INSIKA®: Cryptographic Tamper Protection for Cash Registers and Taximeters

current as of: 08/2014

INSIKA Project

The acronym INSIKA denotes the German project "INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme" (integrated security solution for cash registers processing metered values). This solution has been developed in a project under the direction of the PTB (Physikalisch-Technische Bundesanstalt, the national metrology institute of Germany). It is ready for implementation in practice.

Application of the INSIKA concept guarantees the complete, auditable recording of individual cash transactions when using an electronic cash register or similar systems like taximeters. The INSIKA system is a new approach to prove the compliance with generally accepted accounting principles. "Classical" fiscal systems are made of complex, specialized technical solutions, which in most cases save data in mechanically secured (e.g. sealed) storage modules. In contrast to these fiscal systems, INSIKA's security results from the cryptographically secured transaction data as such.

Using the concept requires a cash register, which communicates with a special smart card following clearly defined rules. All transaction data and data added by the smart card will be converted into a standard format.

Data created in this way is protected by means of standard high-security IT 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 cryptographic keys.

The INSIKA project was started to implement the requirements specification for improved security of POS systems and taximeters developed by two federal working groups of the BMF (Bundesministerium der Finanzen, the German Federal Ministry of Finance). These working groups were formed to comply with a requirement of the BRH (Bundesrechnungshof, the German Federal Court of Auditors). The PTB developed the necessary technical solution together with several partners from the industry.

The project was completed successfully in February 2012.

Principle of Operation

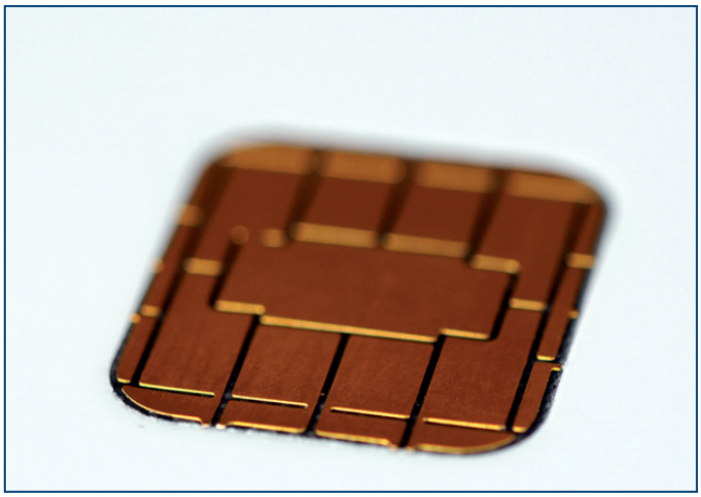
The manipulation protection is based on a digital signature which is generated by a smart card. This smart card is issued by an authorized central body. The system allows the correct recording of transactions to be checked at any time. All data that is protected by the signature cannot be changed undetected. Even with the loss or manipulation of that data the total sales can be determined.

The solution is based on a proven, advanced security technology. The implementation is relatively easy and there are no additional requirements such as type approval or certification for cash registers and taximeters. That is why this solution is outperforming conventional fiscal memory solutions in every way.

The overall design and specifications of all interfaces are fully disclosed.

Technology in Detail

INSIKA Smart Card



The system uses commercially available smart cards, which are equipped with special software to protect cash registers or taximeters. When introduced by appropriate legislation, the financial administration would procure the smart cards in an open tendering procedure and issue them to the taxpayers on

request. This task could also be assigned to accredited service providers.

The smart card can be connected via external smart card reader or integrated into the device (similar to mobile phones). The cash register software has to communicate with the smart card 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.

Digital Signatures

A key element of the solution is the use of digital signatures. Digital signatures guarantee that data comes from a certain person or system (in this case a certain cash register or taximeter) and that data has not been altered since the creation of the signature. The technology of digital signatures is mature, very secure and is widely used, e.g. in the banking sector or in the electronic filing of tax declarations. Most applications – as does the INSIKA-system – use smart cards to create the signature.

Receipts with Digital Signatures

Printed receipts and the related, electronically stored transactions get a digital signature. This signature is generated by the smart card. Furthermore, the smart card has an internal counter, which guarantees that each transaction and the respective printed receipt get a unique and consecutive number. The smart card also manages totalizers, which register the total sales. If stored data is lost, the important key figures (monthly turnover, negative transactions etc.) can still be determined. Signature creation, the management of sequence counter and totals are linked within the smart card so that on creation of a signature a new sequence number is assigned and the totals are updated.

Manipulation of POS Data

Worldwide and in many industries with a large share of cash transactions results are manipulated to evade taxes and social insurance charges. Since operational reasons still require entering all transactions into cash registers, the market demands functions to manipulate the sales data. Such a manipulation can be done either during data acquisition (e.g. by not entering all data or by using software features that manipulated data during the recording process) or after the fact (by changing already stored data, e.g. by so-called "zapper" software).

There are two requirements to prevent fraud: a random check of the correct acquisition of the sales data must be possible and it must be ensured that data cannot be changed undetected once it has been recorded.

Tax authorities try to fulfill these objectives either by technical solutions (conventional fiscal cash registers or INSIKA) or only through intensified tax inspections. To facilitate such inspections, more and more tax authorities require recording individual transactions rather than just totalized values. In Germany this has been done by a decree dated November 26th, 2010. However, with skillful manipulation of transaction data – especially using "zapper" software that automatically executes the appropriate changes – these changes are virtually undetectable, even with modern analytical methods.

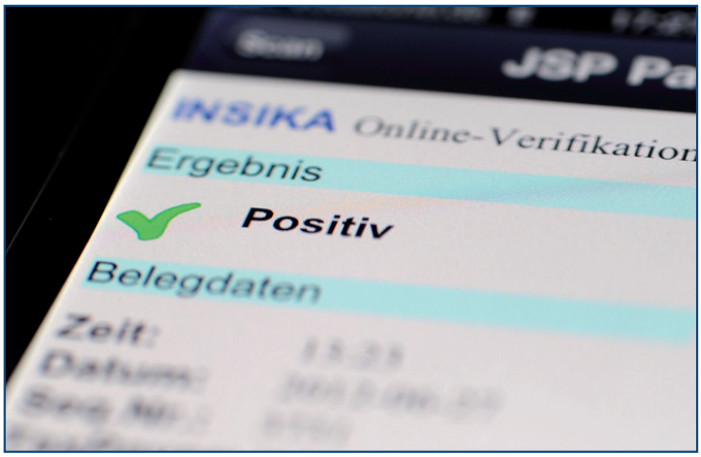
The requirement of issuing receipts with valid signatures ensures the proper recording of data, since all further steps are enforced within the smart card.

For the application to taximeters an online data transmission has been chosen as control mechanism. In this case the correct use of the system can be verified by the transaction data on the server instead of verifying printed receipts.

Verification of Receipts and Cash Register Data

Basically the INSIKA solution only requires the storage of transaction data which has to be archived anyway according to the German decree dated November 26th, 2010 (the situation is quite similar in many other countries). The only additional data is the digital signature. Using so-called profiles the system can be adapted to different types of data. Currently there are profiles for cash registers and taximeters.

Any verification of the data uses the stored and digitally signed transaction data. Since any modification of these data can be detected, all kinds of manipulation of other financial reports or the master data of the cash register are without effect. Even functions that were deliberately integrated into a cash register for data manipulation cannot attack the system. Therefore, a complex certification of the equipment is obsolete. The verification of the recorded data can be automated to a large extent, making this task much more efficient than it used to be. A standardized XML format is used, which allows a reliable verification of the signatures and avoids any uncertainty regarding format and content of the data.



The verification of receipts only requires information that is available on the printout itself. It is not required to have access to stored transaction data. Thus every printed receipt can be used to easily check whether it was created by a cash register using a valid INSIKA smart card. Any receipt with an invalid or without a signature provides clear evidence of fraud. Using a 2D code on the printouts, the verification can be made nearly fully automatic.

In contrast to the current legal and technical situation, taxpayers can prove the correctness of their transaction data for the first time.

Digital Signatures

Electronic signatures suitable for the INSIKA system 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 smart card 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. Even if a specific key has been "hacked" the security of all other systems is not compromised.

In order to guarantee that the public key corresponds to the private key or that the smart card has not been reported as stolen etc., so-called digital certificates are used. These are structured data records which link the owner as well as other key attributes with the public key. 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. Certificates therefore enable the protection of data authenticity and integrity. For the administration of certificates a so-called "Public Key Infrastructure" (PKI) is required.

Costs and Impact on the Market

Classical fiscal solutions are based on a mechanical protection of memory for the data to be secured, the secrecy of technical details and on a number of complex requirements for the operation of cash registers. The compliance is checked during a certification process. This approach makes such systems expensive, reduces functionality and constrains technical improvements (because every change requires a re-certification). The verification of the correct usage is difficult because the printed receipts have no security features. Furthermore, the level of security no longer meets today's standards.

In recent years some classic fiscal systems have been enhanced with cryptographic functions, but without re-designing them (e.g. in Sweden and Belgium). This resulted in complex solu-

INSIKA®: Cryptographic Tamper Protection for Cash Registers and Taximeters

History

The annual report 2003 of the BRH (Bundesrechnungshof, the German Federal Court of Auditors) 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. Therefore two working groups of the BMF (Bundesminsterium der Finanzen, Federal Ministry of Finance) developed a concept to protect the data generated by cash registers and taximeters.

The PTB (Physikalisch-Technische Bundesanstalt, the national metrology institute of Germany) and several industrial partners developed the corresponding technical solution within the frame of the INSIKA project. The INSIKA project was significantly promoted by the Federal Ministry of Economics and Technology within the scope of the "MNPQ-Transfer" support program (promotion of SMEs in the implementation of innovations in the fields of metrology, standardization, testing and quality assurance).

The changes in legislation required to introduce the INSIKA system were part of a draft law presented in July 2008. The sections relevant for INSIKA, however, were withdrawn from the draft before the start of the legislative procedure.

The BMF issued a decree "Archiving of digital files for cash transactions" on November 26th, 2010. It withdraws facilitations for the filing of cash register data and requires the recording of individual transactions. It also demands unchangeable filing but without making precise requirements and without defining any technical and legal framework. The demands of the BRH have not been fulfilled by this decree.

Nonetheless the INSIKA was continued as planned. As early as in 2008 working prototypes of the smart cards were available and could be successfully tested in laboratory and field tests. The technology is currently used in two projects for the protection of taximeter data, after the INSIKA concept was adapted to the taxi environment in 2010.

The INSIKA project was completed successfully in February 2012. Since then the ADM e.V. (Anwendervereinigung Dezentrale Mess-Systeme, Distributed Measurement Systems Users Association) supports and develops the INSIKA concept, especially the technical procedures that emerged from it.

tions which did not overcome the basic drawbacks but mainly increased complexity and costs.

INSIKA was designed to demand only minimal requirements. The correct usage can be verified using signed receipts and signed data, without the need for a type approval or a certification. Hence there are no constraints of innovations for cash registers and taximeters.

As the costs of smart cards are relatively low and there are no restrictions on the market for manufacturers of cash registers and taximeters, INSIKA is far less expensive than any alternative system.

Contact and further Information

The PTB report IT-18 (mainly in German, available under http://dx.doi.org/10.7795/210.20130206a) covers all essential aspects of the INSIKA project in detail.

The technical specifications are freely available to interested parties on request (mainly in German, English translation in progress).

For further information please visit **www.insika.de**

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

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

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages