

Pay-per-Use / Road Charging use cases
PRIVACY IMPLICATIONS AND POSSIBLE SOLUTIONS

Stefaan Motte, Michaël Peeters (NXP)
Carmela Troncoso (KU Leuven-Cosic)

Differentiated payment for mobility

- } Covers various related applications
 - } Road pricing (EETS)
 - } Vehicle insurance (PAYD)

- } 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

Differentiated payment : pros

- } Fair fees

- } For consumers and companies

- } Differentiated fees

- } Government can influence behavior and mentality based on policy

- } Social benefit

- } Less use of cars, responsible driving, less accidents, improve road mobility...

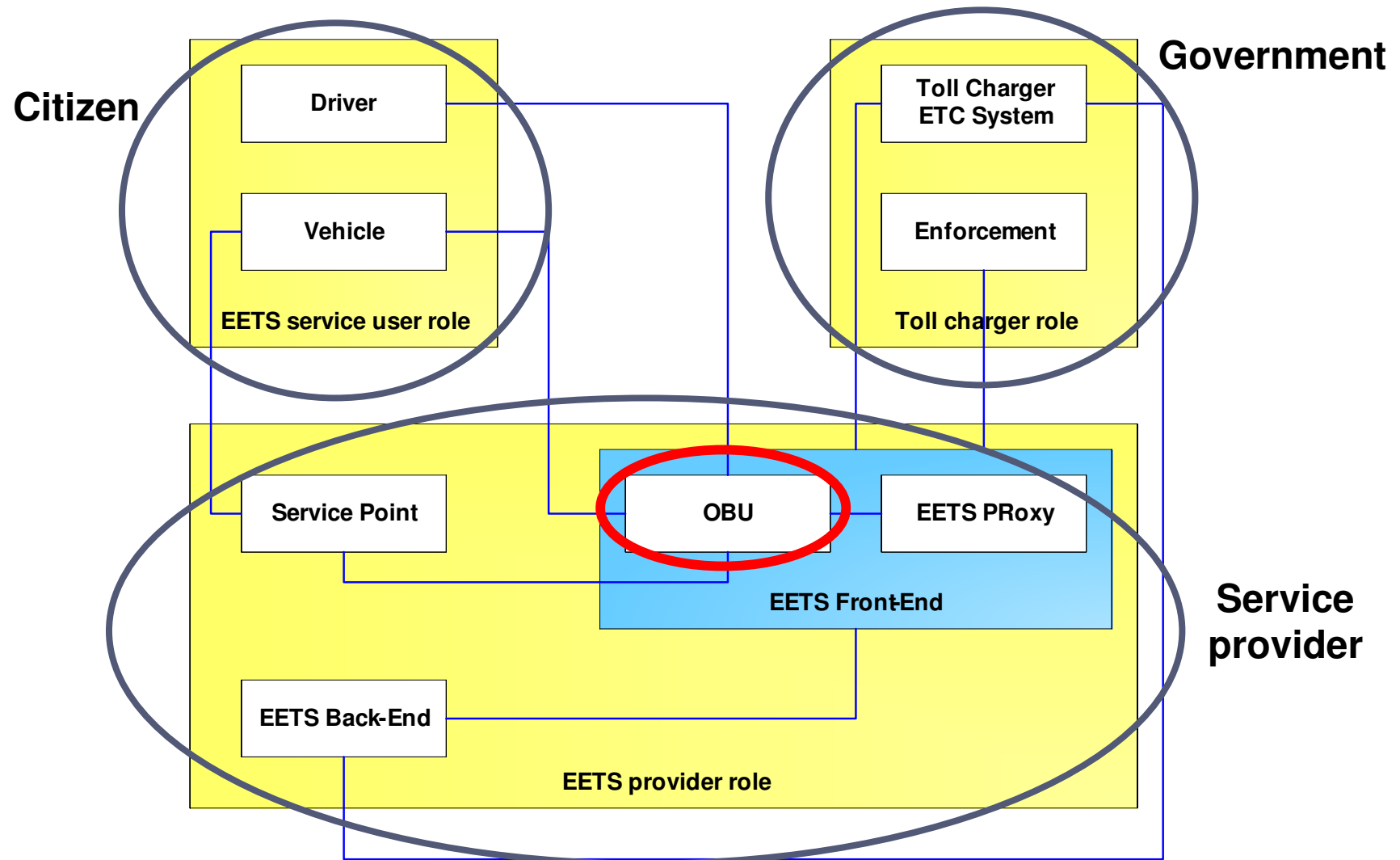
- } Environmental benefit

- } Business advantage position

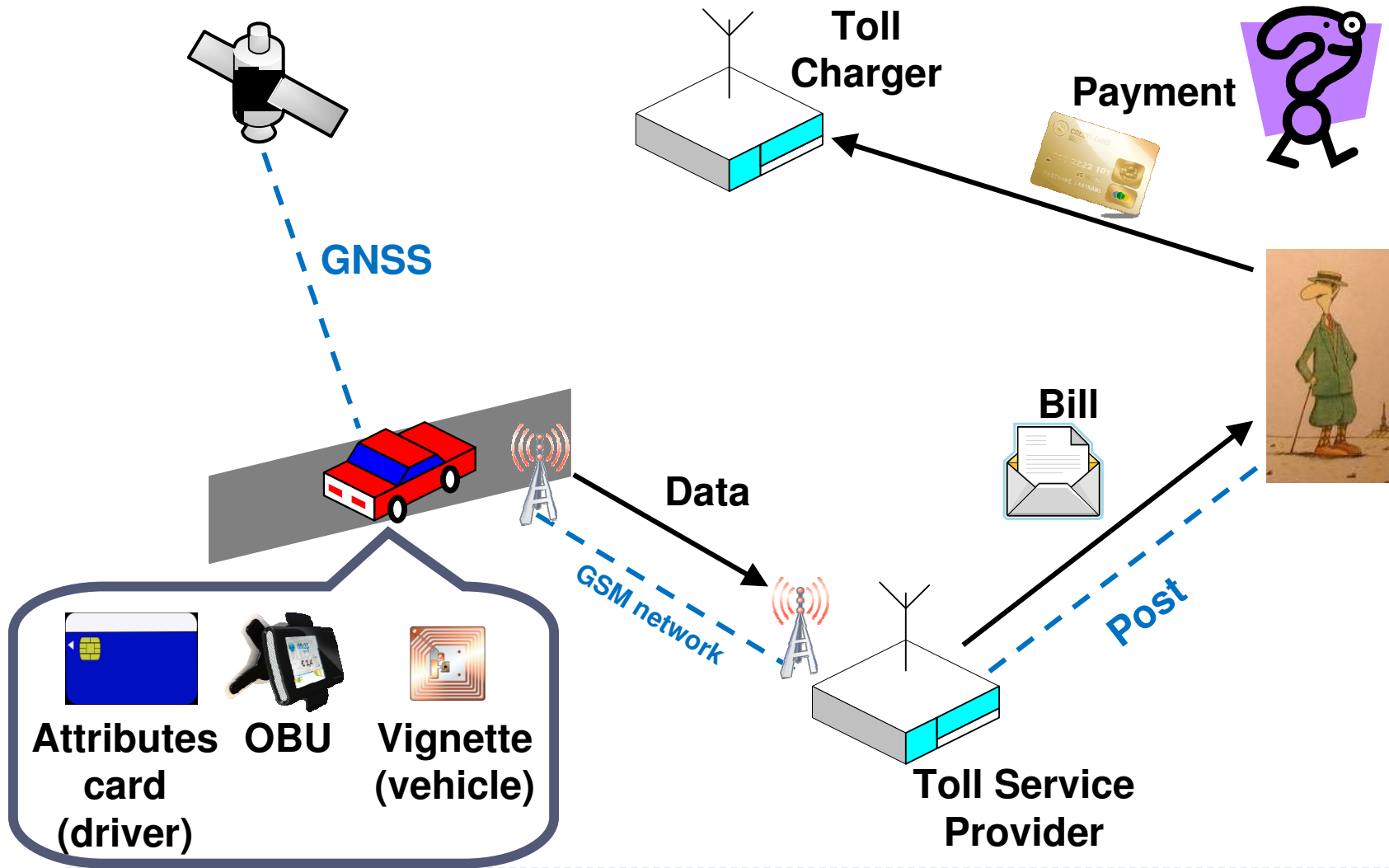
- } Data mining

- ▶ 3} Additional services (LBS, targeted advertising,...)

