KiZOOM

acute technology

DSP DESIGN dspdesign.com

trusted driver

The Trusted Driver Approach to Privacy in TDP Road Pricing Schemes

Charles Palmer & Nick Knowles

Background

- Road congestion a growing problem.
- It could be relieved by “Time, Distance, Place” (TDP) road pricing across the entire road network.
- Concern about driver **privacy** is a significant issue for public acceptance.
- UK Department for Transport Demonstrations Project will trial TDP.
- Technology Strategy Board funds a parallel “Innovation Platform” program to develop key technologies.

Trusted Driver: a TSB Project

- Consortium project funded by the TSB.
- Refining, developing, prototyping and testing the "Trusted Driver" technology to ensure **privacy** for motorists in future road pricing schemes.
- Trusted Driver is novel and **patented.**
- Successful review by leading academic cryptographers
- Partners:
  - **Kizoom**: mobile transport software
  - **Acute Technology**: consultancy
  - **DSP Design**: embedded computing

trusted driver

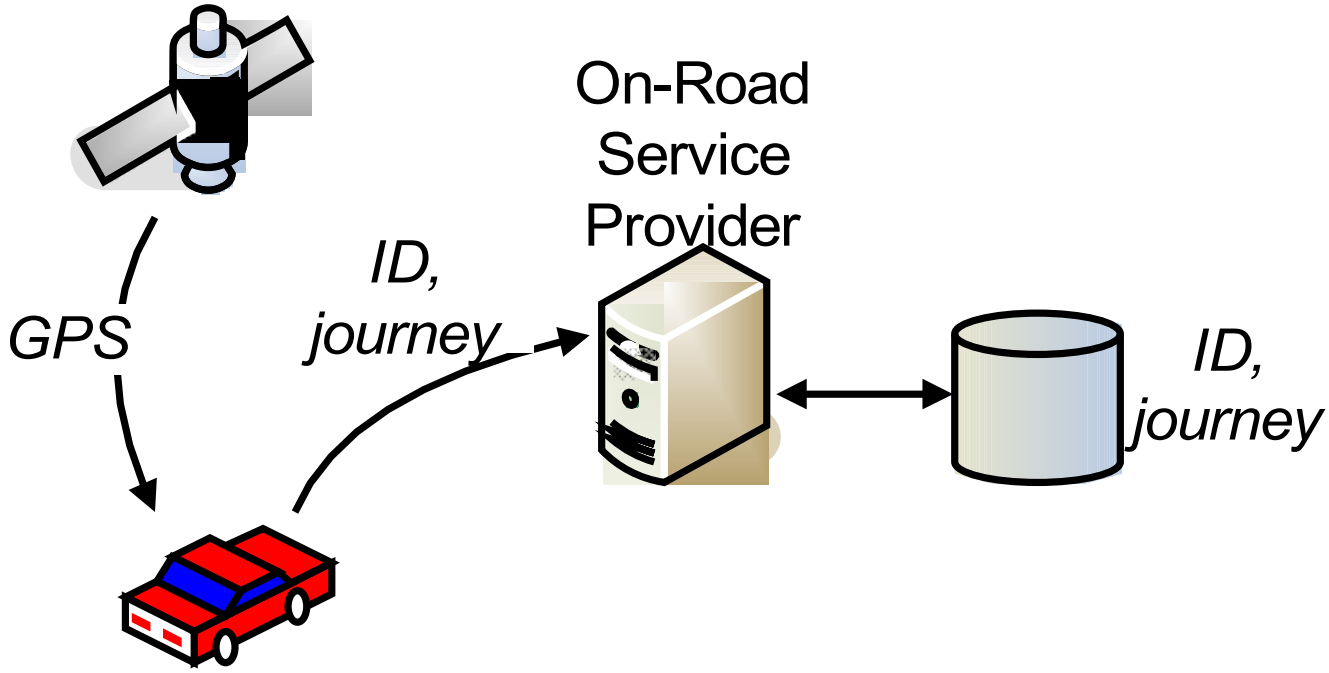
Trusted Driver Technology

- Guarantees **privacy** to motorists.
- Guarantees charging process for operator.
- Provides options for itemised bills.
- Includes enforcement measures to ensure compliance and detect cheating.
- Employs well-established **cryptographic** techniques in a novel way.
- Can be built with commodity technology platforms.

