Schutz von Buchungsdaten gegen unzulässige Veränderungen
-
Erfahrungen bei der praktischen Umsetzung des INSIKA-Konzepts

Norbert Zisky, Jörg Wolff
Physikalisch-Technische Bundesanstalt

ADASYS Solution Day
Kornwestheim 19.11.2010

Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin

Dr. Norbert Zisky

Leiter der Arbeitsgruppe „Datenübertragung und -sicherheit“

Aktuelle Projekte

- INSIKA
- INSIKA-Taxi
- On-Board Metering
- EMRP Smart Grid

1887- 2010

www.ptb.de

Übersicht

- Einleitung - Exkurs „Aktuelle Entwicklungen Kassenprüfung“
- INSIKA-Konzept - Überblick
- Betrieb und Prüfung
- INSIKA-Prototypen und Pilottests
- INSIKA-Demonstration
- Zusammenfassung und Ausblick

Aktuelle Situation

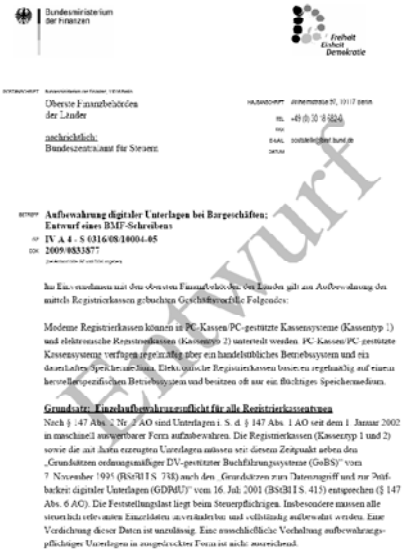
Finanzbehörden intensivieren Datenzugriff
auf Grundlage AO, GoBS, GdPDU

- Gesteigerte Aufmerksamkeit der Betriebsprüfer für Registrierkassen
- Datenzugriff wird immer häufiger verlangt
- Entwurf eines BMF-Schreibens „Aufbewahrung digitaler Unterlagen bei Bargeschäften“ vom 28.01.2010 sieht erhebliche Verschärfungen vor

Aktuelle Situation

Finanzbehörden intensivieren Date
auf Grundlage AO, GoBS, GdPDU

- Gesteigerte Aufmerksamkeit der Registrierkassen
- Datenzugriff wird immer häufige
- Entwurf eines BMF-Schreibens Unterlagen bei Bargeschäften“ v sieht erhebliche Verschärfungen


Bundesministerium der Finanzen

Oberste Finanzbehörden der Länder

Aufbewahrung digitaler Unterlagen bei Bargeschäften; Entwurf eines BMF-Schreibens

IV A 4 - S 0316/08/10004-05

2009/0833877

Entwurf

Verschärfung bei Prüfungen

Praxis: gestern ⇨ heute

- BMF-Schreiben 9. 01.1996 erlaubt Verzicht auf Journale
- Großzügige Anwendung des BMF-Schreibens
- Keine gründlichen Prüfungen
- Gesetzesinitiative für „Fiskalchip“ im Jahr 2008 sollte eindeutige Klarheit schaffen

- Finanzbehörden haben Thema im Fokus
- Anforderungen für Anwendung BMF-Schreiben von1996 werden strenger ausgelegt
- Immer strengere Prüfungen – besonders in „Risikobranchen“
- Es wird häufiger ein Datenzugriff nach GDPdU verlangt

Verschärfung bei Prüfungen

Praxis: Ausblick

- Endgültiges BMF-Schreiben auf Basis des Entwurf vom Januar 2010 noch in diesem Jahr erwartet
- Deutliche Verschärfungen sind wahrscheinlich
- Mittelfristig in den meisten Fällen vollständiges elektronisches Journal erforderlich
- Verwaltung will immer noch saubere Lösung in Form des „Fiskalchips“ – momentan ist diese politisch nichtdurchsetzbar

Schutzziele für Baraufzeichnungen

Sicherung sensibler Daten gegen
bewusste oder unbewusste Verfälschungen

- Vollständige, richtige, geordnete und zeitgerechte Aufzeichnung aller Buchungen
- Verfälschungen von Daten sollen sicher erkannt werden
- Überprüfbarkeit einmal gebuchter Daten auf Vollständigkeit und Richtigkeit durch zuständige Stellen

Entwicklung von INSIKA

2001	Hinweise auf unerlaubte Veränderungen in Kassenjournalen
2002	Länder fordern Fiskalspeicher
2003	Bundesrechungshof: Dringender Handlungsbedarf
2004	PTB/BMF-Konzept → Bildung Bund/Länder-AG Registrierkassen
2005	Empfehlung: Anwendung des PTB/BMF-Konzepts
2006	AG Registrierkassen erarbeitet Fachkonzept
2008	02/2008 Start INSIKA-Projekt
	06/2008 Gesetzentwurf; Aktionsbündnis gg. Schwarzarbeit
2010	Entwurf BMF-Schreiben „Aufbewahrung digitaler Unterlagen…“

