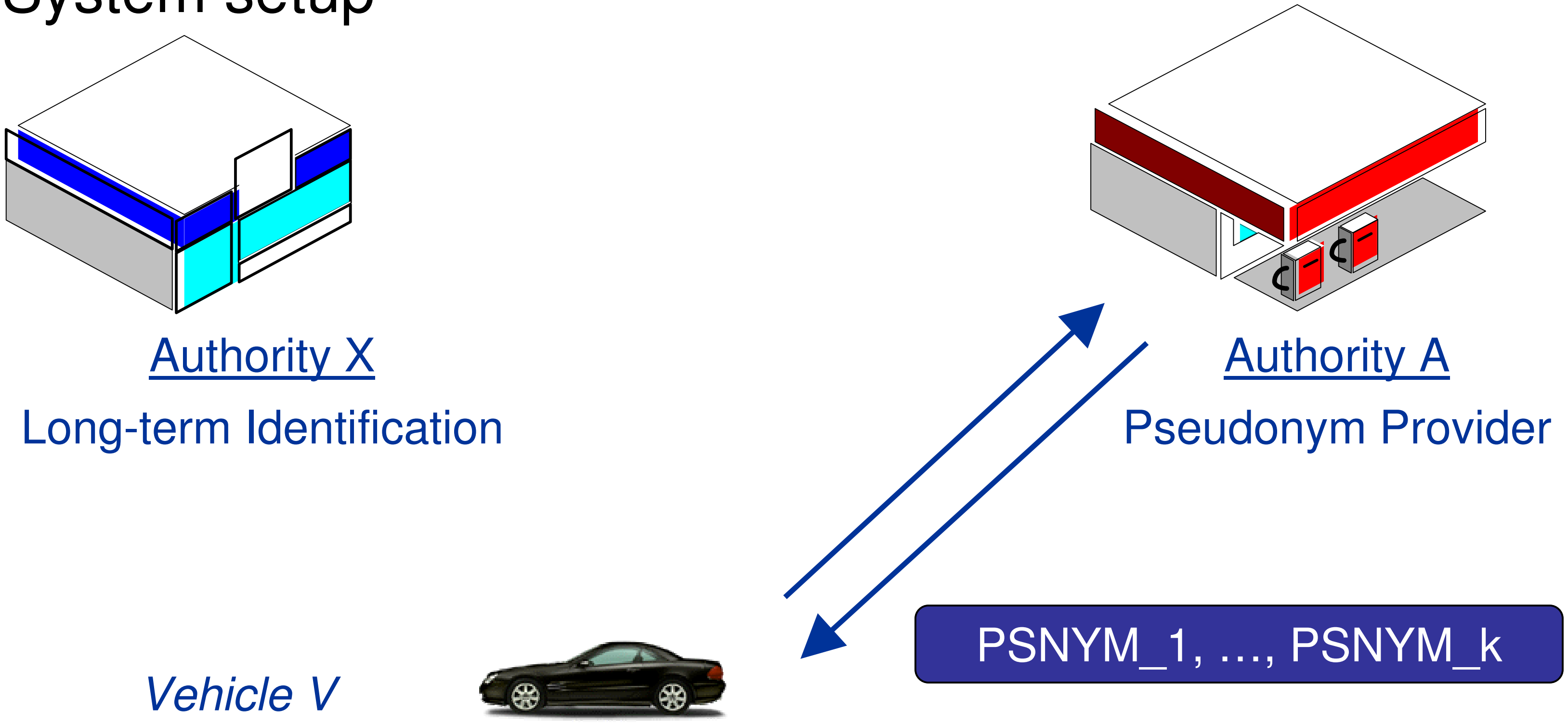
Security Baseline Architecture (cont'd)

- 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)