trusted driver

trusted driver

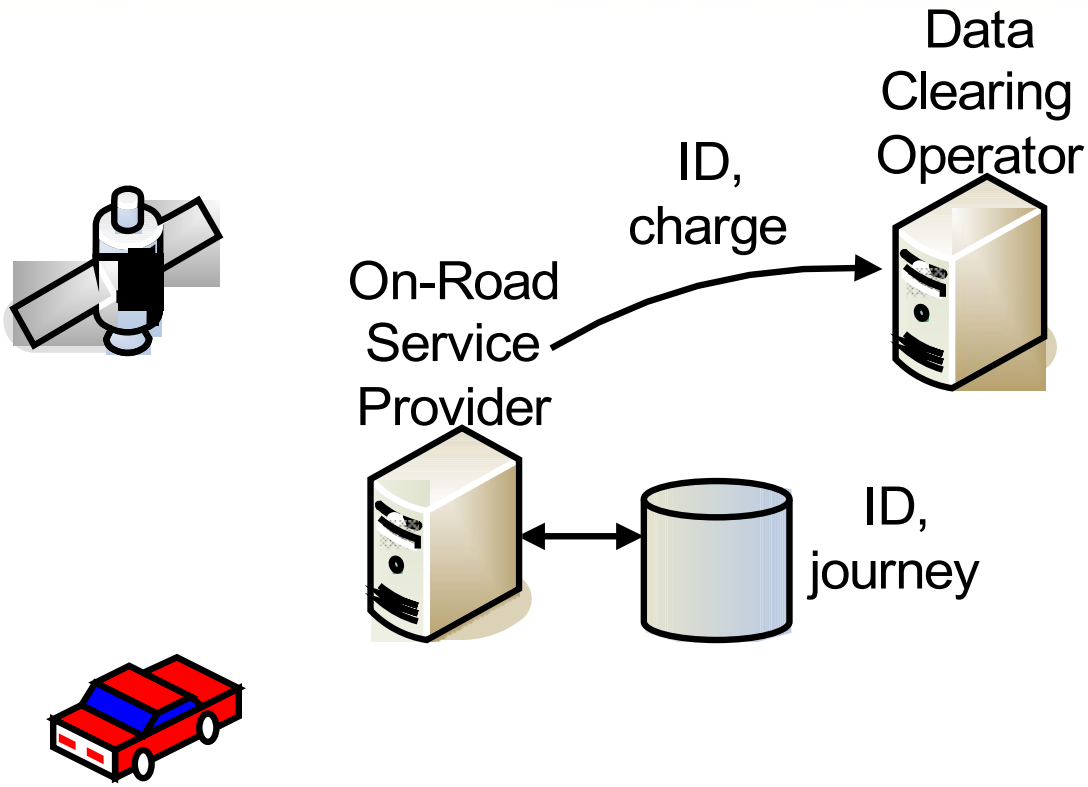
How NOT to do TDP



Vehicle reports journey information and its ID code to an "On-Road Service Provider" server.