Gefördertes MNPQ-Projekt des BMWi
(Messen, Normen, Prüfen, Qualitätssicherung)

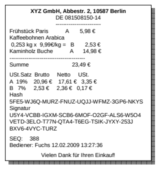
INSIKA-Projekt

- Projektleitung: PTB
  Huth Elektronik Systeme GmbH,
  Quorion Data Systems GmbH,
  Ratio Elektronik Systeme GmbH
  Vectron System AG
- Partner Sicherheitsfragen: cryptovison GmbH
- Laufzeit: 2008 – 2010
- Ziel: Entwicklung einer kostengünstigen Sicherheitslösung für Kassensysteme

Gefördert durch:
Bundesministerium für Wirtschaft und Technologie
aufgrund eines Beschlusses des Deutschen Bundestages

INSIKA-Merkmale

- Jeder Buchungsvorgang wird nach Abschluss elektronisch gesichert (signiert) und gespeichert und ist nicht unerkannt veränderbar
- Mit jedem Beleg ist eine Prüfung möglich, ob die Buchung aufgezeichnet wurde
- Die Summen jeder Buchung werden fortlaufend summiert und in einem sicheren Speicher abgelegt
- Von den Summen wird täglich eine signierte Sicherungskopie angelegt
- Verwendung beliebiger Datenträger und Formate in den Kassensystemen



XYZ GmbH, Abbestr. 2, 10587 Berlin
DE 081508150-14

Frühstück Paris A 5,98 €
Kaffeebohnen Arabica
0,253 kg x 9,99€/kg = B 2,53 €
Kaminholz Buche A 14,98 €

Summe 23,49 €

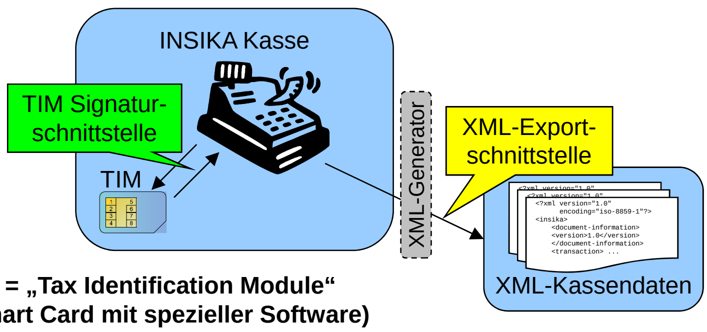
USt.Satz	Brutto	Netto	USt.
A 19%	20,96 €	17,61 €	3,35 €
B 7%	2,53 €	2,36 €	0,17 €

Hash
5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Signatur
U5Y4-VCBB-IGXM-SCB6-6MOF-O2GF-ALS6-W5O4
VETD-3ELO-T77N-QTA4-T6EG-TSIK-JYXY-253J
BXV6-4VYC-TURZ

SEQ: 388
Bediener: Fuchs 12.02.2009 13:27:36

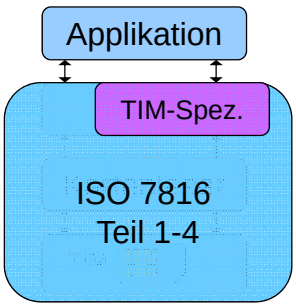
Vielen Dank für Ihren Einkauf!

Signatur- und Exportschnittstelle



- **TIM = „Tax Identification Module“ (Smart Card mit spezieller Software)**
- **Signatur- und Exportschnittstelle durch INSIKA definiert**
- **keine Vorgaben für interne Datenspeicherung der Kasse (Journal)**
- **XML-Kassendaten durch nachgeschaltetes System generierbar (XML-Generator)**

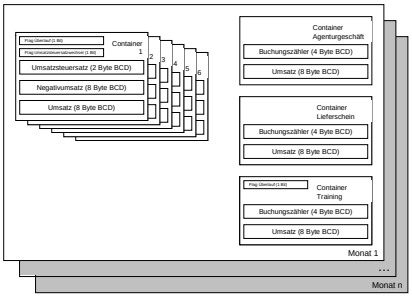
TIM-Signaturschnittstelle
Überblick



- 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)

