Informationsveranstaltung „Manipulationsgeschütztes System zur Aufzeichnung von Daten des Taxengewerbes“ 27.10.2010, TVB Berlin

Übersicht der Systemschnittstellen INSIKA-Taxi

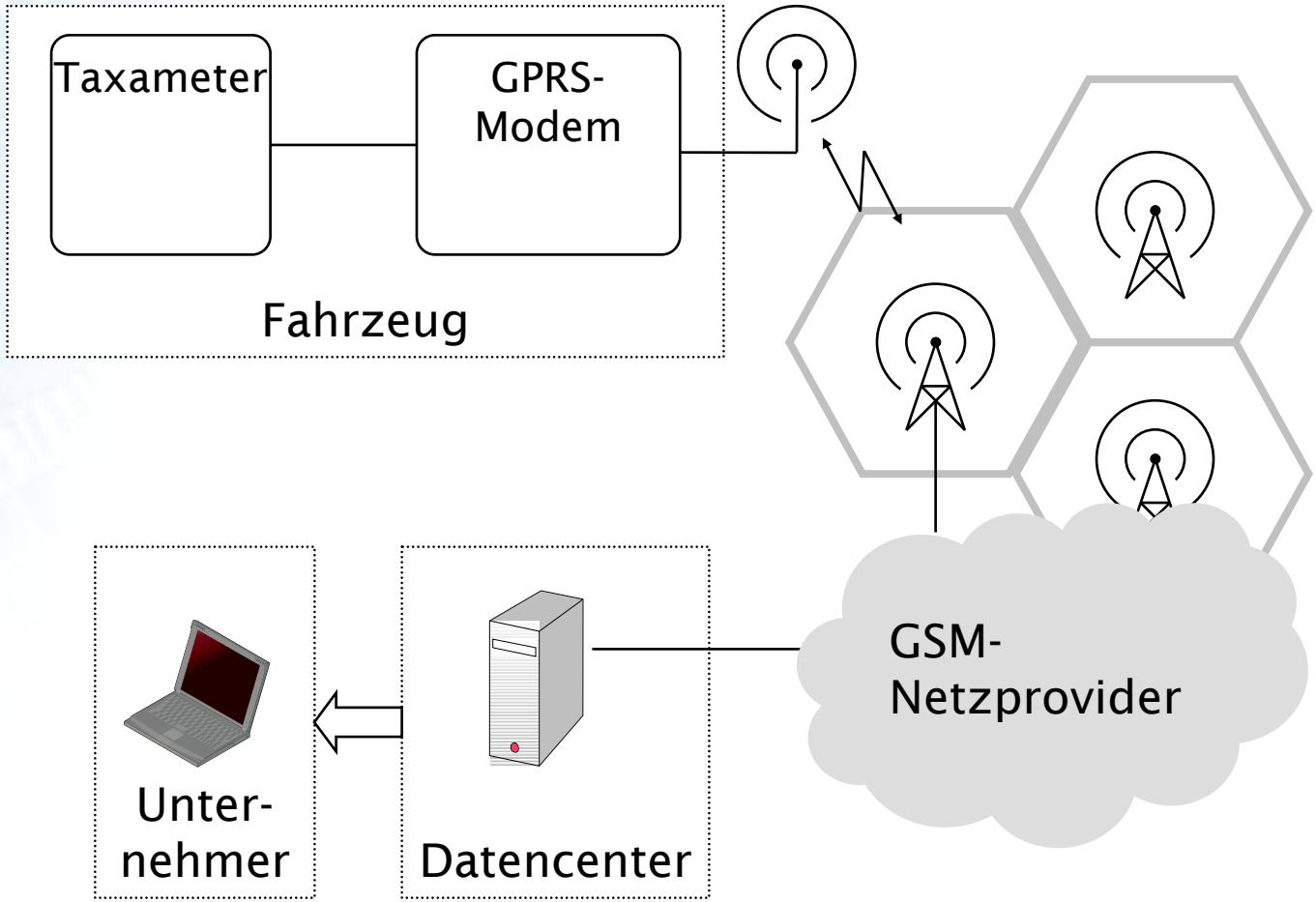
Jörg Wolff
Physikalisch-Technische Bundesanstalt (PTB)
FB 8.5 Metrologische Informationstechnik
joerg.wolff@ptb.de

Bild: Taxameter um 1960, www.ptb.de

Überblick

- Systemkonzept und digitale Signatur
- Schnittstellen des Systems
- Signierte Daten für Fahrten und Schichten

