PTB-Workshop on
“Protection of Measurement Data in Legal Metrology and Related Challenges”,
30.11.-01.12.2011, PTB Berlin

# Protection of Taximeter Data by Secure Elements

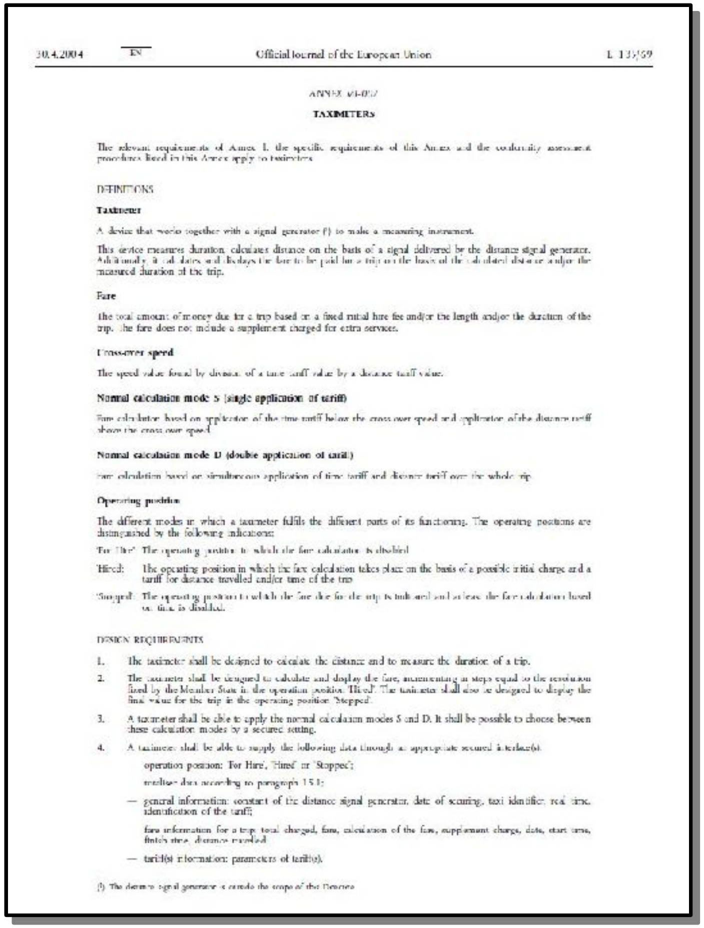
Jörg Wolff
Physikalisch-Technische Bundesanstalt (PTB)
joerg.wolff@ptb.de

# Outline

- Motivation
- How to Protect Taximeter Data?
- INSIKA Solution
- Why Secure Elements?
- Outlook

# Motivation: Protection of Taximeter Data

- different approaches in Greece, Belgium, Netherlands, Poland, Czech Republic,...
  (fiscal memories, fiscal taximeter, OTP, GPS,...)
- taximeter: type approval required, 2004/22/EC “Measurement Instruments Directive” (MID)
- → protection of taximeter data without touching the MID type approval



30.4.2004 EN Official Journal of the European Union L 135/69

ANNEX MI-007

**TAXIMETERS**

The relevant requirements of Annex I, the specific requirements of this Annex and the conformity assessment procedures listed in this Annex apply to taximeters.

DEFINITIONS

**Taximeter**

A device that works together with a signal generator (1) to make a measuring instrument.

This device measures duration, calculates distance on the basis of a signal delivered by the distance signal generator. Additionally, it calculates and displays the fare to be paid for a trip on the basis of the calculated distance and/or the measured duration of the trip.

**Fare**

The total amount of money due for a trip based on a fixed initial hire fee and/or the length and/or the duration of the trip. The fare does not include a supplement charged for extra services.

**Cross-over speed**

The speed value found by division of a time tariff value by a distance tariff value.

**Normal calculation mode S (single application of tariff)**

Fare calculation based on application of the time tariff below the cross-over speed and application of the distance tariff above the cross-over speed.

**Normal calculation mode D (double application of tariff)**

Fare calculation based on simultaneous application of time tariff and distance tariff over the whole trip.

**Operating position**

The different modes in which a taximeter fulfils the different parts of its functioning. The operating positions are distinguished by the following indications:

'For Hire': The operating position in which the fare calculation is disabled

'Hired': The operating position in which the fare calculation takes place on the basis of a possible initial charge and a tariff for distance travelled and/or time of the trip

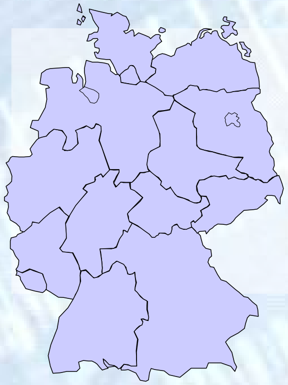
'Stopped': The operating position in which the fare due for the trip is indicated and at least the fare calculation based on time is disabled.

DESIGN REQUIREMENTS

1. The taximeter shall be designed to calculate the distance and to measure the duration of a trip.
2. The taximeter shall be designed to calculate and display the fare, incrementing in steps equal to the resolution fixed by the Member State in the operating position 'Hired'. The taximeter shall also be designed to display the final value for the trip in the operating position 'Stopped'.
3. A taximeter shall be able to apply the normal calculation modes S and D. It shall be possible to choose between these calculation modes by a secured setting.
4. A taximeter shall be able to supply the following data through an appropriate secured interface(s):
   - operation position: 'For Hire', 'Hired' or 'Stopped';
   - totaliser data according to paragraph 15.1;
   - general information: constant of the distance signal generator, date of securing, taxi identifier, real time, identification of the tariff;
   - fare information for a trip: total charged, fare, calculation of the fare, supplement charge, date, start time, finish time, distance travelled;
   - tariff(s) information: parameters of tariff(s).

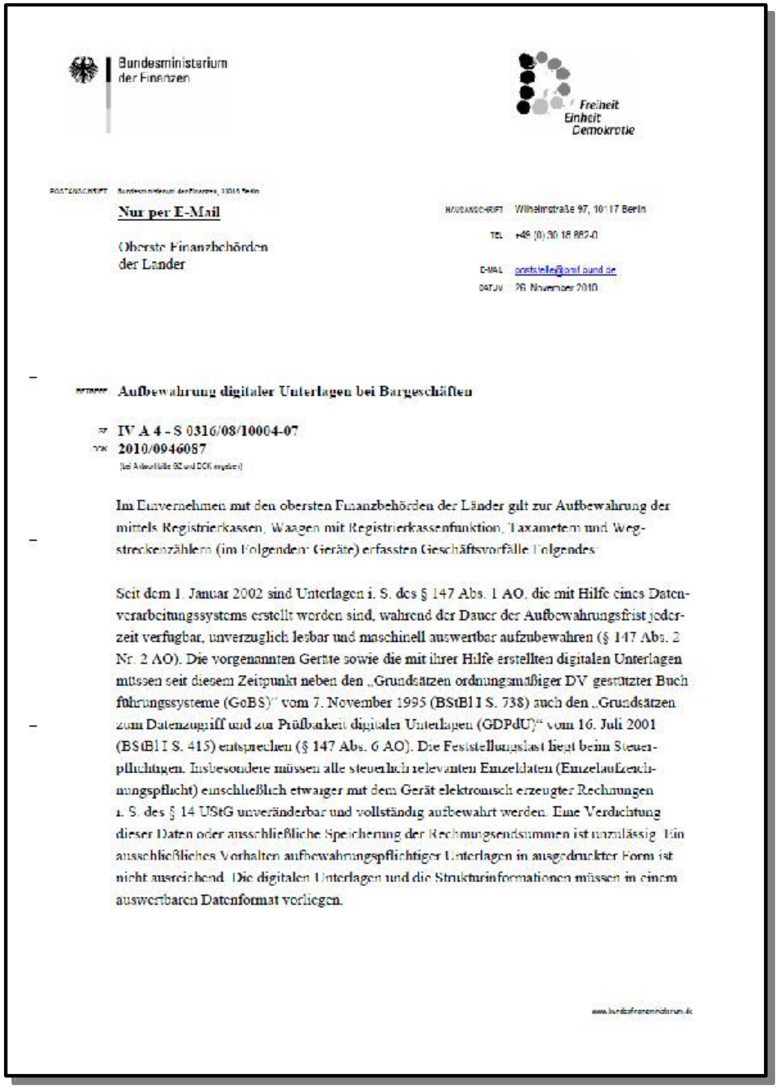
(1) The distance signal generator is outside the scope of this Directive.