EETS architecture



EETS: Straightforward implementation



Straightforward implementation

- Flexible: dynamic fee calculation, depending on situation.
- Centralized computation in back-end
 - → Cheap hardware in the car
- Centralized business and application logic in back-end
 - → Easy to update
- Easier enforcement: TSP has access to all data
- Business advantage: data mining and new services

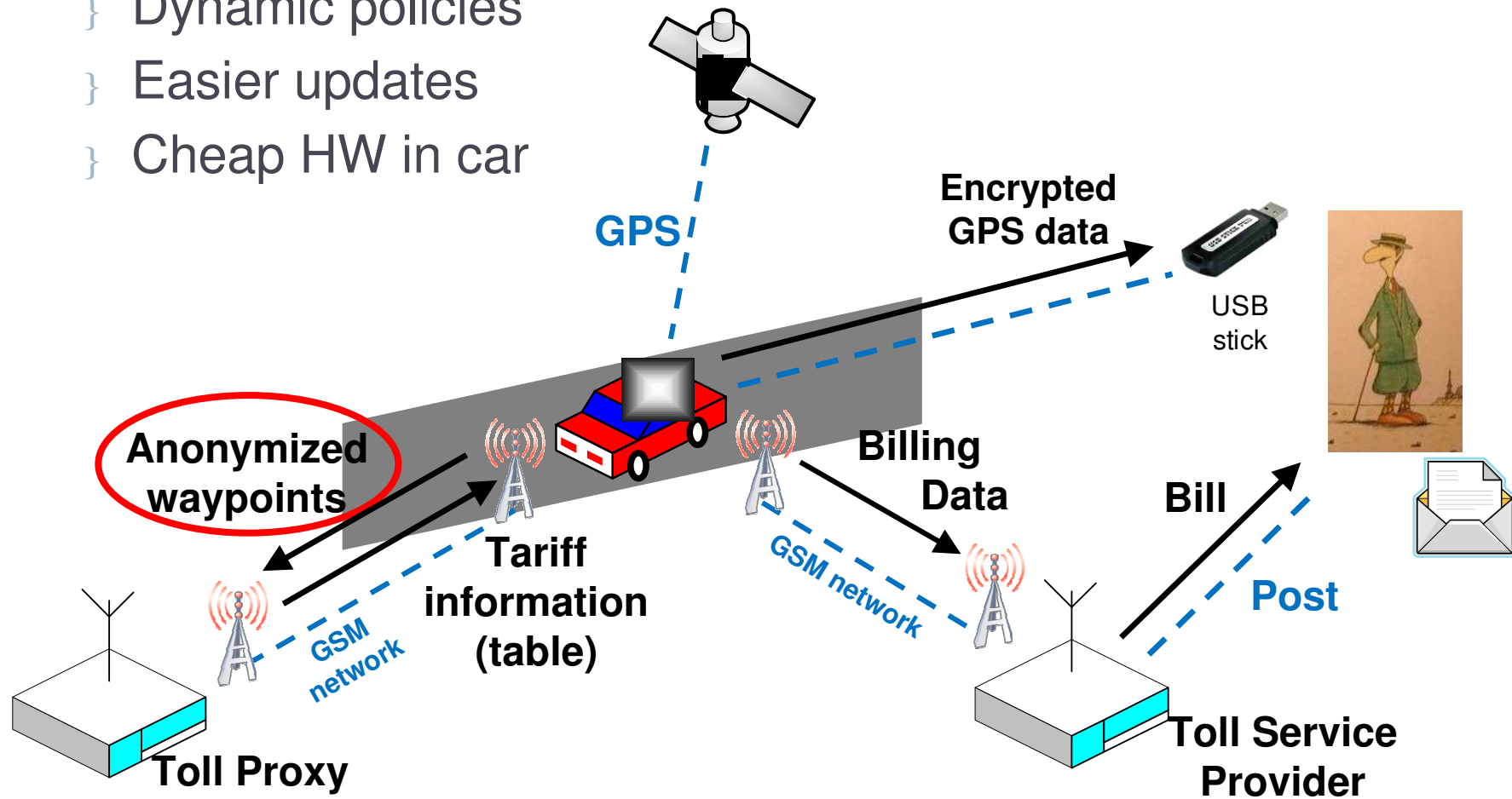
- **Privacy invasive: tracking**
 - Business confidentiality, safety, personal privacy
- Upstream transmission of data
- Third parties (legal implications)

Legal aspects

- } Data subject and data controller are not easy to identify
 - } Driver vs car owner
 - } Box vs TSP
 - } Rental cars, company cars,...
- } Not possible to anonymize data
 - } TSP makes calculation, thus holds all data
 - } Similar to cell phone model
- } Minimization or proportionality
 - } Fine grained GPS data reveal a lot of information
 - speed, time

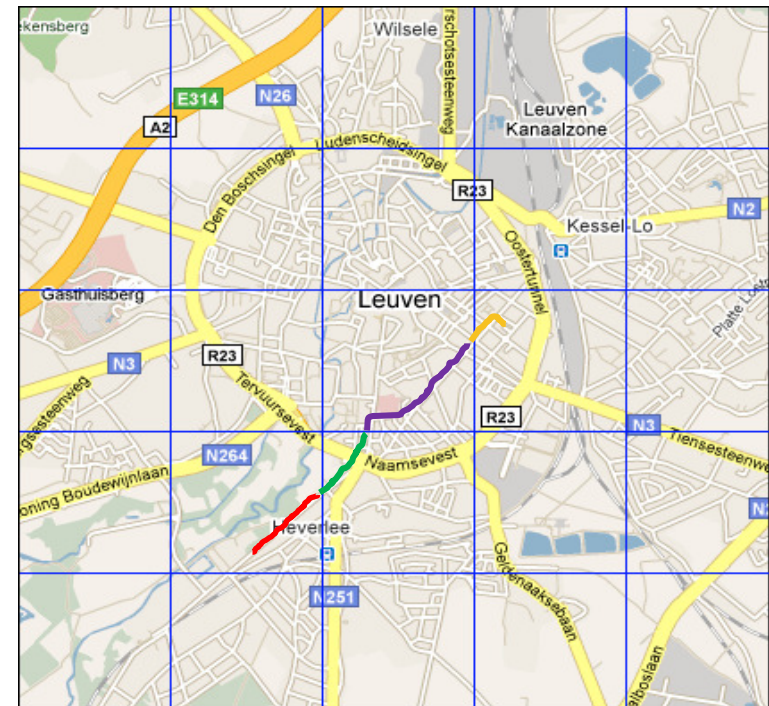
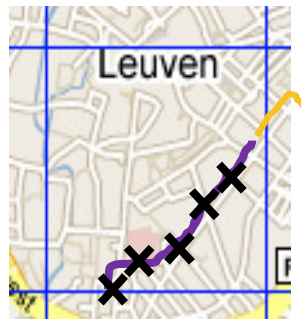
Smart client

- } Tariff look-up in back-end, but calculation in OBU
- } Dynamic policies
- } Easier updates
- } Cheap HW in car



Anonymization

- } Divide trajectories in segments: 1 segment/cell in grid
- } **Remove time and speed information**
- } Dissolve in the noise of the crowd
- } Use GSM operator as anonymizer proxy
 - } GSM NAT hides IP addresses
 - } Encrypted data for the Toll Proxy
 - } Assumes parties do not collude



