

**Protection of POS systems
and measurement systems against
manipulations**

**Norbert Zisky
Physikalisch-Technische Bundesanstalt**

- History
- Problem
- Solution
- Presentation of the technical concept
- Current situation of the needed technique
- Expenditure of money and technique
- Planned tax audit procedures
- Dates for technical point of view
- Conclusion

Germany's way to fiscal solutions

Big problems in tax compliance were indicated in 2003

- The Federal Audit Office (BfR) has complained that later models of electronic cash registers and cash management systems now fail to meet the principles of correct accounting practice 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 cash register group started its work**

Problem

Possibilities of manipulation (1)

Reports generated by ECRs can be manipulated relative easily – possibilities using standard functions:

- Using functions for service technicians for manipulation (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) on (PC-based systems

Possibilities of manipulation (2)

The manufacturer can even provide special functions for data manipulation:

- Deletion of complete transactions from the electronic journal and re-calculation of all reports
- Creation of „wish reports“
- Functions to reduce all sales by a selectable amount while keeping reasonable items prices, quantities etc.

Some, mostly smaller companies offer these functions and even promote them quite frankly

More and more customers use software for communication with POS systems. Problems:

- Modification of (unprotected) data on a PC-platform is technically impossible to detect (direct access to files or data-bases is possible)
- Unclear position of tax auditors concerning POS data stored on PCs
- Complete changeover to electronic reporting is a risk for users

Use of cryptographic mechanisms for the protection of ECRs against manipulation

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

The „Work group cash registers“ of the German Federal Ministry of Finance validates the concept

- Modification of (unprotected) data on a PC-platform is technically impossible to detect (direct access to files or data-bases is possible)
- Approaches discussed by the work group:
 - “Classic“ fiscal memory
 - Recording of all transactions and data protection by digital signature
- “Classic“ fiscal memory was considered incomplete since only sums and not single receipts are stored
- This is why recording of all transactions (“electronic journal“) with digital signatures was proposed
- Concept of digital signatures proposed by PTB was recommended

Current situation in Germany

- Concept was confirmed by federal authorities and German federal countries (2006)
- Draft of a law was published
- Lack of clarity/misgivings to technical feasibility
- Lack of clarity at costs
- Strong resistance came from business associations

But!!!

- German cash register group has developed a well founded professional concept (July 2008)
- Under the leadership of PTB the project group „INSIKA“ work out the technical detail specification; starts February 2008
- All technical and general specifications will be open for everyone after finishing according to detailed operating schedule

