THE FULLY NETWORKED CAR

Dr. Panos Papadimitratos

Ecole Polytechnique Fédéral de Lausanne (EPFL)

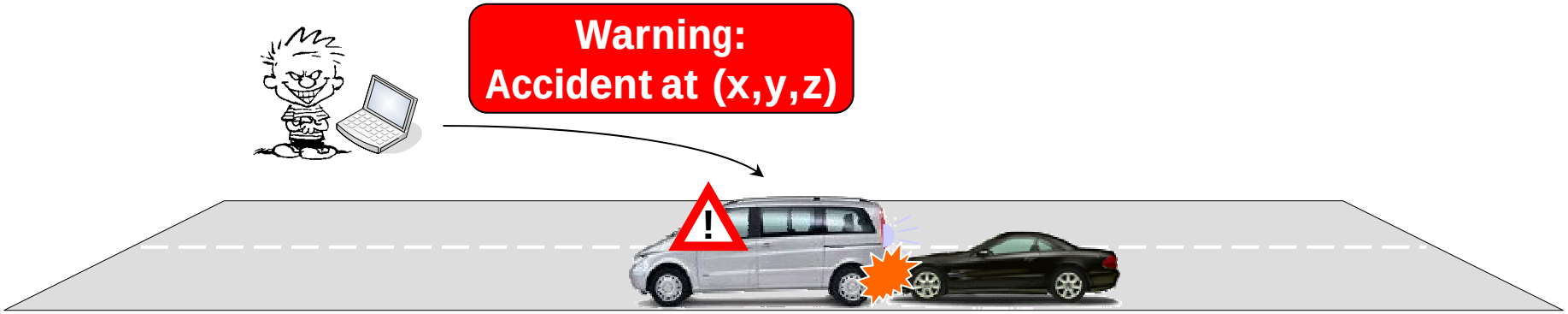
Geneva, 7-9 March 2007

Security in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) Communications

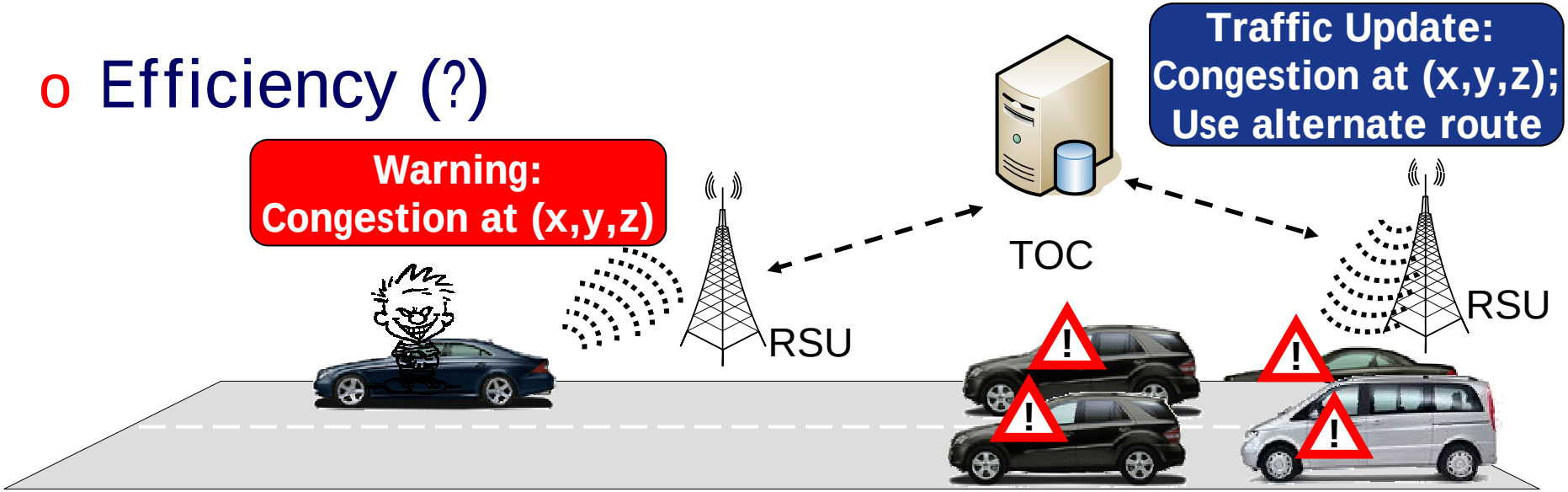
The Fully Networked Car
Geneva, 7-9 March 2007

Security and Privacy – Why?

