
**246. PTB Seminar
„Revisionssicheres System zur Aufzeichnung von
Kassenvorgängen und Messinformationen“**

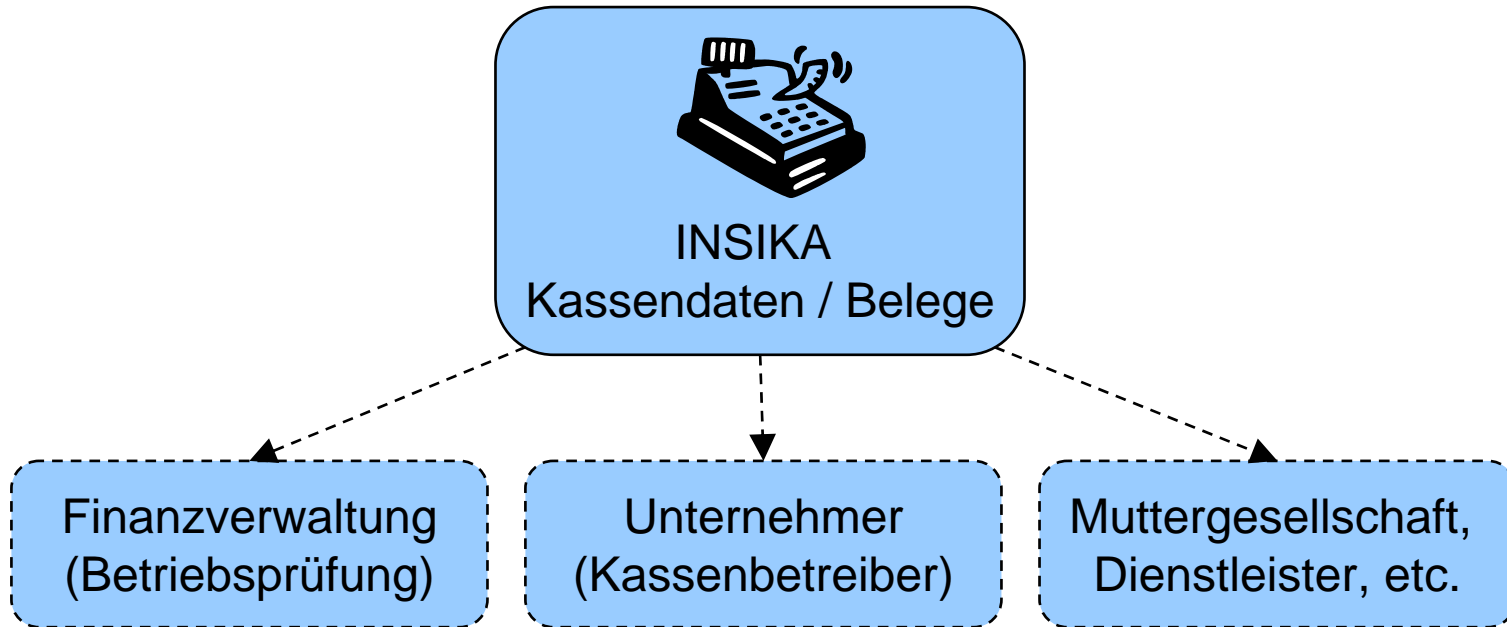
**INSIKA Prüfverfahren
für Kassenbelege und aufgezeichnete Daten**

**Jörg Wolff
Physikalisch-Technische Bundesanstalt
joerg.wolff@ptb.de**

Berlin, 18.02.2009

Wer kann prüfen?

Was wird geprüft?

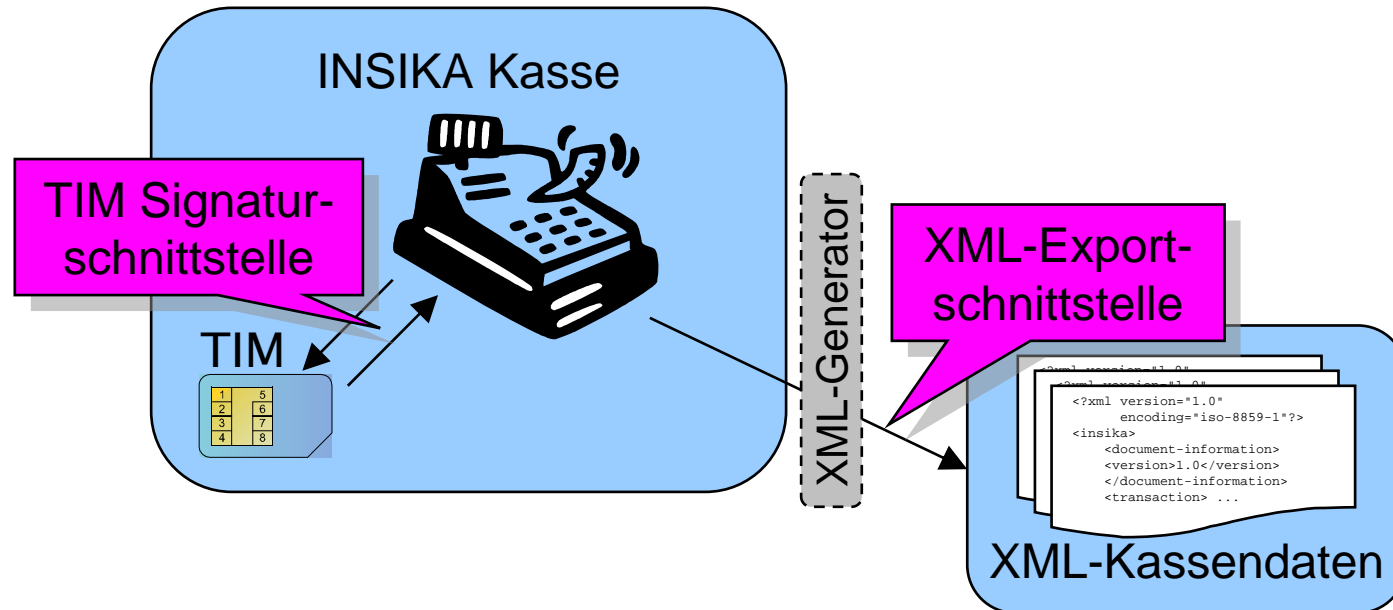


INSIKA Prüfung:

