Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationen

INSIKA – Konzept, Umsetzung und Erprobung

Norbert Zisky, Jörg Wolff (Hrsg.)

Physikalisch-Technische Bundesanstalt (PTB)

PTB-Bericht Informationstechnik IT-18
ISSN 0942-1785
doi:10.7795/210.20130206a

Die gedruckte Version wird durch den Wirtschaftsverlag NW – Verlag für neue Wissenschaft GmbH unter der ISBN 978-3-95606-001-4 verlegt, siehe: http://www.nw-verlag.de/.

Bundesallee 100 Abbestraße 2-12
38116 Braunschweig 10587 Berlin

Inhaltsverzeichnis

Vorwort

Dieser PTB-Bericht fasst die Ergebnisse der Forschungs- und Entwicklungsarbeit des Projekts „INtegrierte SIcherheit für messwertverarbeitende KAssensysteme“ (INSIKA) zusammen. Das Ziel des INSIKA-Konzepts ist der zuverlässige Schutz von Ursprungsaufzeichnungen vor Veränderungen und der Nachweis von deren Korrektheit. Dieser Bericht beschreibt das Konzept, die Umsetzung und die Ergebnisse aus den Erprobungen. Darüber hinaus geben in- und ausländische Experten aus verschiedenen Bereichen des Steuer- und Finanzrechts in ihren Beiträgen Hintergrundinformationen zum Thema Baraufzeichnungen.

Mit dem Abschluss des INSIKA-Projekts steht ein technisch beschriebenes und erprobtes Verfahren zur Sicherung von Datenaufzeichnungen für verschiedene Anwendungsgebiete zur Verfügung.

Gegenüber „klassischen“ Fiskalsystemen bietet INSIKA ein neuartiges Konzept, dass ohne Bauartprüfung oder Zertifizierung des Zielsystems auskommt[1]. Auch die in den letzten Jahren in anderen Ländern (z. B. Schweden, Québec) eingeführten Fiskalsysteme mit kryptografischen Verfahren folgen der klassischen Sichtweise. INSIKA bietet demgegenüber ein modernes, sicheres Verfahren, dass zudem Konzepte für weitgehend automatisierbare Audits bereitstellt. Da sich die Grundlagen und Anforderungen in der Europäischen Union kaum unterscheiden, wäre das INSIKA-System auch in anderen Ländern einsetzbar.

Die Sicherheit des Systems basiert auf digitalen Signaturen, die von einer speziellen INSIKA-Smartcard erzeugt werden. Seit Februar 2010 können Entwickler Smartcards für Evaluationszwecke beziehen. Seit Mitte 2012 sind INSIKA-Smartcards für den Realbetrieb in Taxenunternehmen von der Bundesdruckerei GmbH verfügbar.

Zur Zeit ist die Anwendung des Systems auf Registrierkassen und Taxameter spezifiziert. Dabei sind das Konzept und die Verfahren vollständig offengelegt. Der freiwillige Einsatz von INSIKA-Systemen für Taxameter wird gegenwärtig durch die Freie und Hansestadt Hamburg gefördert. In Hamburg sind bereits einige hundert Fahrzeuge mit dieser Technik unterwegs. In Berlin wird das System bisher noch im Rahmen eines Feldtests eingesetzt.

[1] Bei der Anwendung auf Daten aus dem Taxameter wird das Gerät selbst nicht berührt. Das Taxameter muss unverändert in der Bauart geprüft und zugelassen werden

Schon in einer 2003 durchgeführten Untersuchung des Bundesrechnungshofes wurden erhebliche Defizite bei der Datenaufzeichnung in verschiedenen Bereichen mit Barumsätzen ermittelt. Daraufhin erarbeitete das Bundesfinanzministerium gemeinsam mit den Länderfinanzverwaltungen unter Beteiligung der PTB einen ersten Lösungsansatz, der auf getestete Verfahren zur kryptographischen Sicherung von Messdaten zurückgriff. Wegen der Neuheit des Verfahrens bestanden Zweifel an der Realisierbarkeit von verschiedenen Seiten. Die PTB hat deshalb im Februar 2008 gemeinsam mit interessierten Unternehmen in dem vom Bundesministerium für Wirtschaft geförderten Mittelstandsförderungsprogramm MNPQ (Messen, Normen, Prüfen, Qualitätssicherung) das Projekt INSIKA gestartet. Die geplante gesetzliche Einführung wurde Mitte 2008 zurückgestellt.

Im INSIKA-Projekt wurde das gleichnamige Konzept ausgehend vom o. g. Lösungsansatz bis zur Marktreife als offenes Verfahren vollständig spezifiziert, in praxistauglichen Komponenten implementiert und in Pilotversuchen getestet. Fachlich unterstützt wurde die Projektgruppe von der „Bund-/Länder-Arbeitsgruppe Registrierkassen“, die vor allem in der Konzeptionsphase wichtige Fragen zum Steuerrecht beantwortete. Motivation für die am Projekt beteiligten Unternehmen war es, ein technisch vollständig spezifiziertes Verfahren zu entwickeln, das für alle Betroffenen ein hohes Maß an Wettbewerbsgleichheit garantiert und gleichzeitig alle gesetzlichen Anforderungen erfüllt.

Der Bericht gliedert sich in vier Teile, die thematisch eng miteinander verbunden sind.

Im ersten Teil wird das INSIKA-Konzept von den am Vorhaben direkt Beteiligten beschrieben. Der erste Beitrag stellt das Sicherheitskonzept, die Hauptmerkmale und Schnittstellen des INSIKA-Verfahrens umfassend dar. Im Beitrag von Herrn Neuhaus erfolgt die Beschreibung von Sicherheitsverfahren als Grundlage des INSIKA-Konzepts, der INSIKA-Smartcard mit ihren speziellen Funktionen und der Referenzimplementierung der Smartcard als Sicherheitsanker des Gesamtsystems. Im dritten Beitrag erfolgt ausgehend von den verschiedenen Nutzern und Rollen eine detaillierte Zusammenstellung von Prüfmerkmalen und Prüfverfahren. Herr Reckendorf erläutert in seinem Bericht aus Sicht eines Kassenherstellers, wie das

doi:10.7795/210.20130206a

INSIKA-Konzept in Registrierkassen umgesetzt werden kann. Darüber hinaus werden der Entwicklungsaufwand, erste Praxiserfahrungen und die Übertragbarkeit der Erkenntnisse auf andere Kassenhersteller dargestellt. Von 2010 bis 2012 wurde ein INSIKA-Feldversuch durchgeführt. Im Beitrag von Herrn Osswald wird über diesen Versuch ausführlich informiert. Herr Pleßmann gibt in seinem Beitrag einen Überblick, wie sich INSIKA in die Landschaft bereits etablierter Fiskallösungen integriert und worin die Unterschiede bestehen. Herr Kerling beschreibt in seinem Beitrag die Implementierungsaufwendungen von INSIKA im Vergleich zu bekannten Fiskallösungen. Ausgehend von einer Übersicht über den Einsatz von Fiskallösungen außerhalb Deutschlands und grundsätzlicher Anforderungen an Fiskalkonzepte erläutert er die Vorteile und Einsatzmöglichkeiten von INSIKA im Kassenumfeld.

Der zweite Teil befasst sich mit rechtlichen Fragen und der praktischen Umsetzung des INSIKA-Verfahrens. In einem Kurzbeitrag gibt das Referat IV A 4 des BMF eine Übersicht über die Aufzeichnungspflichten bei Bargeschäften und Anforderungen an elektronische Registrierkassen und anderen Geräten aus steuerlicher Sicht. Frau Klug und Frau Roßberg geben einen Überblick über die Leistungen eines Zertifizierungsdienstanbieters und erläutern Struktur und Arbeitsweise einer PKI (Public Key Infrastructure) am Beispiel des Produkts INSIKA-Smartcard der Bundesdruckerei GmbH. In einem weiteren Betrag beschreibt Herr Reckendorf verschiedene Aspekte des praktischen Einsatzes von INSIKA. Schwerpunkt sind Angriffsmöglichkeiten, deren Erkennung und Verhinderung.

Der dritte Teil des Berichts behandelt spezielle Fragen aus der Anwendung auf Taxameter. Frau Grohne und Herr Dr. Jäger geben einen Überblick über die nationale Umsetzung der europäischen Messgeräterichtlinie für Taxameter. Sie gehen dabei auf nationale und internationale Vorschriften und Normen ein und stellen die grundsätzliche Struktur eines Taxameters und dessen möglich Zusatzgeräte dar. Frau Stering erläutert aus Sicht eines Messgeräteherstellers die Einsatzmöglichkeiten von INSIKA für Taxen und die praktische Umsetzung für den Realbetrieb. Dabei werden sowohl Taxameter als auch Datenabrufsysteme adressiert. Ausgehend von der Situation im Taxigewerbe beschäftigt sich der Beitrag von Herrn Krause und Herrn Ströh ebenfalls mit der praktischen Umsetzung von INSIKA im Taxenumfeld. Durch eine im Beitrag beschriebene Fördermaßnahme der Freien und Hansestadt Hamburg konnte der Übergang von Prototypen in marktkonforme Produkte bedeutend beschleunigt werden.

Der vierte Teil enthält Aufsätze von ausländischen Experten auf dem Gebiet des Steuer- und Finanzrechts zum behandelten Themenkreis. Herr Ainsworth gibt aus US amerikanischer Sicht einen Überblick über den steigenden Missbrauch technischer Systeme bei der Erfassung steuerlich relevanter Daten. Er beschäftigt sich mit internationalen Lösungsansätzen und mit Alternativen für die US Behörden. Mit Entwicklungen von Verfahren und Methoden zur Gewährleistung verlässlicher Datenaufzeichnungen beschäftigen sich Herr van der Zwet und Herr van Heusden in ihrem Beitrag. Sie führen aus, dass Regeln und Vorschriften allein nicht genügen, bestehende Probleme zu lösen. Auf der Grundlage einer Risikobewertung werden neue Ansätze hinsichtlich Einsetzbarkeit untersucht. Der Schlussbetrag des Berichts von Herrn Huber gibt einen umfassenden Gesamtüberblick über das Thema Betriebsprüfung. Er geht dabei auf Manipulationsmöglichkeiten und deren Erkennung und möglichen Verhinderung ein. Ein Kapitel beschreibt die wesentlichen Elemente der österreichischen Kassenrichtlinie.

Ein besonderer Dank gilt unseren Partnern für die erfolgreiche Zusammenarbeit im INSIKA-Projekt und den Mitarbeitern der PTB Arbeitsgruppe „Datenkommunikation und –sicherheit“ sowie den Mitarbeiterinnen und Mitarbeitern des BMF, Ref. IV A 4 und der Länderfinanzverwaltungen. Dank gilt auch der Firma Cryptovison für die engagierte Mitarbeit und Unterstützung bei der Spezifikation und Implementierung der INSIKA-Smartcard. Auch der Bundesdruckerei möchten wir für die schnelle Bereitstellung der PKI und die Übernahme als Produkt danken. Die INSIKA-Projektgruppe dankt weiterhin auch allen, die zum Gelingen des Vorhabens und Verbreitung der Konzeptidee beigetragen haben. Nicht zuletzt gilt unser Dank dem Bundesministerium für Wirtschaft und Technologie, das das INSIKA-Projekt unter dem Kennzeichen MNPQ 11/07 gefördert hat.

Berlin, im Februar 2013

Dr. Norbert Zisky
Jörg Wolff

Konzept zum Aufbau und Betrieb revisionssicherer Kassensysteme und Messeinrichtungen

Norbert Zisky
Physikalisch-Technische Bundesanstalt (PTB)
Abbestraße 2-12, 10587 Berlin
norbert.zisky@ptb.de

Dieser Beitrag stellt ein offenes Konzept vor, mit dessen Hilfe technische Systeme intern erzeugte Daten elektronisch so sichern, dass der Ursprung der Daten auch außerhalb des Systems nachgewiesen und der Inhalt nicht unerkannt verändert werden kann. Das ursprünglich aus der Messtechnik stammende Grundkonzept wurde beispielhaft auf das Systemumfeld Kassensysteme übertragen. Ziel ist ein allgemeingültiges revisionssicheres Verfahren zur Ursprungsaufzeichnung von Daten für beliebige Anwendungsbereiche. Anwendungen auf dieser Grundlage sind eine Alternative zu konventionellen Fiskalspeicher-Systemen. Aufwandschätzungen und bereits vorgenommene Implementierungen zeigen, dass sich die Lösung kostengünstig umsetzen lässt.

1 Einführung in die Problematik

1.1 Allgemeine Schutzziele beim Umgang mit sensiblen Daten

Sollen Daten gegen bewusste oder unbewusste Verfälschungen gesichert werden, sind eine Reihe von Grundanforderungen zu erfüllen. Alle als „zu schützend“ definierten Daten müssen vollständig, richtig, geordnet und zeitgerecht aufgezeichnet werden. Verfälschungen von Daten sollen sicher erkannt werden. Die Aufzeichnungen sollen auf Vollständigkeit und Richtigkeit einfach prüfbar sein. Diese Grundanforderungen gelten gleichermaßen für Mess- und Kassendaten.

1.2 Verfälschungen bei der Aufzeichnung von Bareinnahmen

Im Jahresbericht 2003 des Bundesrechnungshofes wurde auf drohende Steuerausfälle durch Manipulationsmöglichkeiten in modernen Registrierkassen hingewiesen. In Registrierkassen gespeicherte Daten können in vielen Systemen mit relativ geringem Aufwand beliebig verändert werden. Entsprechende Hinweise verschiedener Länderfinanzverwaltungen datieren noch früher. Im o. g. Bericht heißt es:

> „Die Aufzeichnung von Bargeschäften durch elektronische Kassensysteme der neuesten Bauart genügt nicht den Grundsätzen ordnungsgemäßer Buchführung. Bei Bargeldgeschäften in mehrstelliger Milliardenhöhe drohen nicht abschätzbare Steuerausfälle.“

Nach einer Empfehlung des Bundesrechnungshofs sollte das Bundesministerium für Finanzen veranlassen,

> „die Kassen um ein eingriffsicheres Bauteil zu ergänzen und den Nutzern neuerer elektronischer Kassen den Nachweis über die Eingriffsicherheit aufzuerlegen.“

Elektronische Registrierkassen mit offenen Betriebssystemen und ungeschützten Schnittstellen bergen für die Speicherung sensibler Daten erhebliche Risiken, wenn nicht angemessene Schutzmaßnahmen vorgesehen sind.

> „Die Finanzbehörden können falsche Angaben über eingenommene Bargelder bei Verwendung elektronischer Kassensysteme jüngster Bauart nicht mehr aufdecken. Bei

PTB-Bericht IT-18
doi:10.7795/210.20130206a

> solchen Systemen lassen sich eingegebene Daten sowie im System erzeugte Registrier- und Kontrolldaten ohne nachweisbare Spuren verändern.“[1]

Mit entsprechendem Aufwand lassen sich auch proprietäre Registrierkassen mit herstellerspezifischen Betriebssystemen angreifen. In der Praxis werden entsprechende Sicherheitslücken im System teilweise von Herstellern toleriert oder sogar bewusst vorgesehen [2]. Oft genügen bereits Parameteränderungen oder Veränderungen von Summenzählern, um die gesetzlichen Bestimmungen der Aufzeichnungspflichten zu unterlaufen.

Die geschilderten Probleme sind nicht auf Deutschland beschränkt. Daraus resultieren eine Reihe negativer Entwicklungen für die Gesellschaft und den Einzelnen. Insbesondere in Ländern mit hohen Umsatzsteuersätzen führen verkürzte Angaben zum Umsatz zu erheblichen Fehlentwicklungen. Die Umsatzsteuer ist eine indirekte Steuer, die nicht vom Steuerpflichtigen, sondern durch einen Dritten an die Finanzbehörden abgeführt wird. Neben der privaten Verwendung von Mehreinnahmen aus Steuerverkürzungen wird das Geld häufig zur Bezahlung von „Schwarzarbeit“ oder Abwicklung anderer unzulässiger Geschäfte verwendet. Ohne „Schwarzgeld“ gäbe es kaum „Schwarzarbeit“. Auf die negativen Auswirkungen der Schwarzarbeit (keine Lohnsteuer, keine Sozialabgaben) auf die gesamte Wirtschaft wird hier nicht näher eingegangen. Steuerehrliche Unternehmen haben dadurch einen erheblichen Wettbewerbsnachteil, da die Personalkosten bei korrekt angemeldeten Mitarbeitern erheblich höher sind.

Außer den gesetzlichen Anforderungen an die Ordnungsmäßigkeit der Buchführung gibt es in Deutschland keine technischen Anforderungen an Kassensysteme. Zunehmend wird bei Kontrollen durch Steuerprüfer die Ordnungsmäßigkeit der Buchführung angezweifelt. Im Ergebnis dieser Prüfung wird die Buchführung verworfen und es kommt zu Steuerschätzungen mit teilweise erheblichen Nachzahlungsforderungen, siehe [3] S. 33.

Verschiedene Länder haben deshalb so genannte Fiskalsysteme eingeführt. Mit speziell geschützten Zusatzeinrichtungen werden die Buchungsdaten in einem gesicherten Speicher abgelegt. Jedes Kassensystem muss dann über eine Bauartzulassung verfügen und mit einem Fiskalmodul ausgestattet sein. Da das Bedrohungspotenzial im Kassenbereich hoch ist, sind die Sicherungsanforderungen hoch und daraus folgend die Sicherungsmaßnahmen aufwändig. Jede Hardware- oder Softwareänderung zieht eine erneute Überprüfung nach sich. Meist werden bei Fiskallösungen zur Speicherung der Buchungsdaten spezielle Speichermedien als integrierte oder zusätzliche Baugruppe verwendet. Dabei kann je nach Anforderung und Aufwand ein unterschiedliches Schutzniveau für die als sensibel gekennzeichneten, steuerlichen Daten erreicht werden. Die Hersteller von Registrierkassen müssen für die Entwicklung und Zulassung solcher Systeme in den bekannten Fällen erhebliche Aufwendungen tätigen. Als Beispiel für europäische Länder mit einer längeren Fiskalspeicher-Tradition seien Italien, Griechenland oder Polen genannt. In Schweden wurde 2010 eine Fiskalspeicher-Lösung eingeführt, Belgien schreibt den Einsatz ab 2014 vor (nur für die Gastronomie). In anderen Ländern wie Österreich und Portugal wurden die gesetzlichen Anforderungen an Software verschärft ohne eine Hardware-Lösung vorzuschreiben. In Deutschland wird seit 2001 über mögliche Lösungsansätze nachgedacht und nach einer geeigneten Methode gesucht.

1.3 Bemühungen zur Entwicklung eines Lösungsansatzes

Das Bundesministerium für Finanzen legte im Jahr 2008 einen Gesetzentwurf zur Änderung der Abgabenordnung vor [4]. Darin heißt es u. a.:

> „Die Prüfung der Vollständigkeit der baren Betriebseinnahmen für Besteuerungszwecke ist seit jeher ein Hauptproblem bei Branchen mit einem hohen Anteil an Bargeschäften. Die modernen elektronischen Registrierkassen und Taxameter machen Manipulationen möglich, die als solche nicht erkennbar sind und allenfalls durch aufwändige Verprobungen nachgewiesen werden können. Bund und Länder haben dies ebenso erkannt wie der Bundesrechnungshof und wollen Abhilfe schaffen, um die Gleichmäßigkeit der Besteuerung sicherzustellen, die Steuereinnahmen zu sichern und die ehrlichen Unternehmer vor unlauterer Konkurrenz zu schützen. Die Regelungen sollen insbesondere Branchen erfassen, die im Verhältnis zum Gesamtumsatz einen hohen Anteil an Bargeschäften aufweisen. Hierzu gehören neben dem Einzelhandel insbesondere auch die Gastronomie und die Taxiunternehmen. Nach den bisherigen Prüfungserfahrungen ist hier die Gefahr, dass Barumsätze nicht vollständig erfasst werden, besonders groß.“

Grundlage des Gesetzentwurfs für die im Vorblatt G, Anstrich 4 angestrebte Lösung war ein im Jahre 2004 von der Physikalisch-Technischen Bundesanstalt (PTB) vorgeschlagenes Sicherungskonzept für Kassensysteme [5], das von einer Bund-Länder-Arbeitsgruppe in ein Fachkonzept [6] überführt wurde.

> „Die Bund-Länder-Arbeitsgruppe ‚Registrierkassen' hat Vorschläge erarbeitet, um bestehende Manipulationsmöglichkeiten bei modernen Kassensystemen zu beseitigen. Die Bundesregierung beabsichtigt, auf dieser Grundlage eine kryptographische Sicherung der Buchungen in elektronischen Registrierkassen sowie Waagen, Taxametern und Wegstreckenzählern mit Registrierkassenfunktion mittels einer Smart Card einzuführen, damit Manipulationen erkennbar werden. Damit soll die Überprüfbarkeit dieser Geräte verbessert werden. Flankiert werden soll dies durch die Einführung einer Kassen-Nachschau sowie der Bußgeldbewehrung bei Verstößen gegen die Aufzeichnungspflicht." [7]

Von den Ländervertretern der Finanzbehörden erhobene Forderungen nach einer zusätzlichen, gesicherten Aufzeichnung kumulierter Umsätze sollten dabei Berücksichtigung finden. Es sollten nicht nur Manipulationen erkannt, sondern auch mögliche Veränderungen quantifiziert werden können. Fast zeitgleich mit der Fertigstellung des Fachkonzepts der AG Registrierkassen [6] wurde im Februar 2008 unter Leitung der PTB das INSIKA-Projekt (INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme) gestartet. Dabei sollten die Spezifikationen und technischen Details zur Umsetzung des Fachkonzepts auf nationaler Ebene ausgearbeitet werden. Erklärtes Ziel des Vorhabens war die Bereitstellung einer allgemeingültigen Dokumentation des Verfahrens für alle interessierten Kreise. Das Vorhaben wurde vom Bundesministerium für Wirtschaft und Technologie als MNPQ-Projekt (Messen, Normen, Prüfen und Qualitätssicherung) gefördert. Projektpartner sind neben der PTB die vier Kassenhersteller Huth Elektronik Systeme GmbH, Quorion Data Systems GmbH, Ratio Elektronik Systeme GmbH und Vectron Systems AG.