2004/22/EC “MID”



# Protection of Taximeter Data in Germany

- letter of the German Ministry of Finance (BMF) from Nov. 2010
- taxi companies should provide data of every trip and shift in electronic format
- Hamburg and Berlin support pilot tests, Hamburg supports equipment for every cab
- collaboration with Tesymex UG and HALE GmbH
- increasing interest of taxi companies



Bundesministerium
der Finanzen

Freiheit
Einheit
Demokratie

POSTANSCHRIFT Bundesministerium der Finanzen, 11016 Berlin

**Nur per E-Mail**

Oberste Finanzbehörden
der Länder

HAUSANSCHRIFT Wilhelmstraße 97, 10117 Berlin
TEL +49 (0) 30 18 682-0
E-MAIL poststelle@bmf.bund.de
DATUM 26. November 2010

BETREFF **Aufbewahrung digitaler Unterlagen bei Bargeschäften**

GZ **IV A 4 - S 0316/08/10004-07**
DOK **2010/0946087**
(bei Antwort bitte GZ und DOK angeben)

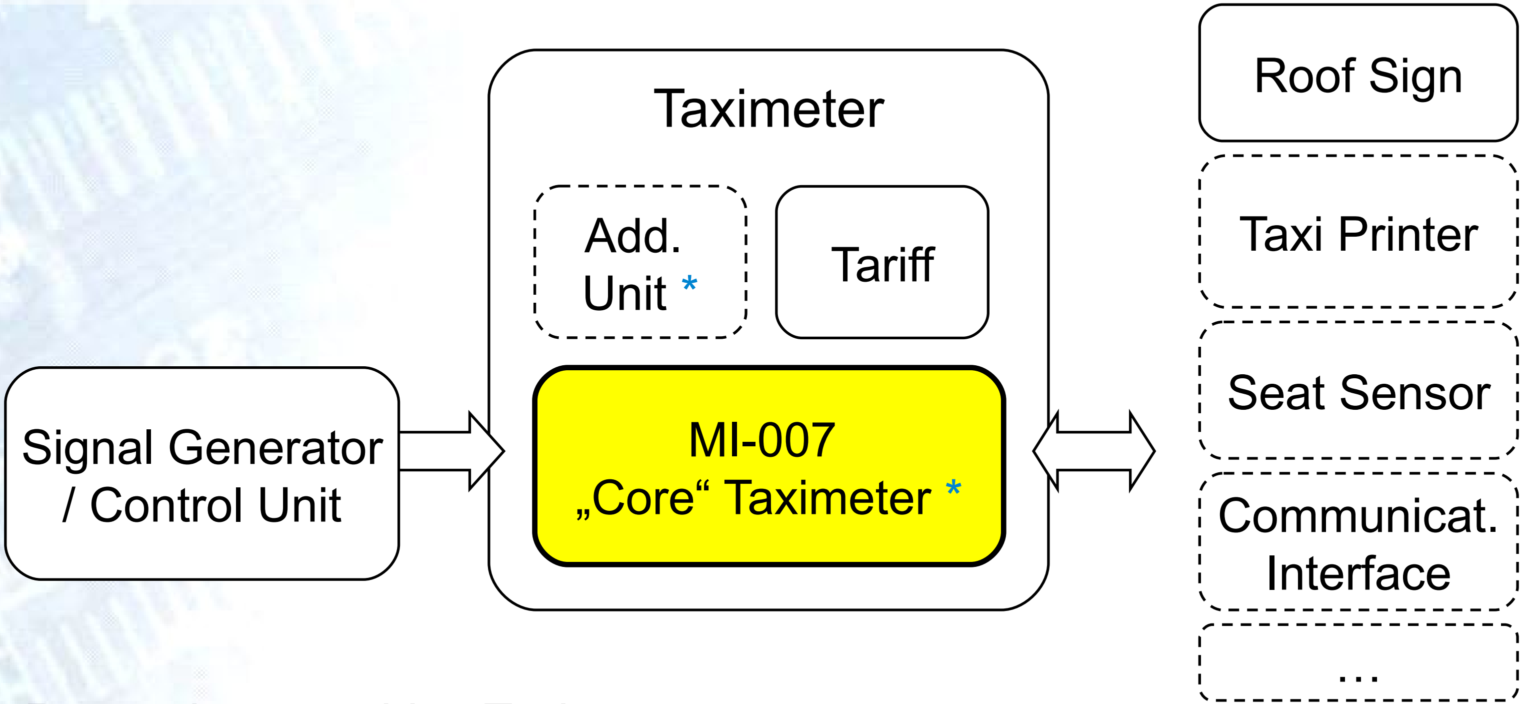
Im Einvernehmen mit den obersten Finanzbehörden der Länder gilt zur Aufbewahrung der mittels Registrierkassen, Waagen mit Registrierkassenfunktion, Taxametern und Wegstreckenzählern (im Folgenden: Geräte) erfassten Geschäftsvorfälle Folgendes:

Seit dem 1. Januar 2002 sind Unterlagen i. S. des § 147 Abs. 1 AO, die mit Hilfe eines Datenverarbeitungssystems erstellt worden sind, während der Dauer der Aufbewahrungsfrist jederzeit verfügbar, unverzüglich lesbar und maschinell auswertbar aufzubewahren (§ 147 Abs. 2 Nr. 2 AO). Die vorgenannten Geräte sowie die mit ihrer Hilfe erstellten digitalen Unterlagen müssen seit diesem Zeitpunkt neben den „Grundsätzen ordnungsmäßiger DV gestützter Buchführungssysteme (GoBS)" vom 7. November 1995 (BStBl I S. 738) auch den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)" vom 16. Juli 2001 (BStBl I S. 415) entsprechen (§ 147 Abs. 6 AO). Die Feststellungslast liegt beim Steuerpflichtigen. Insbesondere müssen alle steuerlich relevanten Einzeldaten (Einzelaufzeichnungspflicht) einschließlich etwaiger mit dem Gerät elektronisch erzeugter Rechnungen i. S. des § 14 UStG unveränderbar und vollständig aufbewahrt werden. Eine Verdichtung dieser Daten oder ausschließliche Speicherung der Rechnungsendsummen ist unzulässig. Ein ausschließliches Vorhalten aufbewahrungspflichtiger Unterlagen in ausgedruckter Form ist nicht ausreichend. Die digitalen Unterlagen und die Strukturinformationen müssen in einem auswertbaren Datenformat vorliegen.

www.bundesfinanzministerium.de

BMF letter from Nov. 2010

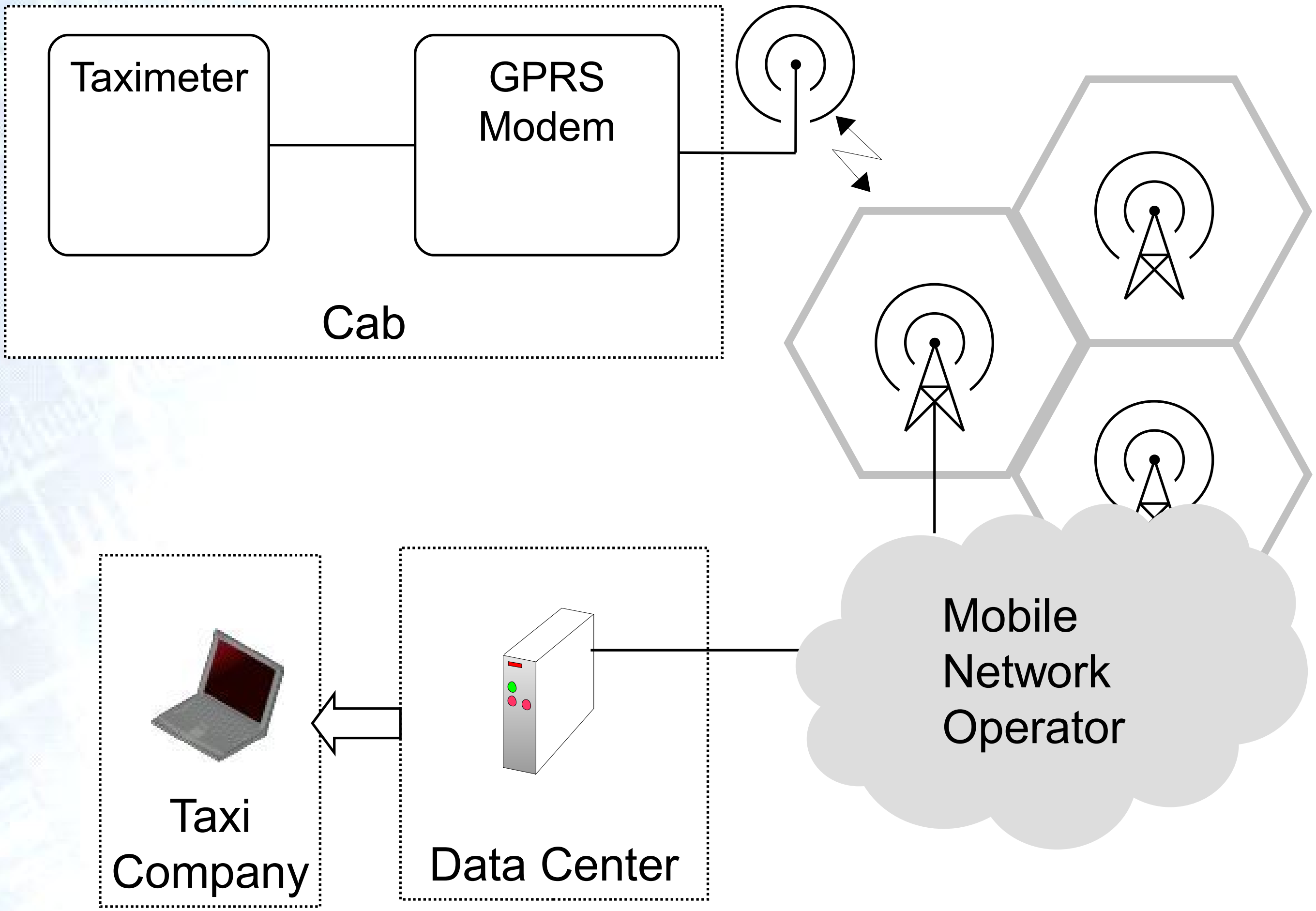
# Taximeter Environment



Regulations touching Taximeters:

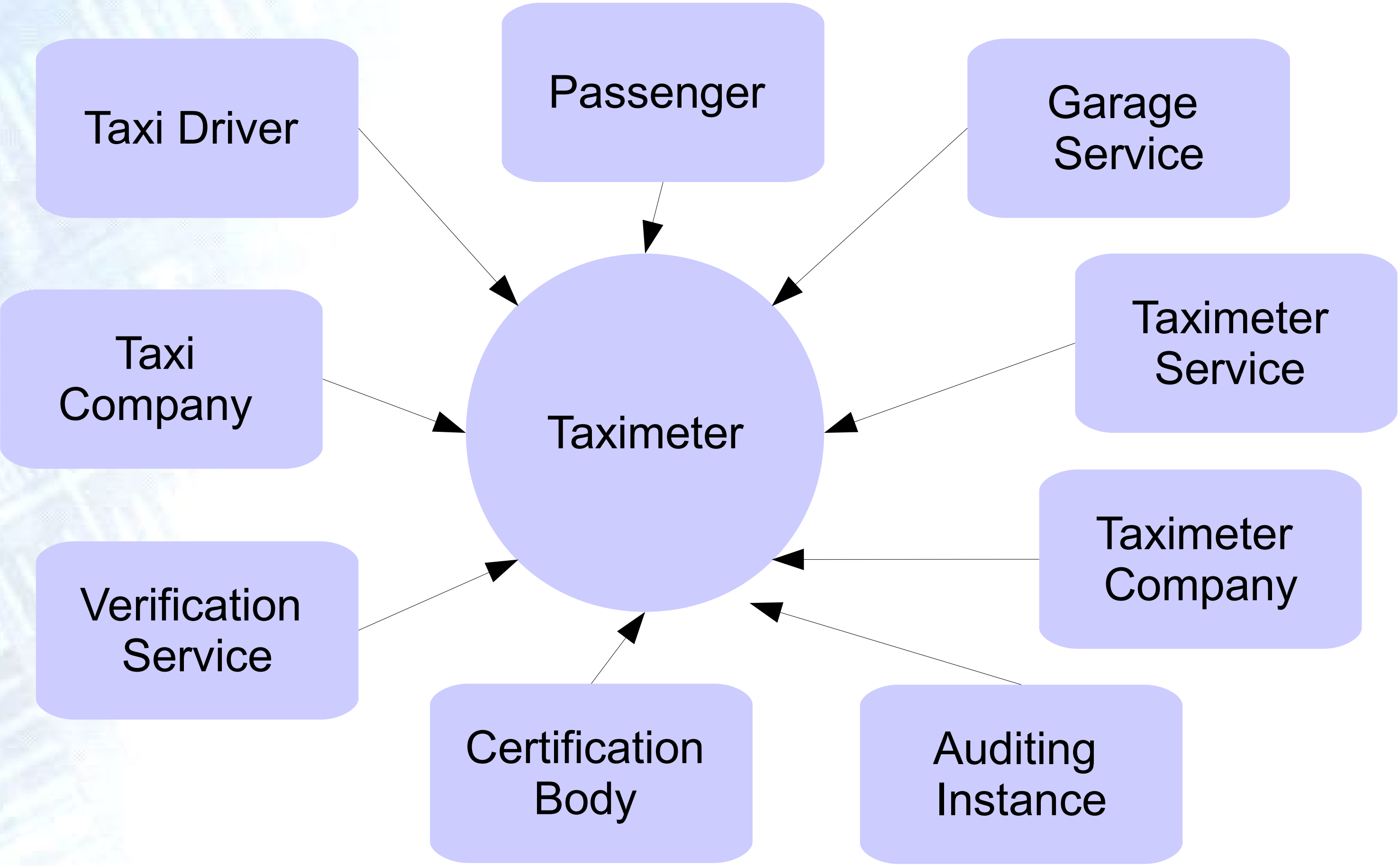
- * MID 2004/22/EC incl. Annex MI-007 for Taximeter
- WELMEC
- OIML R 21 (2007) Taximeters
- CENELEC EN 50148
- CAN CiA 447-3
- national regulations (Germany: EO 18-2, PTB-A 18.21, Eichgesetz, PBefG, BOKraft, ...)

# System Concept I: Plain/Insecure Wireless Link



→ no protection from alterations
→ no assignment to origin

# Taximeter Stakeholders



- taximeter data = turnover data:
  cost of tampering << revenue from tampering
- taxi drivers, taxi companies and allied under general suspicion

# Taximeter Data, as defined in MID, Annex MI-007

4. A taximeter shall be able to supply the following data through an **appropriate secured interface(s)**:

- **operation position**: "For Hire", "Hired" or "Stopped";

