

# PrETP: Privacy-Preserving Electronic Toll Pricing

**Claudia Diaz** / Carmela Troncoso (SCD/COSIC)  
LICT Industrial Affiliation Day

June 3, 2010

# Electronic Toll Pricing

---

- ▶ Differentiated payment for mobility: Congestion pricing
  - ▶ Motivation
    - ▶ Address mobility problem
    - ▶ Mentality and behavioral change
    - ▶ Fairness: heavy users have to pay more
  - ▶ Concept:
    - ▶ Users should pay depending on their use of the car and roads:
      - Long drives, high density roads, rush hours: higher fee
      - Sporadic use, second vehicle for weekends, young drivers with small salary: smaller fee
  - ▶ aka Road Charging, Road pricing, Electronic Road Pricing, ...

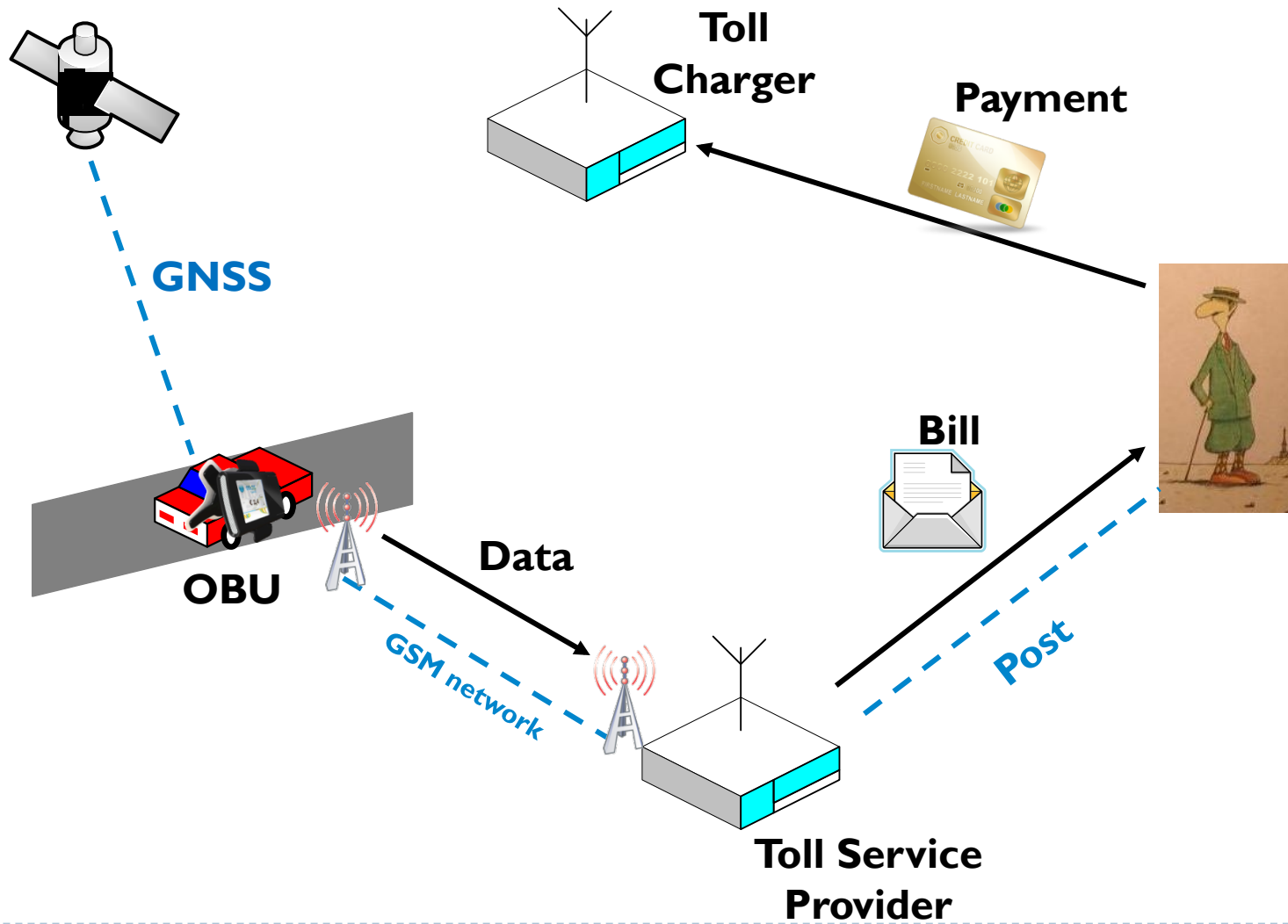
# Road Tolling: EU EETS Decision

---

- ▶ **European Electronic Toll Service**
  - ▶ 6 Oct 2009
  - ▶ Coordinates exchange of information between Member States, to ensure the correct declaration of tolls
  - ▶ Defines the actors involved: EETS architecture
  - ▶ Defines the interfaces to ensure interoperability
    - ▶ GNSS: Global Navigation Satellite System
    - ▶ DSRC
    - ▶ GPRS/GSM network
  
