INSIKA-Demonstration
Quickstart instructions

Last modification: 20.05.2010

Status: preliminary

Explanatory notes

This INSIKA-documentation, in completion to the TIM-interface specification, comprises a brief introduction to the subject, notes on operation of the demonstration software and on implementation.

The document mainly addresses two target groups: (1) groups of persons who want to become familiar with the system by means of the demonstration software and (2) developers who want to integrate an INSIKA smart card (TIM) into existing or new products or who want to get a general idea of correct procedure and required time and effort.

The publication of this document serves to inform interested persons about the basics of the INSIKA-technique and basically enables them to put the concept into practice. The presented procedures, models and interfaces are neither standards nor regulations, nor are they subject of legal provisions.

For fast information about modifications the documentation will only be distributed among registered companies. However, the INSIKA-consortium assumes that a stable version without demand for major changes is already at hand.

No guarantee or warranty can be derived from the technical contents described herein. The authors and the consortium do not accept liability or responsibility when adopting the concept or parts thereof.

At present we cannot support implementations during the development phase. Questions concerning the concept will be answered within the realms of possibility. The INSIKA-consortium will inform continuously about the further course of project.

The INSIKA-Project is funded by the Federal Ministry of Economics and Technology under the grant MNPQ 11/07.

Project information: http://www.insika.de/

History

Version	Date	Modification	Remark
1	12.02.2010		Initial version
0.1.2	26.02.2010		Published version
0.1.2en	12.05.2010		Translation into English

Authors: J. Reckendorf, N. Zisky, J. Wolff, J. Neumann

Contact: Physikalisch-Technische Bundesanstalt (PTB)
FB 8.5, INSIKA-Projekt
Abbestraße 2-12
10587 Berlin
Germany
insika@ptb.de

File name: INSIKA_Quickstart_v0.1.2en.doc
Version: 0.1.2en
Referenced TIM-application: T.1.0.6.
Status: preliminary
Last change: 20.05.2010

Contents

INSIKA-Demonstration Quickstart instructions....1
Explanatory notes....2
History....3
1 Introduction....5
1.1 INSIKA - Overview....5
1.2 Required components for INSIKA-demonstration....6
1.3 Target groups....6
1.3.1 Users of cash registers....6
1.3.2 Manufacturers (cash registers, hardware and software)....6
1.3.3 Tax investigators, tax consultants, auditors....7
1.3.4 Decision-makers in politics, administration and economy....7
1.4 Tasks of demo package....7
2 Basics....8
2.1 Origin of the INSIKA-project....8
2.2 Basic concept....8
2.2.1 Essential coherences....8
2.2.2 Cryptography....9
2.2.3 Auditing procedures....10
2.3 Differences to classic fiscal memories....10
2.4 Security....11
2.4.1 Cryptography....11
2.4.2 Smart cards....11
2.4.3 Link of card-internal procedures....11
2.4.4 Correct use of the system....12
2.5 Cost analysis....12
3 INSIKA-Demonstrator....13
3.1 Current development status....13
3.2 Tasks of the software....13
3.3 Set up....13
3.4 Functionalities....13
3.4.1 Cash register simulator....13
3.4.2 IVM....14
3.4.3 TIM-Browser....14
3.5 Application example....14
4 Implementations in cash register systems....15
4.1 Prerequisites....15
4.2 Control of the TIM....15
4.3 Data preparation, Integration of the TIM....16
4.4 Print of verifiable receipts....16
4.5 Storage of the journal....17
4.6 Daily reports....17
4.7 Journal handling....17
4.8 XML export of the journal....17
4.9 Auxiliary functions....18

1 Introduction

1.1 INSIKA - Overview

The acronym INSIKA denotes the German project „INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme“ (Integrated security solution for cash registers). This solution will be developed to series maturity in a project under the direction of the PTB (Physikalisch-Technische Bundesanstalt, the national metrology institute of Germany).