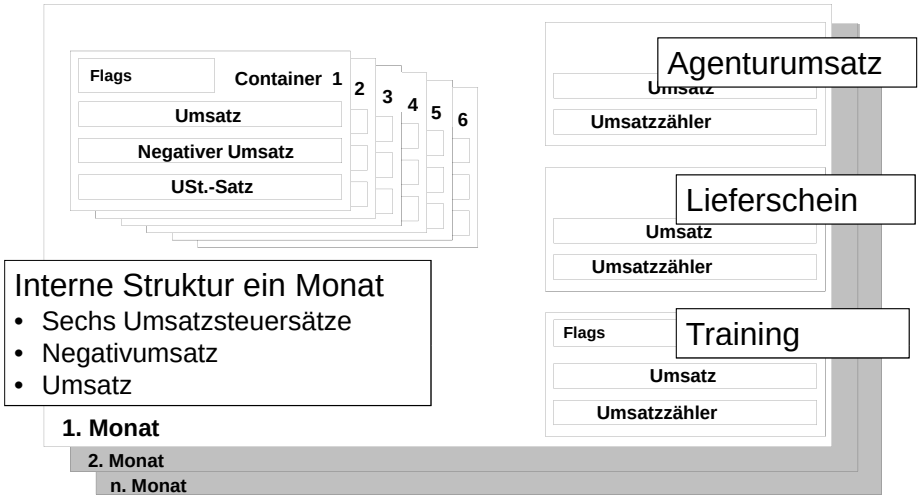
TIM-Signaturschnittstelle
Tax Identification Module (TIM)

- Smart Card bietet gesicherte Umgebung
  → zertifizierter, hoher Manipulationsschutz
- Nutzung asymmetrischer Kryptografie
  → Schlüsselpaar aus privatem und öffentlichem Schlüssel
- Signatur
  → Sicherung der Authentizität & Integrität von Daten, (d.h. Daten lassen sich in Herkunft und Inhalt eindeutig verifizieren)



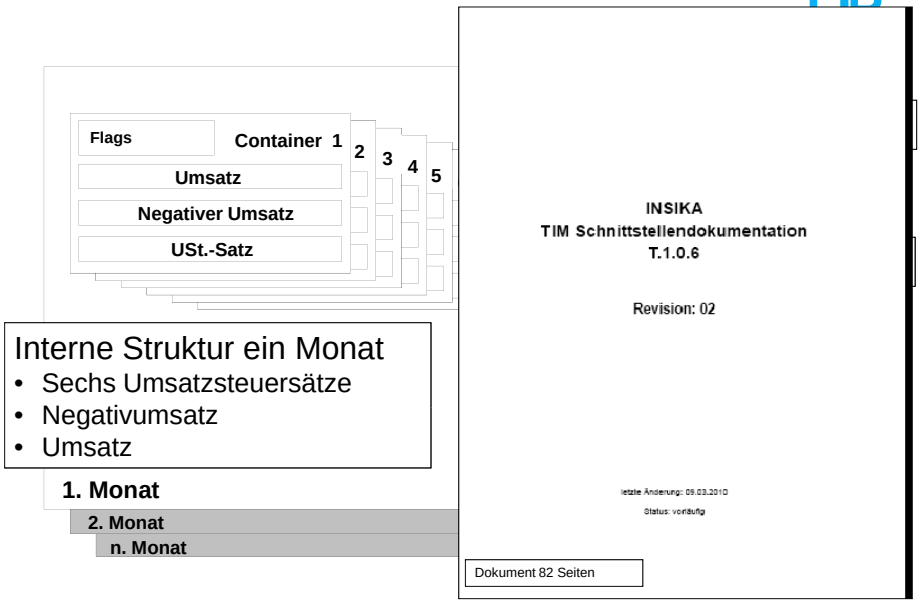
Summenspeicher des TIM

TIM – Aufzeichnung von Umsätzen



Interne Struktur ein Monat
- Sechs Umsatzsteuersätze
- Negativumsatz
- Umsatz

TIM – Aufzeichnung von Umsätzen



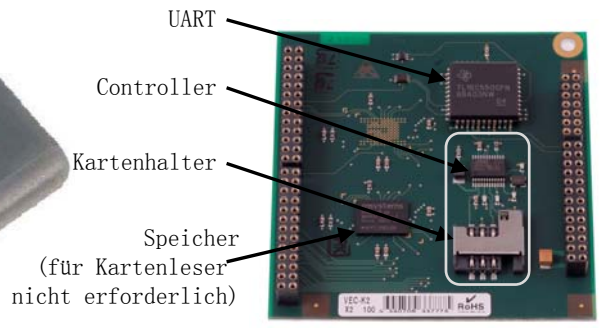
Interne Struktur ein Monat
- Sechs Umsatzsteuersätze
- Negativumsatz
- Umsatz

TIM-Signaturschnittstelle
Beispiel-Buchung („Transaction“)