- Safety (?)

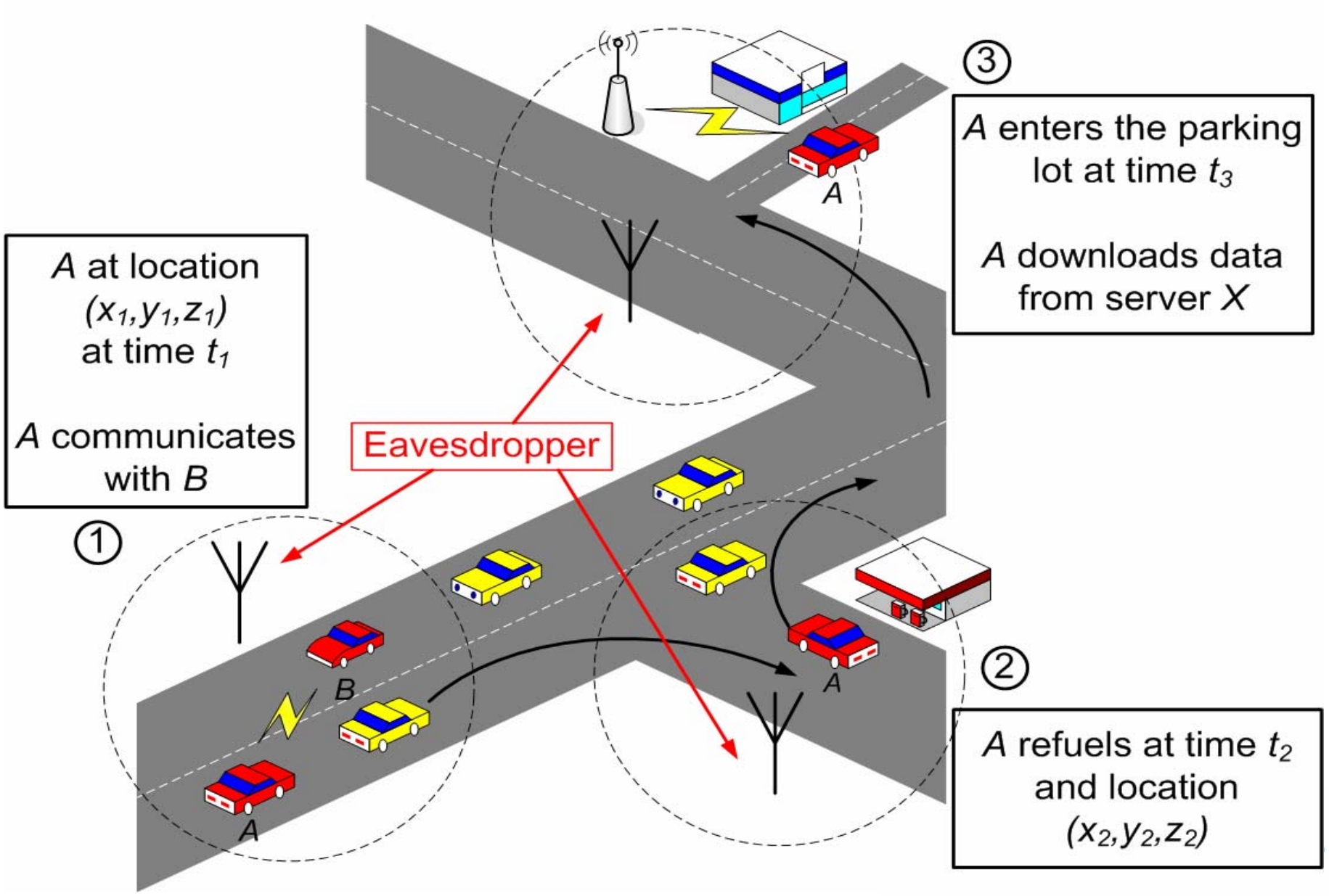


- Efficiency (?)

