INSIKA – A new approach against tax frauds at ECRs

Norbert Zisky
Physikalisch-Technische
Bundesanstalt

Jörg Wolff
Physikalisch-Technische
Bundesanstalt

Mathias Neuhaus
cv cryptovision

Content

- **Background**
- **Technical concept**
- **Technical details**
- **Verification**
- **Summary**

Background

Germany on the way to fiscal solutions

Big problems in tax compliance were indicated in 2003 – Nobody knows the exact loss of money for the society.

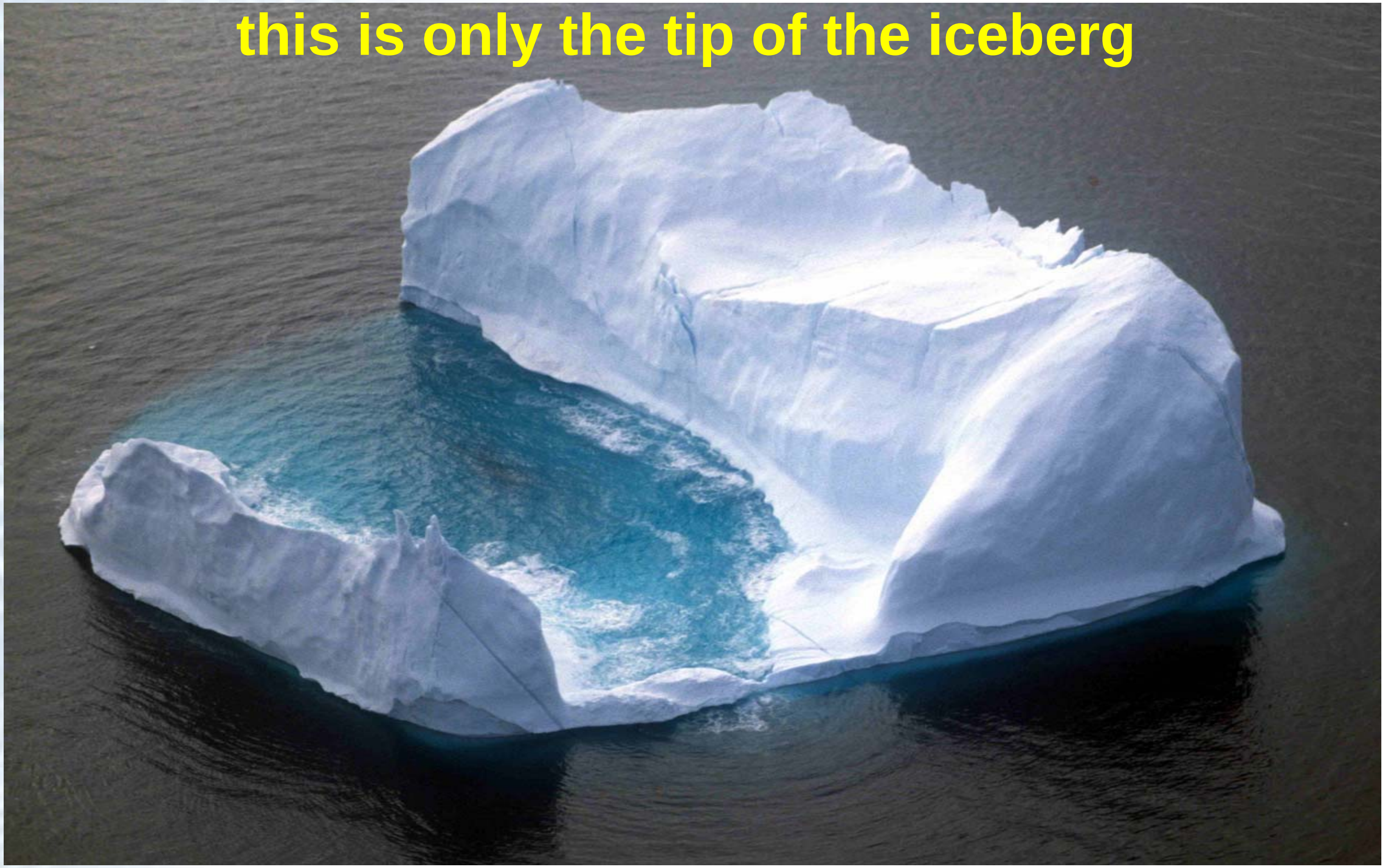
- The Federal Audit Office (BRH) has complained that current models of electronic cash registers and cash management systems fail to meet the principles of correct accounting practices when it comes to recording transactions … The risk of tax fraud running into *many billions* [of euro] should not be underestimated in cash transactions
- **The German Ministry of Finance had to find a solution for this problem**
- **In 2004 PTB proposed the new concept**

Background

Possibilities of Manipulation

- Using functions for service technicians
  (e.g. setting of Z-report-counter or grand total)
- Misuse of training functions
- Using report generators
  (e.g. suppression of voids in printout)
- Direct data modification in files or data bases
  (PC-based systems)

But !



Source: Ansgar Walk, Creative Commons-License Attribution ShareAlike 2.5

Manipulation of ECR Data

A global problem

Possible Solutions

- Better market observation
- Classical fiscal systems
- Online data transfer of each transaction
- New approach in Germany – INSIKA concept

Content

- Background
- **Technical concept**
- Technical details
- Verification
- Summary

Concept – Idea May 2004

Use of cryptographic mechanisms for the protection of ECRs against manipulation

- Finance authorities distribute signature devices and operating instructions for ECR and POS systems
- Finance authorities define sets of data to be signed and data structures
- Manufacturers integrate the signature devices into ECR and POS systems
- Tax audit starts with testing the integrity and plausibility of the tax data by verifying signatures