- System setup



Authority X

Long-term Identification

Authority A

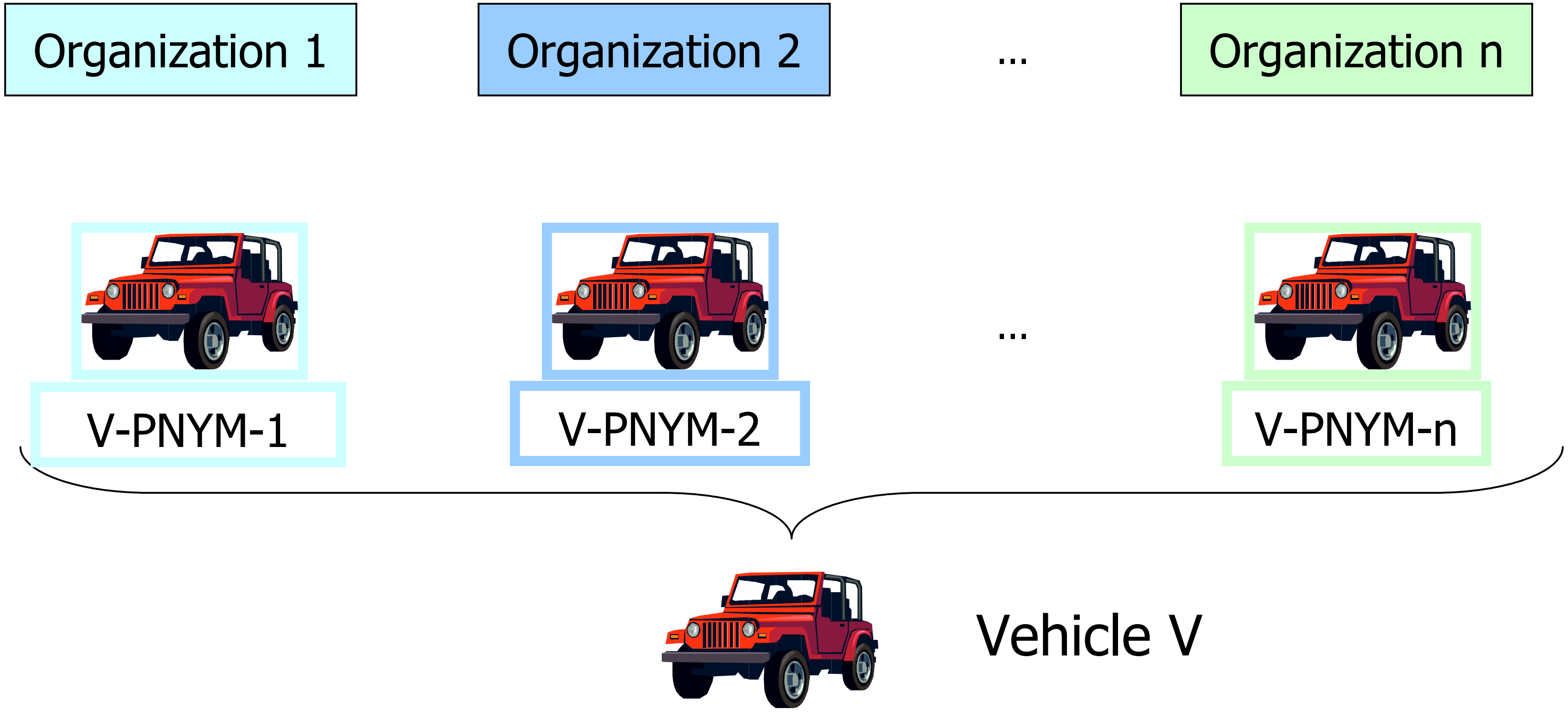
Pseudonym Provider

Vehicle V

PSNYM_1, …, PSNYM_k

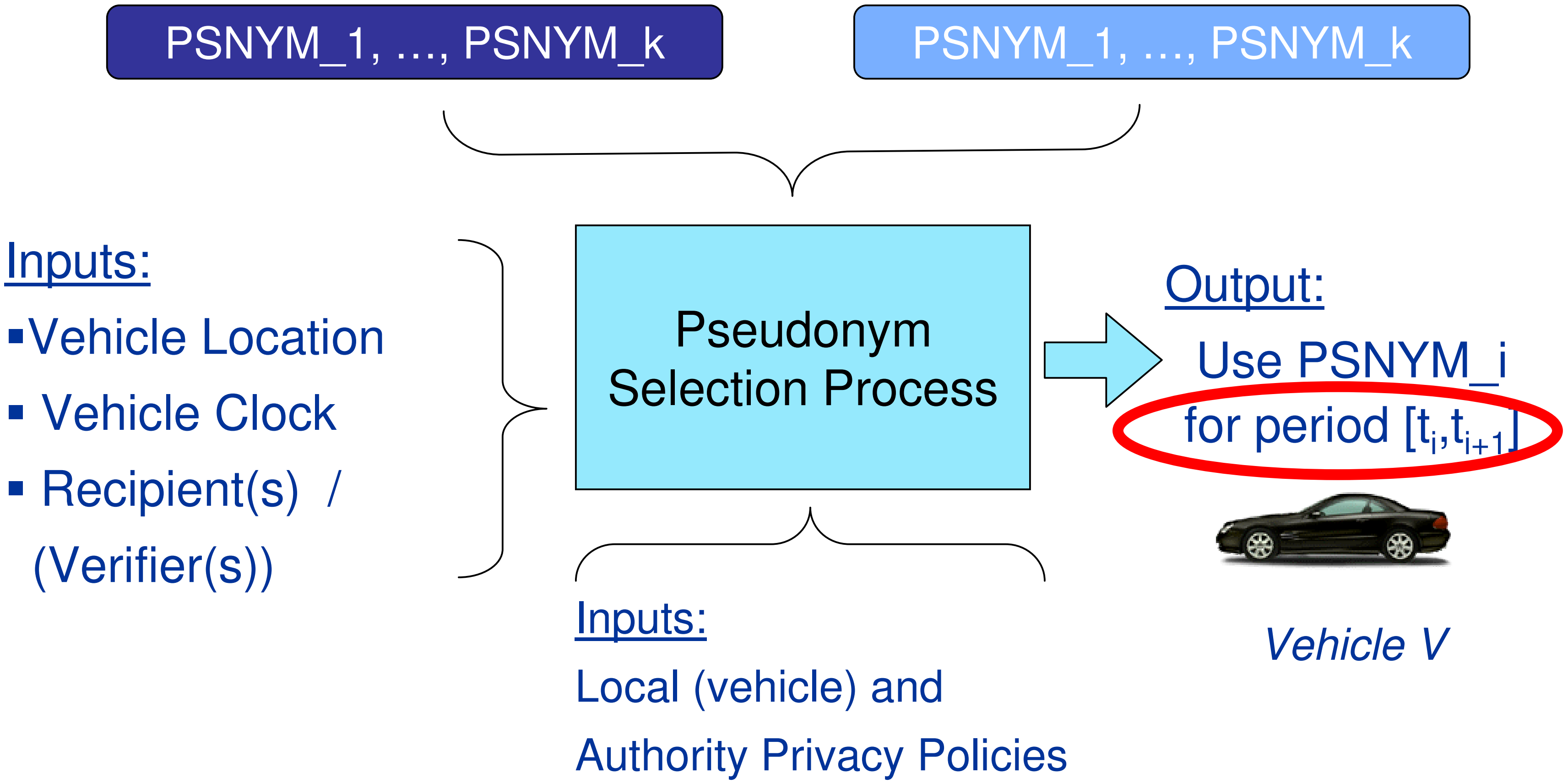
Security Baseline Architecture (cont'd)

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



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

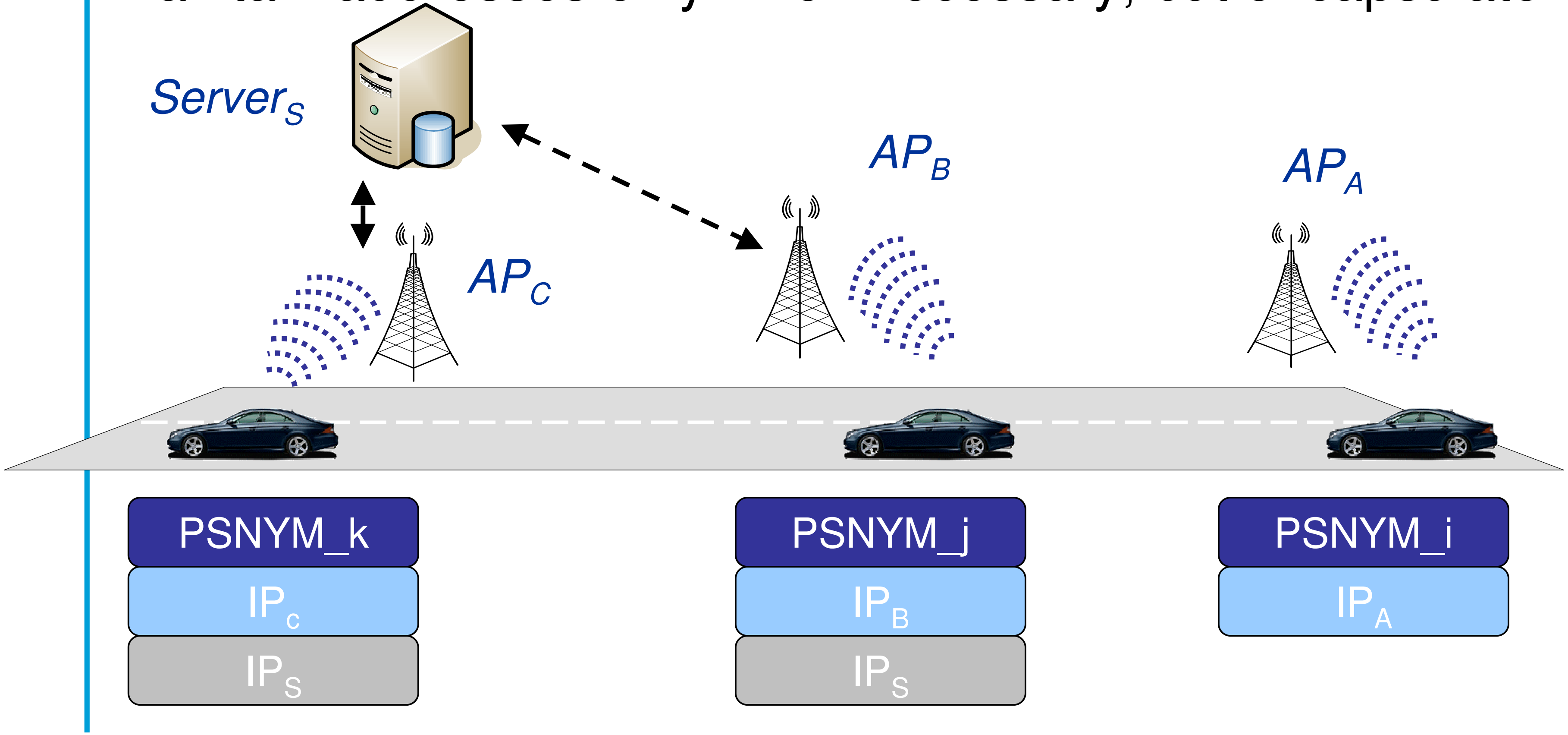
Inputs:

