



# Contribution to Privacy

---

Antonio Kung  
Trialog



- **PR**ivacy **E**nabled **C**apability **I**n co-**O**perative systems and **S**afety **A**pplications
- FP7 STREP Project
- 1/3/2008-31/8/2010
- [www.preciosa-project.org](http://www.preciosa-project.org)

*TRIALOG*

**ORACLE®**



traffic mobility logistics.



ulm university universität  
**uulm**

# Goal and Objectives



## ■ Goal

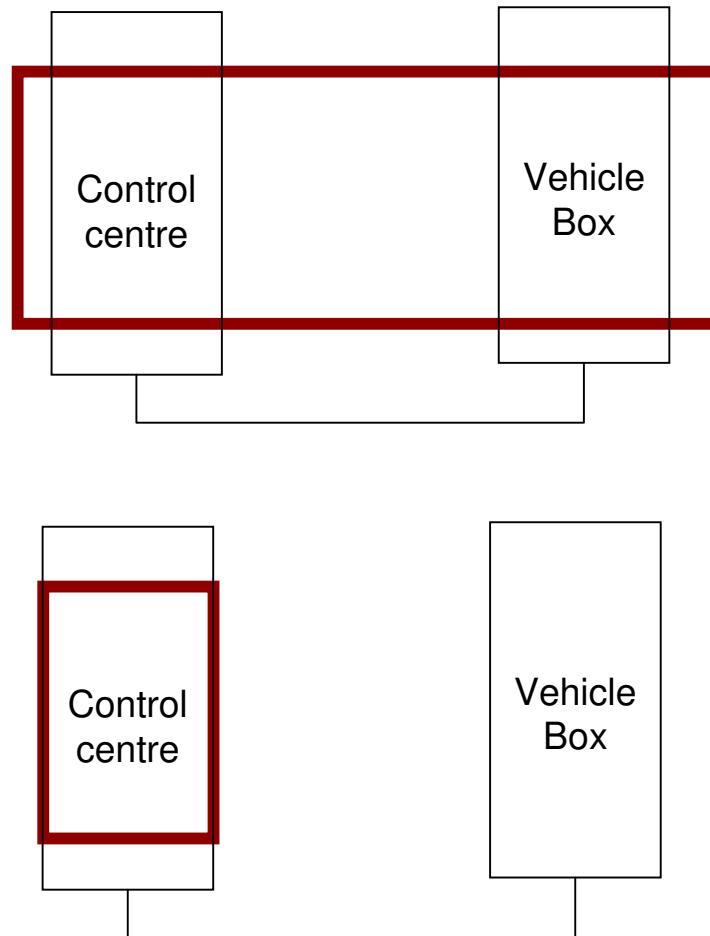
- Ensure that co-operative systems meet (future) privacy regulations
- Demonstrate an example application with suitable technology for privacy protection

## ■ Objectives

- approach for privacy by design
  - privacy verifiability
  - privacy aware architecture
- guidelines for privacy by design
- specific research challenges

