Whitepaper: Fiscal systems – demands and solutions

Jens Reckendorf, Dr. Norbert Zisky

January 2015

"Simplicity is prerequisite for reliability."
– EDSGER W. DIJKSTRA

General remarks

About this document

The authors haven't learnt yet of any systematic presentation and analysis of possible solutions for the demands of fiscal authorities on cash registers as well as their advantages and disadvantages. This document is meant to fill the gap. It should serve as background information for the general discussion about cash registers and fiscal systems, without assuming detailed knowledge in these fields or in the field of IT-security solutions.

This document does not discuss questions concerning the motivation for introducing demands on cash registers, i. e. type and scope of tax evasion by means of manipulations, as well as general problems of the tax system[1]. Only technical aspects and costs are in focus.

Due to lack of space we don't present here any detailed introduction into the basics of cryptography and the INSIKA system. Links to additional literature can be found at the end of the document.

Terms

To have clear terms all systems that serve for registering and documenting cash transactions are referred to as "cash register" in the following – from a simple low-cost-system to the module of an ERP software, which takes on the respective function.[2]

"Fiscal systems" are all cash registers subject to special, technical and organizational demands of the tax authorities exceeding the general demands on electronic accounting systems.

A "trustworthy component" is the part of a system that carries out security-relevant tasks and is protected against unauthorized access in a way that all parties involved can rely legally binding on its correct function. For this purpose, the security of this component needs to be examined by an independent, trustworthy authority.

Authors, possible conflict of interests

Jens Reckendorf is member of the Board of Vectron Systems AG, a manufacturer of POS systems, and responsible for technology and development. He represented Vectron Systems AG in the INSIKA[3] project group.

Dr. Norbert Zisky is head of the working group "Data communication and -security" at the Physikalisch-Technische Bundesanstalt (PTB – national metrology institute of Germany) in Berlin and was the manager of the INSIKA project.

The INSIKA system has been published and is not subject to any patent protection. No licence fees or similar charges arise for use. Neither the authors nor the organizations they represent do have any direct economic advantages or disadvantages if any specific solution described in this document is used. However, it is in the interest of any manufacturer of POS systems who is active in different markets – and this includes Vectron – if demands of fiscal authorities can be met as reliably as possible at the lowest possible initial- and current expenses.

Basics

The problem

With the change from paper-based accounting to electronic systems in the second half of the twentieth century it became basically possible to modify data quite easily and without leaving traces. The legally demanded immutability of accounting data was relatively easy to verify in the paper age – in case

1 In discussions about this topic it is repeatedly argued in a more or less open manner that due to high taxes and social charges a tax evasion would just be some kind of "self-defence". However, this aspect has to be discussed separately from technical solutions that prevent tax evasion, thus contributing to uniform taxation.

2 This includes scales with cash register functions as well as vending machines. With the introduction of legal measures, these terms have to be defined precisely in order to prevent evasions.

3 The acronym INSIKA denotes the German project "INtegrierte SIcherheitslösung für messwertverarbeitende KAssensyteme" ("integrated security solution for cash registers processing metered values"), under the direction of the PTB with participation of several cash register manufacturers and partly funded by the Federal Ministry of Economics and Technology. Cf. http://www.insika.de/en

of digital data however, this is only possible within a suitable technical and legal framework.[4]

In many application fields this problem was and is of hardly any importance. But cash registers were more and more used to reduce registered sales retroactively. With the increasing extent of audits by fiscal authorities the applied methods of manipulation have become more and more sophisticated – ranging up to an almost automated and difficult-to-prove manipulation by means of "zappers", i. e. manipulation software that is loaded to the system temporarily and does not leave any direct traces.[5]

Respective discussions in tax administration and politics started at different times in the various countries – partly as early as in the 1980s, partly after 2010.[6] In Germany the problem was first made a public subject in 2003 by the Federal Court of Auditors,[7] and finally led to the INSIKA development.

History of fiscal systems

At the beginning of the 1980s the first fiscal systems were developed in Italy where they have been mandatory ever since. The basic approach was adopted in other countries with more or less extensive modifications which led to legally, organizationally and technically very inconsistent solutions. The technical development in the field of cash registers also resulted in new approaches to fiscal systems. The actual fiscal memory technology for example was partly moved into modular printers, partly into special "fiscal boxes". The journal recording on paper was mainly replaced by electronic journals. Cryptography (encryption, hash values, signatures) is more widespread now.

Fiscal systems are mandatory e. g. in the following countries: Argentina, Belgium (hospitality only), Brazil, Bulgaria, Greece, Italy, Canada (only Québec, hospitality only), Latvia, Lithuania, Poland, Portugal, Russia, Sweden, Turkey, Hungary and Venezuela.[8]

4 Huber, Reckendorf, Zisky: Die Unveränderbarkeit der (Kassen-) Buchführung nach § 146 Abs. 4 AO im EDV-Zeitalter und INSIKA, BBK Nr. 12 bis 14, NWB Verlag, 2013 (in German).

5 Cf. http://en.wikipedia.org/wiki/Automated_sales_suppression_device (retrieved July 4, 2014)

6 OECD: Electronic Sales Suppression: A Threat To Tax Revenues, February 2013.

7 Bundesrechungshof: Bemerkungen 2003 zur Haushalts- und Wirtschaftsführung des Bundes, 54, S. 197-198 (in German).

8 Source: http://de.wikipedia.org/wiki/Fiskalspeicher (in German, June 19, 2014) and own research.

Special challenges

The organizational, legal and technical frame conditions for fiscal systems lead to some particularities, which differ from designing and implementing other IT-systems. These should be known for a better understanding of the situation.

National solo efforts

So far there has not been any international standardization for fiscal systems. Even if many of the national solutions show certain parallels, every country finally pursued its own way. One reason is definitely the fact that fiscal systems are subject to national tax legislation, even in the European Union. Numerous solutions also show elements of protectionism, thus creating market entry barriers for foreign suppliers.

Individual interests

Interests of the parties involved differ considerably. Tax authorities are mainly interested in making manipulations obvious. The reverse procedure of furnishing proof – the proof of formal correctness – particularly matters to the end-users, i. e. the taxpayers. Another important aspect for the end-users is to minimize costs. Suppliers of different systems (cash registers, fiscal printers or external memory units) have different economical interests. Political influences[9], too, play an important role.

Experience has shown that during the discussion on the introduction of a fiscal system , the interests of all the parties involved are not necessarily represented accordingly and evaluated neutrally. Depending on how intensively a party was involved in the decision process, the resulting systems can vary tremendously and hardly ever lead to the ideal technical solution.

"Cultural differences"

Fiscal systems are designed in cooperation between tax experts (administrative and legal experts) and those for special technical disciplines (cash registers, IT-security solutions). Their approach differs considerably, and the then necessary political decisions also follow different aspects.

In the field of tax administration there is a continuous development of regulations, due to the general framework. This means the regulations are slightly modified repeatedly instead of be-

9 This reaches from lobbying of trade associations to discussions within the administration about assignment of actual or alleged costs to different parts of the administration.

ing completely re-designed. Regulations usually are "principle-based", i. e. a principle or an objective is defined (example: "Data has to be stored immutably"). Scope of interpretation and single case decisions are often inevitable.

Technical solutions however, require completely designed systems. Implementation requires a "rule-based" approach, i.e. precise definitions (example: "Data has to be protected by digital signatures of a trustworthy sub-system"). Interpretation problems have to be avoided.

The most important resulting misunderstandings and misinterpretations will be formulated and discussed in chapters "Security", "Processes" and "Design and introduction".

In politics, compromise and balance of interests often prevent stringent solutions. This is a grave problem when these interventions are made without detailed knowledge of the respective facts.

The quality of fiscal systems developed within this area of conflict strongly depends on how these contradictions are handled and whether a sound concept can be realized after all.

Questions of liability

For manufacturers and users of fiscal systems there are liability risks. If a system is found to be non-compliant, the user is threatened with an estimate of his tax base. Depending on the manufacturer's negligence, claims under criminal or civil law can be asserted. Even if a manufacturer does not act intentionally or through negligence, he will be obliged by the users to rectify the shortcomings of the product – which does not just imply high costs but also damage to his image.

Market pressure

In some trades users exert strong pressure on manufacturers of cash registers to allow for manipulations. As soon as one manufacturer gives in to this pressure, other competitors will follow. This does not just apply for "unprotected cash registers", but also certified fiscal systems, as examples of the recent past show.[10]

What to expect from a good fiscal system?

As with any technical system, requirements and objectives for fiscal systems need to be formulated prior to concept and development. However, respective documents are avail-able only for few systems. We will therefore try to describe the requirements in a universally applicable way.[11] Only the ones for a fiscal system that exceed those to a non-protected cash register are described here.

The requirements are classified into three commonly used categories: functional requirements, non-functional requirements and constraints. Mandatory requirements are denoted by "shall", optional requirements by "should".

Functional requirements

Functional requirements determine what a system is to perform, i. e. the tasks it carries out.

Guarantee integrity

Modification or deletion of already recorded data shall be prevented or shall be identifiable not regarding how the modification occurred (e. g. through deliberate manipulations, technical or operating errors).

Guarantee authenticity

The recorded data shall clearly be traceable to the author. It shall be impossible to record data using a false identity. Consequently the author cannot deny the authorship of the data.

End-to-end protection

The protection mechanism shall be effective from data collection to the audit. So all intermediate units that store or transfer data cannot influence the security of the overall system. Therefore they do not have to be trustworthy. This can be compared to sending a message in a sealed envelope – no matter how the message was sent, the seal will always indicate any unauthorized access.

Making the extent of modifications determinable

If recorded data was modified or deleted – whether through manipulation, technical failure or data loss due to operating

10 In 2014, massive security deficiencies became known for certified fiscal systems in Portugal and Hungary – see footnotes 4 and 5 in box "Misunderstandings: Security".

11 These demands are not based on a norm or any other standard, because these do not exist. They were formulated by the INSIKA project group, among others things based on a concept of the German fiscal authorities and the analysis of existing fiscal systems.

errors – it shall be possible to determine the extent of modifications.

Provide check mechanism

Any fiscal system can be circumvented by not registering data at all (e. g. by using an additional, non-protected cash register). This can only be prevented by random checks. The system shall therefore provide a safe mechanism for these checks.

Guarantee data security

The system shall provide appropriate protection against data loss. This can be implemented within the system (e. g. via data storage on two separate storage media), or, more safely, by allowing data storage to external memories without violating the other requirements (especially concerning integrity and authenticity).

Non-functional requirements

Non-functional requirements determine a number of features that are not covered by functional requirements. They mainly determine how a system works. A large part of the requirements can be considered as "quality measures".

Low complexity

Complexity generally increases a system's error-proneness and its costs. In case of security solutions, errors are often potential security vulnerabilities. The complexity shall therefore be reduced as far as possible.

Fault tolerance

The effects of modified stored data, technical errors, system errors etc. shall be minimized as far as possible. A faulty record for example must not have the effect that following records cannot be verified or evaluated anymore.

Trustworthy part of the system as small as possible

Any security solution requires one or several components that are trustworthy. As soon as this trustworthiness cannot be guaranteed (anymore), the whole system has to be classified as insecure. In order to minimize efforts and security risks this trustworthy part is to be kept as small, simple and inexpensive as possible.

Security evaluation possible

It shall be possible to have the security-relevant system parts (processes, hard- and software) verified by independent third parties. This verification is to guarantee the highest possible level of security and trust level. Check criteria and processes should follow an existing standard if possible (e. g. Common Criteria[12]) and not be defined especially for the respective system.

Easy checks

The check mechanism mentioned under functional requirements shall be as easy as possible at the lowest efforts and should not require access to information that is difficult to provide e. g. data of the fiscal system the correct use of which is being checked.

"Minimally invasive"

A fiscal system is based on available cash registers, which cover a broad range in terms of technology and functionality. In order to minimize integration problems, costs and risks the additional components for data security shall cause the lowest possible intervention into the existing system.

Integrable into as many systems as possible

The demands on the cash registers which present the basis of the fiscal system (e. g. concerning operating system or interfaces) shall be minimized. This allows the largest number of systems to be retrofitted and leads to cost reduction and an easier introduction.

Clearly specified interfaces

The system interfaces shall be specified as clearly as possible to avoid interpretation problems and incompatibility.

Lowest possible dependency on specific technologies

The guidelines for a fiscal system normally prevail much longer than does the life cycle of most IT technologies. The use of certain interfaces or storage media for example is problematic. Dependencies should therefore be minimized and, where they are inevitable, well-thought-out and well specified.

Adjustable to new security standards

For all IT security solutions, including cryptographic procedures, one has to bear in mind that adjustments to new security standards may be required if a system is in danger of being "hacked" or even was. In such cases a fiscal system should be upgradeable with a minimum effort.

12 "Common Criteria for Information Technology Security Evaluation" is an international standard for computer security certification.

Misunderstandings: Processes

"Audit will become more reliable if a lot of redundant information is reconciled"

In designing fiscal systems as well as in auditing, much emphasis is often put on reports, i. e. summarized data. The concept behind this seems be the detection of inconsistencies (by reproducing the totalling). This may be correct for manipulations of paper-based accounting, as manual interventions lead to mistakes sooner or later.

If a system with digital recording of single transactions is manipulated (because it is not protected sufficiently) all the reports will be calculated in such a way that the data in total is plausible. A reconciliation of different reports will therefore not detect manipulations but only increase the efforts for the audit.

Today, the availability of single transactions allows totalling during the audit. When guaranteeing the integrity of each of the single transactions, the summarized data, too, will be reliable.

"Program changes at the cash register must be recorded"

A repeatedly uttered demand is that cash registers and fiscal systems have to record changes of the programming (i. e. parameters, program data etc.). This demand obviously derives from the knowledge that there are manipulable systems, where the manipulation requires a change of programming (e. g. switching on a "training mode" that suppresses the regular recording of sales). If however, you do not trust the manufacturer because he integrated manipulation functions into the system there is no reason to believe that a respective re-configuration is recorded correctly or that the recording could not be changed.

The only working solution therefore is to specify the system in a way that its security cannot be influenced by program changes. If the system security is exclusively guaranteed by a trustworthy component and not by the manufacturer of the cash register, this requirement will be met automatically.

"A technical solution can replace checks"

A number of fiscal systems exist in which regular checks of the correct system use (cf. "Requirements") were not planned. This was obviously done by ignorance or for political considerations, mainly because of the actual or alleged costs for these checks.

In return, one tried to make the check superfluous by introducing technical measures. To evaluate this approach, one has to look at the fundamental manipulation options at the time of data acquisition (later manipulations can be avoided quite easily by means of technical measures):

1. Manipulated data recording using the provided system functions (the recorded sales are lower than those actually generated)
2. Omission of sales (sales are not entered to the cash register)
3. Use of multiple cash registers (part of the sales is entered to a cash register where the data are not declared for taxation)

Of the indicated options above only method 1 can be made more difficult through technical requirements on the cash register (with huge efforts, resulting from the then required certifications and market surveillance).[1] The two other methods[2] cannot be avoided at all without human intervention. A good fiscal system however, can make the required checks easy and safe.

"Compulsory receipts are not that important"

Only a receipt allows the absolutely required random checks with justifiable efforts. These checks are inevitable as they provide the sole means to detect when a system was not used or data was registered with delay.[3] Every fiscal system that the authors know includes the obligation to issue a receipt for every sale.

---

1 With a slightly higher effort manipulations are still possible. Example: A certified fiscal system running in an open-architecture environment (e. g. Windows) is being used together with a second, non-certified cash register software. The operator only uses the second software that transmits only a part of the transactions to the certified software (which does not have any manipulation functions). This is done through keystrokes simulated on the operating system level. There is no way for the certified software to distinguish them from "real" keystrokes. This attack can only be detected by random check but not by retroactive audits. Banning open architecture systems does not seem to be feasible because their high market share.

2 Attentive visitors will have observed in various countries with compulsory fiscal systems that non-registration and parallel use of non-fiscalized cash registers have taken on such an extent that the whole approach was rendered useless. This is made possible by missing or too few checks (whereby it is also important how easily a check of the respective system can be carried out).

3 If data is collected unsecured for a certain time and is only registered later in a safe system (which can be made manually or automatically), any manipulations are possible during this time. The chain of security measures is then interrupted at the very beginning.

Minimize effects of security vulnerabilities

If a single system is compromised (e. g. because a cryptographic key was revealed to non-authorized parties), this must not jeopardize the security of all the other systems.

Constraints

Each technical system is operated in a specific environment. The system has to take into account the restrictions that result from this environment.

Minimize costs

Costs shall be minimized. This applies to one-off costs (mainly development costs) as well as for unit costs. Additional recurring operating costs should be avoided.

Consider tax law as legal framework

A fiscal system is designed to comply with fiscal law guidelines. It has to provide fiscal authorities and users with the highest possible legal security. It therefore shall have a structure that can easily be integrated into the existing fiscal law framework.

Avoid distortion of competition

Any regulatory intervention in an industry can distort competition. This shall be avoided as far as possible. All manufacturers should have the same starting conditions for adjusting their solutions, even if their products and company sizes differ considerably.

Embedded into concept a check and audit

A fiscal system cannot exist as a technical solution alone but must be embedded in a concept for checks and audits, which the administration can put into practice. This concept shall be part of the system's specification and development.

Approaches

Here we will outline all the basic approaches for meeting the demands of fiscal authorities known so far.[13]

Systems without technical protection

In case of unprotected systems there are no tangible guidelines for cash registers. Only the general rules of tax law are applied to these systems. If technical protections exist, they are not acknowledged by fiscal authorities because the legal basis is missing. According to the definition used here, these systems do not belong to fiscal systems.

The greatest disadvantage of these systems is the insufficient security. This results in a high proneness to manipulation, significant audit efforts and a lack in legal security for users of these systems.

Systems without technical protection with certification

For systems without technical protection, declarations of compliance (given by the manufacturer) or certifications (by third parties) are possible; however, these are not very significant.[14] These measures do not provide sufficient security to prohibit data modification.

According to the definition used here, these solutions do not belong to fiscal systems either.

Conventional fiscal systems

In accordance with the technology available in the 1980s these system were mainly based on a mechanical protection of the memory against unauthorized access in conjunction with design requirements for the overall system. At the time, the actual fiscal memory consisted of EPROMs[15], which were tied together with a microprocessor to a module, e. g. with cast resin. That way, the EPROM memory could not be erased. Due to the low memory capacity only the daily sales were stored. To make such a system safe, it had to be protected completely against interventions since otherwise the sales could be manipulated prior to writing them to the fiscal memory. The complete cash register had to be sealed, the hard- and software had to be certified.[16] Today, those systems use more modern technologies though the same basic principle (e. g. flash memories).

13 Parts of this chapter are based on http://de.wikipedia.org/wiki/Fiskalspeicher (in German, retrieved June 10, 2014).

14 For example the "Keurmerk: Het betrouwbare afrekensysteem" in the Netherlands or software certificates of auditors in Germany or Austria.

15 EPROMs are memory chips that can be erased by exposing them to ultraviolet light but which are no longer used today.

16 Any change at the system (hardware and software) requires a new certification. Monitoring the systems during operation requires high efforts and is to be carried out by technical experts.

Misunderstandings: Design and introduction

"POS system manufacturers and tax experts design good security solutions"

Design and implementation of secure IT systems is a special field for which relatively few experts are available.

Most fiscal systems were designed without the support of renowned security experts. Instead, they are mostly designed within the circle of directly involved parties, i. e. members of fiscal authorities and representatives of the cash register industry, especially providers of fiscal systems. Design flaws cannot be avoided with this approach. This problem is all the more critical as IT security solutions seem to be quite simple at first sight so that often people do not see the necessity to involve experts.

"Existing systems are proven and therefore good"

Fiscal solutions practically never arise from competition between various approaches but are designed and legally introduced. Usually there are no previous field tests. Since amendments entail extreme efforts and are only possible with transition periods, existing solutions may only be improved slowly, if at all.

So the very fact that a system is used in practice does not allow any statement on its quality. This also explains why a number of countries use systems that evidentially do not work according to the demands described above.

"Voluntary solutions do also work"

Bei einem freiwilligen Einsatz von Fiskalsystemen ist es grundsUsing fiscal systems voluntarily basically allows creating a situation that ensures data integrity from the time of storage onwards. However, this requires in any case one security component that a trustworthy authority is responsible for.

Further it has to be guaranteed that all sales are entered to the system. This is exclusively possible by means of random checks, which can only be made when the use of the fiscal system is compulsory. For a useful audit, all the fiscal systems that a taxpayer uses have to be known by the auditor – information which is not available in case of voluntary use.

This is why voluntary use only meets a small part of the requirements and therefore does not make sense.

"A fiscal system generally leads to more bureaucracy"

In discussions about the introduction of fiscal systems you normally hear the argument that this involves "even more bureaucracy". A well-designed fiscal system changes practically nothing for the user but guarantees that sales data is documented in a formally correct way. This entails a considerably facilitated audit and reduces the duty to document.

"A fiscal system means total surveillance"

Here you have to bear in mind that tax law already allows far-reaching access of fiscal authorities to taxpayer information – an existing extensive surveillance. Fiscal systems only protect a part of this data from modification, which on the other hand reduces the demand for checks and audits to disclose possible manipulations.

Solutions with online data transfer in contrast increase the surveillance options of authorities which surely is a point for criticism.

"Criminal liability for development and sale of manipulation software is decisive to solve the problem"

Criminal liability for developing manipulation software (together with liability for the consequences of use) is definitely as a supporting measure helpful though the authorship is often difficult to prove. But first and foremost a fiscal system has to be secure thanks to its technical design and not due to the fact that attacks can be prosecuted criminally.

The requirement of legal consequences for non-registration of data (whether by non-entry or by using a second cash register) and for aiding and abetting must of course be taken for granted.

The increasing modularisation of cash registers, i.e. the separation of keyboard, display, CPU and printer was contrary to the original concept of integrating all components into one housing. This was solved by means of the "fiscal printer" where the fiscal memory module is installed in the modular printer.

Since the originally used paper-printed journals (i.e. the recording of all transaction details) can hardly be evaluated and audited in practice and the available memory capacities were increasing quickly e. g. through flash memories, more and more solutions with electronic journal recording were developed.

Although the conventional solutions basically meet the main requirements, the high efforts for development, certification and operation are disadvantageous. Complex technical requirements and the necessary certification of product improvements result in low-performance but extremely expensive products.

Cryptographic solutions

In an effort to make fiscal systems more secure, some systems stored the data crypto-graphically protected. Here, mainly digital signatures but also encryption techniques are used.

A distinction has to be made between systems that use a trustworthy component for the cryptographic functions (e. g. a certified "fiscal box" or a smartcard) and those which implement it in a non-trustworthy part of the system (e. g. as part of the application software).[17]

So far, the "Security through obscurity"[18] principle is used in most cases – cryptographic solutions that meet current standards are rare. Therefore, all the systems known by the authors (except for INSIKA) still require a certification of the overall system.

The addition of cryptographic elements does not avoid the basic problems of conventional solutions (the complex certification in particular), it only means higher effort without significant effects. Cryptographic solutions without trustworthy components can even suggest a security that does not exist.

17 "Fiscal boxes" are used e.g. in Sweden (together with encryption) and Belgium (with digital signatures). A signature-based solution without a trustworthy component is used in Portugal.

18 Attempt to use secrecy of design to provide system security. State-of-the-art cryptographic systems use published algorithms – only the cryptographic keys have to be kept secret.

Online systems

Some countries (e. g. Serbia) use systems that require a direct online data transfer to the fiscal authorities.

In addition to costs for data transfer and storage, the dependency on the data connection is a big problem. In many countries this concept does not comply with the generally accepted ideas of the state's supervisory rights.

Why the INSIKA system is the best available solution

The INSIKA system is based on the above mentioned requirements. It completely meets the functional and non-functional requirements and complies with the constraints.

Concept

The INSIKA system is based on a digital signature for each transaction, which is generated by a smartcard. The smartcard also guarantees that the transactions are numbered consecutively. The signature is printed on the respective receipt and permanently stored together with the transaction data.[19] For an audit the signed data is provided in a defined format, e. g. by data export. This results in the following:

- A valid signature on the receipt proves that the transaction data was signed and numbered by the smartcard – it therefore proves the correct registration. Vice versa, a missing or invalid signature proves that data has not been registered properly.
- The signature reveals any modification of data.
- The numbering shows if bookings are missing in the recording.
- The signature allows the tracing back the record to the smartcard owner.
- On the other hand you can prove that data was not modified and is complete.
- In case of data loss, totalisers on the smartcard and in daily closure reports allow the determination of totals for data gaps.
- The system security is exclusively based on the described mechanisms – there are no additional conditions and hence no certification for the overall system.

19 In most countries cash registers have to store all transaction data anyway so that when using INSIKA only a few data would be added.

For a more detailed introduction to the INSIKA system please see the links at the end of this document.

Advantages

Only minimum intervention to existing cash registers is required. When finalizing a transaction the software has to communicate with the smartcard, print the result onto the receipt and store it electronically together with the transaction data. The proof is provided with every signed receipt. No additional conditions or respective certifications are required. Still, the security level is very high. The intervention in competition is minimized, see "Analysis: Market intervention by INSIKA".

Implementation of requirements

The following overview lists the requirements that were expressed above with an explanation how the INSIKA system meets every single demand.

Practical experience

Starting 2011, INSIKA was introduced to the taxi trade in Hamburg, accompanied by subsidies for hardware installation. Within two years three manufacturers of taximeters developed products ready for mass production, which since mid of 2012 have been installed to 60% of the Hamburg taxis (2,000 of 3,300). The traffic trade supervision and the fiscal authorities Hamburg are completely involved. Application and issuing of smartcards is effected via the D-Trust GmbH, a subsidiary of the Bundesdruckerei, a government-owned company specialized in Secure ID technology and banknote printing.

In parallel, cash registers were tested in practice over several months. The whole chain was covered, from installation to audit of the secured data by the fiscal authorities.

In all cases the INSIKA system worked as specified. The practicability has therefore been clearly proved.

Contact and further information

- INSIKA flyer – brief overview of the system: http://www.insika.de/images/stories/INSIKA/INSIKA_Flyer_EN_2013-04.pdf
- PTB report IT-18 – covers all essential aspects of the INSIKA project in detail: http://dx.doi.org/10.7795/210.20130206a (mainly in German)
- Huber, Reckendorf, Zisky: Die Unveränderbarkeit der (Kassen-) Buchführung nach § 146 Abs. 4 AO im EDV-Zeitalter und INSIKA, BBK Nr. 12 bis 14, NWB Verlag, 2013 (in German)
- After registration you can request the INSIKA specification at http://www.insika.de/de/spezifikationen (in German)

Contact:

INSIKA – ADM e.V.
An der Corvinuskirche 22-26
31515 Wunstorf, Germany
eMail: info@insika.de

The INSIKA project was funded by the Federal Ministry of Economics and Technology under grant number MNPQ 11/07.

Misunderstandings: Security

"A complex system is more secure"

Many – particularly recent – fiscal systems are extremely complex.[1] The sole legitimate reason for this complexity and the inevitably resulting higher costs can only be the fulfilment of the requirements mentioned before.

Experience with different technical systems however shows that complexity increases the probability of errors – in fact above average, as not just the number of components increases but also their interaction. A more complex system therefore normally is more liable to error than a less complex one. In case of security solutions, every error is potential security vulnerability.

1 Even outsiders can easily recognize this at the dimension of the respective specifications. The Belgium system is described on over 100 pages – though a large number of detailed questions remain unanswered. The system's complexity was one of the reasons why the original introduction date January 2011 will be exceeded by at least four years. Efforts for manufacturers are immense.

Good security solutions are therefore only as complex as necessary to meet the requirements. Any additional complexity increases costs and efforts while the security level decreases.

Additional security mechanisms increase security"

Every security system has to be seen as a chain of various measures. If one link of the chain fails, the system as a whole is insecure. If additional measures do not strengthen the weakest links but others, they are obsolete and only increase complexity and costs.

A combination of different methods (e. g. digital signatures and mechanically protected memory) can only be useful if one method compensates the weakness of the other. Yet, you still have to ask whether the basic approach is useful at all.

"A state-of-the-art encryption algorithm is used – the method is therefore safe"

An insecure cryptographic algorithm can of course not provide the basis for a secure system. Yet, a number of secure methods are available today, of which one can assume that they will not be broken in the foreseeable future.

In practice, security vulnerabilities normally occur due to an incorrect architecture or faulty implementation of hard- and/or software. The mere use of a secure algorithm (e. g. RSA or ECDSA with suitable keys for creating digital signatures or AES for symmetric encryption) does not allow a statement on the security of the overall system. If for example the private keys are not exclusively stored and used in secure hardware (like a suitable smartcard), the overall system has to be considered as insecure. A key management carried out by non-trustworthy parties, too, makes a system insecure. "Naive" implementations of cryptography do therefore not correspond to high security standards.

All the up to now successful attacks against modern cryptographic methods did not attack the algorithm but used weak points in implementation or deliberately created "backdoors".[2]

"Certification guarantees security"

Certification first of all just means that an independent third party examines whether the certified object meets defined demands. The suitability of these demands and thus of the certified object for a defined purpose is not assessed.

Smartcard software for instance can be evaluated according to Common Criteria and a cash register can be certified by an auditor[3]. In both cases, the system is certified. The level of trust, however, differs considerably.

Various examples prove that certifications in the field of cash registers do not guarantee security – in the first half of 2014 e. g. in Hungary[4] and in Portugal[5].

"Low security is better than none"

Particularly in view of the "political feasibility" you often hear that introducing a part of the planned measures is "better than nothing". In case of security solutions however, it is crucial that the chain of measures is not interrupted – should this be the case the system will become worthless. If for example you secure data by means of a digital signature after a manipulation was possible, the signature is absolutely useless.

The single measures only create "pseudo security". As a result you may rely on a system although this is not justified. Manipulation may even be hidden behind this pseudo security.

A well-designed security system has to be implemented as it was planned – it is not suitable for "political" compromise.

"Any technical system will be broken"

No system can be absolutely secure. Yet, correctly planned and implemented crypto-graphic security solutions are the best methods for protecting data today.

If the working principle of a system is published and if it uses standard methods (like smartcard hardware and cryptographic algorithms), independent third parties can permanently check the security. Potential weak points can be detected and removed quickly.

2 All the information that Edward Snowdon disclosed about NSA attacks on cryptographic methods suggest that modern techniques are basically safe because always (basically evitable) weak points in the implementation were used.

3 E. g. in Germany according to Prüfungsstandard 880 („audit standard 880") of the IDW (Institut der Wirtschaftsprüfer – „institute of chartered accountants")

4 In Hungary the licences for two certified fiscal systems were withdrawn because there were "backdoors" in the software (http://www.bbj.hu/business/electronic-till-system-in-shambles_75195, retrieved July 9, 2014)

5 End of April 2014, the Portuguese TV channel SIC reported massive fraud with certified fiscal systems in hospitality. According to an estimation of the fiscal authorities, 40 % of the invoices were manipulated. It was stated repeatedly that systems without manipulation options were non-marketable.

Requirement	Implementation in the INSIKA system
Guarantee integrity	Any modification of data can be detected by means of signature and sequence number.
Guarantee authenticity	Any signature can be retraced unambiguously to the respective taxpayer.
End-to-end protection	The data is signed when the receipt is issued and is henceforth secured until the audit takes place.
Making the extent of modifications determinable	Totalisers (in smartcard and daily closure reports) serve for determining the total sales for data gaps.
Provide check mechanism	The signature on the receipt allows a check.
Guarantee data security	The signed data can be copied and thus backed-up without security problems.
Low complexity	The INSIKA system only consists of the defined process, the smartcard with its interface and the export data format.
Fault tolerance	A damage of data does not influence the verifiability and significance of the other data. Faults can be compensated via totalisers.
Trustworthy part of the system as small as possible	Smartcard and smartcard issuer are the sole trustworthy components of the INSIKA system.
Security evaluation possible	The use of high-security standard techniques (Smartcard, ECDSA[20], PKI[21]), for which pre-evaluations are already available, allows evalua-tion according to the highest security standards.
Easy checks	A check only requires a receipt (and access to the certificate data) but no access to the data of the system which generated this receipt. Especially with a QR code for the receipt data the check can be made almost fully automatically.
"Minimally invasive"	INSIKA only requires a simple communication with the smartcard as well as the recording and print-out of some additional data. All the other recording duties are already existing.[22]
Integrable into as many systems as possible	The very simple hard- and software interfaces increase the probability that INSIKA can be integrated into an existing system.
Clearly specified interfaces	Smartcard interface and export data format are precisely specified.
Lowest possible dependency on specific technologies	Except for the use of a smartcard INSIKA is not linked to specific technologies like USB ports, SD cards, Internet protocols etc. Various providers are available for suitable smartcard hardware, soft-ware development and suitable PKI services.[23]
Adjustable to new security standards	By changing the smartcard and if necessary the signature algorithm the INSIKA system can be easily adjusted to new security standards.
Minimize effects of security vulner-abilities	INSIKA uses a standardized, open signature tech-nology with a different private key for each smart-card. If a single key was compromised this does not jeopardize the security of any other smartcard.
Minimize costs	By using a smartcard, easy integration, omission of certifications for cash registers and the upgrade option for many old systems, costs are reduced to an absolute minimum.
Consider tax law as legal framework	Since INSIKA is mainly a process and no specific device, it can be integrated straight into existing tax laws. Mainly additional demands to receipts and the respective digital recording are made.
Avoid distortion of competition	The easy integration, the resulting low development efforts and the lack of certifications minimize the intervention in competition. For a detailed explanation see "Analysis: Market intervention by INSIKA".
Embedded into check and audit concept	INSIKA prescribes the precise frame for checks and audits. The respective techniques successfully passed field tests.

20 ECDSA, the "Elliptic Curve Digital Signature Algorithm", is a method to generate digital signatures that provides extremely high security with relatively short signatures and high processing speed and is therefore perfectly suitable for INSIKA.
21 PKI means "Public-Key-Infrastructure". In the context of INSIKA this is a system which is responsible for issuing and management of smartcards and the management of cryptographic keys.
22 This applies e.g. for Germany, Austria, the Netherlands and France.
23 To be used in practice, all mentioned components have to undergo the respective evaluation process so that they can be acknowledged officially. Changing the provider will therefore cause certain efforts – however, a possible critical dependency on single a manufacturer or provider does not exist.

Analysis: Market intervention by INSIKA

Rights in the INSIKA concept

The INSIKA concept was published and can be used regardless of licences, patents etc. The publication rules out later applications for a patent by "free riders". No dependencies, legal uncertainties or costs arise.[1]

An analogy is the use of XBRL for the "electronic balance sheet".[2] In this case the fiscal authorities use a standard, which in Germany is supervised by an association.

➔ Here, no market interventions occur.

Central body for issuing of smartcards

The central issuing of smart cards and central administration of the cryptographic certificates is not a basic requirement. However, a decentralized approach requires merging the data so that the application is safe and the authorities are informed about all the issued cards. To reduce costs and efforts, a single central body is useful. This considerably facilitates the regulation of this official duty. If required, the respective service can be put out to tender. A permanent dependence on a monopolistic company cannot develop as a change of the provider is relatively easy.

Comparable centralised tasks would be printing bank notes, production of identity cards and passports or smart cards for digital tachographs. A decentralized and more complex solution was selected for the German electronic health insurance card.

➔ The administration of the INSIKA smartcards is a newly introduced process. No intervention into an existing market is made. Unrestricted competition is not possible for allocation of the task to a central body since strict regulation and control is required. Monopolistic situations and dependencies, however, are easily evitable.

Verification software

The audit of INSIKA data by fiscal authorities but also by users, tax consultants or tax auditors requires software for verification of data and receipts. This software implements processes and procedures which are fully described in the INSIKA specification and are not subject to third-party rights. Therefore, no obstacles for implementation of the corresponding software exist. For fiscal audits the manufacturer of the applied software has to be rated as trustworthy by the authorities.

An analogy is the software for data analysis by fiscal authorities, for which there are various providers.

➔ Here, no restrictions in competition arise.

Embedding of smart card to POS systems, taxi meters and other systems

The manufacturers of the respective systems have to embed the INSIKA smartcard, print out and store the supplied data. Compared to any other fiscal system this is just a minor intervention in the products. In comparison to most other legal requirements for electronic accounting systems, the requirements for INSIKA can easily be met. In contrast to the demands on accounting systems, which in most cases use a quite general wording, INSIKA provides the major (system-related) advantage of a precise specification. There is no room for interpretations and doubts – which reduces the implementation efforts considerably. Regulatory interventions in other economic sectors are much more severe.

Regulatory interventions when using digital tachographs, the toll collect system, calibrated scales, calibrated electricity- and water flow meters, smart meters etc. are comparable or even larger.[3]

Conventional fiscal solutions are very detrimental to innovation due to their massive interventions into the systems and the requirement to certify each product change. For INSIKA however, this is not true because interventions are minimized and no certifications are required. Since no resources for dealing with vague regulatory standards and the resulting problems have to be spent, the development of product innovations is even encouraged.

➔ The obligation to integrate smartcards presents an intervention in the market. Compared to numerous other regulatory interventions (on the part of fiscal authorities as well) it has to be considered as minor.

Standardised data format

For access to INSIKA data the data format is predetermined. This is required because the cryptographic verifica-

1 The ADM e.V. is entrusted with the trademark rights for "INSIKA". This is a project name, which doesn't have to be used when applying the process. Yet, if intended, the right to use can be ruled contractually.

2 Electronic transfer of annual statement to fiscal authorities, mandatory in Germany since 2012.

3 The mentioned examples refer to Germany; similar regulations exist for every country.

tion is only possible with a precise definition of contents and format. This definition only concerns the final format of data, i.e. the export from the system. No obligations exist for contents, procedures and technical solutions within the IT-systems. Except for the signature-relevant data, all data required for INSIKA already have to be stored and processed today.[4]

Comparable definitions of standard data formats exist for the electronic balance sheet and the ELSTER[5]-system.

➔ Here the intervention only affects the data format for a small part of data (cash sales), which have to be presented during tax audits due to already existing regulations. Most market participants consider the precise definition of these export formats to be an advantage as disputes about formal correctness can be avoided.

Processes

The INSIKA system has to be integrated into the processes of the respective companies. However, these remain unchanged. Obligations for recording, processing, archiving and provision of digital recordings already exist today. Only minor additions (application for smartcards, internal administration and use of smartcards) are required, which are not general interventions in existing structures.

This is comparable to the regular adjustments of mandatory information on invoices. General procedures remain unchanged but the contents need to be adjusted according to new regulations.

➔ Company processes are only affected to a minimum by INSIKA. There is not distortion of competition.

Costs for tax payers

The introduction of INSIKA involves costs for the modification of existing systems and for the purchase of smartcards. A slight price increase of new systems cannot be ruled out. Costs per POS system amount to far below hundred Euros to up to several hundred Euros depending on the initial situation. No running costs occur. Thanks to simplified tax audits and reduced documentation requirements (process description, cash register reports etc.) one can even assume a cost reduction.

This is comparable to any type of regulatory obligations involving costs for companies, e.g.: environmental protection, health and safety at work, employee rights, statistical reporting obligations, tax law changes etc.

4 This applies to every country that requires the electronic recording of sales transactions in detail. Germany as well as most other countries have such regulations.

5 German system for electronic tax declarations.

➔ In comparison to most other regulatory obligations for companies the costs involved by INSIKA are very low. In fact, even considerable cost reductions are possible.

EU law

Like with every national regulation, questions concerning EU law have to be considered. This question is posed with every fiscal, normally merely national intervention into economy. When discussing technical systems only, this is comparable to the obligation of software providers for accounting, payroll, time and attendance software or similar products to take into account the respective national law.

The same question arose in the past years during the introduction of much more complex fiscal systems in Sweden, Portugal, Belgium, Hungary and Croatia. Partially the so-called 98/34 notification procedure[6] was used; partially the introduction took place on purely national level. There are no known problems with competition law.

➔ The consideration of national, fiscal demands is the normal case for providers of respective systems – so there is no unusual market intervention.

Conclusion

Compared to many other regulations by the legislator or authorities the INSIKA system only presents a minimum intervention in competition. Any known alternative for fiscal systems (i.e. a secure documentation of cash sales) is either ineffective or a considerably greater distortion of competition.

6 Directives 83/189/EEC and 98/34/EC created a procedure where member states inform each other as well as the Commission prior to adopting technical regulations and change their drafts if required. A respective notification was made when the Swedish and the Hungarian fiscal system were introduced but not for the other mentioned countries.