Befehl / Antwort (hex)	Inhalt
80h 40h 00h 00h 40h CDh 04h 20h 09h 05h 01h CEh 02h 17h 37h C6h 08h 6Fh 70h 65h 72h 61h 74h 6Fh 72h C7h 14h 00h 01h 02h 03h 04h 05h 06h 07h 08h 09h 0Ah 0Bh 0Ch 0Dh 0Fh 10h 11h 12h 13h 14h C8h 02h 03h D2h E1h 10h D8h 02h 11h 9Ch D9h 02h 12h 0Ch DAh 02h 01h 9Ch DBh 02h 19h 00h 00h	**Befehl TRANSACTION** LC = 64 Datum : 2009-05-01 Zeit : 17-37 Bediener "operator" Hashwert der Buchungspositionen Währungscode: 978 (Euro) Container 1 Umsatz : +2119 Negativumsatz : +2120 Umsatzsteuer : +2019 Umsatzsteuersatz : 1900 LE = 00h
C4h 0Dh 54h 50h 49h 44h 5Fh 54h 45h 53h 54h 5Fh 50h 54h 42h C5h 01h 03h CBh 01h 19h 9Eh 30h 50h 27h 57h 4Ch 05h 65h B8h E4h 24h 9Ah 64h 24h 48h F4h 77h 0Ch 12h ADh 4Eh FFh 64h D0h B8h 1Eh A1h 48h DDh E3h C4h CCh 13h 61h 17h B5h 83h 18h C6h 84h FFh C4h 21h B5h FCh 24h 88h 81h 33h 6Bh 90h 00h	**Antwort TRANSACTION** TPID:"TPID_TEST_PTB" TPIDNO: 3 Seq.No der Buchung: 25 Signatur SW1/SW2, No Error

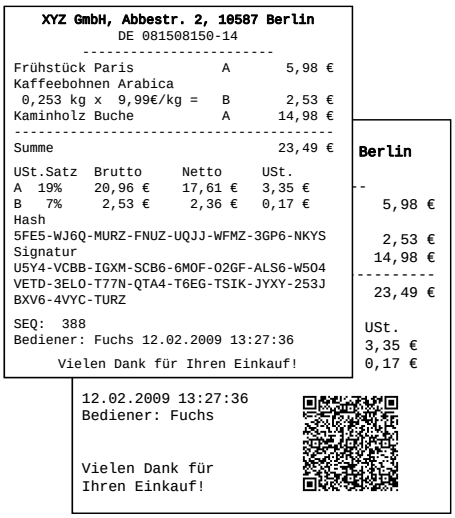
TIM-Signaturschnittstelle
Kartenleser-Varianten

Handelsüblicher Kartenleser



Erweiterungsplatine mit Kartenleser
(hier: VECTRON Systems AG)

INSIKA Kassenbelege



```
XYZ GmbH, Abbestr. 2, 10587 Berlin
DE 081508150-14
------------------------
Frühstück Paris            A       5,98 €
Kaffeebohnen Arabica
 0,253 kg x  9,99€/kg =    B       2,53 €
Kaminholz Buche            A      14,98 €
---------------------------------------
Summe                             23,49 €

USt.Satz  Brutto     Netto     USt.
A  19%    20,96 €    17,61 €   3,35 €
B   7%     2,53 €     2,36 €   0,17 €
Hash
5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Signatur
U5Y4-VCBB-IGXM-SCB6-6MOF-O2GF-ALS6-W5O4
VETD-3ELO-T77N-QTA4-T6EG-TSIK-JYXY-253J
BXV6-4VYC-TURZ

SEQ:  388
Bediener: Fuchs 12.02.2009 13:27:36
      Vielen Dank für Ihren Einkauf!
```

```
Berlin
--
  5,98 €

  2,53 €
 14,98 €
---------
 23,49 €

USt.
3,35 €
0,17 €
```

```
12.02.2009 13:27:36
Bediener: Fuchs


Vielen Dank für
Ihren Einkauf!
```

Sinn & Zweck von INSIKA Kassenbelege:

- Nachweis der Signaturerstellung
- selbst verifizierbar (Erkennen von Fälschungen)
- Stichproben für die Prüfung von XML-Exportdaten

INSIKA Kassenbelege enthalten einen Hashwert und eine Signatur in Textform oder als grafischen Code

Signierte Datenelemente eines Belegs

```
XYZ GmbH, Abbestr. 2, 10587 Berlin
DE 081508150-14
------------------------
Breakfast Paris            A         5,98
Coffee Beans Arabica
 0,253 kg x  9,99€/kg =    B         2,53
Firewood Beech             A        14,98
---------------------------------------
Sum                                 23,49

VAT Rate  Total    w/o Tax    Tax
A  19%    20,96     17,61    3,35
B   7%     2,53      2,36    0,17
Hash
5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Signature
U5Y4-VCBB-IGXM-SCB6-6MOF-O2GF-ALS6-W5O4
VETD-3ELO-T77N-QTA4-T6EG-TSIK-JYXY-253J
BXV6-4VYC-TURZ

SEQ:    388
Operator: Fox 12.02.2009 13:27:36

       Thank You for visiting Us!
```

- Identifikation
- Buchungspositionen
- Umsatzsteuer (pro USt-Satz)
- Hashwert der Buchungspositionen
- Signatur
- Sequenznummer
- Bediener-ID, Datum, Zeit

Signatur (Schritt 1)

```
    XYZ GmbH, Abbestr. 2, 10587 Berlin

        ------------------------
Breakfast Paris           A         5,98
Coffee Beans Arabica
 0,253 kg x  9,99€/kg =   B         2,53
Firewood Beech            A        14,98
---------------------------------------
Sum                                23,49

VAT Rate  Total    w/o Tax    Tax
A  19%    20,96     17,61    3,35
B   7%     2,53      2,36    0,17
Hash
5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Signature



SEQ:    388
Operator: Fox 12.02.2009 13:27:36

       Thank You for visiting Us!
```

Schritt 1: Berechnung des Hashwerts der Buchungspositionen

Signatur (Schritt 2)

```
    XYZ GmbH, Abbestr. 2, 10587 Berlin
              DE 081508150-14
        ------------------------
Breakfast Paris           A         5,98
Coffee Beans Arabica
 0,253 kg x  9,99€/kg =   B         2,53
Firewood Beech            A        14,98
---------------------------------------
Sum                                23,49

VAT Rate  Total    w/o Tax    Tax
A  19%    20,96     17,61    3,35
B   7%     2,53      2,36    0,17
Hash
5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Signature
U5Y4-VCBB-IGXM-SCB6-6MOF-O2GF-ALS6-W5O4
VETD-3ELO-T77N-QTA4-T6EG-TSIK-JYXY-253J
BXV6-4VYC-TURZ

SEQ:    388
Operator: Fox 12.02.2009 13:27:36

       Thank You for visiting Us!
```

Schritt 2: Sende Daten zum TIM

Hashwert	5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Datum, Zeit	12.02.2009 13:27:36
USt normal	20,96(19%)
Ust reduziert	2,53 (7%)
Bediener	Fox
Elemente durch TIM zugefügt	
Sequenznr.	388
Identifikation	DE 081508150-14

Signatur (Schritt 3)

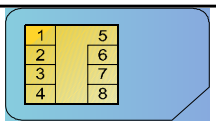
```
     XYZ GmbH, Abbestr. 2, 10587 Berlin
              DE 081508150-14
          ------------------------
Breakfast Paris              A          5,98
Coffee Beans Arabica
 0,253 kg x  9,99€/kg =      B          2,53
Firewood Beech               A         14,98
---------------------------------------------
Sum                                    23,49

VAT Rate  Total    w/o Tax     Tax
A  19%     20,96      17,61     3,35
B   7%      2,53       2,36     0,17
Hash
5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Signature
U5Y4-VCBB-IGXM-SCB6-6MOF-O2GF-ALS6-W5O4
VETD-3ELO-T77N-QTA4-T6EG-TSIK-JYXY-253J
BXV6-4VYC-TURZ

SEQ:    388
Operator: Fox 12.02.2009 13:27:36

        Thank You for visiting Us!
```

Schritt 3: TIM Signatur-Berechnung



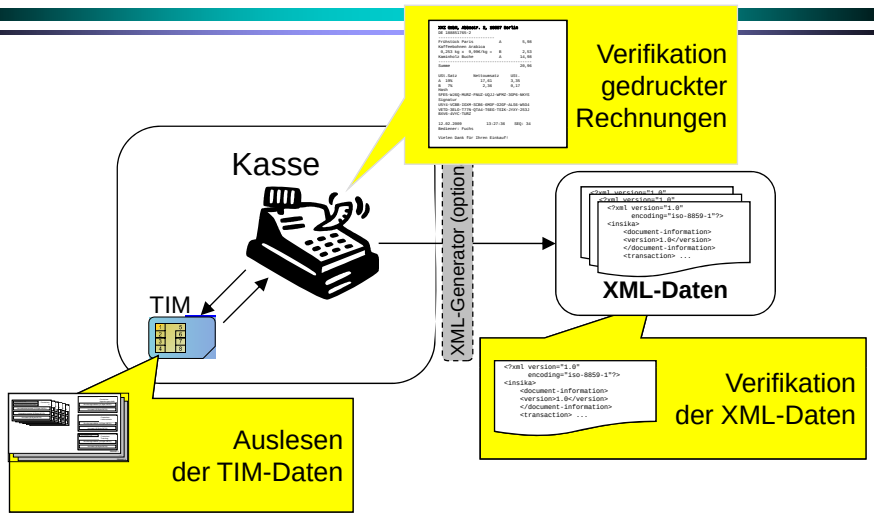
TIM:
Aktualisiere Summenzähler

Notwendige Weiterverarbeitung

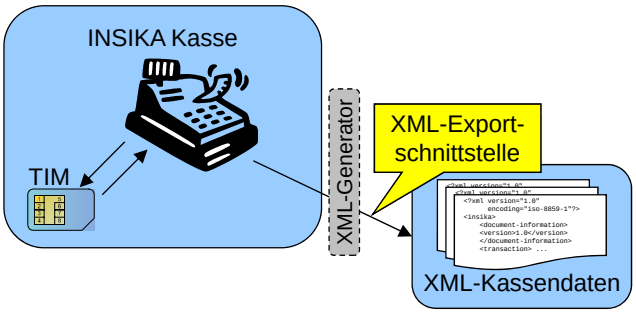
Erforderliche Weiterverarbeitung nach der Erfassung in der Kasse:

- Regelmäßige Übertragung der Daten auf ein Speichermedium (Speicherkarte, USB-Speicher, Festplatte, Abruf per DfÜ, Versand per E-Mail usw.)
- Sicherung von Tagesabschlüssen durch Auslesen der Summenspeicher der Smartcard
- Datenspeicherung auf einem externen PC oder Medium
- Strukturierte Ablage der Daten
- Gezielter Zugriff auf die Daten
- Konvertierung der Daten in ein „prüfungsfähiges“ Format – INSIKA-XML-Exportschnittstelle

Prüfbare Daten



XML-Exportschnittstelle



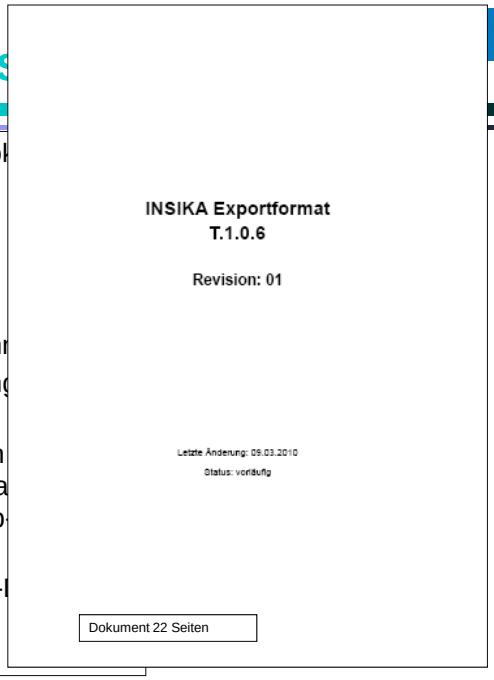
- → XML = Extensible Markup Language:
  standardisiert durch W3C Recommendation
- → INSIKA XML-Exportschnittstelle:
  einheitlich, herstellerunabhängig
- → unabhängig von Ort, Plattform und Medium
  (Web-Services, USB-Stick, CD-Rom, Speicherkarten, etc.)

Verifikation: INSIKA XML-Dokumente

- Inhalt von INSIKA-XML Dokumenten:
  - - Zertifikate,
  - - Buchungen,
  - - Berichte
- INSIKA-XML-Schema:
  - - definiert die XML-Schnittstelle
  - - Ermöglicht die Prüfung von XML- Dokumenten
- XML-Dokumente enthalten nur Textzeichen; sie können daurch mit jedem Texteditor oder Web-Browser angezeigt werden
- Es sind zwei INSIKA-XML-Dokument-typen festgelegt: „Base64“ & „Plaintext“

Verifikation: INS

- Inhalt von INSIKA-XML Dok
  - - Zertifikate,
  - - Buchungen,
  - - Berichte
- INSIKA-XML-Schema:
  - - definiert die XML-Schr
  - - Ermöglicht die Prüfung XML- Dokumenten
- XML-Dokumente enthalten Textzeichen; sie können da jedem Texteditor oder Web- angezeigt werden
- Es sind zwei INSIKA-XML-I typen festgelegt: „Base64“ & „Plaintext“


INSIKA Exportformat
T.1.0.6

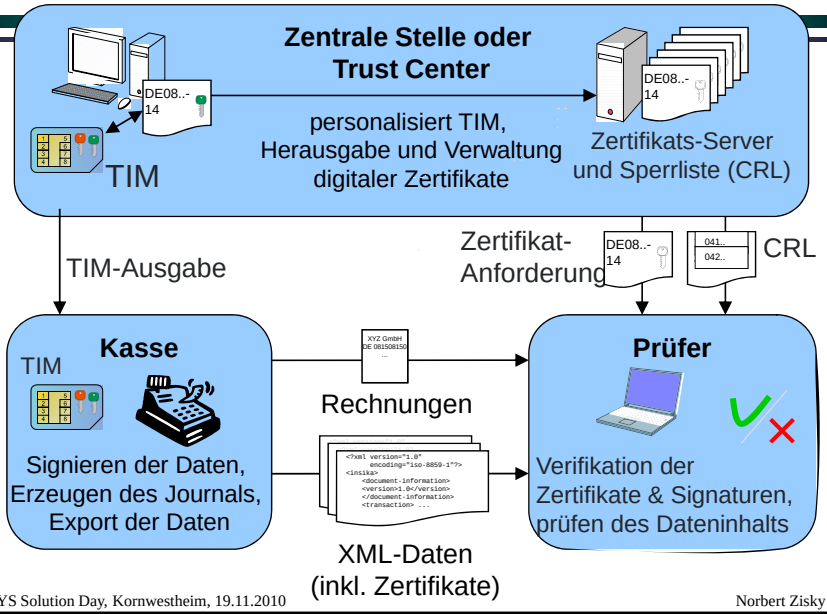
Revision: 01

Letzte Änderung: 09.03.2010

Status: vorläufig

Dokument 22 Seiten

Verifikation: Public Key Infrastructure – PKI



Prüfaufwand/Prüfzeiten

- Vereinfachte Prüfabläufe
  Exakt festgelegte Schnittstellen und
  Datenformate ermöglichen automatisierte Prüfungen
- Prüftiefe wird erhöht
  Durch vollständige Aufzeichnung aller Buchungs- und Journaldaten steht eine sehr gute Datenbasis zur Verfügung
- Prüfzeiten werden verringert

Vorteile von INSIKA

- Sicherheit durch Anwendung bekannter und erprobter Verfahren mit hohem Sicherheitsstandard
- Eindeutig definierte Schnittstellen, offene Specs
- Daten können auf beliebigen Datenträgern in beliebigen Formaten gespeichert werden
- Keine aufwändigen Anforderungen an Systemhersteller
- Keine Bauartzulassungen von Kassen, POS, …
- Effektive Prüfmöglichkeiten
- **Nachweis korrekter Buchungen wird möglich**

Praktische Umsetzung

- Implementierung auf Grundlage der Dokumentation problemlos
  www.insika.de
- Kaum Veränderungen/Ergänzungen nach Abschluss der Systementwicklung
- Kassenprototypen laufen stabil
- Die komplette INSIKA-Systemarchitektur wird getestet
  - Kartenpersonalisierung
  - Signierte Datenerfassung
  - Verifikation

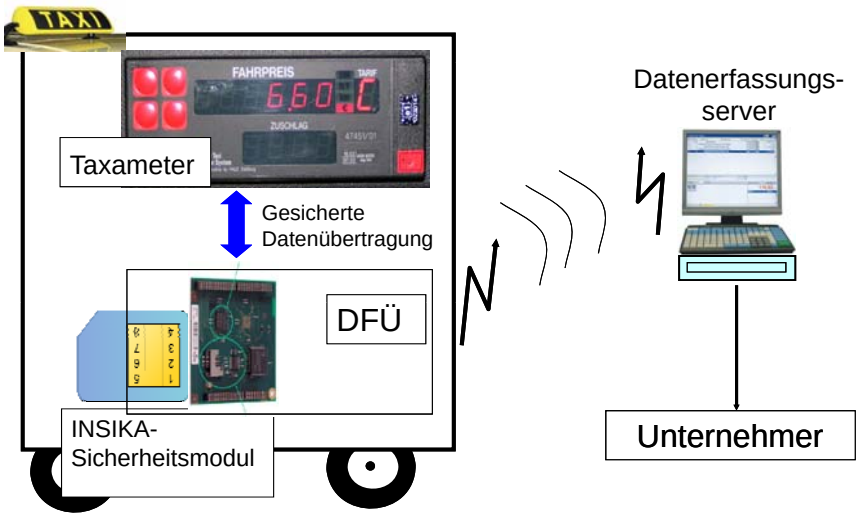
Pilot und Feldversuche

- Seit Mai 2010 Start der Pilotphase Kassen
- Hohes Datenaufkommen mit über 500 Buchungen pro Tag.
- Zusätzliche Datenvolumen: ca. 9 MByte / Monat.
- Pilotanlagen arbeiten ohne Probleme

- Seit September 2010 Start der Pilotphase Taxi
- Anlauf ohne Probleme
- 10 Pilotfahrzeuge in HH und Berlin
- Ausbau auf bis zu 500 Fahrzeuge