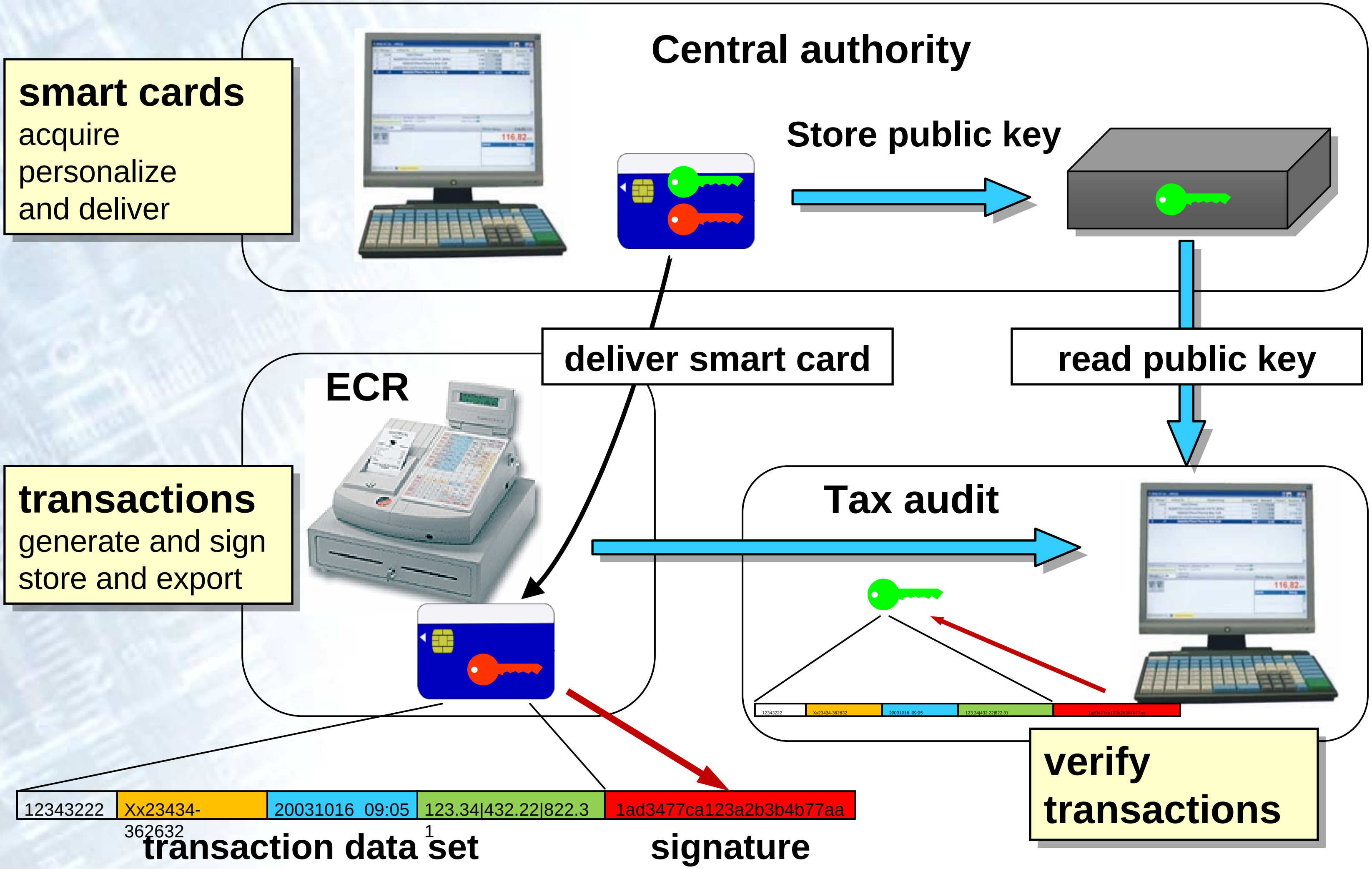
Concept – Basic idea

Simple basic idea:

- Compulsory recording of all transactions
- Access to electronic data for tax auditors
- Protection against manipulation using digital signatures
- In case of data loss estimation possible, using totalizers on smart card

⇨ **Use existing rules and procedures for POS systems with added manipulation protection**

Concept – System architecture



smart cards
acquire
personalize
and deliver

Central authority

Store public key

deliver smart card

read public key

ECR

transactions
generate and sign
store and export

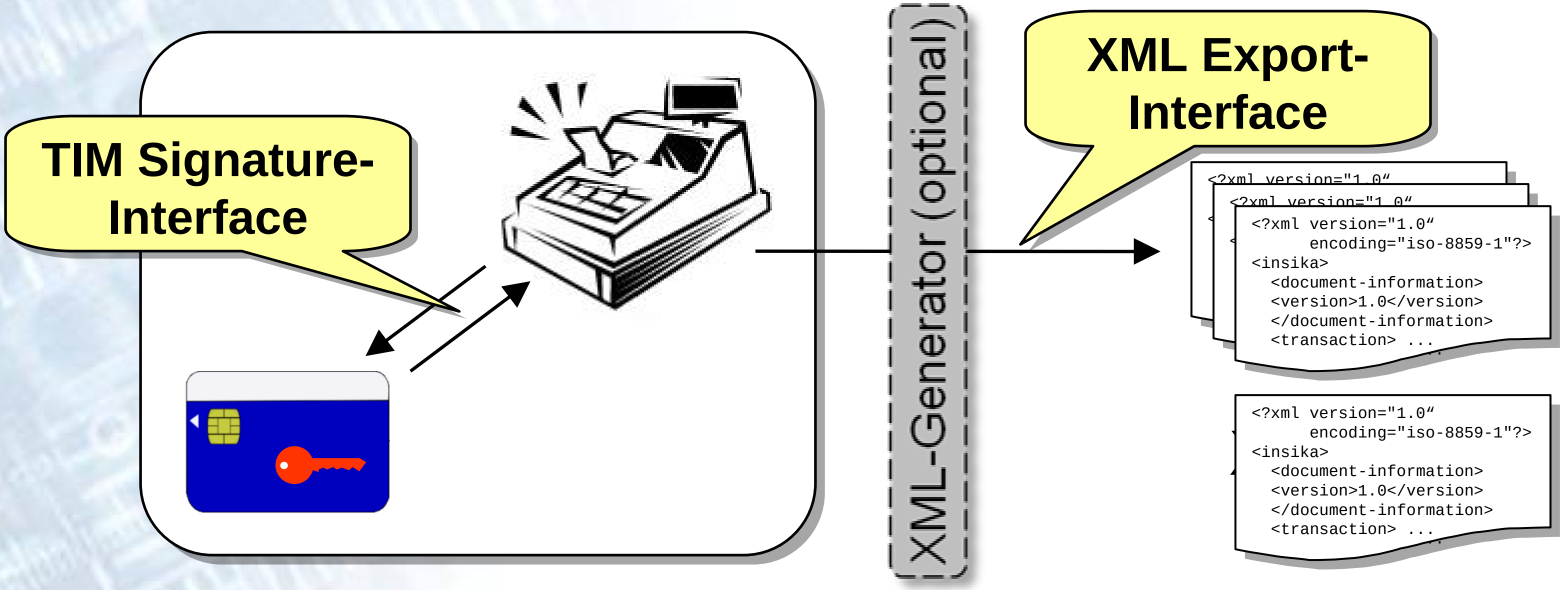
Tax audit

verify transactions

12343222	Xx23434-362632	20031016 09:05	123.34|432.22|822.31	1ad3477ca123a2b3b4b77aa

transaction data set **signature**

Concept – INSIKA Interfaces



```
<?xml version="1.0"
      encoding="iso-8859-1"?>
<insika>
  <document-information>
  <version>1.0</version>
  </document-information>
  <transaction> ...
```

```
<?xml version="1.0"
      encoding="iso-8859-1"?>
<insika>
  <document-information>
  <version>1.0</version>
  </document-information>
  <transaction> ...
```

Signature Device – TIM

- calculates digital signatures (SHA-1, ECC 192 bit)
- safe memory of private key
- management of sequence numbers
- Memory for turnover sums

- **INSIKA defines the TIM Signature and the XML Export interfaces only**
- **there are no specific requirements on the ECR's journal**
- **XML Data can be built by an additional XML-Generator**

Content

- Background
- Technical concept
- **Technical details**
- Verification
- Summary

Details – Transaction and Receipt

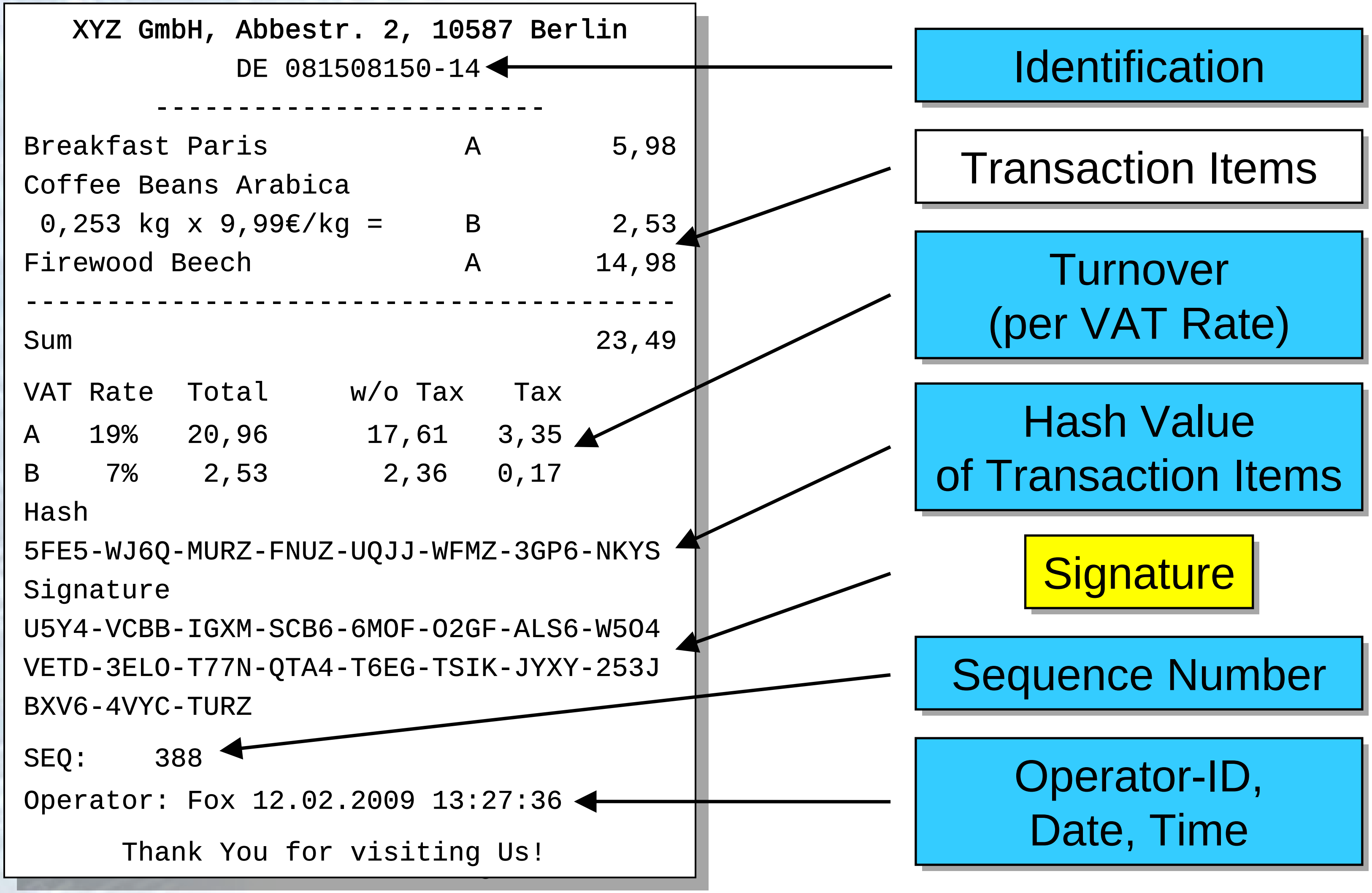
- Data of transaction and on receipt are the same
  signature of transaction = signature on receipt
- With the help of a sequence number the correspondence is defined definitely
- Transaction data can be stored durable on user-defined electronic media

Source: Everaldo Coelho and YellowIcon

Source: Ocrho, Creative Commons-License Attribution ShareAlike 2.5

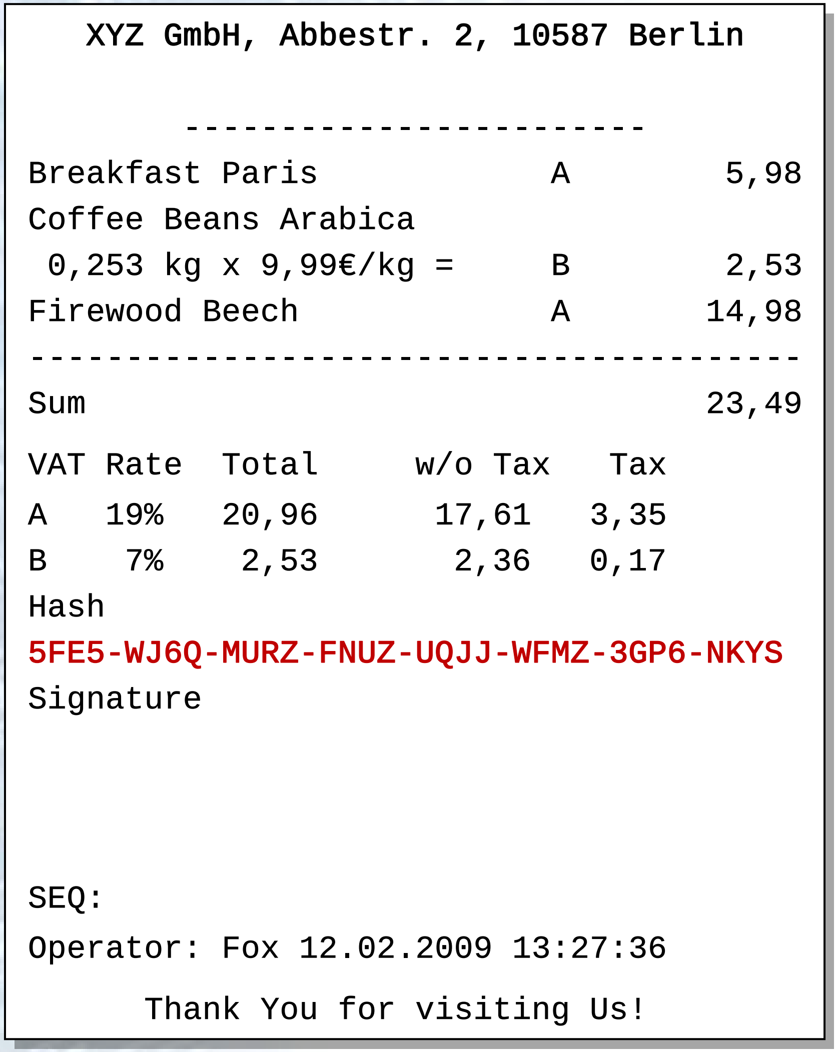
Source: Wikipedia, GNU Public

Details – Signed data elements



```
   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!
```

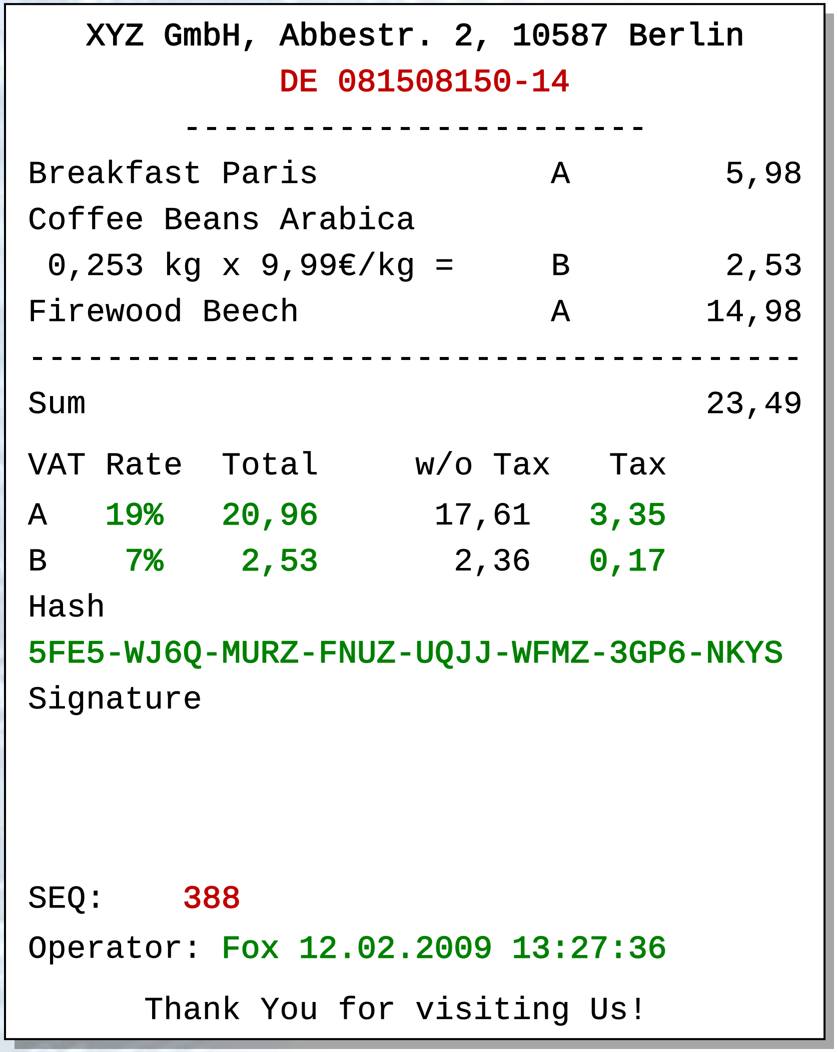
Details – Signature procedure (1)



```
    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:
Operator: Fox 12.02.2009 13:27:36
      Thank You for visiting Us!
```

Step 1:
Calculate hash value
of transaction items

Details – Signature procedure (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