→ Prüfung der Integrität und Authentizität von Kassendaten / Belegen

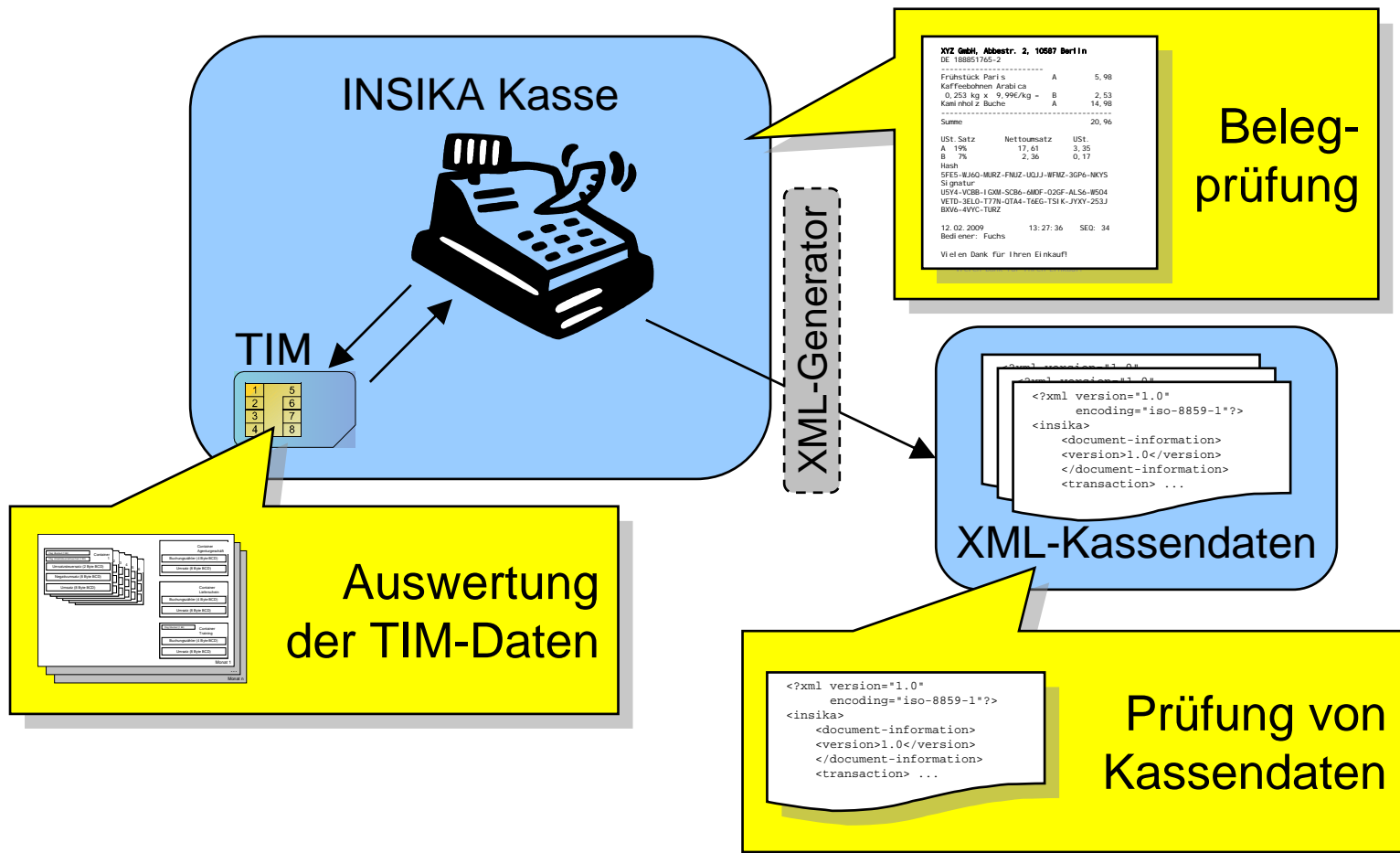
- INSIKA Schnittstellen
- Prüfbare INSIKA Daten
- Prüfung von Kassenbelegen
- XML-Exportformat für aufgezeichnete Kassendaten
- INSIKA IVM-Software
- Prüfung von TIM-Daten (SmartCard)

Signatur- und Exportschnittstelle



- **Signatur- und Exportschnittstelle durch INSIKA definiert**
- **keine Vorgaben für interne Datenspeicherung der Kasse (Journal)**
- **XML-Kassendaten durch nachgeschaltetes System generierbar (XML-Generator)**

Prüfbare Daten



Welche Buchungsdaten werden signiert?

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-02GF-ALS6-W504 ←			
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!			

Identifikationsmerkmal

Positionsdaten
(indirekt, durch Hashwert der Positionsdaten)

Umsatz
(je UStSatz)