Erste Zwischenauswertung: Februar 2011

Systemarchitektur Taxi Prototyp



Flyer europäische Taximesse Köln 2010

Datenübergabe vom Taxameter zur Datenzentrale

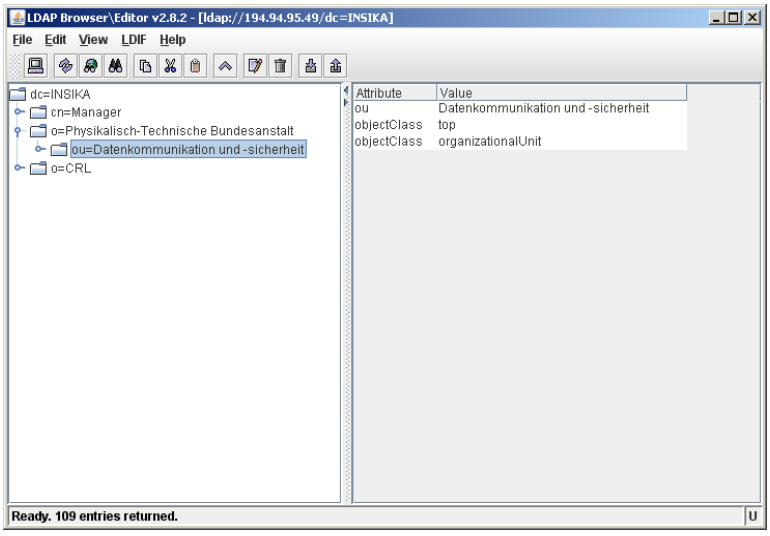
Quelle: Hale electronic GmbH

INSIKA Live –Demo - OFFline

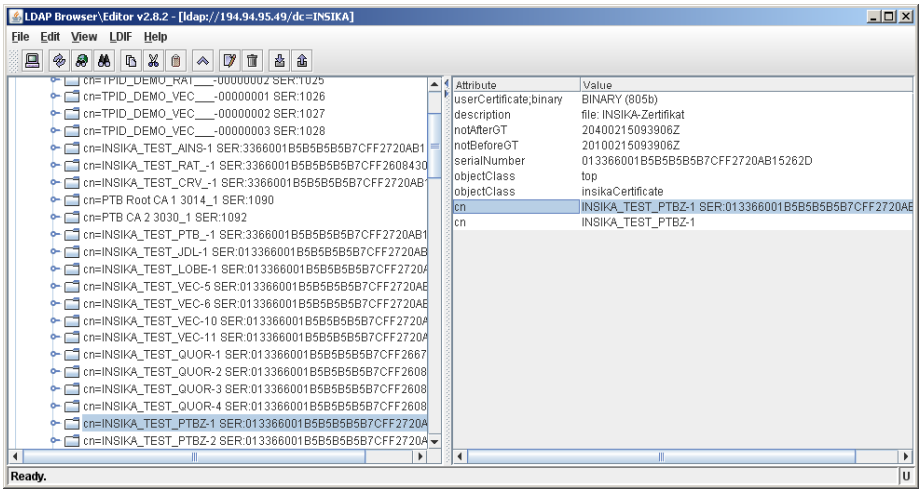
Demonstrationsschritte

- Erzeugen signierter Buchungsdatensätze
- Verifizieren von Buchungsdatensätzen
- Manipulieren von Datensätzen
- Hilfsprogramm TIM-Browser
- Zugriff auf Zertifikate (offline)

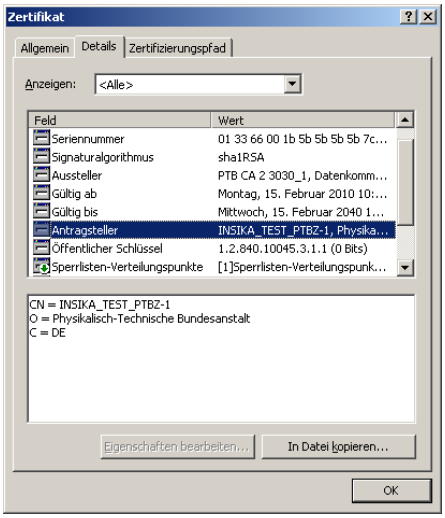
LDAP-Zugriff (1) Zertifikatabruf INSIKA-Testserver

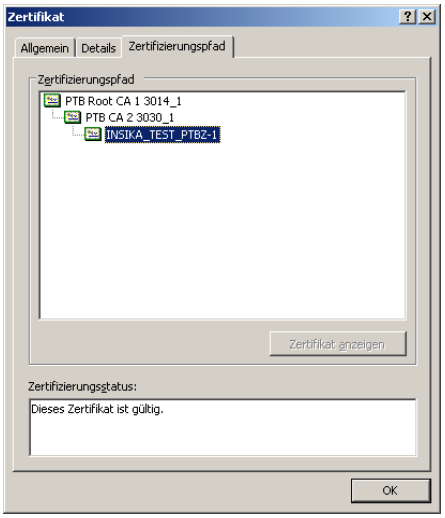


LDAP-Zugriff (2)



LDAP-Zugriff (3)





Zusammenfassung und Ausblick

- BMF und Länder sind weiter aktiv
- Funktionsnachweis INSIKA ist erfolgt
- Vervollständigung der Dokumentation
- Ständige Verbesserung der Programme
- Spezifikationen und TIM stehen Interessenten zur Verfügung – 50 TIM wurden bereits angefordert
- Pilotversuche dauern für Kassen- und Taxiumfeld an
- Starkes Interesse auch aus den Ausland (OECD, europ. Nachbarn)
- Fiskalkassen vs. Fiskallösung – Bauartzulassung von Kassen mit Sicherheitszertifikat – Wer will das??

Vielen Dank!