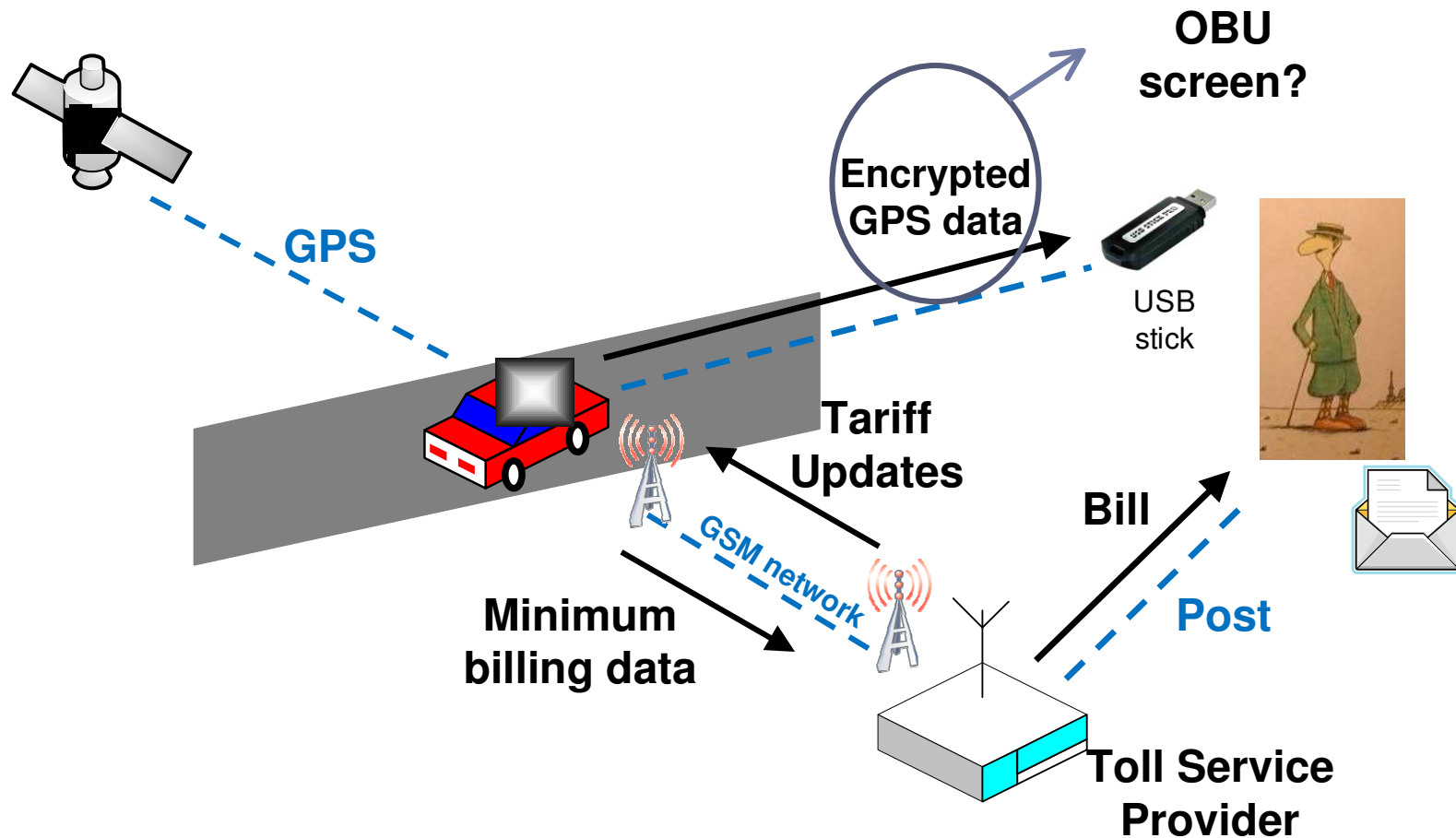
Legal aspects

- } Data subject and data controller are not easy to identify
 - } Is there personal data?
 - } Cost and utility
 - } Box cheaper, no map or policy updates
 - } Trade-off between coarse data and anonymous data mining

- } Best Available Technology, anonymity?
 - } Techniques used in other domains for many years (e.g. spread spectrum communication, sensor node networks, ...)
 - } Fit-for-purpose in telematics applications under analysis (fits with roll-out time-frame).

Fat client

} GPS + OBU (computation) + transmit billing



Fat client

- Privacy friendly
- Easy computation
- Small upstream transmission
- Third parties do not carry personal data
- Privacy-friendly enforcement

- Difficult to update
 - Large amount of vehicles
 - Driving into another country (in Europe is easy...)
 - Digital maps: license costs & network load
- Less dynamic
 - but can be made flexible a posteriori

Legal aspects

- } Data subject still problematic... but no data controller!
 - } No personal data involved

- } No need for anonymization
 - } No personal data involved

- } Data minimization by design
 - } Fine grained GPS data reveal a lot of information

- } Best Available Technology + Privacy by design

Privacy-Friendly Enforcement

} Control mechanisms applied by the Toll Charger to detect misuse of the system

} Law-enforcement

} Includes...