trusted driver

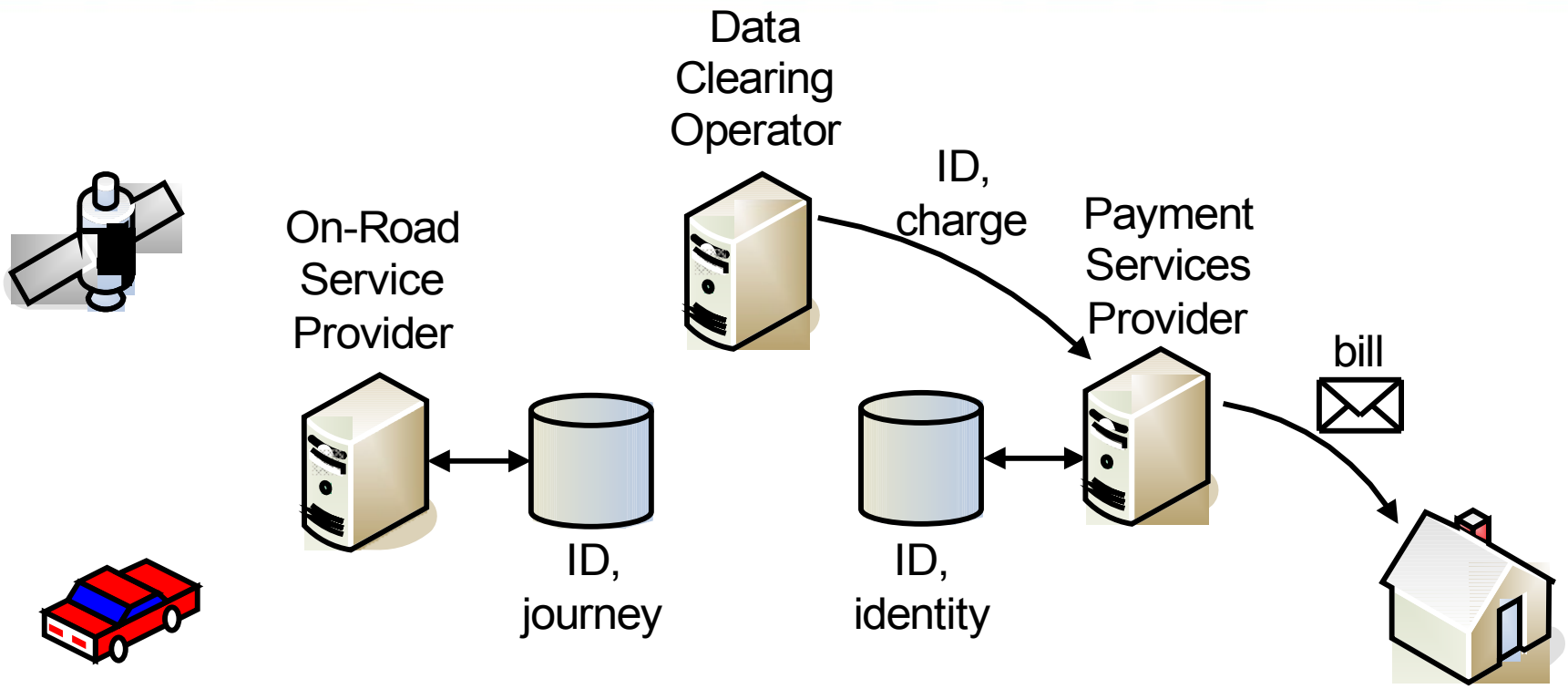
How NOT to do TDP



On Road Service Provider calculates the road charge and sends it to a “Trusted Third Party” - the Data Clearing Operator.