- ▶ Within **three** years for vehicles above 3.5 tons, all other vehicles within **five** years.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:268:0011:0029:EN:PDF>

# EETS straightforward implementation



# Stakeholders

---

- ▶ **Government**
  - ▶ Interest
    - ▶ Mobility Problem
  - ▶ Role
    - ▶ Establishing policies
    - ▶ Law enforcement
- ▶ **Industry (chip manufacturers, GSM providers, ...)**
  - ▶ Interest
    - ▶ New business opportunities
  - ▶ Role
    - ▶ Provide infrastructure
- ▶ **Users**
  - ▶ Interest
    - ▶ Mobility problem, economics
  - ▶ Role
    - ▶ Using the system but...
    - ▶ **privacy in risk**

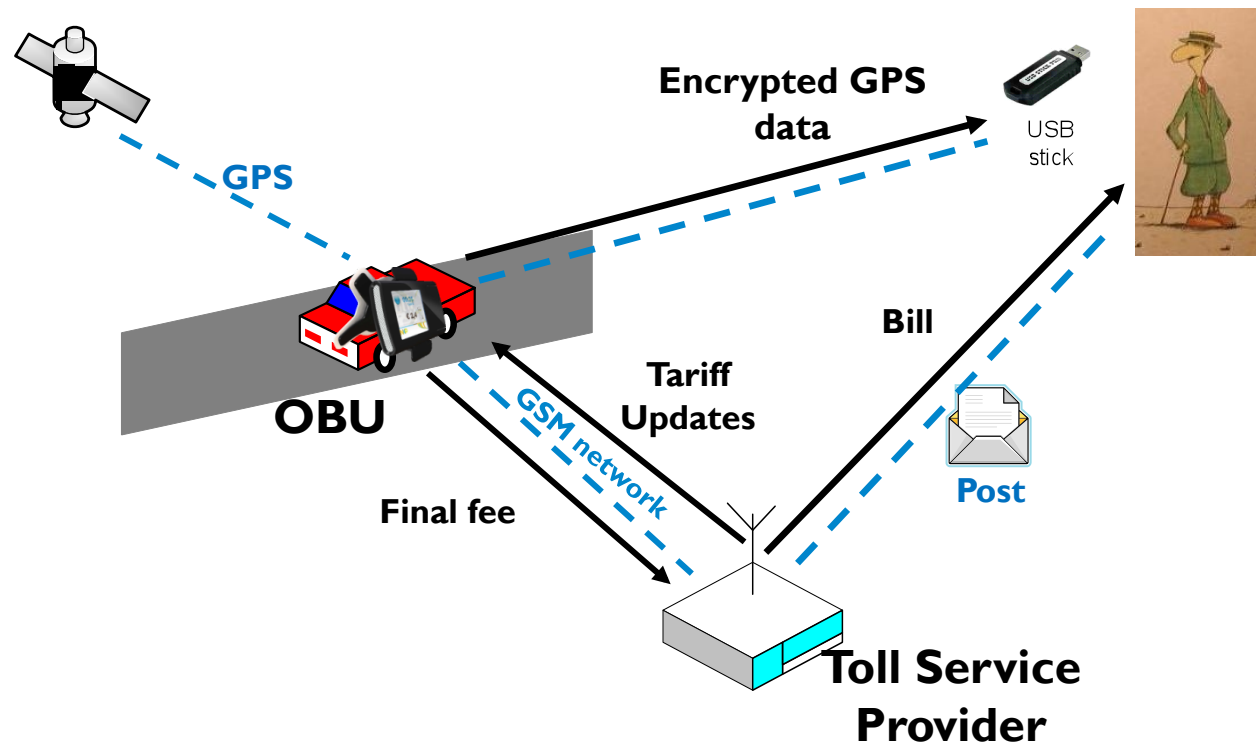
# Privacy for Electronic Toll Pricing

---

- ▶ **Privacy issues?**
  - ▶ *Pay as you drive*
  - ▶ Fine grained GPS data allows for inferences
    - ▶ Medical issues (visits to a Cancer specialized clinic)
    - ▶ Political affiliation (visits to the headquarters of a political party)
    - ▶ Industry espionage (visits to other companies)
- ▶ **What data is necessary?**
  - ▶ Final fee that the user must pay to the provider/government
- ▶ **Legal issues**
  - ▶ Actors must not be able to cheat
  - ▶ Actors must be held liable when misusing the system

# Privacy-Friendly Electronic Toll Pricing

- ▶ No personal data leaves the domain of the user

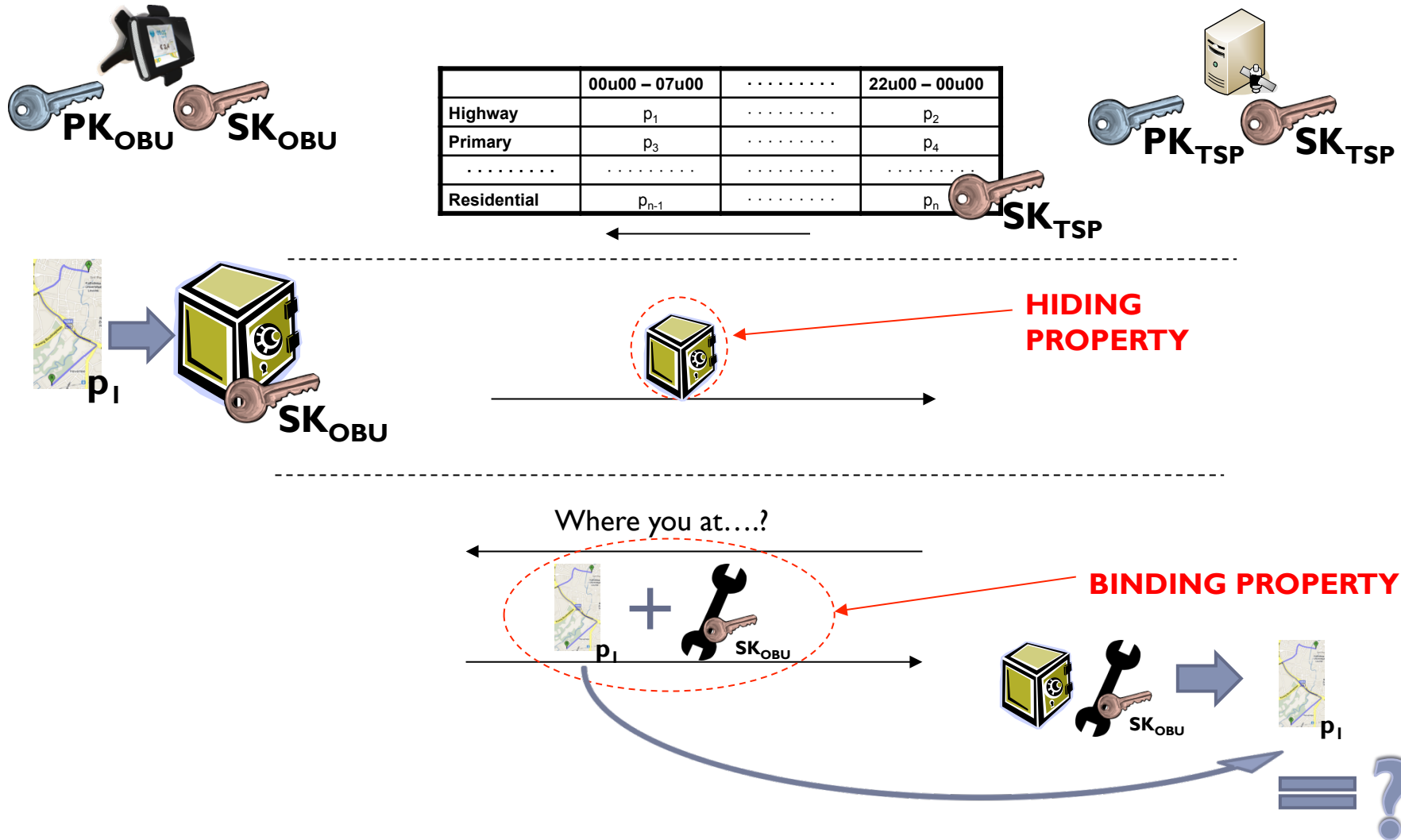


# Law enforcement

---

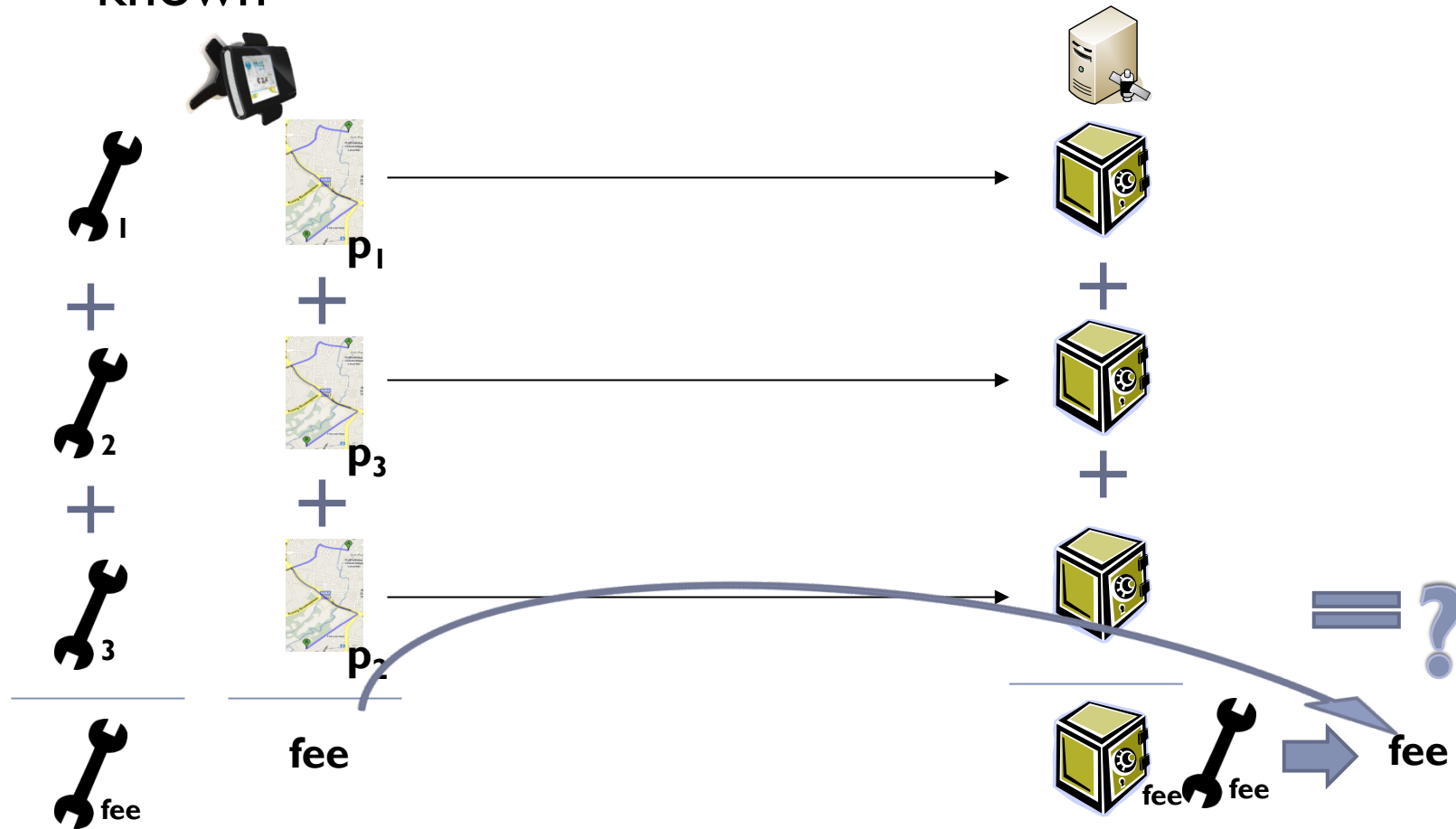
- ▶ **Technical means do not suffice**
  - ▶ OBU in hands of the user
- ▶ **Instead technology can help:**
  - ▶ Detect vehicles with inactive OBUs
  - ▶ Detect vehicles reporting false location data
  - ▶ Detect vehicles using incorrect road prices
  - ▶ Detect vehicles reporting false final fees
- ▶ **Combination of law + technology**