# Technical Concept

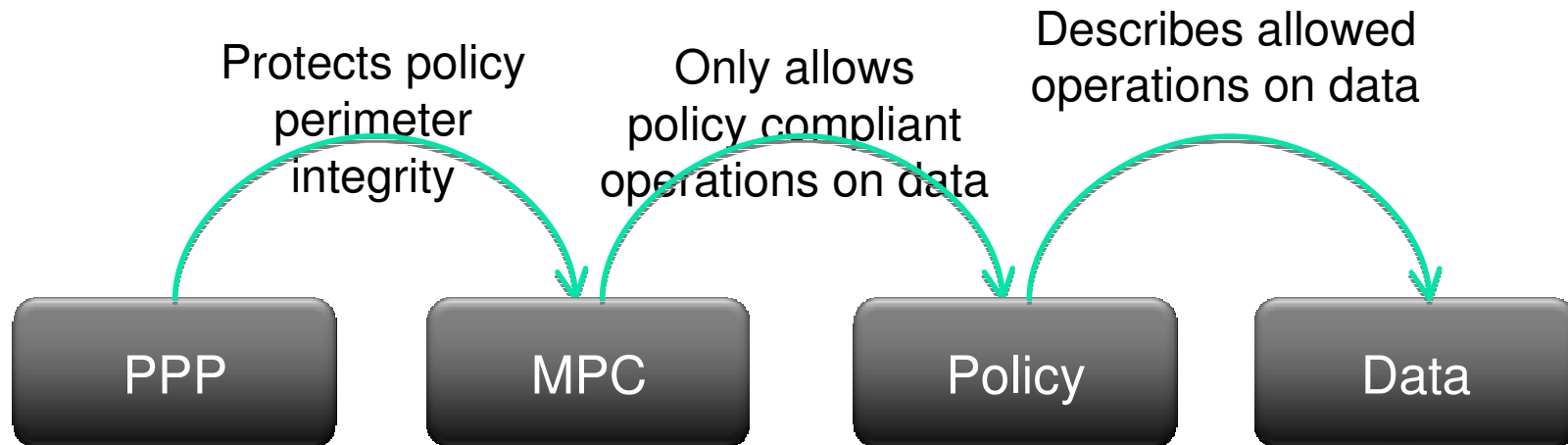
- Privacy Perimeter
- Examples



# Technical Concept



- Enforce privacy policy within perimeter
- Four elements
  - Data
  - Policy (allowed operations)
  - Mandatory Privacy Control (enforces policy)
  - Policy Perimeter Protection (ensures integrity)

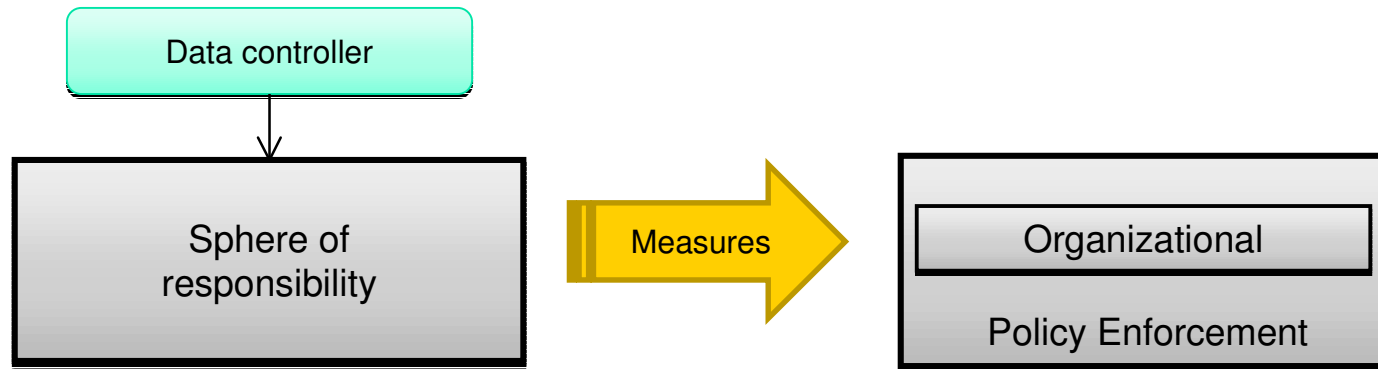


# PRECIOSA Concept vs PETs

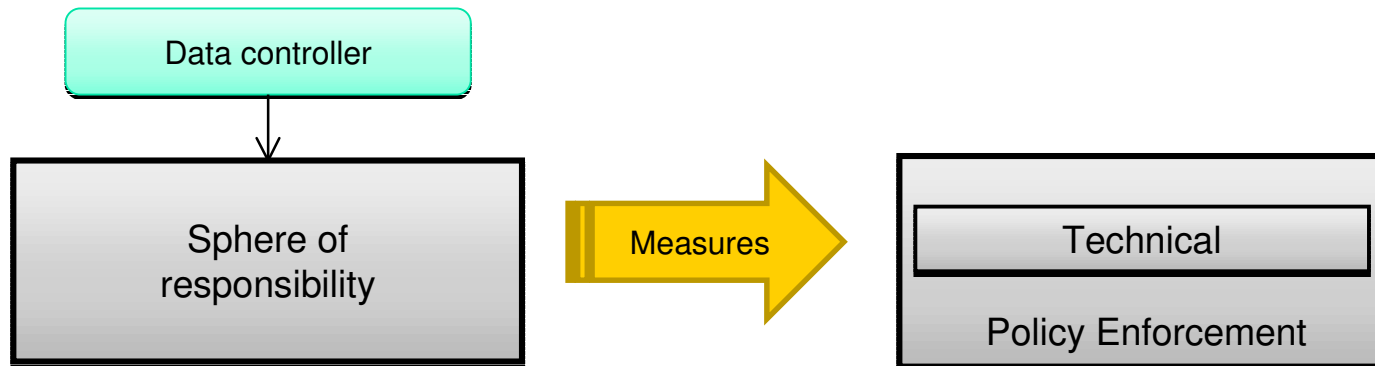


- PETS are often described as a list of technologies:
  - Encryption
  - Anonymisation and pseudonymisation
  - Securely management of logins
  - ...
- PRECIOSA Viewpoint
  - System oriented new PET category
  - Policy Enforcement PET