trusted driver

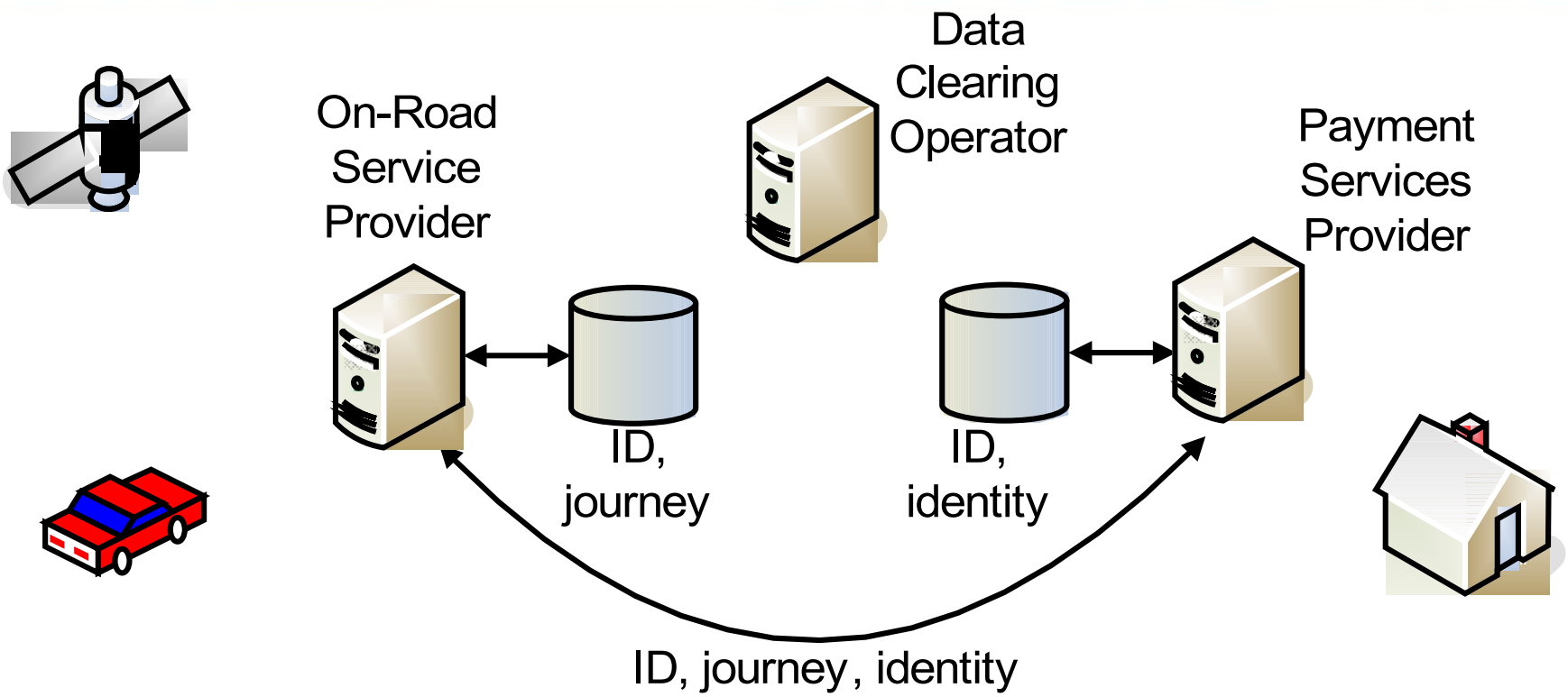
How NOT to do TDP



Data Clearing Operator passes charge data to “Payment Services Provider” which looks up the driver and issues a bill.

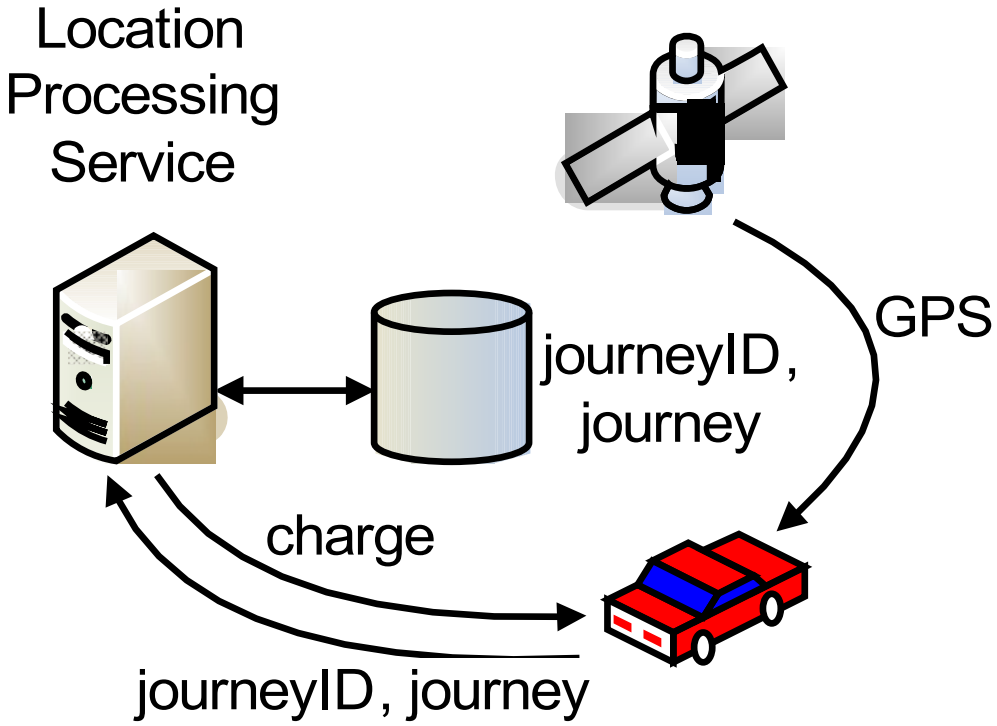
trusted driver

How NOT to do TDP



Privacy can be compromised by hackers, and **must** be compromised to issue an itemised bill.