Ausgehend vom PTB-BMF-Grundkonzept aus dem Jahr 2004 wurden im INSIKA-Projekt die Lösungsansätze für technische Fragestellungen erarbeitet. Dabei erfolgte eine indirekte Zusammenarbeit mit der AG Registrierkassen der Länder indem konkrete steuerrechtliche Anfragen der INSIKA-Projektgruppe von Fachleuten der AG Registrierkassen beantwortet wurden. Die am INSIKA-Projekt beteiligten Kassenhersteller haben jedoch nicht in der AG Registrierkassen mitgearbeitet.

Im November 2010 hat das BMF auf dem Erlassweg eine seit Januar 1996 bestehende Erleichterungsregelung aufgehoben. Diese erlaubte einen Verzicht auf die Einzelaufzeichnung jedes Registriervorgangs. Ein besonderer Manipulationsschutz für die aufgezeichneten Daten ist im neuen Erlass nicht geregelt.

1.4 Angriffsmöglichkeiten auf Kassensysteme

Werden lediglich die Berichte einer Registrierkasse über die Gesamtumsätze eines Tages archiviert, sind Manipulationen dieser Werte bei vielen Systemen sehr einfach. Durch missbräuchliche Verwendung von Funktionen, die für Service- und Trainingszwecke gedacht sind, lassen sich Daten während der Erfassung oder nachträglich verändern.

Bei einer Erfassung von Einzeltransaktionen müssen Manipulationen auch bei diesen ansetzen. Die Problematik hat sich seit den 1990er-Jahren vor allem dadurch verschärft, dass zunehmend Kassensysteme auf PC-Basis genutzt werden. Derartige offene Systeme lassen sich selbst durch den Gerätehersteller kaum noch schützen. Die direkte Änderung von Datenbeständen (Dateien oder Datenbanken) ist relativ leicht möglich. Zur weitgehenden Automatisierung der recht aufwändigen Manipulation der Einzeltransaktionsdaten werden vermehrt spezielle Manipulationsprogramme, die als „Zapper" bezeichnet werden, entwickelt. Eine typische Manipulation eines einzelnen Belegs ist in Abbildung1 veranschaulicht.

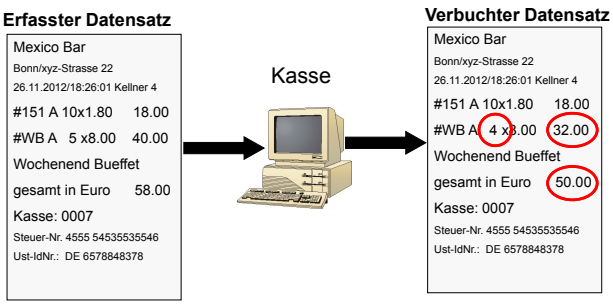


Abbildung 1: Veränderung von Datenbeständen in Registrierkassen

Datenmanipulationen sind teilweise durch den Betreiber unter weitgehender Umgehung des Herstellers möglich. Wenn der Gerätehersteller jedoch bewusst Funktionen zur Datenmanipulation in seinem Kassenkonzept vorsieht, werden Angriffe sehr leicht durch-

führbar sind und in der Praxis kaum noch zu entdecken.

Weitere Manipulationsmöglichkeiten bestehen bei Kassensystemen mit zentraler Speicherung der Registriervorgänge. Mittels der Kommunikationssoftware könnte es zu einer gezielten Verfälschung der Daten kommen.

Ein sehr einfaches Verfahren besteht darin, einzelne Buchungen gar nicht per Registrierkasse zu erfassen. Bei einer sicheren Aufzeichnung von Einzelbuchungen hinterlässt dieses Vorgehen allerdings Auffälligkeiten in den Daten, wie z. B. zeitliche Lücken, die sich mit modernen Prüfungsverfahren relativ leicht erkennen lassen.

2 Anforderungen und Lösungsansätze zum Manipulationsschutz

2.1 Grundlegende Anforderungen

Ein Kassensystem muss Buchungen vollständig, richtig, geordnet und zeitgerecht aufzeichnen. Kasseneinnahmen und -ausgaben sollen täglich festgehalten werden. (§146 Abs. 1 Abgabenordnung – AO [8]). Bei Änderungen muss der ursprüngliche Inhalt immer feststellbar sein (§146 Abs. 4 AO). Daten, die steuerlichrelevante Informationen enthalten, sind so zu schützen, dass deren nachträgliche Veränderung verhindert oder sicher erkannt wird. Damit sollen Barumsätze und sonstige Aufzeichnungen durch die Finanzbehörden sicher auf Vollständigkeit und Richtigkeit überprüfbar sein.

Das höchste Schutzniveau wird dabei erreicht, wenn alle Registriervorgänge und Zugriffe auf die Registrierkasse dauerhaft und unveränderbar gespeichert werden. Nach der derzeitigen Rechtslage ist es in einer Übergangsphase bis Ende 2016 mit vielen Systemen noch möglich, nur die Tagesendsummen zu sichern. Diese Erleichterung der Buchführungspflichten ist ein wesentlicher Angriffspunkt auf Kassensysteme. Durch eine Weiterentwicklung der Manipulationstechniken, vor allem durch Zapper-Software, sind allerdings auch nicht geschützte Einzeltransaktionsdaten leicht angreifbar.

Daher sind für ausreichenden Manipulationsschutz entsprechend geeignete Verfahren und Techniken einzusetzen und es muss eine Marktüberwachung organisiert werden. Dabei müssen die Gesamtkosten einschließlich der Aufwendungen für Prüfungen und Prüfunterhalt sowie Bedienung, Schulung usw. für alle Beteiligten in einer Kosten-Nutzen-Analyse dem zu erwartenden Nutzen (unverkürzte Steuereinnahmen, Steuergerechtigkeit) gegenüberzustellen. Alle o. g. Kosten werden letztlich auf die Gemeinschaft umgelegt. Angaben zur genauen Höhe der Steuerverkürzungen sind nur bedingt möglich.

In Abhängigkeit vom Lösungskonzept müssen Anforderungen an Systeme und Betriebsabläufe exakt definiert werden. Die zu schützenden Daten sind eindeutig festzulegen. Weiterhin müssen Prüfanweisungen und Überprüfungsfristen für Schutzvorrichtungen erarbeitet werden. Für den Einsatz durch die Finanzbehörden sind Auswertungs- und Plausibilisierungsverfahren zu entwickeln. Typische Festlegungen zum Betrieb eines Sicherheitssystems sind Auflagen zum Führen von sicherheitstechnischen Logbüchern, Sanktionen bei Verstößen gegen Festlegungen oder Maßnahmen bei Datenverlust.

2.2 Lösungsansätze zum Manipulationsschutz

Mögliche technische Lösungsansätze zur Erkennung von Manipulationen sind die o. g. Fiskalspeicher-Systeme, eine zeitnahe Online-Übertragung aller Buchungsvorgänge auf zentrale Datenbanken oder die dezentrale Absicherung der Registrierkassen mittels geeigneter kryptographischer Verfahren.

Fiskalsysteme verwenden klassische digitale Speicherbausteine in denen über größere, genau festgelegte Zeiträume steuerlich-relevante Daten, vor unberechtigtem Zugriff geschützt, aufgezeichnet werden. Das Auslesen und Löschen der Fiskalsysteme ist nur autorisierten Personen, z. B. den Steuerbehörden, gestattet. Die Speichermedien werden gegen unbefugten Zugriff mit unterschiedlichen Methoden geschützt. Technisch gesehen kann ein Fiskalspeicher nicht nur als eine in die Registrierkasse integrierte Einheit, sondern auch als eine eigenständige Komponente aufgebaut werden. Fiskalspeicher müssen manipulationssicher sein. Mit geeigneten technischen Mitteln sind marktübliche nichtflüchtige Speichertechniken so aufzubauen, dass Zugriffe und Veränderungen von Daten nach genau festgelegten, überprüfbaren Regeln erfolgen. Unerlaubte Zugriffe und Manipulationsversuche müssen sicher erkannt und protokolliert werden. Die Hardware ist durch Versiegelung oder Verplombung vor unerlaubten Zugriffen oder Veränderungen zu schützen. Voraussetzung für den Betrieb eines Fiskalspeichersystems ist die engmaschige Überwachung der meist komplizierten technischen Systeme durch geschultes Personal. Fiskalspeicher bieten bei entsprechender Auslegung einen mittleren Schutz vor Manipulationen.

Die Einführung eines Fiskalspeichersystems ist mit erheblichen Kosten für den Hersteller, Anwender und die Behörden verbunden.

Eine weitere Möglichkeit zur Verhinderung von Manipulationen ist die sofortige Übertragung jeder Buchung auf ein zentrales unabhängiges Datenzentrum. Voraussetzung zum Einsatz dieses Verfahrens wäre der Aufbau einer komplexen IT-Infrastruktur. Die Daten sämtlicher Registrierkassen und Kassensysteme, mit denen steuerlich-relevante Daten erfasst werden, müssten in Echtzeit von zentralen Datenerfassungssystemen gespeichert und verarbeitet werden. Das setzt eine permanente Online-Verbindung jeder Registrierkasse voraus. Die Datenzentralen müssten von den Finanzbehörden oder einer autorisierten Instanz betrieben werden. Bei ca. zwei Millionen Registrierkassen in Deutschland wäre unter der Voraussetzung der kompletten Anbindung aller Registrierkassen täglich eine sehr große Datenmenge zu verarbeiten. Darüber hinaus wäre je nach verwendetem Kommunikationsmedium ein entsprechender Aufwand in den Schutz der Daten zu erbringen. Auch hier muss ähnlich wie bei einer Fiskalspeicherlösung seitens der zuständigen Behörden ein erheblicher Aufwand in die Konzeptentwicklung und Prozessmodellierung investiert werden.

Ein weiteres Verfahren zum Schutz von Kassendaten ist der Einsatz von Kryptographie. Integrität und Authentizität der Daten sind durch digitale Signaturen sicher nachweisbar. Einmal signierte Daten können so kumuliert werden, dass Aussagen über den Gesamtbetrag von Datenmanipulationen an Einzelbuchungen möglich sind. Der kryptographische Lösungsansatz wird im INSIKA-Verfahren angewendet, da er gegenüber den anderen o. g. Verfahren erhebliche Vorteile hat.

3 Sicherheitskonzept und Lösungsansatz - INSIKA

3.1 Grundprinzip

Das Grundkonzept für den Manipulationsschutz von Aufzeichnungen sieht den Einsatz digitaler Signaturen vor, die von einer Smartcard erzeugt werden. So geschützte Datenaufzeichnungen können nicht unerkannt verändert werden. Die grundsätzliche Idee ist in Abbildung 2 dargestellt. Jede Buchung wird mit einer digitalen Signatur versehen. Die Signatur selbst entspricht einer elektronischen Unterschrift des Steuerpflichtigen. Bestandteile der signierten Buchung sind u. a. eine automatisch erzeugte Buchungsnummer, siehe 3.5.2 und ein Umsatzsteuerkennzeichen des Steuerpflichtigen. Mit diesen Informationen ist jede Buchung einmalig. Buchungsbelege können kopiert werden. Selbst bei einer Manipulation oder beim Verlust der Daten ist durch technische Vorkehrungen eine Abschätzung der Umsätze möglich. Mit spezieller Software kann die Vollständigkeit und Unversehrtheit der Buchungsdaten sowie deren Herkunft geprüft werden.

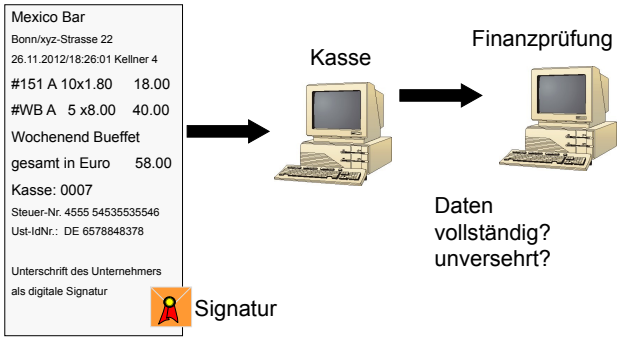


Abbildung 2: Grundsätzliches Lösungskonzept

Die Lösung basiert auf bewährten Sicherheitsverfahren, ist vergleichsweise einfach zu implementieren und hat gegenüber klassischen Fiskalspeicherlösungen Vorteile für fast alle Beteiligten. Grundlage des Sicherheitskonzepts sind die im SELMA-Projekt (Sicherer Elektronischer Messdatenaustausch) von Energieversorgungsunternehmen, Messgeräteherstellern, Eichbehörden und Forschungseinrichtungen entwickelten Verfahren zur Übertragung von Messdaten über offene Netze [9].

3.2 Einsatz kryptographischer Verfahren

Die zwei wichtigsten Sicherheitsziele in Bezug auf die Vollständigkeit und Herkunft von Daten sind die Integrität und Authentizität. Die Integrität von Daten ist dann gegeben, wenn der Empfänger von Daten die Korrektheit und Vollständigkeit der Daten sicher überprüfen kann. Verfälschungen müssen vom Empfänger erkannt werden. Daten sind authentisch, wenn jeder Empfänger prüfen kann, von wem die Daten tatsächlich stammen.

Die Integrität von INSIKA-Daten wird durch die Anwendung von Hashfunktionen geprüft. Hashfunktionen sind mathematische Einwegfunktionen, die Datensätze unterschiedlicher Größe auf eine Zahl mit fester Länge abbilden. Die Gefahr von Kollisionen ist für die strukturierten, relativ kurzen INSIKA-Daten praktisch ohne Bedeutung.

Die Authentizität von INSIKA-Daten wird mit einem asymmetrischen Kryptographieverfahren auf Grundlage elliptischer Kurven gewährleistet. Für die Messtechnik und auch für den Kassenbereich sind

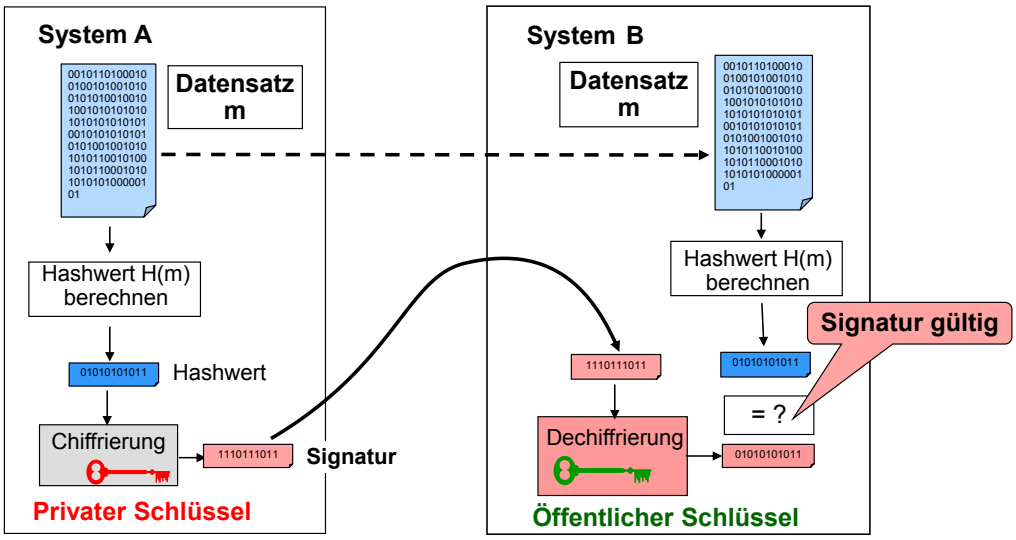


Abbildung 3: Digitale Signatur von Daten

asymmetrische Verfahren besonders geeignet. Zur Verwaltung der Signaturschlüssel muss dabei eine geeignete Struktur aufgebaut bzw. genutzt werden, siehe auch PKI (Public Key Infrastructure). Die organisatorischen Anforderungen sind gegenüber symmetrischen Verfahren wesentlich geringer. Die Sicherheitsziele werden durch Verwendung bekannter mathematischer Zusammenhänge und Verfahren der Kryptographie erreicht. Die eingesetzte Technik ist seit Jahren bekannt, standardisiert und erprobt.

3.3 Berechnung und Prüfung digitaler Signaturen

Abbildung 3 stellt die prinzipiellen Abläufe von der Signaturberechnung bis zur Signaturprüfung dar. Im System A wird über einen beliebigen Datensatz m ein Hashwert berechnet. Im System A existiert ein privater (oder auch geheimer) Schlüssel. Mit diesem Schlüssel wird der zuvor berechnete Hashwert unter Anwendung eines Signaturverfahrens verschlüsselt. Ergebnis ist die digitale Signatur. Der Datensatz m wird zusammen mit der berechneten Signatur zum System B übertragen. B verfügt über den zum privaten Schlüssel vom System A gehörenden öffentlichen Schlüssel. Der öffentliche Schlüssel von A kann allgemein bekannt gemacht werden. Zur Prüfung der Integrität und Authentizität berechnet B als erstes den Hashwert des empfangenen Datensatzes m. In einem zweiten Schritt entschlüsselt B mit dem öffentlichen Schlüssel von A die empfangene digitale Signatur. Nur wenn der zuvor von B berechnete Hashwert über den Datensatz m mit dem entschlüsselten, ursprünglich von A berechneten Hashwert übereinstimmt, kann der Datensatz m als integer und authentisch angesehen werden. Dabei muss sichergestellt sein, dass B der Zugehörigkeit des öffentlichen Schlüssels zu A vertrauen kann.

Daraus lassen sich die Vorteile digitaler Signaturen leicht ableiten. Digitale Signaturen machen Manipulationen an den Daten selbst erkennbar. Jede kleinste Veränderung von Daten ist nach deren Signierung bei Prüfungen erkennbar. Es werden nur die signierten Daten und der Prüfschlüssel (öffentlicher Schlüssel) benötigt.

Digitale Signaturen sind praktisch allen anderen Verfahren zur Manipulationssicherung überlegen. Die „Ende-zu-Ende“-Absicherung gewährleistet einen Schutz der Daten zwischen Endpunkten einer Kommunikationskette, z. B. zwischen Registrierkasse und Unternehmensleitung. Die Sicherheit basiert nicht auf der Geheimhaltung eines Verfahrens, sondern auf sehr gut untersuchten mathematischen Verfahren. Die Sicherheit kann von unabhängigen Prüfern bestätigt werden. Aktuelle Kryptographieverfahren sind praktisch nicht zu brechen.

3.4 Hauptmerkmale der INSIKA-Lösung

Jeder Buchungsdatensatz wird nach Buchungsabschluss digital signiert und zusammen mit der digitalen Signatur gespeichert. Danach ist er nicht mehr unerkannt veränderbar. Mit jedem zur Buchung gehörenden Beleg ist eine Prüfung möglich, ob der Buchungsdatensatz aufgezeichnet wurde. Die Summen jeder Buchung werden fortlaufend summiert und in einem sicheren Speicher abgelegt. Von diesem Speicher wird täglich eine signierte Sicherungskopie angelegt.

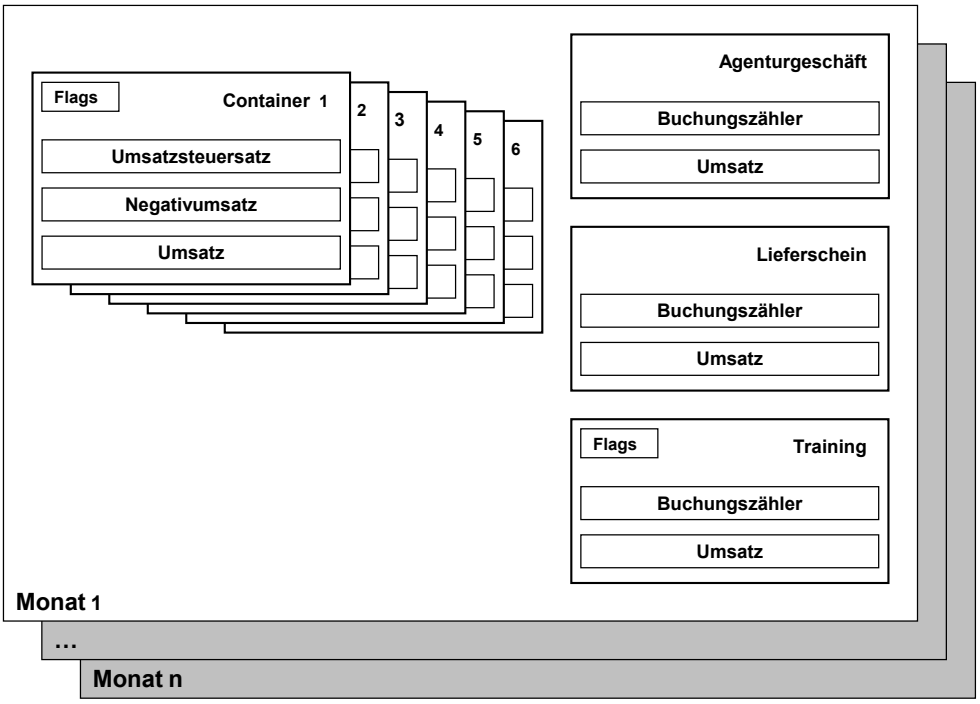


Abbildung 4: TIM-Speichermodell

Die Datenspeicherung kann dabei auf beliebigen Datenträgern erfolgen.

Der entscheidende Hardware-Sicherheitsanker ist eine Signaturerstellungseinheit mit dem Signaturschlüsselpaar. INSIKA verwendet eine Smartcard, die als TIM (Tax Identification Modul) bezeichnet wird. Das Signaturschlüsselpaar wird einmalig kartenintern erzeugt. Der geheime Schlüssel ist nicht auslesbar. Der zugehörige öffentliche Schlüssel kann dagegen ausgelesen werden. Für den öffentlichen Schlüssel wird von einer neutralen Stelle (Zertifizierungsdienstanbieter) ein Zertifikat ausgestellt, das die Zugehörigkeit des öffentlichen Schlüssels zu einem Steuerpflichtigen bestätigt. Der öffentliche Schlüssel ist im Zertifikat enthalten. Die Smartcard muss so angesteuert werden, dass die im INSIKA-Konzept festgelegten Datenstrukturen für die jeweilige Anwendungsumgebung korrekt signiert werden. Andernfalls schlägt jede Prüfung fehl.

