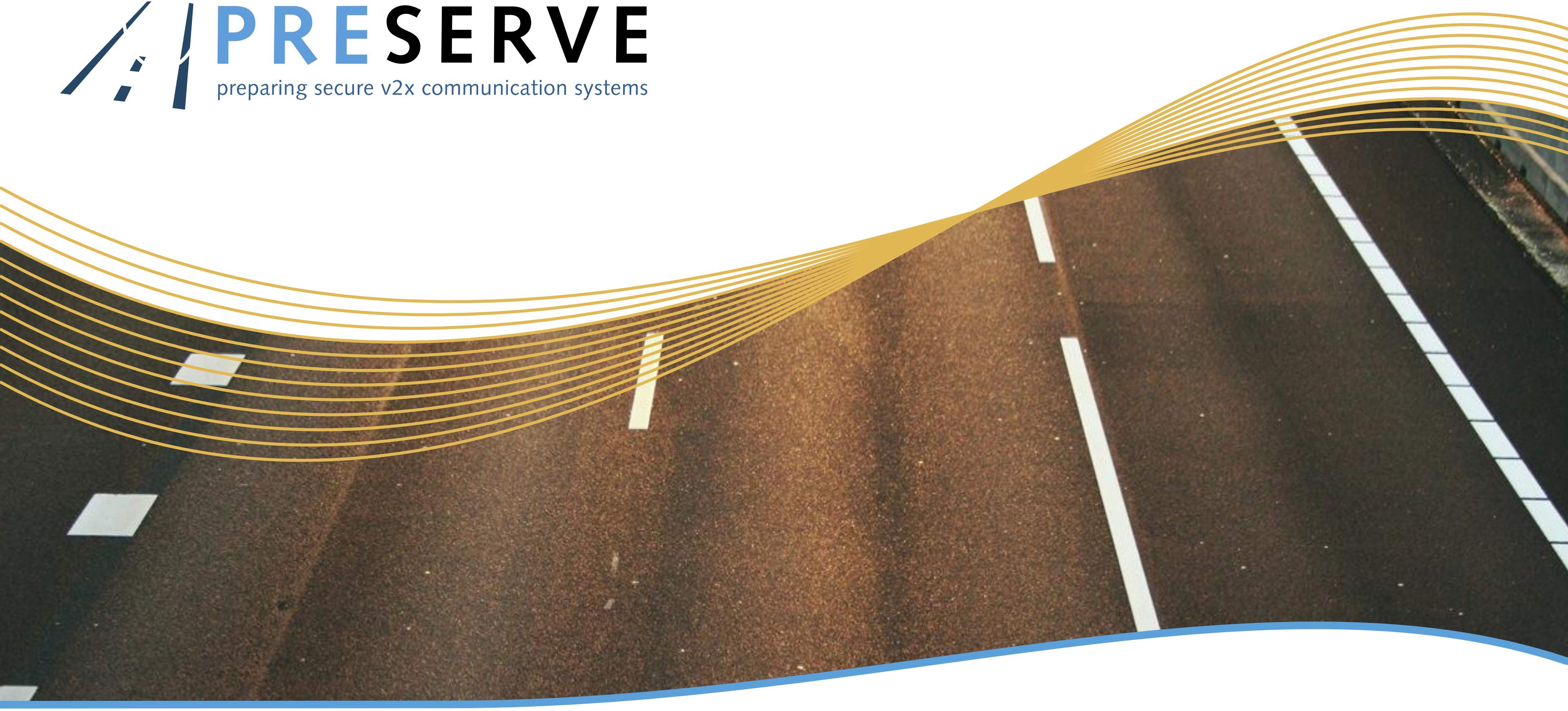
PRESERVE
preparing secure v2x communication systems



# ICT and Privacy: Barriers

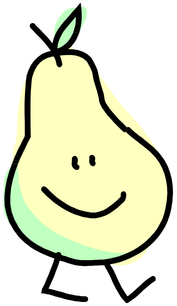
Antonio Kung| Trialog. 25 Rue du Général Foy, 75008, Paris, France | 11.10.2012

# Trialog (www.trialog.com)

- French SME
  - Founded in 1987
  - Traded in French SME stock exchange
- Focusing on embedded systems
  - Research to prepare innovation
  - Helping industry with innovation
- PARIS (PrivAcy pReserving Infrastructure for Surveillance) to start in 2013

# Content of Presentation

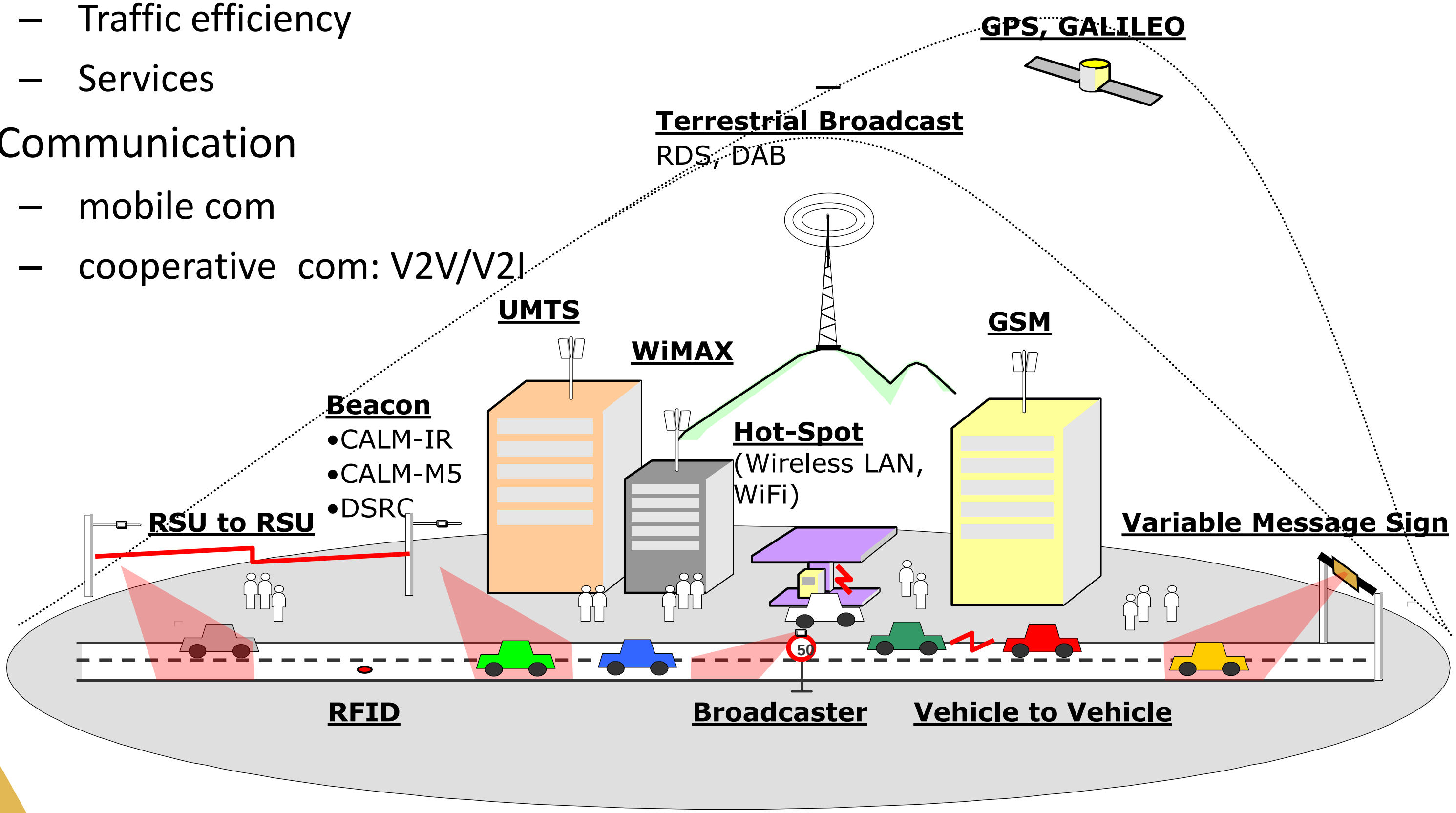
- Experience on ICT and privacy in ITS (Intelligent Transport Systems)
- The architecture barrier
  - Privacy Enhancing Architectures (PEARs)
- Other barriers



PRESERVE
preparing secure v2x communication systems

# Example of Intelligent Transport System (ITS)

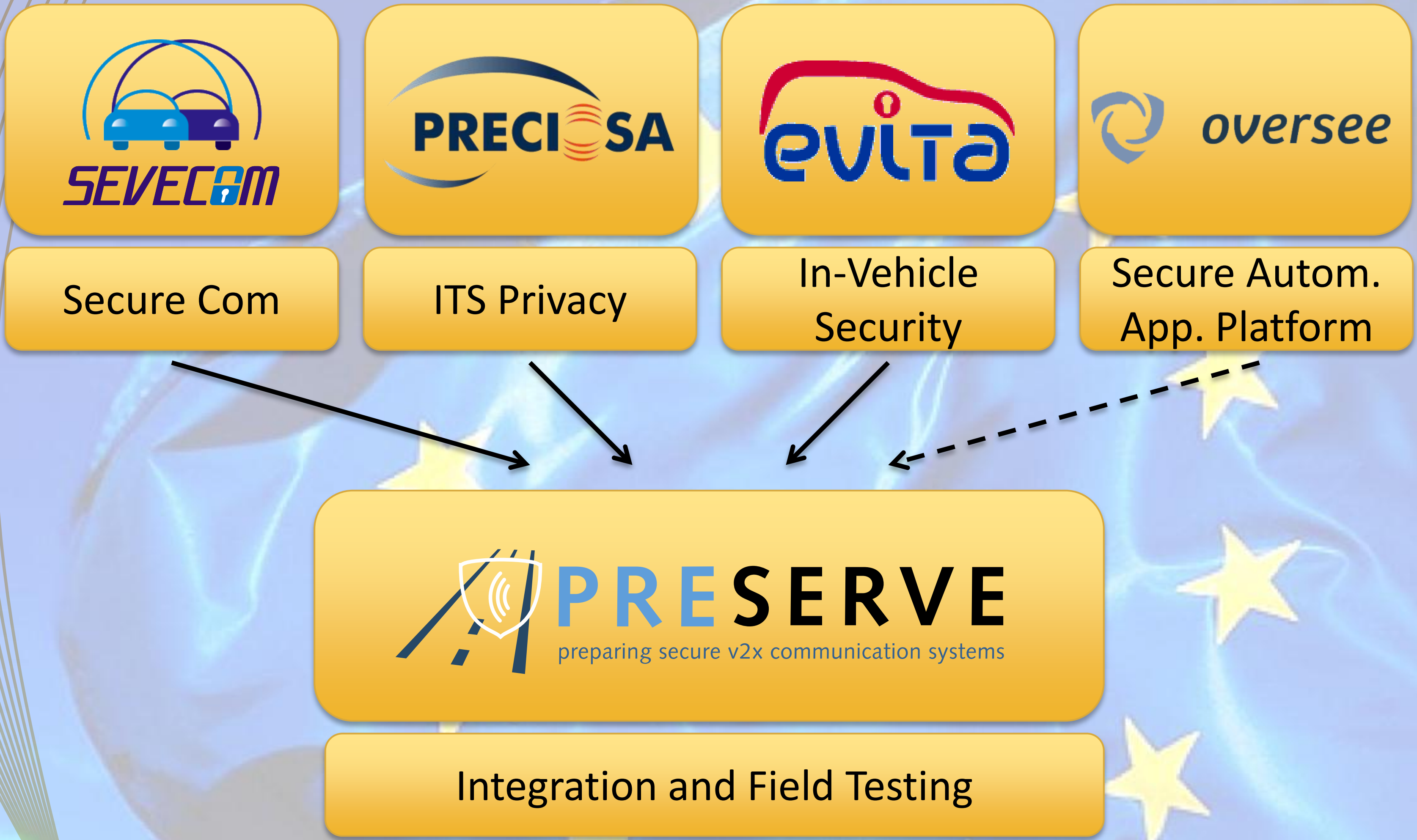
- Apps
  - Safety,
  - Traffic efficiency
  - Services
- Communication
  - mobile com
  - cooperative com: V2V/V2I



Courtesy CVIS

# Action Plan for deployment of Intelligent Transport Systems (ITS) in Europe: 24 Actions

| Area 1 | Area 2 | Area 3 | Area 4 | Area 5 | Area 6 |
|---|---|---|---|---|---|
| **Optimal Use of Road, Traffic & Travel Data** | **Continuity of Traffic & Freight Management** | **Road Safety and Security** | **Integration of Vehicle & Transport Infrastructure** | **Data Protection & Liability** | **European ITS Coordination** |
| EU-wide real time travel information | Continuity of ITS services | Promotion of in-vehicle safety systems | Open in-vehicle Platform architecture | **Security & data protection** | Legal framework for EU ITS cooperation |
| Collection & provision of road data | Services for freight transport & logistics | Introduction of Europe-wide eCall | Development & evaluation of coop. systems | Addressing liability, esp. in-vehicle safety systems | Decision support toolkit for ITS investments |
| Accurate public data for digital maps | European ITS Framework architecture | Regulatory Framework on HMI | Specifications for V2X, I2X communication | | Guidelines for public funding for ITS |
| Free minimum information service | Interoperability of electronic toll systems | Guidelines: Impact on Vulnerable road users | Mandate for European standardisation | | Collaboration platform on urban ITS |
| Promotion of multi-modal journey planners | | Guidelines: Secure parking places for trucks | | | |



Secure Com

ITS Privacy

In-Vehicle Security

Secure Autom. App. Platform

Integration and Field Testing

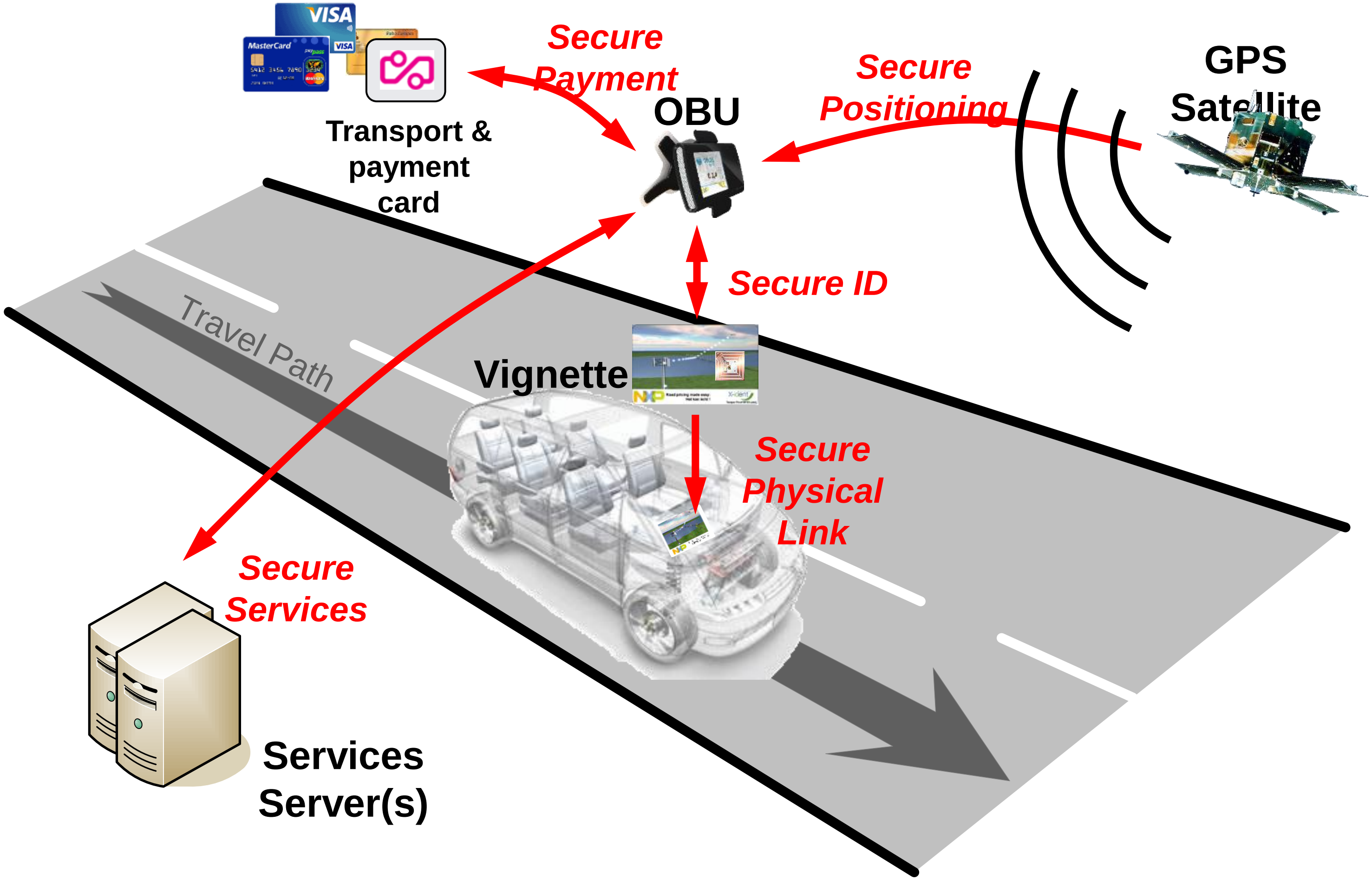
The commission is currently carrying out a study on ITS and data protection

# Electronic Tolling System (ETS) Example

From *PrETP: Privacy-Preserving Electronic Toll Pricing (extended version)*.
J.Balasch et al. 19th USENIX Security Symposium 2010

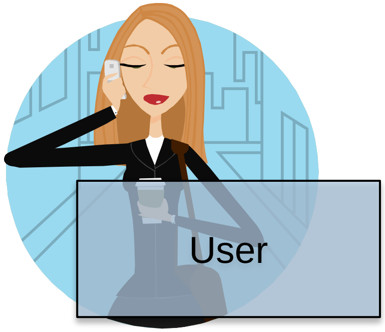
- User pays for using roads, depending on context
  - type of road, time/date, traffic, type of vehicle, …
- Public authority manages infrastructure using policies
  - congestion, energy, …
- Infrastructure requirements
  - Low infrastructure cost
  - Ease of adaption/installation
  - Security and enforcement
- Application requirements
  - Record information about vehicle route
  - Bill driver based on vehicle route
  - Keep info for invoice verification
  - Privacy preservation

# Electronic Tolling System Infrastructure Example

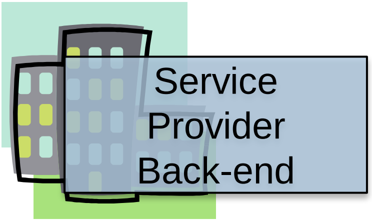


Courtesy NXP – eSecurity WG presentation Oct 2009

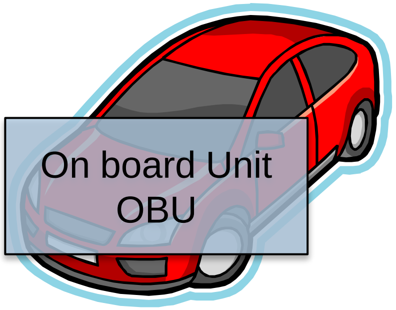
# Electronic Tolling System: Entities at Stake



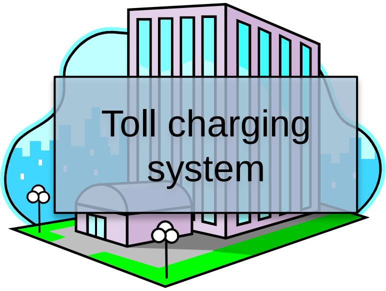
User



Service Provider Back-end



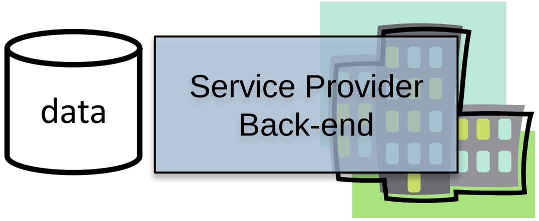
On board Unit OBU



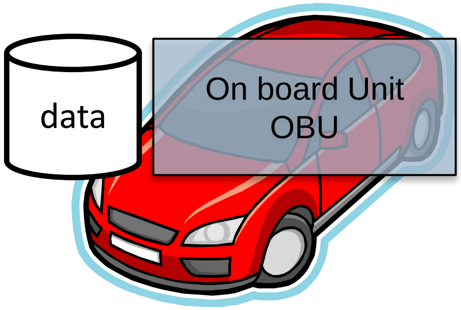
Toll charging system

# Approaches

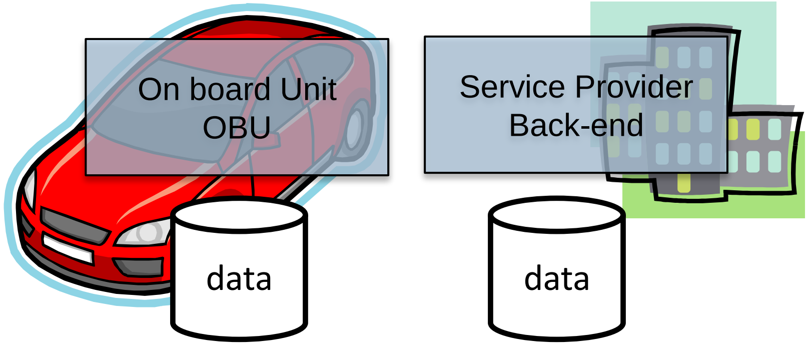
- **Model A**: personal data and fees handled by SP backend



- **Model B**: personal data and fees handled by OBU

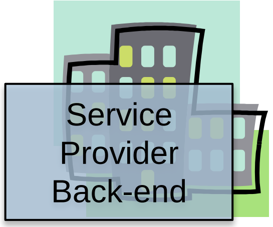


- **Model C (PrETP)**: fees handled by SP backend, personal data handled by OBU
  - OBU reveals subfees



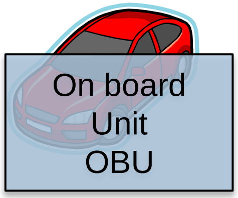
# Comparison

- Model A: Protection at service provider level (millions of users)



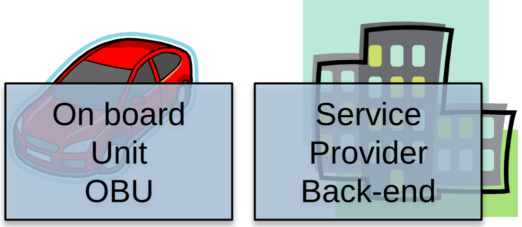
Service Provider Back-end

- Model B: Protection at OBU/user level, but heavy communication overhead



On board Unit OBU

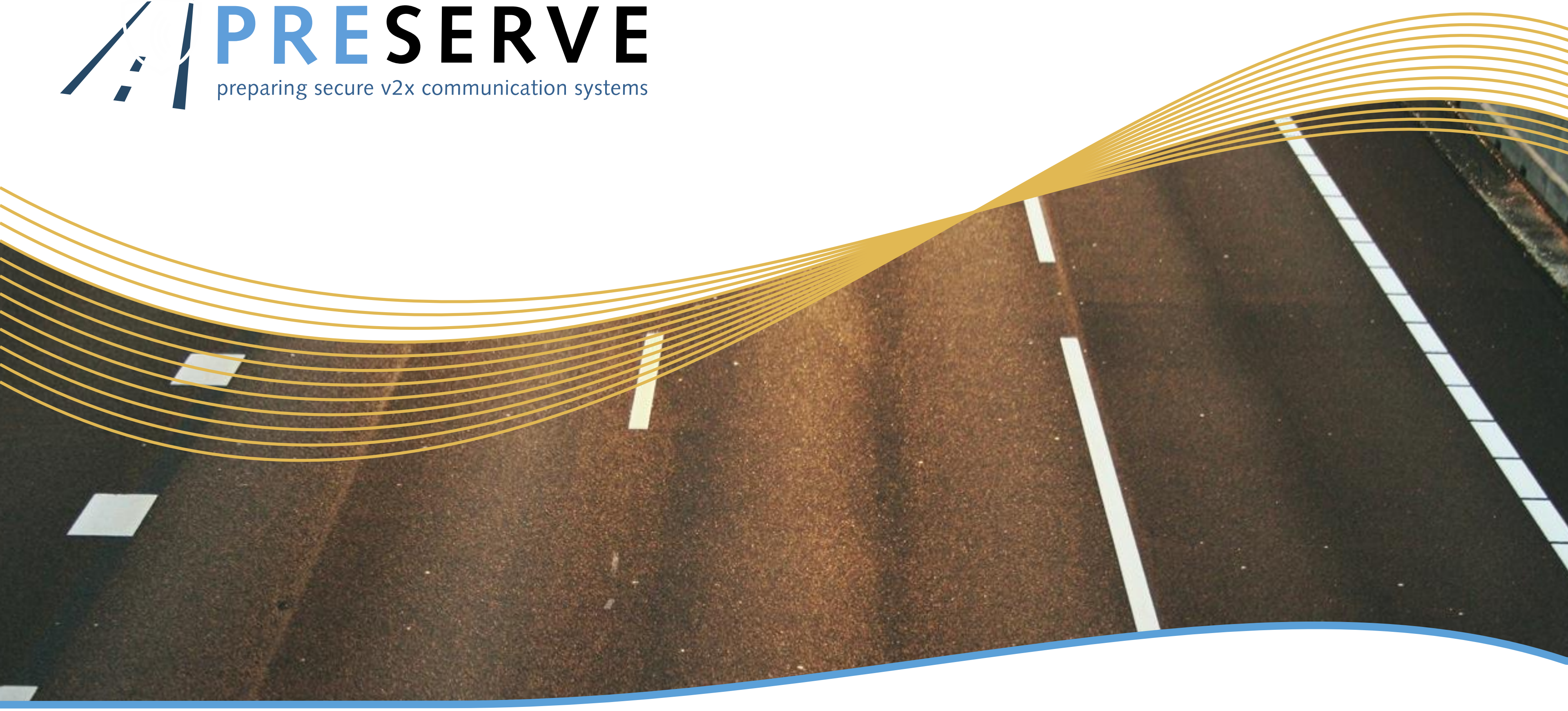
- Model C:  Protection at OBU/user level



On board Unit OBU

Service Provider Back-end

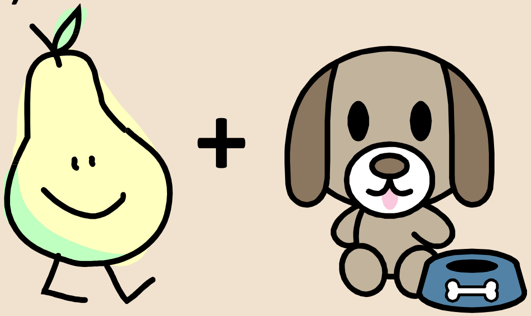
- Conclusion
  - Each model is a **different architecture**!
  - Each model implies different **interoperability requirements**!



# The Architecture Barrier

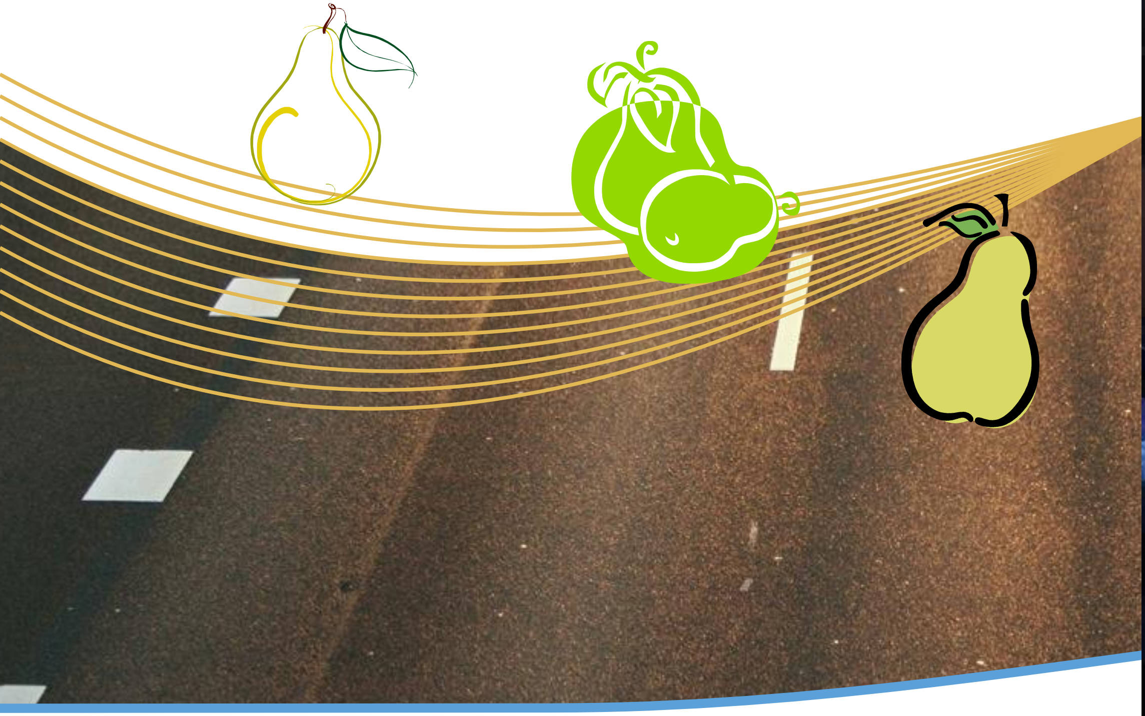
# Neglect of Architecture Impact

## (Design Level Barrier)

| Context | Risk | Policy? |
|---|---|---|
| **Privacy preserving solutions have a profound impact on architecture** | Deployment of ICT infrastructure with non adapted architecture or flexibility for change<br>e.g. ITS, smart grids, … | Take more global architectural view in addition to mechanism centric view.<br>Add Privacy Enhancing Architectures (PEARs) to Privacy Enhancing Techniques (PETs).<br> |

PRESERVE

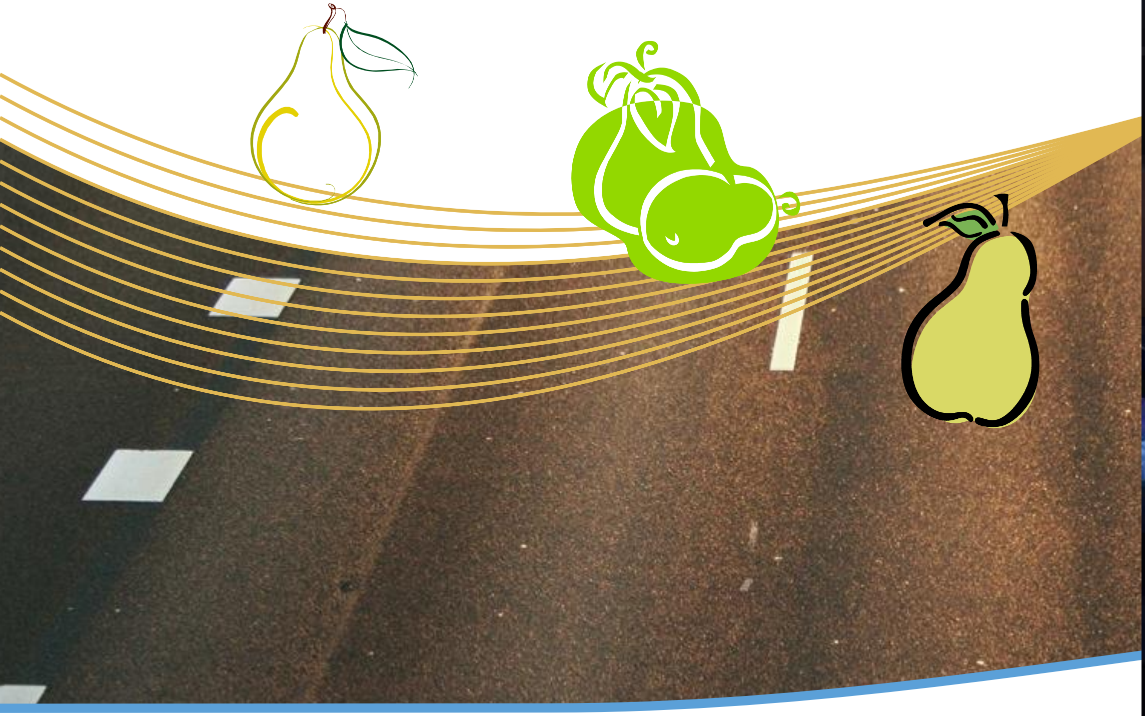
preparing secure v2x communication systems



# PEARs

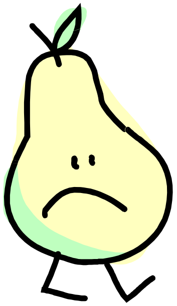
PRESERVE

preparing secure v2x communication systems



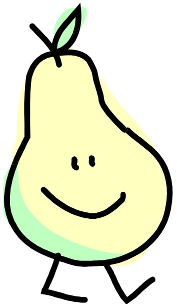
# PEARs

# PEARs Neglected



- A PET often associated with a PEAR
  - – Pay-per-use PriPayd
  - – Electronic Tolling  PrETP
- PEARs often considered specific but they are *architecture patterns*
- and PEARs have profound impact on deployment
  - – Smart grid example

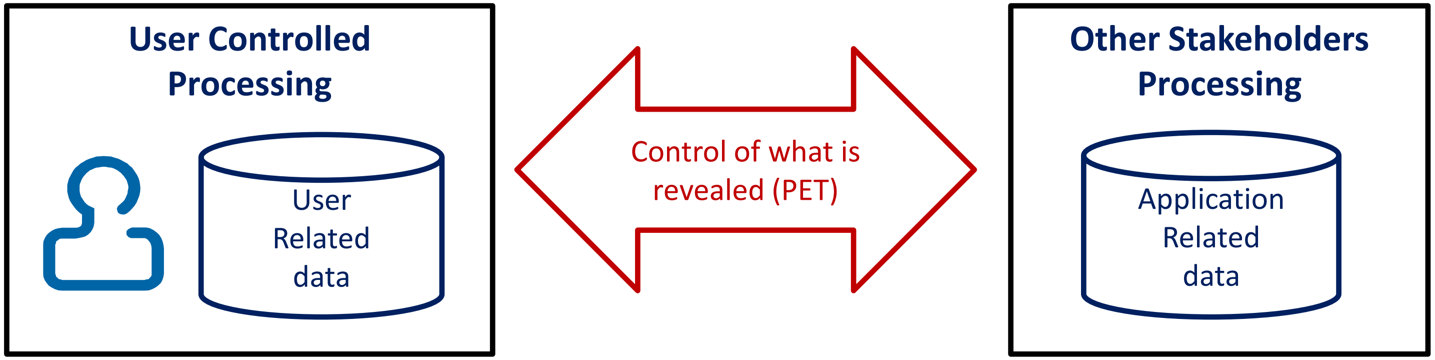
# PETs vs PEARs



- PET: Privacy Enhancing Technology
  - Focus on mechanisms. Often crypto-centric
  - Foundational
- PEAR: Privacy Enhancing Architecture
  - Focus on design. Architecture-centric
  - Deployment impact (i.e. € impact)

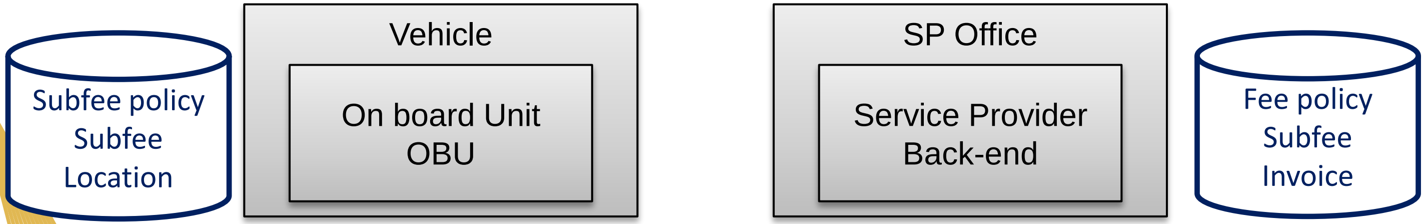
# Example: the Physical Confinement PEAR

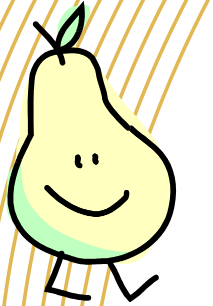
- Collected data physically controlled by user
  - vehicle, user computer, home gateway, disk, USB stick…


User Controlled Processing
User Related data
Control of what is revealed (PET)
Other Stakeholders Processing
Application Related data

- Used in contributions pay-per-use, electronic toll systems, metering, …
- At odds with clouds, … (Logical confinement PEAR?)

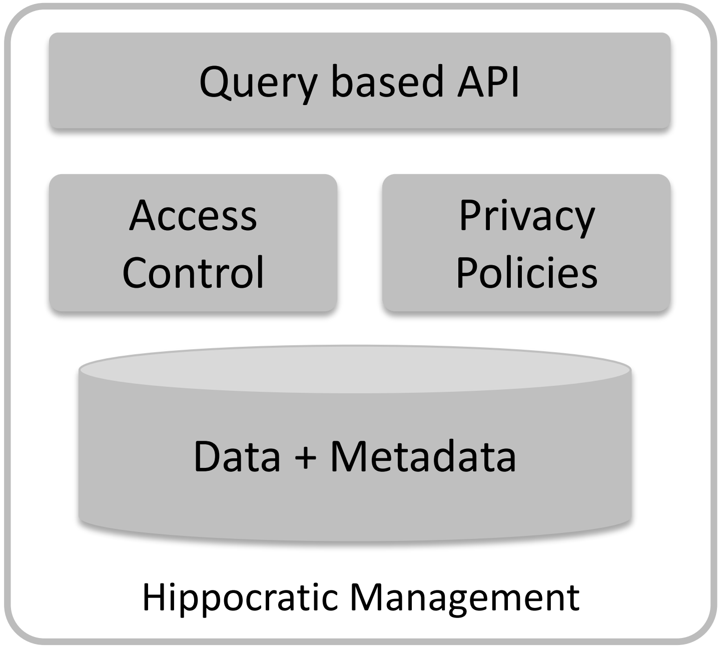
**PrETP is based on the Physical confinement PEAR**

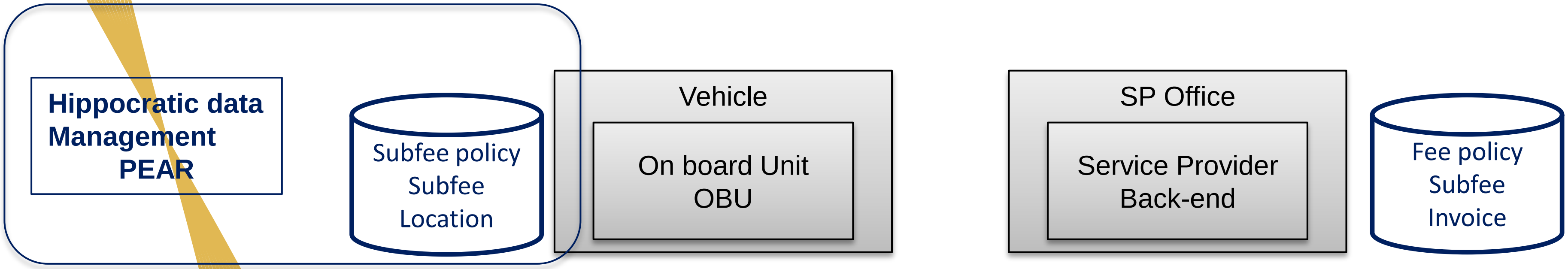




# Example: the Hippocratic Management PEAR

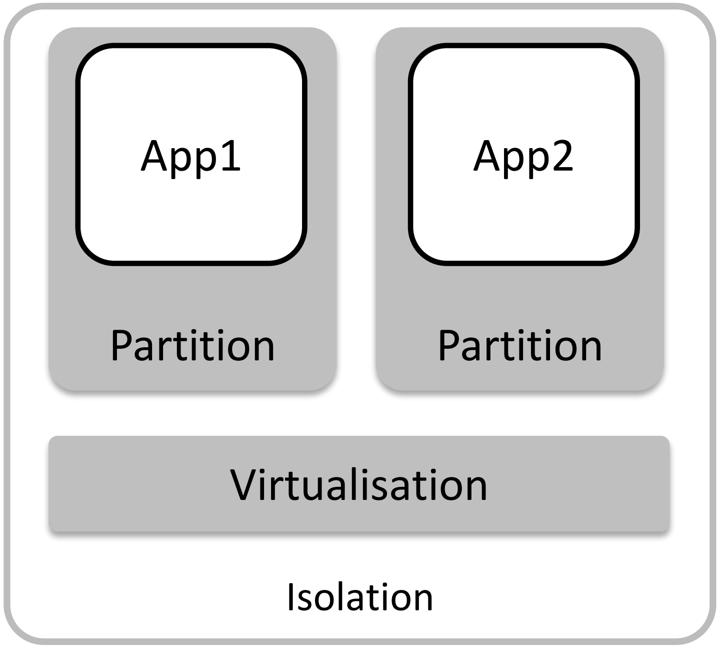
- Data management follows principles for data protection
  - Purpose specification, Consent, Limited collection/use/disclosure/retention, Accuracy, Safety, Openness, Compliance
- Coined by Agrawal 2000 (after the Hippocratic Oath)

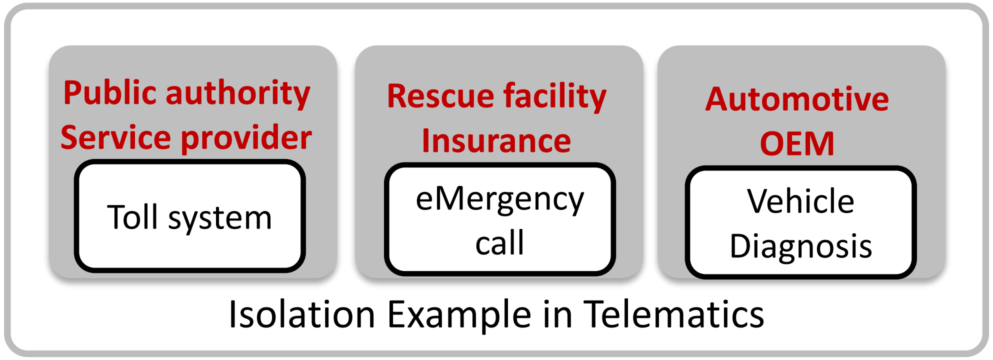




# Example: the Isolation PEAR

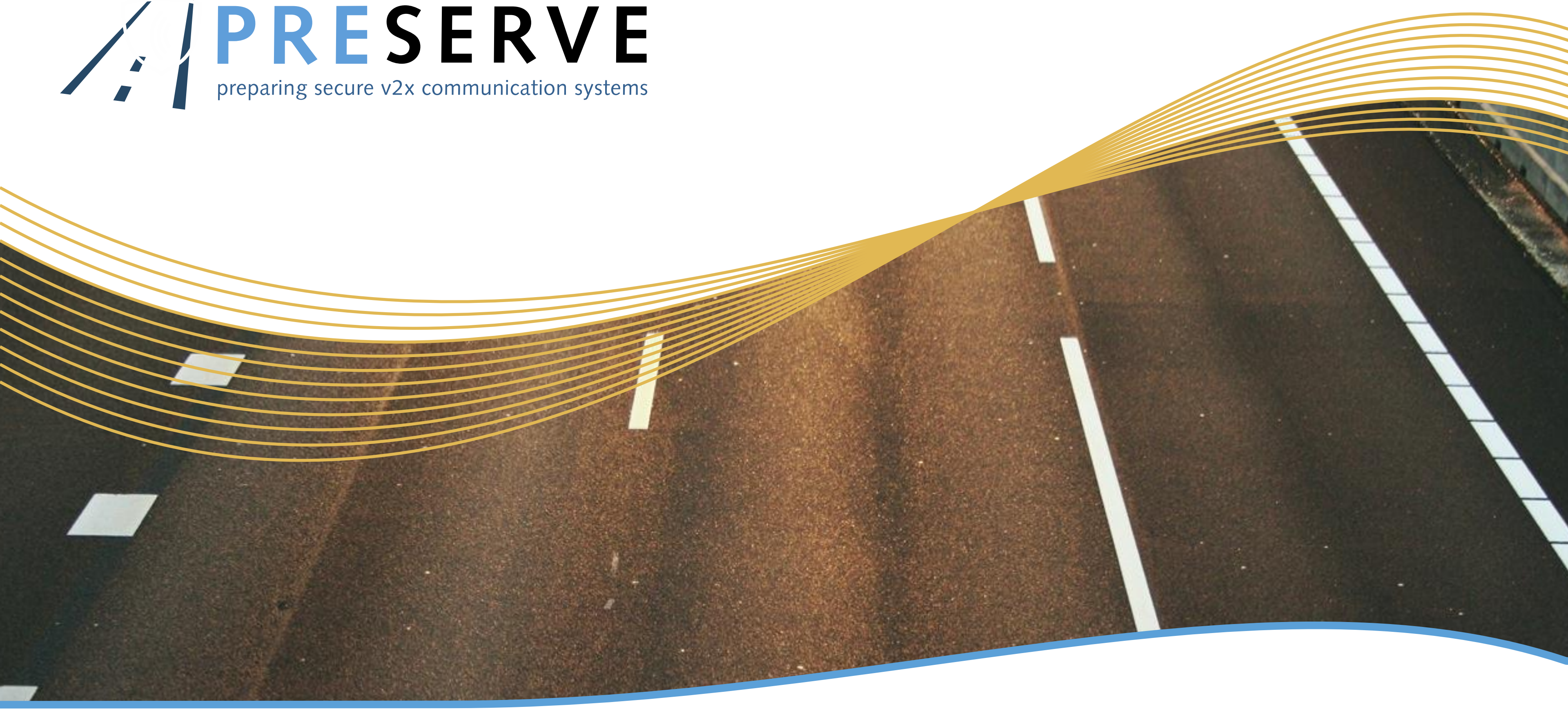
- Applications isolated from each other
  - Resource isolation
    - CPU
    - Memory
    - I/O
    - Consumption
- Security issue / Mixed criticality
- Liability issue (Different **stakeholders**)





PRESERVE

preparing secure v2x communication systems



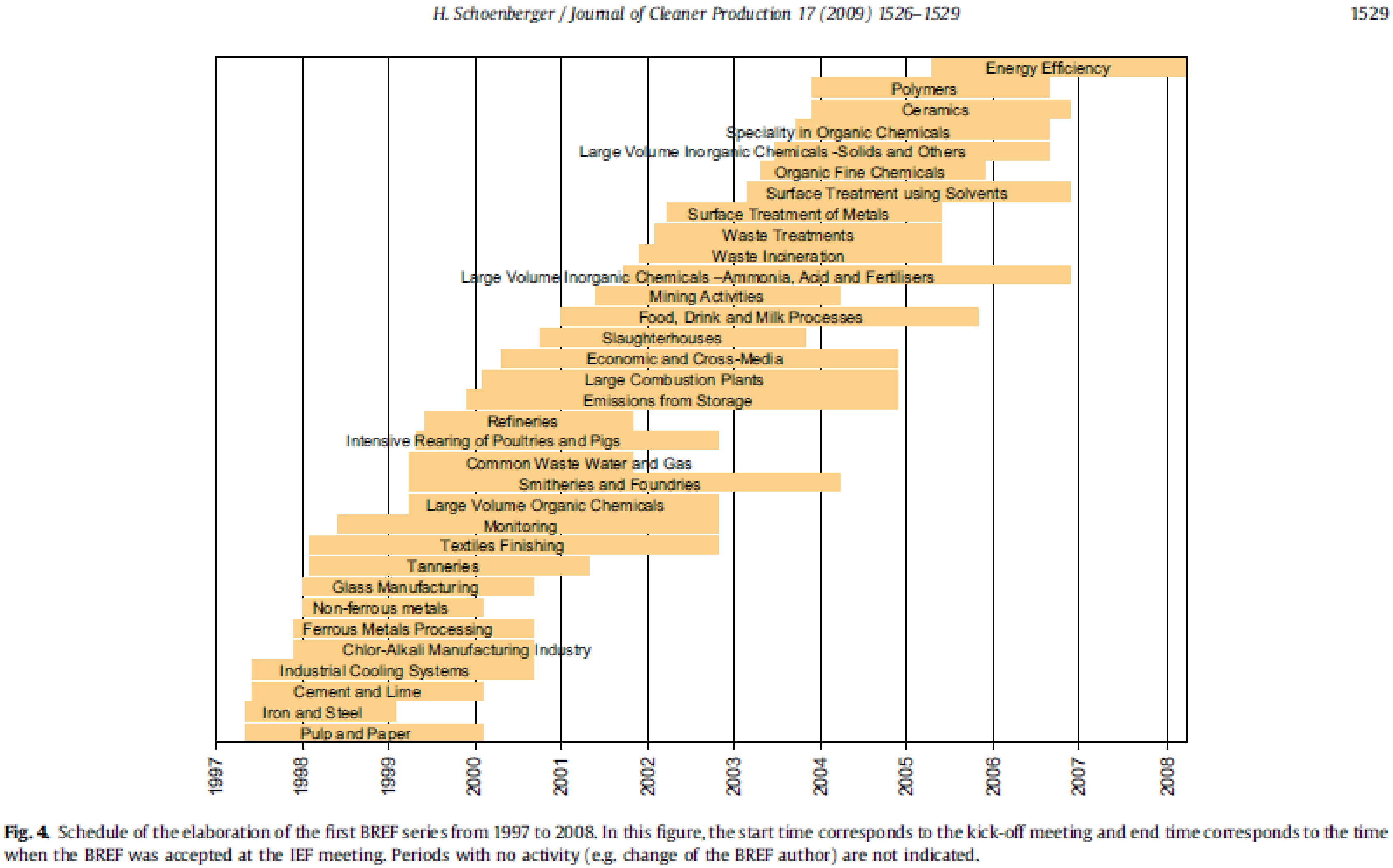
# Other Barriers

# Conflict of Interest

## (Application Level Barrier)

| Context | Risk | Policy? |
|---|---|---|
| **Applications value:**<br>**exploitation of user data** | Privacy regulation and Privacy-by-Design considered as an obstacle for deployment.<br>Lead to the ***weakest interpretation*** on how to apply Privacy-by-Design | Consensus process supported by policy makers<br>e.g. EDPS recommendation<br>• BAT (Best Available Techniques)<br>• BREF (BAT Reference document)<br>• Comitology (Sevilla Process) |

# Example of BREFS



H. Schoenberger / Journal of Cleaner Production 17 (2009) 1526–1529 1529

**Fig. 4.** Schedule of the elaboration of the first BREF series from 1997 to 2008. In this figure, the start time corresponds to the kick-off meeting and end time corresponds to the time when the BREF was accepted at the IEF meeting. Periods with no activity (e.g. change of the BREF author) are not indicated.

# Lack of Consensus on Protection Policies

## (Application Level Barrier)

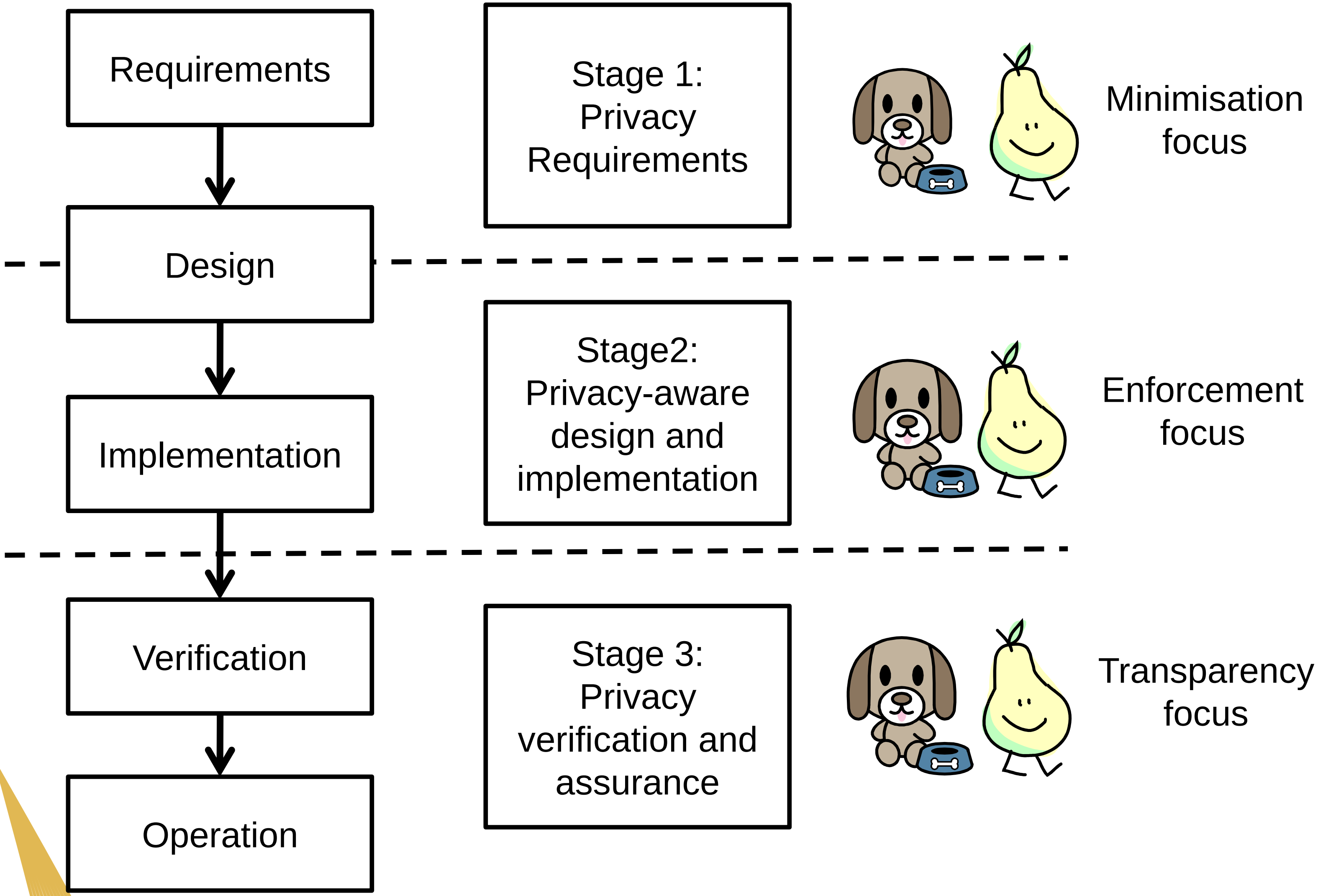
| Context | Risk | Policy? |
|---|---|---|
| **Agreement on protection policies** | Interoperability problem e.g. retention of exchanged data | A process supported by policy makers to agree on policies |
| | Level of protection reached is that of stakeholders applying the least protective policy | A more agile process for interoperability agreement? |

# Interpretation of Privacy-by-Design

## (Design Level Barrier)

| Context | Risk | Policy? |
|---|---|---|
| Orientation towards risk assessment<br>Not agreed yet meaning | Gap between risk assessment and core engineering<br>Multiple interpretations<br>• Minimisation+Enfocement +Transparency (Kung)<br>• Minimise, Hide, Separate, Aggregate, Be transparent, and enforce (Hoepman) | Create a multidisciplinary working group to define an agreed model. |

# Sketch of Overall Process



Requirements

Design

Implementation

Verification

Operation

Stage 1: Privacy Requirements

Stage2: Privacy-aware design and implementation

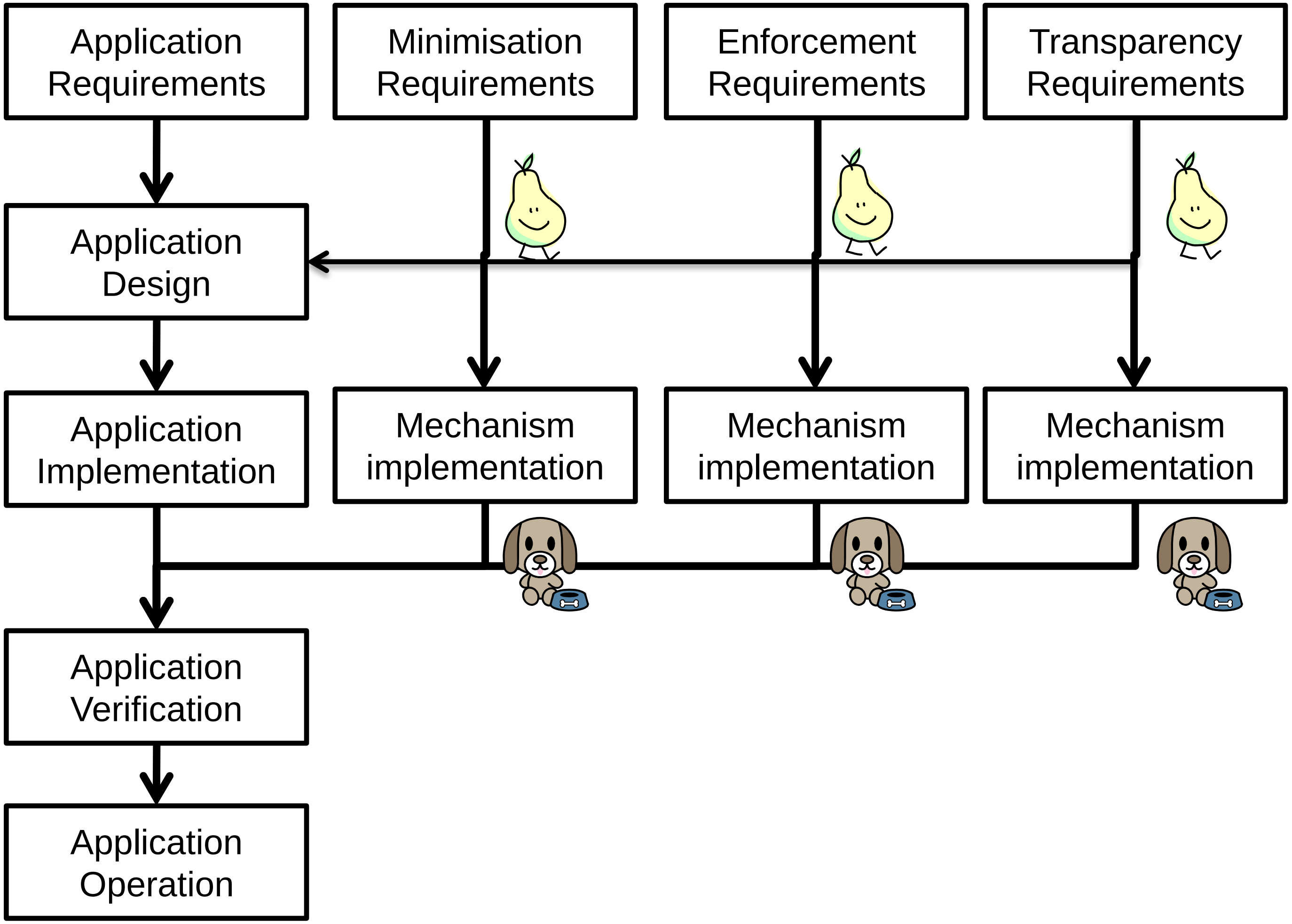
Stage 3: Privacy verification and assurance

Minimisation focus

Enforcement focus

Transparency focus

# Mainstream Approach


Application Requirements

Minimisation Requirements

Enforcement Requirements

Transparency Requirements

Application Design

Application Implementation

Mechanism implementation

Mechanism implementation

Mechanism implementation

Application Verification

Application Operation

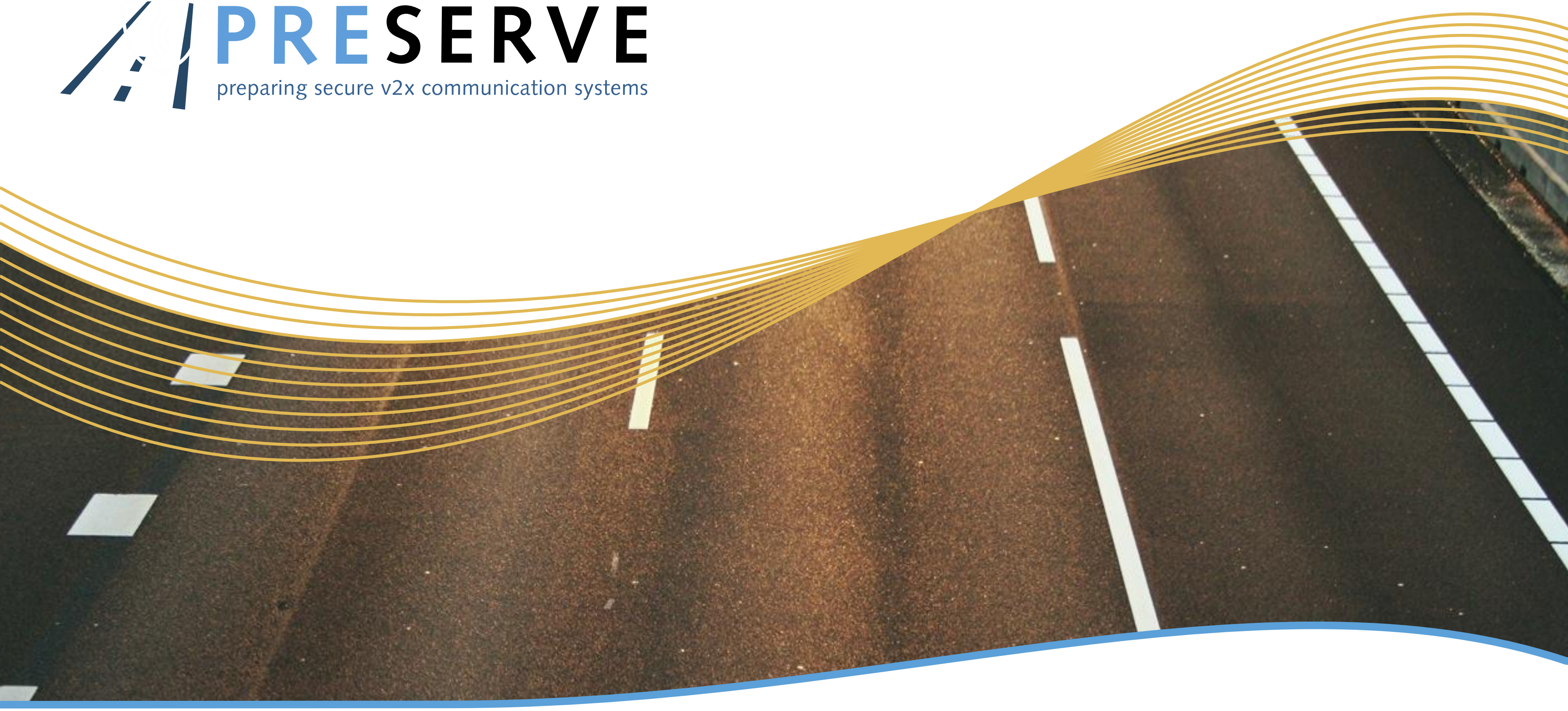
# Lack of PbD Practice

## (Design Level Barrier)

| Context | Risk | Policy? |
|---|---|---|
| **Little PdB Practice** | No education | Privacy and PbD in the curriculum |

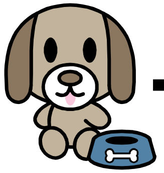
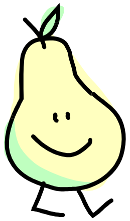
# Other Barriers to be covered later

- Integration of PbD into processes
- Leaks in ICT infrastructures
- Flexibility in ICT infrastructures



# Thanks

Antonio Kung

PIA +  +  → !

Thanks to Gabriel Gauthier-Shalom (distinguished crypto research U.Waterloo /pear Juggler)