# Non-Interactive Commitment Schemes



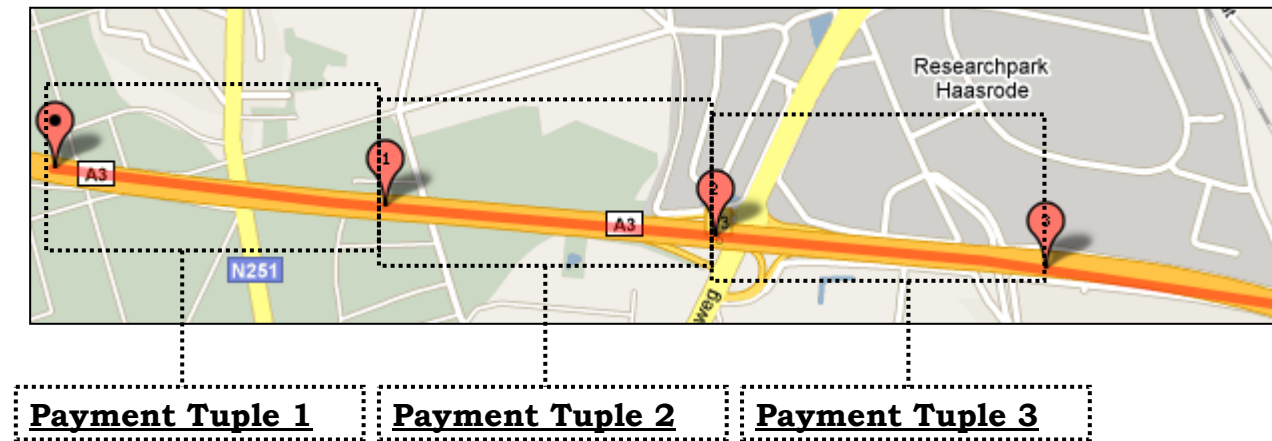
# Homomorphic commitments

- ▶ The content of the vaults can be added up without being known



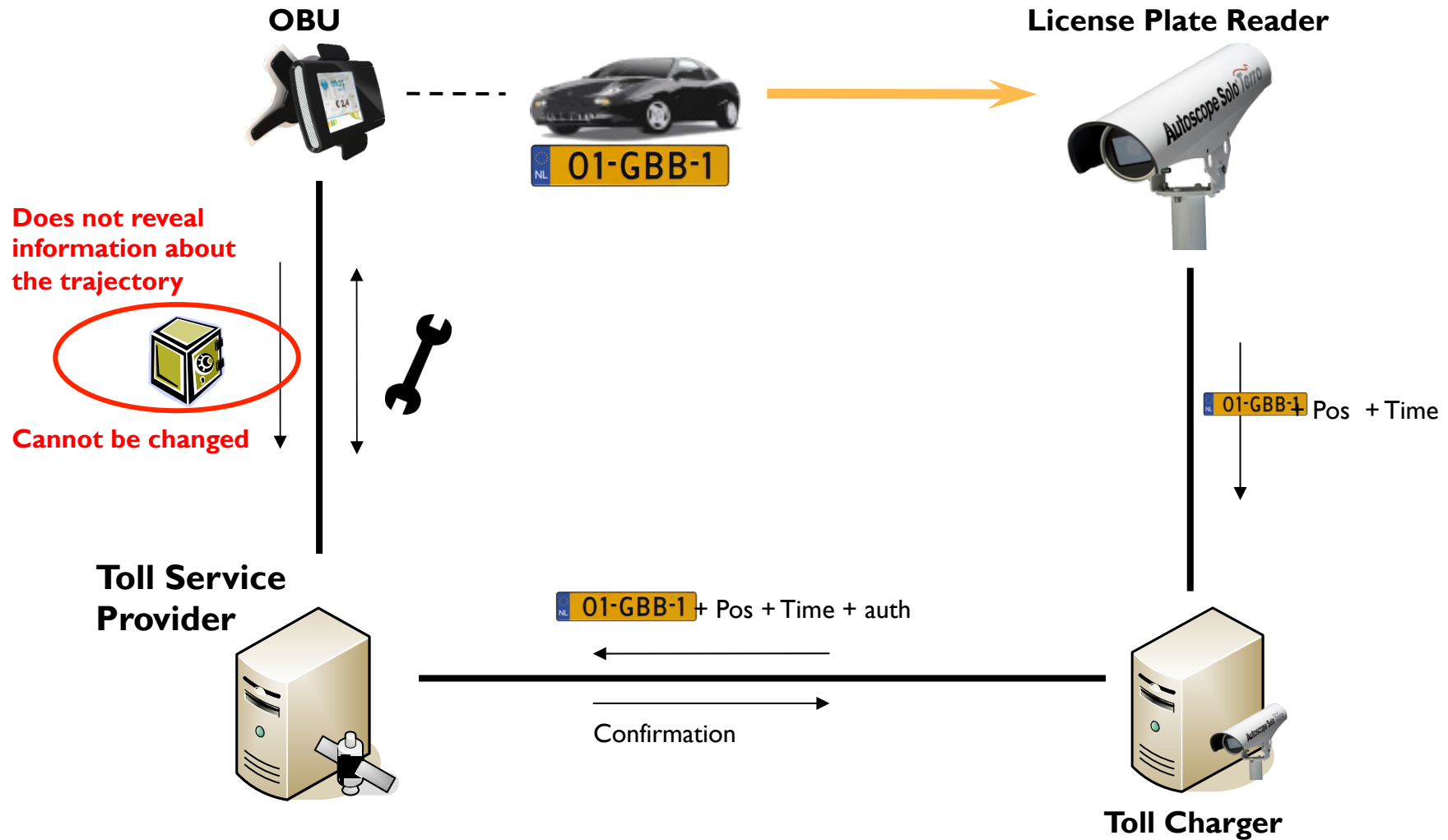
# Creating commitments

- ▶ Slice trajectory in segments (e.g., 1 Km)



- ▶ Each segment has assigned a price per Km  $p_i$
- ▶ This price is specified by the policy, example:
  - ▶  $p_i = f(\text{type road, time day})$
- ▶ A commitment per segment is created

# How does it work?



# What can we prove?

---

- ▶ **OBU was active**
  - ▶ A commitment with the committed location and time must be available
- ▶ **OBU used correct prices**
  - ▶ Prices in the table signed by Toll Service Provider
  - ▶ Check correct pricing upon commitment opening
- ▶ **OBU was at reported location**
  - ▶ Compare photo location with committed location
- ▶ **OBU made correct operations**
  - ▶ Homomorphic commitments: prices in the “vaults” can be added to verify that they correspond to the reported final fee without being opened

# Holistic analysis

---

- ▶ **From a theoretic point of view**
  - ▶ The cryptography in the system ensures both privacy and law enforcement
- ▶ **From a legal point of view**
  - ▶ No personal data involved
  - ▶ Data minimization by design
- ▶ **From a practical point of view**
  - ▶ Prototype
  - ▶ Performance analysis