Application of the INSIKA-concept guarantees the complete, audit-compliant recording of individual cash transactions when using an electronic cash register. The INSIKA-technique is a new approach to prove the compliance with generally accepted accounting principles. In contrast to “classic” fiscal systems with complex, technical special solutions, which in most cases save data in mechanically secured (e.g. sealed) storage modules, security here results from the cryptographically secured transaction data as such.

Application of the concept requires a cash register, which communicates with a special smart card according to clearly defined rules and which converts all data created with the smart card together with the transaction data into a standard format.

Data created in this way is protected by means of high-security IT-standard methods. There are no demands concerning the type – and in particular concerning the security of the cash register. The security of the INSIKA-system results from evaluated protection mechanisms of the smart card and the included software and keys.

Access to the INSIKA-technique is easy. Everybody with basic PC-knowledge can understand the main processes. Application/evaluation of the system does not require specialized knowledge.

The INSIKA-project group presents the results of the two years’ project as complete demonstration package to all interested parties. The latter can request components (smart card) that were developed during the project. When using the smart card, all processes can be reproduced. These are:

- Provision of INSIKA-smart cards (personalisation incl. digital certificate)
- Creation of signed cash register data (with a specially developed cash register simulator or with existing, accordingly adjusted cash register systems)
- Verification of INSIKA-transaction data

Expenditure for the development of cash registers with INSIKA-functionality and test methods is therefore easily estimable. Chapter 1.3 (“Target groups”) lists the target groups of the respective chapters in this documentation.

1.2 Required components for INSIKA-demonstration

Demonstration of INSIKA on a Windows-PC requires the following components:

- Smart card (with special software, this unit is designated as “TIM” = „Tax Identification Module“) with digital certificate: on request, we provide any interested party with this card for test purposes.
- Smart card reader with USB: Standard reader for smart cards without special security requirements, driver software for smart card reader is usually included in vendor's shipment.
- INSIKA demonstration software:
  - Cash register simulator: Special program for creation of INSIKA-cash register data incl. brief instructions for program operation. Any interested party will be provided with this software for test purposes free of charge. The program only provides simple cash register functions. However, the stored data correspond completely to the INSIKA-specification.
  - INSIKA Verification Module (IVM): This software verifies the INSIKA-transaction data, independent of the cash register software
  - TIM-Browser: Software for reading information from the TIM

1.3 Target groups

1.3.1 Users of cash registers

The demo package helps the users of cash registers to get a general idea of the INSIKA-system and to evaluate the expenditure of a change-over and the effects on daily business.

We recommend reading at least the following chapters of this documentation (and the respective other documents mentioned therein):

- 2.2.1 Essential coherences
- 2.3 Differences to classic fiscal memories
- 3 INSIKA-Demonstrator

1.3.2 Manufacturers (cash registers, hardware and software)

Manufacturers can reproduce the interface specification details using the logging functions of the cash register simulator software. This allows fast access to the INSIKA-technique. In combination with the test software, they can easily evaluate the procedure and expenditure required for integrating the INSIKA-smart card into their cash register installations. Complete integration into existing or new products is likewise possible.

We recommend reading at least the following chapters of this documentation (and the respective other documents mentioned therein):

- 2 Basics
- 4 Implementations in cash register systems

1.3.3 Tax investigators, tax consultants, auditors

Tax investigators, tax consultants or auditors can familiarize themselves with the INSIKA-technique within a short time, since the INSIKA-data of any manufacturer is unambiguously determined by the uniform export format. The otherwise required analysis of the applied data structures and –formats can be omitted.

We recommend reading at least the following chapters of this documentation (and the respective other documents mentioned therein):

- 2.2 Basic concept
- 3 INSIKA-Demonstrator

1.3.4 Decision-makers in politics, administration and economy

This documentation helps decision-makers, who want to form an opinion on the INSIKA-system, to get a quick overview on functioning, security and the main cost aspects. These aspects are described in chapter 2 (“Basics“).

We recommend going a bit deeper into the subject by using the demonstration software (chapter 3).

1.4 Tasks of demo package

The demo package is to provide all target groups with a fast access to the INSIKA-technique by testing and reproducing the individual steps. Decision-taking on this basis is much easier than on basis of just the documentation.

Even non-technical users can quickly get an overview when working with a real system.

As of spring 2010, prototypes of cash registers will undergo a field trial. The INSIKA-consortium will inform about the results of these field trials and about the reactions to work with the INSIKA-demo package in regular intervals.

According to our experience, it is relatively easy and inexpensive to integrate the INSIKA-smart card into an existing, modern cash register system, particularly into PC-based systems.

2 Basics

2.1 Origin of the INSIKA-project

The annual report 2003 of the German Federal Audit Office referred to imminent tax revenue shortfalls due to manipulation in modern cash registers. In numerous cash registers, the stored data can be changed in any way, without leaving the slightest trace. This urgently calls for remedy.

The Federal Ministry of Finance therefore prepared a law to avoid such manipulation, with reference to a technique that was elaborated by the PTB and the Federal Ministry of Finance. A “Cash register” working group, including representatives of the Federal Government and the "Länder", developed a concept for the implementation of the law. Under the direction of the PTB a corresponding technical solution is designed and implemented within the frame of the INSIKA-project. The law was presented in July 2008, but withdrawn again. Several European countries are basically interested in the INSIKA-solution.

The overall concept and the specification of all interfaces are disclosed completely. There is no patent protection at all. No licence fees or similar will be charged for the use of the concept. Application of the system does not lead to any basic dependencies. However, the cash register software implemented within the frame of the project comes under the copyright of the respective companies; it is not an open source or freeware.

The INSIKA-Project is significantly promoted by the Federal Ministry of Economics and Technology within the scope of the support programme “MNPQ-Transfer” (promotion of SMEs in the implementation of innovations in the fields of metrology, standardisation, testing and quality assurance).

2.2 Basic concept

2.2.1 Essential coherences

The protection from manipulation is mainly based on an electronic signature, created by a smart card with special software (TIM) that is issued by an authorized central office. So-protected data cannot be modified without being detected. Even in case of manipulation or data loss the turnover can still be estimated due to technical provisions.

Electronic signatures guarantee that data come from a certain person or system (in this case a defined cash register) and the data has not been altered since creation of the signature. Most applications – as does the INSIKA-system – use smart cards to create the signature.

The system uses customary smart cards, which are equipped with special software and designated “TIM”. On implementation of the law, the financial administration would procure the smart cards in an open tendering procedure and issue them to the taxpayers on request.

The TIM can be connected via external smart card reader or integrated into the device (like in mobile phones). The cash register software has to communicate with the TIM and has to guarantee printout and storage of the data. Further modifications of the cash register are not required. The major part of cash registers and POS systems on the market can be upgraded without great effort.

Printed receipts and the appropriate, electronically saved transactions get an electronic signature. This signature is generated by the TIM. Furthermore, the TIM has an internal counter, which guarantees that each transaction and the respective printed receipt get an unambiguous and consecutive number ("sequence number").

The TIM also manages sum totals, which register the total turnovers in such a way that if stored data gets lost the important key figures (monthly turnover, negative transactions etc.) can still be determined. Signature creation and the management of sequence counter and sum totals are linked within the TIM so that on creation of a signature a new sequence number is assigned and the totals are updated.

Compulsory receipt output together with the obligation that each receipt requires a valid signature ensure that data is recorded correctly, since all further steps are compelled via various linked functions within the TIM.

This means that basically only those data is saved, to the storage of which the taxpayer is already obliged today. The new part is the obligation to save the additional signatures and sequence numbers for each transaction.

Each audit of the cash register data uses the stored and signed transactions. Since this data cannot be modified undetected, any conceivable manipulation of cash register reports or master data remains ineffective, because a simple comparison with the stored transaction data will unveil the manipulation. Even a deliberately integrated manipulation function cannot attack the system, which means that a time-consuming certification of the devices becomes unnecessary.

The audit of the recorded data can be automated to a large extent and is thus much more efficient than in the past.

The verification of the printed receipts only requires information, which is available on the printout. Access to the stored transaction data is not necessary. It is therefore easy to verify whether a printed receipt was generated by a cash register with valid TIM. Every wrong created receipt with invalid or without signatures is clear proof of manipulation.

Tax payers can use the INSIKA-system to prove the correct registration and unmodified storage of data recorded at the cash register.

2.2.2 Cryptography

Electronic signatures suitable for the INSIKA-method are created by asymmetric cryptography. Here the so-called elliptic curve cryptography (ECC) is used, which offers a high security level and fast processing whilst using short keys and signatures.

A valid electronic signature can only be created using a so-called private key. The key is securely stored on the TIM and not accessible. You can easily verify the authenticity of the signature with the so-called public key that belongs to the private key. Free access to the public key is no security risk, since the private key cannot be computed on basis of the public one. This means that unauthorized persons cannot generate valid signatures.

In order to guarantee that the public key corresponds to the private (i.e. that an auditor does not get a forged key) or that the smart card has not been reported as stolen etc., so-called digital certificates are used. These are structured data which confirm the owner as well as other key attributes. This is mainly assured by a certificate, which is digitally signed by a

trustworthy authority. Furthermore, a list of all revoked certificates (and therefore smart cards) is kept centrally.

Users of the system can use a certificate to assign a public key to an identity (e.g. a person, an organization or an IT-system – in this case a company) and to define its scope. Digital certificates enable the protection of privacy, authenticity and integrity of data through correct use of the public key. For the administration of certificates a so-called “Public Key Infrastructure” (PKI) is applied. This is common technique in modern security applications.

2.2.3 Auditing procedures

Verification of data that was created by an INSIKA-based system differs distinctively from conventional systems.

Of essential importance is the fact that the storage of the turnover data is precisely standardized. This is the prerequisite for a manufacturer-independent signature and in addition results in a completely identical data audit for all INSIKA-compliant systems. This standardized data format maps the existing regulations for the storage of transaction data (particularly the principles of due computer-aided bookkeeping systems = GoBS and the principles of data access and verifiability of digital documents = GDPdU). It can therefore be used by practically every system, which complies with these regulations.

The check whether data is complete and unchanged is carried out fully automatically by means of signatures and sequence numbers.

This verified data allows the plausibility of all derived data (e.g. daily takings, sales of defined products over certain periods). It is possible to evaluate INSIKA-transaction data without having to access additional data (e.g. master data). On demand, raw data can be analyzed in detail; the profundity of the analysis can be adjusted to the individual case.

In practice, verification is presumably best made by implementing an import module for the software used by the tax investigators (IDEA for Germany). It can thus be integrated smoothly into existing applications and procedures.

In contrast to the presently applied methods, analyses for the detection of manipulations (Benford-analysis, comparison of sales of individual products and respective purchase quantities etc.) can be reduced considerably.

If data is missing despite the obligation to keep records or if data is incomplete, turnovers can still be calculated on basis of the so-called daily reports and the sum totals stored in the TIM.

2.3 Differences to classic fiscal memories

In contrast to “classic” fiscal memory solutions like those used for example in Italy or various South American and East European countries, the security of the INSIKA-system is exclusively based on cryptography.

As soon as a correctly signed receipt is issued, the correct functioning of the system is proven. Data storage does not require a special protection. Since no other restrictions of the cash register functions are necessary to guarantee security, no type approval, certification or similar of the cash registers is required. In classic fiscal memory systems these steps lead to high costs, distortion of competition and delay or even prevention of technical development.

2.4 Security

To assess the security of the system we will examine the main aspects in the following. We will deal with these questions in detail in the security analysis, which will be drawn up within the framework of the project.

2.4.1 Cryptography

The technique of electronic signatures is mature, very safe and is often used today, e.g. in the banking sector or for electronic tax declarations.

In order to get the short signatures and to minimize processing time, the INSIKA-project selected signatures on basis of elliptic curves (ECC = “Elliptic Curve Cryptography”, here ECDSA = “Elliptic Curve Digital Signature Algorithm”). The applied key length is 192 Bit, which according to current knowledge provides sufficient security also in the future. However, the architecture provides the option of using longer signatures if required.

For proof of completeness and integrity of the transaction data, a cryptographic hash function (the “finger print” of transaction details so to speak) is used.

What is essential for secure cryptographic methods is that security does not depend on the confidentiality of the technique itself but on the confidentiality of the private keys only. The techniques are published and are therefore subject to permanent expert evaluation.

2.4.2 Smart cards

The INSIKA-system is designed for application of commercial, evaluated smart cards with security software. In addition, software in accordance with the INSIKA-specification is stored on the cards.

Protection of the cards’ hardware and system software against all known attacks is state-of-the-art.

In some time applying new generations of smart cards may increase the security level. This can be done during operation if required.

2.4.3 Link of card-internal procedures

Important for security is the fixed link of card-internal functions among each other and to transactions in the cash register. These are:

- Sequence counter: The sequence counter, which numbers the transactions consecutively, is managed by the TIM, which includes it directly to signature generation. Manipulations are thus excluded here inherently. External modification of the counter is not possible.
- Plausibility checks in the TIM: The TIM checks the relation between single amounts (tax calculation and plausibility of included negative turnover) prior to signature generation. If data is not plausible, no signature is created.
- Sum totals: The TIM stores exactly determined data as monthly sums (e.g. total turnovers separated by VAT rates). If transaction data (the storage of which is compulsory) is no longer available, incomplete or faulty, the sum totals are still available and allow closing the data gaps. The sum totals are updated together with signature creation and can therefore not be manipulated.

2.4.4 Correct use of the system

As with every fiscal or non-fiscal cash register system, the correct registration of **all** transactions is a decisive basic requirement**.**

This is guaranteed in the INSIKA-concept and the underlying law of July 2008 by the following measures:

- Obligation to apply the INSIKA-system in every cash register
- Obligation to print a receipt with a valid signature for each sales transaction. The receipt has to contain all data in order to verify the signature without accessing other data (e.g. those stored in the cash register).
- Unannounced audit visits, which ensure adherence to the obligations (within the scope of the so-called “audit of cash register”)

The technical part of the solution can basically guarantee easy and reliable detection should the system be applied incorrectly or not at all. Via a corresponding surveillance the risk of discovery has to be high enough that fraud is either prevented or detected.

2.5 Cost analysis

According to our experience during the project, one has to allow for approximately one to five man-months for development to integrate the INSIKA-solution to an existing cash register system. Expenses vary much depending on the technical prerequisites.

Material costs for a smart card reader (external or internal) are in the low double-digit range. Integration of a smart card reader requires one-off expenses that cannot be estimated in general (for instance, changes of electronic assemblies or housing parts may become necessary).

Overall, the following aspects are to be considered:

- In most cases the upgrade of existing systems will comprise the connection of a smart card reader and an update of the cash register software.
- During the transition period (i.e. the period between the coming into force of the respective regulation and the obligation to use the system) numerous cash registers will be exchanged or maintained anyway, so that this will not cause significant additional costs.
- The comparably easy implementation of the INSIKA-system will not decrease competition, so that this factor will have a cost-reducing effect.

According to analyses, the development, introduction and operation of the INSIKA-system is considerably less expensive than all known fiscal systems whilst at the same time security is increased.

3 INSIKA-Demonstrator

3.1 Current development status

The entire demonstration software is in a testing stage, thus conceptual and implementation errors cannot be excluded.

Especially the cash register simulator and the verification software (IVM) have explicitly the status of demonstration software. Both programs were developed by the PTB within the INSIKA project.

The software of the TIM has already been tested carefully. The occurrence of errors cannot be excluded completely.

3.2 Tasks of the software

By the INSIKA demo package the function of INSIKA can be demonstrated. This includes the generation of signed cash register data, the storage of the signed data, the conversion into the INSIKA export format and the verification of the signed data (incl. the access to the INSIKA certificate server). All these processes are similarly executed within the real prototypes of INSIKA cash registers.

3.3 Set up

All three programs of the INSIKA demo run directly on a PC without installation. Usage instructions can be found in every software package.

3.4 Functionalities

3.4.1 Cash register simulator

The simulator allows for testing of all INSIKA features of a cash register. This includes the activation of the TIM, the execution of transactions and daily reports. An electronic journal will be generated, that can be verified by the IVM tool. The simulator allows the mapping of a wide range of application scenarios. This includes training features, cancels, articles with multiple VAT parts and changes of VAT rates. Special cases as delivery note and third party turnover can be tested. Additionally the simulator allows checking reactions on inconsistent time.

To work with the cash register simulator, only a PC with Windows XP, a smart card reader installed and supported by Windows XP and a personalized TIM are required. Other operating systems, especially Windows Vista, have not yet been tested. The installation of the software is not necessary. In the simulator's main window, single transactions can be carried out. A click on a product from the product list or a click on the button "Add Item" adds a product. The communication between PC and TIM can be followed in two different windows. A detailed description can be found in the program documentation "INSIKA_KassSim_Manual.pdf".

3.4.2 IVM

The program IVM (INSIKA Verification Module) enables the verification of signed transactions, signed daily reports and printed receipts with signature.

Transactions have to be supplied in the INSIKA XML export format. For the verification digital certificates are required, that can be read from the XML data directly or from the INSIKA certificate server. The result of the verification is signalised by the program via the colours green - verification successful or red – verification error. On some computer networks certain ports need unblocking for the online access to the certificate server. Detailed information can be found in the program documentation "INSIKA_IVM_Manual.pdf".

3.4.3 TIM-Browser

The TIM-Browser is a program for displaying INSIKA-relevant data of the TIM. To start the program, a smart card reader has to be installed. The program was tested under Windows XP. A short description can be found in the <Readme.txt> file of the program's folder.

3.5 Application example

In this section essential sequences of an INSIKA demo are described, making use of the presented software programs. Details can be found in the particular software documentations.

To follow the steps generation and verification of INSIKA data, the cash register simulator and the IVM are needed.

After the start of the cash register simulator a click on a product from the product list or a click on the button "Add Item" adds a product to a transaction. For the next step the button "Sum Up" can be clicked. Now the transaction is ready to be signed. This can be done by clicking the button "Register and Sign". By this button the transaction data will be sent to the TIM and the signature will be returned. The result of the transaction will be shown as a receipt that can be printed. The transaction has been saved within the simulator's journal. The register processes can be repeated unlimited times.

Apart from transactions, daily reports can be generated. The corresponding window opens after clicking the button "Open Report". When generating a singed report the corresponding signature will be stored in the journal and shown on the receipt.

To verify the generated data, the cash register simulator has to be closed first. After that the journals, which can be found in the "Journal" sub-folder, can be opened. The simulator maintains the electronic journals in the INSIKA XML export formats. For demonstration purposes both of the two different versions are supplied: the XML "Plaintext" (long format) and the XML "Base64" (short format). Both files can be verified by the use of the IVM.

After the start of the IVM single XML files or groups can be accessed using the "Open File" button. The program verifies the included signatures and displays the results ("Verification successful" – green or "At least one verification incorrect" – red). Further details can be shown by the "Show Content" button.

The TIM Browser has been developed to read out the TIM's data very easily. So every user can check the data that has been stored on the TIM. Additionally the digital certificate can be read from the TIM directly.

4 Implementations in cash register systems

This section gives a general overview on implementing INSIKA into cash register systems. By this the reader will be able to estimate the processes and efforts of an implementation very quickly. Additionally it may improve the understanding of the TIM interface specification.

4.1 Prerequisites

An electronic cash register has to fulfil some prerequisites for an implementation of INSIKA:

- The cash register must be capable of controlling a smart card via an external smart card reader or an integrated device.
- A printer for alphanumeric signs must be available.
- Basically the INSIKA system is defined by two interfaces: the TIM signature interface and the XML export interface. The TIM interface is specified in the document "INSIKA_TIM_Schnittstelle-[version]". The XML export interface is specified in the document "INSIKA_Exportformat-[version]". A cash register has to handle both interfaces, whilst the XML export interface can be handled via an external XML generator (e.g. PC software).
- An INSIKA system has to keep a journal that stores every transaction and every daily report. The internal size, format and implementation are completely left to the manufacturer on one condition - the data must be fully convertible into the defined XML format. Only under this condition an audit of data, and specially signature verification, will be successful. A cash register has to have enough storage capacity and appropriate management mechanisms. If there is an existing journal available, it has to be expanded for sequence numbers and signatures at minimum. The journal has to exchangeable to a computer system (e.g. via serial-, network- or USB-interfaces, USB sticks, SD memory or Internet protocols).

4.2 Control of the TIM

The TIM is a common smart card that embeds an operating system and a special TIM package. The TIM interface is defined by the ISO/IEC 7816 part 1-4 in the physical, data link and application layer. The extensions for INSIKA on application layer are specified in the document "INSIKA_TIM_Schnittstelle-[version]".

The TIM is supplied in ID-1 dimensions (size of common credit cards). As the smart card is perforated it can be break into the ID-000 dimensions (size of GSM SIM cards) very easily.

The TIM can be controlled by every common smart card reader. There is no need for a pin-pad, a smart card reader of class 1 is fully sufficient. The reader has to support the "T=1" protocol, following the ISO/IEC 7816. The transport PIN used for the first activation of the TIM will be sent from the host to the TIM via the interface. The cash register simulator can be used for that.

For many cash registers the integration of the TIM and the smart card reader into the system will be an appropriate choice. Different integrated circuits can be used for the control of the

ISO/IEC 7816 interface. Beside the physical layer some of them include a full protocol stack for "T=1". As the control of smart cards is standardised to a high extend, it will not referred here any further. An overview of smart cards and technology is given e.g. in "The Smart Card Handbook" of W. Rankl and W. Effing.

One has to notice that the speed of communication with the TIM depends on the smart card reader and the corresponding drivers. In real optimal configurations the time for an INSIKA transaction is determined by the generation of the signature only. A transaction lasts about 300 ms, for the currently used smart cards. For a clear integration this will not cause troubling delays.

As the communication with smart cards is standardised to a high extend, libraries may be available for many systems. If the communication has to be implemented from scratch, the generation and parsing of TLV objects will be one major programming task. TLV denotes data objects of a "Tag-Length-Value" structure: a tag will be followed by the length information and the data itself.

The communication is always as follows. The host (cash register) sends a request to the TIM. This request consists of a command APDU ("Application Protocol Data Unit"). According to the command the TIM answers with a response and a result code.

4.3 Data preparation, Integration of the TIM

A transaction consists of the following steps:

- Preparation of the data (incl. calculation of the hash value of transaction items, therefore the items have to be coded in a defined way, a SHA-1 hash value has to be calculated from this data)
- Some special details of the transaction have to declared
  - Third party turnovers: turnovers on behalf a third party, e.g. fuel at petrol stations
  - Delivery notes: turnovers that are declared on the receipt but will be processed via a different system (e.g. central billing) but will be invoiced by the same company
  - Training turnovers: transactions that are made for testing or instruction reasons
- All data has to be processed in the specified format to the TIM.
- The responses of the TIM (at least the sequence number and the signature) have to be stored and printed along with the other data on the receipt
- In case of errors an appropriate handling has to be applied (error signalisation, retry if appropriate).

4.4 Print of verifiable receipts

One essential element of the INSIKA system is the verification of printed receipts without the access of stored data.

Thus, the receipts have to contain all data, which are included within the signature. Due to legal requirements this has to be done anyway. Further information on printed receipts is included in the document "INSIKA_Exportformat-[version]".

4.5 Storage of the journal

All transactions have to be saved with the corresponding sequence numbers and signatures.

There is only one requirement on the journal – the XML export data has to be generated from the journal. For the journal itself own optimised formats can be used. Then the XML format will be generated when exporting data.

It is possible to storage the data in the cash register for longer periods. The data may also be transferred to another system (e.g. PC) on a daily or weekly basis.

When using optimised journals current tests result in data volumes from less than 50 kByte per day (at 200 transactions with 3 items each) up to 600 kByte per day (at 1.000 transactions with 20 items each).

In any case data backups on a regular basis have to be followed, as there is no difference to other fiscal relevant data.

4.6 Daily reports

Daily a signed INSIKA report has to be done. A report reads the sum totals inside of the TIM that contain the total turnovers and returns it as signed data from TIM to the cash register. The reports have to be added to the journal. In most cases the INSIKA report will be integrated within a cash registers function that is already available.

The reports speed up the verification process, as in many cases the signature verification of every single transaction can be omitted.

Additionally the reports allow for an estimation of turnovers for periods where no other data is available.

4.7 Journal handling

Especially in companies managing several branches relatively high data volumes can be generated. For a tax audit the data must be provided for every consecutively.

Depending on organisational conditions (e.g. operation of cash registers on different locations, temporal replacement devices, etc.) a pre-processing of transaction data has to be applied. These requirements are not derived from the INSIKA system but determined by current legal regulations ("GoBS", "GDPdU") and should be part of every back office software today.

4.8 XML export of the journal

As mentioned before all transaction data has to be provided in a defined XML format.

Internally cash registers can use various journal formats that may result in reduced storage size or enhanced speed. The XML data has to be generated when exporting data at the latest.

The XML export interface is specified in the document "INSIKA_Exportformat-[version]". This document contains the XML schema and the structure and contents of INSIKA XML docu-

ments. All data that has been signed by the TIM has to be recovered from the XML data. This is a prerequisite for successful signature verifications.

For every transaction the export data has to contain the sequence number that was generated by the TIM. The consistency of these sequence numbers ensures the completeness of the data.

4.9 Auxiliary functions

For a proper operation of the system the following auxiliary functions are required to be implemented in a cash register:

- TIM activation: a new TIM will be activated once, using a transport PIN. This avoids misuse of the TIM (e.g. stolen from mail delivery)
- TIM deactivation: A TIM can be used for a defined period only (e.g. 10 years). After this period the TIM should be deactivated, preventing further signature generations. The deactivation provides a signed report that proves the deactivation. Therefore there is no need for a physical access to the TIM.
- Readout of the digital certificate: The XML export file has to contain the certificate for every used TIM. The cash register has to read the certificate once a new TIM is inserted. This digital certificate has to be stored inside cash register and added to the XML export data.

The following functions will increase handling comforts:

- Further reports: Apart from daily reports the TIM provides reports for arbitrary periods. This feature allows users to check signed turnovers.
- Catalogue of TIMs: When using a considerable number of TIMs (as in companies managing several branches) central managing software will help keeping track of the current situation (e.g. Which TIM is integrated in which cash register and since when?)
- One's own verification: For ensuring correct data all data can be verified before e.g. supplied in a tax audit. The verifying procedures can be integrated into cash registers or made available via back office software. As INSIKA is based on open standards (XML, ISO7816, ..) and the specifications are freely available there is no limitation in developing one's own verification software.

All listed functions can be implemented in a cash register or in a separate PC system. The latter will be advantageous especially to centralise the TIM handling for companies managing several branches.