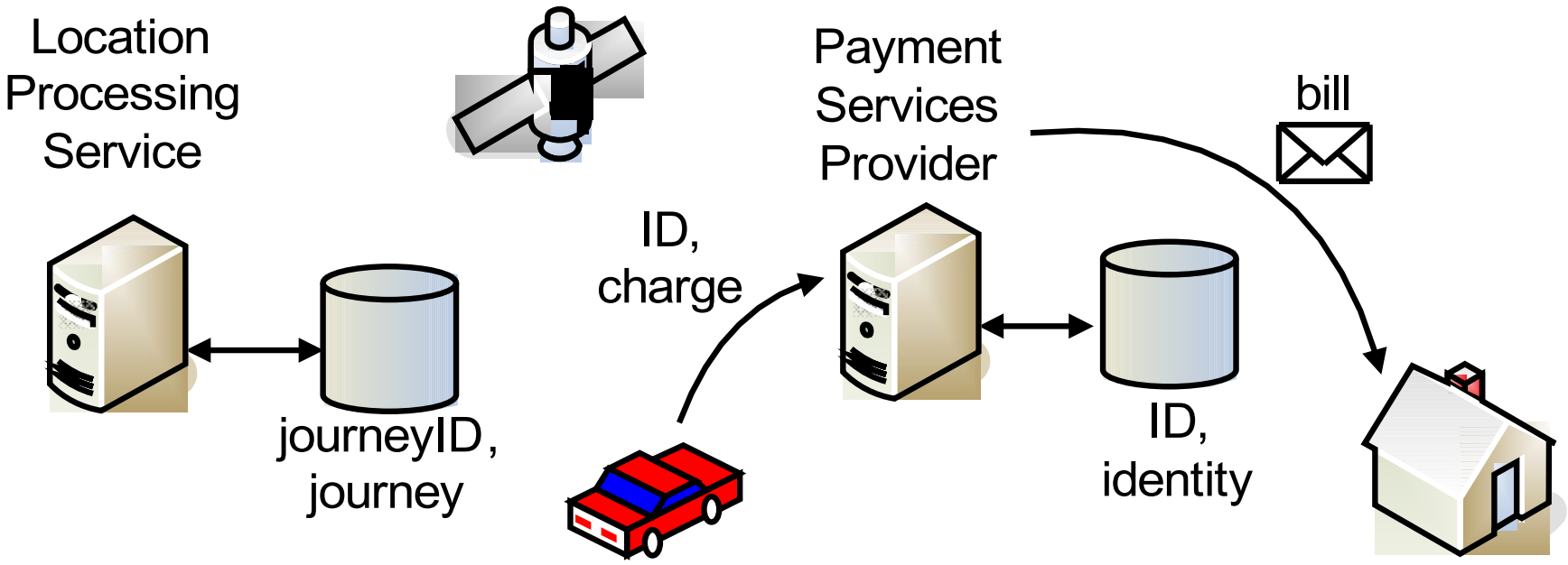
The Trusted Driver Model



Vehicle reports journey information **anonymously** to Location Processing Service which returns road charge **to the vehicle**. The journey IDs are based on a secret key.