Systemkonzept (I): ungesicherte GPRS-Datenübertragung



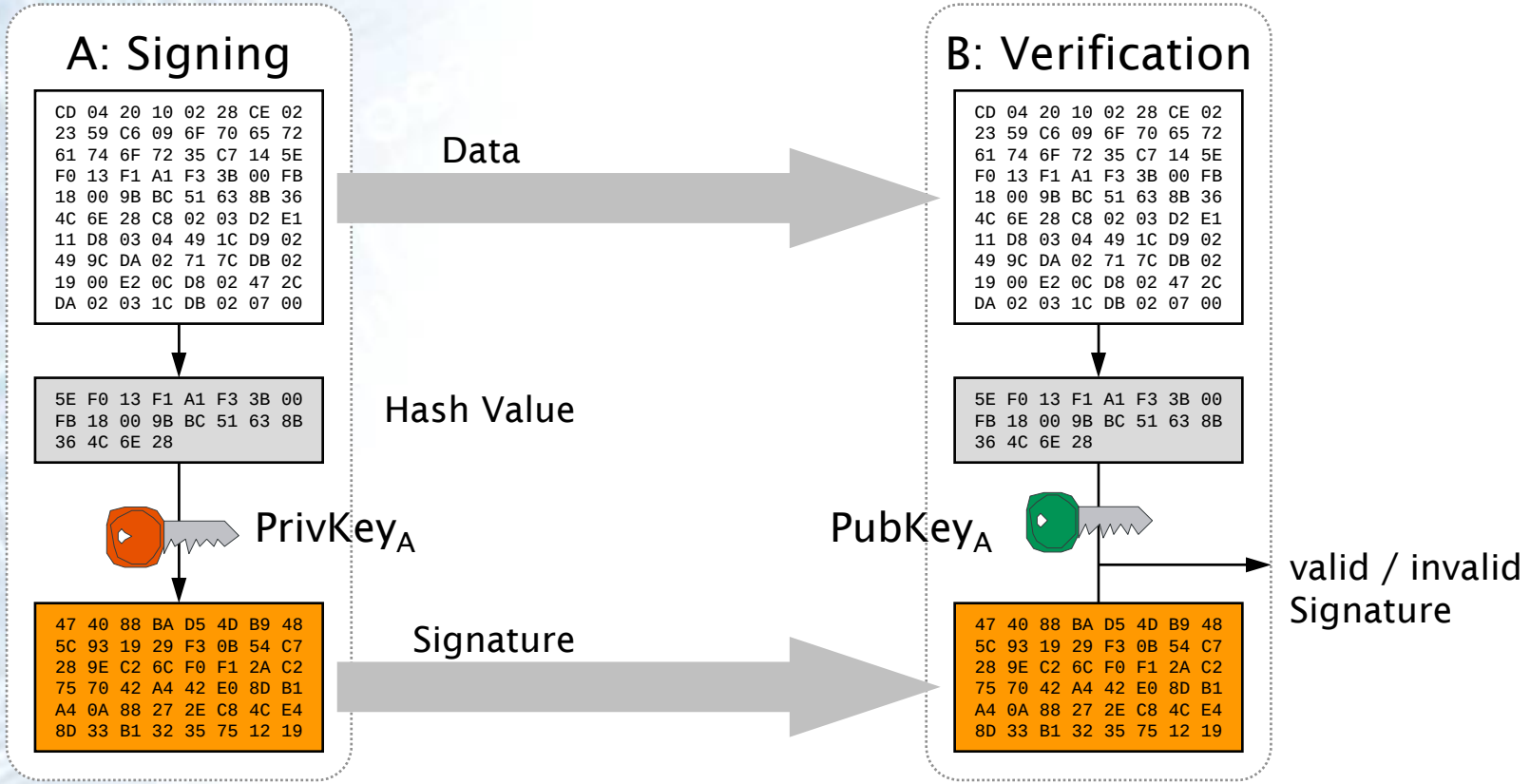
Schutzziele für Taxameterdaten

- **Integrität**: Schutz der Daten vor Modifikation
  → Anwendung von **Hash-Funktionen** (Einwegfunktionen)
  Secure Hash Algorithm (SHA-1)

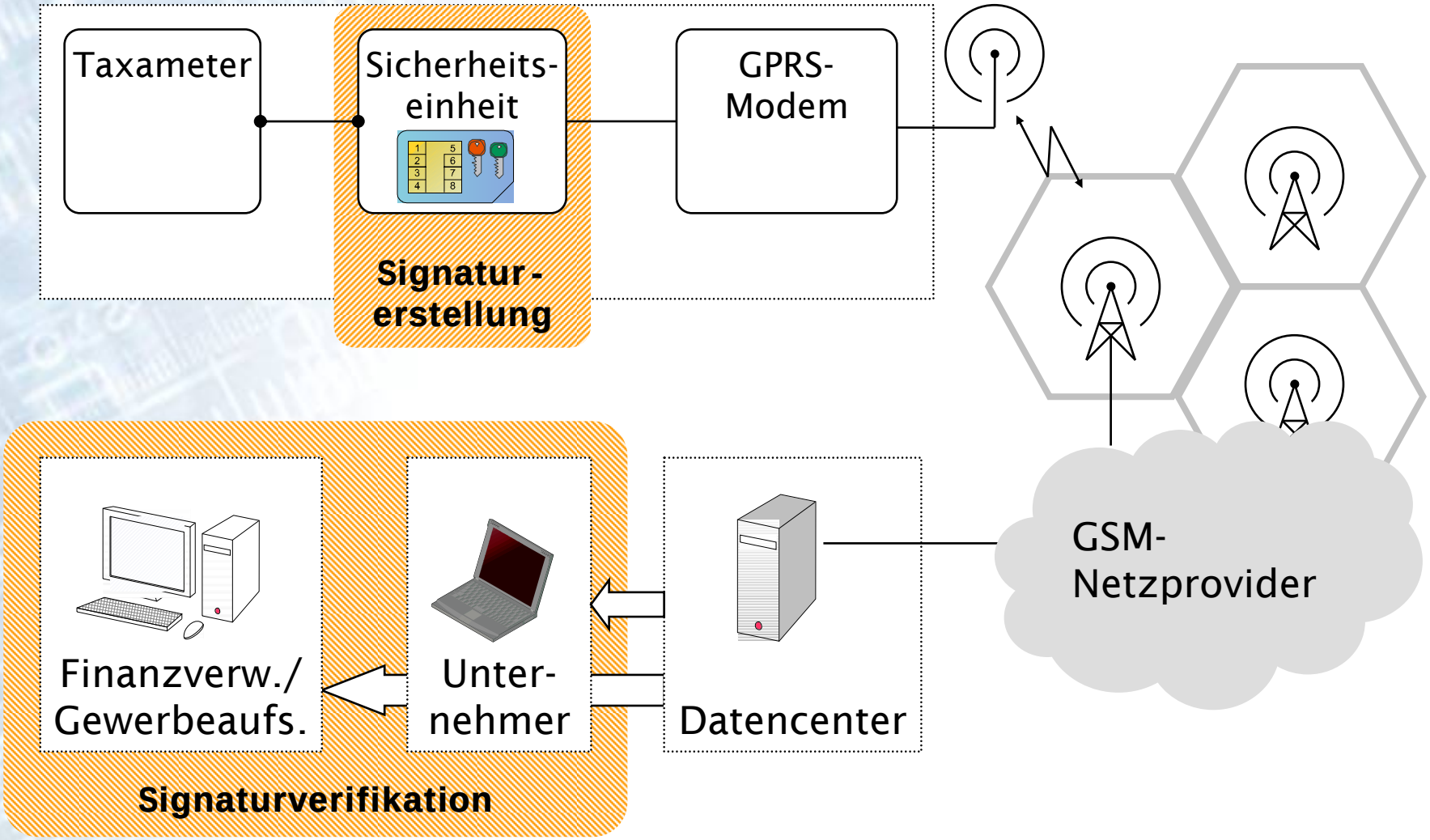
- **Authentizität**: Nachweis der Urheberschaft
  → Anwendung **asymmetrischer Kryptografie,** speziell **Signaturverfahren**
  Elliptic Curve Digital Signature Algorithm (ECDSA), 192 bit

→ Sicherheit durch Verwendung von bewährten, offenen und standardisierten kryptografischen Verfahren

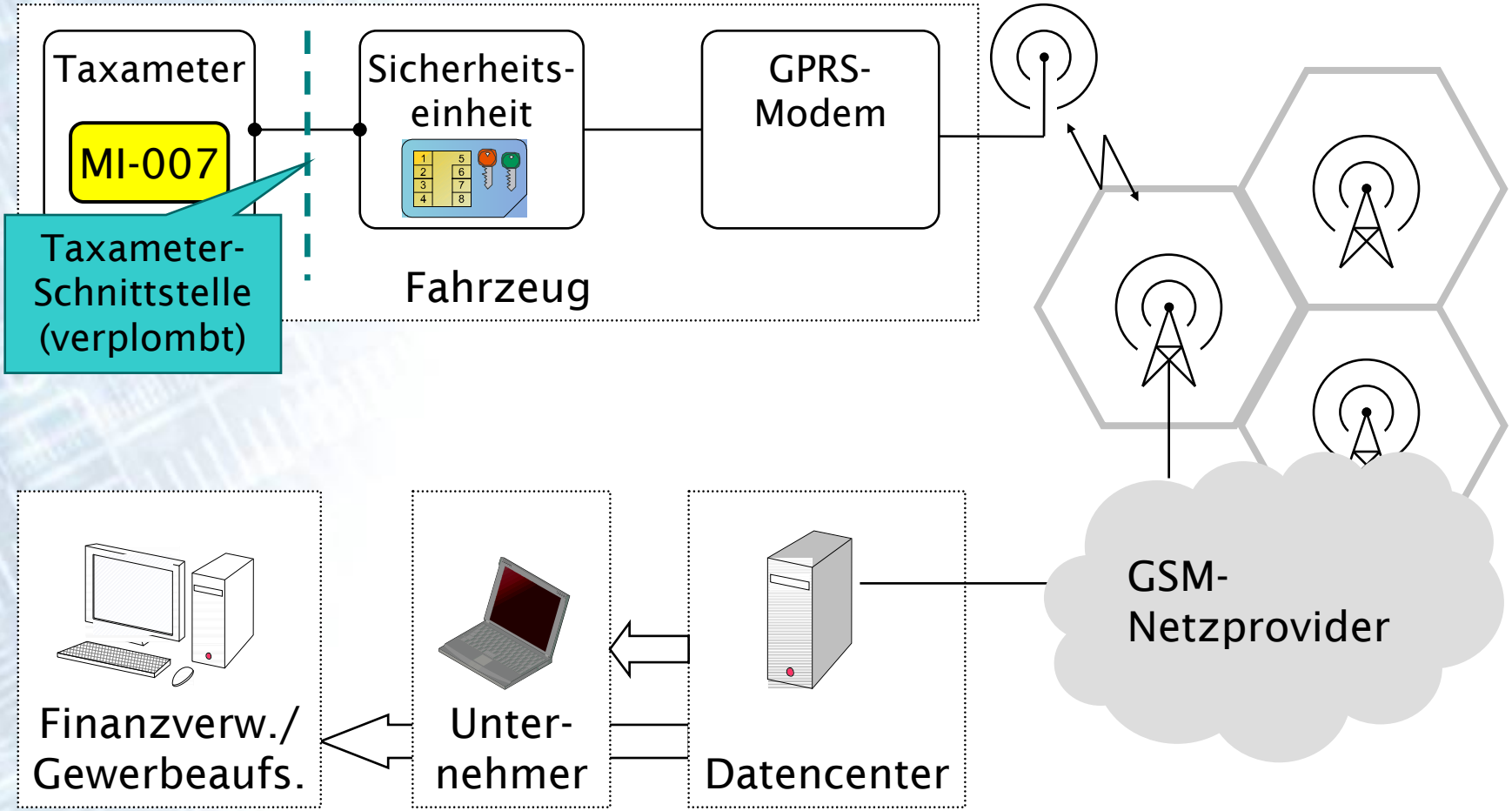
INSIKA-Basis: Digitale Signatur



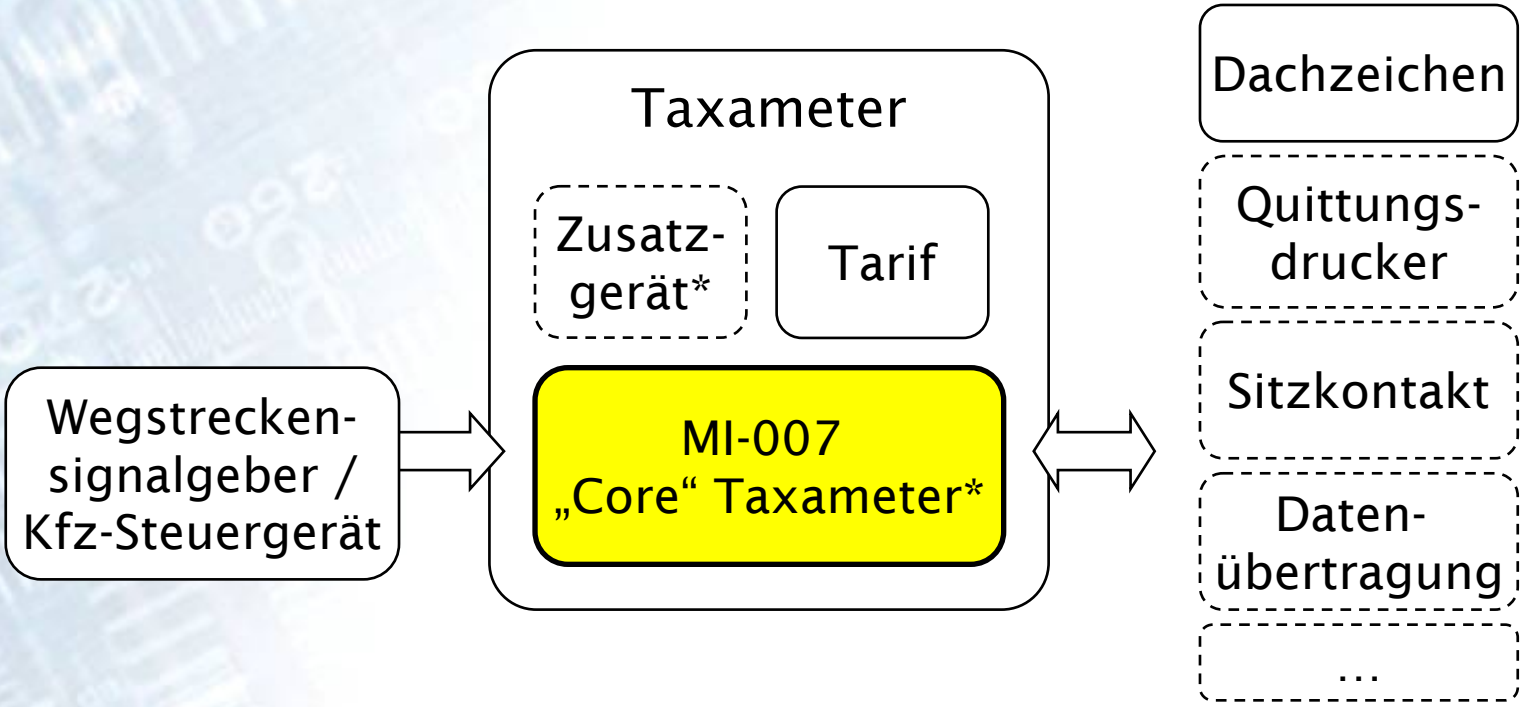
Systemkonzept (II): GPRS-Datenübertragung + INSIKA