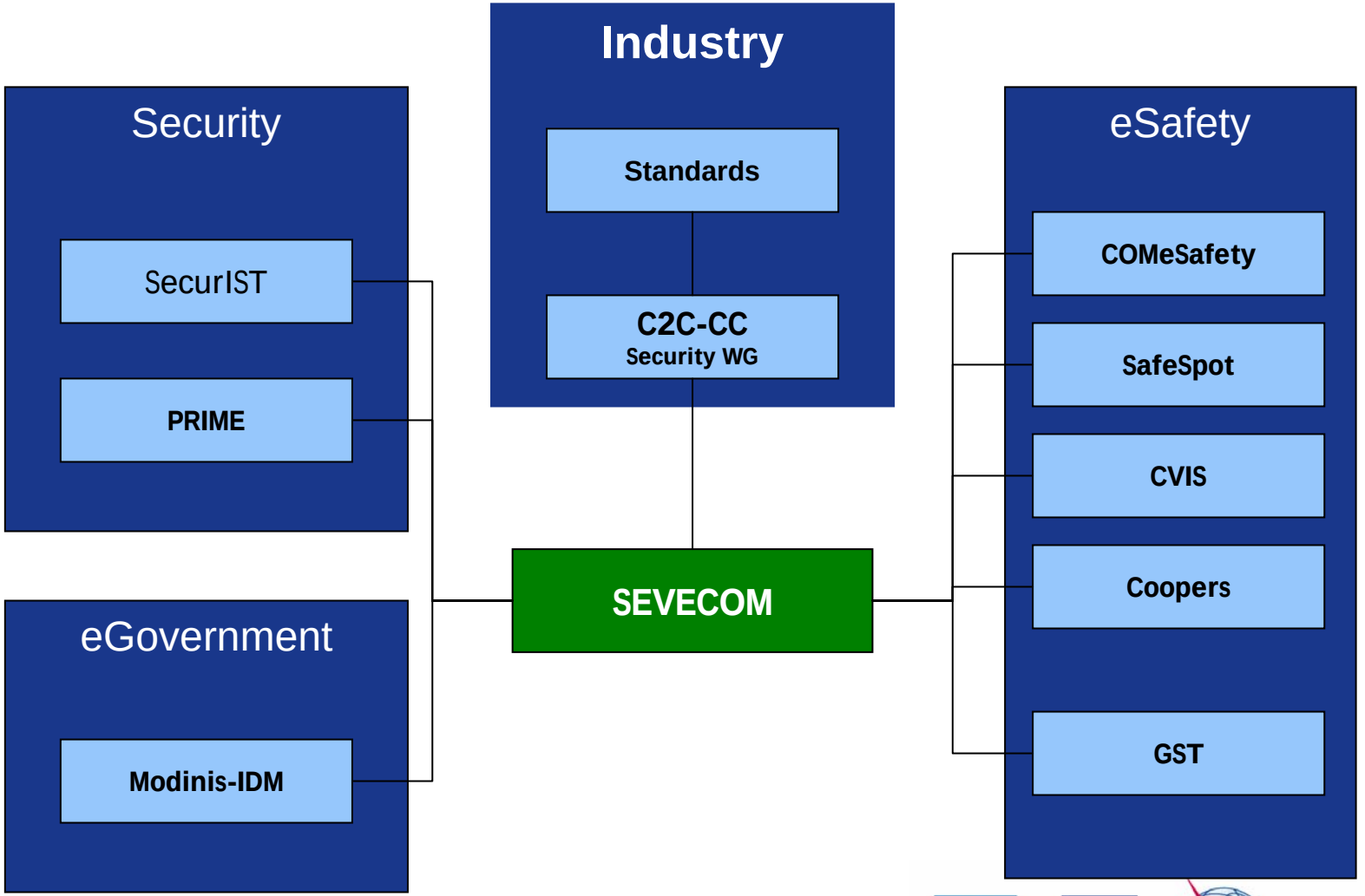


ISO IEC ITU International Telecommunication Union

Security and Privacy – Why?