trusted driver

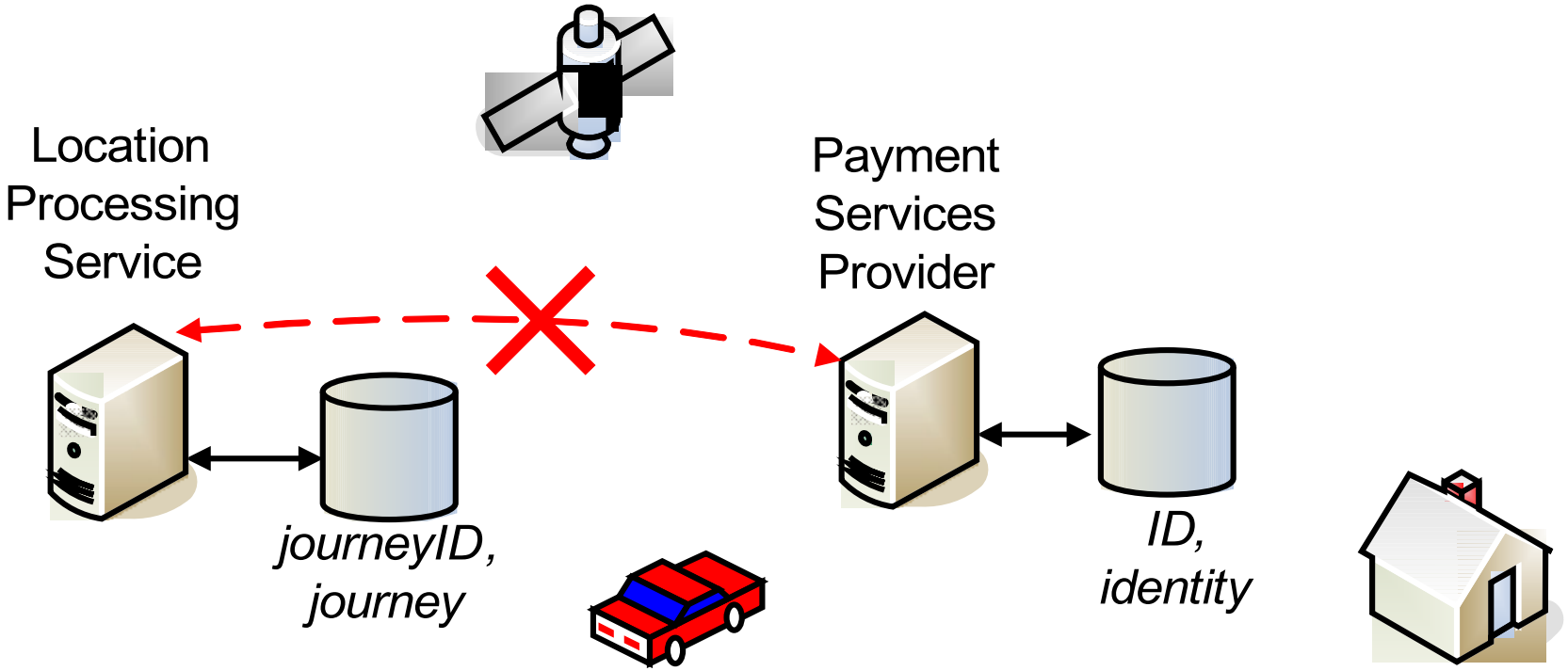
The Trusted Driver Model



Vehicle sends accumulated charge data, with its ID, to Payment Service Provider which looks up the driver and issues a bill. No journey details (time, position) are sent.

trusted driver

The Trusted Driver Model



Even someone with access to both databases cannot link the driver's ID with the journey.

The Trusted Driver Model

- **Cryptographic protocols** ensure that billing service can trust the vehicle.
- **Journey** and **identity** data only linked inside secure cryptographic module.
- Even people with access to both servers **can't link journey** information to **identity**.
- Now the vehicle is the “Trusted Third Party”.
- Hence the name: Trusted Driver Model

trusted driver

Cryptographic Module

- Tamper-resistant cryptographic module in OBU = Smart Card (combined with SIM card).
- Contains secret keys to use with PKI authentication, encryption protocols (as in https, SSL).
- Contains all sensitive data, including the accumulated price and the key that generates the journey IDs.
- Allows OBU to authenticate itself to servers, and to generate and check digital signatures.
- Signatures allow detection of hacked OBU software, spoof GSM messages and GPS data.
- Thus all players can trust the OBU messages.