Hashwert der Positionsdaten

Signatur

Sequenznummer

Bediener-ID,
Datum, Uhrzeit

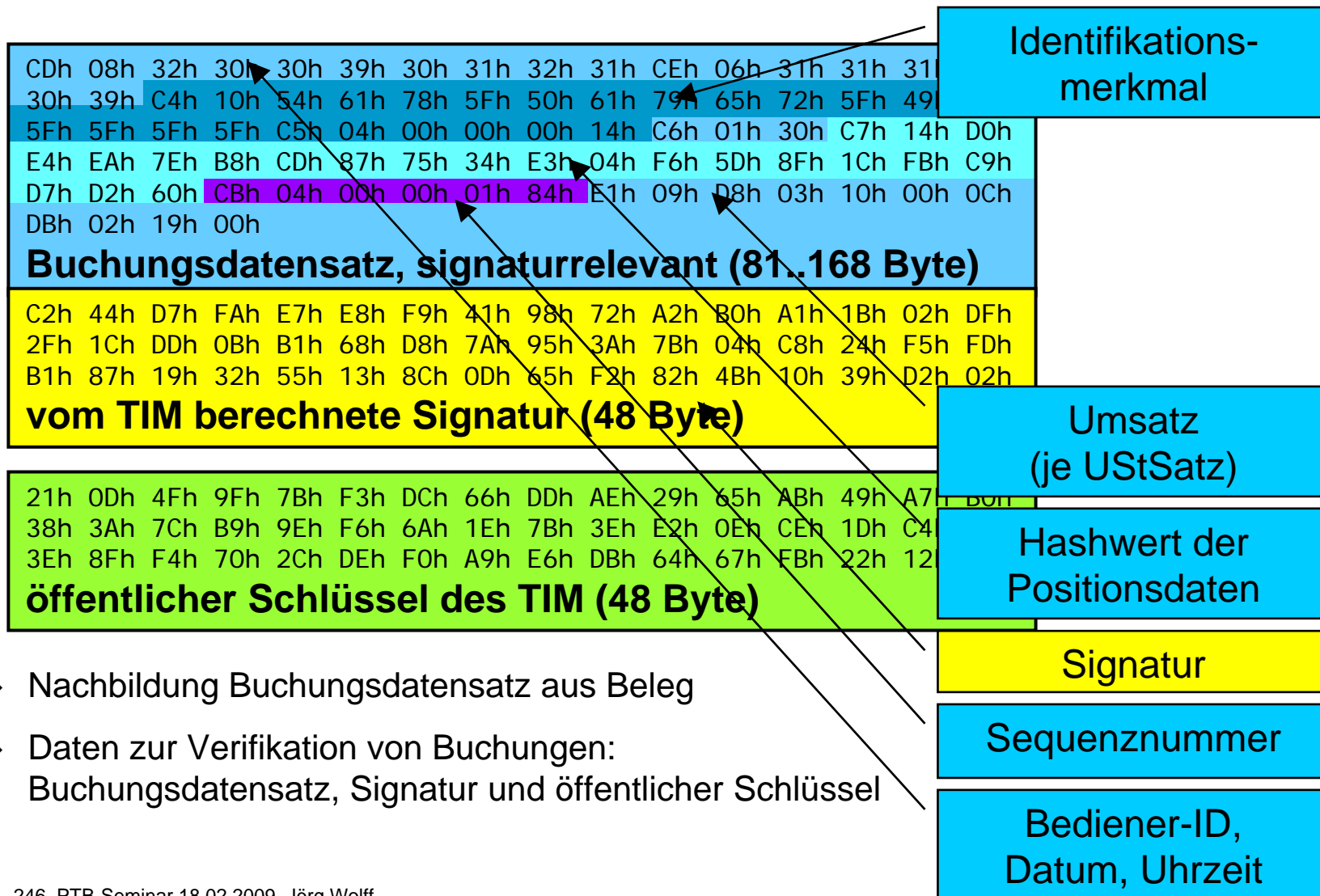
Prüfung von Kassenbelegen anhand Buchungsdaten und Signatur

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

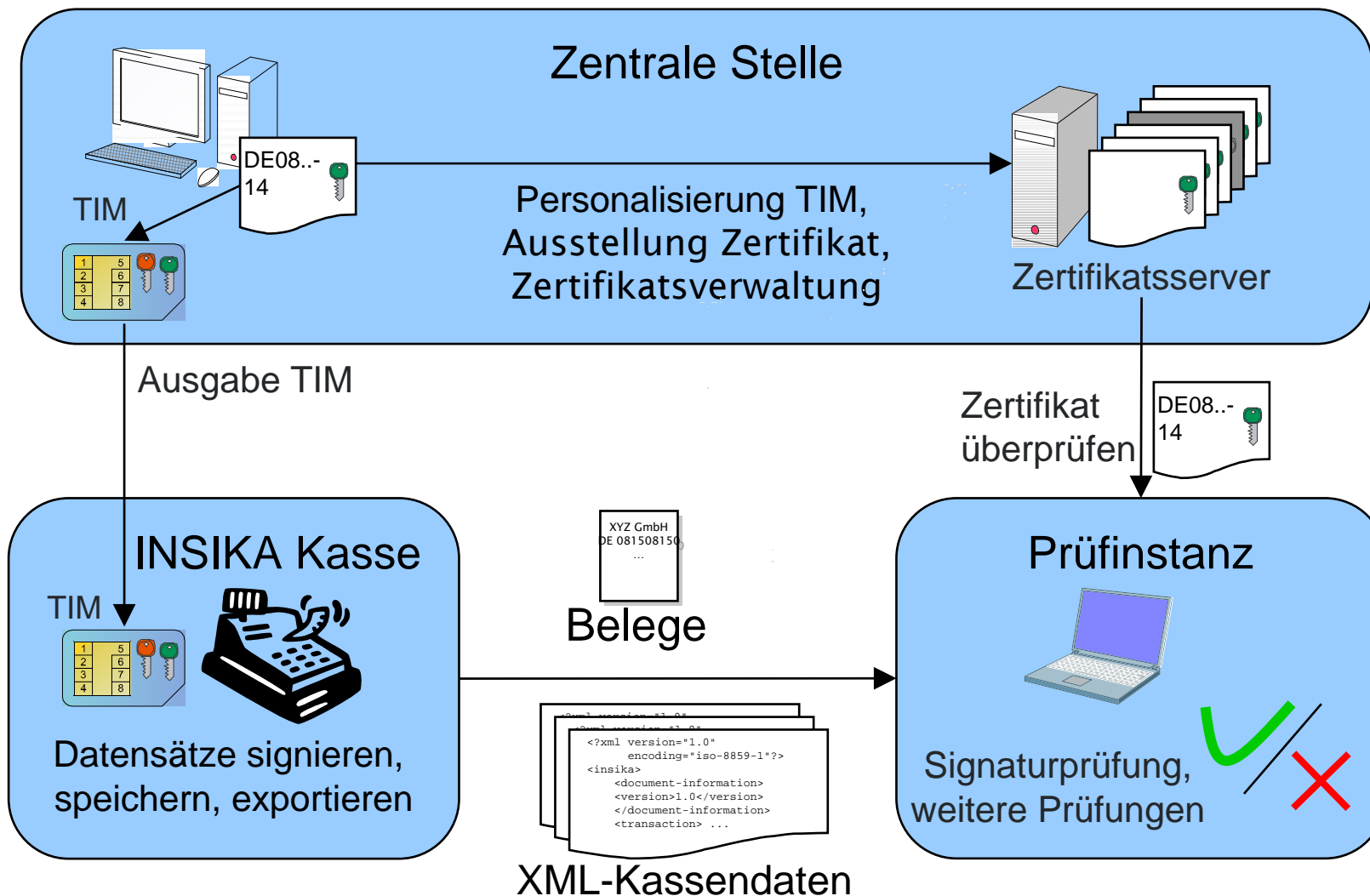
Frühstück Paris		A		5,98
Kaffeebohnen Arabica				
0,253 kg x 9,99€/kg =		B		2,53
Kaminholz Buche		A		14,98

Summe				23,49
USt. Satz	Brutto	Netto	USt.	
A 19%	20,96	17,61	3,35	← Umsatz (je UStSatz)
B 7%	2,53	2,36	0,17	
Hash	5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS ← Hashwert der Positionsdaten			
Signatur	U5Y4-VCBB-IGXM-SCB6-6MOF-02GF-ALS6-W504 ← Signatur			
	VETD-3ELO-T77N-QTA4-T6EG-TSIK-JYXY-253J			
	BXV6-4VYC-TURZ			
SEQ: 388	← Sequenznummer			
Bediener: Fuchs	12.02.2009	13:27:36	← Bediener-ID, Datum, Uhrzeit	
Vielen Dank für Ihren Einkauf!				

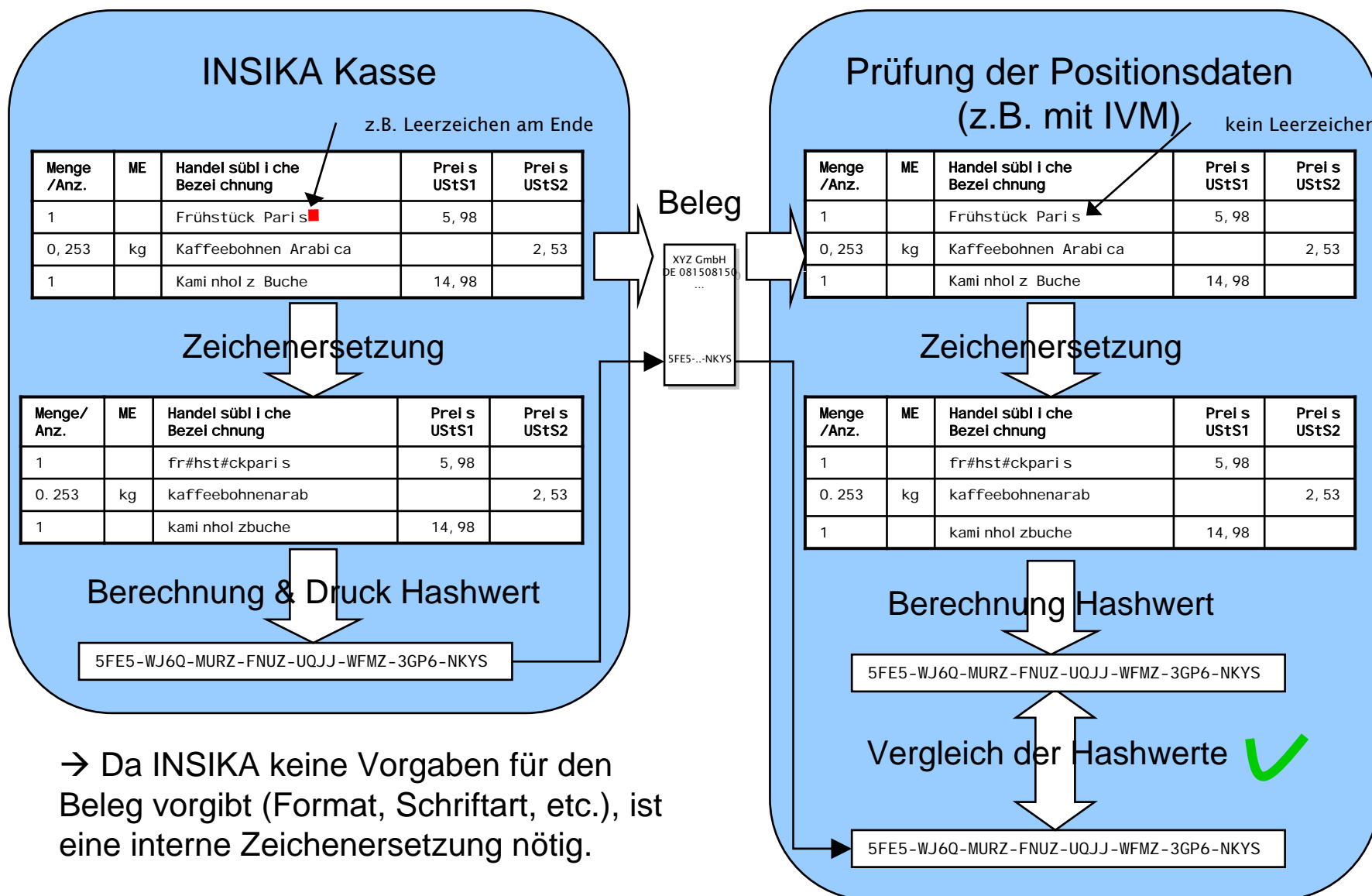
Verifikation von Buchungsdaten



Zertifikatsverwaltung (vereinfacht)



Sonderfall der Belegprüfung: Prüfung der Positionsdaten



→ Da INSIKA keine Vorgaben für den Beleg vorgibt (Format, Schriftart, etc.), ist eine interne Zeichenersetzung nötig.

IVM-Software: Prüfung von Kassenbeleggen

Belegeingabe

Verifikation Positions-Hash

Gesamtpreis

Positionen (Reihenfolge wie auf Beleg !):		Umsatzsteuerklasse:						
		1	2	3	4	5	6	
Anzahl	Einheit	Bezeichnung	Std	Erm 1	Erm 2	frei	Spez 1	Spez 2

Positions-Hash: (berechnet)

Positions-Hash: PFBG-RWxK-LT3C-P2EA-CYNB-IZPR-UE3D-GB7Q

	1 - Standard	2 - Ermäßigt 1	3 - Ermäßigt 2	4 - frei (ohne)	5 - Spezial 1	6 - Spezial 2
Umsatzsteuersatz:	19,00 %	7,00 %	0,00 %	0,00 %	10,70 %	5,50 %
Umsatzsteuer:	0,94	0,29				
Nettoumsatz:	4,96	4,10				
Bruttoumsatz:	5,90	4,39				

Tax-Payer-ID: Tax_Payer_ID____ Nr.: 00000001 Bediener-ID: ich

Sequenz-Nr.: 417 Training

Datum: 2009-02-09 Zeit: 15:21:18 Exklusiv USt

Signatur: QYY-ZVCB-YTA6-TASS-VHCQ-DC7L-BSLX-GRUP-DOE5-XLT7-6PW3-OSH0-V24C-KORX-VMOA-S7ED-L3UP-WCDH-0X6J-

Ergebnis Verifikation: Verifikation fehlgeschlagen

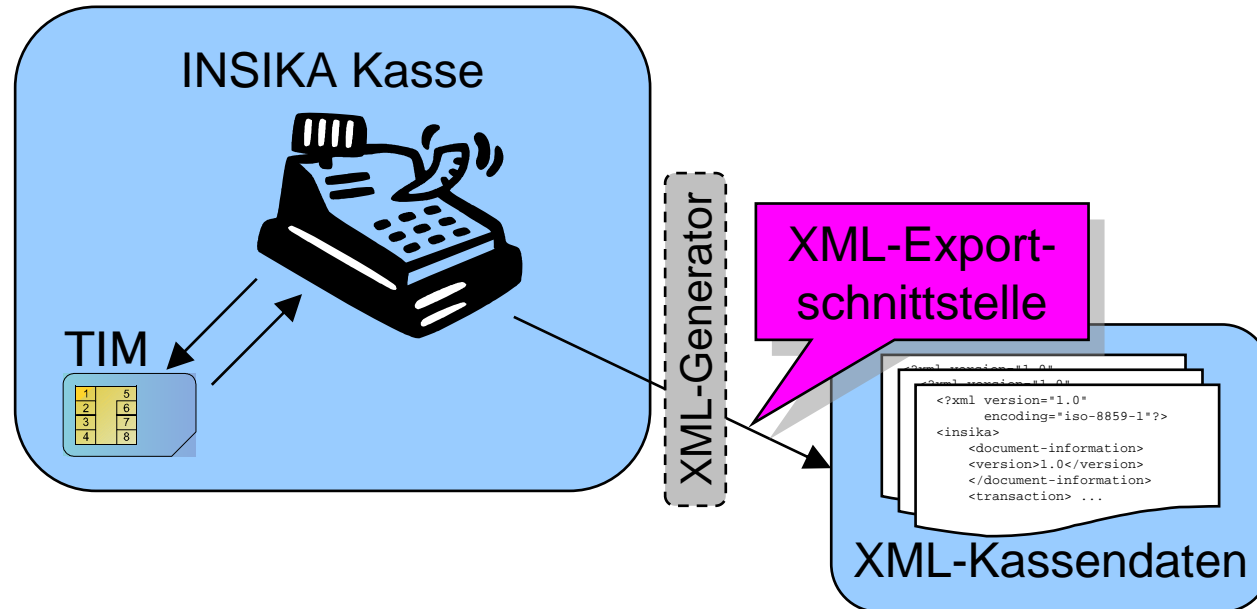
Ende Beispiele:

Prüfung Hashwert der Positionsdaten

Belegprüfung

- Hashwert der Positionsdaten und Signatur hier Base32-kodiert (32 bzw. 77 Zeichen)
- Verbesserung der Handhabung durch Texterkennung möglich
- Verwendung von 2D-Codes denkbar, weit verbreitete Dekodierbarkeit vorausgesetzt

INSIKA XML-Exportschnittstelle



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

XML-Formate „Base64“ und „Klartext“

```

<?xml version="1.0" encoding="ISO-8859-1"
- <insika>
+ <document-information>
- <transactionEncoded>
  <itemListEncoded>oAExogt6dWdiYW5k
  <transactionRequest>zQgyMDA5MDIxN
  <transactionResponse>xBBUUEIEX0RFT
  </transactionEncoded>
+ <transactionEncoded>
+ <transactionEncoded>
+ <transactionEncoded>
- <reportEncoded>
  <reportRequest>gEIBABLNCDIwMDkwI
  <reportResponse>wAEDxBBUUEIEX0R
  </reportEncoded>
- <certificate>
  <certificateId>TPID_DEMO_PTB____-00
  <certificateKey>1625FD519AA37F228F

```

Datensätze
Base64-kodiert

```

<?xml version="1.0" encoding="iso8859-1" ?>
- <insika>
+ <document-information>
+ <certificate>
- <transaction>
  <date>20090212</date>
  <time>132736</time>
  <operatorId>Fuchs</operatorId>
- <itemList>
  - <item>
    <qnt>1</qnt>
    <name>Frühstück Paris</name>
    <price1>598</price1>
  </item>
  - <item>
    <qnt>0.253</qnt>
    <unit>kg</unit>
    <name>Kaffeebohnen Arabica</nam
    <price2>253</price2>
  </item>
  - <item>
    <qnt>1</qnt>

```

Daten in
Textform

→ zwei Formate definiert, je nach Voraussetzungen der Kasse bedienbar

Prüfbare Inhalte von XML-Dokumenten

```

<?xml version="1.0" encoding="iso8859-1" ?>
- <insika>
+ <document-information>
+ <certificate>
- <transaction>
  <date>20090212</date>
  <time>132736</time>
  <operatorId>Fuchs</operatorId>
- <itemList>
  - <item>
    <qnt>1</qnt>
    <name>Frühstück Paris</name>
    <price1>598</price1>
  </item>
  - <item>
    <qnt>0.253</qnt>
    <unit>kg</unit>
    <name>Kaffeebohnen Arabica</nam
    <price2>253</price2>
  </item>
  - <item>
    <qnt>1</qnt>

```

Automatisiert prüfbare Inhalte:

- Gültigkeit Zertifikat
- Buchung:
 - Positionsdaten \leftrightarrow Hashwert der Positionsdaten
 - Signatur
- Tagesabschluss:
 - Umsätze \leftrightarrow Umsatzsummen der eingeschlossenen Buchungen
 - streng monoton steigende Sequenznummern eingeschlossener Buchungen
 - Signatur

Zuordnung von Beleg und XML-Exportdaten

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-02GF-ALS6-W504
VETD-3ELO-T77N-QTA4-T6EG-TSIK-JYXY-253J
BXV6-4VYC-TURZ

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

Vielen Dank für Ihren Einkauf!

```

<?xml version="1.0" encoding="utf-8" ?>
- <insika>
+ <document-information>
+ <certificate>
- <transaction>
  <date>20090205</date>
  <time>140333</time>
  <operatorId>ich</operatorId>
+ <itemList>
  <hashTransactionItems>A3F45FEF34D94C0
  <currency>0978</currency>
+ <containerVat1>
+ <containerVat2>
+ <containerThirdparty>
  <tpId>Tax_Payer_ID____</tpId>
  <tpIdNo>00000001</tpIdNo>
  <seqNoTransaction>388</seqNoTransaction>
  <sig>8F138C2D1DE3C260481FB5DFE5770
  <debugHashTransaction>14E38BA76EA35D
</transaction>
+ <report>

```

Sequenznummer

→ eindeutige Rückführbarkeit von Beleg auf XML-Exportdaten durch Identifikationsmerkmal und Sequenznummer

INSIKA Verifikations Modul (IVM)

INSIKA - Verifikations-Modul

Datei Ansicht Hilfe

Belegverifikation Datei(en) laden Überprüfte Dateien: 2

Gesamtergebnis: **Verifikationen erfolgreich**

Nr.	Datei	Verifikation
1	D:\wolff05\Programmierung\Bsp-Daten\51-01.txt.xml	ok
2	D:\wolff05\Programmierung\Bsp-Daten\export1L.xml	ok

Inhalt Datei Nr.: 2 Datei: D:\wolff05\Programmierung\Bsp-Daten\export1L.xml **ok**

Transaction: 4

SeqNo TrAct	Date	Time	TaxPayer-ID	TPID-No	Operator	Verifikation
00000010	2009-02-16	17:23:54	TPID_DEMO_PT...	00000001	fuchs	ok
00000011	2009-02-16	17:23:59	TPID_DEMO_PT...	00000001	fuchs	ok
00000012	2009-02-16	17:24:06	TPID_DEMO_PT...	00000001	fuchs	ok
00000013	2009-02-16	17:24:14	TPID_DEMO_PT...	00000001	fuchs	ok

selektierte Transaction Inhalt zeigen

Report: 1

SeqNo Rept	Date	Time	TaxPayer-ID	TPID-No	SeqNo TrAct	LifeCycle	Verifikation
00000010			TPID_DEMO_PT...	00000001	00000013	undefiniert	ok

selektierter Report Inhalt zeigen

Zertifikat: 1

TPID_DEMO_PT... -00000001 Zertifikat zeigen

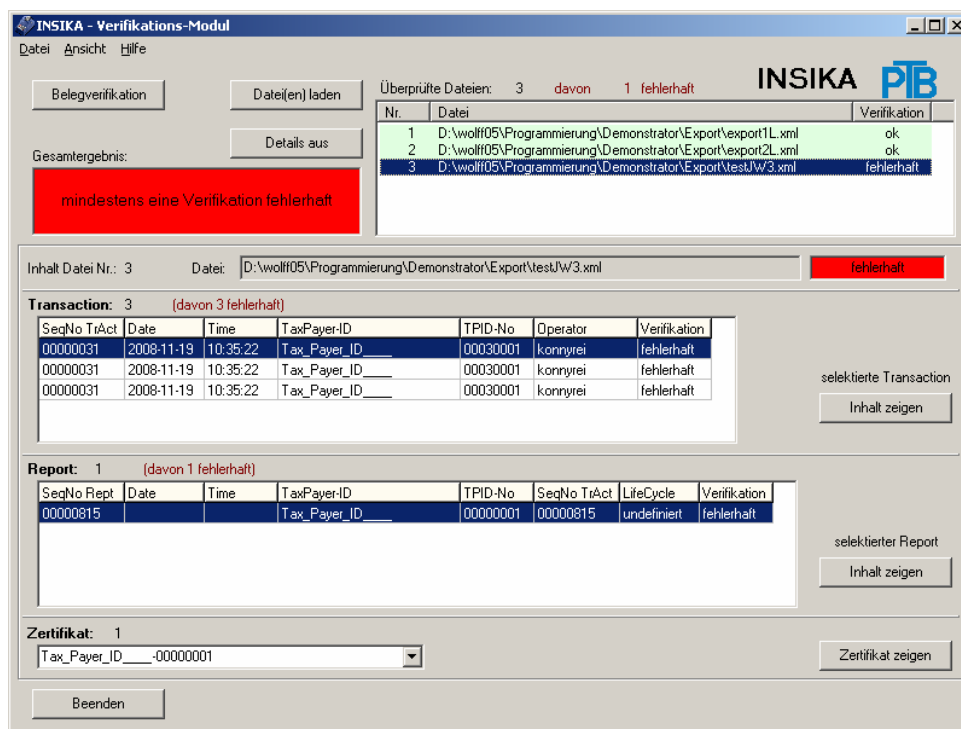
Beenden

Buchungen

Tagesabschlüsse

Zertifikate

INSIKA Verifikations Modul (II)



INSIKA - Verifikations-Modul

Überprüfte Dateien: 3 davon 1 fehlerhaft

Nr.	Datei	Verifikation
1	D:\wollf05\Programmierung\Demonstrator\Export\export1L.xml	ok
2	D:\wollf05\Programmierung\Demonstrator\Export\export2L.xml	ok
3	D:\wollf05\Programmierung\Demonstrator\Export\testJW3.xml	fehlerhaft

mindestens eine Verifikation fehlerhaft

Inhalt Datei Nr.: 3 Datei: D:\wollf05\Programmierung\Demonstrator\Export\testJW3.xml fehlerhaft

Transaction: 3 (davon 3 fehlerhaft)

SeqNo TrAct	Date	Time	TaxPayer-ID	TPID-No	Operator	Verifikation
00000031	2008-11-19	10:35:22	Tax_Payer_ID___	00030001	konnreyi	fehlerhaft
00000031	2008-11-19	10:35:22	Tax_Payer_ID___	00030001	konnreyi	fehlerhaft
00000031	2008-11-19	10:35:22	Tax_Payer_ID___	00030001	konnreyi	fehlerhaft

Report: 1 (davon 1 fehlerhaft)

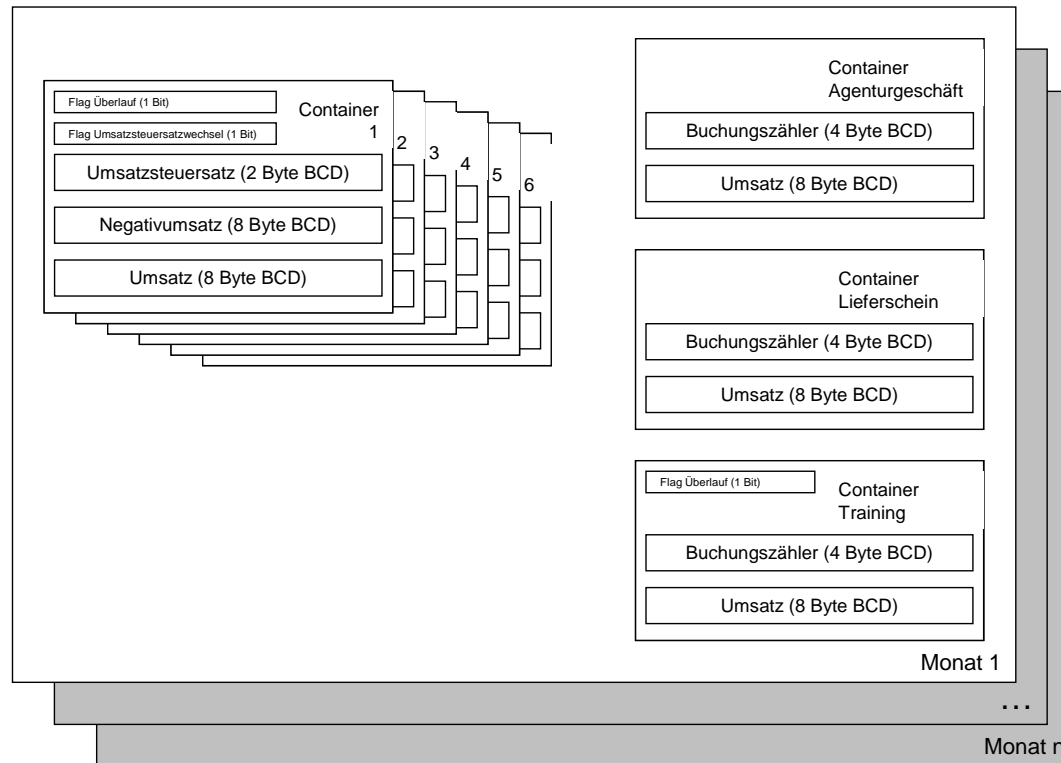
SeqNo Rept	Date	Time	TaxPayer-ID	TPID-No	SeqNo TrAct	LifeCycle	Verifikation
00000815			Tax_Payer_ID___	00000001	00000815	undefiniert	fehlerhaft

Zertifikat: 1
Tax_Payer_ID___-00000001

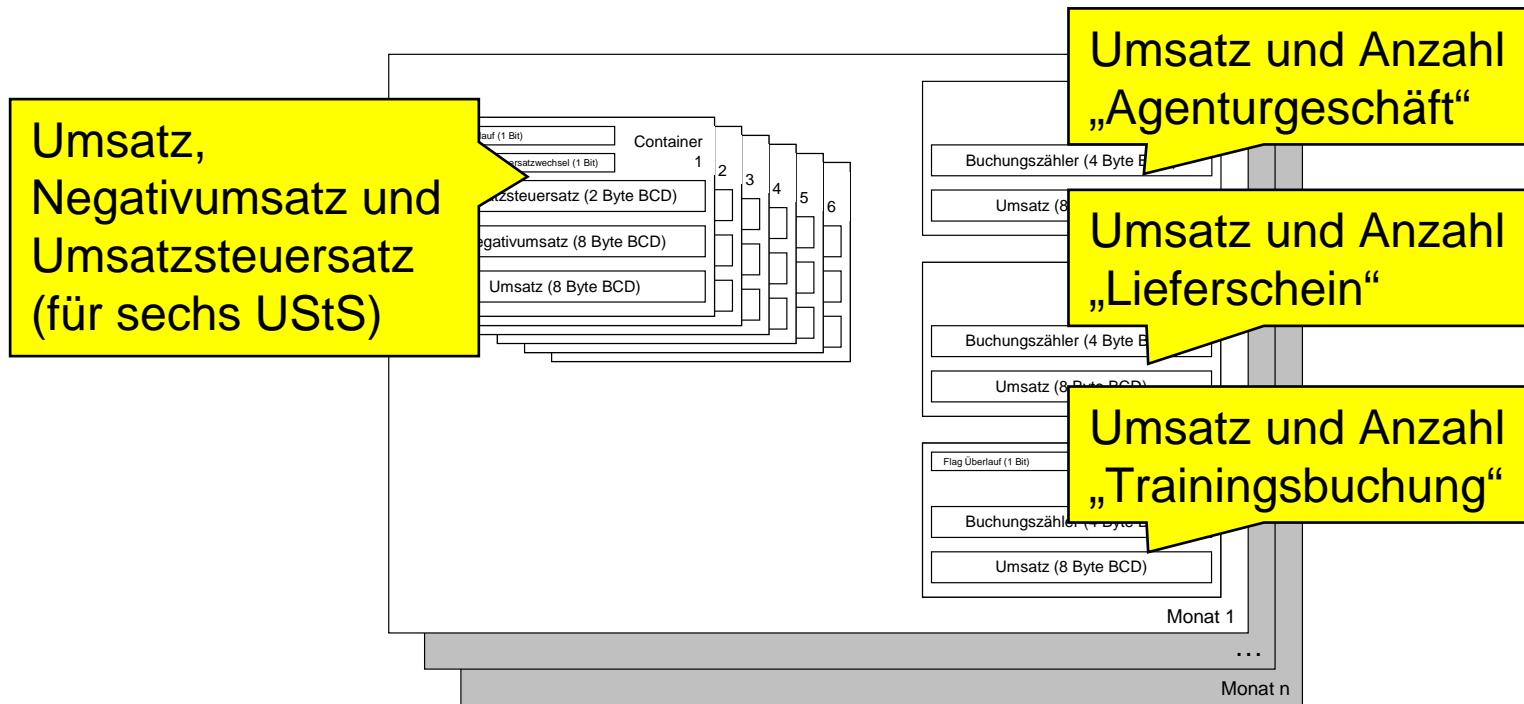
- IVM-Software zur Signaturverifikation von
 - INSIKA XML-Dokumenten
 - Kassenbelegen
- wesentliche Komponenten: XML-Parser mit Bildung des Datensatzes, ECDSA-Bibliothek, Belegverifikation und Hauptprogramm

- nutzt veröffentlichte und frei zugängliche Verfahren
- Nachbau einer Verifikationssoftware für INSIKA-Daten ohne größere Probleme möglich

Prüfung der TIM Summenspeicher



- Prüfung der TIM Summenspeicher bildet Sonderfall (z.B. bei Verlust der Kassendaten)
- jeder Monat einzeln gebucht, geplante Nutzungsdauer 10 Jahre
- sechs Umsatzsteuersätze buchbar, (z.B. Standard, ermäßigter Satz 1 & 2, umsatzsteuerfrei, Spezial 1 & 2)



- Negativumsatz wird in den Umsatz einberechnet
- Umsatzanteile „Agenturgeschäft“ und „Lieferschein“ reduzieren die Steuerpflicht → „vier Augen Prinzip“, Kontrolle über nachgeschaltete Systeme möglich
- auf Basis der Summen Abschätzung der monatlichen Umsätze je Umsatzsteuersatz möglich

Beispielhaftes Prüfzenario

1. Anforderung von XML-Exportdaten vom Kassensbetreiber über einen bestimmten Zeitraum
2. Überprüfung des Zertifikats auf Gültigkeit
3. Überprüfung der Tagesabschlüsse
 - Signaturprüfung
 - Summe der eingeschlossenen Buchungen = Umsatz des zugehörigen Tagesabschlusses
 - Kontrolle der Sequenznummern
4. bei Bedarf
 - stichprobenartige oder vollständige Prüfung der einzelnen Buchungen (eindeutige Rückführbarkeit von Belegen \leftrightarrow Exportdaten)
 - Belegprüfung anhand Buchungssatz, Signatur und Zertifikat, optional: Verifikation des Hashwert der Positionsdaten
5. auf INSIKA aufsetzende Prüfverfahren:
 - Auswertung von Umsätzen, Umsatzsteuern, Warenumsatz etc.

Zusammenfassung

- vollständig automatisierte Prüfung der Integrität und Authentizität von Exportdaten der Kasse
- eindeutig definiertes Format der Exportdaten, herstellerunabhängig
- geringe Prüfzeiten durch automatisierte Prüfung
- hohe Prüftiefe durch Aufzeichnung aller Buchungsdaten
- Kassenbelege können als Stichproben genutzt werden
- Kassenbelege selbst können geprüft werden, gefälschte Kassenbelege werden erkannt
- durch Auswertung der TIM Summenspeicher Abschätzung von Umsätzen möglich

Vielen Dank für Ihre Aufmerksamkeit!

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

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

Summe

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

Hash
5FE5-WJ6Q-MURZ-FNUZ-UOJ
Signatur
USY4-VCBB-IGXM-SCB6-6MOF
VETD-3ELO-T77N-QTA4-T6EC
BX16-4VYC-TUR7

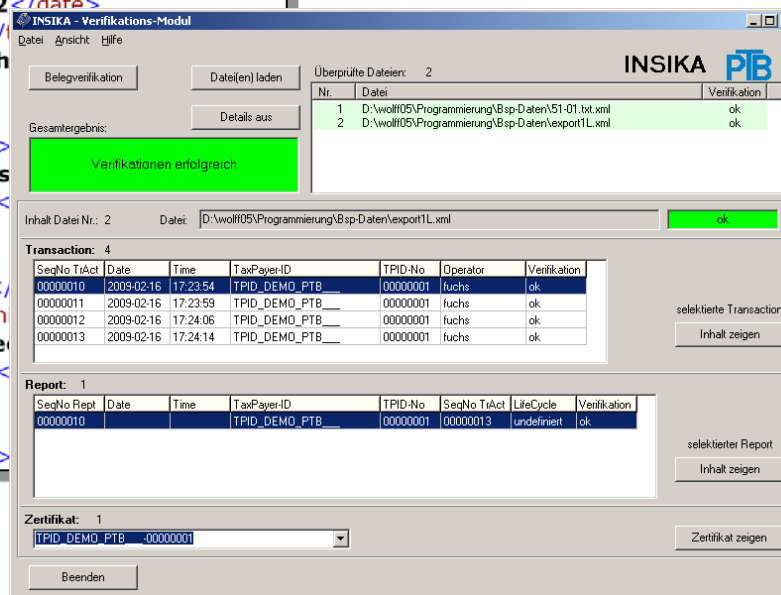
12.02.2009 13:27:3
Bedienung: Fuchs

Vielen Dank für Ihre Aufmerksamkeit!

```

<?xml version="1.0" encoding="iso8859-1" ?>
- <insika>
+ <document-information>
+ <certificate>
- <transaction>
  <date>20090212</date>
  <time>132736</time>
  <operatorId>Fuchs</operatorId>
- <itemList>
- <item>
  <qnt>1</qnt>
  <name>Frühstück</name>
  <price1>598</price1>
</item>
- <item>
  <qnt>0.253</qnt>
  <unit>kg</unit>
  <name>Kaffeebohnen Arabica</name>
  <price2>253</price2>
</item>
- <item>
  <qnt>1</qnt>

```



INSIKA - Verifikations-Modul

Überprüfte Dateien: 2

Nr.	Datei	Verifikation
1	D:\wollf05\Programmierung\Bsp-Daten\51-01.txt.xml	ok
2	D:\wollf05\Programmierung\Bsp-Daten\export1L.xml	ok

Gesamtergebnis: Verifikationen erfolgreich

Inhalt Datei Nr.: 2 Datei: D:\wollf05\Programmierung\Bsp-Daten\export1L.xml

Transaction: 4

SeqNo	TrAct	Date	Time	TaxPayer-ID	TPID-No	Operator	Verifikation
00000010		2009-02-16	17:23:54	TPID_DEMO_PT...	00000001	fuchs	ok
00000011		2009-02-16	17:23:59	TPID_DEMO_PT...	00000001	fuchs	ok
00000012		2009-02-16	17:24:06	TPID_DEMO_PT...	00000001	fuchs	ok
00000013		2009-02-16	17:24:14	TPID_DEMO_PT...	00000001	fuchs	ok

Report: 1

SeqNo	Rept	Date	Time	TaxPayer-ID	TPID-No	SeqNo TrAct	LifeCycle	Verifikation
00000010				TPID_DEMO_PT...	00000001	00000013	undefiniert	ok

Zertifikat: 1
TPID_DEMO_PT...-00000001

Beenden