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

      Thank You for visiting Us!
```

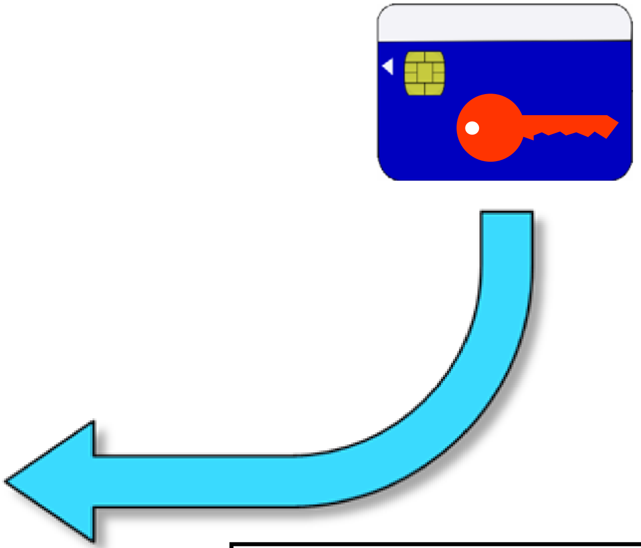
Step 2:
Send data set to TIM

Hash value	5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WFMZ-3GP6-NKYS
Date and Time	12.02.2009 13:27:36
Turnover (normal VAT)	20,96 (19% 3,35)
Turnover (reduced VAT)	2,53 (7% 0,17)
Operator	Fox
Elements added to set of data by TIM	
Sequence no.	388
Identification	DE 081508150-14

Details – Signature procedure (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!
```

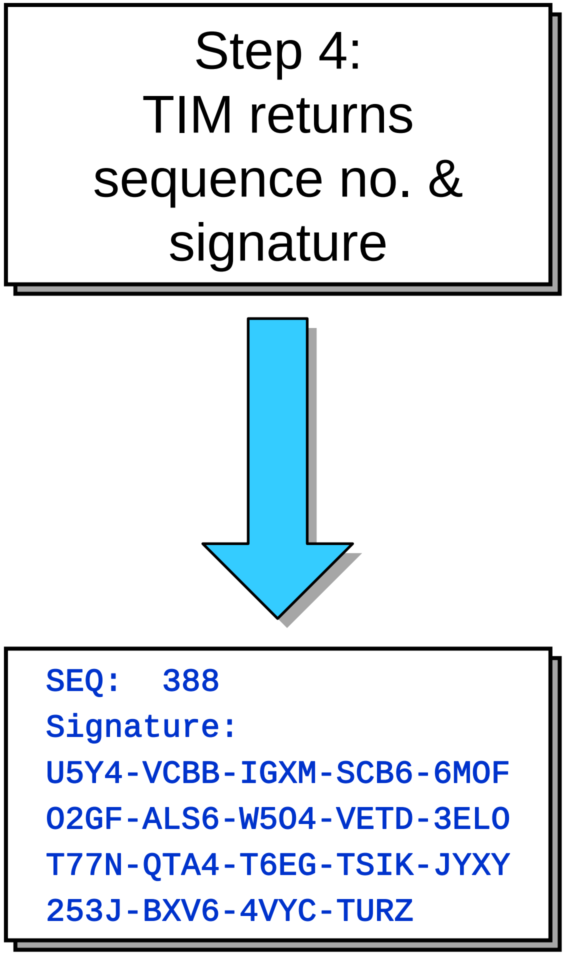
Step 3a:
TIM verifies & signs
turnover data



Step 3b:
TIM updates
totalizers

Details – Signature procedure (4)

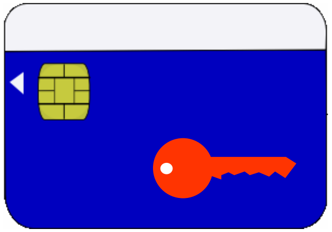
```
      XYZ GmbH, Abbestr. 2, 10587 Berlin
                DE 081508150-14
            ------------------------
Breakfast Paris            A        5,98
Coffee Beans Arabica
 0,253 kg x 9,99€/kg =     B        2,53
Firewood Beech             A       14,98
----------------------------------------
Sum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



Step 4:
TIM returns
sequence no. &
signature

```
SEQ:  388
Signature:
U5Y4-VCBB-IGXM-SCB6-6MOF
O2GF-ALS6-W5O4-VETD-3ELO
T77N-QTA4-T6EG-TSIK-JYXY
253J-BXV6-4VYC-TURZ
```

Details – INSIKA TIM (1)

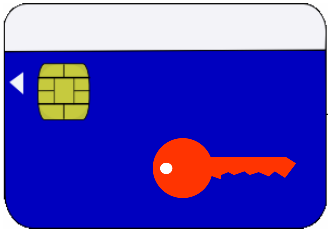


TIM Functions

- Verifies Turnover Data and VAT
- Signs Turnover Data
- Records Turnover Data
- Uniquely and immutably identifies
  - the Tax Payer
  - each Transaction
- Generates Reports of Turnover Data

Details – INSIKA TIM (2)

Secured against Manipulations

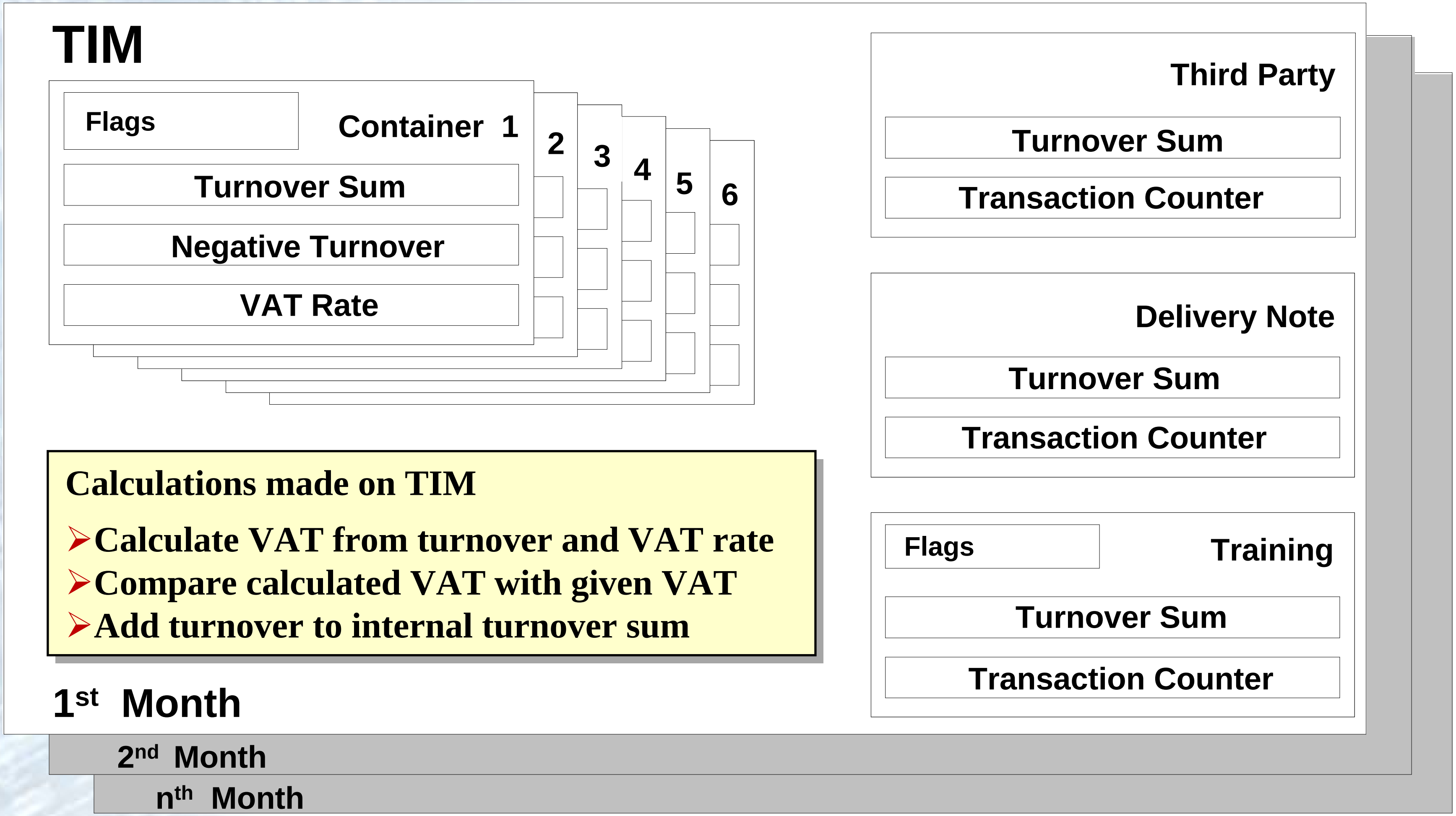


- “Read Only” Memory for all Data
- Key Pair is generated on the TIM Smart Card
- Secure Storage of the Private Key
- Unique Serial Number (Hardware based)

Reference Implementation of TIM

- Siemens CardOS V4.3b 64 KB Smart Card
- cryptovision ECC-Package
- INSIKA TIM-Package
- Uses SHA-1 and 192 Bit ECC
- Other ECC Parameters and Hash Algorithm possible

Details – TIM Totalizers (1)



TIM

Flags

Container 1

2

3

4

5

6

Turnover Sum

Negative Turnover

VAT Rate

Calculations made on TIM

- Calculate VAT from turnover and VAT rate
- Compare calculated VAT with given VAT
- Add turnover to internal turnover sum

1st Month

2nd Month

nth Month

Third Party

Turnover Sum

Transaction Counter

Delivery Note

Turnover Sum

Transaction Counter

Flags

Training

Turnover Sum

Transaction Counter

Details – TIM Totalizers (2)

Totalizers on TIM deliver turnover data even if the journal is lost (or deleted on purpose)

- Each set of totalizers records turnovers, training transactions, VAT rates etc.
- Memory of TIM allows multiple sets of totalizers
  - 121 monthly totalizers for ten years since smart card distribution
  - 6 containers for 6 coexistent VAT rates
  - Flags for overflow and VAT rate changes

TIM provides a built-in automatic back-up for most important data

Details – Changes to ECR systems

Few changes required in existing ECR systems and back-office software:

➢ECR systems must be able to create the required electronic journal (must be “self-contained”: evaluation must be possible without access to any other data)

➢Software for transfer to PC and for further processing must be made available for all users (low-cost-solution)

➢Memory extension for data storage in the ECR system might be needed (to work without frequent transfer of sales data to a PC)

⇨ **ECR systems comply with “good accounting practices”**

Cost for ECR manufacturers (1)

Simple external smart card reader

- Connection of external smart card reader or full integration
- Suitable especially for PC based ECR/POS systems
- Single-unit end-user price less than € 25

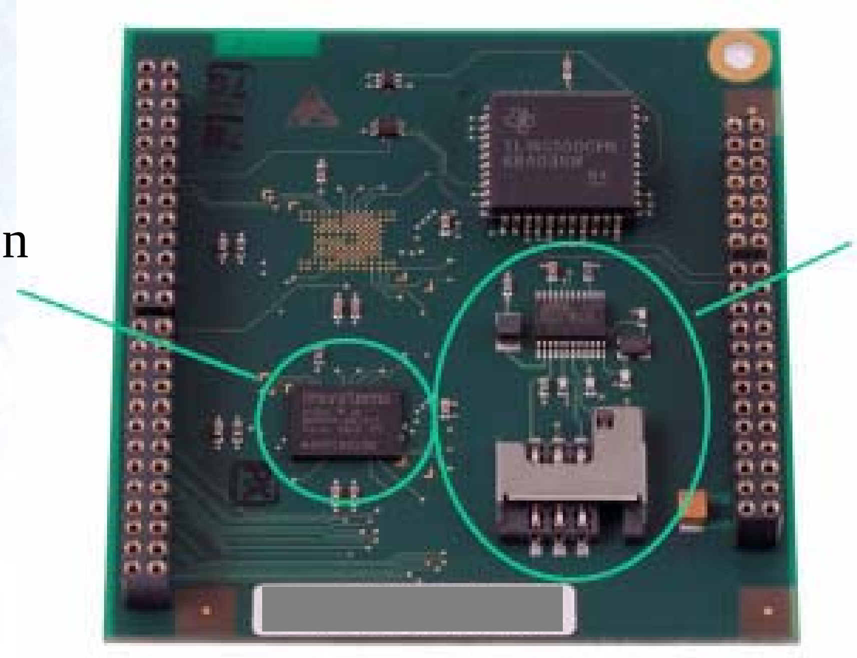
Smart card

(10 €)

Cost for ECR manufacturers (2)

Hardware

- Memory extension approx. 5-10 €



Card reader unit and controller

approx. 10 €

Smart card

(10 €)

Software

- Triggering of smart card
- Changing / Adoption of data bases
- Support of export interface

Details – Central points

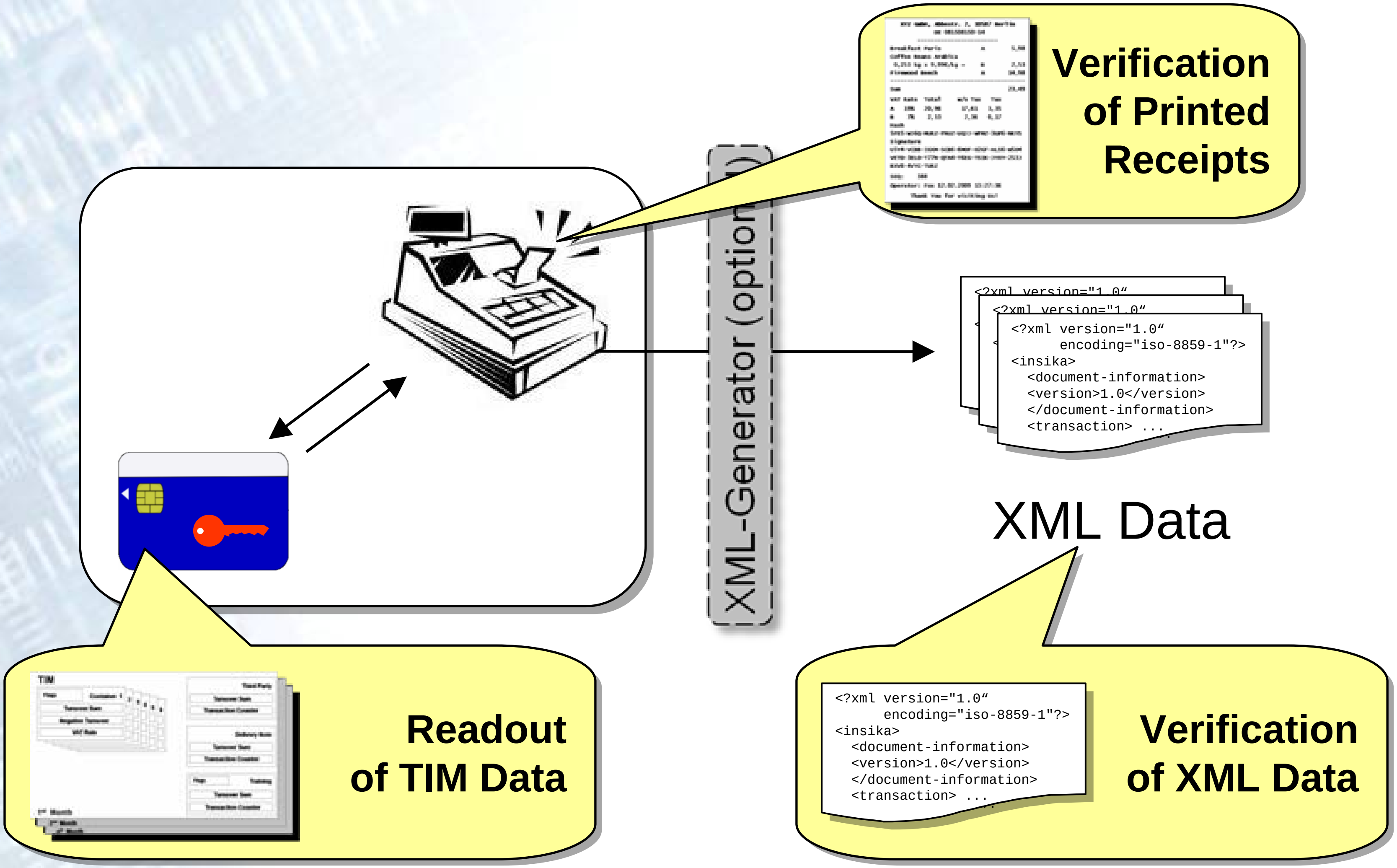
Main elements of the solution:

- Electronic journal
- Manipulation-proof through digital signature (smart card)
- Printed receipt can be verified by digital signature
- Evaluation of ECR/POS data with common instruments (software-based analysis of transactions)
- Totalizers in smart card contain information about total sales even if journal data gets lost
- Audits not relying on „traditional“ reports (like transaction report, PLU report etc.)
- Technically quite simple – no unnecessarily high (and therefore expensive) demands

Content

- Background
- Technical concept
- Technical details
- **Verification**
- Summary

Verification – Verifiable Data



Verification of Printed Receipts

XML-Generator (optional)

```
<?xml version="1.0“
      encoding="iso-8859-1"?>
<insika>
  <document-information>
  <version>1.0</version>
  </document-information>
  <transaction> ...
```

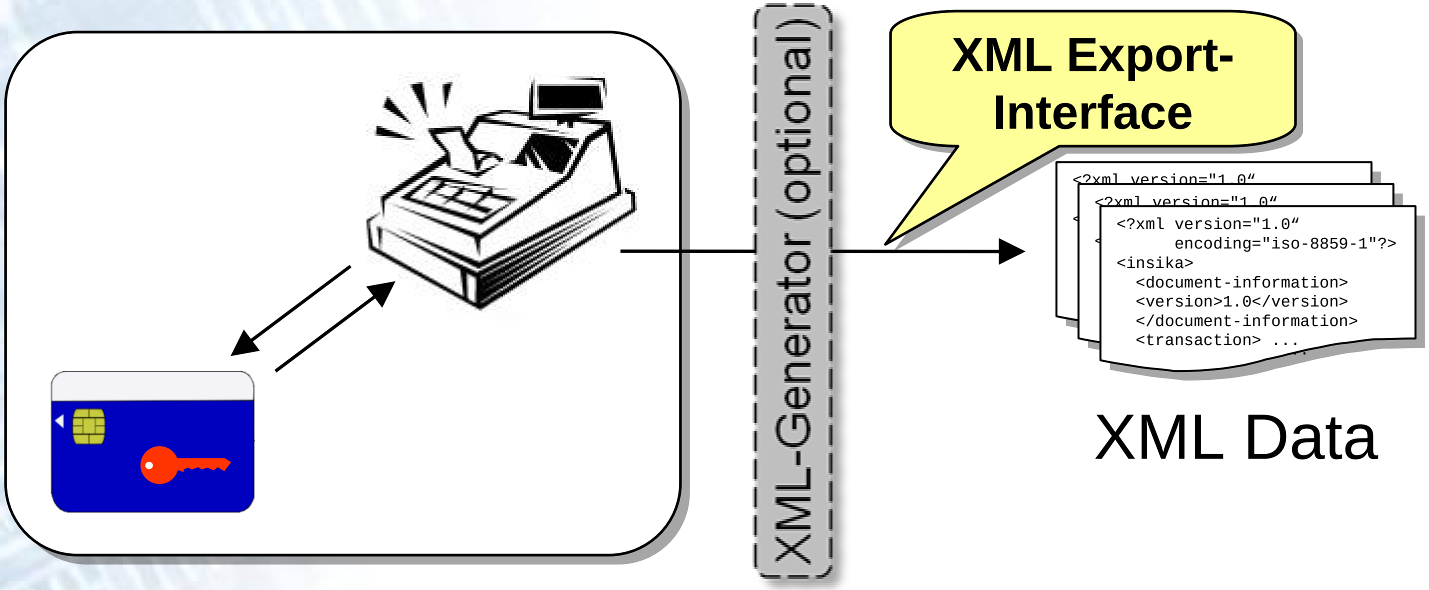
XML Data

Readout of TIM Data

```
<?xml version="1.0“
      encoding="iso-8859-1"?>
<insika>
  <document-information>
  <version>1.0</version>
  </document-information>
  <transaction> ...
```

Verification of XML Data

Verification – XML Export Interface

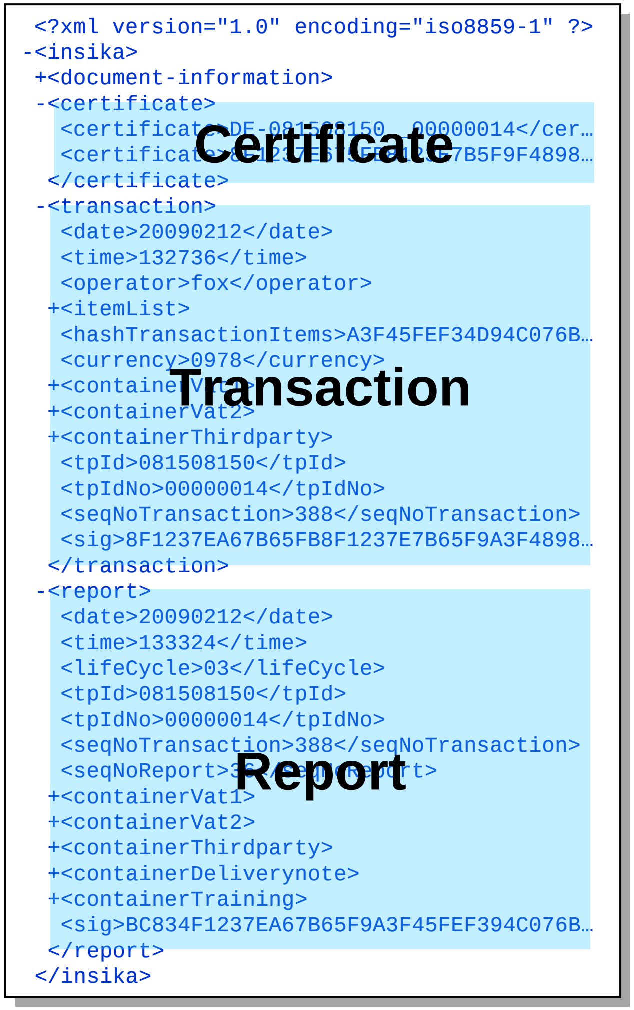


```
<?xml version="1.0“
      encoding="iso-8859-1"?>
<insika>
  <document-information>
  <version>1.0</version>
  </document-information>
  <transaction> ...
```

- **XML = Extensible Markup Language standardized in W3C Recommendation**
- **INSIKA XML Export-Interface:**
  - **uniform, independent of manufacturers**
  - **independent of location, platform and medium (transmission via Internet, USB-stick, CD-R, memory card etc.)**

Verification – XML Documents

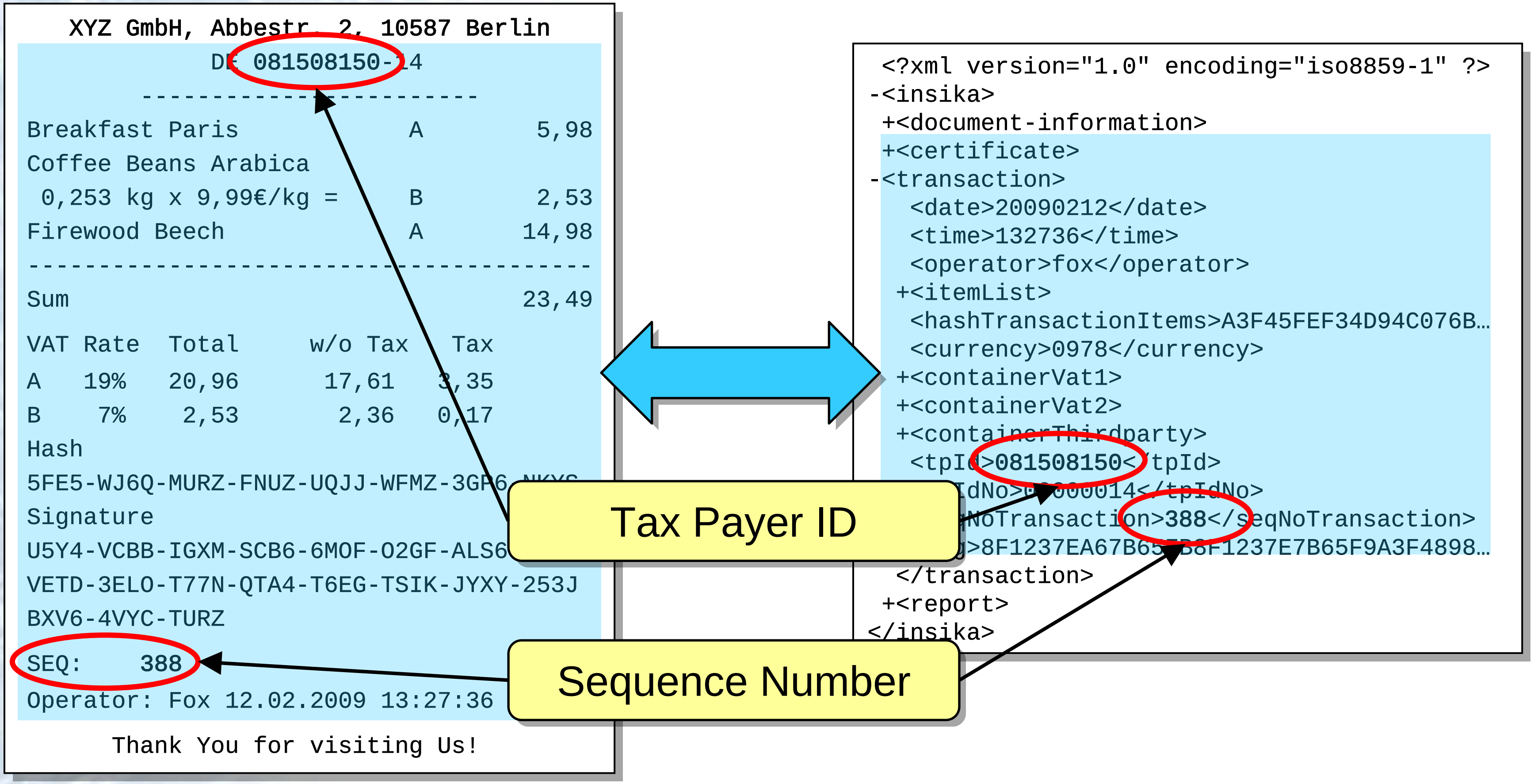
- Content of INSIKA XML documents
  - certificate(s),
  - transaction(s),
  - report(s)
- INSIKA XML schema
  - defines the XML interface
  - allows for the validation of XML documents
- XML documents contain text characters only, can be displayed with any text editor or web browser
- Two different INSIKA XML document types: „Base64“ & „Plaintext“



```
 <?xml version="1.0" encoding="iso8859-1" ?>
-<insika>
 +<document-information>
 -<certificate>
   <certificate>DE-081508150_00000014</cer…
   <certificate>8F1237E67B65FB8F1237E7B5F9F4898…
  </certificate>
 -<transaction>
   <date>20090212</date>
   <time>132736</time>
   <operator>fox</operator>
  +<itemList>
   <hashTransactionItems>A3F45FEF34D94C076B…
   <currency>0978</currency>
  +<containerVat1>
  +<containerVat2>
  +<containerThirdparty>
   <tpId>081508150</tpId>
   <tpIdNo>00000014</tpIdNo>
   <seqNoTransaction>388</seqNoTransaction>
   <sig>8F1237EA67B65FB8F1237E7B65F9A3F4898…
  </transaction>
 -<report>
   <date>20090212</date>
   <time>133324</time>
   <lifeCycle>03</lifeCycle>
   <tpId>081508150</tpId>
   <tpIdNo>00000014</tpIdNo>
   <seqNoTransaction>388</seqNoTransaction>
   <seqNoReport>36</seqNoReport>
  +<containerVat1>
  +<containerVat2>
  +<containerThirdparty>
  +<containerDeliverynote>
  +<containerTraining>
   <sig>BC834F1237EA67B65F9A3F45FEF394C076B…
  </report>
 </insika>
```

Certificate
Transaction
Report

Verification – Receipt & XML Data



```
      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
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!
```

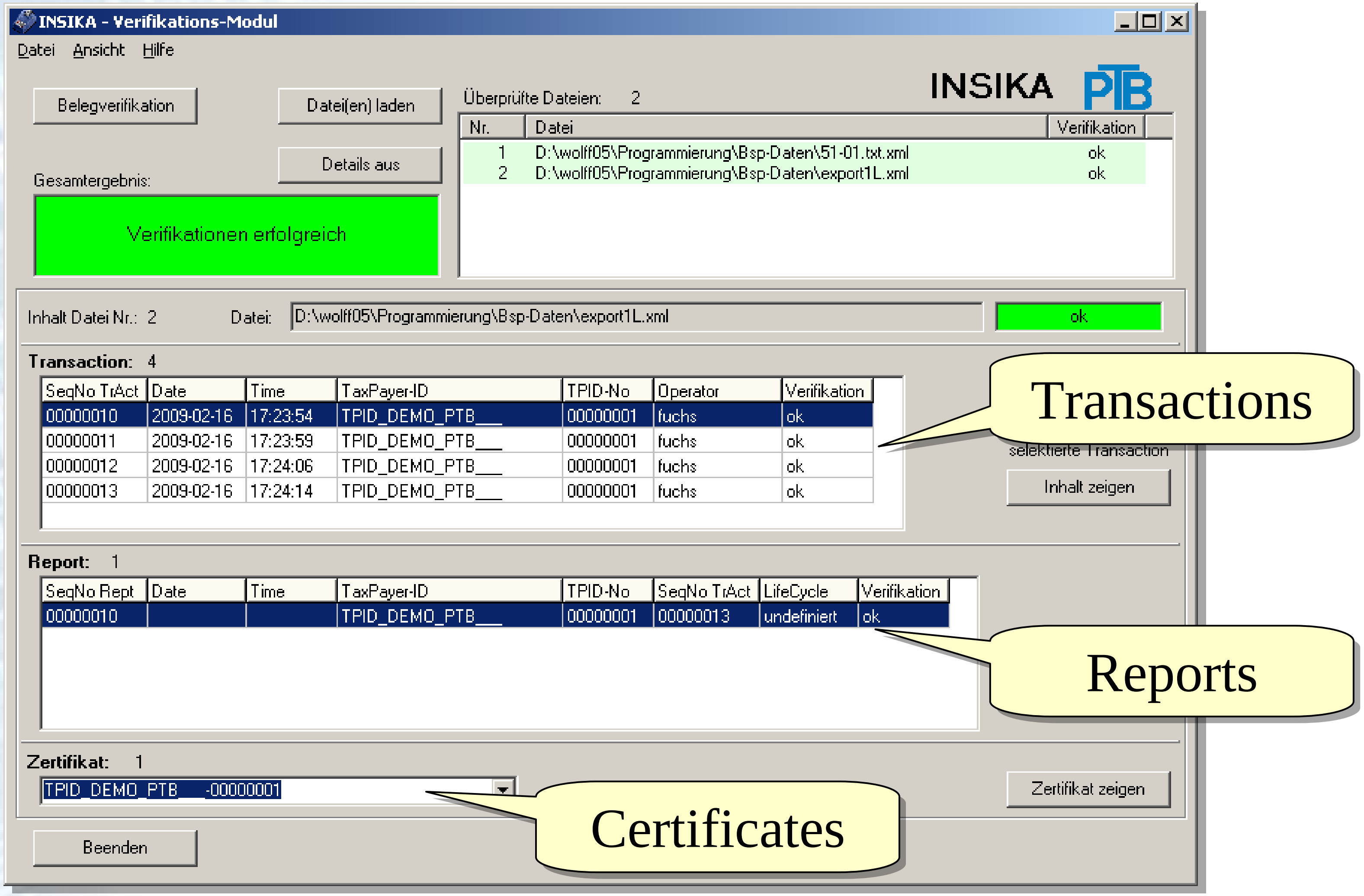
```
 <?xml version="1.0" encoding="iso8859-1" ?>
-<insika>
 +<document-information>
 +<certificate>
-<transaction>
   <date>20090212</date>
   <time>132736</time>
   <operator>fox</operator>
  +<itemList>
   <hashTransactionItems>A3F45FEF34D94C076B…
   <currency>0978</currency>
  +<containerVat1>
  +<containerVat2>
  +<containerThirdparty>
   <tpId>081508150</tpId>
       IdNo>00000014</tpIdNo>
       qNoTransaction>388</seqNoTransaction>
       g>8F1237EA67B657B8F1237E7B65F9A3F4898…
  </transaction>
 +<report>
</insika>
```

Tax Payer ID

Sequence Number

By means of the sequence number and the identification the printed receipt corresponds to the XML data in a definite way.

INSIKA Verification Module (IVM)



Überprüfte Dateien: 2

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

Gesamtergebnis: Verifikationen erfolgreich

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_PTB___	00000001	fuchs	ok
00000011	2009-02-16	17:23:59	TPID_DEMO_PTB___	00000001	fuchs	ok
00000012	2009-02-16	17:24:06	TPID_DEMO_PTB___	00000001	fuchs	ok
00000013	2009-02-16	17:24:14	TPID_DEMO_PTB___	00000001	fuchs	ok

selektierte Transaction

Report: 1

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

Zertifikat: 1

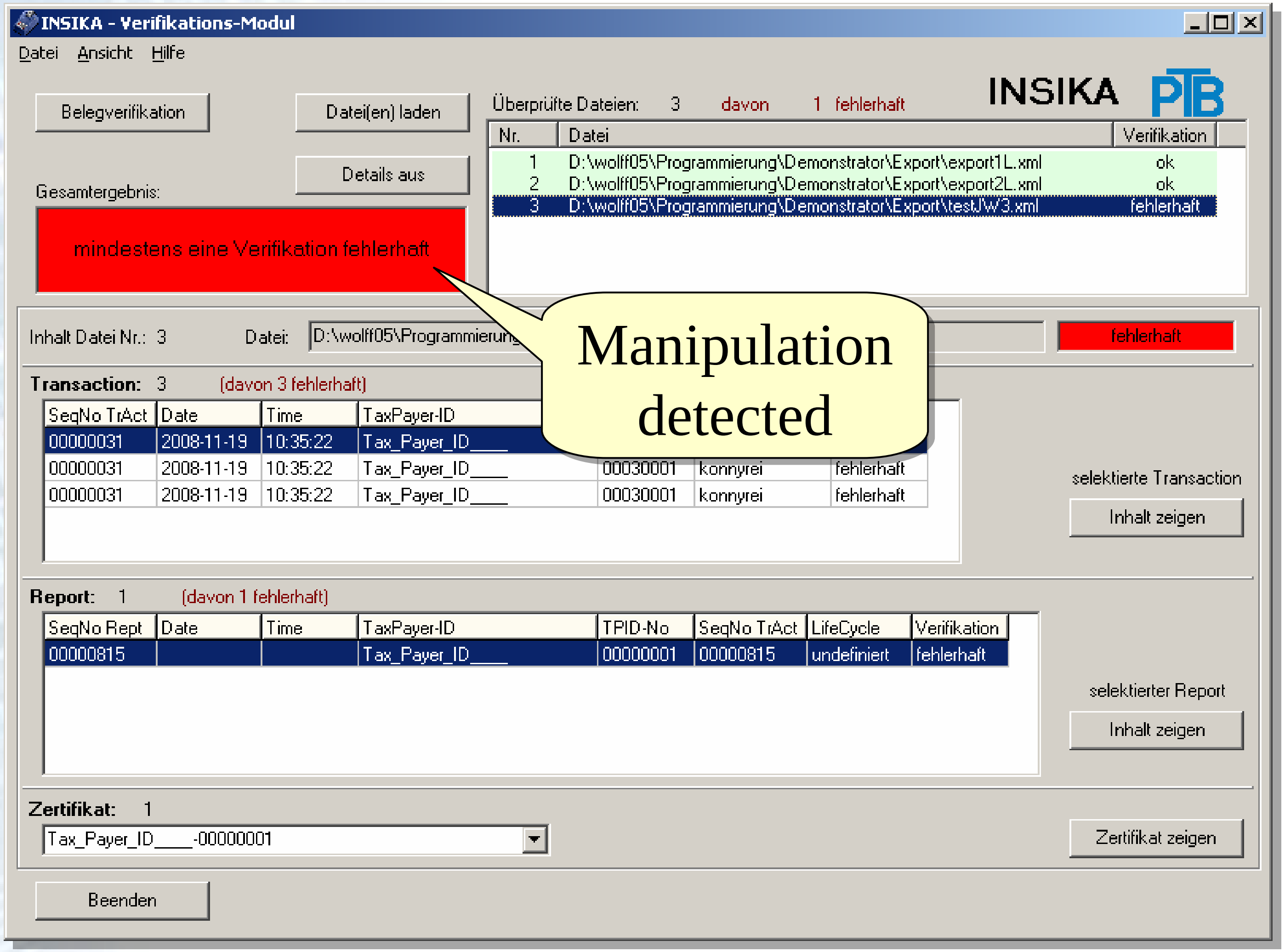
TPID_DEMO_PTB -00000001

Transactions

Reports

Certificates

INSIKA Verification Module



Überprüfte Dateien: 3 davon 1 fehlerhaft

Nr.	Datei	Verifikation
1	D:\wolff05\Programmierung\Demonstrator\Export\export1L.xml	ok
2	D:\wolff05\Programmierung\Demonstrator\Export\export2L.xml	ok
3	D:\wolff05\Programmierung\Demonstrator\Export\testJW3.xml	fehlerhaft

Gesamtergebnis:

mindestens eine Verifikation fehlerhaft

Inhalt Datei Nr.: 3 Datei: D:\wolff05\Programmierung fehlerhaft

Transaction: 3 (davon 3 fehlerhaft)

SeqNo TrAct	Date	Time	TaxPayer-ID			
00000031	2008-11-19	10:35:22	Tax_Payer_ID____			
00000031	2008-11-19	10:35:22	Tax_Payer_ID____	00030001	konnyrei	fehlerhaft
00000031	2008-11-19	10:35:22	Tax_Payer_ID____	00030001	konnyrei	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

Manipulation detected

INSIKA Verification Module

- IVM software can be used to verify signatures of
  - INSIKA XML documents
  - printed receipts
- INSIKA uses published, standardized and open accessible methods (ISO 7816, SHA1, ECDSA,..)
- It’s no problem to build your own verification software for INSIKA

Content

- Background
- Technical concept
- Technical details
- Verification
- **Summary**

Summary - Advantages

- General structure working well for „fiscal journal“
- Absolute tamper-proof ECR/POS data – “end to end” security
- Data files instead of paper rolls
- Automated verification possible – saving a lot of time
- Authenticity check of paper receipts easily possible
- Upgrade of old systems possible and inexpensive
- Data is secured cryptographically and not physically – Remote data transfer, E-Mail etc. easily possible
- Central data management is possible in chain-operations – no visit of each outlet required during tax audit

Summary - Outlook

- INSIKA-system is ready to use
  - TIM has a stable state
  - Interfaces spec’s freely available on request
- System is under international discussion
  see publications by
  - Richard Ainsworth (USA) or
  - Erich Huber (A)
- Field test planned this year
- Every country can use the system as an alternative
  to expensive fiscal boxes

Summary – Further Information

For further information please visit
http://www.insika.de/

or contact Dr. Norbert Zisky at

norbert.zisky@ptb.de