Secure Vehicle Communication

Security in Architectures for Cooperative Systems

Antonio Kung

Trialog

antonio.kung@trialog.com

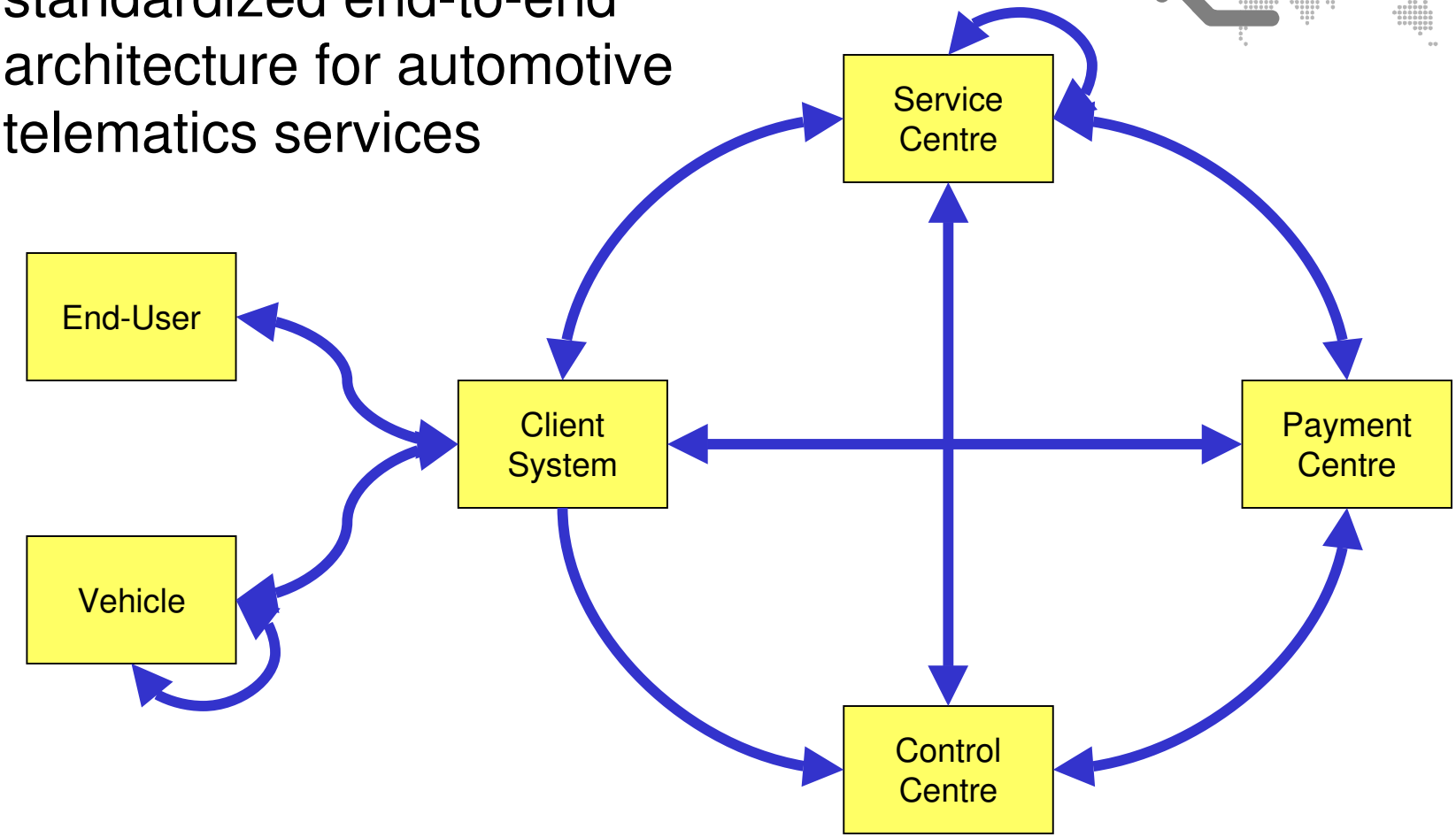
http://www.sevecom.org/

Presentation Outline

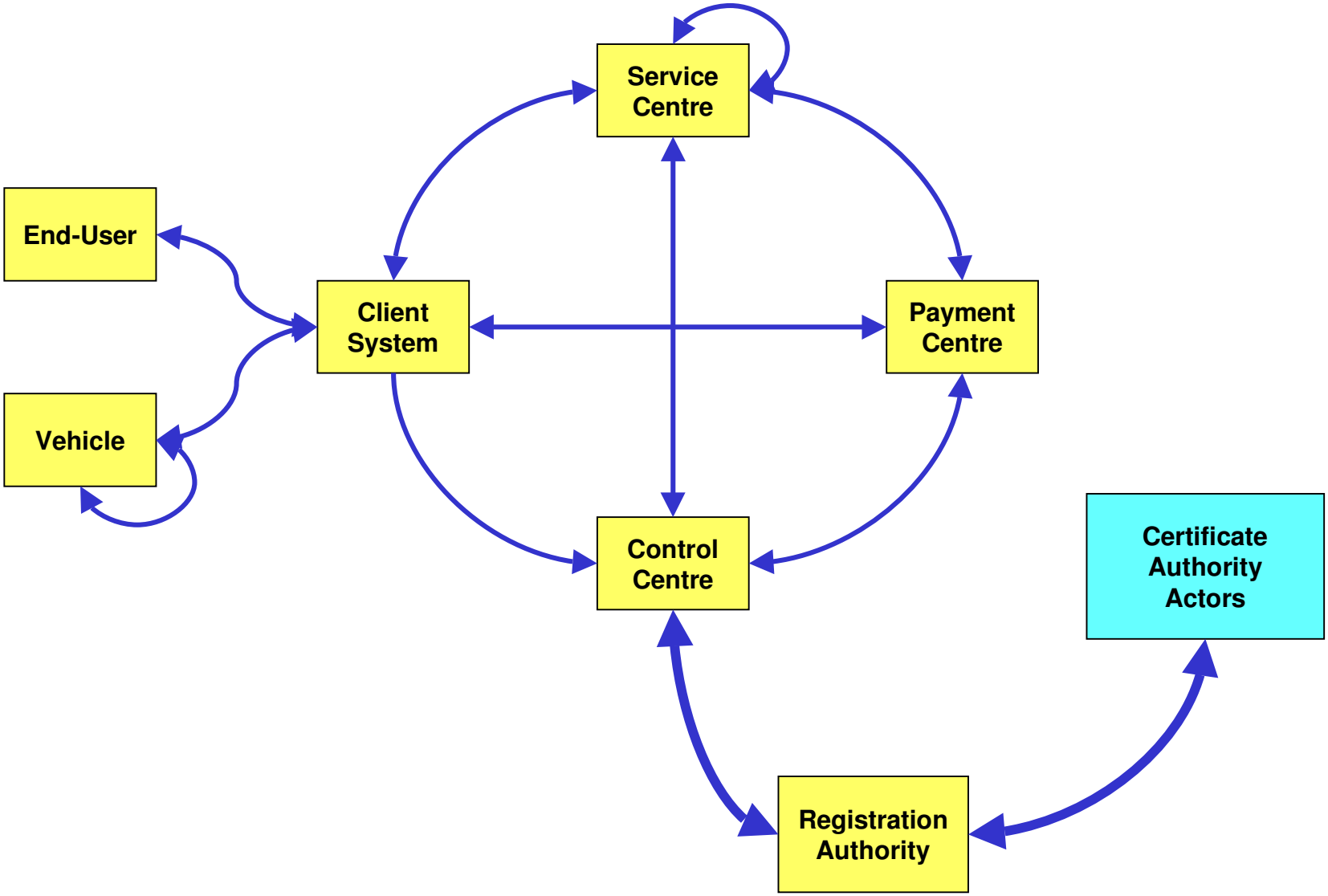
- The GST Security Architecture
- Requirements for security in V2V and V2I infrastructures
- The SEVECOM Initiative

Global Systems for Telematics

- GST : creating an open and standardized end-to-end architecture for automotive telematics services