Local (vehicle) and Authority Privacy Policies

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

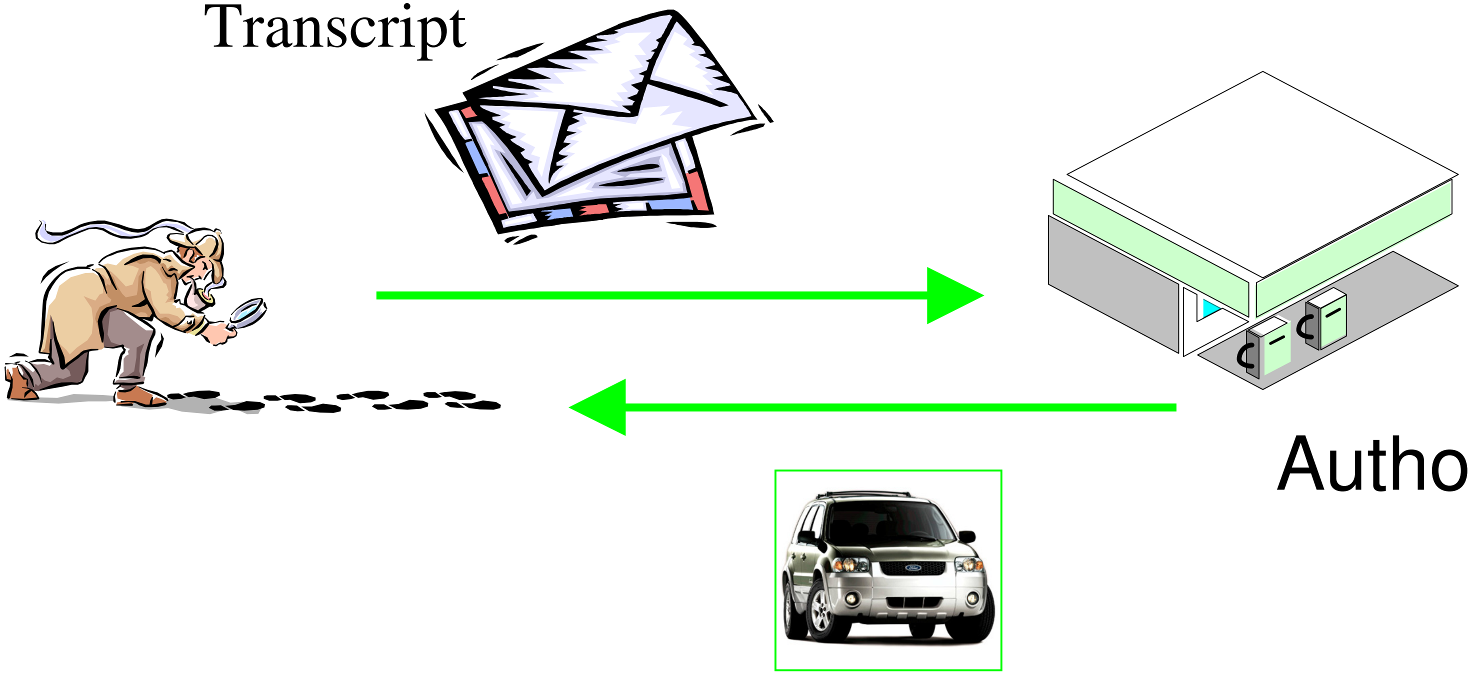
Privacy Baseline Architecture (cont'd)

- 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”

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

Thank You

www.sevecom.org