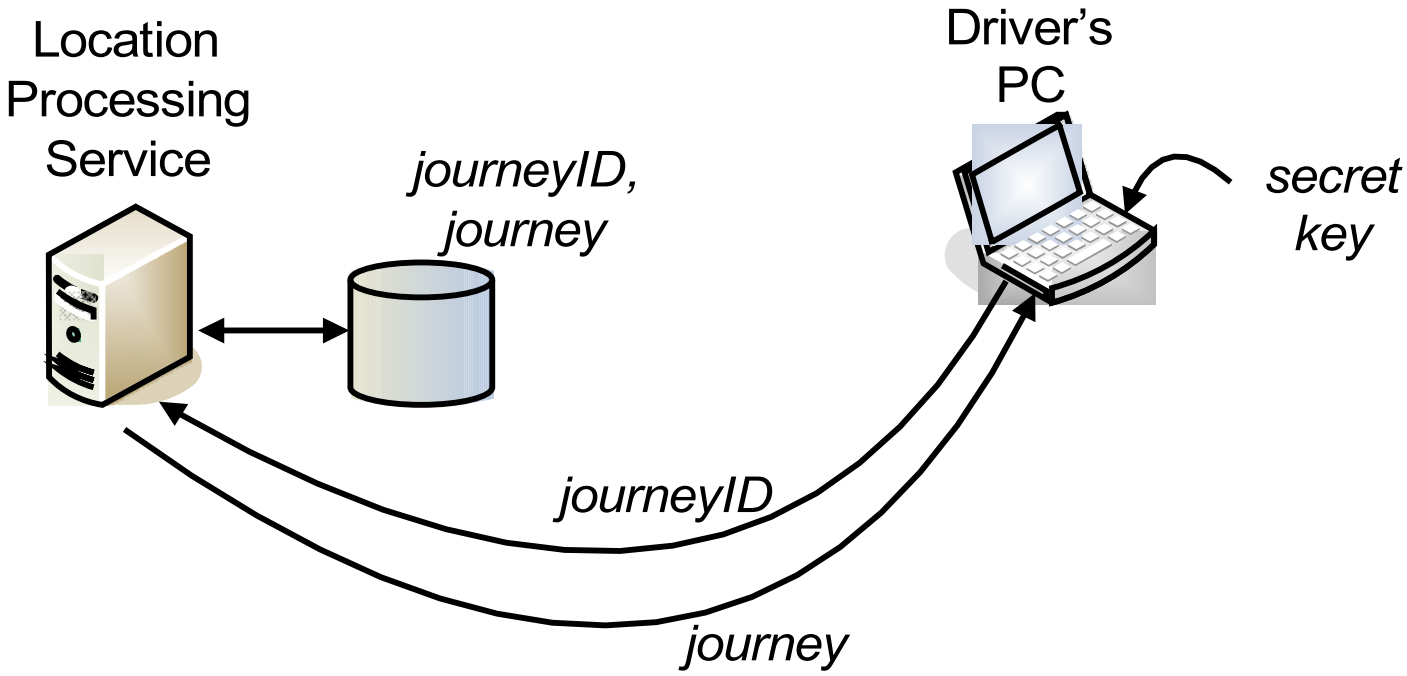
Itemised Bills

- Public Key Encryption secures on-line journey data.
- Drivers can choose options to match their privacy preferences:
  - No itemised bills = greatest privacy.
  - Driver creates itemised bill on-line by using driver-owned secret key.
  - Driver can get itemised bill by post, by deliberately revealing secret key.

trusted driver

trusted driver

Itemised Bill on Driver's PC



The driver's PC recreates the sequence of journey IDs using the secret key (shared with the OBU), and retrieves journey data so itemised bill can be generated at the PC.

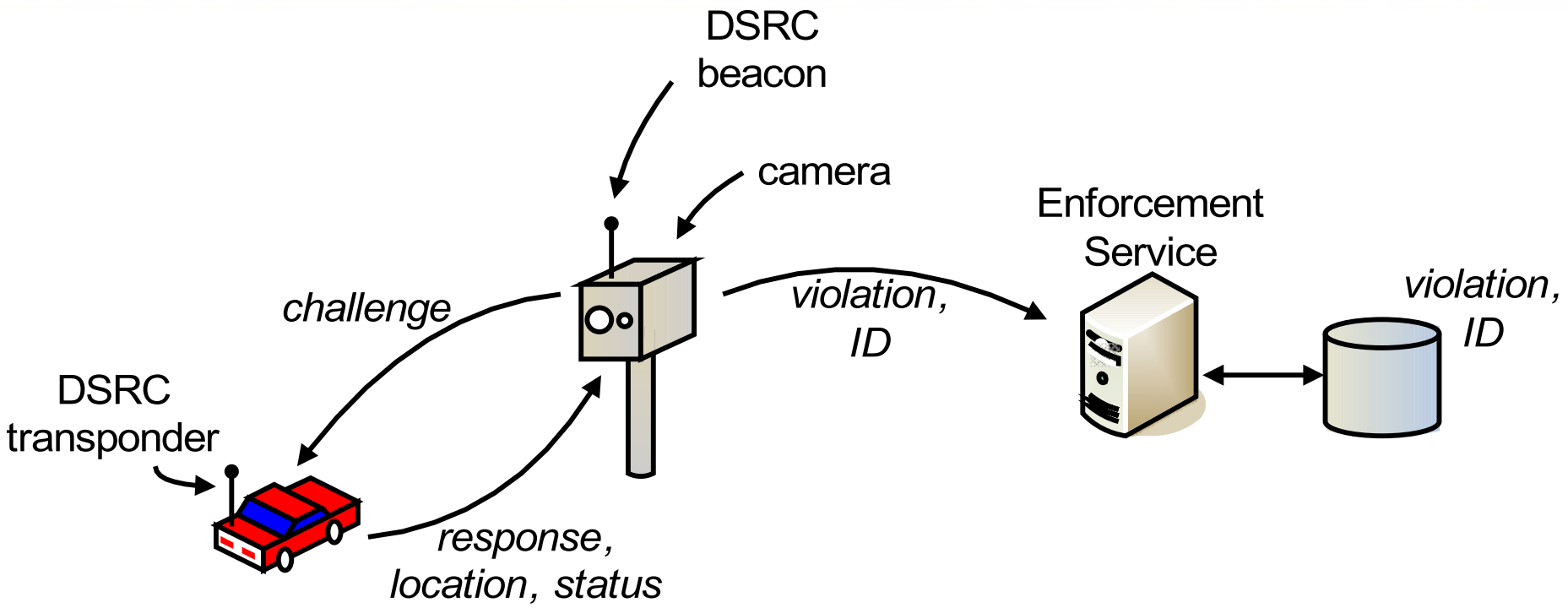
Ensuring Compliance

- Cryptographic authentication in a tamper-resistant SIM card secures On-Board Unit against fakes, clones.
- External cross-checks (cameras, RF beacons) challenge the OBU to prove it is operating honestly.
- Response to challenge (yes/no) is managed by the trusted OBU.
- Privacy is maintained: journey history is not leaked by the challenge.

trusted driver

trusted driver

Challenge from Road-Side Beacon



A road-side beacon challenges vehicle, which responds with its location and status, digitally signed. If location, status or signature are wrong a violation is recorded.