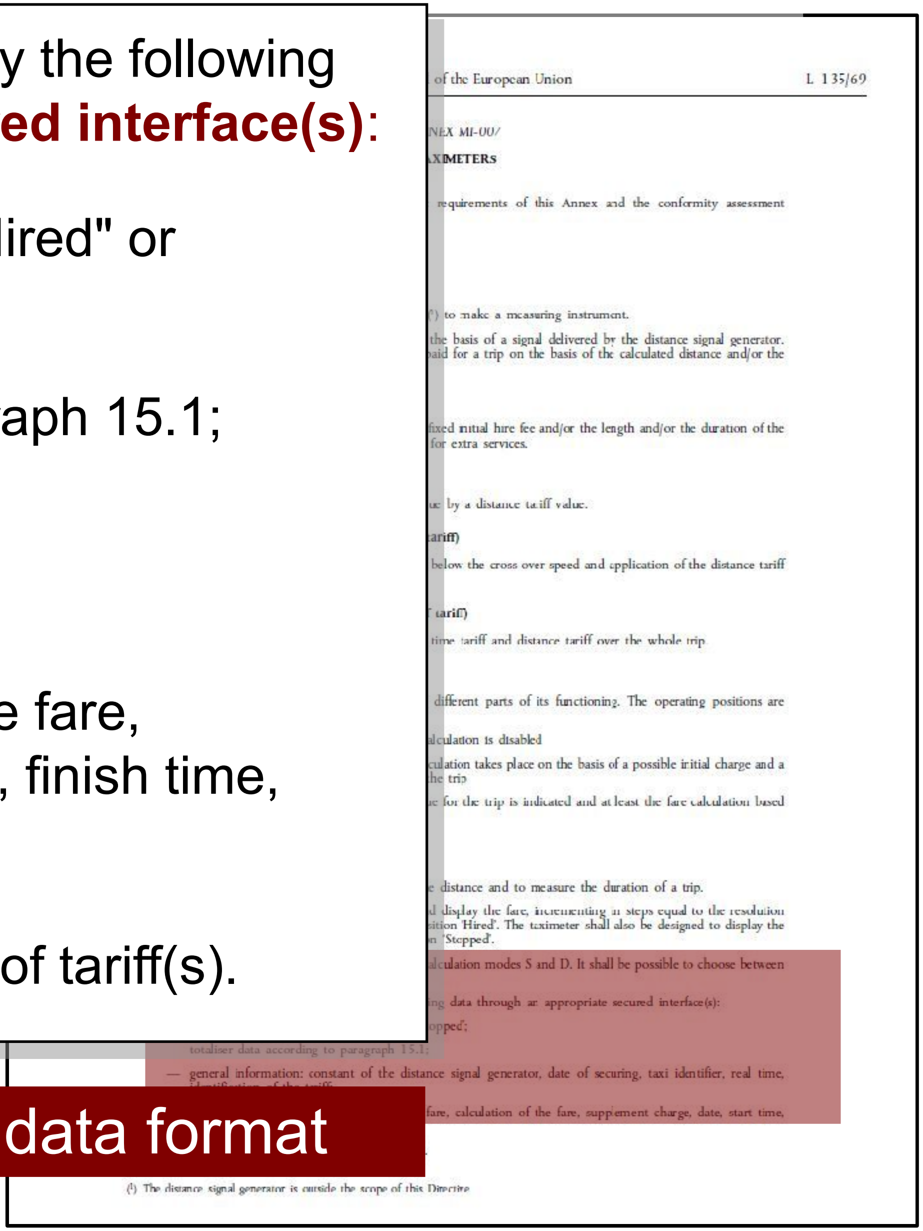
- **totaliser data** according to paragraph 15.1;

- **general information**: (…)

- **fare information for a trip**:
total charged, fare, calculation of the fare, supplement charge, date, start time, finish time, distance travelled;

- **tariff(s) information**: parameters of tariff(s).

→ no demand on interface or data format



of the European Union L 135/69

NEX MI-007

XIMETERS

requirements of this Annex and the conformity assessment

(¹) to make a measuring instrument.

the basis of a signal delivered by the distance signal generator.
paid for a trip on the basis of the calculated distance and/or the

fixed initial hire fee and/or the length and/or the duration of the
for extra services.

ue by a distance tariff value.

tariff)

below the cross over speed and application of the distance tariff

f tariff)

time tariff and distance tariff over the whole trip

different parts of its functioning. The operating positions are

alculation is disabled

culation takes place on the basis of a possible initial charge and a
the trip

ue for the trip is indicated and at least the fare calculation based

e distance and to measure the duration of a trip.

d display the fare, incrementing in steps equal to the resolution
sition 'Hired'. The taximeter shall also be designed to display the
n 'Stopped'.

alculation modes S and D. It shall be possible to choose between

ing data through an appropriate secured interface(s):

opped';

totaliser data according to paragraph 15.1;

— general information: constant of the distance signal generator, date of securing, taxi identifier, real time,

fare, calculation of the fare, supplement charge, date, start time,

(¹) The distance signal generator is outside the scope of this Directive

# Security Properties for Taximeter Data

- **Integrity**
  protection from modifications
- **Authenticity**
  prove of origin
- **Non-Repudiation**
  protected assets cannot be repudiated

**primary**

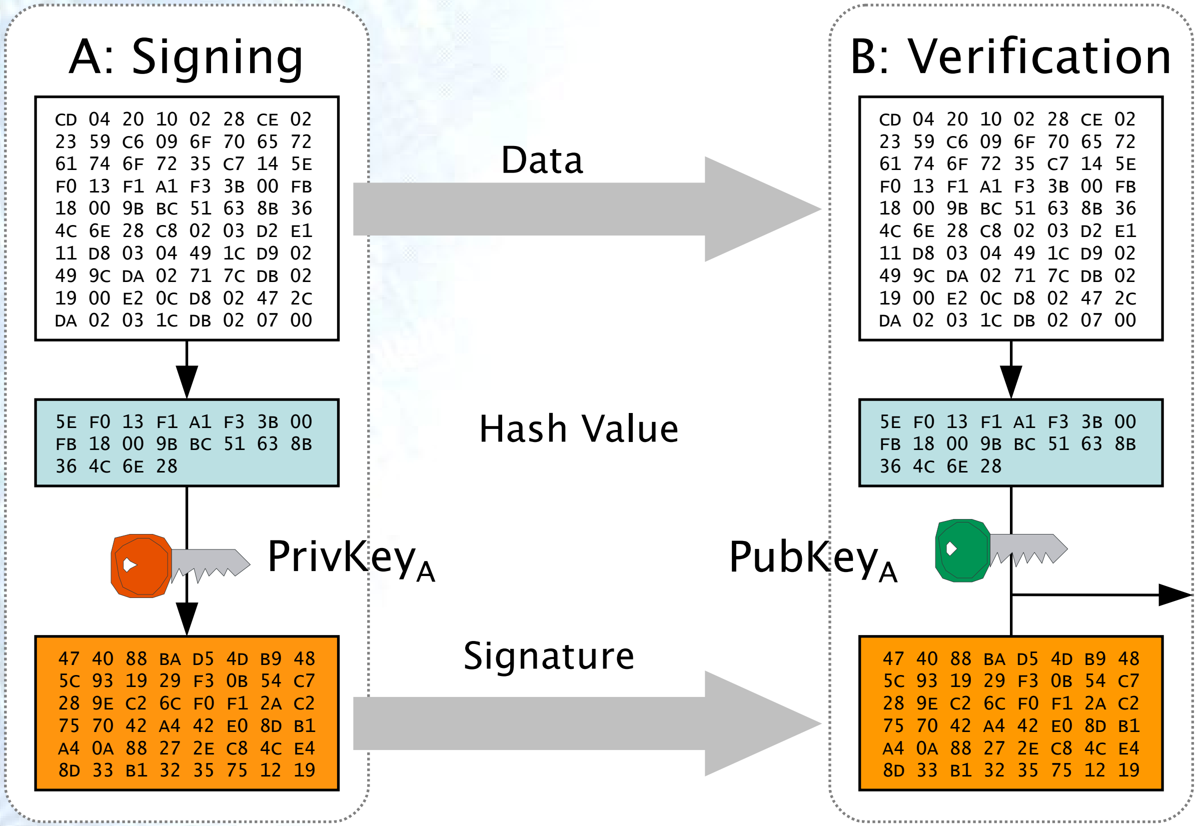
- **Confidentiality**
  protection from eavesdropping

**secondary**

→ cryptographic technology can assure all security properties

(other security properties: availability, etc.)

# Asymmetric Cryptography: Digital Signatures



A: Signing

```
CD 04 20 10 02 28 CE 02
23 59 C6 09 6F 70 65 72
61 74 6F 72 35 C7 14 5E
F0 13 F1 A1 F3 3B 00 FB
18 00 9B BC 51 63 8B 36
4C 6E 28 C8 02 03 D2 E1
11 D8 03 04 49 1C D9 02
49 9C DA 02 71 7C DB 02
19 00 E2 0C D8 02 47 2C
DA 02 03 1C DB 02 07 00
```

```
5E F0 13 F1 A1 F3 3B 00
FB 18 00 9B BC 51 63 8B
36 4C 6E 28
```

$\text{PrivKey}_A$

```
47 40 88 BA D5 4D B9 48
5C 93 19 29 F3 0B 54 C7
28 9E C2 6C F0 F1 2A C2
75 70 42 A4 42 E0 8D B1
A4 0A 88 27 2E C8 4C E4
8D 33 B1 32 35 75 12 19
```

B: Verification

```
CD 04 20 10 02 28 CE 02
23 59 C6 09 6F 70 65 72
61 74 6F 72 35 C7 14 5E
F0 13 F1 A1 F3 3B 00 FB
18 00 9B BC 51 63 8B 36
4C 6E 28 C8 02 03 D2 E1
11 D8 03 04 49 1C D9 02
49 9C DA 02 71 7C DB 02
19 00 E2 0C D8 02 47 2C
DA 02 03 1C DB 02 07 00
```

```
5E F0 13 F1 A1 F3 3B 00
FB 18 00 9B BC 51 63 8B
36 4C 6E 28
```

$\text{PubKey}_A$

```
47 40 88 BA D5 4D B9 48
5C 93 19 29 F3 0B 54 C7
28 9E C2 6C F0 F1 2A C2
75 70 42 A4 42 E0 8D B1
A4 0A 88 27 2E C8 4C E4
8D 33 B1 32 35 75 12 19
```

valid / invalid Signature

Algorithm Examples:

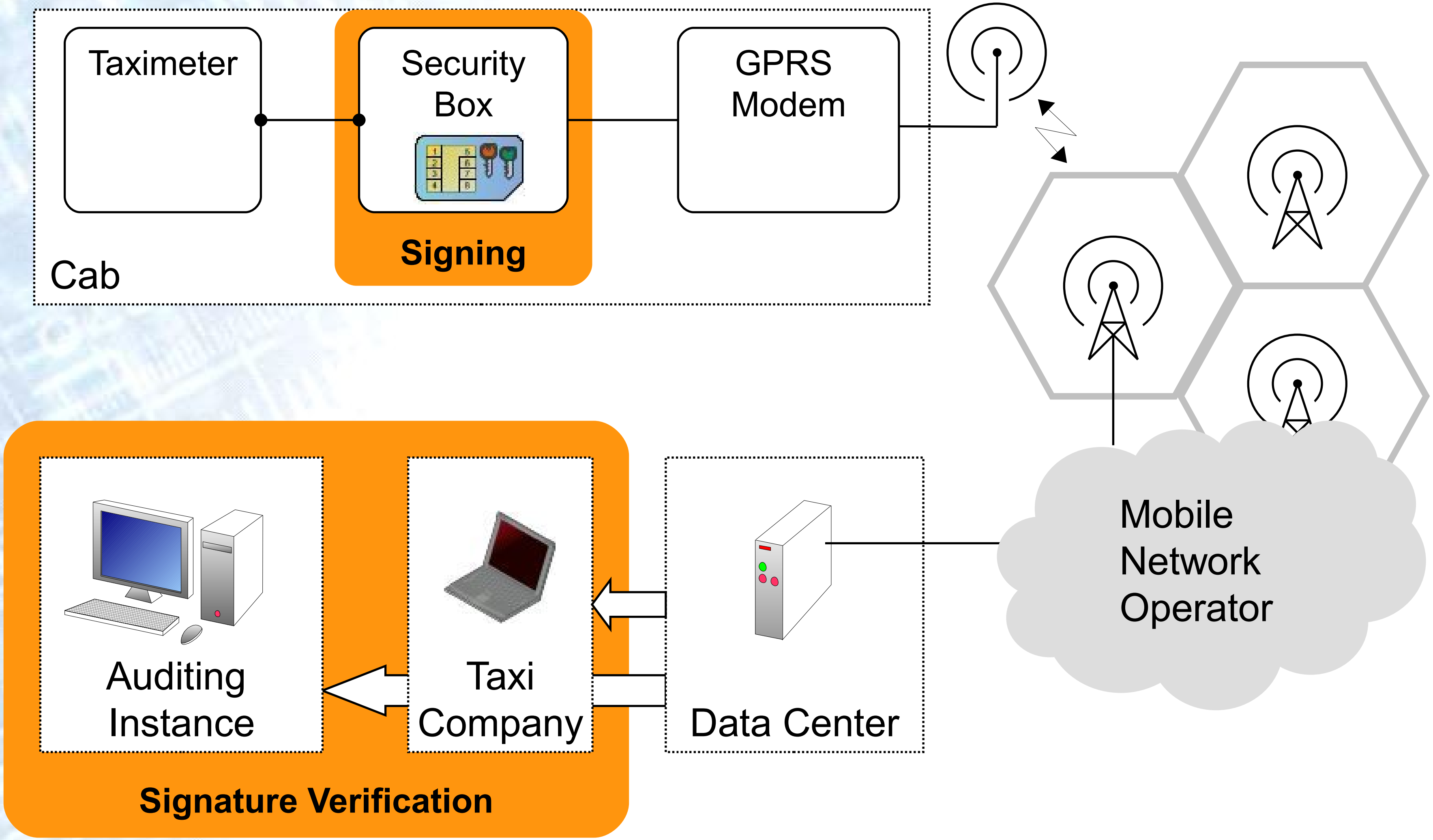
- RSA Signatures
- Digital Signature Algorithm (DSA)
- Elliptic Curve Digital Signature Algorithm (ECDSA)

A calculates hash value of data and signs using the private key ($\text{PrivKey}_A$)

B calculates hash value of data and can verify the signature by the use of A's public key ($\text{PubKey}_A$)

[x] Integrity
[x] Authenticity
[c] Non-Repudiation
[ ] Confidentiality

# INSIKA Solution: End-to-End Security



# INSIKA Solution

- **INSIKA**
  integrated security solution for cash registers & measuring instruments
- **Intention**
  sign data of cash registers and taximeters by secure elements
- **Demands**
  error-free operation, trust of the users in the solution, long term protection (up to 10 years)
- **Kerkhoffs's principle**
  security of a crypto-system depends on secrecy of keys only, not on secrecy of the algorithm
- **Environment**
  developed for environments where
  cost of tampering << revenue from tampering

INSIKA Smart Card

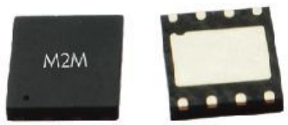
# INSIKA Profile for Taximeters

- profiles for cash registers and taximeters
- digital signatures (ECDSA) & sequence numbers
- special smart card software-package
- smart cards personalised to VAT-ID of taxi company
- certificates and smart cards issued by a trust centre (PKI)
- other secure elements feasible

INSIKA Smart Card

# Secure Elements

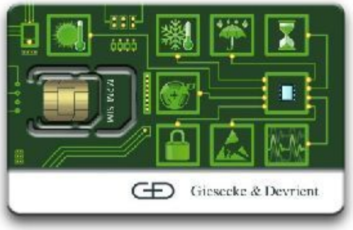
- hardware based security
- secure environment: ability to protect data (e.g. private key) on a high level
- costs for readout of protected data (e.g. one particular private key) >> revenue from readout
- resistance against many side channel attacks (SPA, DPA, Timing,..)
- available as certificated hard- & software (up to CC EAL 4..5+..)
- most secure elements are smart card based components

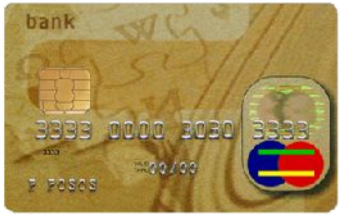


Images: Oberthur Technologies, Giesecke & Devrient, Infineon

# Applications of Smart Cards

- Subscriber Identity Modules (SIM), [SIMalliance members shipped 3.9 billion SIM cards in 2010]
- payment cards: EMVCo (American Express, JCB, MasterCard and Visa) [1.4 billion cards used worldwide, except USA]
- new German identity card
- passports (MRTD - machine readable travel documents),
- new German health card
- signature cards