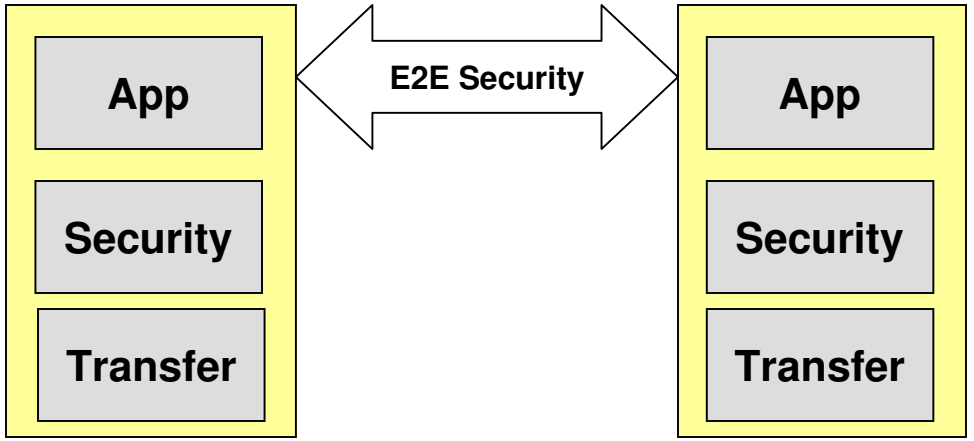


Security Impact on Infrastructure

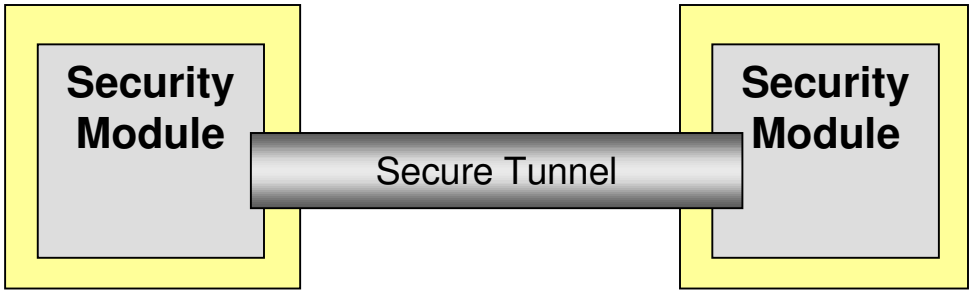


Security impact on Communication

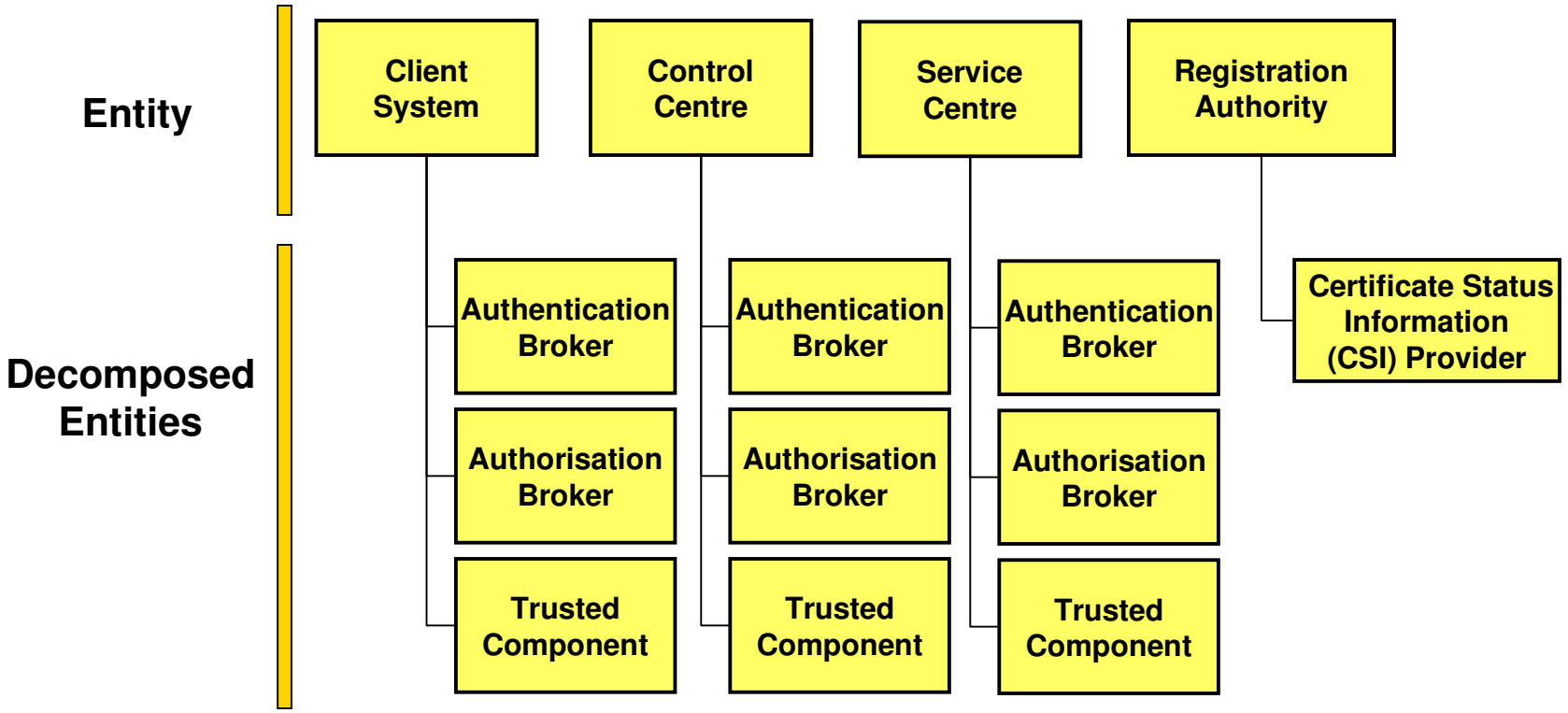
- 4 levels of communication
  - Insecure, Authenticated, Confidential, Secure (A+C)
- Layered view



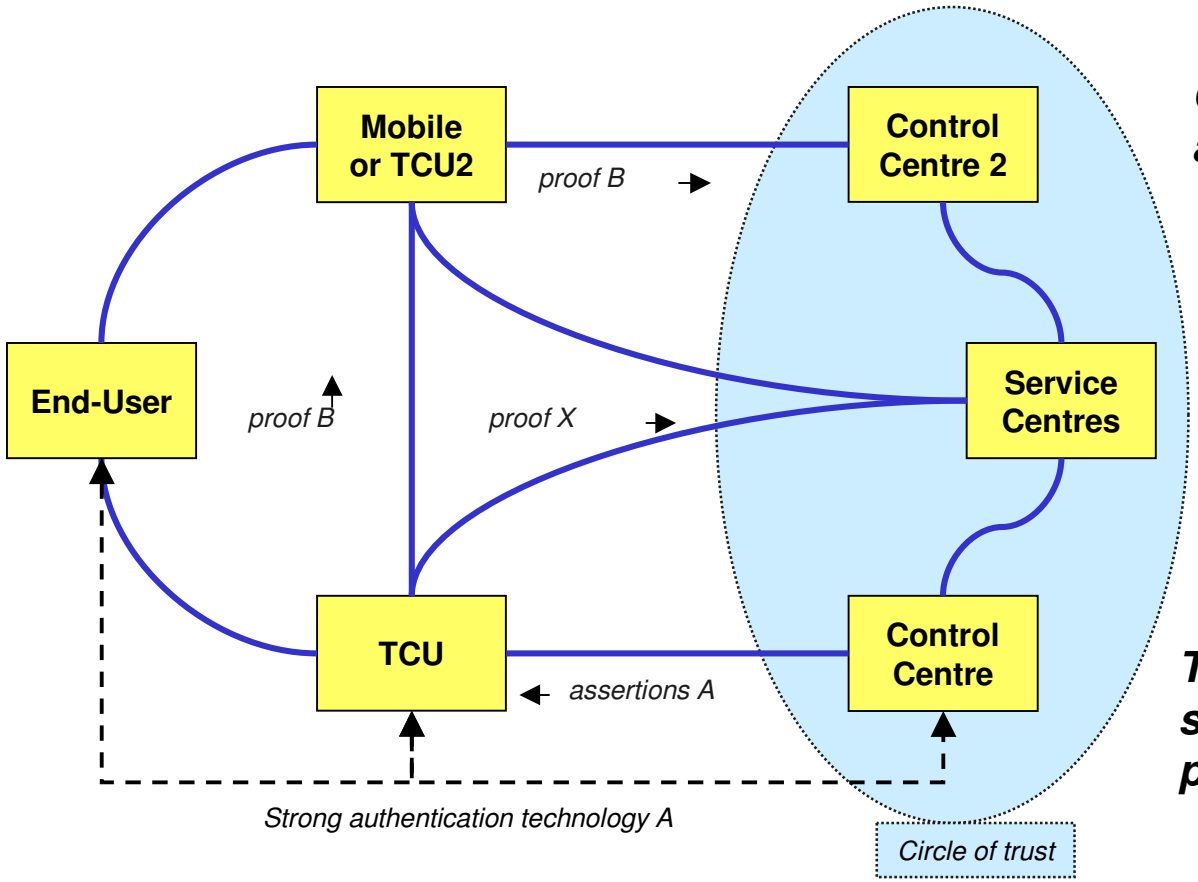
- Platform view



Security impact on Nodes



One User, N Business Stakeholders

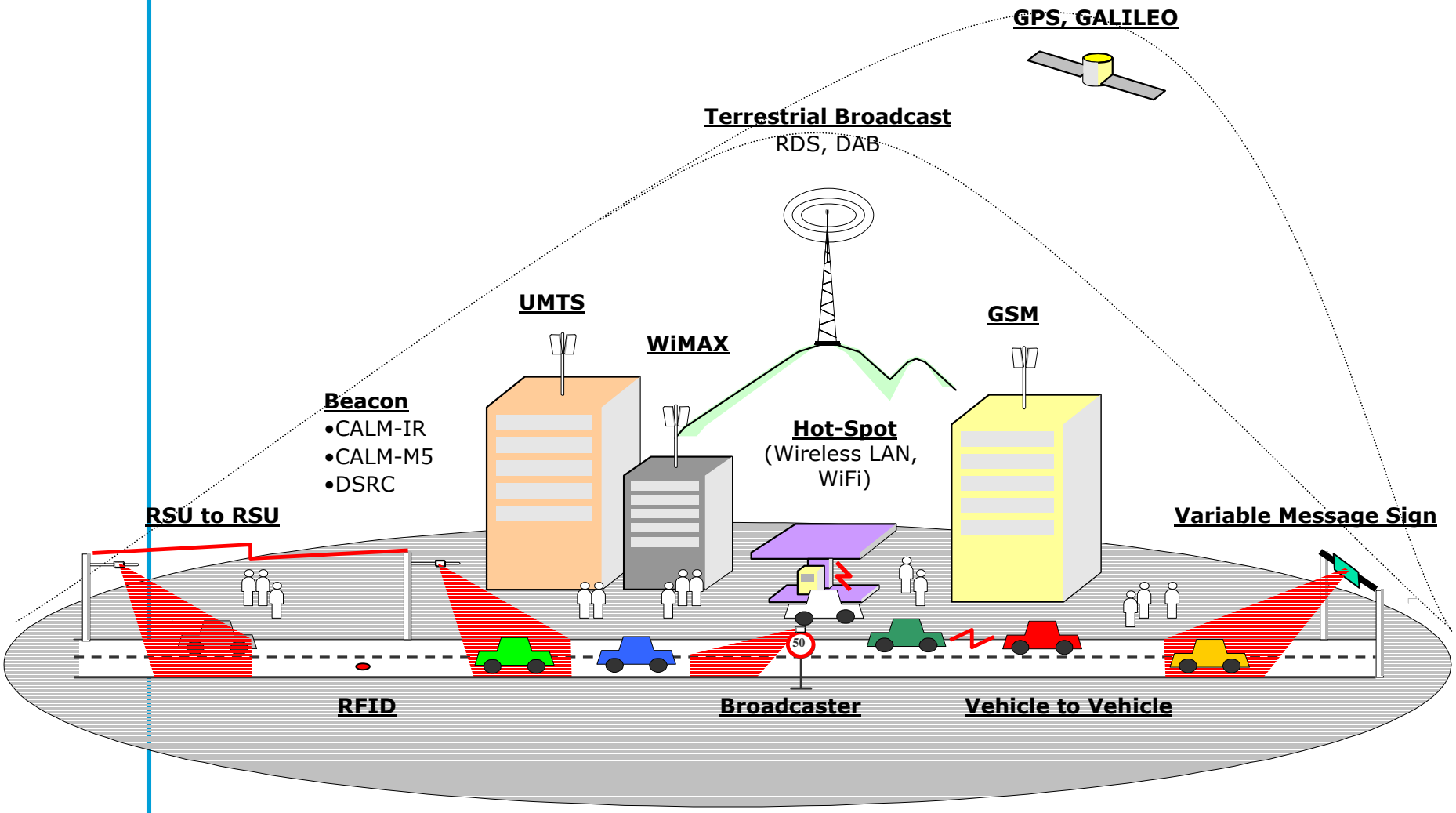


One single authentication

Business stakeholders share identifications

Through some security protocols

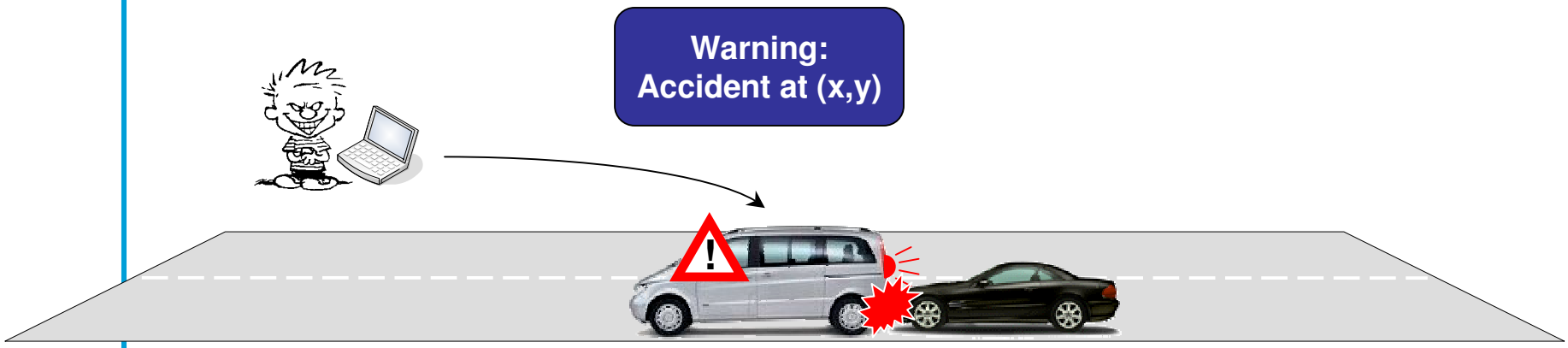
Requirements for V2V/V2I Infrastructure



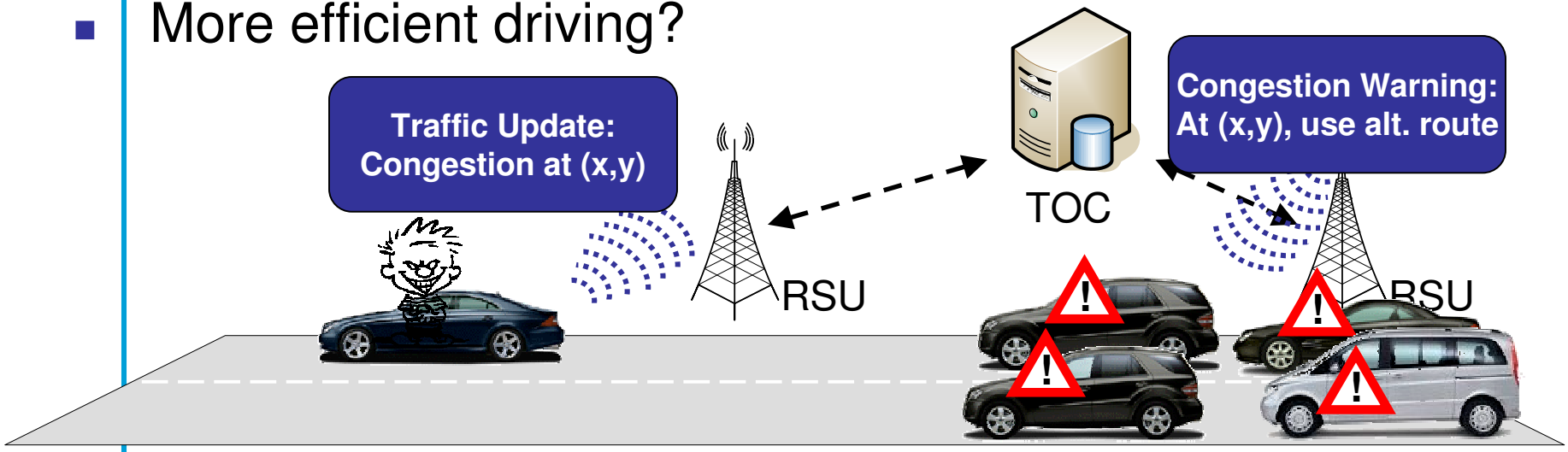
Security and Privacy???

SEVECOM

- Safer roads?

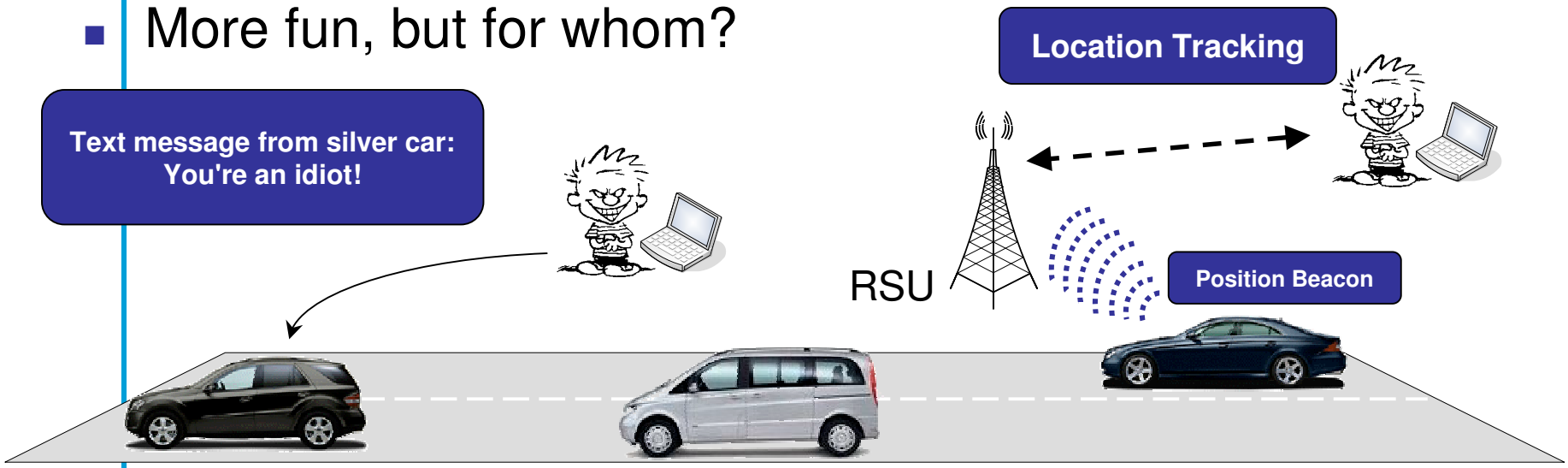


- More efficient driving?

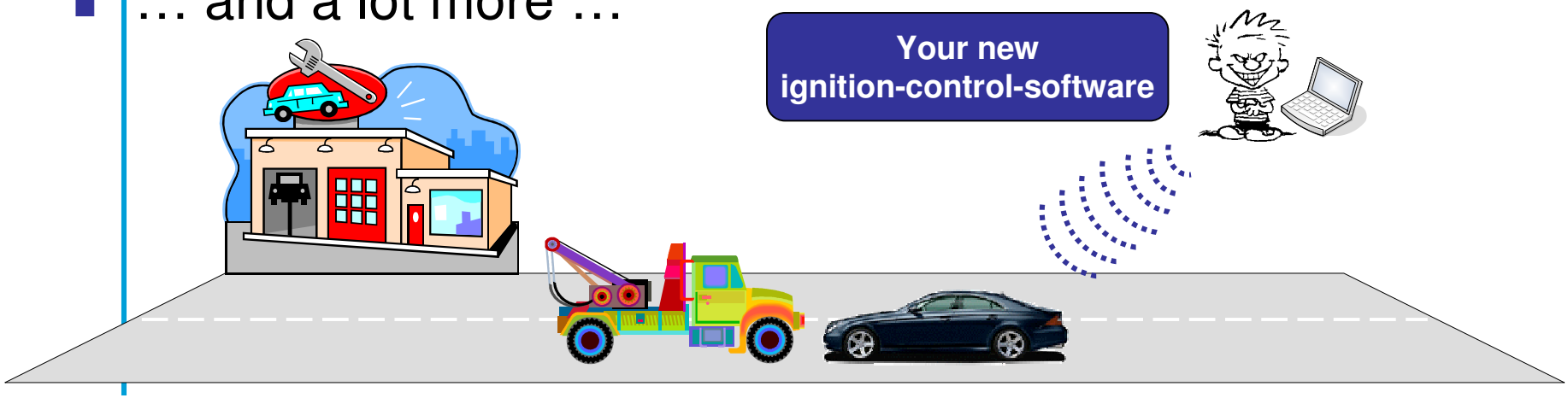


Security and Privacy???

- 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

- IST STREP Project. 1/1/2006-1/1/2009
- Partners
  - Trialog (Coordinator)
  - DaimlerChrysler
  - Centro Ricerche Fiat
  - Philips
  - Ecole Polytechnique Fédéral de Lausanne
  - University of Ulm
  - Budapest University of Technology and Economics

Objectives

SEVECOM

- Large projects have explored and will explore vehicular communications
  - Fleetnet, NOW, CVIS, Safespot, Coopers, …
  - But no solution can be deployed if not properly secured
- Problems and Opportunities
  - A real setting with real scenarios and applications
  - Very dynamic network with high speeds and real-time constraints
  - Real-world constraints, e.g. who will pay for CA?
  - No energy constraints
  - Contradictory expectations (e.g. position vs. privacy)
- SEVECOM will focus on:
  - Identification of threats against the communication system, transferred data, and the vehicle itself
  - Specification of a usable security architecture
  - The definition of suitable cryptographic primitives

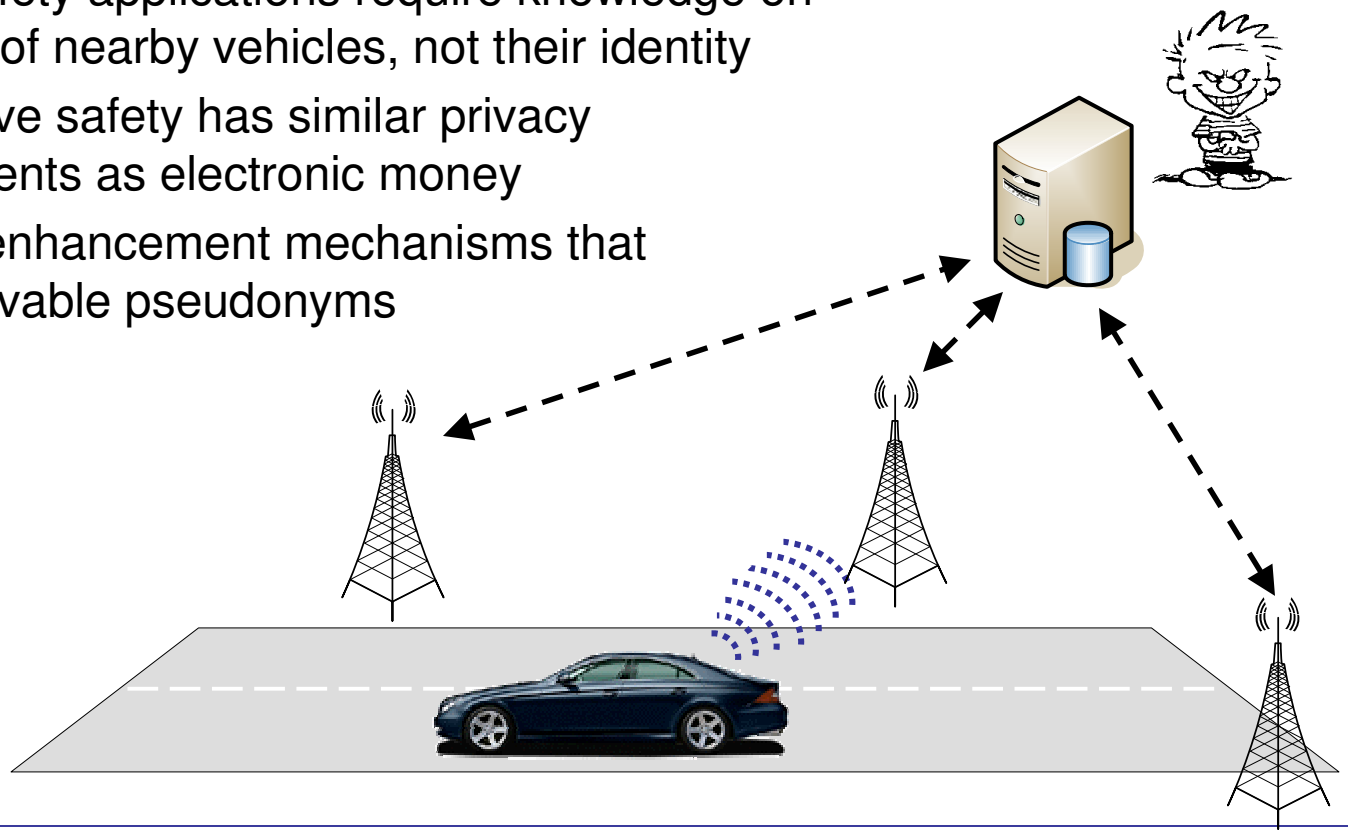
Research topics

	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

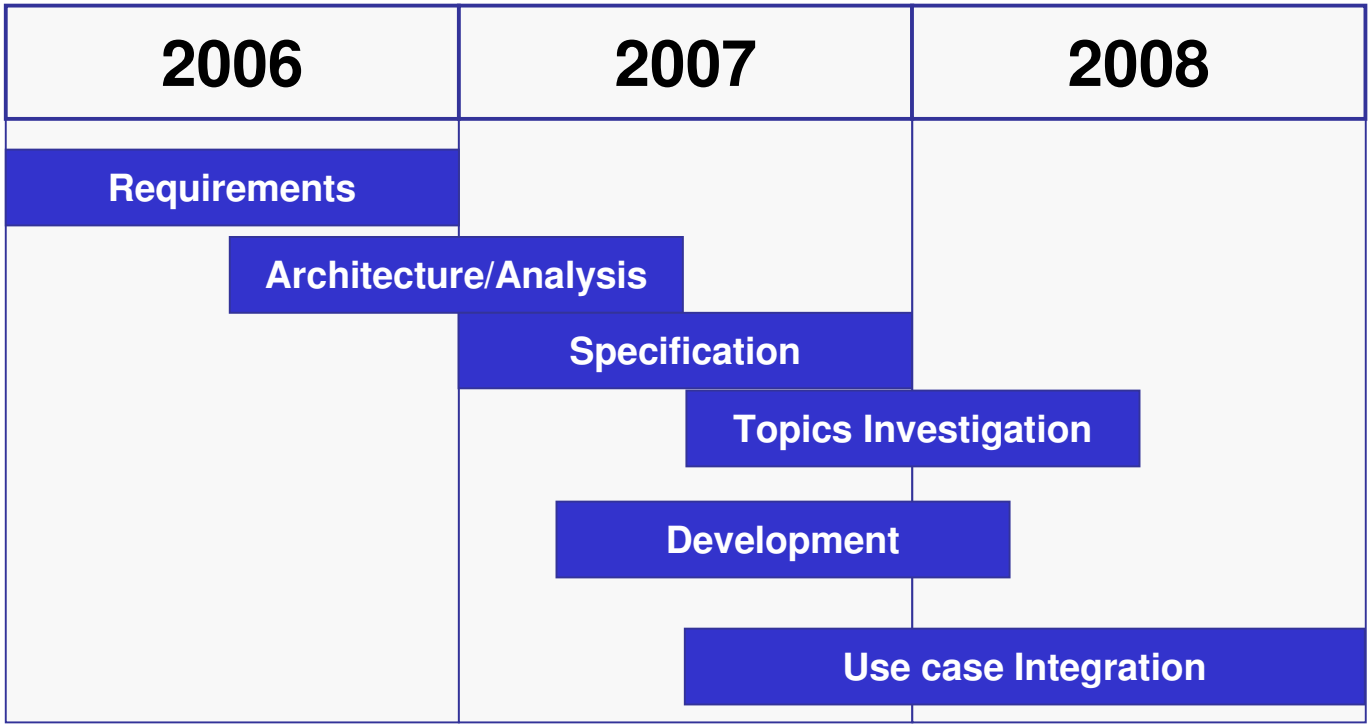
Example: A6 – Privacy

- 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
  - Automotive safety has similar privacy requirements as electronic money

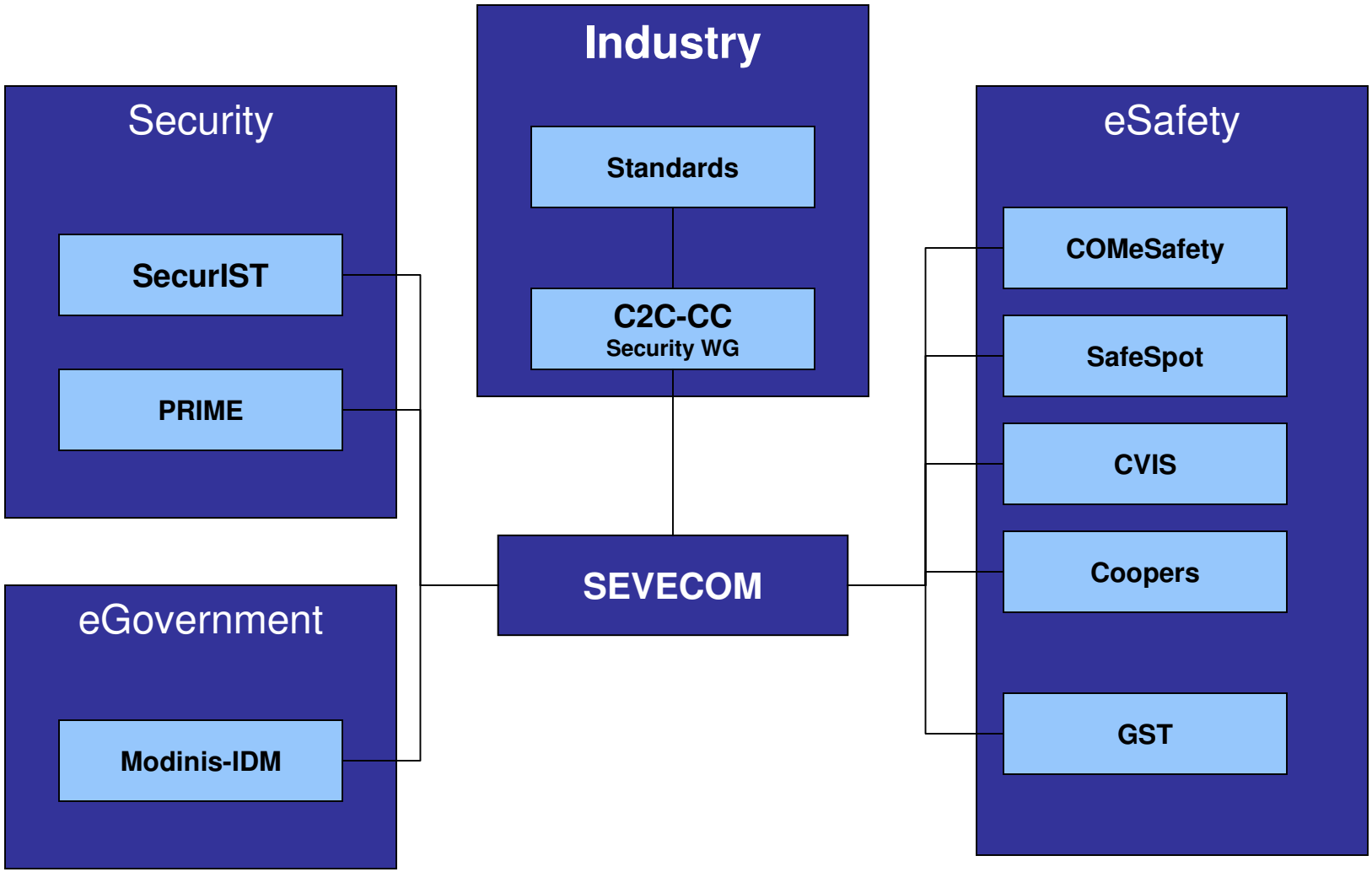
➔ Privacy-enhancement mechanisms that use resolvable pseudonyms



Timetable


2006
2007
2008
Requirements
Architecture/Analysis
Specification
Topics Investigation
Development
Use case Integration

SEVECOM is a Transversal Project



Questions?