    - ▶ Computation
    - ▶ Communication



# Performance Analysis

- ▶ OBU platform: NXP ARM7 microcontroller (32 bit) / SW
- ▶ TSP platform: commodity computer (Inter Core2Duo)

OBU timings and average speed tolerance for a 1-hour journey

Security Operation	Medium (1024 bit)	High (1536 bit)	Very High (2048 bit)
Map-Matching	839.11 s		
One segment	7.88 s	22.13 s	47.79 s
Max. Speed	350 km/h	124 km/h	57 km/h

TSP capacity tolerance assuming an average of 1500 km/month/vehicle

Security Commit	Medium (1024 bit)	High (1536 bit)	Very High (2048 bit)
0.5 Km	82 000	29 000	14 000
1 Km	164 000	58 000	29 000
2 Km	329 000	117 000	58 000

- ▶ Communication overhead
  - ▶ Sending full GPS: 2.05Mbytes for 1500Km
  - ▶ PrETP:
    - ▶ 1.5Kbytes per segment
    - ▶ ~2Mbytes a month
    - ▶ Eventual 50Kbytes to open a commitment

# Conclusions

---

- ▶ Privacy-friendly Electronic Toll Pricing is feasible
- ▶ Strong security and privacy guarantees
  - ▶ No location information is disclosed to the provider
  - ▶ No actor can undetectably commit fraud
- ▶ Law compliant
- ▶ Working prototype on an ARM7
- ▶ More info:
  - ▶ J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede, "PrETP: Privacy-Preserving Electronic Toll Pricing," In *19th USENIX Security Symposium 2010*, Usenix, 26 pages, 2010. <https://www.cosic.esat.kuleuven.be/publications/article-1408.pdf>