Proposal for an IT security standard for preventing tax fraud in cash registers

Mathias Neuhaus, Jörg Wolff, Norbert Zisky

cv cryptovision GmbH
mathias.neuhaus@cryptovision.com

Physikalisch-Technische Bundesanstalt
{joerg.wolff | norbert.zisky}@ptb.de

Abstract

This paper describes a technology solution for preventing tax fraud in electronic cash registers (ECR) and point of sale (POS) systems. The solution is based on electronic signatures, and as a result, any alterations to protected data will be detected. The signed transaction data can be stored on various electronic memory devices. Technical provisions enable the estimation of transaction volumes, even after tampering or loss of data. In this way the solution presented here differs significantly from other fiscal solutions where a pattern of approvals for ECRs and permanent technical supervision of the market is necessary. This paper is focused on the architecture, the protocols and the usability of the proposed system.

1 Introduction

Tax fraud has become a serious problem in our society. This is especially true in countries with high value-added tax (VAT) rates. As a result, it has become necessary to fight against manipulations of cash takings. This problem exists in all member states of the European Union. Anyone dealing with this area of tax fraud will find that the key words include skimming, phantom-ware and zappers:

"Skimming cash receipts is an old fashioned tax fraud; a fraud traditionally associated with small or medium sized enterprises. …. Businesses that skim frequently keep two sets of books (one for the tax man, the other for the owner). In its simplest (nontechnological) form there are two tills, and the cashier simply diverts some cash from selected sales into a secret drawer…. Technology is changing how businesses skim. The agents of change are software applications – phantom-ware and zappers. Phantom-ware is a "hidden," pre-installed programming option(s) embedded within the operating system of a modern electronic cash register (ECR). …

Zappers are more advanced technology than phantom-ware. Zappers are special programming options added to ECRs or point of sale (POS) networks. They are carried on memory sticks,

removable CDs or can be accessed through an internet link. Because zappers are not integrated into operating systems their use is more difficult to detect….. Zappers allow owners to place employees at the cash register, check their performance (monitor employee theft), but then remotely skim sales to cheat the taxman." [AINS09]

Deficits in tax revenues caused by manipulations of electronic cash registers (ECR) are a major problem of all industrial countries.

"The German financial authorities are not able to detect forged statements of cash earnings when using state of the art electronic cash registers. In modern PC-based ECRs it is possible to tamper internal records without leaving any traces. … It is not unlikely that the tax fraud in cash transactions runs into many billions of Euros." [translated from BUND03]

Thus, an immediate remedy is needed. In 2003 a number of different activities to detect and prevent this fraud were started in Germany. The Ministry of finance engaged the German countries in discussions about a number of solutions. The outcome was the development of a new approach for the protection of ECR against manipulations. The proposal was advanced by the German National Metrology Institute (Physikalisch-Technische Bundesanstalt - PTB), and a working group on cash registers was founded. From 2003 until 2008 this group published two reports and developed an operational concept for the use of a smart card solution. In 2008 a project named "INSIKA" (INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme – integrated security concept for ECRs) was launched with the goal of making the technical solution for this problem a reality.

Other countries have developed different solutions. One of the oldest answers is to regulate ECRs. Bulgaria, Italy, Turkey, Lithuania, Latvia, Poland, Russia, Hungary, Brazil, Argentina, and Venezuela are some of the countries that rely on classical fiscal law regulations with strong requirements for ECRs. Detailed requirements for ECRs mandate a complex government approval process and involve reasonably sophisticated technical field observations. As the threats to such a system are very high, the security and enforcement demands need to be equally high. The conditions are similar to regulation of the banking sector.

"Globally, two policy orientations guide enforcement actions in this area – one approach is rules-based; the other is principles-based. They are not mutually exclusive – degrees of blending are common. Rules-based jurisdictions adopt comprehensive and mandatory legislation regulating, and/or certifying cash registers. Jurisdictions taking this approach include Greece and Germany. These jurisdictions are classified generally as "fiscal till" or "fiscal memory" jurisdictions.

Principles-based jurisdictions rely on compliant taxpayers following the rules. Compliance is enforced with an enhanced audit regime. Comprehensive, multi-tax audits (the simultaneous examination of income, consumption and employment returns) are performed by teams that include computer audit specialists. Audits are frequently unannounced and preceded by undercover investigations that collect data to be verified. Jurisdictions taking this approach include the UK and the Netherlands. " [AINS09]

Classical fiscal system are best characterised as "security by obscurity". In most cases they consist of a fiscal memory in a separate device and/or a fiscal printer. Often the fiscal memory and the fiscal printer form a single unit. The key element of the fiscal solution is the printed receipt indicating that the fiscal data set has been stored inside the fiscal memory. Often the receipts have to contain special characters. The technical requirements differ substantially from country to country.

The on-line data transfer to central tax servers in real time is another solution of a fiscal system which was introduced in Serbia: “Additionally Serbian Tax Administration introduced GPRS terminals for remote readouts of fiscal cash registers in 2005. Since 2006, fiscal certification is also necessary for POS applications. By Serbian law, all printers are obliged to have a journal, unfortunately an electronic journal is still not accepted.” [SERV09]

2 Goals, requirements and measures

2.1 Goals

The ultimate goal is the development and implementation of a mechanism for the protection of ECR and POS against tax fraud. The solution should provide protection against manipulations of cash registers and offer a wide range of testing opportunities for tax auditors. The system itself should be revision-safe. The general costs of all system components have to be minimised.

2.2 Requirements

2.2.1 General requirements

As a general requirement transactions have to be recorded completely, correctly, orderly and timely. Cash receipts and expenditures should be kept daily. In cases where changes are made, the original content must always be able to be retrieved.

Data, which contains fiscal-relevant information, must be protected in such a way that subsequent changes are prevented or recognised with a high probability to provide manipulation protection.

The highest level of protection is achieved if all registration procedures and access to the cash register are durably stored. A long-term archive of cumulated values of exactly defined periods could offer data reduction.

In the case of registration and processing of turnovers a high threat potential is to be expected.

Techniques must be used which ensure substantial manipulation protection in cases where high potential threats are expected.

The sum of all costs for subsystems guaranteeing protection from manipulation, including expenditures for examinations, test maintenance as well as operation, training etc. for all participants are to be compared with the expected benefit of unstinted tax revenues. In the end, all costs are ultimately born by the community.

2.2.2 Technical requirements

As a technical requirement all data referred as fiscal-relevant information must be stored in electronic systems in such a way that any change or falsification is not possible or must be readily detectable.

- It must take into account fixed system architecture, data formats and access methods
- Each ECR or POS must be clearly identifiable.
- It must keep non-erasable logs with exactly specified registrations.

2.3 Essential measures

Some of the most critical measures for implementing a fiscal system are listed below:

- Definition of the data that must be protected
- Definition of protection requirements, technical requirements for the approval of technical systems for the recognition of manipulations by cash registers,
- Specification of testing instructions (test criteria)
- Specification of inspection interval
- Deposit of critical software
- Development of evaluation software for revenue offices
- Control of version numbers and digital signature of software modules
- Keeping safety logs
- Specification of sanctions/penalties in case of non-compliance

3 Solution

3.1 Establishment of the INSIKA project

The German working group on cash registers, headed by the German Ministry of Finance, has been examining automated sales suppression within the country. Two reports have been released in 2004 and 2006. The problem is deemed to be serious. Finally, in 2008 this group proposed an operational solution for the protection of ECR against manipulations which was based on a general concept of the PTB from 2004. A parallel development was the publication of a draft law which clearly defined the main topics of the solution. The working group supported the set-up of a technical project for developing and testing of the system. This was a lesson learned from other countries. In February 2008 the INSIKA project (Integrierte Sicherheitslösung für Kassensysteme – Integrated Security Solution for Cash Registers) was started. INSIKA is funded by the German Federal Ministry of Economics and Technology within the MNPQ program for small and medium-sized enterprises. Four ECR manufacturers and the PTB are the project partners. This project group is supported by security specialists from cv cryptovision. In addition to the technical specifications of the smart card it was critical that there was a determination of the data structures and formats, communication protocols and the security analysis. Currently the technical solution is entering the final stages of testing.

3.2 System concept, architecture and protocols

3.2.1 System concept

The essential concept involves the signing of critical data from the ECR by the use of a smart card. This technique is used in many other areas. The PTBs experience includes the securing of metering data by the use of electronic signatures. Within the SELMA project a technically-based secure architecture had been developed and rigorously tested for secure communication of measuring instruments (see SELMA project – www.selma.eu).

The basic idea of the INSIKA concept is very simple. It is compulsory that all transactions are recorded. Each transaction is signed with an electronic signature, generated by a smart card. The cryptographic functions involve the Elliptic Curve Digital Signature Algorithm (ECDSA,

192 bit) [ECDSA00] and the Secure Hash Algorithm (SHA-1, 160 bit) [SHA08]. As the system makes use of asymmetric cryptography, the smart card contains a public and private key. The total length of data to be signed is less than 168 bytes. The tax payer is responsible for the use of the smart card. A Public Key Infrastructure (PKI) is used, and the public key is personalised to the tax payer of each ECR. The German working group on cash registers planned that the Federal Central Office for Taxes will operate as the central authority. Tax auditors must have access to the electronic data in a direct or indirect way. After the recording each manipulation of transaction data is detectable now. Audits by the revenue authority can validate the records of the cash register by the use of the public key and can determine if the data has been tampered.

Based on these basic principles some additional features are defined. It is absolutely necessary, that for each transaction a printed receipt must be presented to the customer. In doing so, the usage of the signature device is shown. The data of the receipt must contain the same data as in the electronically recorded one, including the signature. As a result, the printed receipt can be verified by its digital signature too. In the case of lost data monthly turnovers can be estimated by the use of totalisers, located in the secure memory of the smart card. These totalisers have to be read out by the ECR daily and stored within the electronic journal as signed reports.

The fiscally relevant data records can be examined both locally and after their transmission over various communication channels. Processes will be fully automatic with respect to data's integrity and authenticity.

3.2.2 System architecture

The solution uses a centralised system architecture, as seen in Fig.1. The smart cards will be distributed by the central authority. For the generation of electronic signatures and the recording of totalisers special smart cards have to be used. The tax payer may request as many smart cards as he needs from the central authority. For each smart card a certificate will be generated, which will be stored on a central server and the smart card itself. The distinguished name of the certificate contains the tax payer identification and a consecutive card number. For generating valid transactions the smart card must be integrated into the ECR or POS system. The data sets are well defined within the interface specification. By reading the totalisers the case of cards not being used can be checked easily.

The first step of a taxpayers' audit is the delivery of stored tax data to the auditor. This can be done via various mediums, e.g. memory sticks, CDs or web services. The data format is specified as an XML-export description. Therefore there is no need for the auditor to have direct access to the taxpayer’s system. For the verification of the transactions the auditor will need a standard PC or laptop and the verification software only. Aside from the tax data the public key of the particular smart card is necessary. This key can be obtained either by a request for the certificate from the central server, from the XML-audit-file or from the smart card itself. Both latter versions additionally require access to the certificate revocation list which is distributed by the central authority.

Of course one can think of other system architectures. Some of them are currently under discussion - keeping in mind that each system architecture needs a discrete threat analysis. Systems with decentralised architectures can operate quite well, especially when there are no stringent fiscal regulations and the system is used for in-house control purposes.

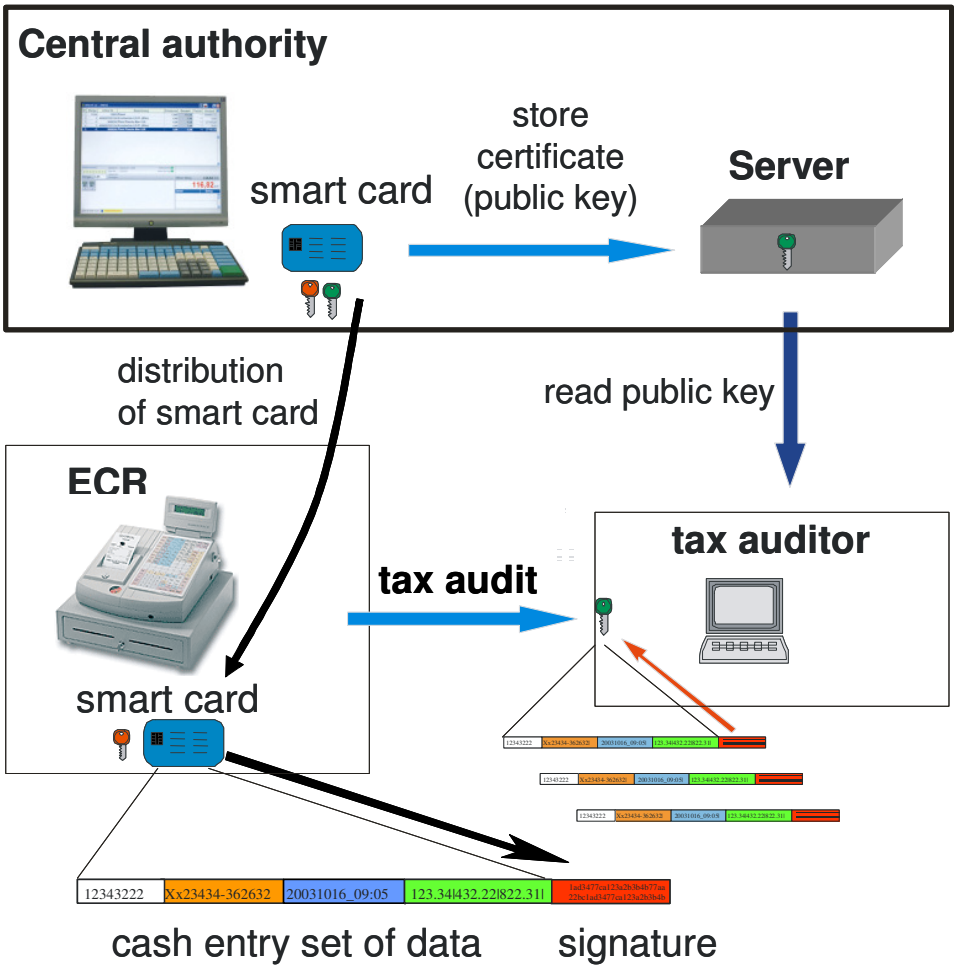

Fig. 1: System architecture

3.2.3 Protocols and interfaces

As described above, INSIKA defines two interfaces only. As seen in Fig. 2 one of them is the interface between the ECR and smart card, called TIM signature interface. As the smart card has some special features, it is named TIM (Tax Identification Module). The data transfer is based on the T=1-protocol according to the ISO/IEC 7816 standard. The data itself follows the Simple-TLV approach, which means that the data is coded according to the pattern Tag-Length-Value. Approximately 50 tags were defined to cover the data model. Mainly three commands (transaction, report, read certificate) are needed in the communication between ECR and TIM. Because of this the handling with the TIM is very easy from the ECR's point of view.

A consecutive sequence number – which is a very important security feature – is generated inside the TIM and will be added by it to the signed data set automatically. This sequence number is sent to the ECR together with the signature as the response of the TIM. It must be stored and printed by the ECR together with other relevant data. If this is not done, the verification will fail. The detailed specification of the TIM signature interface is available for all interested parties. It will be sent for free upon request and registration.

The INSIKA concept does not define any specification for the internal journal of the ECR. The ECR manufacturer is free to decide these specifications. This is one of the main advantages of this solution. Even embedded ECRs with an 8-bit-architecture should be able to implement this system. That means that a high number of older ECRs can be easily upgraded to work with this system.

The second system interface does not include physical layers. With this interface the ECR itself or any other system will be able to generate XML-export files for the auditing processes. The structure and content of the XML data is defined by an XML-Schema. The XML export interface is also defined in a document which will be sent to all interested parties upon request. Considering the wide range of computing power from 8-bit ECRs to PC-based POS systems two different types of XML-data were defined. The first type is specified as "XML Plaintext", which means that the data is placed the classical way in-between XML-tags. The second type called "XML Base64" contains the original TLV-requests and responses from the TIM signature interface. As XML allows for textual data only, this binary data must be coded as Base64.

Both types of XML-data contain the same information from the electronic journal, i.e. transactions, reports and certificates.

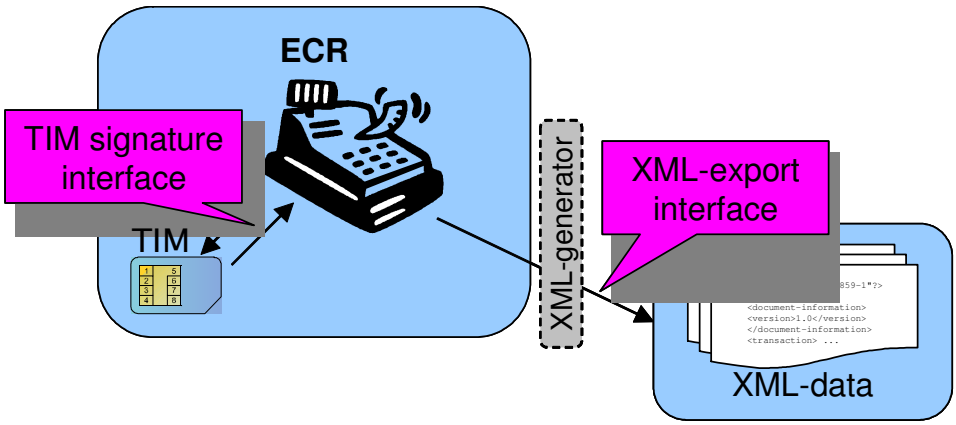

Fig. 2: System interfaces

3.2.4 Usability of the system.

The INSIKA solution is based upon open and established cryptographic algorithms and widely used microchips. Digital signatures have advantages over any other mechanisms for protecting data. The data is protected between the two end points of signed data sets/printed receipts to tax auditor's software. Therefore it is “end-to-end” security. The security is not based on keeping technical secrets but on generally accepted mathematics. As there is no proprietary technology used, the security of the system can be verified independently. Finally, the solution is based on state-of-the-art cryptographic algorithms. The applied ECDSA-192-algorithm has not been broken and is expected remain secure for many years. And as the signatures of this algorithm are comparatively short, they qualify for being easily printed on receipts.

The digital signature is not only visible in the export file, but also on the printed paper receipt that is generated by the ECR for each transaction. On the receipt the signature can be coded as an ASCII string or a two-dimensional code, depending on the ECR's and the printer's capabilities.

All data verification is based on stored and signed transaction data. Any imaginable manipulation of cash register's reports or master data is ineffective because the entire data set cannot be modified without being discovered. Even intentionally installed manipulation functions within the cash register cannot compromise the system, making any device certification procedure obsolete.

Stored data can be verified automatically to a large extent, which is more efficient than previous audits. As the verification of printed receipts is based on the printout information only, there is no need to use saved transaction data. Hence, every printed receipt can be checked to see whether it was generated by an ECR with a valid smart card. All printed receipts without or with faulty signatures clearly signal tampering. Vice versa, taxpayers are able to prove the validity of their cash registers data very easily.

4 Conclusion

A protection system is proposed and implemented for ECRs and similar systems. The solution offers a new approach for fiscal systems in the fight against tax fraud. No system approvals and technical observations are needed for checking the running system. Without doubt, market observations by auditors will be necessary as they are today. But the auditors will have a powerful auditing tool at their disposal. Within a short time they will be able to examine the accuracy of any system.

The concept and specifications developed by INSIKA have raised interest in many countries. The specification details were published in the beginning of 2009. The system could be a template for an European solution. The solution offers flexibility for ECR manufacturers combined with a high level of security. It can break down the trade barriers that are raised when extensive national approval procedures for ECR and POS are instituted. Plans are underway to adapt this technique for use in the taxi business and other related fields.

The INSIKA project is supported by the German Ministry of Economics and Technology under the grant MNPQ 11/07.

References

[AINS09] Ainsworth, Richard: CALIFORNIA ZAPPERS: A PROPOSAL FOR CALIFORNIA'S COMMISSION ON THE 21ST CENTURY ECONOMY, Boston University School of Law Working Paper No. 09-01 (January 8, 2009)

[BUND03] Drohende Steuerausfälle.., Deutscher Bundestag – 15. Wahlperiode Drucksache 15/2020, 54.0, 2003, p.

[ECDSA00] U.S. Department of Commerce and National Institute of Standards and Technology, FIPS PUBLICATION 186-2: DIGITAL SIGNATURE STANDARD (DSS),

Januar 2000 und CHANGE NOTICE 1, Oktober 2001
http://csrc.nist.gov/publications/PubsFIPS.html

[SHA08] U.S. Department of Commerce and National Institute of Standards and Technology, FIPS PUBLICATION 180-3: SECURE HASH STANDARD (SHS), October 2008
http://csrc.nist.gov/publications/PubsFIPS.html

[SERV09] Service Plus D.O.O. : INFORMATION TECHNOLOGIES FOR RETAIL, accessed on July 6th, 2009,
http://www.serviceplus.rs/eng_txt__serbian_fiscal_printers_comparison.php

Index

Catchwords: tax fraud, manipulation protection, cryptography, security concept, electronic cash register, hash, ECDSA, ECR, POS, INSIKA, receipt, XML, sales suppression, skimming, zapper