Used Technique

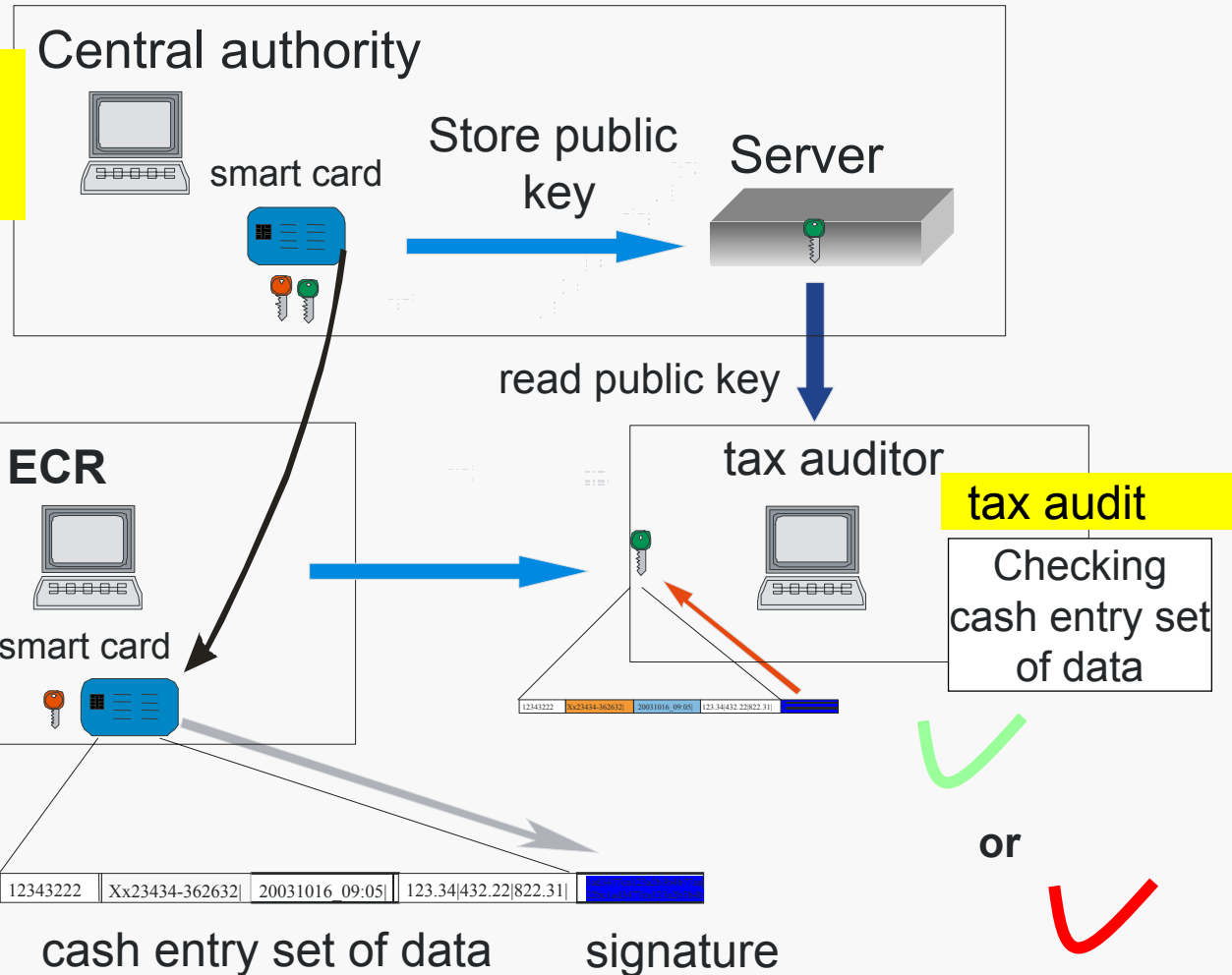
- Basis of the solution are well known, tested and standardised procedures of data protection
- Mass production of main components leads to favourable prices
- No new technique is necessary

System architecture (easy model)

Protection of ECR against manipulation

Recruitment of cards
card management,
card delivery

Sets of data
generate
sign
store
export



System architecture (easy model)

Life cycle

Once every 10 years

Recruitment of cards
card management,
card delivery

Central authority



smart card



Store public key

Server



1 kbyte for 20 years

read public key

Sets of data
generate
sign
store
export

ECR



smart card



tax auditor

tax audit

Checking
cash entry set

Once within 10 years

Once for 10 years

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

cash entry set of data

signature

or



Solution

Solution Growing awareness

Fiscal authorities have recognized the problems:

- Europe-wide cooperation of tax authorities
- Increased attention towards POS data during tax audits
- Better defined demands for POS systems, e.g.:
 - Austria: New law (“Betrugsbekämpfungsgesetz”)
 - The Netherlands: Brochure „Uw bedrijf en het afrekenstelsel”
 - Germany: Legislative procedure in progress
 - Sweden: New law about cash registers

Estimation Netherland

Ben van der Zwet, Belastingdienst.nl Feb.2008

- In 2004 Dieter Paschmans introduced your work in the EU Fiscalis Cash Register Project Group.

Meanwhile Germany is working in the same direction and thanks to the Working Group for Cash Registers, I think Germany is way ahead of the Dutch project.

In this way the outcome of your work would not only be applicable in Germany.

It might set a global standard.

- MEPs gave a first reading to the EU's new programme to facilitate cooperation between national tax authorities over the next six years, Fiskalis 2013.
- They are proposing a number of changes aimed at enhancing transparency of the scheme, and also want to limit it to EU Member States, where the Commission was proposing to include countries participating in the EU's Neighbourhood Policy too.
- The proposed budget for Fiskalis 2013 is around €157m

Title: Project Group for defining the tax reliable cash register

The following known solutions and approaches should be examined, evaluated and/or assessed:

- Fiscal memories
- Securing data via Electronic signatures
 - Greece - Fiscal Electronic Signature Devices (FESD)
 - German “Zisky” concept (obligatory?)
 - Netherlands “Zisky” concept” (compliance driven)
- Use Trusted Third market parties,
 - USA, Streamlined Sales and Use Tax Agreement (SSUTA)
- On-line data signing

Richard Ainsworth, Boston University of law

- **ZAPPERS: TAX FRAUD, TECHNOLOGY AND TERRORIST FUNDING, WORKING PAPER NO. 08-07**
- **ZAPPERS & PHANTOM-WARE: A GLOBAL DEMAND FOR TAX FRAUD TECHNOLOGY, Boston University School of Law Working Paper No. 08-20**

A comprehensive approach seems to be favored by Germany, and is currently under development.

Rather than use mini computers, the German preference is to require that smart cards be embedded in all

ECRs to encrypt an record all transactions passing through the terminal.

Solution Basic idea

Simple basic idea:

- Compulsory recording of all transactions
- Electronic data access for tax auditors
- Protection against manipulation using digital signatures
- In case of data loss estimation possible using totalizers in smart card

 **Using existing rules and procedures for POS systems completed by manipulation protection**

Technology Central points

Main elements of the presented solution:

- Electronic journal
- Manipulation-proof through digital signature (smart card)
- Printed receipt can be verified by digital signature
- Evaluation of 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 unnecessary high (and expensive) demands

Technology Electronic journal

Important demands on electronic journal:

- Definition of useful minimum content (must be feasible in all POS systems and contain sufficient information for effective check)
- Evaluation without accessing other data (e.g. article data) must be possible
- No „brand-specific“ knowledge required for evaluation of journal
- Backward compatibility – „new“ software must be able to work with „old“ data

Technology Advantages of digital signatures

Digital signatures have advantages over any other mechanism to protect data:

- “End to end” security – protection of data between the end points (from printing receipts to tax auditor’s software)
- No proprietary technology – security not based on keeping „technology secrets“ but on generally accepted mathematics
- Security of the system can be verified independently
- Today’s algorithms have not been broken for many years

Technology Receipt and cash slip

- Data of receipt and cash slip are the same
signature of receipt = signature of cash slip
- With the help of a receipt sequence number the assignment is possible clearly
- Receipt data can be stored durable on user-defined media electronically

Technology Receipt structure

XYZ GmbH	
DE 188851765-2	
1 beer 0,5l A	2,50
1 wine 1 l A	5,00
Total	7,50
taxable. A=19%	6,30
VAT 19%	1,20
Cash	7,50
10.08.2008 14:38 34134	
3a23cf11ff312288a121	
55fe327ab21ecf791322	

Thank you	

Tax no. and consecutive ECR no.

PLU bookings

VAT

Unambiguous receipt no.

Hash value for PLU bookings

Signature

Red = special elements for „Fiscal receipts“

Technology Signature procedure (1)

XYZ GmbH
 DE 188851765-2

1 beer 0,5l A	2,50
1 wine 1 l A	5,00
Total	7,50
taxable A=19%	6,30
VAT 19%	1,20
Cash	7,50

10.08.2008 14:38 34134
 3a23cf11ff312288a121
 55fe327ab21ecf791322

Thank you

1	piece	beer 0,5l	19	2,50
1	piece	wine 1 l	19	5,00

Hash value PLU

1. step:
 Calculation of Hashcode for
 PLU bookings

Technology Signature procedure (2)

XYZ GmbH	
DE 188851765-2	

1 beer 0,5l A	2,50
1 wine 1 l A	5,00
Total	7,50
taxable A=19%	6,30
VAT 19%	1,20
Cash	7,50
10.08.2008 14:38 34134	
3a23cf11ff312288a121	
55fe327ab21ecf791322	

Thank you	

Hash value PLU	3a23cf11ff312288a121
Tax number	DE 188851765-2
date and time	10.08.2008 14:38
sequence no.	34134
VAT normal	6,30 / 1,20 (19%)
VAT reduced	0,0 / 0,0 (7%)

Receipt signature

2. Step:
smart card computes
the receipt signature

Technology Signature procedure (2)

XYZ GmbH DE 188851765-2	

1 beer 0,5l A	2,50
1 wine 1 l A	5,00
Total	7,50
taxable A=19%	6,30
VAT 19%	1,20
Cash	7,50
10.08.2008 14:38 34134 3a23cf11ff312288a121 55fe327ab21ecf791322	

Thank you	

Hash value PLU	3a23cf11ff312288a121
Tax number	DE 188851765-2
date and time	10.08.2008 14:38
sequence no.	34134
VAT normal	6,30 / 1,20 (19%)
VAT reduced	0,0 / 0,0 (7%)

Check of authenticity possible through receipt signature using the data on cash slip

Technology Signature procedure (3)

hash value PLU	3a23cf11ff312288a121
tax number	DE 188851765-2
date and time	10.08.2008 14:38
sequence no.	34134
VAT normal	6,30 / 1,20 (19%)
VAT reduced	0,0 / 0,0 (7%)

Monthly totalizers on smart card

sales normal	180.422,86
Sales reduced	10.404,96
negative sales normal	33.278,23
sales training	48.642,27
sales delivery receipt	22.122,33
.....

**3. step:
smart card
refeshs totalizers**


signature

55fe327ab21ecf791322

Technology Signature procedure (4)

The following procedures take place in one step within the smart card:

- Allocation of new receipt no.
- Calculation of receipt signature
- Calculation of journal signature
- Update of totalizers

 **No manipulation (e.g. data modification and recalculation of signature) possible. The security is in the smart card and not depending on the POS system**

Technology Signature procedure (5)

hash value PLU	3a23cf11ff312288a121
tax number	DE 188851765-2
date and time	10.08.2008 14:38
sequence no.	34134
VAT normal	6,30 / 1,20 (19%)
VAT reduced	0,0 / 0,0 (7%)

Storage of signed data in ECR: manufacturer specific!! No requirements!!!

1,0,5,"beer",2.50,A

1,1,0,"wine",5.00,A

2,DE 188851765-2,200808101438,34134,6.30,1.20,0,0

3,55fe327ab21ecf791322

Technology Totalizers

Totalizers on smart card deliver data even if journal is lost

- Each set of totalizers records sales, voids, training transactions, VAT etc
- Memory of smart card allows multiple sets of totalizers proposal:
 - 120 monthly totalizers for ten years since smart card distribution
 - Each container holds 6 tax values
 - Control elements against overflow



”Built-in back-up for most important data

Technology data processing

Requirements to ECR data processing after data acquisition :

- Periodic transmitting of data to an external media (memory card, USB stick, hard disk)
- Backup of daily statements by reading the totalizers of the smart card
- Backup of data on external PC
- Structured saving of data
- Well-defined access to data
- Conversion of data to testable format – export interface

Technology Daily statements

Daily statements accelerate the verification of data

- Daily statement contains the totalizers of the smart card in signed form
- In most cases a verification of each transaction signature (which takes some time for calculation) is not necessary if
 - the sum of all transactions between two daily statements corresponds to the difference of the totalizers from the statements
 - the number of transactions corresponds to the difference of the invoice number between two daily statements.

Technology Tax audit

Steps for checking the journal data:

- Conversion to standard XML-export format
- Comparison of the sums of receipts with the daily statements
- Verification of the signature of daily statements
- If required:
 - complete or random verification of signed transaction
 - checking of printed receipts to recognize forgeries

Implementation

Implementation

Changes at POS systems (1)

Following changes in existing POS systems and back-office software are required:

- POS-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)
- If necessary memory extension for longer storage of data in the POS system might be needed (to work without frequent transfer of sales data to a PC)



POS systems comply with “good accounting practice”

Implementation

Changes at POS systems (2)

The digital signature only requires some minor additions:

- Connection of external smart card reader or full integration of card reader
- Software features so that signatures be created, printed and stored
- Use of ECC („Elliptic Curve Cryptography“) proposed:
 - Relatively short keys and signatures (112 to 192 bit keys and 224 to 384 bit signatures)
 - Ideal for implementation in smart cards



Additional manipulation security

Simple external smart card reader

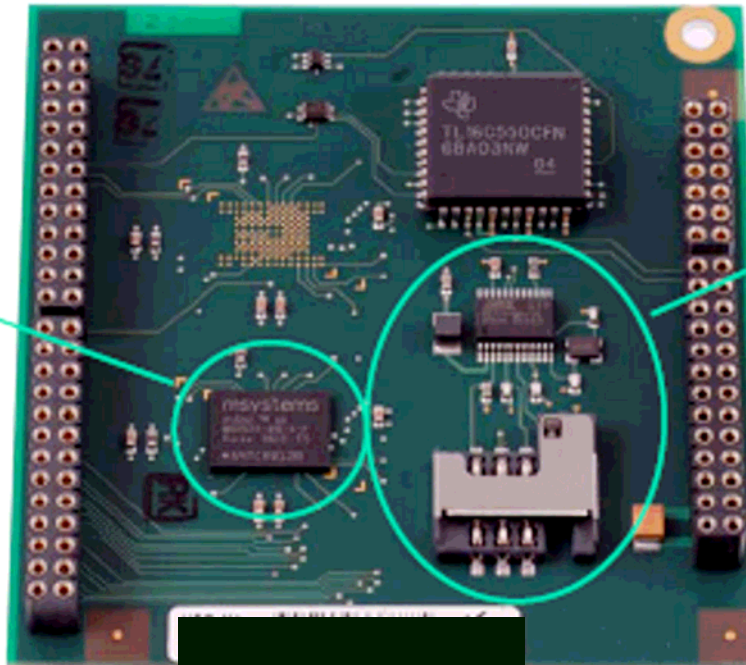
- Connection of external smart card reader or full integration
- Suitable especially for PC-based POS systems
- Single-unit end-user price less than € 25



Hardware

Memory extension

approx. 5-10 €



Card reader unit and controller

approx 10 €

Software

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

Smart card



(10 €)

Implementation

Expenditure for ECR manufacturers (3)

item	price	price per ECR*
Hardware card reader	10 €	10 €
Hardware memory/interface	5 €	5 €
Software smart card triggering	30 000 €	15 €
Software memory extension	10 000 €	5 €
Software XML-export	10 000 €	5 €
sum		40 €

* Refer to 2000 ECRs produced

- Apply for smart card
- Assembly of smart card (once for 10 years)
- Backup system for ECR data (is not new)
- Keep ready data in export format

item	price	price per ECR
Application	0 €	0 €
Price smart card	10 €	10 €
Data backup	0 €	0 €
Assembly smart card re-fitting	80 €	80 €
Assembly smart card new system	0 €	0 €
sum		10 to 90 €

- Acquisition of smart cards (organisation of tender)
- Distribution of smart card, support of database (Germany up to 2 million ECR)
- Supply of certificates (LDAP server)
- ECR review of tax authority
- Field auditing of tax authority

Required standardization to avoid insecurity, distorted competition and security holes

- Extent of recording (what does a stored receipt have to contain?)
- Application fields (Who is obliged to record the data? Are POS systems compulsory?)
- Precise definition of manipulation security as concrete solution based on smart cards

XML export File is suitable for data exchange

- General structure working well for „fiscal journal“
- Digital signatures have to added
- Definition of compulsory fields required
- Minor details have to be discussed
(characters sets etc.)

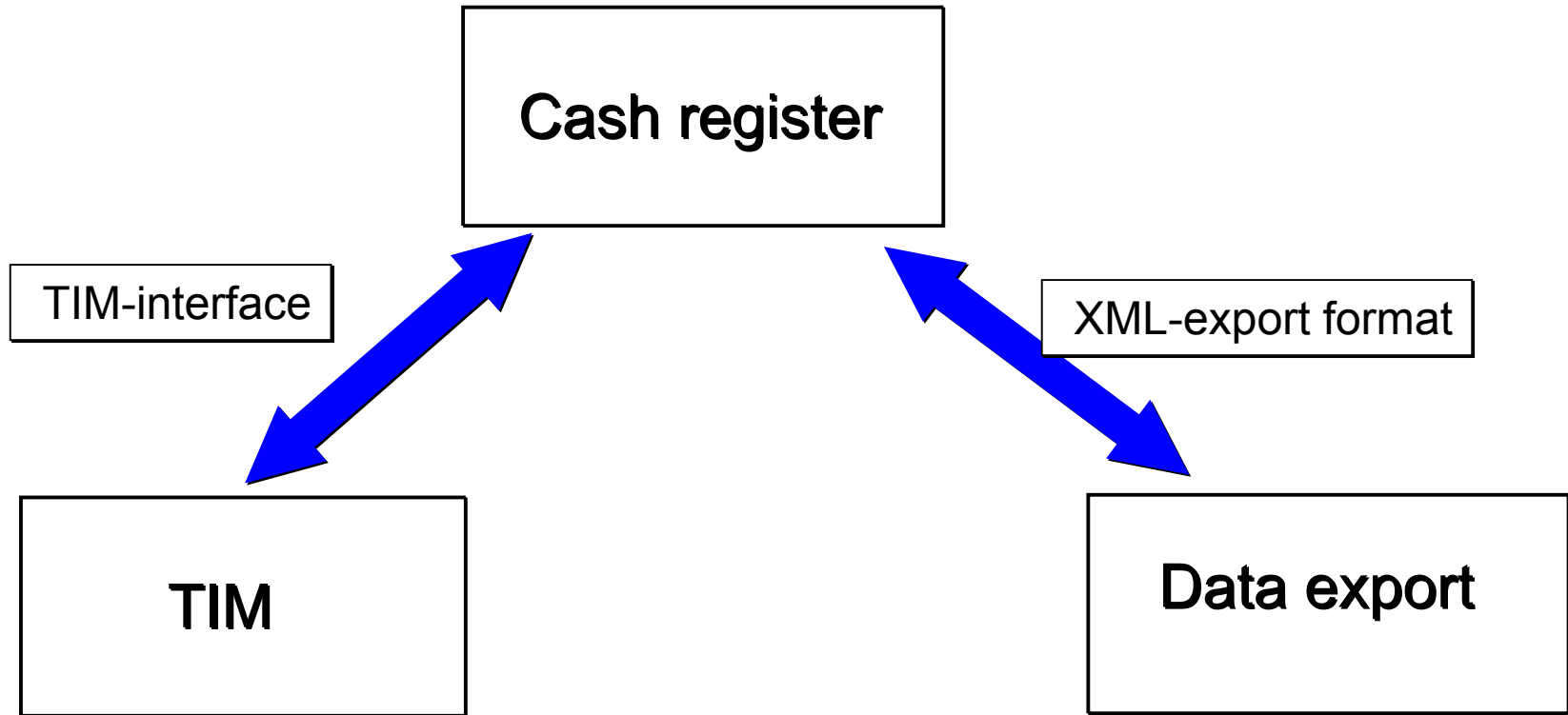
Digital signature systems require “Public Key Infrastructure”

- General structure working well for „fiscal journal“
- Public keys are usually stored in “certificates”: Identity of person or institution that signed the data can be verified
 - Identity of certificate issuer can be verified
 - Integrity of key data can be verified
 - Mechanism to revoke certificates
- If smart cards are issued by tax authorities and public keys are distributed and used within the organization the system can be simplified significantly
- „Certificate servers“ operated by any private organization are an alternative approach

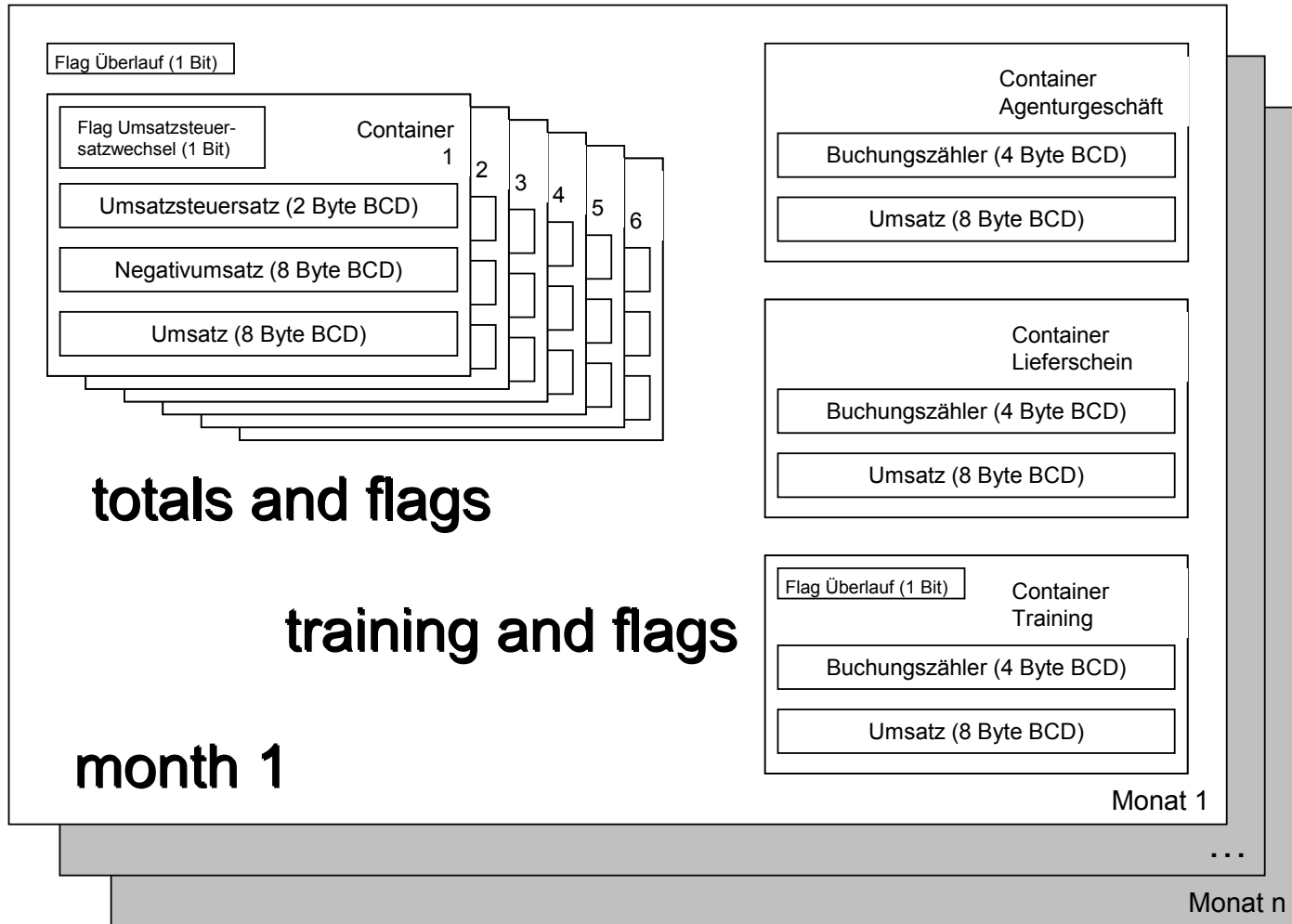
Actual development status of the specifications

- Security analysis
- Data modelling
- Description of interfaces ECR to signature device
- Description of interfaces XML export
- Audit and verification activities

System interfaces



Model of totals inside TIM



Important dates of INSIKA-Project

- 08/2008 Specification of signature device
- 09/2008 Prototype of signature device
- 09/2008 Specification XML export
- 10/2008 Prototypes cash registers
- 10/2008 Start of test
- 10/2008 Publication of specification (Workshop, Internet)

Main advantages of the system

- General structure working well for „fiscal journal“
- Absolute tamper-proof 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 in most cases and relatively 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

**Many
Thanks for
Your Attention!**