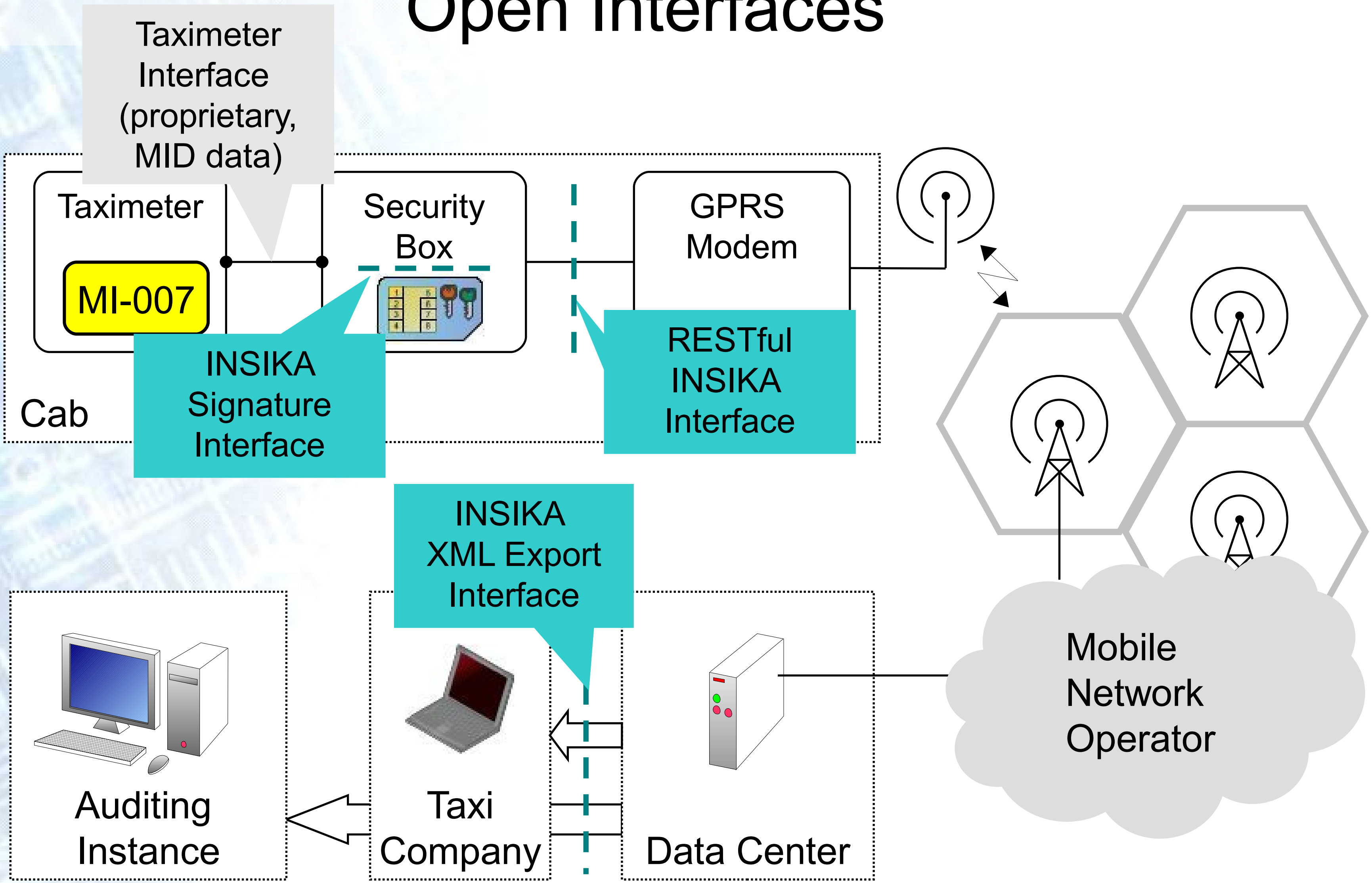
new German identity card

new German health card

electronic passport

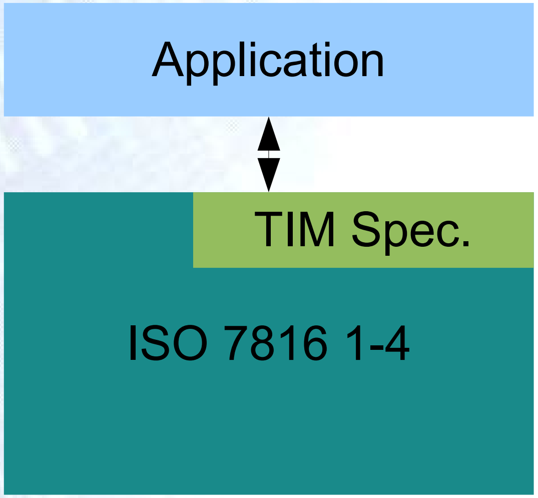
Images: Giesecke & Devrient, Gematik, Federal Ministry of the Interior of Germany

# INSIKA Solution: Open Interfaces

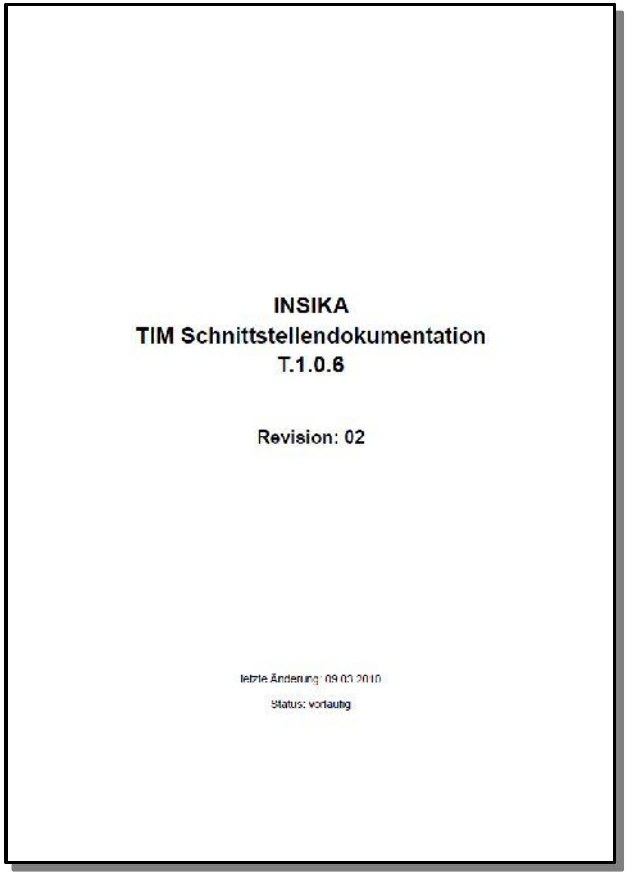


open interfaces, based on standards, independent from manufacturers, freely available (http://insika.de/)

# Open Interfaces:
# INSIKA Signature Interface



- ISO/IEC 7816 1-4 standard for smart cards
- defines physical layer up to application layer
- TIM interface adds 4 commands on application level
- master-slave, “T=1” protocol



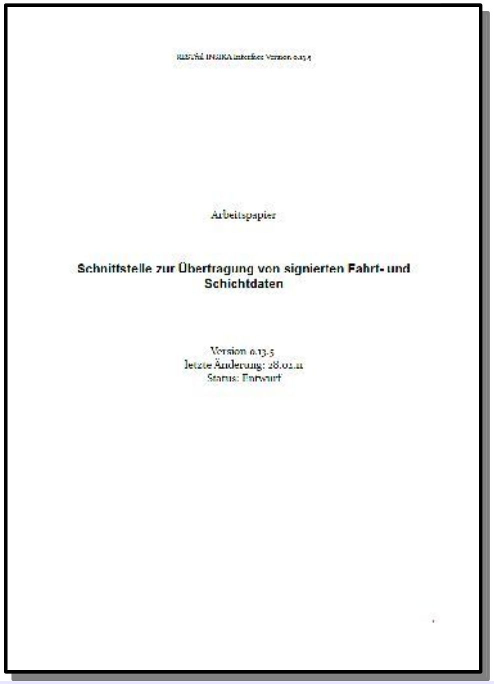
**INSIKA**
**TIM Schnittstellendokumentation**
**T.1.0.6**