Web-based Demo

- Google Maps mash-up with web services for the Location Processing Service and Payment Processing Service.
- Please email for the URL, password:
- charles.palmer@acutetechnology.com

trusted driver

Trusted Driver - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.trusteddriver.com/demo/liveDemo

Most Visited | Contents Contents | Latest Headlines | rss.xml | /Message: New Vision... | Derbyshire County Co... | Google Bookmark

trusted driver

Home | Background | Technology | Demonstration | About Us

Demonstration of Trusted Driver Technology at Work

The middle panel represents the On Board Unit in the car and the other two panels the two servers: the Location Processing Service (LPS) and the Payment Processing Service (PPS). Click on the links in the OBU panel to watch the data transfer between the OBU and the other two servers. **At each step, an explanation is displayed in the bottom right-hand corner of the screen.**

LPS

The panel shows the contents of the Location Processing Service database (as of **04:12:54 PM**).

The journeys in the database are shown as text and on the map. Journeys for all cars (not just yours) are displayed.

	Journey ID:	Time band:	Journey data:	Price:
1	a0085f92c...	Peak	yqqbInj_F...	£0.15
2	357f08eb7...	Peak	_~rbIvt~D...	£0.15
3	bebb60eee...	Peak	ac{aIrfaE...	£0.15

OBU

This panel represents the On Board Unit in the car. You are the driver! Select a car and time! Then drag the two map markers and click "Travel" to simulate journeys. Next click "Report travel" to report each of the journeys at random to the LPS. Then click "Report charge" to report accumulated costs to the PPS.

Select car: Yellow

Time Band: Peak

1: Travel

2: Report travel

3: Report charges

You have **0** trips to report to LPS. You have **£0.00** in charges to report to PPS.

Number Plate: Yellow_222
Sequence number: 1
Accumulated Price: £0.15
Digital signature: 2873b0cc0...

PPS

The panel shows the contents of the Payment Processing Service database (as of **04:12:54 PM**).

The PPS server knows who drives the vehicles, but not where they have been. That is why there is no map shown in this panel.

	Vehicle:	Sequence:	Price:
1	Red_111	1	£0.30
2	Yellow_222	1	£0.15

Digital signature verified (named OBU)
Number plate: Yellow_222
Next sequence number: 2
Digital signature: e61c6591...

Accumulated price sent to Payment Processing Service

When you click the "Report charges" button a message is sent from the OBU across the Internet to the PPS.

You can see the message sent by the OBU in box with the arrow, below the buttons. The OBU identifies itself and sends a sequence number, the accumulated price and a digital signature.

When the PPS gets the message it adds the message to its database, increments the sequence number and sends these back to the OBU as an acknowledgement. You can see the message sent by the PPS in box with the arrow in the right-hand panel.

You can see the journey being recorded in the PPS database. Note that the PPS knows the identity of the OBU, but not where it has been. Charges for all cars (not just yours) are displayed.

When the OBU receives the acknowledgement from the PPS it zeros the outstanding charges and notes the new sequence number.

Done

Trusted Driver
Working Prototype

- Proof of concept implementation
  - Protocol design
  - Prototype OBU & Web services
  - Business Processes & system requirements
- Trusted Driver Web services
  - Location Processing Service
  - Pricing processing Service
  - Compliance Service
- Trusted Driver OBU Software
  - Location Service
  - Payment Service
  - Compliance Service
- OBU Hardware Design

trusted driver

Privacy in DfT TDP Demonstrations Project

- Represents an opportunity to examine ***all*** aspects of TDP, ***including privacy***:
- Which uses and users require privacy?
- What are the additional costs of privacy?
- What consequences of privacy violations?
- What will users understand and trust?
- Greatest TDP benefits come from fine-grained time and place resolution measurements: what are privacy implications?
- What privacy principles/policies?
- Which Privacy Enhancing Technologies are available to help?

trusted driver

Constructive Suggestions to DfT:

- Have (and be seen to have) a joined-up understanding of why privacy matters.
- Commission formal privacy studies including a Privacy Impact Assessment.
- Proactively examine Privacy Enhancing Technologies.

trusted driver

trusted driver

Thank you

- Trusted Driver technology offers one contribution to the TDP road pricing privacy problem.
- It should be evaluated.

Charles Palmer:
charles.palmer@acutetechnology.com

Nick Knowles:
nick_knowles@kizoom.com