SEVECOM is a Transversal Project



ISO IEC ITU International Telecommunication Union

Security Baseline Architecture

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

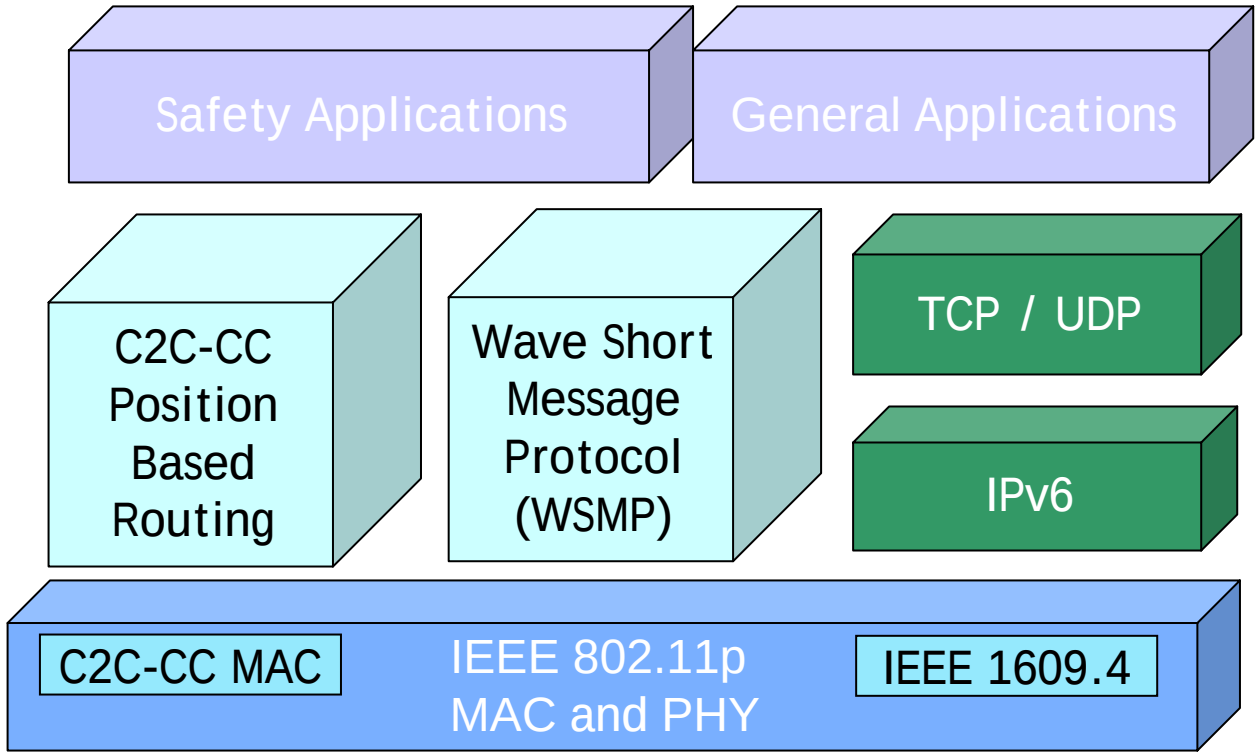
Security Baseline Architecture (cont'd)

- Objectives
  - Focus on communication
  - Baseline Privacy Enhancing Technology (PET)
  - Future dynamic deployment of stronger PETs

- Baseline solution design approach
  - Standardized cryptographic primitives
  - Easy-to-implement
  - Low overhead
  - Adaptable protection

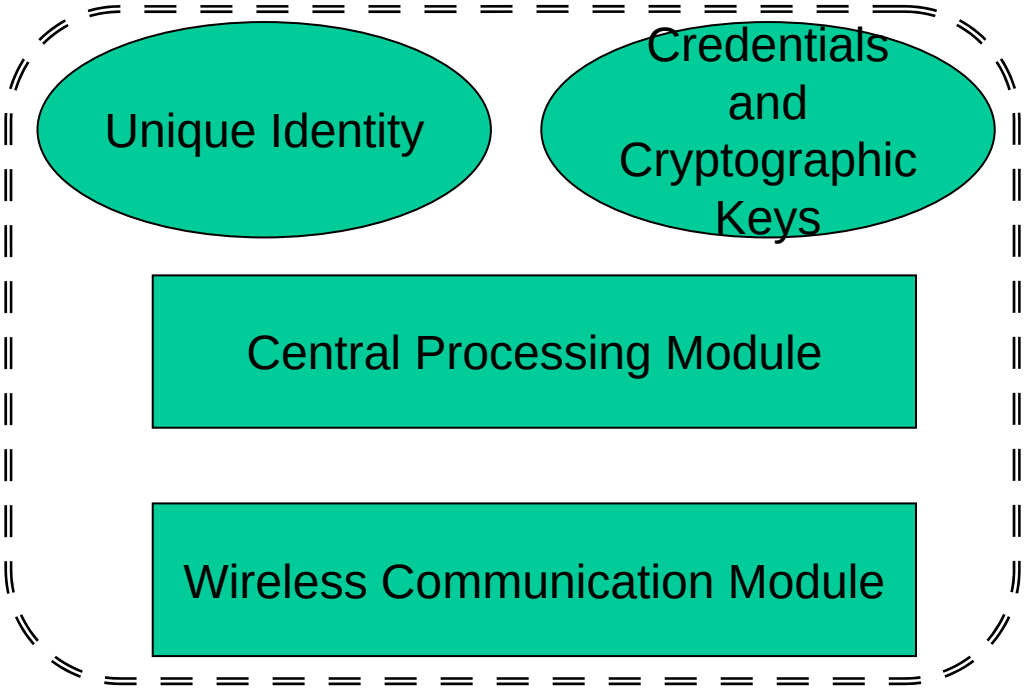
Security Baseline Architecture (cont'd)

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



Security Baseline Architecture (cont'd)

- Basic ideas



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

Abstract view of a vehicle

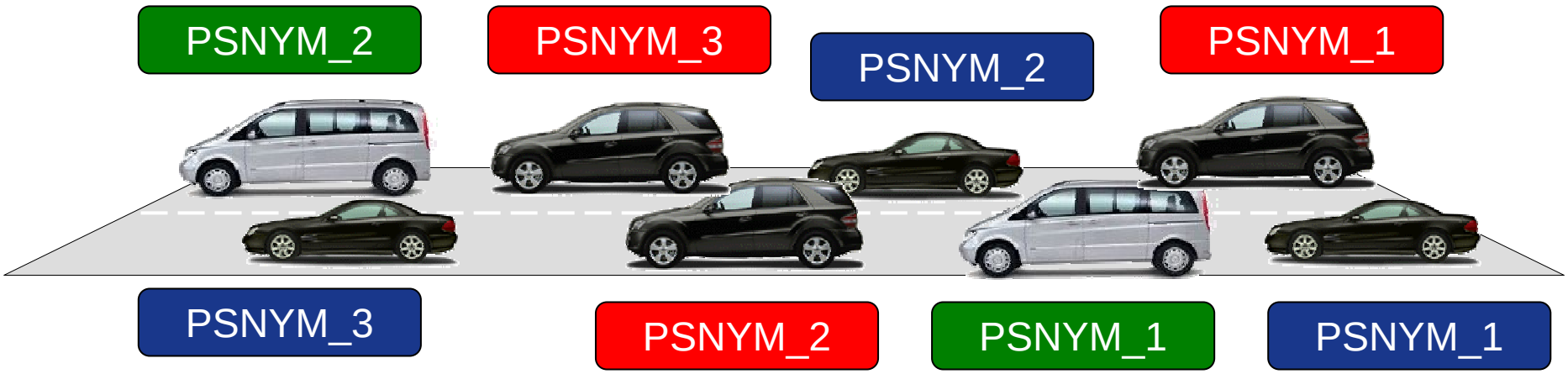
ISO IEC ITU International Telecommunication Union

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

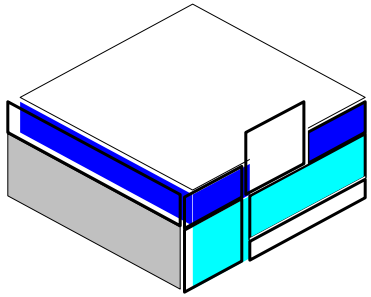
Security Baseline Architecture (cont'd)

- Basic Ideas (cont'd)
  - Using Pseudonyms



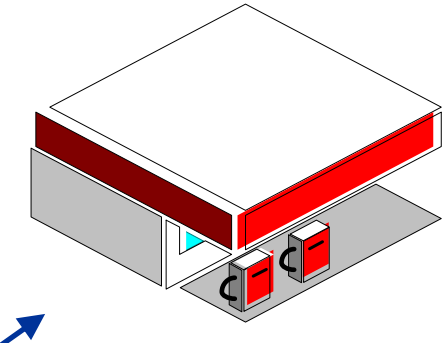
Security Baseline Architecture (cont'd)

- System setup



Authority X

Long-term Identification



Authority A

Pseudonym Provider

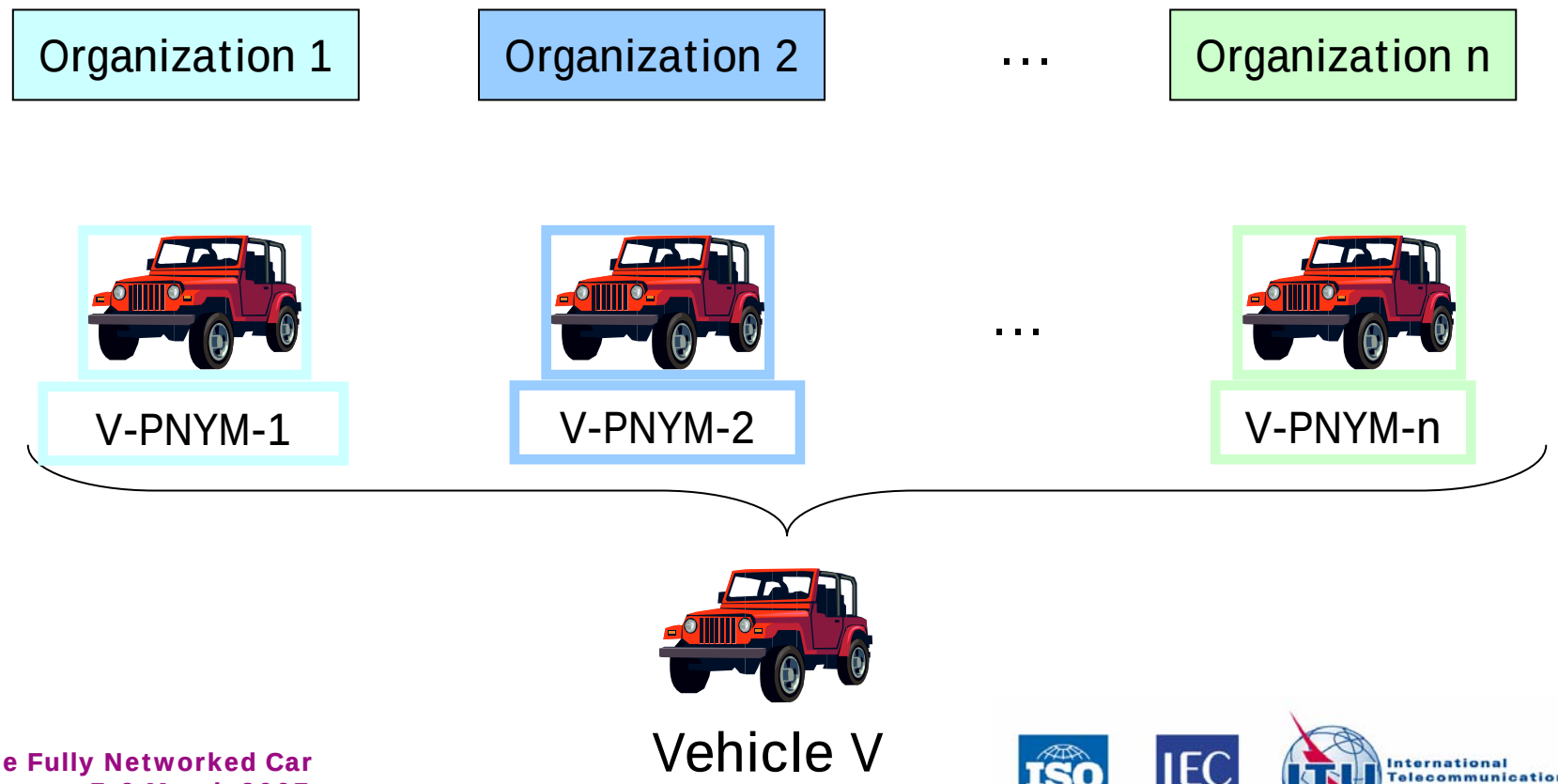
PSNYM_1, …, PSNYM_k

Vehicle V

ISO IEC ITU International Telecommunication Union

Security Baseline Architecture (cont'd)

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



Security Baseline Architecture (cont'd)

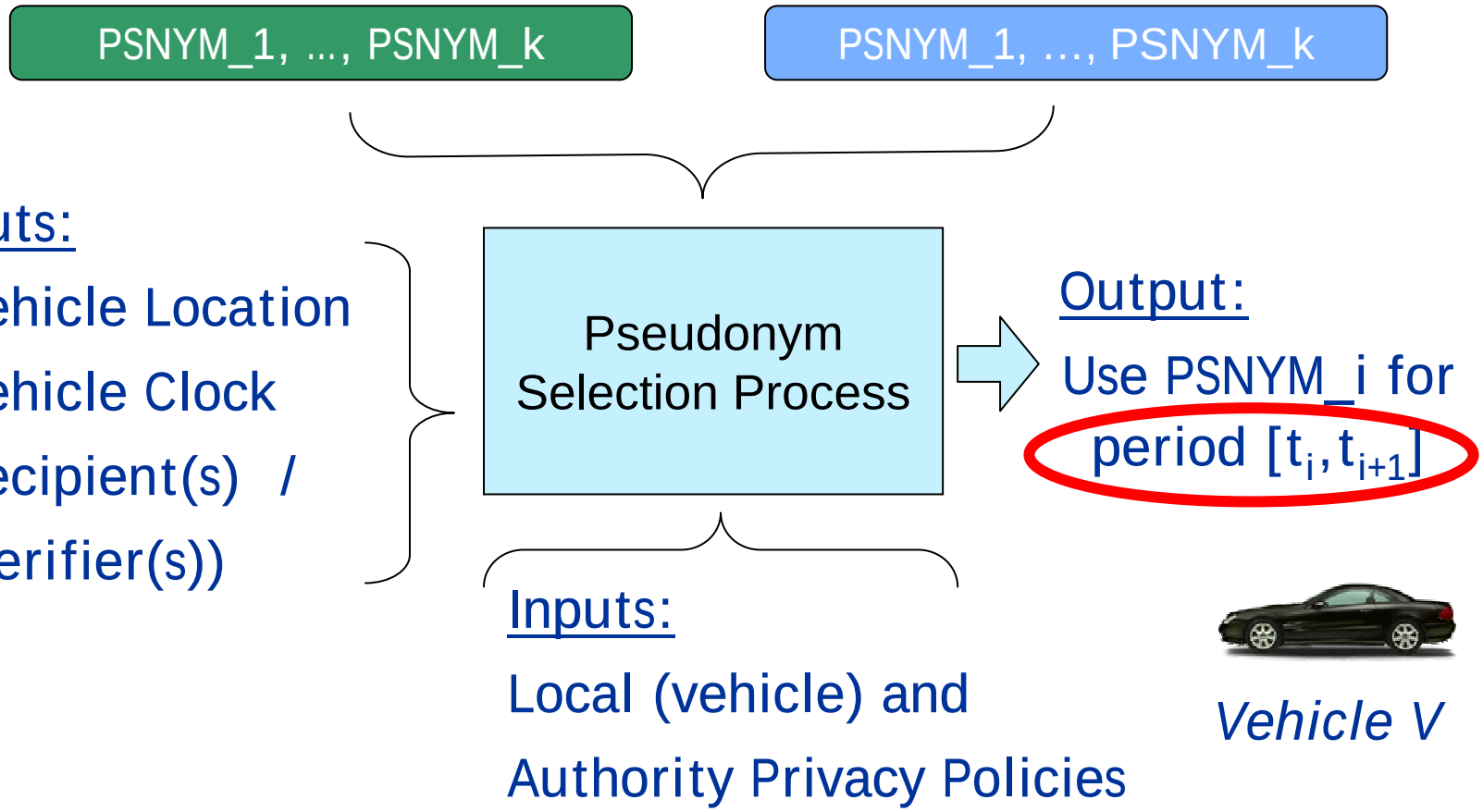
- Pseudonym format

PSNYM-Provider ID	PSNYM Lifetime
Public Key	
PSNYM-Provider Signature	

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

Security Baseline Architecture (cont'd)

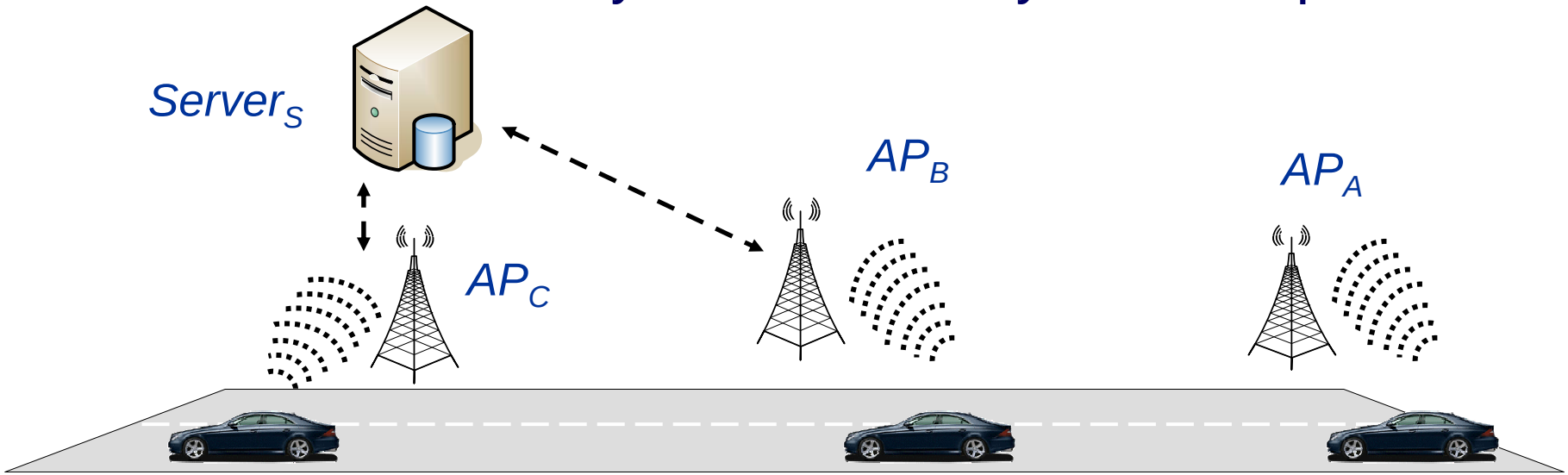
- Pseudonym Change Mechanism



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

Security Baseline Architecture (cont'd)

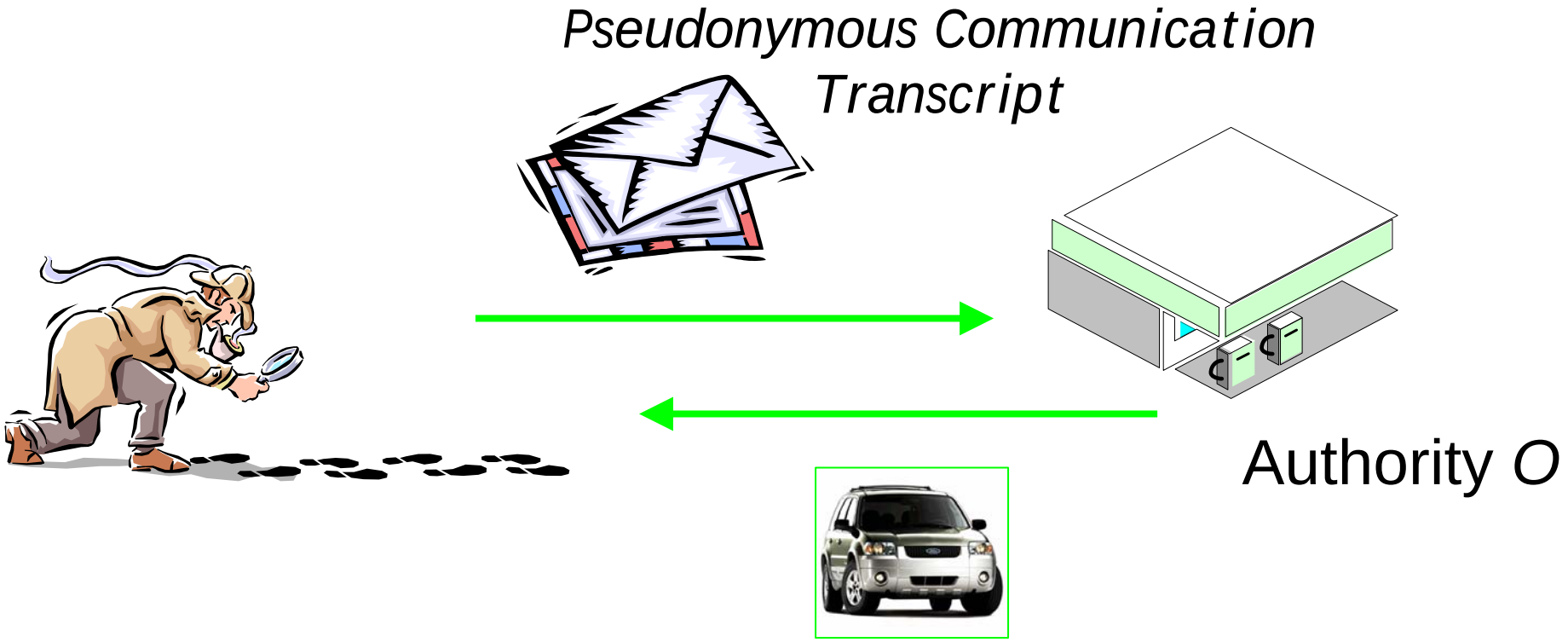
- Other vehicle network identifiers: e.g., IP and MAC addresses
- Change addresses along with pseudonyms
- Maintain addresses only when necessary, but encapsulate



ISO IEC ITU International Telecommunication Union

Security Baseline Architecture (cont'd)

- Pseudonym resolution



Security 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

Thank you!

- Questions?

- http://www.sevecom.org