- From organisational enforcement

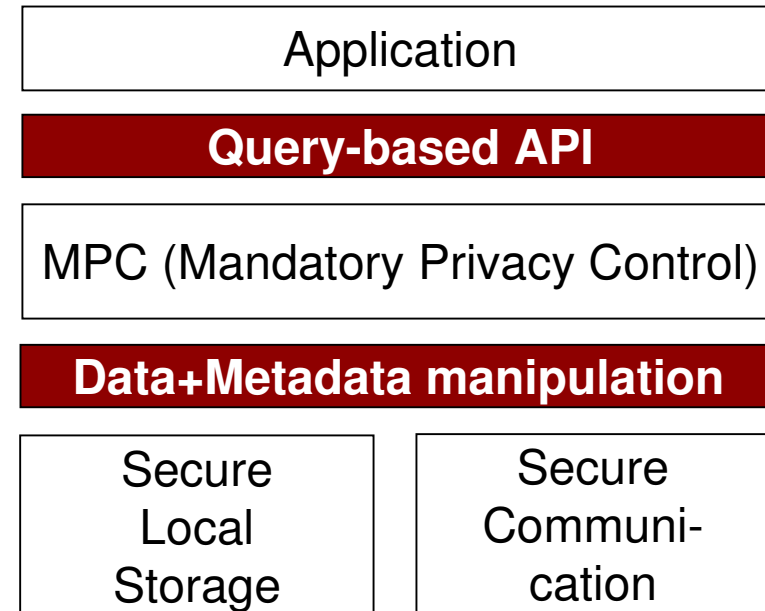


- To technical enforcement



# Technologies (PETs)

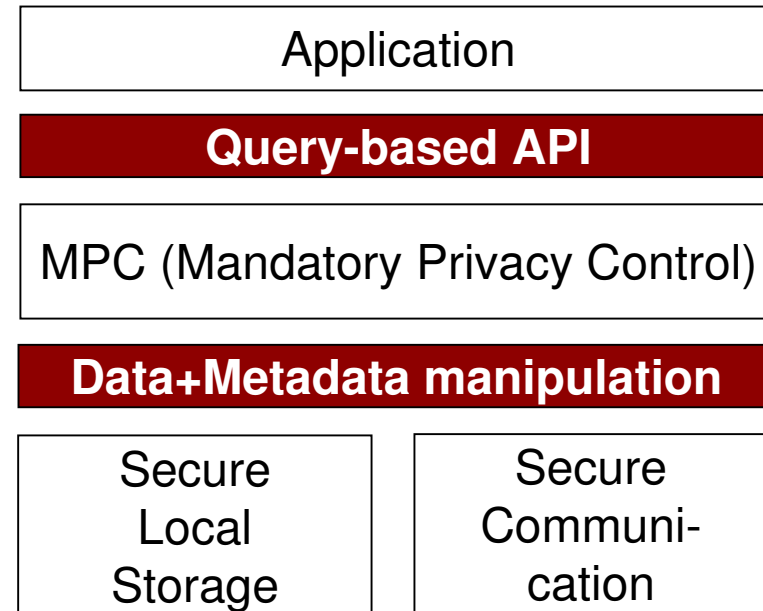
- Storage Secure access through Metadata
  - Data and meta data bound together securely
  - MPC verifies policy stored in meta data
  - Access through a query-based API



# Technologies (PETs)



- Communication
  - Pseudonymisation (from Sevecom)
  - Trusted computing for remote attestation



# Conclusion



- PRECIOSA promotes
  - Privacy by design
  - Privacy preservation (vs privacy enhancement)
- PRECIOSA PET
  - Policy enforcement PET
  - Notion of distributed perimeter could lead to notion of logical minimisation
    - E.g. Lots of data collected, but very limited access