Schnittstelle I_t – Taxameter



Taxameter im Fahrzeugumfeld



* MID 2004/22/EG inkl. Anhang MI-007

Vorschriften und Normen für Taxameter

- **MID (2004/22/EG) mit Anhang MI-007 für elektronische Taxameter**
- WELMEC
- OIML R 21 (2007) Taximeters
- CENELEC EN 50148
- CAN CiA 447-3
- National:
  - Eichordnung 18-2
  - PTB-A 18.21 Quittungsdrucker für Taxameter
  - Eichgesetz, PBefG, BOKraft
- …

(Hale electronic GmbH / Kienzle Argo Taxi International GmbH)

Taxameterdaten,
MID Anhang MI-007, Punkt 4:

4. Ein Taxameter muss über eine (oder mehrere) **geeignete gesicherte Schnittstelle(n)** folgende Daten übertragen können:

– **Betriebseinstellung**: "FREI", "BESETZT" oder "KASSE";

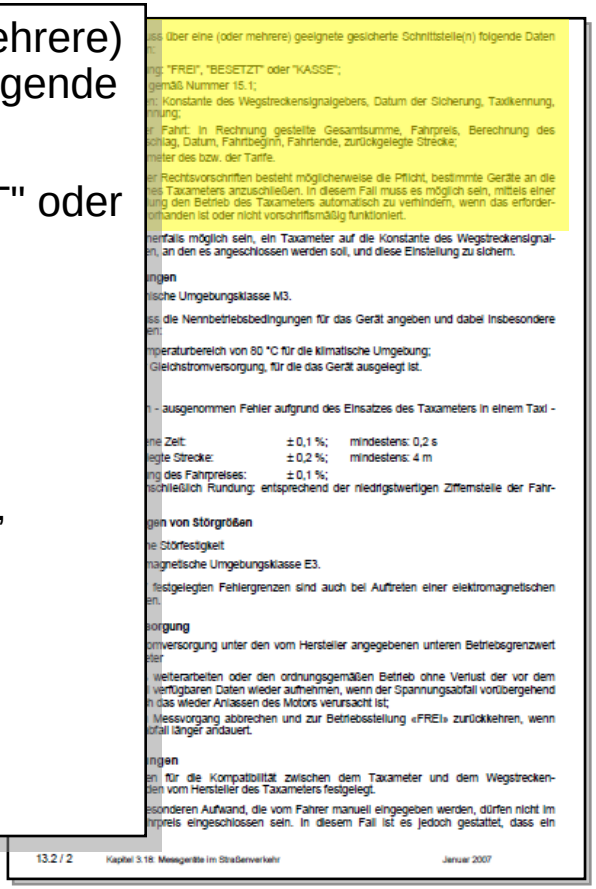
– **Zählwerksdaten** gemäß Nummer 15.1;

– **allgemeine Daten**: (..)

– **Preisdaten einer Fahrt**:
in Rechnung gestellte Gesamtsumme, Fahrpreis, Berechnung des Fahrpreises, Zuschlag, Datum, Fahrtbeginn, Fahrtende, zurückgelegte Strecke;

– **Tarifdaten**: (..)

…


über eine (oder mehrere) geeignete gesicherte Schnittstelle(n) folgende Daten

"FREI", "BESETZT" oder "KASSE";

gemäß Nummer 15.1;

Konstante des Wegstreckensignalgebers, Datum der Sicherung, Taxikennung,

Fahrt: In Rechnung gestellte Gesamtsumme, Fahrpreis, Berechnung des schlag, Datum, Fahrtbeginn, Fahrtende, zurückgelegte Strecke;

ter des bzw. der Tarife.

Rechtsvorschriften besteht möglicherweise die Pflicht, bestimmte Geräte an die es Taxameters anzuschließen. In diesem Fall muss es möglich sein, mittels einer ung den Betrieb des Taxameters automatisch zu verhindern, wenn das erforder- handen ist oder nicht vorschriftsmäßig funktioniert.

nfalls möglich sein, ein Taxameter auf die Konstante des Wegstreckensignal- n, an den es angeschlossen werden soll, und diese Einstellung zu sichern.

ngen

sche Umgebungsklasse M3.

die Nennbetriebsbedingungen für das Gerät angeben und dabei insbesondere en:

peraturbereich von 80 °C für die klimatische Umgebung;

Gleichstromversorgung, für die das Gerät ausgelegt ist.

- ausgenommen Fehler aufgrund des Einsatzes des Taxameters in einem Taxi -

ne Zeit: ± 0,1 %; mindestens: 0,2 s

egte Strecke: ± 0,2 %; mindestens: 4 m

ng des Fahrpreises: ± 0,1 %;

schließlich Rundung: entsprechend der niedrigstwertigen Ziffernstelle der Fahr-

gen von Störgrößen

e Störfestigkeit

agnetische Umgebungsklasse E3.

festgelegten Fehlergrenzen sind auch bei Auftreten einer elektromagnetischen en.

orgung

rversorgung unter den vom Hersteller angegebenen unteren Betriebsgrenzwert er

weiterarbeiten oder den ordnungsgemäßen Betrieb ohne Verlust der vor dem verfügbaren Daten wieder aufnehmen, wenn der Spannungsabfall vorübergehend n das wieder Anlassen des Motors verursacht ist;

Messvorgang abbrechen und zur Betriebsstellung «FREI» zurückkehren, wenn bfall länger andauert.

ngen

n für die Kompatibilität zwischen dem Taxameter und dem Wegstrecken- den vom Hersteller des Taxameters festgelegt.

sonderen Aufwand, die vom Fahrer manuell eingegeben werden, dürfen nicht im rpreis eingeschlossen sein. In diesem Fall ist es jedoch gestattet, dass ein

13.2 / 2 Kapitel 3.18: Messgeräte im Straßenverkehr Januar 2007

→ keine Vorgaben in Bezug auf Schnittstelle oder Datenformat

Abbildung von Taxameterdaten, Signierte Datenobjekte

Präfix „TAXI“: INSIKA Profil Taxameter
Präfix „ITEM“: INSIKA Profil Registrierkasse
…

Name	ag	Beschreibung	
TAXI_...			
TAXI_...			
…			
TIM_...			
TIM_...			
…			

Präfix „TIM“: INSIKA TIM

→ Abbildung anwendungsspezifischer Daten durch das Konzept der Profile

→ Datenobjekte anhand Präfix eindeutig unterscheidbar

Signierte Daten einer Fahrt (I): Profil Taxameter

Name	Tag	Beschreibung	ggfs. nicht übertr.
TAXI_TRIP_DIST	B0h	**Zurückgelegte Strecke** einer Fahrt in m	
TAXI_TRIP_CHARGED_1 … TAXI_TRIP_CHARGED_6	B1h .. B6h	**Gesamtsumme 1..6** (Fahrpreis + Zuschläge) einer Fahrt je Umsatzsteuerklasse 1..6	
TAXI_TRIP_DATE_START	BDh	**Datum Fahrtbeginn**	
TAXI_TRIP_TIME_START	BEh	**Uhrzeit Fahrtbeginn**	

Signierte Daten einer Fahrt (II): TIM Daten

Name	Tag	Beschreibung	ggfs. nicht übertr.
TIM_DATE	CDh	aktuelles **Datum**	
TIM_TIME	CEh	aktuelle **Uhrzeit**	
TIM_OPERATOR	C6h	hier **Fahrer(-nummer)**	
TIM_HASH_TRANSACTION_ ITEMS	C7h	**Hashwert** über Profildaten	
TIM_CURRENCY	C8h	**Währungscode**	
TIM_CONTAINER_VAT_1	E1h	falls **Pauschalfahrt**	x
TIM_TURNOVER	D8h	Gesamtsumme VAT 1	x
TIM_TURNOVER_VAT	DAh	USt VAT 1	x
TIM_TURNOVER_VAT_RATE	DBh	UStS VAT 1	x
TIM_CONTAINER_VAT_2	E2h	falls **Tariffahrt**	x
TIM_TURNOVER	D8h	Gesamtsumme VAT 2	x
TIM_TURNOVER_VAT	DAh	USt VAT 2	x
TIM_TURNOVER_VAT_RATE	DBh	UStS VAT 2	x

Signierte Daten einer Schicht (I): Profil Taxameter

Name	Tag	Beschreibung	ggfs. nicht übertr.
TAXI_VEHICLE_ID	A0h	**Fahrzeugidentifikation** (Taxikennung)	
TAXI_OPERATOR	A1h	**Fahrernummer**	
TAXI_TOT_DIST	A5h	**Gesamte Wegstrecke** in m	
TAXI_TOT_DIST_HIRED	A6h	**Gesamte Wegstrecke** in Betriebseinstellung "**Besetzt**" in m	
TAXI_TOT_HIRINGS_NO	A7h	**Gesamtzahl Touren**	
TAXI_TOT_SUPPLEMENTS	A8h	**Gesamtsumme Zuschläge** in Euro-Cent	
TAXI_TOT_FARE	A9h	**Gesamtsumme Fahrpreis** in Euro-Cent	
TAXI_SHIFT_DATE_START	ADh	**Datum Schichtanmeldung**	x
TAXI_SHIFT_TIME_START	AEh	**Uhrzeit Schichtanmeldung**	x

Signierte Daten einer Schicht (II): TIM Daten

Name	Tag	Beschreibung	ggfs. nicht übertr.
TIM_DATE	A0h	aktuelles **Datum**	
TIM_TIME	A1h	aktuelle **Uhrzeit**	
TIM_HASH_REPORT_ITEMS	A5h	**Hashwert** über o.g. Profildaten	

INSIKA Datenkodierung (I)

Zurückgelegte Strecke (m)	10500
Beginn (Datum, Zeit)	2010-01-25, 17-12
Ende (Datum, Zeit)	2010-01-25, 17-53
Gesamtsumme 2 (EUR-Cent, brutto, 7% UStS)	10 70
Besetzkilometer, gesamt (m)	132 055 120
…	

Abbildung in Form von „TLV-Objekten“

Tag	Length	Value
D8h	02h	56h 40h
…	…	…

ASN.1-BER
Abstract Syntax Notation One – Basic Encoding Rules
(ITU-T Rec. X.680 ff.)

INSIKA Datenkodierung (II)

Zurückgelegte Strecke (m)	10500
Beginn (Datum, Zeit)	2010-01-25, 17-12
Ende (Datum, Zeit)	2010-01-25, 17-53
Gesamtsumme 2 (EUR-Cent, brutto, 7% USt$)	10 70
Besetzkilometer, gesamt (m)	132 055 120
…	

Abbildung in Form von „TLV-Objekten“

```
CDh 08h 32h 30h 30h 39h 30h 31h 32h 31h CEh 06h 31h 31h 31h 37h
30h 39h C4h 10h 54h 61h 78h 5Fh 50h 61h 79h 65h 72h 5Fh 49h 44h
5Fh 5Fh 5Fh 5Fh C5h 04h 00h 00h 00h 14h C6h 01h 30h C7h 14h D0h
E4h EAh 7Eh B8h CDh 87h 75h 34h E3h 04h F6h 5Dh 8Fh 1Ch FBh C9h
D7h D2h 60h CBh 04h 00h 00h 01h 84h
```

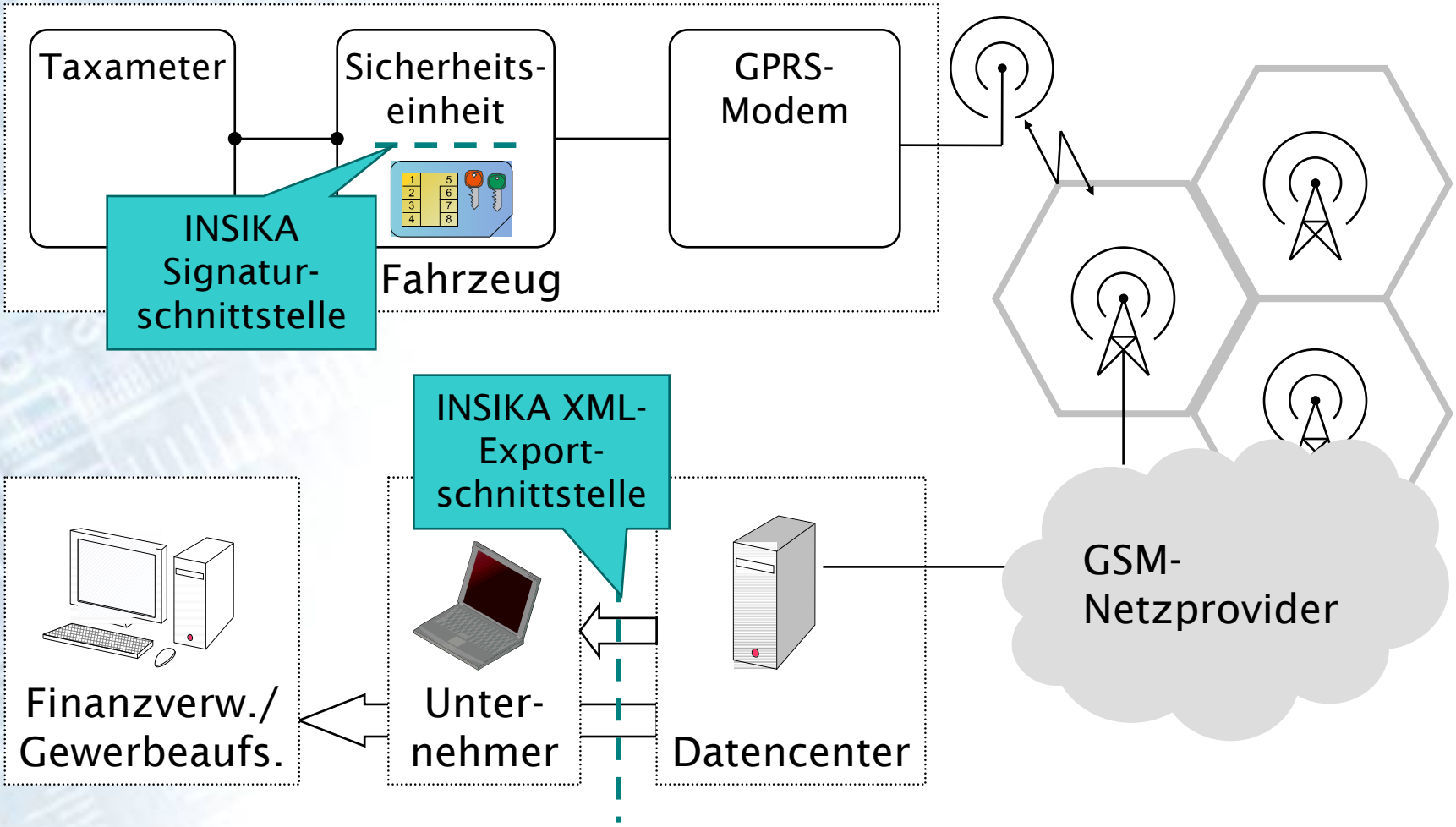
Hashwert

```
00h 01h 02h 03h 04h 05h 06h 07h 08h 09h 0Ah 0Bh 0Ch 0Dh 0Fh 10h
11h 12h 13h 14h
```

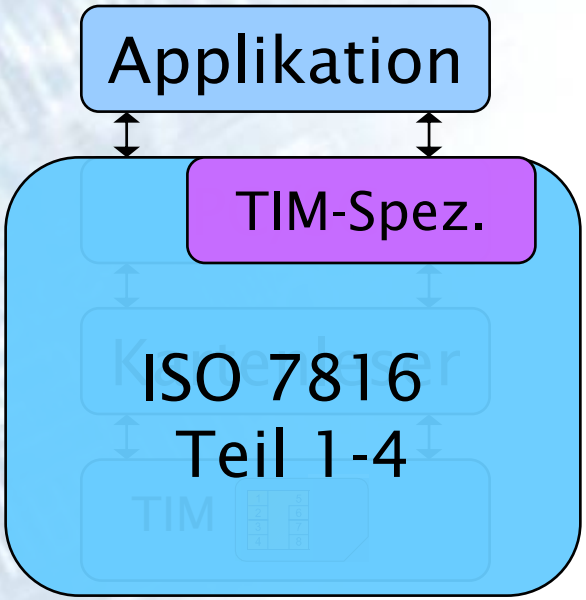
Signatur

```
C2h 44h D7h FAh E7h E8h F9h 41h 98h 72h A2h B0h A1h 1Bh 02h DFh
2Fh 1Ch DDh 0Bh B1h 68h D8h 7Ah 95h 3Ah 7Bh 04h C8h 24h F5h FDh
B1h 87h 19h 32h 55h 13h 8Ch 0Dh 65h F2h 82h 4Bh 10h 39h D2h 02h
```

Schnittstellen I_s & I_e – INSIKA Signatur & Export



I_S: INSIKA TIM-Signaturschnittstelle

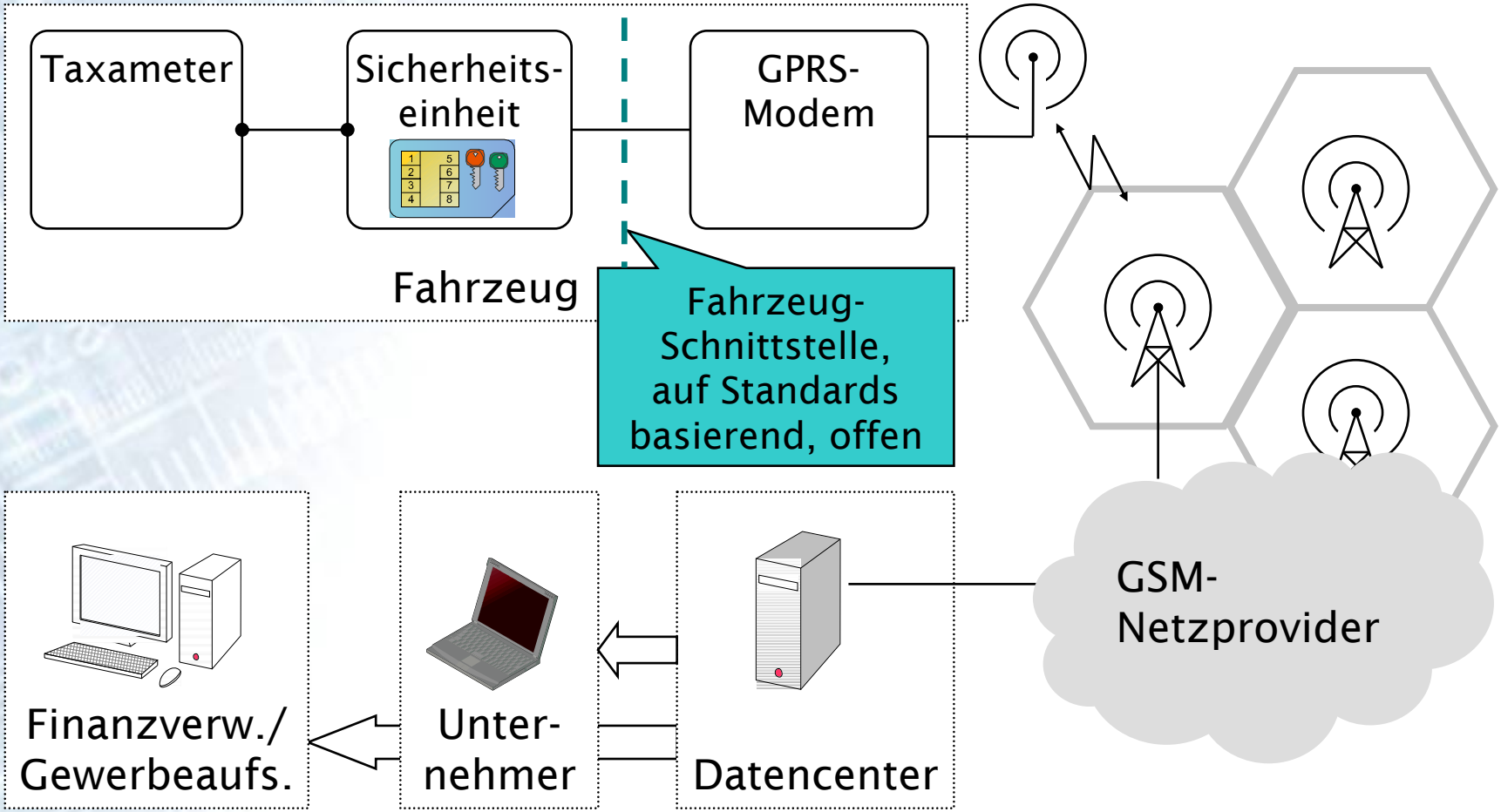


- Physikalische Schicht bis Applikationsschicht durch die ISO 7816 Teil 1-4 standardisiert
- Erweiterung um 4 TIM-Befehle auf Applikationsebene
- Master-Slave Prinzip
- Standard „T=1“ Protokoll
- große Auswahl an verfügbaren Schnittstellenkomponenten (auch mit integriertem Protokollstack)
- PC/SC-Protokollstack im Betriebssystem integriert (ab WinXP) bzw. frei verfügbar (Linux, BSD, etc)

I_e: INSIKA XML-Exportschnittstelle

- XML = Extensible Markup Language: W3C Recommendation
- INSIKA XML-Exportschnittstelle: einheitlich, herstellerunabhängig
- enthält alle Daten zur Signaturverifikation
- unabhängig von Ort, Plattform und Medium (Webservice, USB-Stick, CD-Rom, Speicherkarten, etc.)

Schnittstelle I_c – Fahrzeug

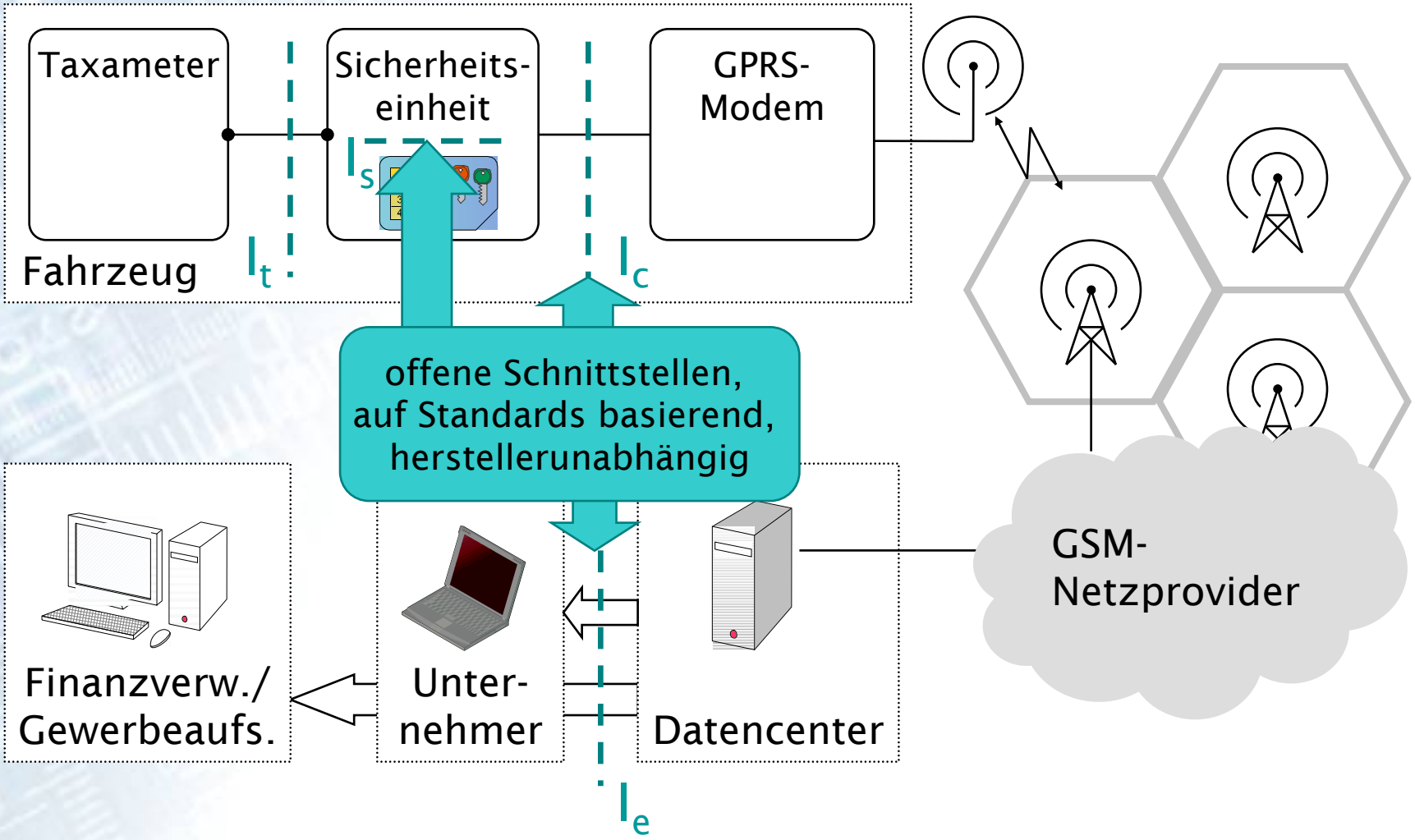


I_c : Fahrzeugschnittstelle, „RESTful Taxi Interface“

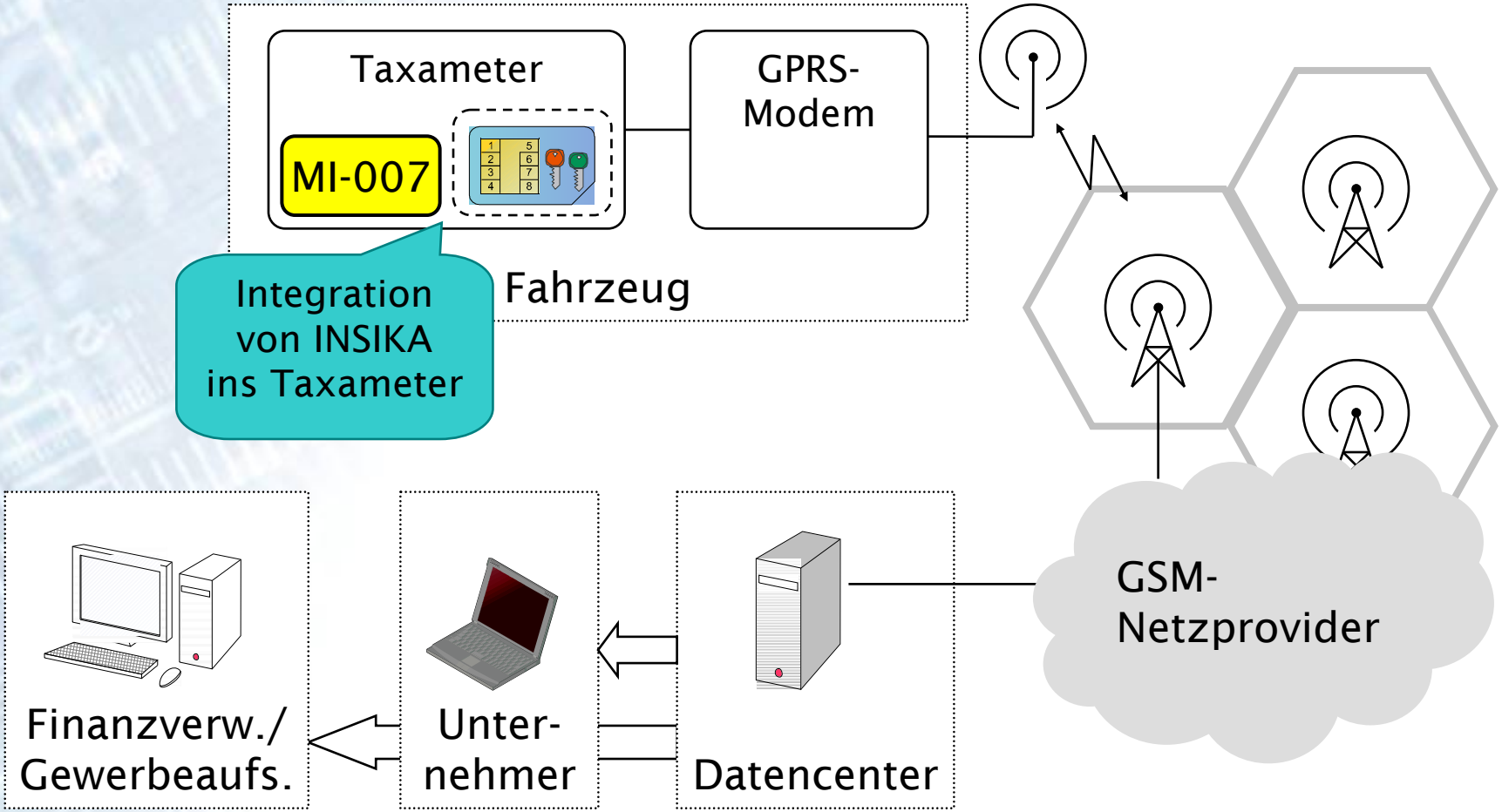
- REST = Representational State Transfer, (Sammlung von Architekturprinzipien)
- einfacher Webservice
- hier: HTTP Protokoll mit fest definierten Methoden, URIs und Fehlercodes
- Übertragung von XML-Nachrichten, Bsp.:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<insika xmlns="http://insika.de/msg">
    <transactionEncoded>
        <itemListEncoded>sAIpBLIDAQcMvQQgEAYpvgIVAA==</itemListEncoded>
        <transactionRequest>zQQgEAYpzgIVMMYCMTLHFNo5o+5ea0sNMlW/75VgGJ
        Cv2AcJyAID0uIN2AMBBwzaAgcM2wIHAA==</transactionRequest>
        <transactionResponse>xA9JTlNJS0FfVEVTVF9QVELFAQLLAguqnjAN+rue2I
        8wFvWGvtiA+bOnUfOTQzNOGkAiB5T67
        go53VPoJR6QWbSNW2zqW2lsak8=</transactionResponse>
    </transactionEncoded>
</insika>
```

Systemkonzept, Zusammenfassung



Ausblick:
Zielkonzept (langfristig)



Kosmos Taxameter, Berlin um 1900, www.ptb.de

Vielen Dank für Ihre Aufmerksamkeit!

http://www.insika.de
eMail: insika@ptb.de