} 1) Detect vehicles with inactive OBUs


} 2) Detect vehicles reporting false location data

} 3) Detect vehicles using incorrect road prices

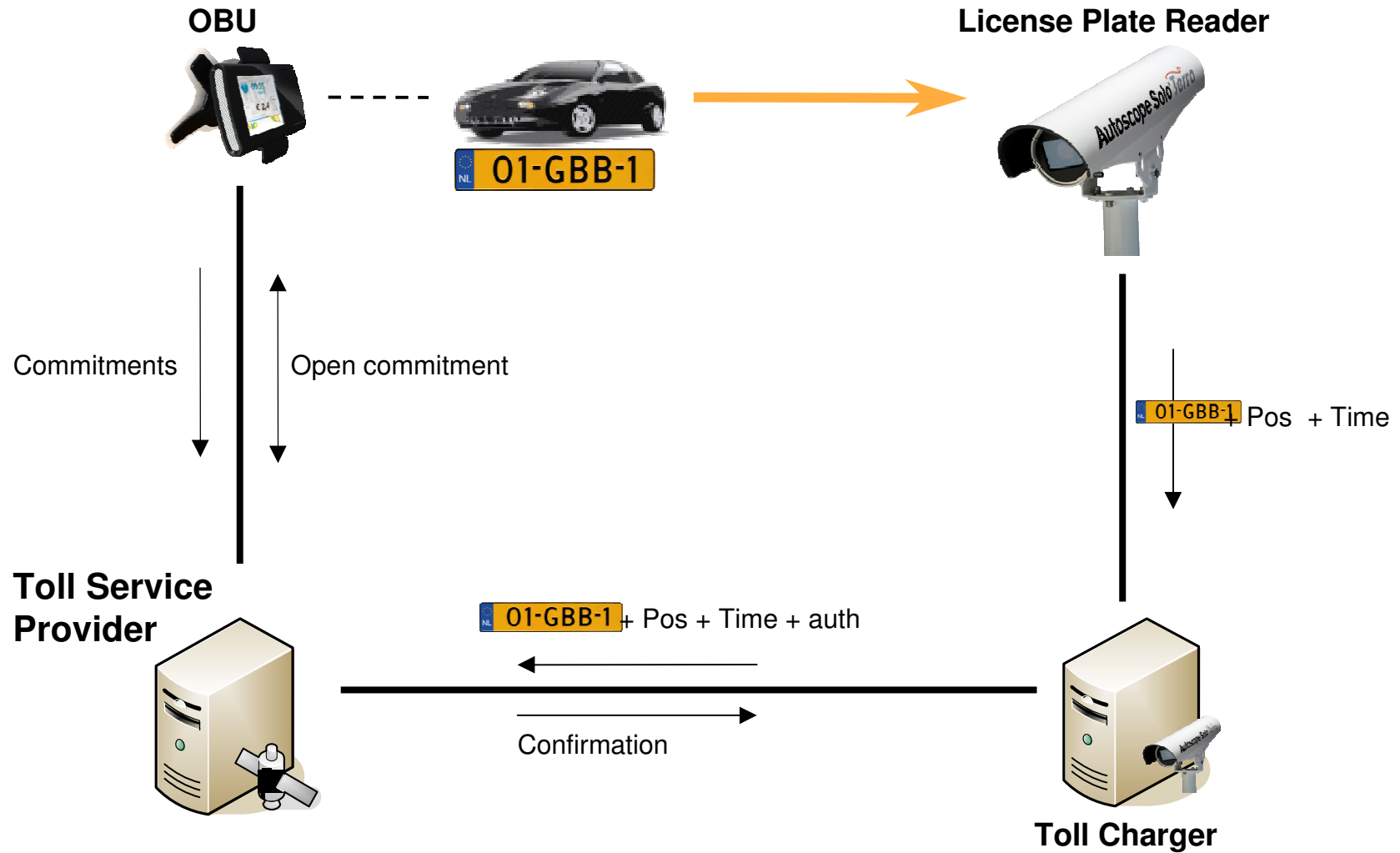
} 4) Detect vehicles reporting false final fees

} ... in a privacy-friendly way

} Minimize disclosure of location data

- 
- Visual inspection
 - DSRC
 - Comparison with odometer

How does it work?



What can we prove?

- } OBU used correct prices
 - } Prices in the table signed by Toll Service Provider
- } OBU was at reported location
 - } Compare photo location with committed location
- } OBU made correct operations
 - } Homomorphic commitments
- } Ongoing work: theory and implementation
 - } Similar to [Popa et al 09], more flexible

Conclusions

- } “Pay per use” has many advantages but its implementation may have catastrophic privacy consequences

- } Straightforward implementation
 - } Privacy invasive
 - } Not BAT

- } Smart Client
 - } Has advantages towards dynamism, price and maintenance
 - } Anonymity properties under analysis

- } Fat Client
 - } Offers strong privacy and data minimization by design
 - } BAT