**Revision: 02**

letzte Änderung: 09.03.2010
Status: vorläufig

# Open Interfaces:
# RESTful INSIKA Interface

- open interface - allows change of data center
- REST = Representational State Transfer
- simple webservice
- HTTP/HTTPS protocol and clearly defined methods, URIs and status codes
- transfer of XML messages in body:



RESTful INSIKA interface Version 0.13.5

Arbeitspapier

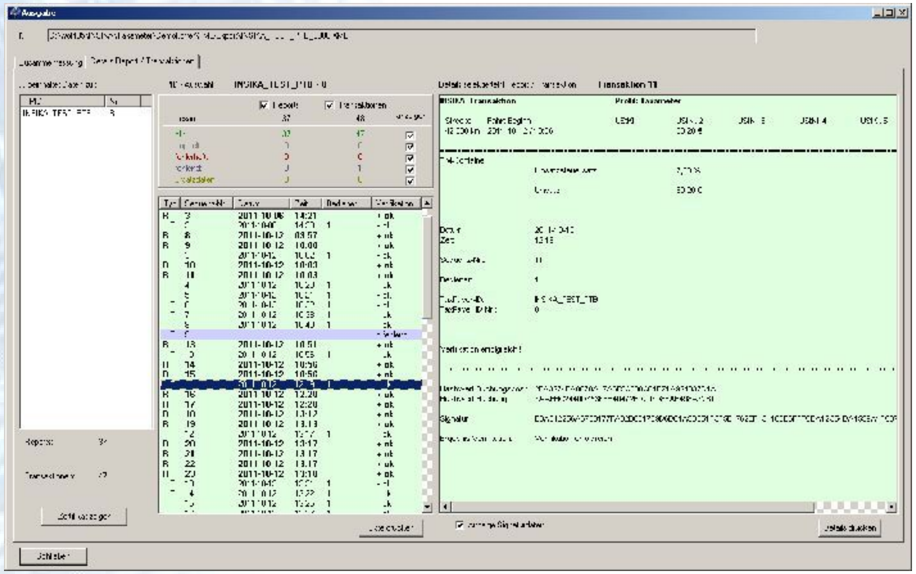
**Schnittstelle zur Übertragung von signierten Fahrt- und Schichtdaten**

Version 0.13.5
letzte Änderung: 28.02.11
Status: Entwurf

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<insika xmlns="http://insika.de/msg">
    <transactionEncoded>
        <itemListEncoded profile="taxi">sAEAsgIBDL0EIBEQBr4CFBE=
        </itemListEncoded>
        <transactionRequest>zQQgERAGzgIUE8YFNDAwMDHHFO/o11PEPlnlHT
        6ucNs2z1rch0niyAID0uIL2AIBDNoBHNsCBwA=</transactionRequest>
        <transactionResponse>xA9JTlNJS0FfVEVTVF9QVELFAQjLAQGeMF9EuXi
        SieiyGr44FMEzW7q7X2Cf78CD64x6Ovcoa6evwWFC5hSqmLKebj95d8+28g==
        </transactionResponse>
    </transactionEncoded>
</insika>
```

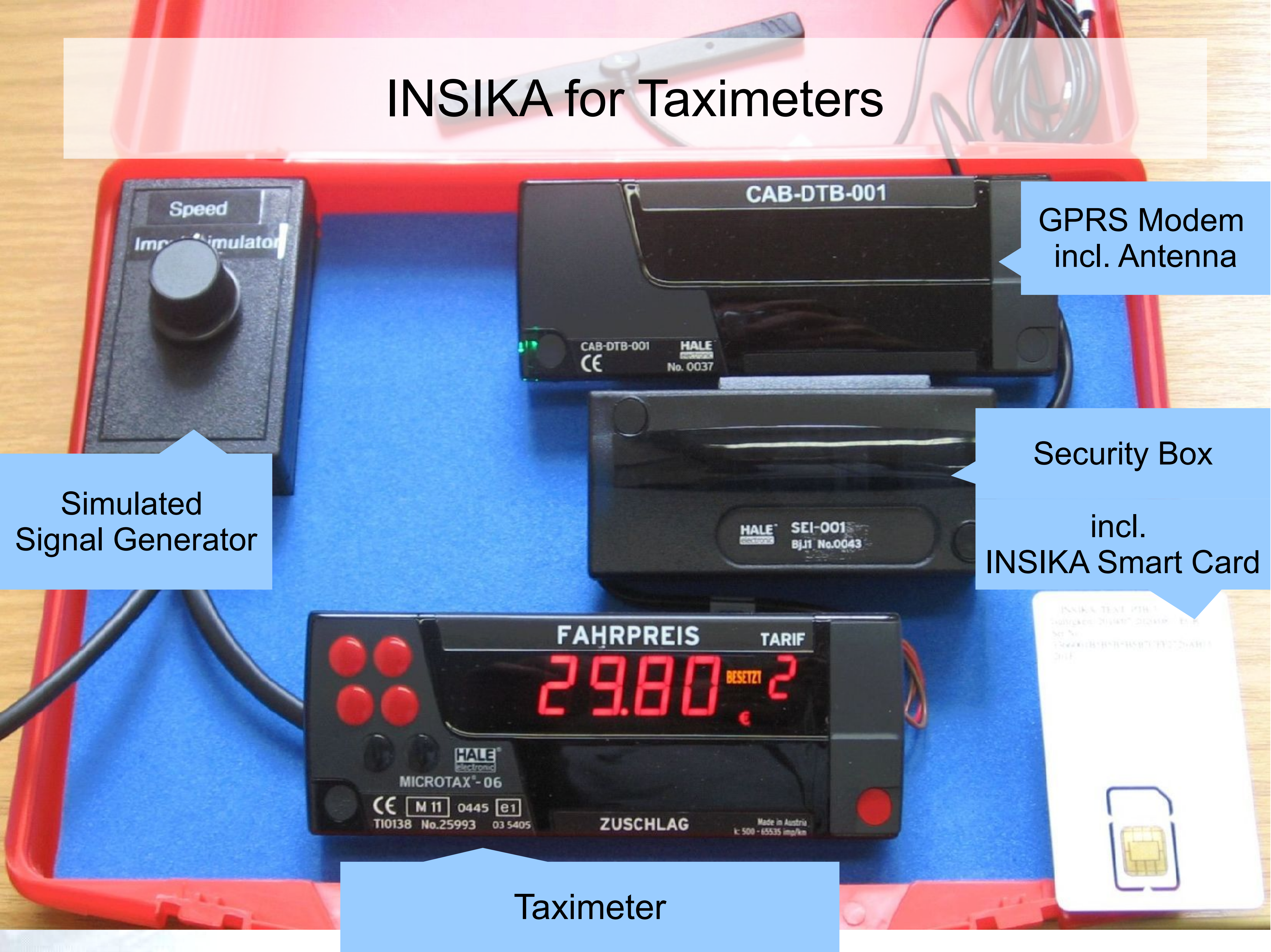
# Open Interfaces:
# XML Export Interface

- XML export contains signed taximeter data: smart card certificate, trips, shifts
- can be verified by INSIKA Verification Module (IVM) or any other tool



```
<?xml version="1.0" encoding="iso-8859-1"?><insika
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://insika.de/export"
xsi:schemaLocation="http://insika.de/export
insikaB64.xsd"><timParams><timVersion>T.1.1.0</timVersi
on><tpId>INSIKA_TEST_PTB</tpId><tpIdNo>8</tpIdNo><certi
ficate>MIIB46ADAgECAgMLOywwDQYJKoZIhvcNAQEFBQAwgYQxCzAJ
BgNVBAYTAkRFMS4wLAYDVQQKDCVQaHlzaWthbGlzY2gtVGVjaG5pc2N
oZSBCdW5kZXNhbnN0YWx0MSswKQYDVQQLDCJEYXRlbmtvbW11bmlrYX
Rpb24gdW5kIC1zaWNoZXJoZW10MRgwFgYDVQQDDA9QVEIgQ0EgMiAzM
DMwXzEwHhcNMTExMDEwMTM0NjAyWhcNMTYxMDMxMTM0NjAyWjA3MQsw
CQYDVQQGEwJERTEMMAoGA1UECgwDUFRCMRowGAYDVQQDDBFJTlNJS0F
fVEVTVF9QVEItODBJMBMGByqGSM49AgEGCCqGSM49AwEBAzIABM6Yrq
Sno6j8tQGPc8JhZcORu3zQDixjwK77yIMyTYJJb2iwlM9RCRBbeW2VF
MLxNaOBnDCBmTCBhgYDVR0fBH8wfTB7oHmgd4ZGbGRhcDovL2xkYXAu
aW5zaWthLmRlOjM4OS9jbj1JTlNJS0EtQ1JMLCBvPUNSTCBEaXN0cml
idXRpb24sIGRjPUlOU0lLQYYtaHR0cDovL2xkYXAuaW5zaWthLmRlL2
NybGRvd25sb2Fkcy9JTlNJS0EuY3JsMA4GA1UdDwEBAAQEAwIAgA==<
/certificate></timParams><reportEncoded><itemListEncode
d
profile="taxi">oAExoQU0MDAwMaUCSQymAkhEpwENqAIVDKkDA1YM
rQQgEQkprgISUw==</itemListEncoded><reportRequest>zQQgER
AGzgIUE9QUimm3DieANEBn9tqpb/1c+VIlrHw=</reportRequest><
reportResponse>wAEDxA9JTlNJS0FfVEVTVF9QVELFAQjMAQLSAQHT
AQHiC9gCAQzZAQzbAgcAnjCa9icVrnHulwqNetsc+AJjWJh/cYElvUf
PruBfRy0VfyF2lRlNGGeGznHD+TF+dnw=</reportResponse></rep
ortEncoded><transactionEncoded><itemListEncoded
profile="taxi">sAEAsgIBDL0EIBEQBr4CFBE=</itemListEncode
d><transactionRequest>zQQgERAGzgIUE8YFNDAwMDHHFO/o11PEP
lnlHT6ucNs2z1rch0niyAID0uIL2AIBDNoBHNsCBwA=</transactio
nRequest><transactionResponse>xA9JTlNJS0FfVEVTVF9QVELFA
QjLAQGeMF9EuXiSIeiyGr44FMEzW7q7X2Cf78CD64x6Ovcoa6evwWFC
5hSqmLKebj95d8+28g==</transactionResponse>w=</itemListE
ncoded><reportRequest>zQQgEREhzgIUINQU7r2QLRq10wGVPnr3y
TAyQOhNdQ8=</reportRequest><reportResponse>wAEDxA9JTlNJ
S0FfVEVTVF9QVELFAQjMASnSAQHTASTiDdgEARZ0DNkBDNsCBwCeMDB
3BvzmFXjwEcCpDmV6o3dN5BrIUVCN+zemdolTaYyaFU2a7loni5L1Ad
1j0VbpSg==</reportResponse></reportEncoded></insika>
```

# INSIKA for Taximeters



GPRS Modem incl. Antenna

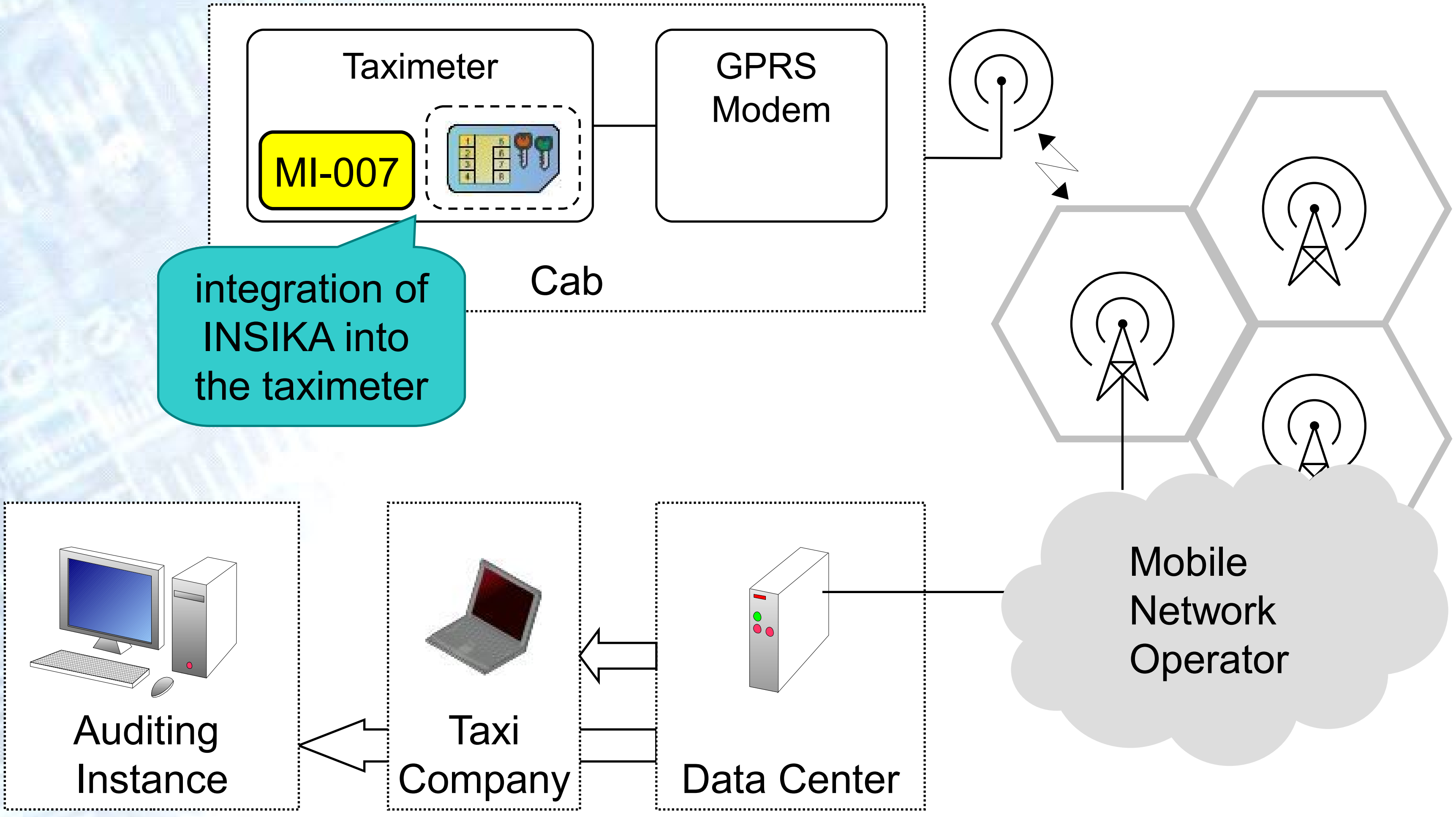
Simulated Signal Generator

Security Box

incl. INSIKA Smart Card

Taximeter

# Outlook



Taximeter

MI-007

GPRS Modem

integration of INSIKA into the taximeter

Cab

Mobile Network Operator

Auditing Instance

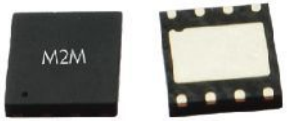
Taxi Company

Data Center

# Outlook

potential technical influences:

- upcoming: ETSI standard for embedded SIM (eUICC)
- other wireless technologies (LTE, taxi radio,..)
- other protocols (FTP, MQTT, IPv6,.. )
- other secure elements: ( eUICC/UICC with integrated application,.. )
- usage of time stamp services
- new developments in M2M market



Images: Oberthur Technologies

# Thank You!

The work of the INSIKA Project has been funded by the German Federal Ministry of Economics and Technology under the grant MNPQ 11/07.

For further information please contact insika@ptb.de
or visit: http://www.insika.de/

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages