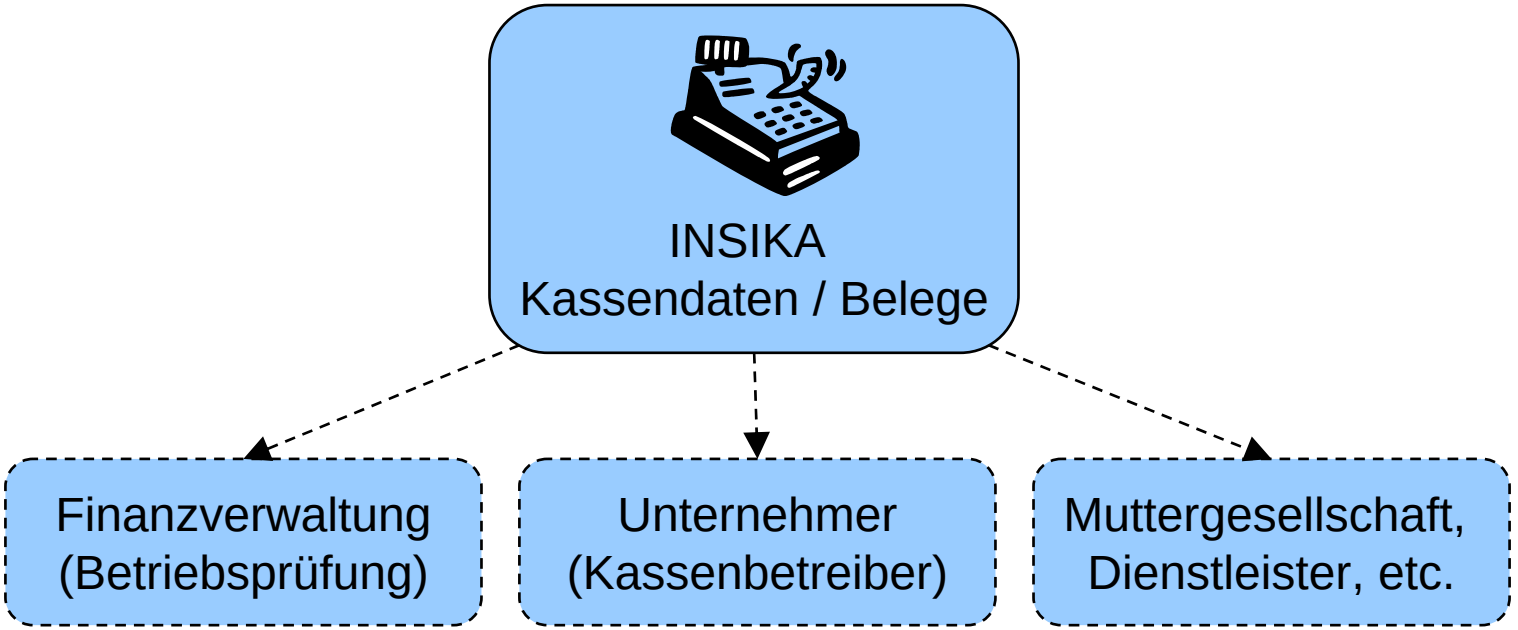
246. PTB Seminar
„Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationen“

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?



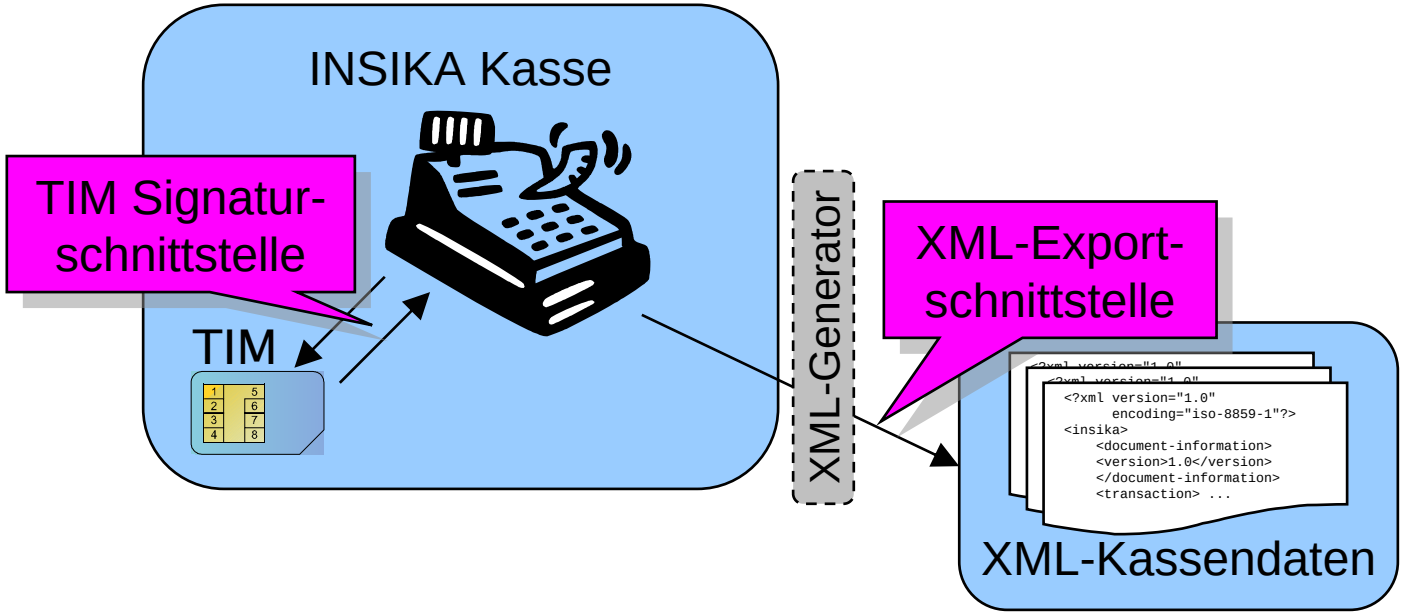
INSIKA Prüfung:

→ Prüfung der Integrität und Authentizität von Kassendaten / Belegen

Übersicht

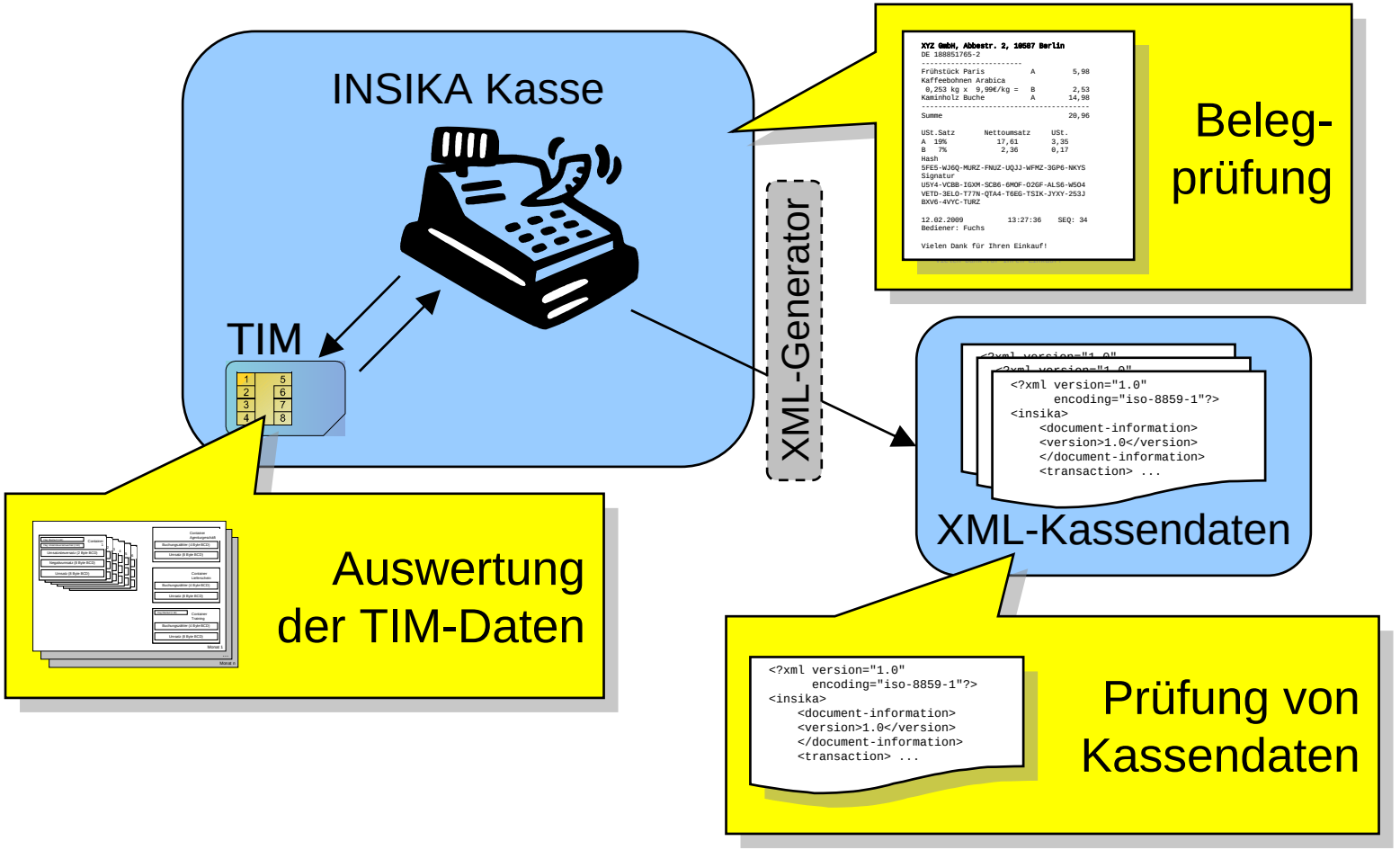
- INSIKA Schnittstellen
- Prüfbare INSIKA Daten
- Prüfung von Kassenbelegen
- XML-Exportformat für aufgezeichnete Kassendaten
- INSIKA IVM-Software
- Prüfung von TIM-Daten (SmartCard)

Signatur- und Exportschnittstelle

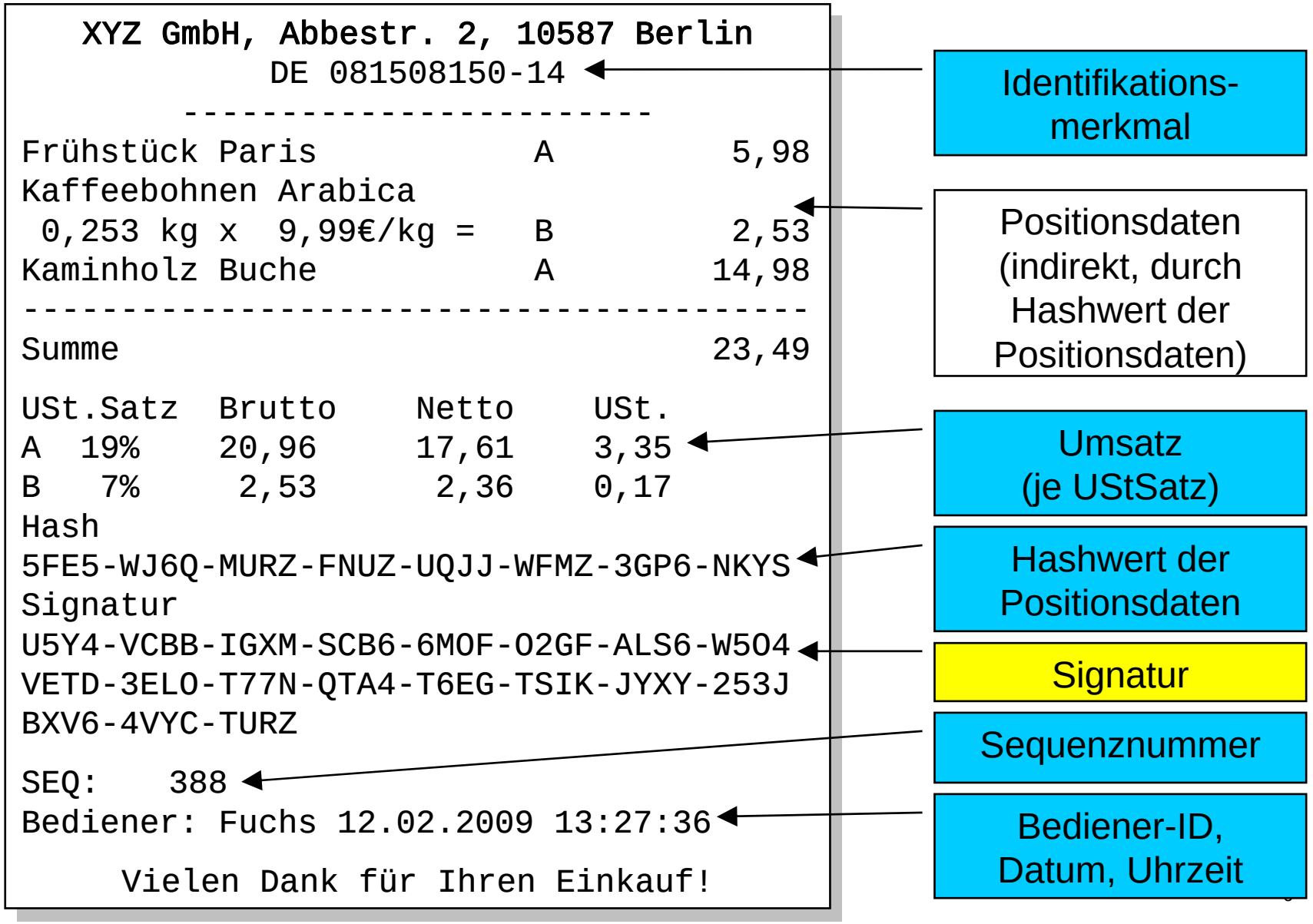


- **Signatur- und Exportschnittstelle durch INSIKA definiert**
- **keine Vorgaben für interne Datenspeicherung der Kasse (Journal)**
- **XML-Kassendaten durch nachgeschaltetes System generierbar (XML-Generator)**

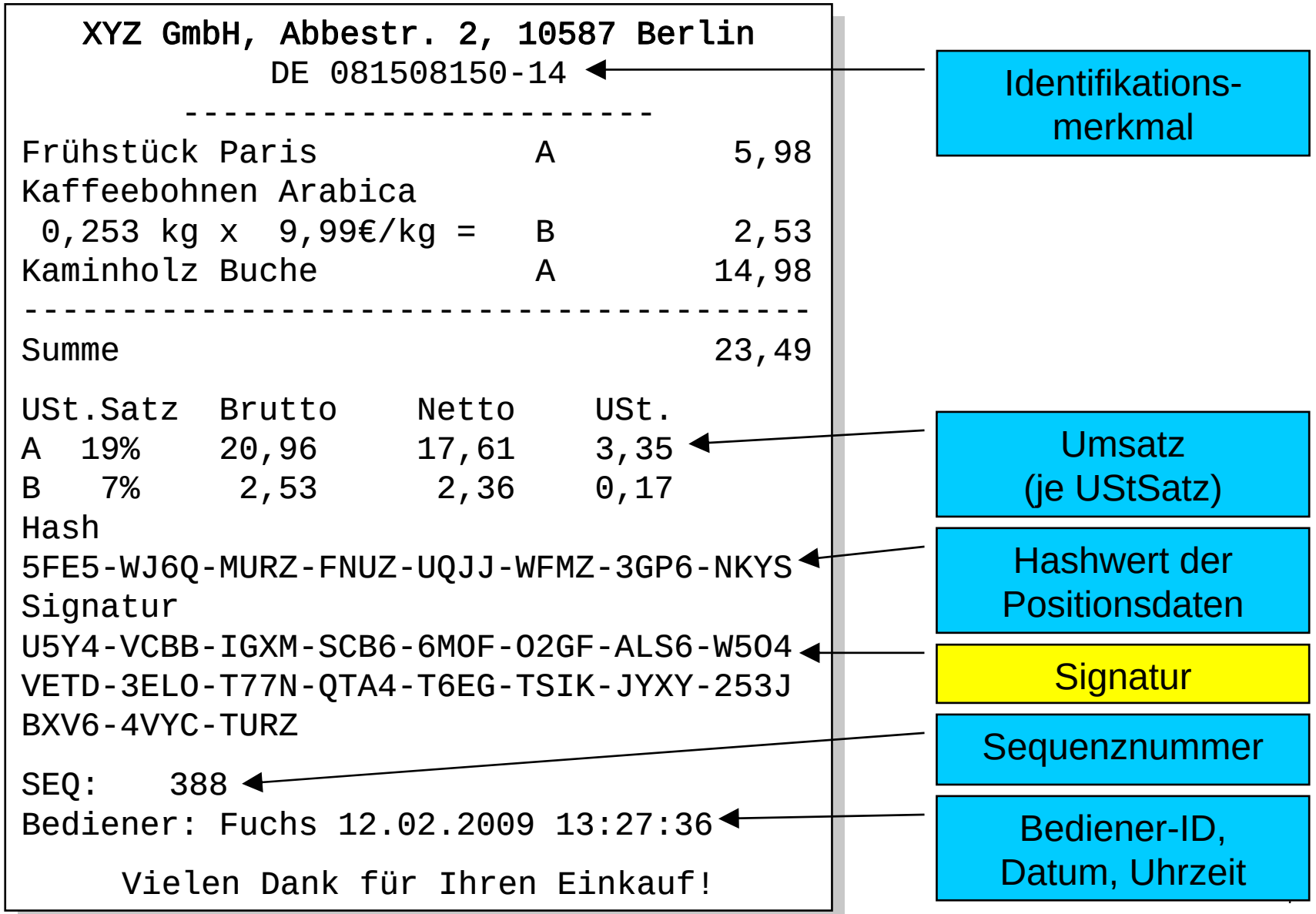
Prüfbare Daten



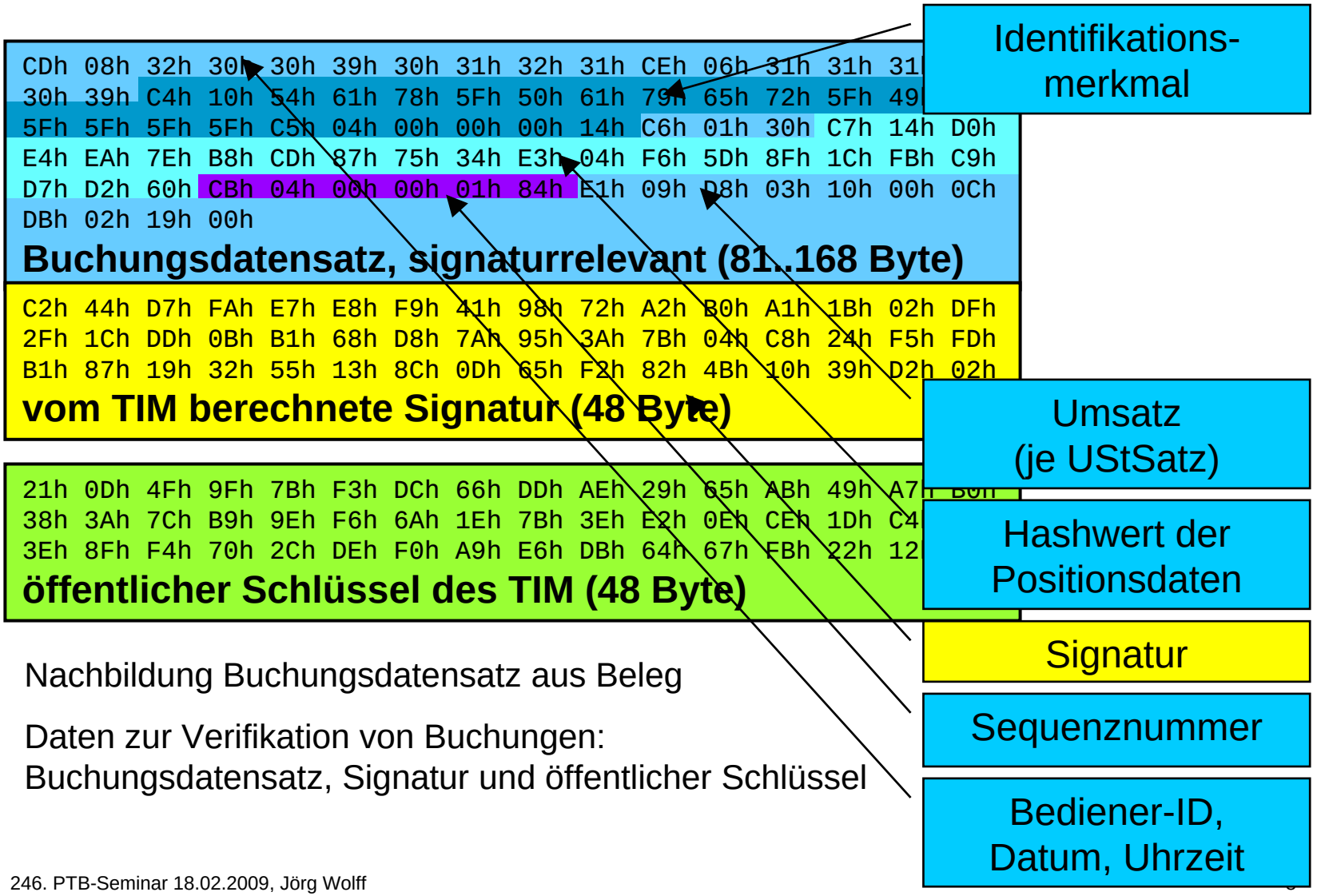
Welche Buchungsdaten werden signiert?



Prüfung von Kassenbelegen anhand Buchungsdaten und Signatur

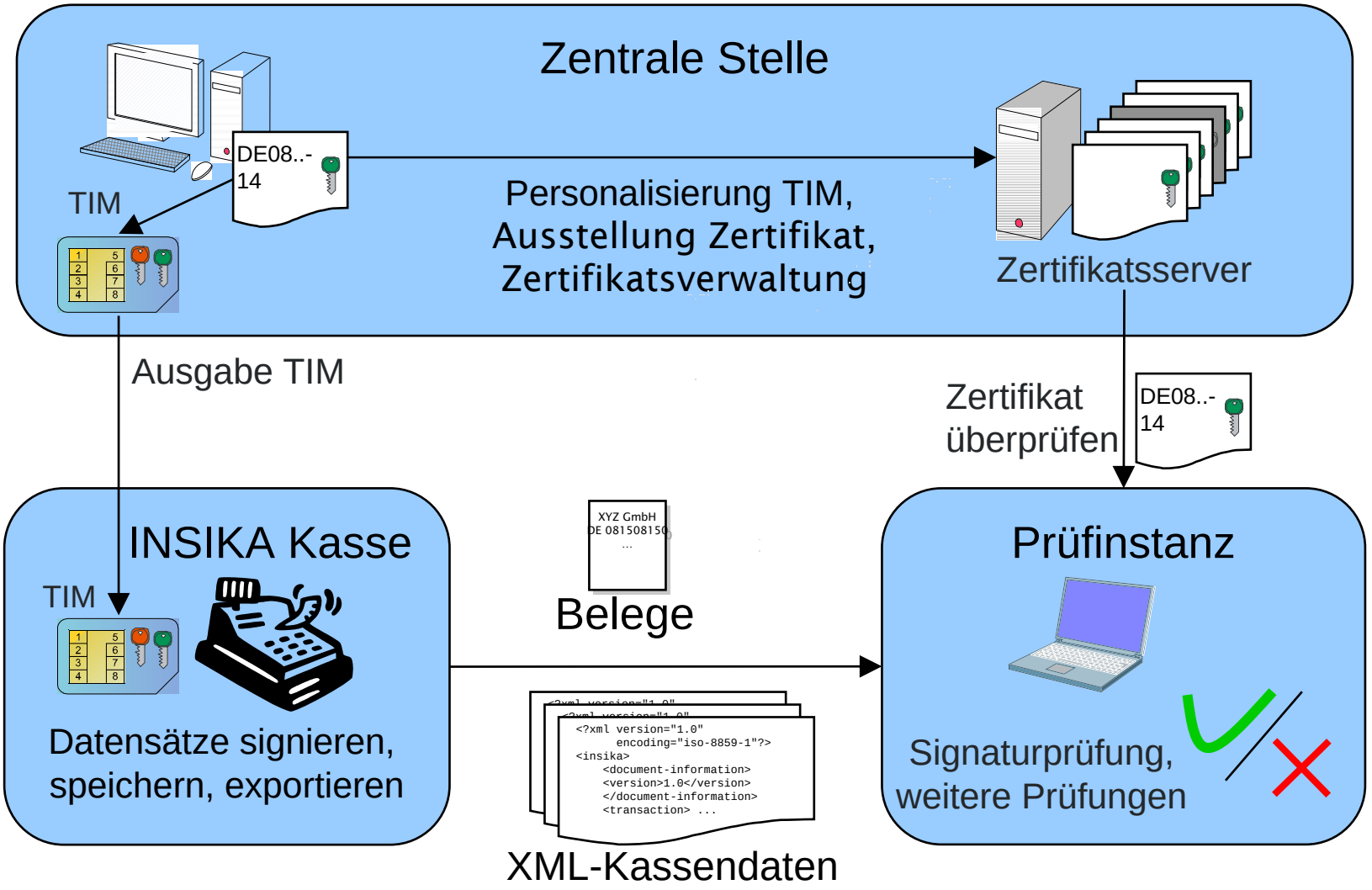


Verifikation von Buchungsdaten

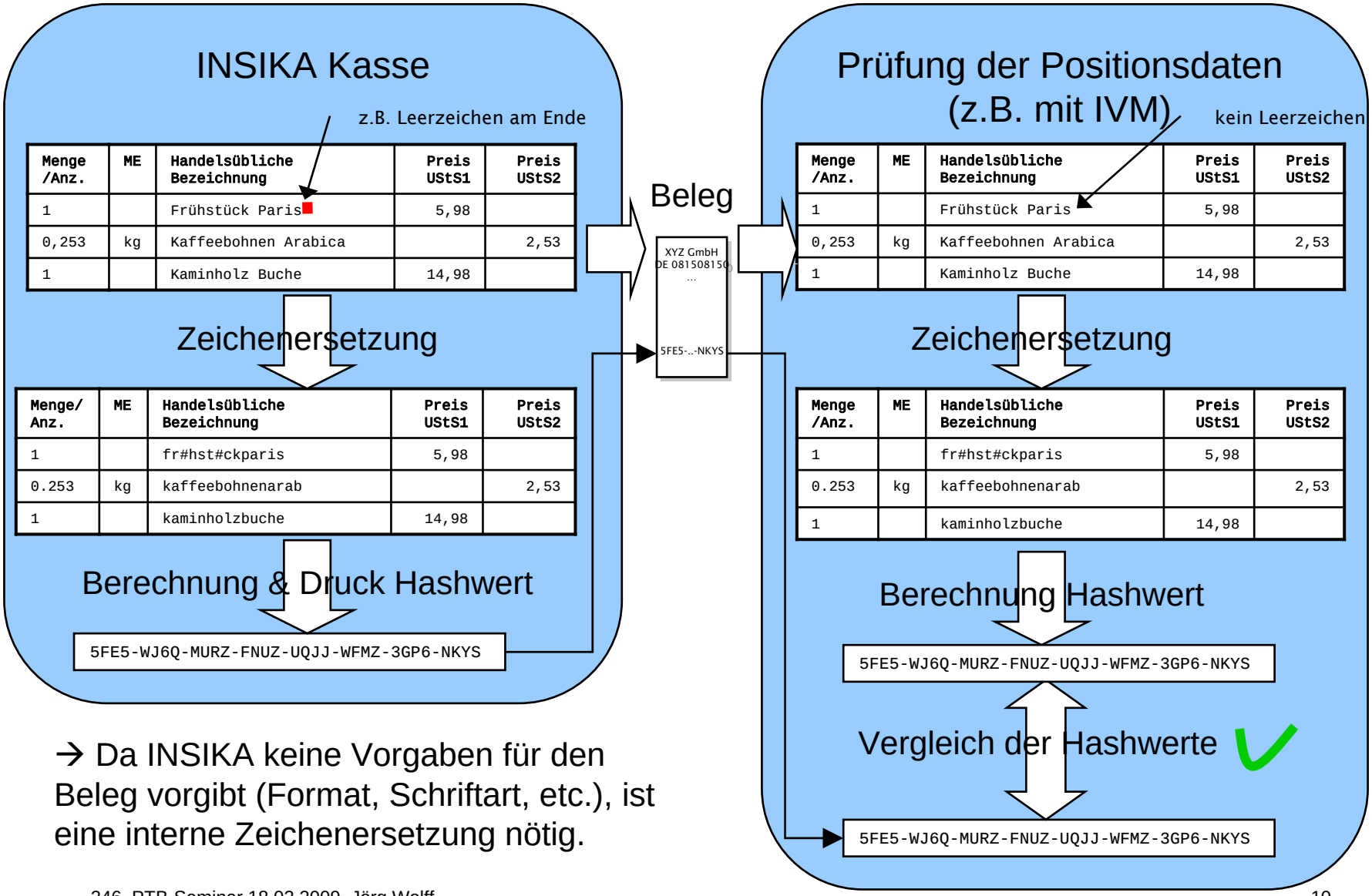


- → Nachbildung Buchungsdatensatz aus Beleg
- → Daten zur Verifikation von Buchungen: Buchungsdatensatz, Signatur und öffentlicher Schlüssel

Zertifikatsverwaltung (vereinfacht)

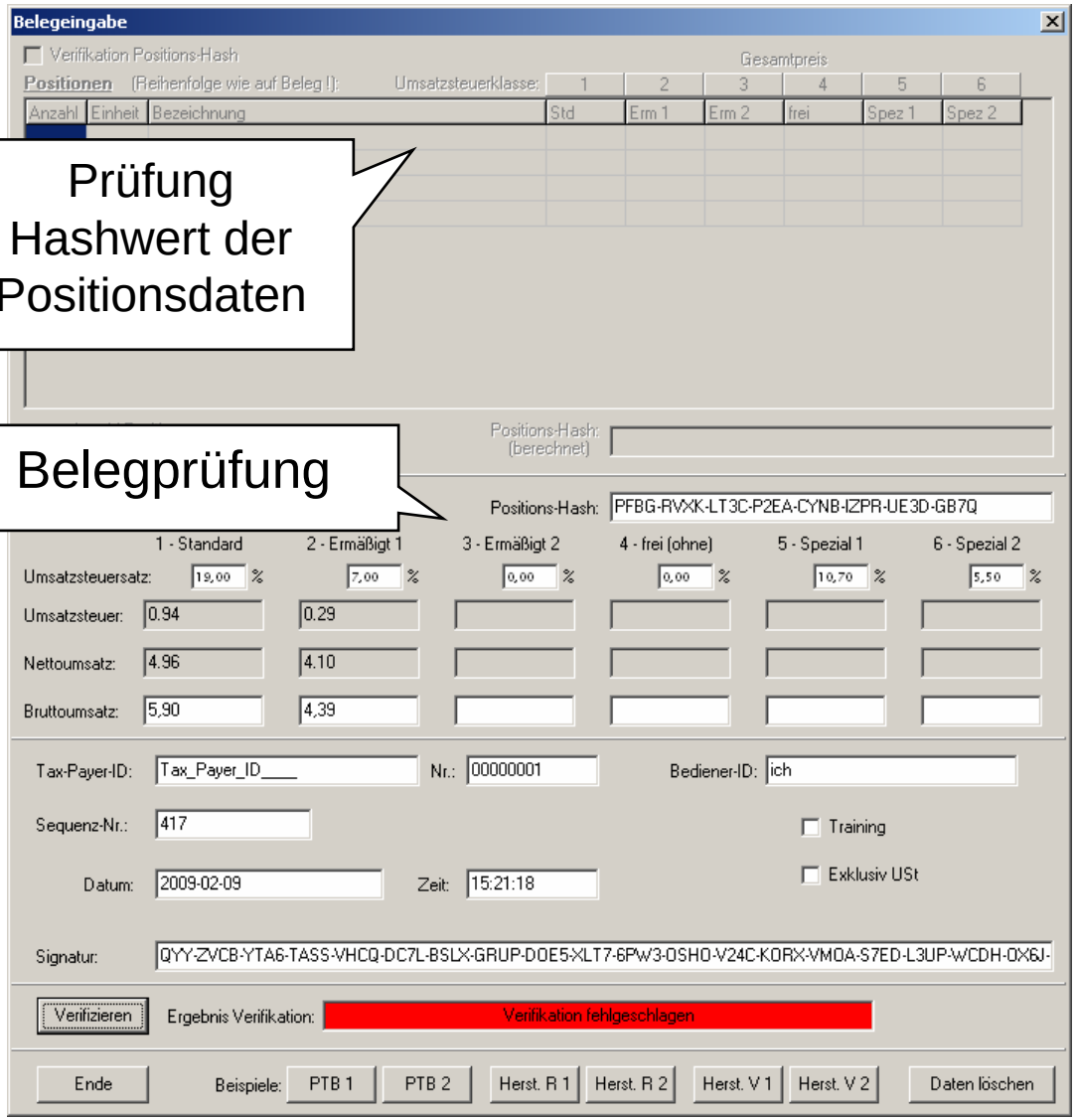


Sonderfall der Belegprüfung: Prüfung der Positionsdaten



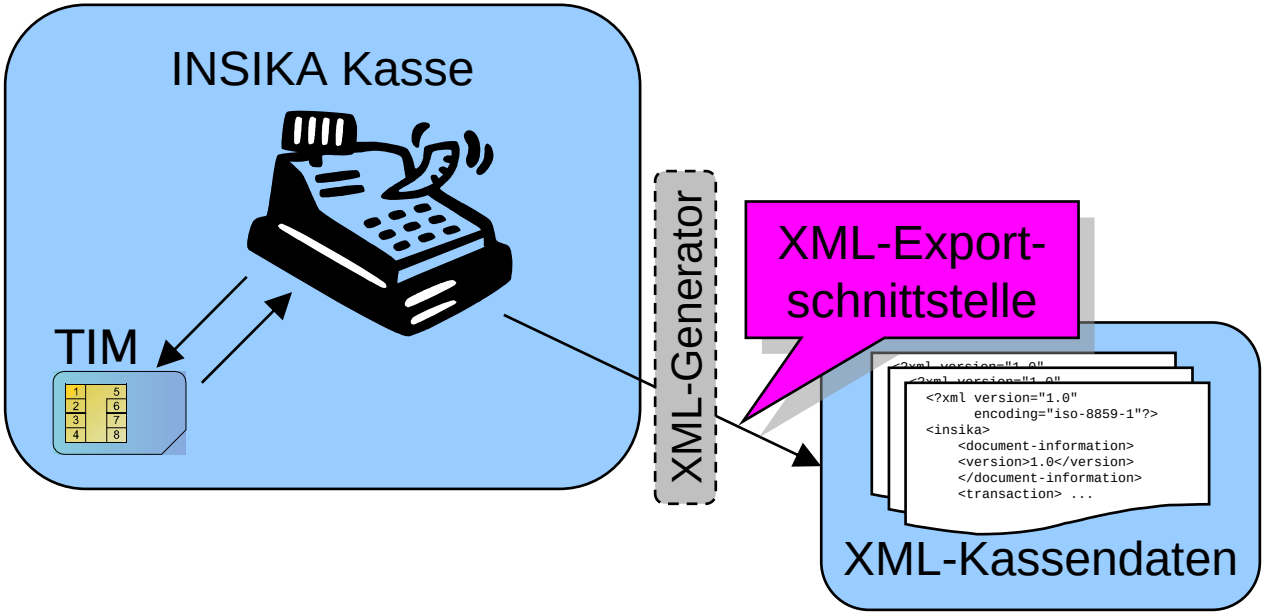
→ Da INSIKA keine Vorgaben für den Beleg vorgibt (Format, Schriftart, etc.), ist eine interne Zeichenersetzung nötig.

IVM-Software: Prüfung von Kassenbelegen



- 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

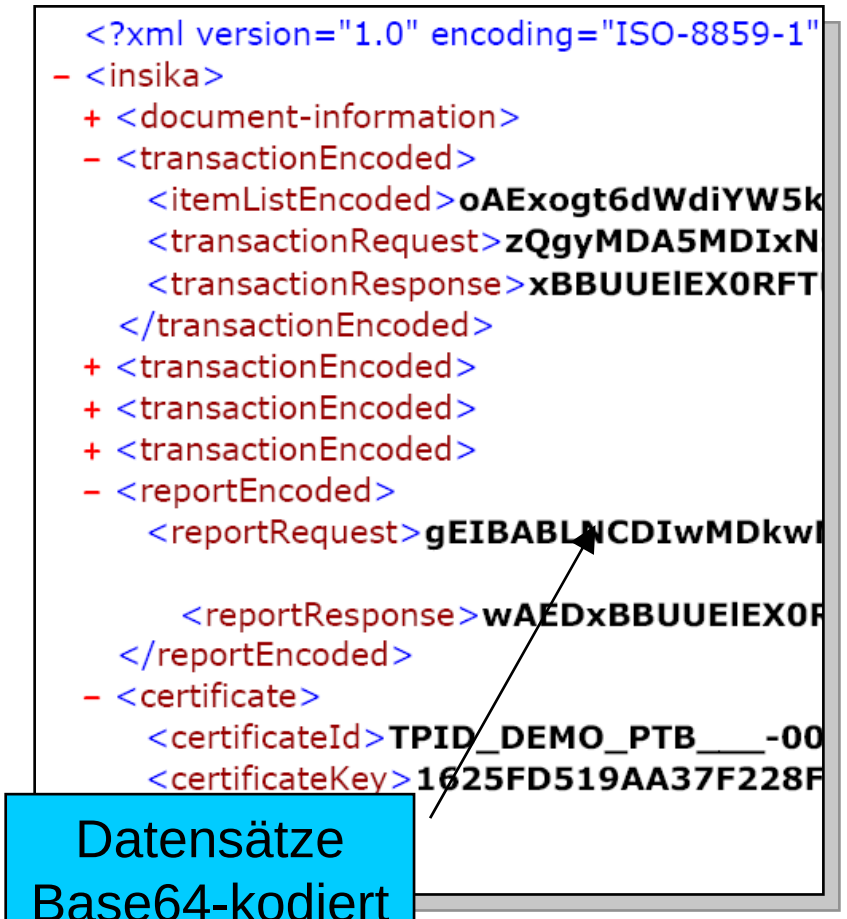
→ INSIKA XML-Exportschnittstelle:
einheitlich, herstellerunabhängig

→ unabhängig von Ort, Plattform und Medium
(Web-Übermittlung, USB-Stick, CD-Rom, Speicherkarten, etc.)

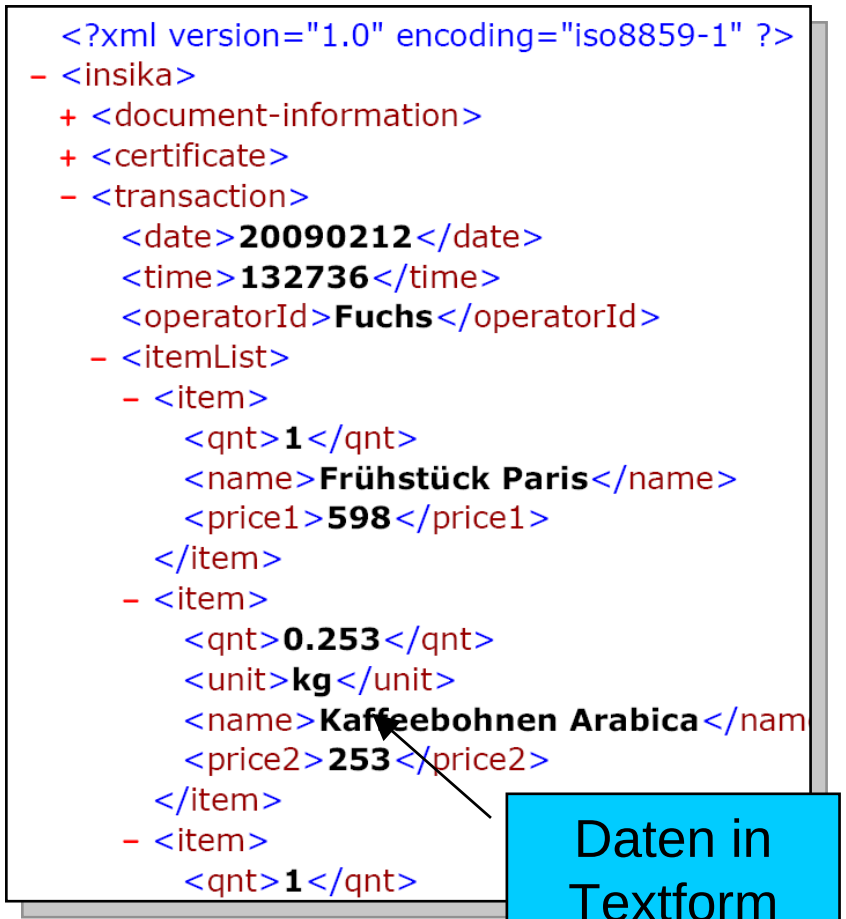
INSIKA XML-Dokumente

- Inhalt von INSIKA XML-Dokumenten:
  - Zertifikate,
  - Buchungen,
  - Tagesabschlüsse
- INSIKA XML-Schema:
  - XML-Schnittstellendefinition
  - Validierung von XML-Dokumenten
- XML-Dokument enthält lesbare Textzeichen → mit Texteditor oder Webbrowser darstellbar
- zwei INSIKA XML-Formate: „Klartext“ und „Base64“

XML-Formate „Base64“ und „Klartext“



Datensätze Base64-kodiert



Daten in Textform

→ zwei Formate definiert, je nach Voraussetzungen der Kasse bedienbar

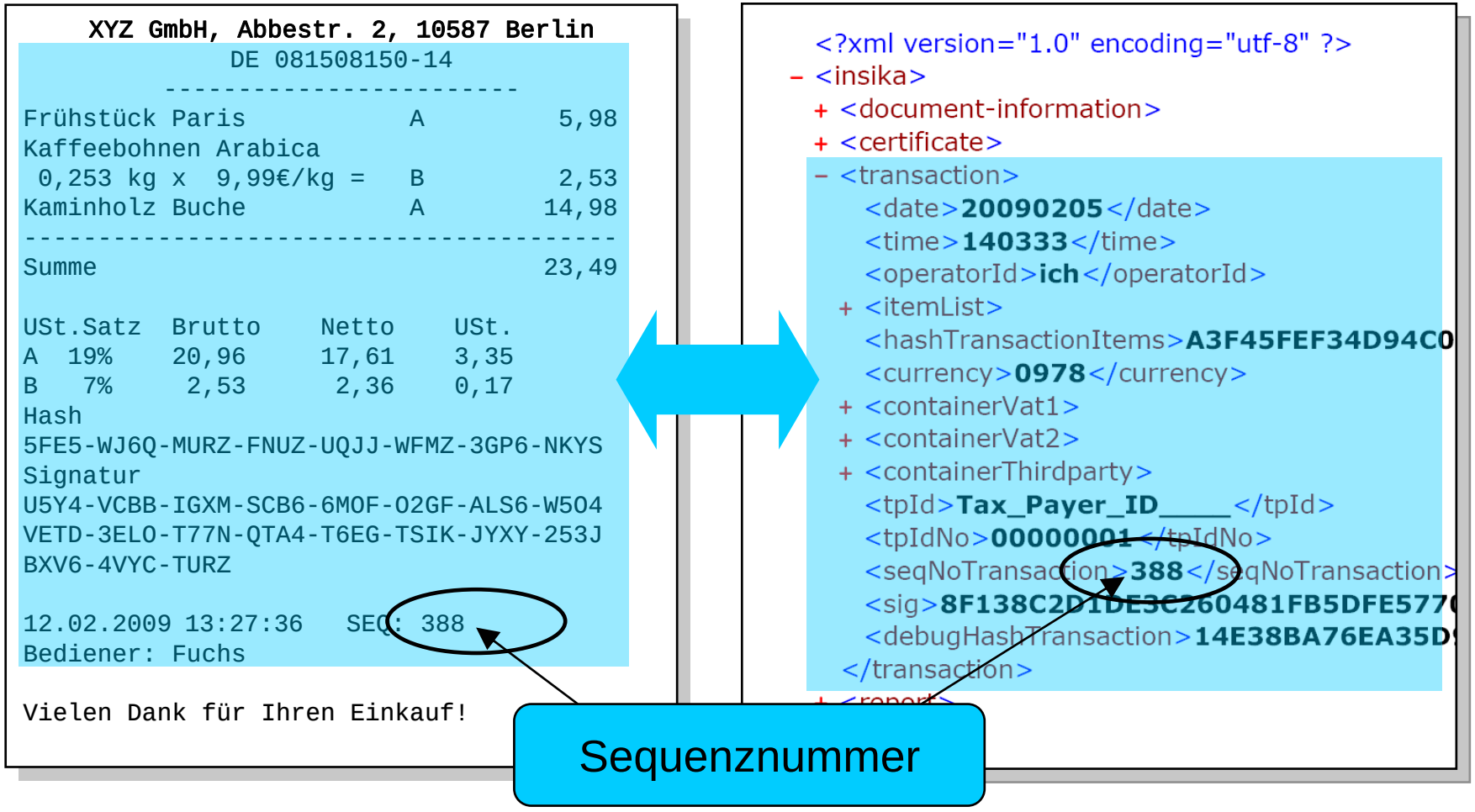
Prüfbare Inhalte von XML-Dokumenten

```
<?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:

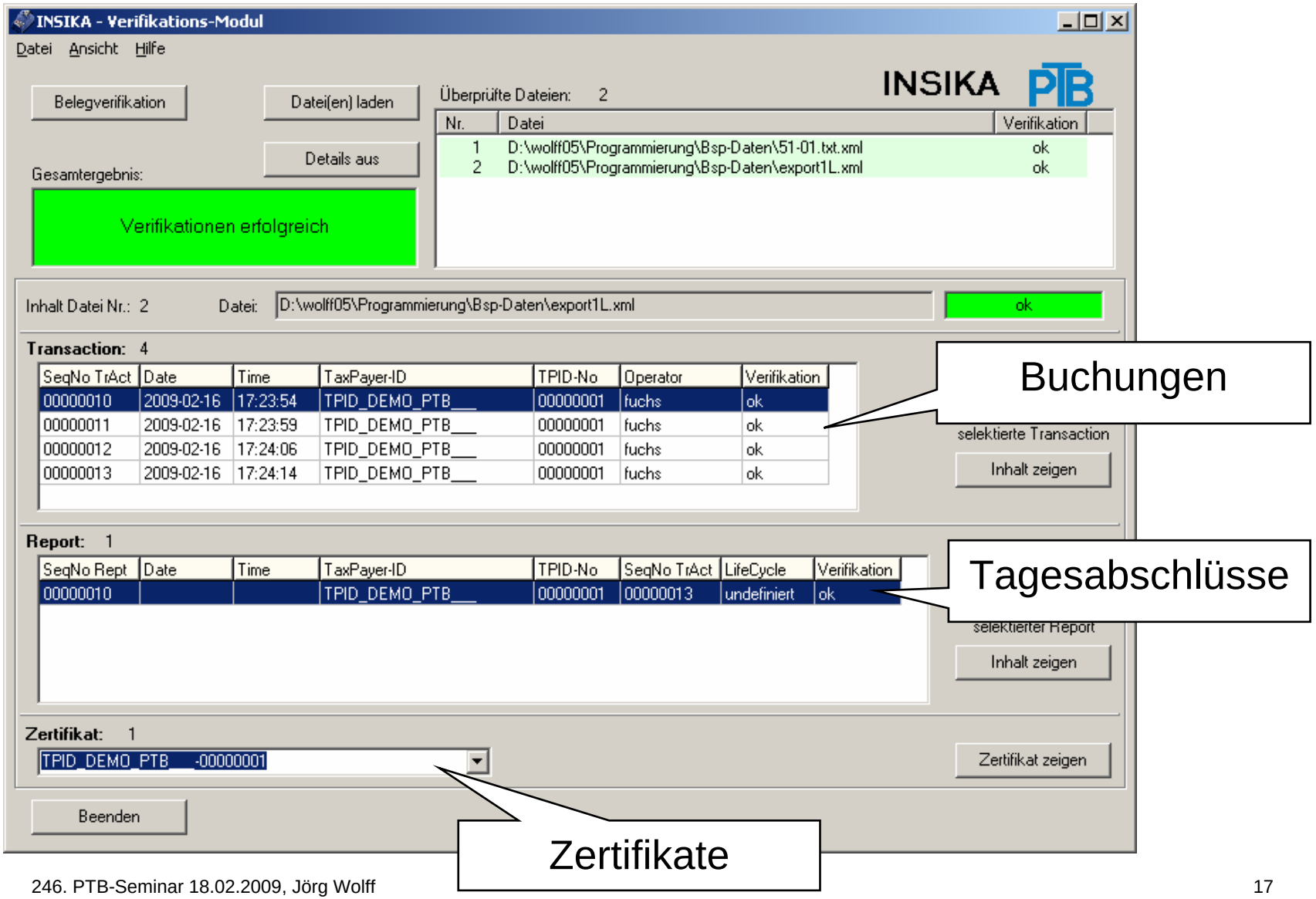
- Gültigkeit Zertifikat
- Buchung:
  - Positionsdaten ←→ Hashwert der Positionsdaten
  - Signatur
- Tagesabschluss:
  - Umsätze ←→ Umsatzsummen der eingeschlossenen Buchungen
  - streng monoton steigende Sequenznummern eingeschlossener Buchungen
  - Signatur

Zuordnung von Beleg und XML-Exportdaten

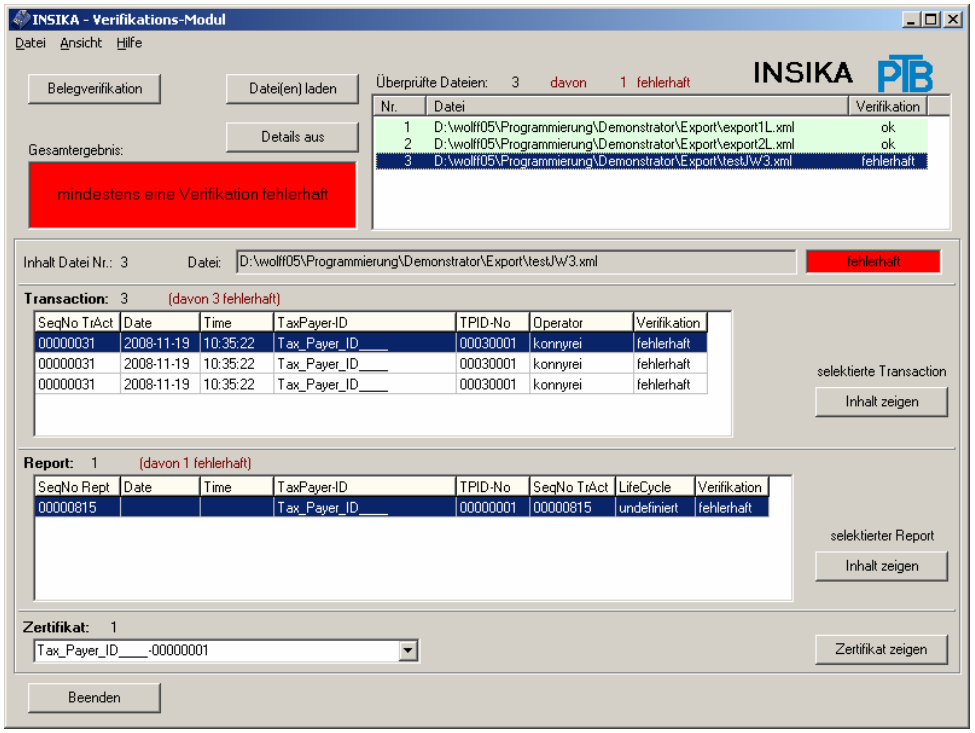


→ eindeutige Rückführbarkeit von Beleg auf XML-Exportdaten durch Identifikationsmerkmal und Sequenznummer

INSIKA Verifikations Modul (IVM)



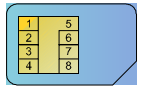
INSIKA Verifikations Modul (II)

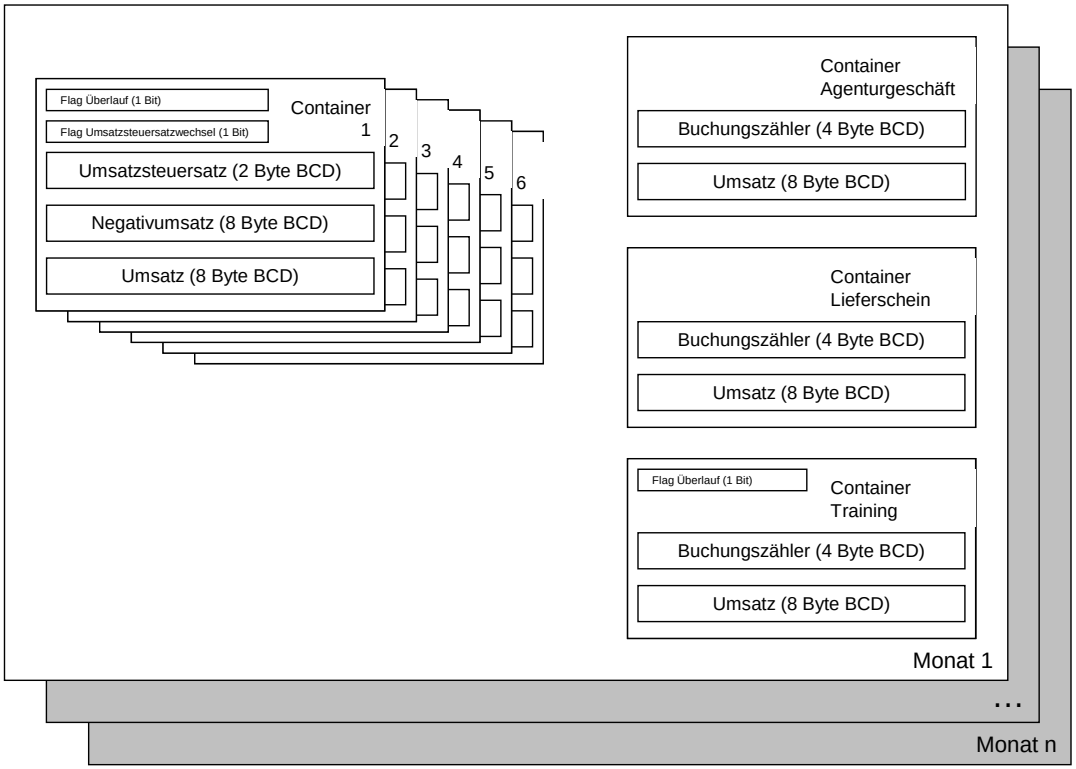


- nutzt veröffentlichte und frei zugängliche Verfahren
- Nachbau einer Verifikationssoftware für INSIKA-Daten ohne größere Probleme möglich

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

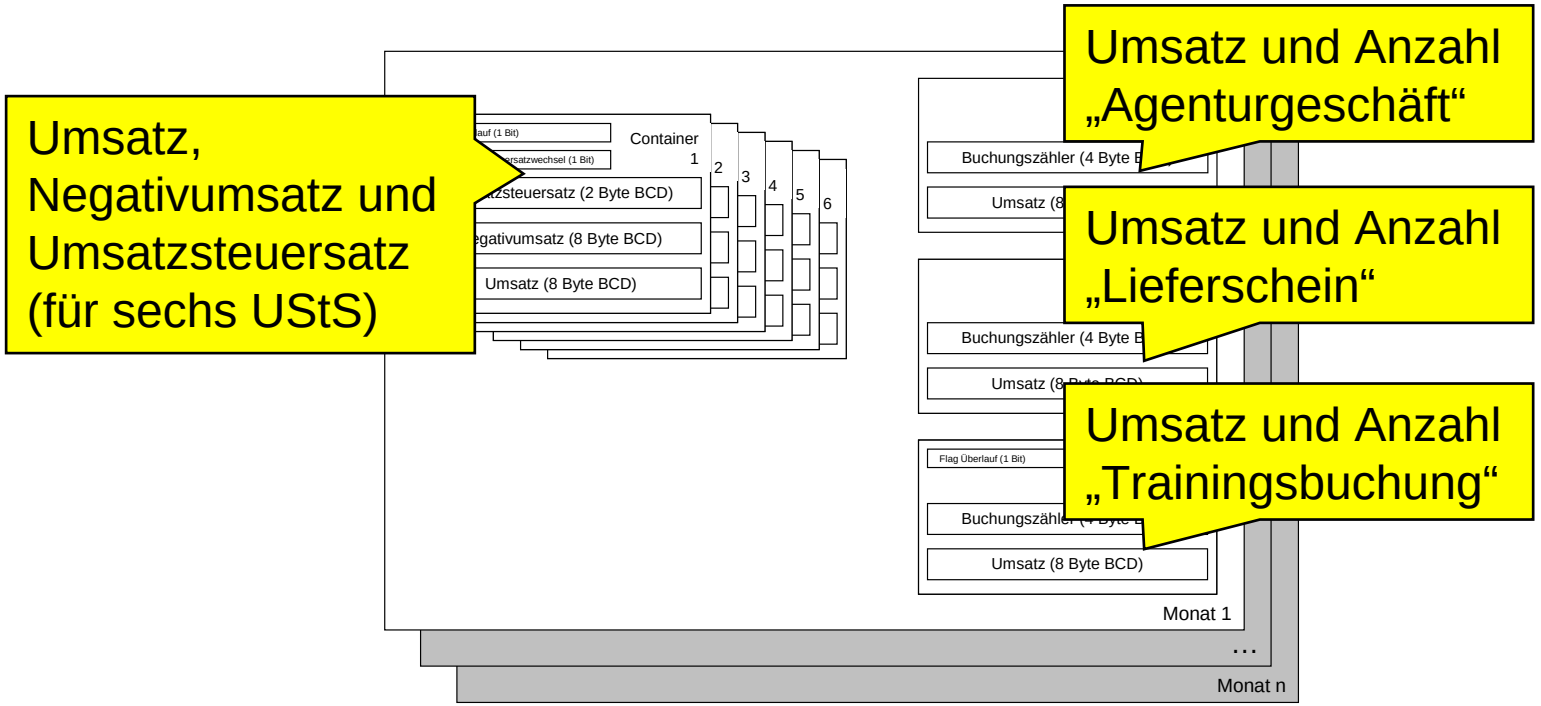
Prüfung der TIM Summenspeicher





- 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)

Prüfung der TIM Summenspeicher (II)



- 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 Prüfszenario

1. Anforderung von XML-Exportdaten vom Kassenbetreiber 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 ←→ Exportdaten)
   - Belegprüfung anhand Buchungsdatensatz, 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!