3.5 Funktionen der INSIKA-Smartcard

3.5.1 Signaturerstellung

Die digitalen Signaturen werden mit einer handelsüblichen Smartcard erzeugt, die neben den im Sicherheitskonzept festgelegten Kryptographieverfahren über ein zusätzliches, speziell für INSIKA entwickeltes Softwarepaket verfügen. INSIKA verwendet als Hashverfahren SHA-1 (Secure Hash Algorithm) gemäß FIPS 180-1 mit 160 bit und als Kryptographieverfahren ECDSA (Elliptic Curve Discrete System Algorithm) gemäß ANSI X9.62 auf dem Grundkörper GF(p) mit einer Schlüssellänge von 192 bit. Bei den zu signierenden Daten handelt es sich ausnahmslos um kurze, strukturierte Daten im TLV-Format (Tag, Length, Value). Die Smartcard wird über eine Kartenleseeinheit von der Registrierkasse gemäß der INSIKA TIM Schnittstellendokumentation [10, 11] angesteuert. Nur so können INSIKA-konforme Buchungen und Belegdrucke erzeugt werden. Anders kann man die vom Gesetz geforderten Ursprungsdaten nicht im INSIKA-Format bereitstellen.

3.5.2 Sequenzzähler und Summenspeicher

Gedruckte Kassenbelege und die zugehörigen, elektronisch gespeicherten Buchungen werden mit der von der Smartcard erzeugten digitalen Signatur versehen. Entsprechend dem INSIKA-Sicherheitskonzept führt die Smartcard intern einen von außen nicht beeinflussbaren Sequenzzähler. Jedem Buchungsdatensatz wird von der Smartcard-Software im Zuge der Signaturberechnung der aktuelle eindeutige und monoton steigende Wert des Sequenzzählers hinzugefügt. Der jeweilige Wert des Sequenzzählers ist somit Bestandteil des signierten Datensatzes.

Die Smartcard verwaltet verschiedene, kartenintern Summenspeicher, welche die Gesamtumsätze so erfassen, dass selbst im Falle des Verlustes von extern gespeicherten Daten wesentliche Kennzahlen (Monat-

sumsätze, negative Buchungen usw.) ermittelt werden können – siehe Abbildung 4. Für jeden Monat sind Container für sechs Umsatzsteuersätze mit dem Umsatzsteuersatz, Umsatz und Negativumsatz sowie Container für Agenturumsatz, Lieferscheinumsatz und Umsatz bei Nutzung von Trainingsfunktionen mit dem entsprechenden Umsatz und je einem Buchungszähler vorhanden. Darüber hinaus werden eventuelle Speicherüberläufe angezeigt. Änderungen des Umsatzsteuersatzes innerhalb eines Monats werden ebenfalls detektiert. Der Wechsel eines Umsatzsteuersatzes erfolgt i.d.R. monatsgenau. Die Summenspeicher sind nur im Zusammenhang mit der Berechnung von Buchungssignaturen ansprechbar. Die komplette Zugriffskontrolle hat nur die unveränderbare TIM-Software. Der erste Monat kann frühestens ab dem im TIM gespeicherten Personalisierungsdatum angesprochen werden.

Die Kartensoftware muss sowohl die Aufsummierung der einzelnen Umsätze aus jeder Einzelbuchung als auch die Abfrage von Umsätzen über unterschiedliche Zeiträume durch die Registrierkasse unterstützen. Die Erzeugung der Signaturen ist mit der Verwaltung von Sequenzzähler und Summenspeichern so miteinander verknüpft, dass mit der Signaturberechnung eine neue Sequenznummer vergeben wird und die Summenspeicher aktualisiert werden. Sequenzzähler, die karteninternen Summenspeicher und der gedruckte Beleg sind die wesentlichen Sicherheitsmerkmale der INSIKA-Lösung.

3.5.3 Datenplausibilisierung

Die festgelegten Daten einer Buchung und des dazugehörigen gedruckten Belegs sind identisch. Dadurch ist sichergestellt, dass es keinen Unterschied zwischen Buchungs- und Belegsignatur gibt. Über die in beiden Datenstrukturen enthaltene identische Sequenznummer ist eine eindeutige Zuordnung eines Belegs zu einer Buchung möglich. Buchungsdatensätze können auf beliebigen Medien gespeichert werden. Dadurch sind Datenverluste weitgehend ausgeschlossen.

Über die Belegausgabe zu jeder Buchung ist die korrekte zeitnahe Aufzeichnung der Daten nachweisbar, da alle weiteren Schritte über Verknüpfung der verschiedenen Funktionen innerhalb der Smartcard erzwungen werden. Erkennt die Smartcard Syntaxfehler, unplausible Daten, Pufferüberläufe, Speicherfehler, kryptographische Angriffe oder sonstige Unregelmäßigkeiten werden entsprechende Statusinformationen ausgegeben.

3.6 Datenschnittstellen

3.6.1 TIM-Schnittstelle

Von der Registrierkasse werden die Daten in der in den INSIKA-Dokumentationen festgelegten Art und Weise an die Smartcard übergeben. Die Smartcard prüft die Daten auf syntaktische Fehler und filtert bestimmte Datenelemente heraus. Der zu signierende Datensatz wird kartenintern um die o. g. Sequenznummer und die Identifikation des Steuerpflichtigen ergänzt. Beide Informationen werden zusammen mit der Signatur der Registrierkasse als Antwortdatensatz zurückgegeben.

3.6.2 INSIKA-XML-Export-Schnittstelle

Die Registrierkasse bzw. ein nachgelagertes System muss eine weitere Datenschnittstelle unterstützen. Dabei handelt es sich um die INSIKA-XML-Export-Schnittstelle zur Bereitstellung gespeicherter Buchungsdaten zu Prüfzwecken, siehe [12]. Aus den XML-Daten lassen sich alle zur Verifikation erforderlichen Informationen gewinnen. Neben allen Einzelbuchungen werden signierte Tagesabschlüsse und Zertifikate der zugehörigen Signaturschlüssel übergeben.

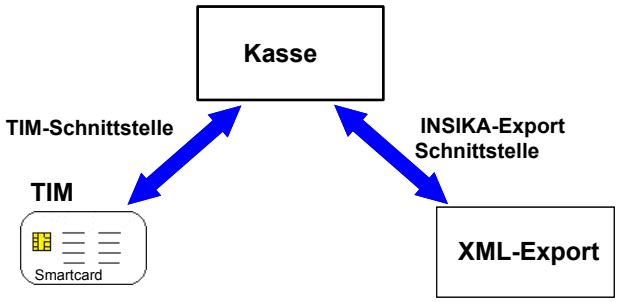


Abbildung 5: INSIKA-Schnittstellen

3.7 Elemente eines Buchungsdatensatzes

Ein zu signierender Buchungsdatensatz muss nach [6] folgende Datenelemente enthalten:

1. Identifikationsmerkmal (Steuerkennzeichen und Kartenkennung)
2. Buchungs-/Belegnummer (Signatursequenznummer)
3. Tag und der Uhrzeit der Buchung
4. Handelsübliche Bezeichnung der Ware oder Dienstleistung
5. Preis der Ware oder Dienstleistung

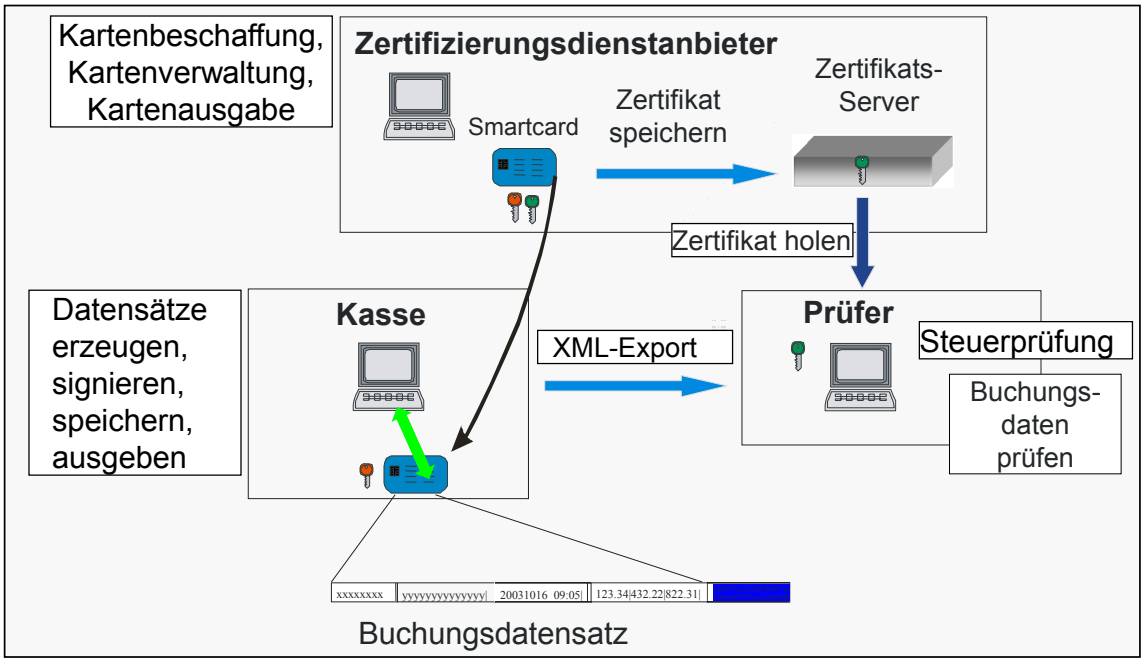


Abbildung 6: INSIKA-Systemumfeld

6. Umsatzsteuersatz
7. Bedieneridentifikation
8. Art der Buchung: Umsatz normal, Agenturgeschäft, Lieferschein, Training Dieses, in [6] als Buchungsstatus geforderte Datenelement wird nach INSIKA-Konzept über die Ansteuerung der in 3.5.2 beschriebenen Summenspeicher unterstützt.
9. Gesamtsummen je Steuersatz (Umsatz, Negativumsatz)
10. Umsatzsteuer je Steuersatz

Die Elemente 1 und 2 werden von der Smartcard in den zu signierenden Datensatz eingefügt. Die Elemente 4 bis 6 können als unterschiedliche Buchungspositionen mehrfach auftreten. Über alle Einzelbuchungspositionen muss die Registrierkasse den Hashwert der Buchungspositionen mit der SHA-1-Funktion berechnen. Anstelle einer Vielzahl von Buchungspositionen muss die Registrierkasse nur noch den Hashwert der Buchungspositionen in den zu signierenden Datensatz einfügen. Der Hashwert der Buchungspositionen muss auf dem Beleg ausgegeben werden.

3.8 Systemumfeld und Kartenbereitstellung

3.8.1 INSIKA-Systemumfeld

Abbildung 6 stellt eine mögliche Ausprägung des Systemumfeldes mit allen wesentlichen Komponenten und Abläufen dar. Für jede Registrierkasse muss eine auf den Steuerpflichtigen personalisierte Smartcard entsprechend 3.4 vorhanden sein. Das Zertifikat mit dem öffentlichen Schlüssel wird auf dem Zertifikatsserver des Zertifizierungsdienstanbieters bereitgestellt und darüber hinaus auf der Smartcard selbst gespeichert. Der Zertifizierungsdienstanbieter verwaltet auch eine Sperrliste von INSIKA-Zertifikaten. Die Smartcard wird wie beschrieben mit der Registrierkasse gekoppelt und signiert mit dem geheimen, für Niemanden zugänglichen Schlüssel alle steuerlich-relevanten Datensätze entsprechend INSIKA-Festlegungen.

Die Datensätze werden nach der Rückgabe von Sequenznummer und Signatur vom TIM zur Registrierkasse mit den Signaturen auf beliebigen Speichermedien abgelegt und können auch mehrfach gesichert (gespeichert) werden. Die Eindeutigkeit der Daten wird über den Zeitbezug und die in der Smartcard erzeugte Sequenznummer sichergestellt. Die Sequenznummer verhindert eine unzulässige Duplizierung von Datensätzen und die Manipulation des Zeitbezugs.

Zur Prüfung müssen die Daten im XML-Exportformat durch den Steuerpflichtigen für einen vom Prüfer angeforderten Zeitraum bereitgestellt werden. Mit geeigneten Prüfprogrammen kann die Unversehrtheit und Vollständigkeit der Ursprungsaufzeichnungen ermittelt werden.

3.8.2 Nutzungsdauer einer INSIKA-Smartcard

Nach Personalisierung der Smartcard, d.h. der Ausstellung eines Zertifikats durch einen Zertifizierungsdienstanbieter, ist diese für höchstens zehn Jahre einsetzbar. Die Zertifikate müssten in diesem Falle für 20 Jahre zur Verfügung stehen, da die Daten zehn Jahre aufbewahrt werden müssen.

3.8.3 Beschaffung von INSIKA-Smartcard

Zum Betrieb des INSIKA-Systems müssen für die Bereitstellung und Nutzung der Smartcard eindeutige Festlegungen getroffen werden, die von allen Beteiligten anerkannt werden. Optimal wäre hier eine klare gesetzliche Regelung. Die akzeptierte Struktur zu signierender Datensätze und die daraus gewonnenen INSIKA-Export-Daten sind Grundelemente zur Anerkennung des Verfahrens als nichtmanipulierte Ursprungsaufzeichnungen. Für die Kartenbereitstellung bieten sich verschiedene Alternativen an. In jedem Fall sollte eine zentrale Stelle diese Funktion übernehmen.

Einheitliche Handlungsanweisungen für die Kartenverwendung erlauben den Aufbau und Betrieb des in sich abgeschlossenen Sicherheitssystems. Die Kartenpersonalisierung, d. h. die Zuordnung einer oder mehrerer Smartcard zu einem Unternehmer erfordert keine Synchronisierung zwischen verschiedenen Kartenausgebern. Finanzbehörden, andere Prüfinstanzen oder die Steuerpflichtigen selbst können auf die in den INSIKA-Dokumentationen festgelegten Datenstrukturen und Abläufe zurückgreifen. Die Kassenhersteller integrieren die Kartenleseeinheit und die INSIKA-Funktionalität in die Kassensysteme. Bei dezentraler Kartenausgabe durch mehrere unterschiedliche Zertifizierungsdienstanbieter wäre eine Synchronisation zwischen allen beteiligten Zertifizierungsdienstanbietern erforderlich. Zur vollständigen Datenprüfung muss die Anzahl auf einen Steuerpflichtigen ausgestellter INSIKA Smartcard bekannt bzw. abrufbar sein.

4 INSIKA-Konzept für Registrierkassen

4.1 Kassenfunktionen

Bei korrekter Anwendung des INSIKA-Konzepts werden von der Registrierkasse alle Buchungen nachweisbar aufgezeichnet. Somit kann die in den GoBS geforderte Qualität von Ursprungsaufzeichnungen erfüllt werden. Zusätzlich zu den Buchungsdaten sind lediglich die zugehörigen Signaturen zu speichern. Zur Prüfung wird eine geeignete Prüfsoftware verwendet, die eine Verifikation der signierten Datensätze vornimmt. Die Unversehrtheit der Daten wird durch die digitalen Signaturen nachweisbar. Selbst bei Verlust gespeicherter Daten kann durch Auslesen der Summenspeicher der Smartcard der kumulierte Umsatz für alle Umsatzarten nachgewiesen werden. Wesentliche Funktionen von Registrierkassen im INSIKA-Umfeld sind vollständige elektronische Einzelaufzeichnungen aller Buchungen und die Ausgabe prüfbarer, gedruckter Belege. Die Konzeptumsetzung ist technisch relativ einfach, da keine besonderen bauartbedingten Anforderungen von den Registrierkassen erfüllt werden müssen.

Das elektronische Journal muss nur die in den INSIKA-Spezifikationen festgelegten Daten enthalten mit denen der INSIKA-Export korrekt ausgeführt werden kann. Die Datenprüfung ist ohne Rückgriff auf weitere Daten (z. B. Artikelstammdaten) möglich. Durch das festgelegte INSIKA- Exportformat ist kein herstellerspezifisches „Spezialwissen“ zur Auswertung des Journals erforderlich.

4.2 Typische Elemente eines INSIKA-Belegs

Im Folgenden wird ergänzend zu 3.7 am Beispiel eines Belegs gezeigt, welche konkreten Elemente zur Kontrolle einer Buchungssignatur verwendet werden. Abbildung 7 zeigt notwendige Elemente eines typischen INSIKA-Belegs. Die Zuordnung des Belegs zu einem Unternehmen ist über die Umsatzsteueridentifikationsnummer ergänzt um die eindeutige laufende TIM-Kartennummer möglich. Diese Kombination verweist auf das TIM, mit dem die Buchungssignatur berechnet wird. Über alle Artikelpositionen wird nach genau festgelegten Verfahren der SHA-1-Hashwert berechnet. Dieser wird zusammen mit den Umsätzen, den Umsatzsteuersätzen, dem Datum und der Zeit sowie der Bedieneridentifikation an das TIM zur Signaturberechnung übergeben. Die Sequenznummer wird nach der Signaturberechnung vom TIM zurückgegeben. Der QR-Code enthält alle zur Belegprüfung erforderlichen INSIKA-Elemente. Dabei muss sichergestellt sein, dass die Druckqualität des QR-Codes das Lesen der darin enthaltenen Daten ermöglicht. Kann kein QR-Code gedruckt werden, müssen Hashwert der Buchungspositionen und Buchungssignatur im festgelegten Format auf dem Beleg erscheinen [1].

[1] Die Angaben entsprechend Abbildung 7 lauten für den Hashwert der Buchungspositionen: 76JHC-OK5F7-S3YHJ-E6KES-LY4MZ-2XNHL-NR und für die Signatur: W7PQA-73P7K-INMSU-YGK2L-44CVB-S4336-EWQL6-T5ZJQ-G5YDV-EE7NO-GVIAK-HCV6A-GNBID-2I63J-6L23M-UY=

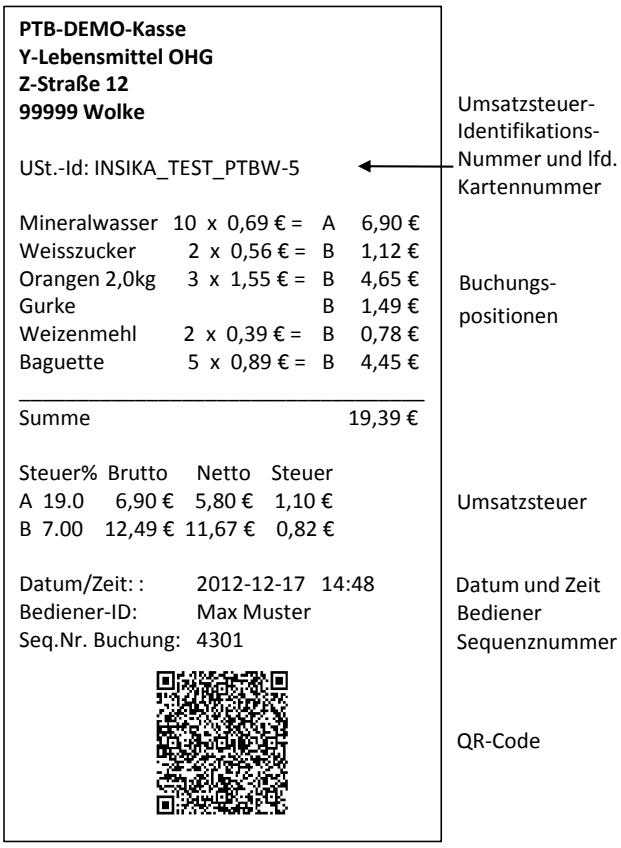


Abbildung 7: Typische Elemente eines INSIKA-Belegs

In Abhängigkeit vom Geschäftsvorfall müssen weitere steuerlich-relevante Informationen wie Agenturgeschäft, Trainingsmodus oder Stornobuchungen ebenfalls auf dem Beleg deutlich abgebildet werden, da sie Bestandteil des für INSIKA festgelegten Buchungsdatensatzes sind.

4.3 Datenspeicherung und Datensicherung

Für die Datenspeicherung kassenintern oder auf externen Systemen gibt es keine Vorgaben. Es muss nur sichergestellt sein, dass auf Anforderung die Buchungsdaten auch aus herstellerspezifischen Datenstrukturen im festgelegten INSIKA- Exportformat bereitgestellt werden können. Zusätzlich zu den bekannten Daten sind lediglich die Sequenznummern und die berechneten Signaturen zu speichern.

Zur sicheren Speicherung der nachweispflichtigen Buchungen sollten die Daten aus der Registrierkasse in regelmäßigen Abständen auf ein anderes Speichermedium (Speicherkarte, USB-Speicher o. ä.) oder anderes System übertragen werden. Zusätzlich müssen nach dem INSIKA-Konzept die signierten Tagesabschlüsse durch Auslesen der TIM-Summenspeicher als Report bereitgestellt werden. Das Auslesen muss zu keinem exakt festgelegten Zeitpunkt erfolgen. Jeder Report enthält eine eigene Reportsequenznummer, die ebenfalls vor Berechnung der Reportsignatur vom TIM bereitgestellt wird. Die Struktur der signierten Reports ist ebenfalls in der XML-Beschreibung exakt festgelegt [12]. Die Konvertierung von Daten aus einem beliebigen, auch herstellerspezifischen Format in ein „prüfungsfähiges“ Format der INSIKA-XML-Exportschnittstelle ist ohne größeren Aufwand möglich.

4.4 Aufwand für INSIKA-Implementierung in Kassen

Der Aufwand zur Errichtung und zum Betrieb von INSIKA ist im Vergleich zu den anderen Lösungsansätzen klein. Bei einer Abschätzung des Gesamtaufwands müssen Kassenhersteller, Kassenbetreiber und Finanzbehörden berücksichtigt werden. Kassenhersteller müssen die Smartcard in die Registrierkasse integrieren und dabei die Kassensoftware so verändern, dass die INSIKA-Anforderungen erfüllt werden. Zum Betrieb der Smartcard ist eine Kartenleseeinheit erforderlich. In Abhängigkeit von der vorhandenen Kassenhardware muss entweder ein Kartenleser aus einzelnen Komponenten aufgebaut und in das bestehende System integriert werden oder es wird auf einen handelsüblichen Kartenleser zurückgegriffen. Die zweite Variante empfiehlt sich insbesondere für PC-basierte Lösungsansätze. Die Gesamtkosten je Registrierkasse für die Hardware und Softwareanpassung ist gering und relativ leicht abschätzbar. Der Aufwand für Kassenbetreiber ist ebenfalls vergleichsweise gering. Er muss ein TIM beschaffen und diese in sein Kassensystem einbauen bzw. einbauen lassen. Er hat sicherzustellen, dass die Daten in dem durch den Gesetzgeber festgelegten Zeitraum zuverlässig elektronisch gespeichert werden. Die Kosten für die vom Konzept geforderte Belegausgabe sind gering. Auf Nachfrage können die Daten im INSIKA- Exportformat für den nachgefragten Zeitraum bereitgestellt werden.

Die Anforderungen an das TIM wurden gemeinsam mit Experten der Finanzverwaltung festgelegt. Damit sind wesentliche Voraussetzungen zur Anerkennung des INSIKA-Verfahrens bereits erfüllt. Es muss für einen flächendeckenden Einsatz von INSIKA sichergestellt sein, dass TIM in ausreichender Anzahl mittel- und langfristig zur Verfügung stehen. Das kann weitgehend durch die Einbeziehung eines geeigneten Zertifizierungsdienstanbieters geschehen, der INSIKA-Smartcard einschließlich der Zertifikate als Produkt anbietet. Die Prüfung der Übereinstimmung der An-

forderungen an die INSIKA-Smartcard muss durch eine unabhängige Prüfinstanz erfolgen.

4.5 Prüfung der Datenaufzeichnungen

Zur Prüfung der gespeicherten elektronischen Daten ist die Konvertierung in das festgelegte INSIKA-Exportformat zwingend erforderlich. Ein Prüfprogramm muss als erstes die Signaturen der Tagesabschlüsse verifizieren. Bei Übereinstimmung der aufsummierten Einzelbuchungen mit den Summenangaben in den Tagesabschlüssen ist keine Signaturprüfung der Einzelbuchungen erforderlich. Bei Bedarf kann jedoch eine vollständige oder stichprobenartige Kontrolle der einzelnen Buchungen vorgenommen werden. Gedruckte Belege können unter Anwendung unterschiedlicher Methoden überprüft werden. Manipulationen und Fälschungen werden sicher erkannt. Die Eingabe der Belegdaten kann durch den Einsatz moderner Methoden so optimiert werden, dass eine hohe Prüfdichte möglich wird. Der Prüfaufwand wird durch automatisierte Prüfungen stark verringert, was durch exakt festgelegte Schnittstellen und Datenformate ermöglicht wird. Durch die vollständige Aufzeichnung aller Buchungs- und Journaldaten steht eine exakte, nicht unerkannt veränderbare Datenbasis zur Verfügung. Die Prüftiefe kann bei gleichzeitiger Verringerung der Prüfzeiten deutlich erhöht werden.

5 Vorteile des INSIKA-Konzepts

Die Anwendung bekannter und erprobter kryptografischer Verfahren gewährleistet einen hohen Sicherheitsstandard. Eindeutig definierte Schnittstellen garantieren einerseits eine hohe Systemstabilität und lassen andererseits Freiraum bei der Entwicklung von Komponenten. Es gibt keine Bauartanforderungen an Systemhersteller, da die Signierung nur dann möglich ist, wenn die an die INSIKA-Smartcard übergebenen Daten den Anforderungen der INSIKA-Spezifikation entsprechen. Bauartzulassungen von Systemen und Komponenten sind demzufolge nicht erforderlich. Die Datenspeicherung kann auf beliebigen Datenträgern in beliebigen Formaten erfolgen. Bei konsequenter Nutzung des Verfahrens können effektive Prüfmethoden entwickelt werden. Für den Nutzer des Verfahrens wird der Nachweis korrekter Datenaufzeichnungen möglich.

Systeme, die das offene INSIKA-Verfahren nutzen, entsprechen der in 1.2 genannten BRH-Empfehlung eines eingriffssicheren Bauteils, das verfahrensbedingt nachträgliche Veränderungen an aufgezeichneten Daten erkennbar macht.

6 Zusammenfassung und Ausblick

Das INSIKA-Konzept zum Schutz von Kassensystemen hat national und international Beachtung gefunden. Grundzüge des Konzepts wurden bereits seit 2004 in internationalen Gremien diskutiert. Seit 2008 wurden im vom BMWi geförderten INSIKA-Projekt das Konzept verfeinert und die Spezifikationen erarbeitet. Lösungsansatz, Projektfortschritt und Ergebnisse der Pilot- und Feldversuche sind während der Projektlaufzeit auf mehreren Veranstaltungen dargestellt worden.

Die technischen Spezifikationen zur Umsetzung des Konzepts stehen als stabile Versionen interessierten Unternehmen zur Verfügung. In mehrjährigen Pilot- und Feldversuchen wurde für die Anwendungsgebiete Kassen und Taxi der Funktionsnachweis erbracht. Die Bundesdruckerei GmbH hat Produktion und Vertrieb der INSIKA-Smartcard übernommen. Als anerkannter Zertifizierungsdienstanbieter garantiert die Bundesdruckerei GmbH die geforderte Verfügbarkeit der ausgestellten INSIKA-Zertifikate. Das Land Hamburg fördert seit 2012 den Einsatz manipulationsgeschützter Systeme für die Datenaufzeichnung von Taxameterdaten. Die Verkehrsaufsichtsbehörde Hamburg ist Registrierungsstelle für Hamburger Taxiunternehmer als Vorstufe der Zertifikatserstellung durch die Bundesdruckerei GmbH. Derzeit sind bereits über 100 Hamburger Taxen mit INSIKA-Komponenten ausgestattet. Die Verantwortlichen in Hamburg gehen davon aus, dass bis zum Ende der Fördermaßnahme zum 31.12.2013 etwa fünfzig Prozent der Hamburger Taxen über INSIKA-Technik verfügen. Das Land Berlin fördert einen Pilotversuch mit fünf Taxen und plant weitere Schritte nach dem Hamburger Modell.

Nach wie vor gibt es in Deutschland keine gesetzlich geregelte technische Lösung. Der Gesetzgeber beschränkt sich auf grundsätzliche Anforderungen ohne technische Konkretisierungen. Bei konsequenter Anwendung des INSIKA-Konzepts wird Steuerbetrug verhindert und mehr Steuergerechtigkeit erreicht. Der steuerpflichtige Unternehmer hat bei Anwendung des Systems den Vorteil, dass er nachweisen kann, dass alle elektronischen Aufzeichnungen über Bareinnahmen den gesetzlichen Anforderungen entsprechen. Die Mehrkosten sind sowohl bei der Nachrüstung bestehender Kassensysteme als auch bei neuen Systemen wesentlich geringer als bei den bekannten Fiskalsystemen. Es muss darauf hingewiesen werden, dass auch INSIKA als Fiskallösung eine Marktaufsicht benötigt.

Für den erfolgreichen INSIKA-Einsatz müssen Betriebsprüfer mit den entsprechenden Kenntnissen, Techniken und Prüfanweisungen für die Marktaufsicht ausgestattet werden. Ohne Marktaufsicht kann das System dadurch unterlaufen werden, dass die gesicherte Registrierkasse nicht oder nur sporadisch benutzt wird.

Literatur

[1] Bundesrechnungshof. »54 – Drohende Steuerausfälle aufgrund moderner Kassensysteme«. In: *Unterrichtung durch den Bundesrechnungshof*. Deutscher Bundestag, 15. Wahlperiode, Drucksache 15/2020 (24. Nov. 2003), S. 197–198. URL: http://dip.bundestag.de/.

[2] Erich Huber. »Über Registrierkassen, Phantomware, Zapping und Fiskallösungen aus Deutschland und Österreich - Teil I«. In: *Die steuerliche Betriebsprüfung* (Juni 2009). URL: http://www.stbpdigital.de/STBP.06.2009.153.

[3] Willi Härtl und Susanne Schieder. »Ordnungsmäßigkeit digital geführter Erlösaufzeichnungen - Elektronische Registrierkassen und digitale Erlöserfassungssysteme im Brennpunkt des Steuerrisikos Erlösverkürzung - Teil I«. In: *Die steuerliche Betriebsprüfung* (Feb. 2011). URL: http://www.stbpdigital.de/STBP.02.2011.033.

[4] BMAS. »Zweites Gesetz zur Änderung des Sozialgesetzbuches Viertes Buch (SGB IV) und anderer Gesetze (2. SV-ÄndG). Referentenentwurf«. 5. Juni 2008.

[5] Norbert Zisky. »Manipulationsschutz elektronischer Registrierkassen und Kassensysteme. Konzeptpapier BMF IV/2/PTB«. 15. März 2004.

[6] BMF AG Registrierkassen. *Fachkonzept zur Einführung eines neuen Verfahrens zum Manipulationsschutz elektronischer bzw. PC gestützter Registrierkassen und –systeme*. Juli 2008.

[7] BMAS und BMF. *Aktionsprogramm der Bundesregierung für Recht und Ordnung auf dem Arbeitsmarkt*. Bundesrepublik Deutschland, Bundesministerium für Arbeit und Soziales, Bundesministerium der Finanzen, 4. Juni 2008. URL: http://www.olafscholz.de/media/public/db/media/1/2010/12/191/20080604_gemeinsames_schreiben_bmf_und_bmas_zum_aktionsprogramm_recht_undordnung_auf_dem_arbeitsmarkt1.pdf.

[8] BMJ. *Abgabenordnung*. Version 22.12.2011. Bundesrepublik Deutschland, Bundesministerium der Justiz, Dez. 2011. URL: http://www.gesetze-im-internet.de/ao_1977/index.html.

[9] Luigi Lo Iacono u. a. »Sicherheitslösung für die automatisierte Messdatenkommunikation«. In: *Datenschutz und Datensicherheit - DuD* 30 (6 2006), S. 347–352. ISSN: 1614-0702. DOI: 10.1007/s11623-006-0105-6.

[10] INSIKA-Projekt. *INSIKA TIM Schnittstellendokumentation*. Version T.1.0.6-02. Physikalisch-Technische Bundesanstalt, März 2010. URL: http://insika.de/.

[11] INSIKA-Projekt. *INSIKA TIM Schnittstellendokumentation, Zusatz*. Version T.1.1.0-01. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: http://insika.de/.

[12] INSIKA-Projekt. *INSIKA Exportformat*. Version T.1.0.6-01. Physikalisch-Technische Bundesanstalt, März 2010. URL: http://insika.de/.

Einsatz von Kryptographie zum Schutz von Daten

Mathias Neuhaus
bis 02/2011 bei: cv cryptovision GmbH
Munscheidstr. 14, 45886 Gelsenkirchen
mathias@dokom.net

Der Beitrag bietet einen Überblick über in der modernen Kryptographie eingesetzte Verfahren und bewertet deren Eignung für die Zwecke der Verschlüsselung oder Signatur. Im zweiten Teil werden die Aufgaben der im INSIKA Projekt eingesetzte Smart Card (TIM) beschrieben. Die Smart Card bildet die zentrale Instanz zur Absicherung der in der Kasse erfassten Umsatzdaten gegen eine nachträgliche Manipulation.

1 Kryptographie

1.1 Grundlagen der Kryptographie

1.1.1 Ziele beim Einsatz von Kryptographie

Zur Erreichung unterschiedlicher Ziele werden unterschiedliche kryptographische Verfahren eingesetzt. Typische Ziele umfassen:

Geheimhaltung: Zum Schutz gegen unbefugtes Lesen können Dokumente verschlüsselt werden.

Integrität: Eine Veränderung an einem Dokument lässt durch einen Message Authentication Code (MAC) oder eine digitale Signatur zweifelsfrei nachweisen.

Authentizität: Der Urheberschaft eines Dokumentes lässt sich durch eine digitale Signatur dokumentieren.

Nicht-Bestreitbarkeit: Durch eine digitale Signatur lässt sich der Verfasser eines Dokumentes zweifelsfrei ermitteln. Damit ist es für diesen auch nicht möglich die Urheberschaft abzustreiten.

1.1.2 Kryptographische Paradigmen

Bei der Auswahl eines geeigneten Verfahrens sollten einige grundlegende Überlegungen nicht außer Acht gelassen werden.

Auguste Kerkhoffs formulierte schon 1883 seinen Grundsatz für die moderne Kryptographie, dass die Sicherheit eines kryptographischen Verfahrens durch Geheimhaltung des Schlüssels, nicht aber durch alleinige Geheimhaltung des Verfahrens beruhen darf (Kerkhoffs‘ Paradigma). Dies steht im klaren Gegensatz zum leider viel zu häufig angewandten „Security by Obscurity“.

Die Forderungen nach Praxisnähe und absoluter Sicherheit schließen einander weitgehend aus. So bieten Einmalschlüssel zwar eine absolute Sicherheit. Leider ist dieses Verfahren in der Praxis nicht anwendbar, da die sichere Übertragung der Schlüssel denselben Aufwand erfordern würde wie die sichere Übertragung der Daten selbst.

Die Sicherheit heute praktisch einsetzbarer Verfahren basiert auf Annahmen aus der Zahlen- und Komplexitätstheorie.

1.2 Kryptographische Verfahren

Die in der modernen Kryptographie verwendeten Verfahren lassen sich grob in symmetrische, asymmetrische und sonstige Verfahren einteilen.

1.2.1 Symmetrische Verfahren

Symmetrische Verfahren verwenden einen einzelnen geheimen Schlüssel. Sie basieren typischerweise auf einfachen Bitoperationen.

Bild 1 stellt den typischen Verlauf einer Ver- und Entschlüsselung mit symmetrischer Kryptographie dar. Dabei wird die zu sichernde Nachricht mittels des geheimen Schlüssels verschlüsselt. Die Nachricht wird an den Empfänger übertragen. Dieser kann die Nachricht dann mit demselben geheimen Schlüssel wieder in eine lesbare Form entschlüsseln.

Die Vorteile der symmetrischen Verfahren liegen

PTB-Bericht IT-18
doi:10.7795/210.20130206a

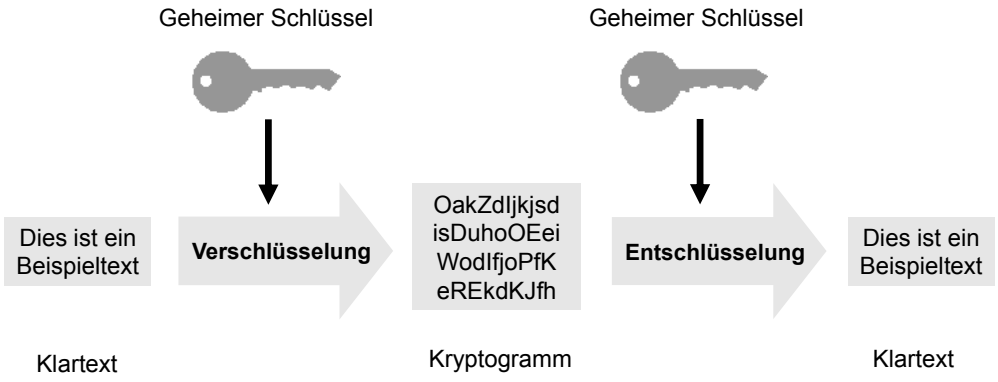


Abbildung 1: Symmetrische Verschlüsselung

in der leichten Implementierbarkeit (in Hardware und Software) und der erzielbaren hohen Performance.

Der wesentliche Nachteil der symmetrischen Verfahren ist die Verwaltung der benötigten Schlüssel.

Wird ein einziger geheimer Schlüssel für alle Kommunikationsteilnehmer verwendet, ist die eindeutige Zuordnung des Schlüssels zu einem Teilnehmer nicht mehr möglich und damit die Forderung nach der Nicht-Bestreitbarkeit nicht erfüllbar. Darüber hinaus wäre durch die Offenlegung des Schlüssels die gesamte Kommunikation kompromittiert.

Alternativ kann man für je zwei Kommunikationsteilnehmer einen eigenen Schlüssel verwenden. Damit werden bei n Teilnehmern $n^2 - 1$ Schlüssel benötigt – was nur mit erheblichem Aufwand zu verwalten ist.

Typische Verfahren dieser Gruppe sind DES, Triple-DES, AES oder RC4. Im Einsatz sind diese Verfahren wegen der mangelhaften Schlüsselverwaltung praktisch nur für die Verschlüsselung.

1.2.2 Asymmetrische Verfahren

Asymmetrische Verfahren verwenden ein Schlüsselpaar aus einem privaten und einem öffentlichen Schlüssel. Diese Verfahren basieren auf komplexer Langzahlenarithmetik.

Bild 2 stellt den Vorgang einer digitalen Signatur (und Verifikation) unter Verwendung asymmetrischer Kryptographie grafisch dar. Dabei wird die abzusichernde Nachricht zunächst gehashed und der Hashwert mit dem privaten Schlüssel des Absenders signiert. Nachricht und Signatur werden an den Empfänger übertragen. Der Empfänger führt nun dieselbe Hashberechnung durch und kann dann mit dem öffentlichen Schlüssel des Absenders die Gültigkeit der Signatur überprüfen.

Der große Vorteil asymmetrischer Verfahren liegt in der einfachen Schlüsselverwaltung. Der öffentliche Schlüssel kann problemlos an alle Teilnehmer verteilt werden, ohne die Sicherheit des Verfahrens zu gefährden. Durch die eindeutige Zuordnung eines Schlüssels zu einem Teilnehmer sind auch die Forderungen nach Authentizität und Nicht-Bestreitbarkeit erfüllbar.

Nachteile sind die aufwändige Implementierung und die geringe Performance.

Typische Vertreter dieser Gruppe sind RSA und ECC. Asymmetrische Verfahren werden aufgrund der begrenzten Performance praktisch nur für elektronische Signaturen und den Schlüsselaustausch eingesetzt.

1.2.3 Sonstige Verfahren

Aus der Gruppe der sonstigen Verfahren sollen hier nur die Hashfunktionen und Zufallszahlengeneratoren erwähnt werden.

Hashfunktionen werden eingesetzt, um einen kurzen „kryptographischen Fingerabdruck“ eines Datensatzes (z.B. einer Nachricht) zu erzeugen. Realisiert wird das durch eine kollisionsfreie Einwegfunktion. Kollisionsfrei bedeutet dabei, dass unterschiedliche Eingabedaten zu unterschiedlichen Ergebnissen führen müssen; der erzeugte Fingerabdruck lässt nicht auf die ursprünglichen Daten zurückschließen (Einwegfunktion). Beispiele für Hashfunktionen sind RIPEMD160, SHA-1 oder SHA-2 (SHA-256) [1].

Zufallszahlengeneratoren (RNG) erzeugen „kryptographisch nutzbare“ Zufallszahlen. Diese Zufallszahlen müssen insbesondere statistisch zufällig und nicht voraussagbar sein. Im Einsatz sind Hardware-RNG und Pseudo-RNG. Pseudo-RNG werden in Software realisiert und bedürfen einer möglichst zufälligen Initialisierung. Ein häufig eingesetzter Pseudo-RNG ist im Standard FIPS 186-2 definiert [2].

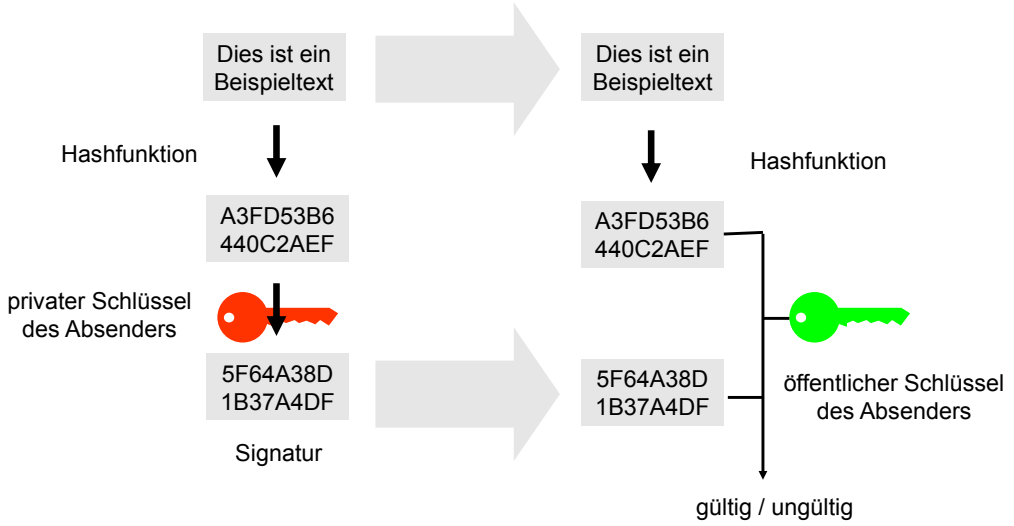


Abbildung 2: Digitale Signatur mit asymmetrischer Kryptographie

1.3 Public Key Infrastruktur (PKI)

Eine Public Key Infrastruktur dient der Verifikation und sicheren Verteilung von öffentlichen Schlüsseln für asymmetrische Verfahren. Eine zentrale Instanz – das TrustCenter (TC) – bietet dazu eine gemeinsame Basis für alle Kommunikationsteilnehmer.

Bild 3 stellt die Abläufe beim Einsatz einer PKI zur Schlüsselverwaltung dar. Das TrustCenter erstellt aus dem öffentlichen Schlüssel des Teilnehmers A zusammen mit einem eindeutigen Identifikationsmerkmal (Name, Adresse) ein Zertifikat und signiert dieses Zertifikat mit seinem privaten Schlüssel. Jeder andere Teilnehmer (hier B benannt) kann die Echtheit des Zertifikates – und damit auch die Echtheit und die Zuordnung des enthaltenen Schlüssels – anhand der Signatur des TC validieren.

Wichtige Voraussetzung für die Nutzung einer PKI ist damit natürlich das Vertrauen aller Teilnehmer in die Integrität des TrustCenters.

2 Signaturverfahren für INSIKA

2.1 RSA

RSA war das erste asymmetrische kryptographische Verfahren. Es wurde im Jahr 1977 durch Ron Rivest, Adi Shamir und Leonard Adleman am MIT entwickelt und ist seit 2000 patentfrei nutzbar. RSA bietet Algorithmen für typische kryptographische Anwendungen wie Signatur und Verschlüsselung, aber kein generisches Verfahren zum Schlüsselaustausch.

RSA basiert auf dem „Problem der Faktorisierung“. Dabei wird genutzt, dass die Multiplikation zweier langer Zahlen (mehr als 100 Dezimalstellen) sehr leicht berechenbar ist, die Umkehroperation – die Zerlegung einer Langzahl (mit mehr als 200 Dezimalstellen) in ihre Primfaktoren – aber nur mit erheblich höherem Aufwand zu leisten ist.

2.2 ECC

Elliptic Curve Cryptography (ECC) wurde im Jahr 1985 „erfunden“ und ist eine heute sehr populäre Alternative zu RSA. ECC bietet Algorithmen für Signatur, Verschlüsselung und Schlüsselaustausch.

ECC basiert auf dem „Problem des Diskreten Logarithmus“. Es nutzt aus, dass eine (modulare) Exponentiation leicht berechenbar ist, die Umkehrung – die Berechnung des „Diskreten Logarithmus“ – aber wesentlich höheren Aufwand erfordert.

2.3 Vergleich RSA – ECC

Für die Erreichung vergleichbarer Sicherheit werden bei ECC wesentlich kürzere Parameter als bei RSA benötigt. Durch die Verwendung kürzerer Parameter ist eine höhere Performance erreichbar. So bietet ECC mit 192 Bit Schlüssellänge eine vergleichbare Sicherheit wie RSA mit 2048 Bit Schlüsseln.

Darüberhinaus skaliert ECC besser als RSA (siehe Bild 4). Die notwendige Schlüssellänge steigt bei ECC linear mit der geforderten Sicherheit, bei RSA jedoch exponentiell, so dass in Zukunft der Vorteil von ECC gegenüber RSA noch größer wird.

Als Beispiele für den Einsatz von ECC seien hier der elektronische Reisepass und der neue Personalausweis genannt.

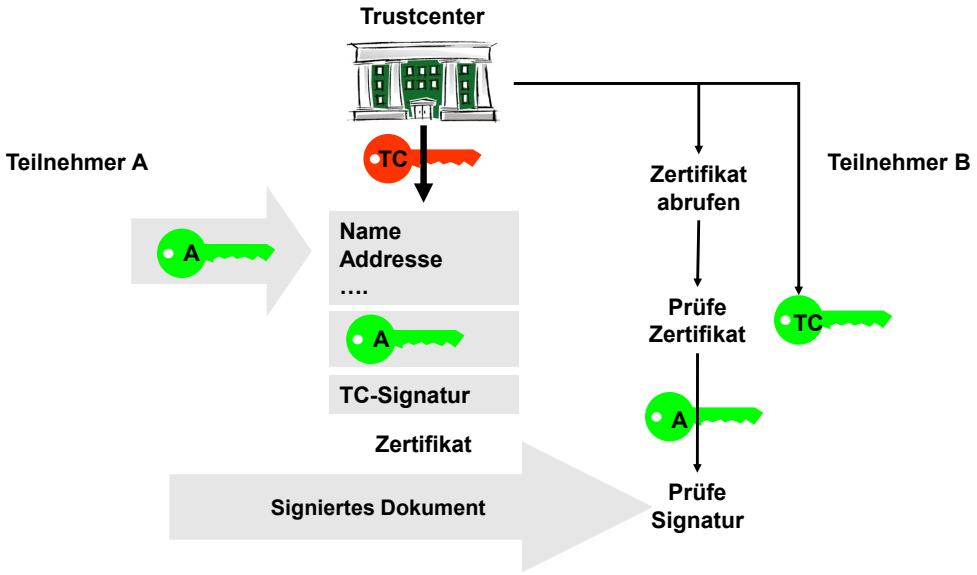


Abbildung 3: Public Key Infrastruktur

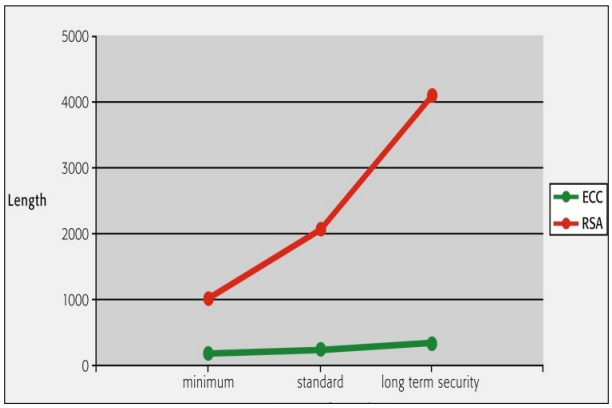


Abbildung 4: Skalierung RSA & ECC

Die Sicherheit einer Signatur steht und fällt mit der verwendeten Schlüssellänge. Die Bundesnetzagentur und das BSI empfehlen für elektronische Signaturen folgende Schlüssellängen:

Tabelle 1: Empfohlene Schlüssellängen (Stand 2012, siehe [3])

	Früher	Heute	Zukunft
RSA	1024 Bit	2048 Bit	4096 Bit
ECC	160 Bit	224 Bit	224 / 256 Bit

2.4 INSIKA nutzt ECC mit 192 Bit

Für die Auswahl des verwendeten Verfahrens für INSIKA waren verschiedenste Aspekte zu berücksichtigen:

Hohe Sicherheit: Für den Einsatz bei INSIKA kommen ausschließlich als sicher anerkannte kryptographische Verfahren in Frage. Da hier lediglich Signaturen verwendet werden, ist ein asymmetrisches Verfahren zu wählen.

Einfache Schlüsselverwaltung: Diese Forderung ist nur durch Verwendung einer PKI erfüllbar; diese wiederum ist nur mit asymmetrischen Verfahren sinnvoll einsetzbar.

Preiswerte Hardware: Für den Einsatz bei INSIKA sollte eine preiswerte und praktikable Lösung gefunden werden. Daher kam die Neuentwicklung eines „Fiskalspeichers“ nicht in Frage. Es gibt zwar sogenannte „Hardware Security Module“ (HSM) zur sicheren digitalen Signatur; diese kosten aber mehrere tausend Euro. Als preiswerte Alternative bietet sich eine Smart Card an.

Einfache Integration in Kassensysteme: Smart Cards lassen sich auch in aktuell verfügbare Kassensysteme mit geringem Aufwand integrieren. Im einfachsten Fall wird dazu lediglich eine serielle Schnittstelle benötigt.

Performance: Die für die Signatur einer Buchung (eines Beleges) verfügbare Zeit liegt bei deutlich unter einer halben Sekunde – sonst wird sie beim Kassiervorgang als störend empfunden. Diese Forderung kann lediglich ECC erfüllen. Bei der verwendeten Smart Card werden mit ECC 192 Bit Signaturzeiten von etwa 160 ms erreicht – bei RSA mit 2048 Bit benötigt eine Signatur etwa 2 Sekunden.

Länge der Signatur: Da die Signatur auf die Belege gedruckt werden soll und für eine Überprüfung

ggf. auch wieder eingetippt werden muss, sollte eine möglichst kurze Signatur verwendet werden.

Aufgrund der Abwägung zwischen Sicherheit und Druckbarkeit wird für INSIKA ECC mit 192 Bit Schlüssellänge verwendet [4]. Eine Änderung ist dabei leicht möglich (siehe 3.7).

3 INSIKA TIM

Die zentrale Instanz zur Absicherung der Umsatzdaten bildet eine Smart Card. Diese Karte – das Tax Identification Module (TIM) – erfüllt mehrere Aufgaben, die sich aber nicht getrennt voneinander realisieren lassen.

3.1 Funktionen des TIM

Hauptaufgabe des TIM ist die Plausibilisierung, Speicherung und Signatur jedes einzelnen Kassenumsatzes. Zusätzlich sorgt das TIM für eine eindeutige Identifikation jeder Buchung und des Steuerpflichtigen.

3.2 Plausibilisierung der Umsatzdaten

Für jede Buchung müssen dem TIM der Umsatz, der Umsatzsteuersatz und der Umsatzsteuerbetrag übergeben werden. Die Übergabe kann als Brutto- oder Nettoumsatz erfolgen.

Zur Plausibilisierung der Umsätze berechnet das TIM aus den übergebenen Daten (Umsatz und Umsatzsteuersatz) den Umsatzsteuerbetrag und bei Brutto-Buchungen zusätzlich den Nettoumsatz. Der errechnete Umsatzsteuerbetrag wird mit dem übergebenen Wert verglichen. Bei Abweichungen wird die Buchung als „ungültig“ abgewiesen. Der (ggf. berechnete) Nettoumsatz und die berechnete Umsatzsteuer werden anschließend zu den gespeicherten Umsatzdaten addiert.

Um die Kumulierung von Rundungsfehlern zu vermeiden, werden alle Währungsbeträge auf zehntausendstel Cent genau berechnet und gespeichert.

Das TIM ist in der Lage, Umsätze getrennt nach verschiedenen Umsatzsteuersätzen – auch mehrere in einer einzigen Buchung – zu verarbeiten. Zusätzlich können mit dem TIM Umsätze im Agenturgeschäft, über Lieferscheine oder Trainingsbuchungen verarbeitet werden.

3.3 Aufzeichnung der Umsatzdaten

Die Umsatzdaten werden auf dem TIM als Summen monatsweise aufgezeichnet. Die Aufzeichnung erfolgt getrennt für verschiedene Umsatzsteuersätze.

Bild 5 stellt den grundsätzlichen Aufbau des Umsatzspeichers auf dem TIM dar. Für jeden Monat werden dort die Umsätze – getrennt nach Umsatzsteuersätzen – gespeichert. Diese Speicher sind mit „Container 1“ bis „Container 6“ bezeichnet. Zusätzlich zu diesen werden getrennte Speicher für Agenturgeschäfte, Lieferschein-Umsätze und Trainingsbuchungen vorgehalten. Diese Umsätze werden vom TIM als „nicht umsatzsteuerrelevant“ behandelt. Die Umsatzsteuer wird in einer – nicht von der Kasse erstellten – Rechnung ausgewiesen.

3.4 Signatur der Umsatzdaten

Nach Plausibilisierung der Umsätze erstellt das TIM eine Signatur für diese Buchung. Dabei werden folgende Daten signiert:

- Datum und Uhrzeit
- ID des Steuerpflichtigen
- ID des Bedieners (z.B. Kellner)
- Buchungsdaten (der Hashwert über alle Positionen einer Buchung)
- Kennzeichen Brutto- / Nettoumsatz
- Kennzeichen Trainingsbuchung
- Eindeutige Sequenznummer
- Umsätze getrennt nach Umsatzsteuersätzen

Dabei ist die ID des Steuerpflichtigen fest auf dem TIM gespeichert. Die Sequenznummer wird für jede Buchung vom TIM selbst erzeugt. Alle anderen Daten werden dem TIM übergeben.

Über diesen Datensatz wird zunächst der Hashwert (Verfahren SHA-1) gebildet und dieser anschließend signiert. Die so erstellte Signatur wird im Kassenjournal gespeichert und auf dem Beleg ausgedruckt.

3.5 Sonstige Funktionen

3.5.1 Identifikation einer Buchung

Zur eindeutigen Identifikation jeder einzelnen Buchung führt das TIM eigenständig eine Sequenznummer. Diese wird bei jeder Signatur erhöht und – von außen unveränderlich – auf dem TIM gespeichert.

3.5.2 Identifikation des Steuerpflichtigen

Jedes TIM wird mit der Umsatzsteuer-Identifikationsnummer des Steuerpflichtigen personalisiert. Dieses Merkmal geht in jede mit dem TIM erstellte Signatur ein.

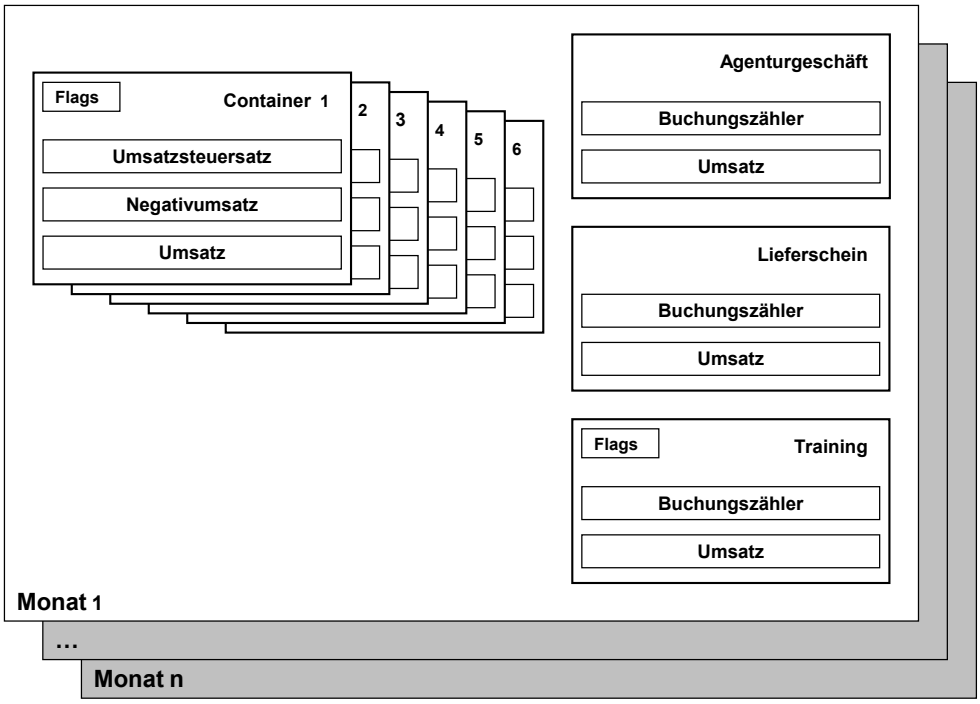


Abbildung 5: Umsatzspeicher des TIM

3.5.3 Reportfunktion

Über die Reportfunktion können Tagesabschlüsse realisiert werden. Jeder Tagesabschluss wird mit einer eindeutigen Sequenznummer versehen und signiert. Dadurch erfordert eine Revision deutlich weniger Aufwand. Weiterhin liefert diese Funktion auf Anfrage monatsgenaue Umsatzsummen.

3.5.4 Umgang mit verschiedenen Steuersätzen

Das TIM ist für die gleichzeitige Verwendung von 6 verschiedenen Umsatzsteuersätzen ausgelegt. Diese Sätze sind aber nicht fest konfiguriert, sondern werden dem TIM mit jeder Buchung von außen neu vorgegeben. Das TIM speichert Umsatzsteuersätze mit in dem zugehörigen Umsatz-Container. Werden in einem Monat verschiedene Steuersätze in einen Umsatz-Container gebucht, so zeichnet das TIM diese Umsatzsteueränderung auf. Bei Revision / Auswertung können (müssen) so gebuchte Speicher dann gesondert behandelt werden.

3.6 Sicherung gegen Manipulationen

Zur Sicherung gegen Manipulationen werden alle Daten auf der Smart Card als „Nur Lesbar“ gespeichert. Lediglich die im TIM realisierten Befehle können diese Daten ändern.

Das verwendete ECC Schlüsselpaar wird auf der Smart Card selbst erzeugt. Der private Schlüssel ist nicht lesbar auf der Smart Card gespeichert. Der öffentliche Schlüssel wird in einem Zertifikat auf dem TIM selbst gespeichert.

Jedes TIM hat eine eindeutige Seriennummer, die schon bei der Produktion des Chips festgelegt wird. Über diese ist ein TIM immer eindeutig identifizierbar.

3.7 Referenzimplementierung des TIM

Die Referenzimplementierung des TIM basiert auf einer Smart Card mit CardOS V4.3b Betriebssystem von Siemens. Die kryptographischen Algorithmen stellt das ECC-Package von cryptovision zur Verfügung.

Die Funktionen des TIM werden durch das INSIKA TIM-Package von cryptovision realisiert. Die Umstellung auf „längere“ ECC-Schlüssel oder das SHA-2 Hashverfahren ist jederzeit mit minimalem Aufwand möglich.

4 Fazit

Mit dem INSIKA Konzept und dem INSIKA TIM wird erstmals eine praxisgerecht einsetzbare Plattform für revisionssichere Kassensysteme geschaffen.

Der Einsatz des kryptographischen Verfahrens ECC bietet eine von anderen Systemen bisher nicht erreichte Sicherheit gegen Manipulationen an Kassenumsätzen.

Die Verwendung der TIM Smart Card ist nicht nur sicher, sondern darüber hinaus kostengünstig und auch für ältere Kassensysteme mit überschaubarem Aufwand zu realisieren.

Literatur

[1] NIST. *FIPS Publication 180-4: Secure Hash Standard (SHS)*. National Institute of Standards und Technology, März 2012. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

[2] NIST. *FIPS Publication 186-2: Digital Signature Standard (DSS)*. National Institute of Standards und Technology, Jan. 2000. URL: http://csrc.nist.gov/publications/PubsFIPSArch.html.

[3] Damien Giry. *Keylength - Cryptographic Key Length Recommendation*. 2012. URL: http://www.keylength.com/ (besucht am 27. 09. 2012).

[4] NIST. *FIPS Publication 186-3: Digital Signature Standard (DSS)*. National Institute of Standards und Technology, Juni 2009. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

INSIKA-Prüfverfahren für Kassenbelege und aufgezeichnete Daten

Jörg Wolff
Physikalisch-Technische Bundesanstalt (PTB)
Abbestraße 2-12, 10587 Berlin
joerg.wolff@ptb.de

Durch Prüfverfahren lässt sich die Integrität und Authentizität von INSIKA-Belegen und -Daten sicherstellen. Eine erfolgreiche Verifikation sichert somit die Zuordnung zum Urheber, die Vollständigkeit der jeweiligen Belege oder Daten und weist nach, dass diese nicht verändert wurden.

Der folgende Beitrag erläutert die Prüfverfahren aus einer technischen Betrachtungsweise. Zunächst wird das INSIKA-System im Überblick dargestellt. Danach werden die Inhalte von Kassenbelegen und aufzuzeichnenden Daten und die sich daraus ergebenen Möglichkeiten der Prüfung vorgestellt. Anschließend wird die durch INSIKA definierte Schnittstelle zum Datenexport dargelegt und abschließend die an der PTB entwickelte Prüfsoftware vorgestellt.

1 INSIKA-Systemüberblick

Bei Verwendung des INSIKA-Systems lassen sich mit elektronischen Registrierkassen und Taxametern aufgezeichnete Vorgänge sicher, schnell und automatisiert prüfen. Die dabei verwendeten Prüfverfahren lassen sich direkt aus dem System ableiten. In diesem Abschnitt soll daher zunächst ein Überblick zum INSIKA-System gegeben werden.

1.1 Nutzergruppen der Prüfverfahren

INSIKA-Prüfverfahren stehen grundsätzlich jedem zur Verfügung. Da die INSIKA-Spezifikationen auf Standards basieren und offen zugänglich sind, können Prüfwerkzeuge von verschiedenen Anbietern erstellt und genutzt werden. Die Nutzer der Prüfverfahren lassen sich in die folgenden Gruppen einteilen:

1.1.1 Unternehmer

Zunächst kann der Kassenbetreiber, also der Unternehmer selbst, jederzeit seine Daten in vollem Umfang einsehen und verifizieren. Somit ist eine Kontrolle von Daten vor einer Herausgabe an Dritte jederzeit problemlos möglich. Bei der Anwendung der Prüfverfahren hat der Urheber – hier also der Unternehmer – in allen Phasen die Rechte an den gesicherten Daten.

Durch die INSIKA-Prüfverfahren bietet sich dem Unternehmer zusätzlich die Möglichkeit, seine Kassen oder Taxameter auch im Innenverhältnis gegenüber den Bedienern abzusichern.

1.1.2 Muttergesellschaften, Dienstleister

Als zweite mögliche Anwender von Prüfverfahren lassen sich Muttergesellschaften oder externe Dienstleister benennen. Hierbei sind verschiedene Konstellationen denkbar, die im Wesentlichen vom Grad der Abhängigkeit der Unternehmen abhängen.

Auch Dienstleister aus den Bereichen IT, Archivierung, Steuerdaten o. ä. können im Auftrag des Unternehmers Prüfaufgaben übernehmen. So werden beispielsweise bei der Anwendung des INSIKA-Systems auf Taxameter die Daten aus dem Fahrzeug an einen Datendienstleister übergeben. Dieser kann im Auftrag des Unternehmers Prüfungen durchführen.

1.1.3 Finanzverwaltungen und Ordnungsbehörden

Finanzverwaltungen und Ordnungsbehörden bilden eine weitere Prüfinstanz. Bei korrekter Anwendung des Systems können diese im Rahmen einer Betriebsprüfung schnell auf gesicherte, herstellerunabhängige

PTB-Bericht IT-18
doi:10.7795/210.20130206a

und automatisiert auswertbare Informationen zurückgreifen.

Das System entspricht den in Deutschland geltenden „Grundsätzen zum Datenzugriff und der Prüfbarkeit digitaler Unterlagen“ [1] und ist konform zum Schreiben „Aufbewahrung digitaler Unterlagen bei Bargeschäften“ des Bundesfinanzministeriums vom November 2010 [2]. Durch die Absicherung von Umsätzen an Registrierkassen und Taxametern und einen einheitlichen Datenexport kann das System erheblich zur Vereinfachung, Beschleunigung und Objektivität von Betriebsprüfungen der Finanzverwaltungen beitragen.

In Branchen, die speziellen Regelungen unterliegen, können zusätzlich Aufsichtsbehörden ein Prüfinteresse besitzen. Ein Beispiel hierfür bilden im Bereich der Taxen die zuständigen Behörden für Konzessionen.

1.1.4 Hersteller von Registrierkassen oder Taxametern

Auch für die Hersteller von Registrierkassen oder Taxametern können sich Vorteile aus der Nutzung von INSIKA-Prüfverfahren ergeben. Zunächst kann jeder Hersteller Prüfverfahren implementieren und dem Kunden als Zusatznutzen anbieten. Bei klaren gesetzlichen Rahmenbedingungen ist es Herstellen von Registrierkassen zudem möglich, nachweisbar gesicherte Systeme anzubieten. Im Gegensatz zu anderen Systemen kann dabei auf den Aufwand und die Innovationsbeschränkung von Bauartzulassungen oder Zertifizierungen verzichtet werden.

Bei Taxametern bleibt die vorgeschriebene Bauartzulassung unverändert verpflichtend, da das INSIKA-System nur auf die Taxameter-Daten angewendet wird, das Gerät selbst aber nicht verändert.

1.2 INSIKA-Systemstruktur

Grundsätzlich ist die INSIKA-Systemstruktur für Registrierkassen und Taxametern durch die Schnittstellenspezifikationen festgelegt. Bei beiden Anwendungen werden Ursprungsdaten mit Hilfe digitaler Signaturen gesichert. Die Signaturen werden dabei durch eine Smartcard erzeugt. Diese Smartcard ist mit einer speziellen Software ausgestattet und wird bei INSIKA als „Tax Identification Module“ (TIM) bezeichnet. Abbildung 1 zeigt die grundlegende Systemstruktur am Beispiel von Registrierkassen.

Die TIM-Schnittstelle spezifiziert das Datenformat und die Kommunikation mit der Smartcard. Die signierten Daten werden in einem einheitlichen Format exportiert, diese Schnittstelle wird XML-

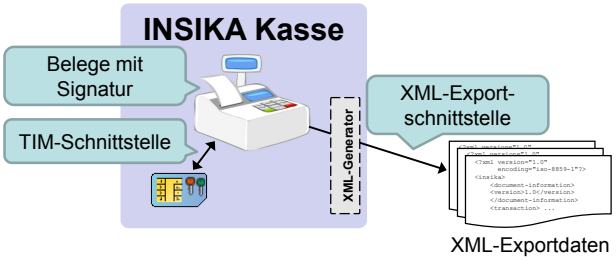


Abbildung 1: INSIKA-Schnittstellen

Exportschnittstelle genannt. Nachfolgend werden diese Schnittstellen detailliert betrachtet.

1.2.1 TIM-Schnittstelle

Über die TIM-Schnittstelle wird die Smartcard an das Kassensystem angebunden. Buchungsdaten werden über diese Schnittstelle von der Kasse an das TIM übergeben und zunächst durch dieses plausibilisiert. Bei positivem Ergebnis wird eine Signatur berechnet und in der Antwort zurückgegeben. Gleichzeitig werden dabei auf dem TIM die entsprechende Sequenznummer und die Summenspeicher aktualisiert. Durch einen sog. Tagesabschluss werden diese Summenspeicher vom TIM signiert ausgegeben.

Die TIM-Schnittstelle ist durch den Standard ISO/IEC 7816 Teil 1-4 in der physikalischen Schicht, sowie in der Sicherungs- und Anwendungsschicht definiert [3–6]. Die für INSIKA nötigen Erweiterungen auf Ebene der Anwendungsschicht sind in der „TIM-Schnittstellendokumentation“ spezifiziert [7, 8]. Das verwendete ECDSA-Signaturverfahren ist z. B. in FIPS186 des NIST definiert [9].

1.2.2 XML-Exportschnittstelle

Um alle Buchungen und Tagesabschlüsse mit den entsprechenden Signaturen abzuspeichern, muss eine INSIKA-Kasse ein Journal führen. Für die Datenspeicherung in diesem Journal bestehen seitens des INSIKA-Systems keine Vorgaben, sie ist also dem Kassenhersteller überlassen. Einzig die Exportdaten müssen aus dem Journal generierbar sein, d. h. die Buchungen und Tagesabschlüsse müssen sich inklusive ihrer Signaturen vollständig zurückgewinnen lassen.

Als Datenformat wird die Auszeichnungssprache XML („Extensible Markup Language“) verwendet. Das Kassensystem selbst muss dabei nicht unbedingt XML-Dateien generieren können. Für diese Aufgabe ist auch ein nachgeschaltetes System in Form eines PC o. ä. nutzbar. In der Abbildung 1 wird dies durch die optional gekennzeichnete Einheit „XML-Generator“

deutlich gemacht. Die XML-Exportschnittstelle ist eine Schnittstelle zum einseitigen Datenexport, deren Struktur und Form durch ein INSIKA-XML-Schema definiert ist [10].

1.2.3 Gedruckte Belege

In Abbildung 1 ist zu erkennen, dass bei Registrierkassen grundsätzlich gedruckte Belege mit Signatur ausgegeben werden. Hauptzweck dieser Belege ist der unmittelbare Nachweis der Signaturerstellung.

1.2.4 Webservice für Taxameterdaten

Auf Grund der besonderen Verhältnisse bei Taxametern und angeschlossenen Quittungsdruckern wurde hierfür eine erweiterte Systemstruktur entworfen. Dabei werden die Daten permanent aus dem Fahrzeug mit Hilfe eines RESTful-Webservice auf einen Server übertragen. Details dieser zusätzlichen Schnittstelle finden sich in der zugehörigen Spezifikation [11].

Die TIM-Schnittstelle und die XML-Exportschnittstelle sind jedoch die selben wie bei Registrierkassen. Damit sind auch die INSIKA-Prüfverfahren für Daten in beiden Anwendungen identisch.

1.3 Prüfbare Daten

Grundsätzlich können im INSIKA-System drei verschiedene Daten zur Prüfung herangezogen werden: XML-Exportdaten, gedruckte Belege und TIM-Daten. Die Prüfung von bereitgestellten XML-Exportdaten stellt den Normalfall dar. Die stichprobenhafte Prüfung von Belegen und die Zuordnung von Belegen zu Exportdaten sollte diese Prüfung untermauern. Das Auswerten der TIM-Daten ist nur als Rückfall gedacht, sofern XML-Exportdaten nicht mehr vorhanden sein sollten.

1.4 Signierte Buchungsdaten

Wie zuvor beschrieben, werden auf dem TIM die Buchungsdaten vor der Signaturberechnung plausibilisiert. Bei positivem Ergebnis sind die Buchungsdaten in Bezug auf Umsatz, Umsatzsteuersatz und Umsatzsteuer rechnerisch richtig. Der Buchungsdatensatz wird durch das TIM signiert und die Signatur wird an die Kasse zurückgegeben. Bei negativem Ergebnis der Plausibilisierung wird vom TIM anstelle der Signatur ein Fehlercode zurückgeben.

In der späteren Betrachtung lassen sich grundsätzlich nur Datenelemente verifizieren, über die die Signatur direkt oder indirekt gebildet wurde. Alle möglicherweise darüber hinaus bereitgestellten Daten haben aus INSIKA-Sicht rein informativen Charakter. Im Rahmen einer Buchung gehen die folgenden Datenelemente in die Signatur ein:

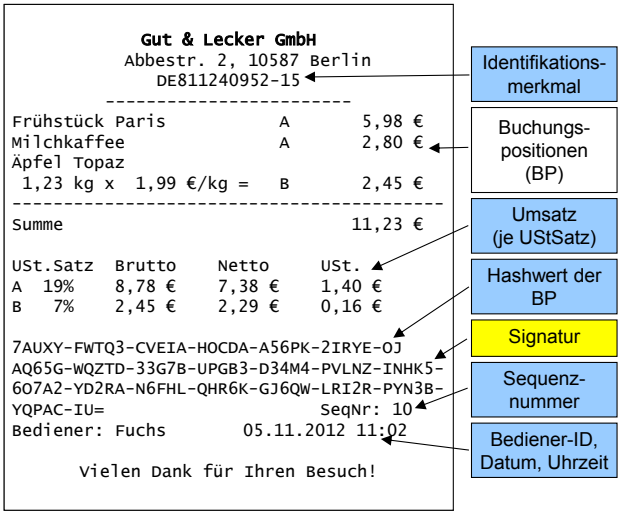


Abbildung 2: INSIKA-Kassenbeleg mit signierten Datenelementen

- Identifikationsmerkmal,
- Umsatz je Umsatzsteuersatz,
- Hashwert der Buchungspositionen,
- Sequenznummer,
- Bediener-Identifikation,
- Datum und
- Uhrzeit.

Diese signierten Datenelemente lassen sich sowohl in den XML-Exportdaten als auch auf dem Beleg wiederfinden. Die Abbildung 2 zeigt dazu beispielhaft einen INSIKA-Beleg. Die signierten Datenelemente sind hierbei blau markiert und werden nun nachfolgend näher erläutert.

1.4.1 Identifikationsmerkmal

Das Identifikationsmerkmal dient der eindeutigen Zuordnung des TIM in Bezug auf die Umsatzsteuer [12]. Da diese Steuer durch Unternehmen abgeführt wird, eignet sich in Deutschland die Wirtschafts-Identifikationsnummer (W-IdNr) als Identifikation. Die W-IdNr ist das Gegenstück zur persönlichen Steuer-Identifikationsnummer und wird wie diese nur einmal vergeben [13].

Bis zur Einführung der W-IdNr kann auch die Umsatzsteuer-Identifikationsnummer (USt-IdNr) verwendet werden. Diese Nummer wird in der gesamten Europäischen Union an Unternehmen eindeutig vergeben. Um die einzelnen TIMs eines Unternehmens direkt identifizieren zu können, wird die W-IdNr bzw.

USt-IdNr um einen Bindestrich und eine forlaufende Zahl erweitert. Alles zusammen bildet dann das Identifikationsmerkmal.

Durch die fortlaufende Zahl kann die Anzahl der TIMs je Unternehmen jederzeit leicht nachvollzogen werden. Dies ist eine wichtige Voraussetzung in der korrekten Anwendung des INSIKA-Systems.

1.4.2 Umsatz je Umsatzsteuersatz

Der Umsatz einer Buchung wird immer aufgeschlüsselt für jeden Umsatzsteuersatz signiert. In einem Buchungsdatensatz können gleichzeitig Umsatzsteueranteile von sechs verschiedenen Umsatzsteuersätzen an das TIM übergeben werden. Im Abschnitt 4.1 wird dies noch näher erläutert.

1.4.3 Hashwert der Buchungspositionen

Vor der Übergabe der Buchungsdaten an das TIM wird über die Buchungspositionen ein Hashwert – also eine Art eindeutiger Fingerabdruck – berechnet. Mit „Hashwert“ wird bei INSIKA ausschließlich das Ergebnis einer kryptografisch sicheren Hashfunktion bezeichnet. Aufgrund der kurzen Ergebnislänge wird in der derzeitigen Spezifikation das SHA-1 Verfahren genutzt [14]. Prinzipiell lassen sich aber auch andere Hashfunktionen festlegen.

Um diesen Hashwert zu berechnen, werden die Buchungspositionen nach einer definierten Vorschrift abgebildet. Da in verschiedenen Einsatzgebieten des Systems unterschiedliche Datenobjekte abgebildet werden müssen, wurden sogenannte „INSIKA-Profile“ definiert. Diese Profile werden nachfolgend im Abschnitt 1.5 erläutert.

Der Hashwert der Buchungspositionen geht direkt in die Signatur ein. Jede nachträgliche Veränderung der Buchungspositionen würde zu einem veränderten Hashwert führen und damit eindeutig erkannt werden.

1.4.4 Sequenznummer

Auch die Sequenznummer ist Teil des signierten Buchungsdatensatzes. Im INSIKA-System wird die Sequenznummer durch das TIM vergeben und fortlaufend mit jeder Signatur inkrementiert. Da die Sequenznummer auf dem TIM gespeichert wird, besitzt diese Nummer einen hohen Grad an Manipulationssicherheit. Die Sequenznummer bildet eine unabhängige Basis, aus der sich die Chronologie von Buchungen und Tagesabschlüssen wiederherstellen lässt.

1.4.5 Bediener-Identifikation, Datum und Uhrzeit

Die Bediener-Identifikation, Datum und Uhrzeit gehen ebenfalls mit in die Signatur ein. Wie nachfolgend noch im Abschnitt 3.5 erläutert wird, werden diese Daten jedoch nur als Zusatzinformationen behandelt und nicht zur Prüfung der Konsistenz oder zur Wiederherstellung der Chronologie genutzt.

1.5 INSIKA-Profile

INSIKA-Profile dienen der Abbildung anwendungsspezifischer Daten eines Systems. Zur Zeit sind Profile für Registrierkassen und für Taxameter spezifiziert.

Ein Profil definiert die Datenobjekte, über die der Hashwert der Buchungspositionen gebildet wird. Wie zuvor im Abschnitt 1.4.3 beschrieben, wird im Rahmen einer Buchung dieser Hashwert zusammen mit den anderen zu signierenden Datenobjekten an das TIM übergeben und dort signiert.

Die Datenobjekte eines Profils, also die Buchungspositionen selbst, werden nicht an das TIM übergeben. Da jedoch der Hashwert dieser Datenobjekte signiert wird, gehen auch diese Datenobjekte indirekt in die Signatur mit ein. Somit können eine große Zahl von Datenobjekten in die Signatur eingehen, ohne dass diese auf der TIM-Schnittstelle übertragen werden müssen. Die Zeit der Datenübertragung und Signaturerstellung ist damit unabhängig von der Anzahl dieser Datenobjekte.

Durch das Konzept der Profile ist es zudem möglich, das INSIKA-System auf unterschiedliche Anwendungen anzupassen. Insbesondere lassen sich hiermit verschiedene messwertverarbeitende Systeme abbilden. Dabei finden sich eine Reihe von Analogien zur Sicherung von Messdaten in verteilten Messsystemen [15]. Bei allen Anpassungen durch Profile kann das Sicherungselement, also das TIM, unverändert bleiben.

1.5.1 Profil Registrierkasse

Dieses Profil ist für die gesamte Bandbreite der Registrierkassen von embedded Plattformen, PC-basierten Point-of-Sale (POS) Systemen bis zu verteilten Kassensystemen nutzbar. Es definiert für jede Buchungsposition die folgenden Datenobjekte:

- Menge/Anzahl,
- Mengeneinheit,
- handelsübliche Bezeichnung,
- Merker (Rabatt, Aufschlag, Gutschein,..),
- Preis je Umsatzsteuersatz

Damit werden auch gemessene Größen aus verbundenen Messgeräten definiert abgebildet. Nach der Zusammenstellung der Buchungspositionen wird über diesen Datensatz dann der Hashwert der Buchungspositionen berechnet. Dies kann in der Kasse oder auch auf dem TIM selbst durchgeführt werden. Weitere Details finden sich in der Spezifikation dieses Profils [7].

1.5.2 Profil Taxameter

Mit dem Profil für Taxameter wurde das INSIKA-System für Taxameterdaten erweitert. Dieses Profil kann für alle Taxameter verwendet werden, deren Bauart nach der Europäischen Messgeräterichtline 2004/22/EG („MID“) geprüft und zugelassen ist [16]. Die Zulassung des Taxameters wird dabei in keiner Weise berührt.

Die Datenobjekte diese Profils basieren auf den in der MID definierten Informationen. Eine Fahrt wird durch eine Buchung abgebildet, die die Datenobjekte aus 1.4 und die folgenden enthält:

- zurückgelegte Strecke,
- Gesamtsumme einer Fahrt je Umsatzsteuersatz,
- Datum Fahrtbeginn,
- Uhrzeit Fahrtbeginn

Auch Schichten (also die An- und Abmeldung des Fahrers am Taxameter) werden abgebildet, sofern das Taxameter dazu in der Lage ist. Detaillierte Informationen finden sich in der Spezifikation des Profils für Taxameter [17].

1.6 Zertifikatsverwaltung

Die INSIKA-Prüfverfahren sind fest in das INSIKA-Gesamtsystem eingebettet. Zum besseren Verständnis soll hier zunächst ein kurzer Überblick zur Zertifikatsverwaltung, der sog. Public-Key Infrastructure (PKI), gegeben werden. Die vereinfachten Instanzen und Abläufe der Zertifikatsverwaltung zeigt die Abbildung 3.

Da das INSIKA-System auf asymmetrischer Kryptographie beruht, lassen sich auch hier mit einem privaten Schlüssel signierte Daten durch den dazugehörigen öffentlichen Schlüssel verifizieren. Das Paar aus privatem und öffentlichem Schlüssel wird vor der Ausgabe des TIM auf diesem generiert. Der private Schlüssel ist dabei nicht lesbar und verlässt das TIM niemals. Der öffentliche Schlüssel wird vor der Ausgabe des TIM ausgelesen und zusammen mit dem Identifikationsmerkmal des Unternehmers in einem Zertifikat abgelegt. In der Abbildung 3 sind schematisch der private und der öffentliche Schlüssel rot bzw. grün eingezeichnet.

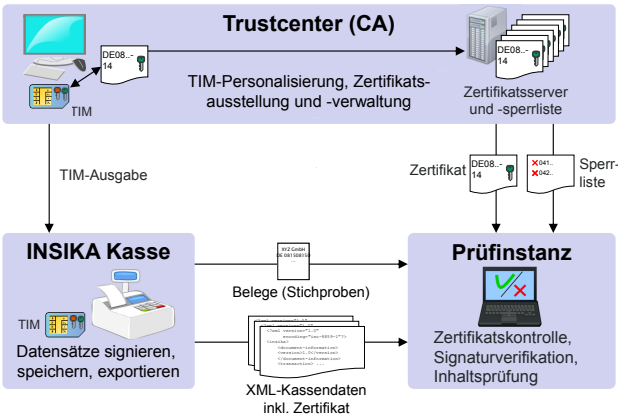


Abbildung 3: Zertifikatsverwaltung (vereinfacht)

Die zuvor genannten Schritte vor der Ausgabe des TIM dienen also der Zuordnung des TIM auf den Unternehmer. Diese sog. Personalisierung wird durch eine zentrale Stelle oder ein privat betriebenes Trustcenter durchgeführt.

Durch das Zertifikat wird die Authentizität, also die eindeutige Zuordnung des TIM und der damit signierten Daten und Belege zu einem Unternehmer, hergestellt. Das Zertifikat findet sich sowohl auf dem TIM als auch auf dem Zertifikatsserver. Die Gültigkeit kann anhand eines Abgleichs mit der Sperrliste („Certificate Revocation List“) überprüft werden. Bei Verlust des TIM, Auflösung des Unternehmens o. ä. kann der Unternehmer das zugehörige Zertifikat auf die Sperrliste setzen lassen. Ab diesem Zeitpunkt können dann keine gültigen Signaturen mehr erzeugt werden. Die Sperrliste und der Zertifikatsserver werden durch die zentrale Stelle bzw. das Trustcenter bereitgehalten und gepflegt.

2 Prüfverfahren für Belege

Die Prüfung gedruckter Kassenbelege kann in zwei unterschiedlichen Tiefen erfolgen. Der übliche Fall ist die Verifikation der Signatur. Dazu werden die unter 1.4 erläuterten signierten Buchungsdaten, die Signatur und der öffentliche Schlüssel benötigt. Durch die Verifikation des Hashwerts der Buchungspositionen lässt sich die Prüfung zusätzlich auf die einzelnen Buchungspositionen ausweiten. Diese Option wird am Ende dieses Abschnitts erläutert.

2.1 Verifikation der Signatur

Wie bereits in der Abbildung 2 dargestellt, können alle signierten Buchungsdaten dem gedruckten Beleg entnommen werden. Bei der Belegverifikation

werden diese Buchungsdaten wieder auf das Format der TIM-Schnittstelle zurückgeführt. Damit wird genau der Datensatz erstellt, der ursprünglich durch das TIM signiert wurde. Zusammen mit der ebenfalls auf dem Beleg gedruckten Signatur und dem öffentlichen Schlüssel des TIM kann dann die Verifikation durchgeführt werden.

Da der öffentliche Schlüssel nicht auf dem Beleg gedruckt wird, muss dieser aus dem Zertifikat gewonnen werden. Anhand des auf dem Beleg gedruckten Identifikationsmerkmals kann auf dem Zertifikatsserver das jeweilige Zertifikat – und damit auch der öffentliche Schlüssel – gefunden werden. Wie in Abbildung 3 gezeigt, kann jede Prüfinstanz auf diesen Zertifikatsserver zugreifen. Die Prüfinstanz kann aber auch lokale Kopien vorhalten, da Zertifikate nur eine geringe Speichergröße besitzen. Die Belegverifikation lässt sich beispielsweise mit der nachfolgend im Abschnitt 5 erläuterten IVM-Software durchführen.

2.2 Zeichenersetzung der Buchungspositionen

Abgesehen von der Bedingung, dass sich ein gedruckter Beleg verifizieren lassen muss, werden durch das INSIKA-System keine Vorgaben in Bezug auf Format, Größe oder Schriftart des Belegs gemacht. Um bei der Zurückgewinnung von gedruckten Texten dennoch robuste Ergebnisse zu erhalten, werden Textfelder vor der Hashwertbildung (und somit vor dem Signieren und vor dem Drucken) einer Zeichenersetzung unterzogen. Hierbei werden besonders fehleranfällige Zeichen und Sonderzeichen weggelassen oder durch ein festgelegtes Zeichen ersetzt [7].

So werden beispielsweise Leerzeichen ausgelassen, da sie sich nicht eindeutig aus gedruckten Belegen zurückgewinnen lassen. Auch Umlaute werden aufgrund ihrer unterschiedlichen Repräsentation in den jeweiligen Zeichensätzen durch ein definiertes Zeichen ersetzt. Diese Zeichenersetzung findet intern als Vorstufe der Hashwertbildung statt und ändert am Ausdruck des Belegs selbstverständlich nichts.

2.3 Format von Hashwert der Buchungspositionen und Signatur

2.3.1 Base32-Kodierung

Der Hashwert der Buchungspositionen und die Signatur müssen auf jedem INSIKA-Beleg gedruckt werden. Um den dazu nötigen Platz auf dem Beleg zu minimieren, wurde in Abbildung 2 eine Base32-Kodierung genutzt [18]. Damit verkürzt sich die Ausdrucklänge gegenüber einem Ausdruck in hexadezimaler Kodierung um ca. ein Fünftel auf 32 bzw. 77 Zeichen. Eine Kodierung in Base64 würde die Ausdrucklänge weiter reduzieren, allerdings sind die dabei verwendeten Groß- und Kleinbuchstaben sehr fehleranfällig in der Erfassung.

Die Base32-Kodierung erlaubt ein gutes Verhältnis zwischen der Ausdrucklänge und der Fehlerrate bei der Rückgewinnung der Daten aus dem gedruckten Beleg. In der Prüfung kann diese Kodierung jederzeit per Bilderkennung, Stift-Scanner oder auch manuell eingelesen werden.

Da jeder alphanumerische Drucker in der Lage ist, die Base32-Kodierung auszugeben, bildet dies eine einfache Möglichkeit zur Integration von INSIKA in bestehende Kassensysteme.

2.3.2 QR-Code

In der Prüfung ergeben sich weitere Vereinfachungen durch die Verwendung von grafischen Codes. Insbesondere bieten sich dafür standardisierte 2D-Codes wie PDF417, Data Matrix oder QR-Code an [19]. Bei Verwendung dieser Codes lassen sich zudem bereits integrierte, leistungsfähige Verfahren zur Fehlererkennung und -korrektur nutzen.

Abbildung 4 zeigt beispielhaft einen Kassenbeleg mit QR-Code. In diesem Code sind die signierten Buchungsdaten und die Signatur enthalten.

Da viele Drucker bereits heute QR-Codes generieren und drucken können, ist die Integration dieser Technik in Kassensysteme in vielen Fällen einfach und kostengünstig.

2.4 Online-Verifikation

Um die Belegprüfung noch weiter zu vereinfachen, sind die Daten des QR-Code in Form einer URL (Uniform Resource Locator) eingebettet. Diese URL[1] kann mit jedem Lesegerät für QR-Codes gelesen und aufgerufen werden. Eine spezielle Software auf dem Lesegerät ist dafür nicht notwendig.

Zur Prüfung wird einfach der QR-Code gescannt und die enthaltene URL aufgerufen. Beim Aufruf werden die signierten Buchungsdaten und die Signatur an einen Verifikationsservice auf dem angegebenen Server übergeben. Auf diesem Server wird mit Hilfe des

[1] Inhalt des QR-Code aus Abbildung 4: `http://insika.de/verify.php?t1=zQQgEhIDzgIXNsYFZnVjaHPHFMDqz775LBLNQF1nA4ak0O_gIfdM4QjYAhY82wIZAOII2AJ3fNsCBwDEEE1OU01LQV9URVNUX1BUQ1fFAQXLAhDLnjBcFrO4vOfzbkRNp-WI8vobRWB9KBMMoHbhhbX5I3XH9u85B_azU7LmA7ZMr-ixSHg=`

```
            Gut & Lecker GmbH
           Abbestr. 2, 10587 Berlin
            INSIKA_TEST_PTBW-5
         ------------------------
Baguette
 2  x  0,89 € =           B        1,78 €
Japan Sencha
 0,12 kg x  49,90 €/kg =  B        5,99 €
Mineralwasser
 2  x  0,69 € =           A        1,38 €
Pfandartik.Einweg
 2  x  0,25 € =           A        0,50 €
Leergut                  A       -0,25 €
----------------------------------------
Summe                                9,40 €

Steuer%  Brutto    Netto     USt.
A  19.0  1,63 €    1,37 €    0,26 €
B  7.00  7,77 €    7,26 €    0,51 €

SeqNr:4299 Bediener:Fuchs 03.12.2012 17:36

      Vielen Dank für Ihren Besuch!
```

Abbildung 4: INSIKA-Kassenbeleg mit QR-Code

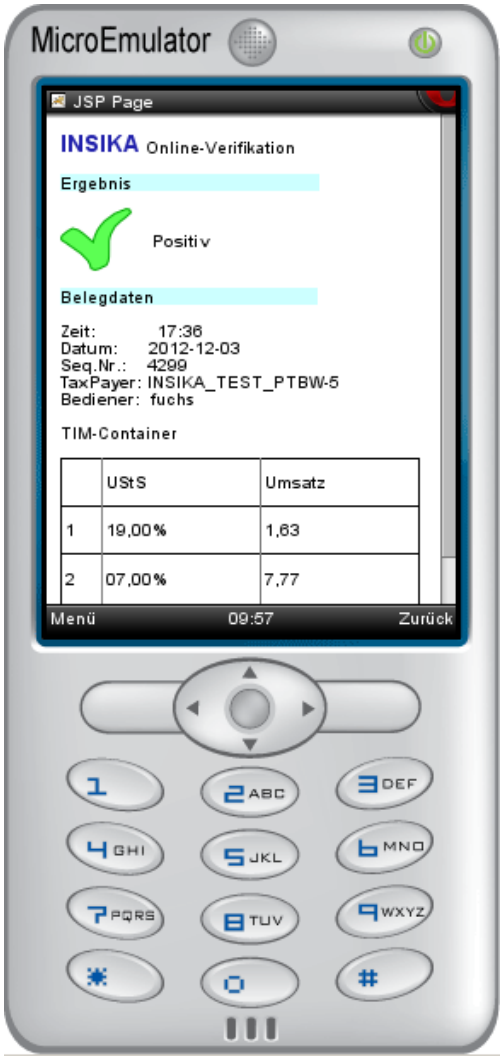


Abbildung 5: Ergebnis der Online-Verifikation des Belegs aus Abbildung 4

Identifikationsmerkmals das Zertifikat vom Zertifikatsserver abgefragt und ein Abgleich mit der aktuellen Sperrliste durchgeführt. Danach wird der öffentliche Schlüssel aus dem Zertifikat ausgelesen. Zusammen mit den signierten Buchungsdaten wird dann auf dem Server die Signatur verifiziert und das Ergebnis auf einer Webseite dargestellt.

Abbildung 5 zeigt das Ergebnis für die erfolgreiche Online-Verfikation des Belegs aus Abbildung 4. Deutlich zu erkennen ist dabei die Übereinstimmung der signierten Inhalte (Sequenznummer, Umsatz, usw) in beiden Abbildungen.

Mittlerweile können eine Vielzahl von Mobiltelefonen, Smartphones oder Handscannern QR-Codes lesen. Sofern diese Geräte einen Zugang zum Internet besitzen, können sie für eine sofortige Belegprüfung genutzt werden. Durch diese Online-Verfikation ist es für jeden Kunden möglich, den Beleg zu prüfen.

Denkbar wäre, dieses Potential mit Hilfe von Anreizsystemen zu nutzen und damit eine sehr hohe Prüfdichte zu erreichen. So könnten Vorgaben zur Anerkennung von Belegen seitens der Finanzverwaltung Anreize schaffen. Auch wäre die Verknüpfung der Online-Verifikation mit Verlosungen vorstellbar.

Sofern gesellschaftlich akzeptiert und datenschutzrechtlich unbedenklich, könnte die Online-Verifikation auch zur Sammlung von Stichproben zur späteren Prüfung mit eingereichten Daten genutzt werden. Nicht nur aus diesem Grund sollte der Service der Online-Verifikation durch eine vertrauenswürdige Instanz und zukünftig auf einem gesicherten Weg bereitgestellt werden.

2.5 Verifikation des Hashwerts der Buchungspositionen

Die Prüftiefe in der Belegprüfung kann weiter erhöht werden, in dem auch die Richtigkeit der auf dem Beleg gedruckten Buchungspositionen kontrolliert wird. Die Buchungspositionen werden durch den gedruckten und signierten Hashwert eindeutig abgebildet. Anhand der gedruckten Buchungspositionen kann nun dieser Hashwert neu berechnet und mit dem gedruckten verglichen werden. Hierzu sind die gleichen Schritte wie bei der Erstellung dieses Hashwerts vor dem Signie-

ren nötig. Bei der Prüfung werden somit zuerst die Buchungspositionen aus dem Beleg erfasst und in einer fest definierten Weise abgebildet. Anschließend werden die Textfelder durch die Zeichenersetzung gewandelt. Stimmt der nun über die Buchungspositionen ermitteltet Hashwert mit dem gedruckten Hashwert überein, sind auch die gedruckten Buchungspositionen korrekt.

3 Prüfverfahren für XML-Exportdaten

Die Prüfung von XML-Exportdaten – also quasi dem Kassenjournal – stellt den üblichen Fall der Prüfung dar. Auf Anfrage der Prüfinstanz stellt der Unternehmer XML-Exportdaten über einen bestimmten Zeitraum bereit. Die Prüfung läuft nun in drei Stufen ab. Auf die Validierung des XML-Formats folgt die Verfikation der Signaturen, worauf schließlich die Prüfung der Inhalte aufsetzt. Diese Prüfschritte und das XML-Format werden nachfolgend genauer erläutert.

3.1 XML zum Datenexport

Die Extensible Markup Language (XML) ist eine Beschreibungssprache, die durch das World-Wide-Web Consortium (W3C) standardisiert wurde [20]. XML wird vor allem zum Datenaustausch zwischen maschinellen Systemen eingesetzt. Im INSIKA-System kann durch die Verwendung von XML der Datenexport einheitlich und herstellerunabhängig definiert werden. Damit erleichtert sich eine Prüfung erheblich. Zudem ist diese Prüfung unabhängig von Ort, Plattform und Medium. Bei der Datenübermittlung können Internet-Protokolle (HTTPS, E-Mail, usw.) oder beliebige Datenträger (USB-Sticks, CD-ROMs, Speicherkarten, usw.) zum Einsatz kommen. Sofern nötig, können XML-Daten meist zu einem hohen Grad komprimiert werden.

Auch eine Wandlung des INSIKA XML-Exportformats entsprechend anderer Vorschriften ist einfach möglich. So wird XML auch im „Standard Audit File – Tax“ (SAF-T) der OECD verwendet. Kassendaten können einen Bestandteil des SAF-T bilden, allerdings werden dabei keine Signaturen verwendet. Daher ist die Verwendung von SAF-T in dieser Form hier zur Zeit nicht zielführend.

3.2 Formate der XML-Exportdaten

XML-Dokumente enthalten ausschließlich Textzeichen und lassen sich daher mit jedem Editor oder Webbrowser darstellen. Die INSIKA-XML-Exportdaten enthalten Zertifikate, Buchungen und Tagesabschlüsse. Es sind zwei Formate definiert, die nachfolgend als „Klartext“ und „Base64“ bezeichnet werden.

In der INSIKA-XML-Variante „Klartext“ sind die Daten in lesbarer Form abgelegt. In der Abbildung 6 ist eine solche XML-Exportdatei beispielhaft für eine Buchung dargestellt. Wie im XML üblich, werden die Informationen als Textzeichen kodiert und zwischen öffnenden und schließenden Bezeichnern („Tags“) abgelegt. Die Tags sind an den Zeichen „<..>“ und „</..>“ zu erkennen und für INSIKA eindeutig definiert. Die Abbildung hierarchischer Ordnungen wird dabei durch Verschachtelung vorgenommen. XML ist hierfür besser geeignet als tabellenorientierte Formate.

Abbildung 4 und 6 zeigen den Beleg und die XML-Daten ein und derselben Buchung. Beim Vergleich ist deutlich zu erkennen, dass alle signaturrelevanten Datenelemente und Buchungspositionen des Belegs auch in der XML-Datei wiederzufinden sind. Beispielhaft sei auf den Umsatz von 7,77 € zum reduzierten Umsatzsteuersatz in Abbildung 4 und den zugehörigen Umsatz in Cent `<turnover>777</turnover>` in Abbildung 6 hingewiesen. Auch die Sequenznummer 4299 findet sich auf dem Beleg und in den zugehörigen Daten.

Die zweite INSIKA-XML-Variante „Base64“ wurde geschaffen, um eine sehr einfache Implementierung des Systems zu ermöglichen. In der Kasse werden dazu die binären Telegramme der TIM-Schnittstelle in beliebiger Form abgelegt. Zum Datenexport werden diese Telegramme in die textbasierte Base64-Kodierung [18] gewandelt und in eine einfache XML-Struktur abgelegt. Diese Lösung eignet sich insbesondere für Kassensysteme die bisher kein Journal führten, stark ressourcenbegrenzte Systeme und für Taxameter.

3.3 Validierung von XML-Dokumenten

Die erste Stufe der Prüfung von XML-Dokumenten ist die Validierung, d. h. die Prüfung auf Struktur und Format. Da die XML-Dokumente von maschinellen Systemen generiert werden, sind Fehler hierbei vorrangig in der Phase der Systemimplementierung oder bei beschädigten Dokumenten zu erwarten.

Zur Validierung wird ein XML-Schema genutzt, dass alle INSIKA-spezifischen XML-Tags, Datentypen und die dazugehörigen Strukturen festlegt [10, 21]. Durch die Validierung kann automatisch die korrekte Bedienung der XML-Exportschnittstelle sichergestellt werden.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<insika xmlns="http://insika.de/export" xmlns:xsi="
    http://www.w3.org/2001/XMLSchema-instance" xsi:
    schemaLocation="http://insika.de/export
    INSIKA_ExportT106-04.xsd">
  <document-information>
    <version>1.0</version>
  </document-information>
  <timParams>
    <timVersion>T.1.1.0</timVersion>
    <tpId>INSIKA_TEST_PTBW</tpId>
    <tpIdNo>5</tpIdNo>
    <itemProfile>1</itemProfile>
    <certificate>MIIC/D ... udlfcWGYyLEdE/Q0Ke
    </certificate>
  </timParams>
  <transaction>
    <date>20121203</date>
    <time>1736</time>
    <operatorId>Fuchs</operatorId>
    <itemList profile="cashRegister">
      <item>
        <qnt>2</qnt>
        <name>Baguette</name>
        <price2>178</price2>
      </item>
      <item>
        <qnt>0.12</qnt>
        <unit>kg</unit>
        <name>Japan Sencha</name>
        <price2>599</price2>
      </item>
      <item>
        <qnt>2</qnt>
        <name>Mineralwasser</name>
        <price1>138</price1>
      </item>
      <item>
        <qnt>2</qnt>
        <name>Pfandartik.Einweg</name>
        <price1>50</price1>
      </item>
      <item>
        <qnt>1</qnt>
        <name>Leergut</name>
        <price1>-25</price1>
      </item>
    </itemList>
    <hashTransactionItems>
    C0EACFBEF92C12CD405D670386A4D0EFE021F74C
    </hashTransactionItems>
    <currency>0978</currency>
    <containerVat1>
      <turnover>163</turnover>
      <turnoverNeg>25</turnoverNeg>
      <vat>26</vat>
      <vatRate>1900</vatRate>
    </containerVat1>
    <containerVat2>
      <turnover>777</turnover>
      <vat>51</vat>
      <vatRate>0700</vatRate>
    </containerVat2>
    <tpId>INSIKA_TEST_PTBW</tpId>
    <tpIdNo>5</tpIdNo>
    <seqNoTransaction>4299</seqNoTransaction>
    <sig>5C16B3B8BF47F36E444DA7E588F2FA1B4560
    7D28130CA076E185B5F92375C7F6EF3907F6B353B
    2E603B64CAFE8B14878</sig>
  </transaction>
</insika>
```

Abbildung 6: „Klartext“-XML-Exportdatei mit der Buchung aus Abbildung 4

3.4 Verifikation der Signaturen

Die Verifikation der Signaturen bildet die nachfolgende Prüfstufe. Bei positivem Ergebnis werden die durch die Signatur gesicherten Daten in Integrität und Authentizität bestätigt. Wie bereits im Abschnitt 1.4 erwähnt, gilt dies nur für die signierten Datenelemente.

Die im Abschnitt 5 nachfolgend beschriebene IVM-Software führt diese Signaturverifikation automatisiert durch. Intern werden dazu die im XML-Dokument enthaltenen Textdaten wieder in das Format auf der TIM-Schnittstelle gewandelt. Zusammen mit den durch das TIM ergänzten Informationen ergibt sich dann der Datensatz, der im TIM signiert wurde. Die Verifikation kann aus diesem Datensatz, dem öffentlichen Schlüssel und der Signatur vorgenommen werden. Im Ergebnis wird die Signatur bestätigt oder als fehlerhaft gekennzeichnet. Durch die Signaturverifikation kann in folgenden Prüfstufen auf vertrauenswürdige Daten zurückgegriffen werden.

3.5 Konsistenz von Exportdaten

Im vorhergehenden Abschnitt wurde gezeigt, wie sich in der Prüfung die Integrität und Authentizität von Exportdaten nachweisen lässt. Aufgrund des Systemkonzepts kann zudem die Konsistenz der erfassten Daten geprüft werden.

Um die Zuverlässigkeit des Systems zu erhöhen, wird die Chronologie von Buchungen und Tagesabschlüssen grundsätzlich nicht durch Datum und Uhrzeit sichergestellt. Wie bereits beschrieben, werden zur chronologischen Ordnung die vom TIM vergebenen Sequenznummern genutzt. Diese sind nicht rücksetzbar und werden mit jeder Signaturvergabe inkrementiert. Dadurch lässt sich die korrekte Reihenfolge von Buchungen und Tagesabschlüssen wiederherstellen. Auch eventuell vorhandene Lücken in den Exportdaten (wie fehlende Buchungen oder Tagesabschlüsse) oder doppelte Datensätze (z. B. durch Bedienungsfehler) sind damit automatisiert auffindbar.

Im INSIKA-System wird eine unbestimmte Anzahl von Buchungen immer durch einen Tagesabschluss abgeschlossen. Der Umsatz zwischen zwei Tagesabschlüssen muss somit auch den Umsatzsummen der eingeschlossenen Buchungen entsprechen. Für die Prüfung heißt das, dass die Signaturverifikation von einzelnen Buchungen unter Einschränkungen entfallen kann. Somit würden nur die Signaturen der Tagesabschlüsse und die Übereinstimmung mit den eingeschlossenen Umsätzen der Buchungen überprüft. Einzig Umsatzverschiebungen zwischen Buchungen ließen sich damit nicht erkennen. Diese Vereinfachung

bietet die Möglichkeit, die Prüfung noch weiter zu beschleunigen.

3.6 Stichproben in Exportdaten

Die grundlegende Voraussetzung für das INSIKA-System ist der zeitnahe Nachweis der Signaturerstellung durch das TIM. Üblicherweise wird dies durch die verpflichtende Ausgabe eines signierten Belegs erfüllt. Jeder Beleg muss sich wiederum in den entsprechenden Exportdaten wiederfinden lassen. Vorhandene Belege können somit nicht nur in ihrer Gültigkeit geprüft werden, sondern bilden auch die Grundlage für Stichproben in den XML-Exportdaten. Anhand dieser Stichproben kann die korrekte und durchgängige Verwendung des TIM überprüft werden. Der Grad ausreichender Sicherheit ist dabei auf der Basis von statistischen Methoden oder Erfahrungswerten durch die Prüfinstanz vorzugeben, und kann hier nicht übergreifend festgelegt werden.

3.7 Inhaltsprüfung von Exportdaten

Die genaue Ausgestaltung der Inhaltsprüfung von Exportdaten wird üblicherweise von der jeweiligen Prüfinstanz vorgegeben. Dabei kann die Prüfung sich auf die Erfassung von Umsätzen beschränken oder auch die Korrelation mit anderen Datenbeständen einbeziehen.

Einige in der Betriebsprüfung genutzte statistische Verfahren (Newcomb-Benford-Analyse und Chi-Quadrat-Test für Tagesgesamtumsätze) werden keine Ergebnisse liefern, da sie der Aufdeckung frei erfundener Werte dienen. Dies kann es bei der Nutzung von INSIKA prinzipiell nicht geben.

Bei Verteilungsanalysen (z. B. Umsatzverteilungen im Tages- oder Wochenverlauf, Vorjahresvergleiche, etc.) wird die Aussagekraft durch INSIKA wesentlich erhöht. Vor allem führt die zeitweise Nichterfassung von Daten mit diesen Analyseverfahren zu Auffälligkeiten.

Die Anwendung der genannten Verfahren auf ungesicherte Daten kann auf Dauer keine zuverlässige Aufdeckung von Manipulationen mehr erlauben. Da die Verfahren bekannt sind, kann mit Hilfe von intelligenter Manipulationssoftware (sog. „Zapper“) der Datenbestand so verändert werden, dass statistische Methoden keine Manipulation mehr aufdecken können. Nur bei einer gesicherten Ursprungsaufzeichnung, wie sie bei INSIKA verwendet wird, kann jede nachträgliche Veränderung sofort erkannt werden.

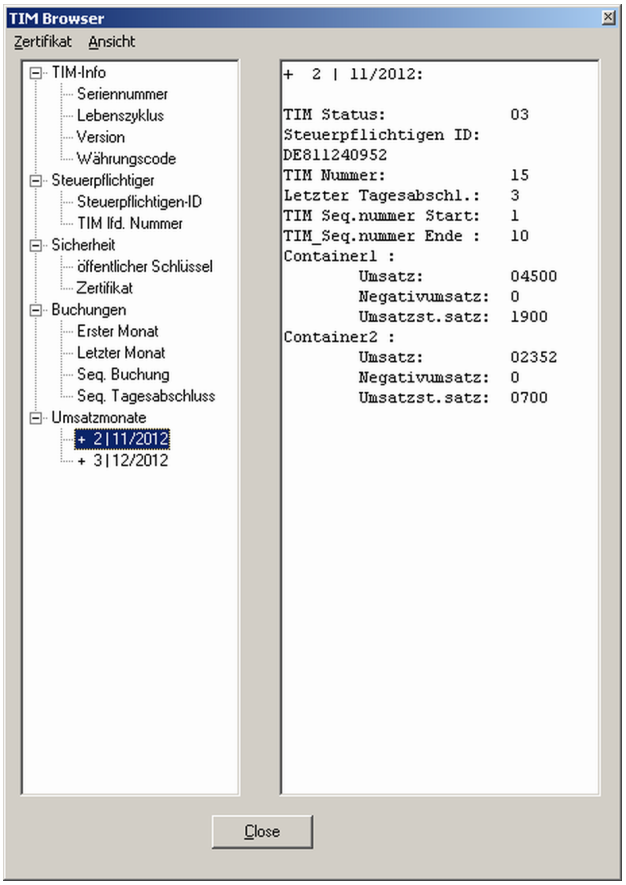


Abbildung 7: TIM-Browser

4 Auswertung von TIM-Daten

Die Auswertung der TIM-Daten kann als Sonderfall der Prüfung angesehen werden. Nur für den Fall, dass keine Exportdaten vorgelegt werden können, ist die Auswertung der TIM-Daten sinnvoll. Da die auf dem TIM gespeicherten Daten mit jedem Tagesabschluss ausgegeben werden, kann auch jeder Unternehmer diese problemlos einsehen.

4.1 Umsatzspeichermodell des TIM

Auf dem TIM werden die Umsätze in Monatssummen für jeweils sechs verschiedene Umsatzsteuerklassen gespeichert. Mit einer Buchung ließen sich somit sechs unterschiedliche Umsatzsteuersätze übertragen. Der jeweilige Umsatzsteuersatz ist dabei auf dem TIM nicht in der Höhe, sondern in der Klasse festgelegt. Für Deutschland bilden der Standardsatz, der ermäßigte Satz und die Umsatzsteuerbefreiung die üblichen Klassen [12].

Die Höhe der Umsatzsteuersätze wird erst mit einer Buchung in den entsprechenden Monatssummenspeicher eingetragen. Änderungen der Umsatzsteuersätze erfordern damit keine Änderungen auf dem

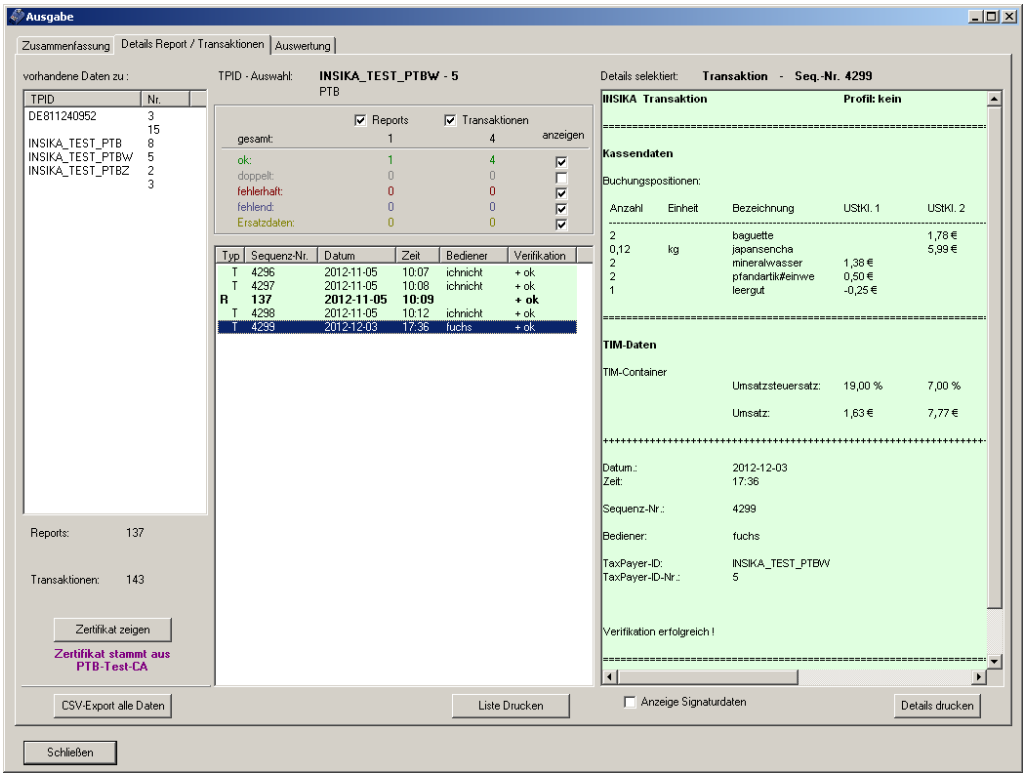


Abbildung 8: Verifikation von XML-Exportdaten mit der IVM-Software

TIM und können im laufenden Betrieb vorgenommen werden. Durch das System der sechs Umsatzsteuerklassen lassen sich zudem alle Umsatzsteuersysteme der Europäischen Union abbilden [22].

4.2 TIM-Browser

Zur Auswertung der TIM-Daten kann z. B. der an der PTB entwickelte „TIM-Browser“ genutzt werden. Wie Abbildung 7 zeigt, kann mit dieser Applikation der Inhalt des TIM ausgelesen werden. Auch lassen sich die entsprechenden Umsatzsummen ermitteln, anhand derer sich eine Abschätzung von Monatsumsätzen durchführen lässt. In einem möglichen Streitfall zwischen Unternehmer und Prüfinstanz bietet sich damit eine Grundlage zur Einigung.

5 IVM-Verifikationssoftware

An der PTB wurde im Rahmen des INSIKA-Projekts beispielhaft die Software „INSIKA Verifikations Module“ (IVM) entwickelt. Mit dieser Software lassen sich Signaturen sowohl von XML-Exportdaten als auch von gedruckten Belegen verifizieren. Bei letzteren lässt sich zusätzlich die Übereinstimmung von Buchungspositionen und Hashwert eines gedruckten Belegs prüfen (siehe 2.5). Damit steht mit dem IVM ein Werkzeug zur Verfügung, das alle INSIKA-Prüfverfahren für Belege und XML-Exportdaten abdeckt.

Neben einer eigenständigen Applikation wie dem IVM kann natürlich auch eine webbasierte Architektur zur Prüfung von XML-Exportdaten entworfen werden. Je nach Anforderung kann dabei die Signaturverifikation auf dem Server oder auf dem Client durchgeführt werden. Auch bei einer webbasierten Architektur kommt natürlich der Vertrauenswürdigkeit des Anbieters eine besondere Bedeutung zu.

5.1 IVM zur Prüfung von XML-Exportdaten

Abbildung 8 zeigt das IVM mit der Prüfung von einigen XML-Exportdaten. Enthalten sind u. a. Daten aus dem Beispiel in Abbildung 6. Die dreispaltige Ansicht zeigt das Identifikationsmerkmal, Buchungen und Tagesabschlüsse und die dazugehörigen detaillierten Inhalte. Die Ergebnisse der jeweiligen Signaturverifikation sind farbig hinterlegt. Damit stehen die Ergebnisse im Vordergrund und möglichen Fehlern lässt sich auf einfache Weise nachgehen.

Über den Export der Daten als „CSV“ stellt das IVM auch Daten für das Programmpaket „IDEA“ bereit. Diese Software dient der Datenanalyse und wird bundeseinheitlich von der deutschen Finanzverwaltung im Bereich der Betriebsprüfung verwendet [23].

5.2 IVM zur Prüfung der Zertifikatskette

Im IVM ist auch die Abfrage vom Zertifikatsserver, die Zertifikatsprüfung und der Abgleich mit der Zertifikatssperrliste integriert. Abbildung 9 zeigt beispielhaft die Verifikation der Zertifikatskette. Damit kann der Ursprung der Daten eindeutig zugeordnet werden. Die Prüfung der Zertifikatskette wird im IVM selbstverständlich automatisch durchgeführt.

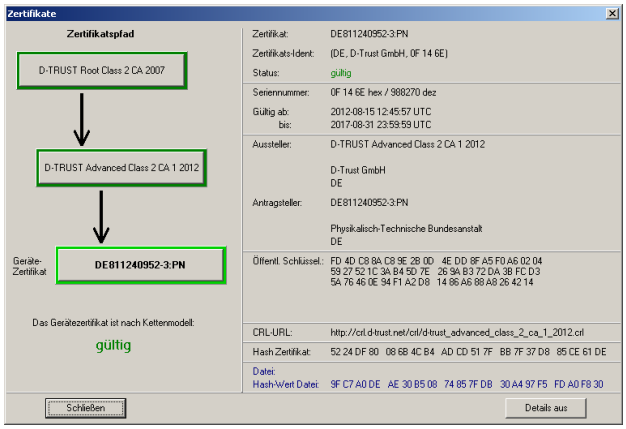


Abbildung 9: Verifikation der Zertifikatskette im IVM

6 Zusammenfassung

Im INSIKA-Konzept werden Daten an Registrierkassen und Taxametern mit Hilfe einer Smartcard gesichert. Mit Prüfverfahren können alle Veränderungen an diesen Daten sicher, schnell und automatisiert erkannt werden. Die Prüfverfahren lassen sich direkt aus dem Systemkonzept ableiten und stehen jedem frei zur Verfügung. Da das Konzept und die Spezifikationen offen zugänglich sind, können Prüfwerkzeuge von verschiedenen Anbietern bereitgestellt werden.

Im INSIKA-System lassen sich Exportdaten, gedruckte Belege und auf dem TIM gespeicherte Umsatzsummen prüfen. Den Kern der Prüfung stellt dabei die Signaturverifikation von Exportdaten und Belegen dar. Durch eine erfolgreiche Signaturverifikation wird die Integrität und Authentizität der geschützten Daten sichergestellt.

Die Konsistenz von Exportdaten lässt sich anhand der Sequenznummern nachweisen. Die Exportdaten sind durch das XML-Format einheitlich und unabhängig von Medium und Hersteller definiert. Umsatzanalysen oder weitergehende Methoden der Datenauswertung können auf gesicherte Exportdaten zurückgreifen.

Gedruckte Belege dienen nicht nur dem zeitnahen Funktionsnachweis des Systems, sie können auch zu Stichproben in den korrespondierenden Exportdaten herangezogen werden. Bei der Verwendung von 2D-Codes auf den Belegen kann die Online-Verifikation jederzeit mit vielen Mobiltelefonen und Smartphones durchgeführt werden, ohne dass dafür eine spezielle Software benötigt wird. Da die Online-Verifikation damit prinzipiell von jedem Kunden durchgeführt werden kann, könnte eine sehr hohe Prüfdichte erreicht werden.

Literatur

[1] BMF. *BMF-Schreiben vom 16. Juli 2001 - IV D 2 - S 0316 - 136/01 - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Juli 2001. URL: `http://bundesfinanzministerium.de/`.

[2] BMF. *BMF-Schreiben vom 26.11.2010 - IV A 4 - S 0316/08/10004-07 - (2010/0946087) - Aufbewahrung digitaler Unterlagen bei Bargeschäften*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Nov. 2010. URL: `http://bundesfinanzministerium.de/`.

[3] ISO. *ISO/IEC 7816-1:1998 Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics*. International Organization for Standardization, 1998.

[4] ISO. *ISO/IEC 7816-2:1999 Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimensions and location of the contacts*. International Organization for Standardization, 1999.

[5] ISO. *ISO/IEC 7816-3:1997 Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols*. International Organization for Standardization, 1997.

[6] ISO. *ISO/IEC 7816-4:1995 Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange*. International Organization for Standardization, 1995.

[7] INSIKA-Projekt. *INSIKA TIM Schnittstellendokumentation*. Version T.1.0.6-02. Physikalisch-Technische Bundesanstalt, März 2010. URL: `http://insika.de/`.

[8] INSIKA-Projekt. *INSIKA TIM Schnittstellendokumentation, Zusatz*. Version T.1.1.0-01. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: `http://insika.de/`.

[9] NIST. *FIPS Publication 186-3: Digital Signature Standard (DSS)*. National Institute of Standards und Technology, Juni 2009. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

[10] INSIKA-Projekt. *INSIKA Exportformat*. Version T.1.0.6-01. Physikalisch-Technische Bundesanstalt, März 2010. URL: http://insika.de/.

[11] INSIKA-Projekt. *RESTful INSIKA Interface. Schnittstelle zur Übertragung von signierten Fahrt- und Schichtdaten*. Version 0.13.5. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: http://insika.de/.

[12] BMJ. *Umsatzsteuergesetz (UStG)*. Version 07.12.2011. Bundesrepublik Deutschland, Bundesministerium der Justiz, Dez. 2011. URL: http://www.gesetze-im-internet.de/ustg_1980/index.html.

[13] BMJ. *Abgabenordnung*. Version 22.12.2011. Bundesrepublik Deutschland, Bundesministerium der Justiz, Dez. 2011. URL: http://www.gesetze-im-internet.de/ao_1977/index.html.

[14] NIST. *FIPS Publication 180-4: Secure Hash Standard (SHS)*. National Institute of Standards und Technology, März 2012. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

[15] Jörg Wolff u. a. »Sicherung von Messdaten in verteilten Messsystemen«. In: *Verteilte Messsysteme*. Hrsg. von F. Puente León, K.-D. Sommer und M. Heizmann. KIT Scientific Publishing, Karlsruhe, März 2010, S. 193–205. ISBN: 978-3-86644-476-8. DOI: 10.5445/KSP/1000015670.

[16] Rat der Europäischen Union. *Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte*. Amtsblatt der Europäischen Union L135 vom 30.04.2004. März 2004. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0022:DE:NOT.

[17] INSIKA-Projekt. *INSIKA Profil Taxameter*. Version T.1.1.0-10. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: http://insika.de/.

[18] S. Josefsson. *RFC4648: The Base16, Base32, and Base64 Data Encodings*. The Internet Engineering Task Force (IETF), Okt. 2006. URL: http://tools.ietf.org/html/rfc4648.

[19] ISO. *ISO/IEC 18004:2006 Information technology - Automatic identification and data capture techniques - QR Code 2005 bar code symbology specification*. International Organization for Standardization, 2006.

[20] *Extensible Markup Language (XML) 1.0 (Fifth Edition). W3C Recommendation 26 November 2008*. World Wide Web Consortium (W3C). Nov. 2008. URL: http://www.w3.org/TR/xml/ (besucht am 24. 04. 2012).

[21] *XML Schema Part 0: Primer Second Edition. W3C Recommendation 28 October 2004*. World Wide Web Consortium (W3C). Okt. 2004. URL: http://www.w3.org/TR/ (besucht am 24. 04. 2012).

[22] Rat der Europäischen Union. *Richtlinie 2006/112/EG des Rates vom 28. November 2006 über das gemeinsame Mehrwertsteuersystem*. Amtsblatt der Europäischen Union L347 vom 11.12.2006. Dez. 2006. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0112:DE:NOT.

[23] BMF. *Information zum „Beschreibungsstandard für die Datenträgerüberlassung“*. Version 15.08.2002. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Aug. 2002. URL: http://bundesfinanzministerium.de/.

Erfahrungen bei der Implementierung des INSIKA-Systems in proprietären und PC-basierten Registrierkassen

Jens Reckendorf
Vectron Systems AG
Willy-Brandt-Weg 41, 48155 Münster
jreckendorf@vectron.de

In diesem Beitrag werden die Erfahrungen der Vectron Systems AG, eines Herstellers von Kassensystemen, mit der ersten durchgeführten vollständigen Integration der INSIKA-Lösung in proprietäre und PC-basierte Kassensysteme sowie Ergebnisse von Praxistests beschrieben. Es werden die wesentlichen technischen Änderungen an Hard- und Software und die aufgetretenen Probleme sowie deren Lösungen vorgestellt. Es wird eine Übersicht über den Entwicklungsaufwand gegeben und es werden die wesentlichen Erfahrungen zusammengefasst. Dabei werden auch Hinweise zur Übertragbarkeit dieser Erkenntnisse auf andere Hersteller gegeben.

1 Ausgangssituation

1.1 Unternehmen Vectron

Vectron ist ein deutscher Hersteller von Kassensystemen (bestehend aus Hard- und Software) und Backoffice-Software zur Steuerung dieser Systeme. Das Unternehmen besteht seit 1990 und erwirtschaftete im Jahr 2011 mit ca. 120 Mitarbeitern einen Umsatz von etwa € 22,5 Mio.

Vectron tritt seit 1996 als Anbieter von Kassensystemen auf und hat seitdem über 125.000 Systeme ausgeliefert. Die Produktpalette von Vectron umfasst proprietäre und PC-basierte Kassensysteme. Es werden stationäre und mobile Systeme angeboten. Die nicht-PC-basierten Systeme stammen aus eigener Entwicklung und Fertigung.

Vectron deckt mit den Kassensystemen verschiedene Branchen ab. Schwerpunktmäßig werden sie in der Gastronomie und in Bäckereiketten eingesetzt. Des Weiteren verfügt Vectron auch über Lösungen für den Einzelhandel – diese Branche steht jedoch nicht im Fokus.

Die wichtigste Vertriebsregion ist Deutschland mit einem Anteil von gut 60 %. Weitere wichtige Märkte sind die Niederlande, Frankreich, Spanien, Schweiz und Österreich. Insgesamt wird in über 20 Länder exportiert. Vectron ist auch in Ländern mit klassischen Fiskalspeichersystemen tätig, z. B. in der Türkei.

Abbildung 1 zeigt eine Übersicht der Vectron-POS-Kassensysteme. Weitere Details sind auf der Website des Unternehmens zu finden [1].

1.2 Teilnahme am INSIKA-Projekt

Vectron ist eines der Partnerunternehmen im MNPQ-Projekt „INSIKA“ der PTB. Dies geht zurück auf die Kontaktaufnahme des BMF im Jahr 2002, als eine Reihe von Herstellern angesprochen wurden, um das Problem von Datenmanipulationen an Kassensystemen näher zu untersuchen und Lösungsideen zu deren Verhinderung zu erarbeiten.

Die Hauptmotivation für das Engagement von Vectron lag darin, technisch sinnvolle Lösungen mitzugestalten. Diese sollen – z. B. im Gegensatz zu klassischen Fiskalspeicherlösungen – preiswert sein und die technische Weiterentwicklung nicht behindern.

Folgende eigene Entwicklungen wurden von Vectron im Zusammenhang mit dem INSIKA-Projekt durchgeführt:

- Prototyp, um die generelle Machbarkeit zu zeigen (unter Nutzung einer handelsüblichen Signaturkarte)

PTB-Bericht IT-18
doi:10.7795/210.20130206a

Abbildung 1: Übersicht der Vectron-POS-Kassensysteme

- Praxistaugliche Integration des Smartcard-Prototypen („TIM“) in Vectron-Produkte (in diesem Beitrag vorgestellt)
- Erprobung in der Praxis

2 Aufgaben und Lösungen

2.1 Grundsätzlich zu lösende Aufgaben

Die nötigen Anpassungen eines Kassensystems zur Umsetzung des INSIKA-Konzepts dürften nach bisherigen Erfahrungen im Wesentlichen immer identisch sein. Sie lassen sich wie folgt aufteilen:

- Integration TIM:
  - Mechanische und elektrische Integration (Smartcardleser)
  - Kommunikation mit dem TIM (Low-Level-Software)
- Software Kasse:
  - Anpassung verschiedener Abläufe in der Software
  - Speicherung der Journaldaten
- Software Backoffice:
  - Übertragung und Weiterverarbeitung der Journaldaten
  - Export der Daten

2.2 Aufbau

Die grundsätzlichen Abläufe lassen sich anhand der Abbildung 2 nachvollziehen. Im Registriervorgang kommuniziert das Kassensystem mit dem TIM, um Buchungen signieren zu lassen. Diese werden als Beleg mit einigen Zusatzinformationen gedruckt. Alle Buchungen werden in der Kasse gespeichert, um die spätere Weiterverarbeitung zu ermöglichen. In der vorgestellten Lösung erfolgt die Weiterverarbeitung durch Übertragung in ein Backoffice-System. Dort werden die Daten mehrerer Kassenplätze gespeichert, verwaltet und auf Anforderung in das festgelegte Exportformat konvertiert.

2.3 Kartenleser

Jedes Kassensystem, das nach dem INSIKA-Konzept arbeitet, muss über eine Schnittstelle zum TIM verfügen. Diese wird hier vereinfachend „Kartenleser“ genannt.

Smartcards sind mechanisch, elektrisch und in Bezug auf die Software weitgehend genormt (in der Normenfamilie ISO 7816), so dass grundsätzlich nur geringe Schwierigkeiten bei der Integration und kaum Kompatibilitätsprobleme zu erwarten sind. Aufgrund der Standardisierung sind fertige Hardware und Software sowie entsprechende Komponenten verfügbar. Neben dem „Scheckkartenformat“ ID-1 gibt es Smartcards im

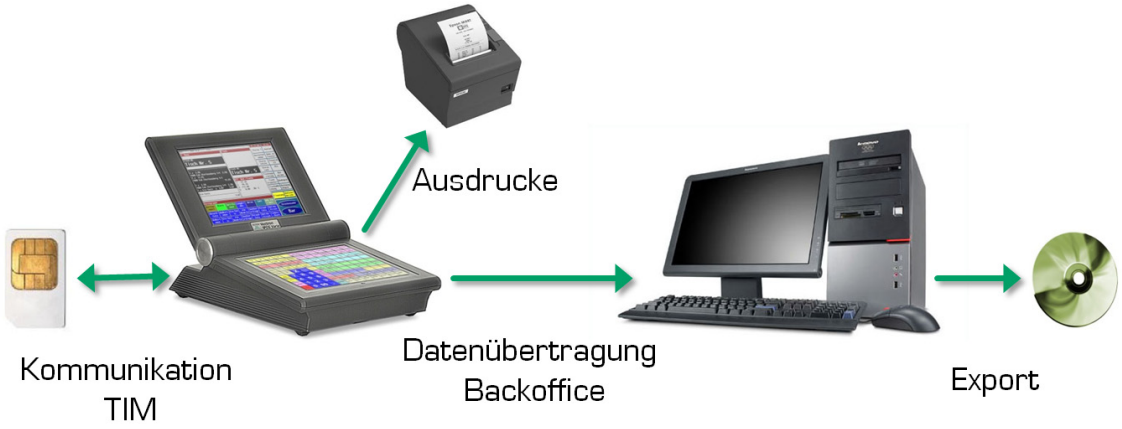


Abbildung 2: Schematischer Aufbau des Gesamtsystems

ID-000-Format (wird z. B. bei Mobilfunk-SIM-Karten verwendet), das ideal für eine direkte Integration des TIM in Handhelds geeignet ist.

Je nach technischer Plattform des Kassensystems und abhängig von Stückzahl- und Kostenbetrachtungen ist der Einsatz von unterschiedlichen Kartenlesern möglich:

- Für Geräte auf PC-Basis können handelsübliche Standard-Kartenleser (z. Zt. vor allem mit USB-Schnittstelle) eingesetzt werden.
- Speziell bei nicht-PC-basierten Systemen bietet sich ein integrierter Kartenleser an. Durch Verwendung eines speziellen Controllers mit entsprechender Firmware (hier wurde ein Atmel AT83C21GC verwendet) ist die Ansteuerung der Smartcards über eine serielle Schnittstelle mit einem einfachen Protokoll möglich.
- Zur Minimierung der Stückkosten ist auch eine direkte Ansteuerung der Smartcard per Microcontroller möglich. In diesem Fall müssen u. a. das Timing der verwendeten Schnittstelle und das Transportprotokoll selbst implementiert werden.

Bei der Implementierung des INSIKA-Systems in die Vectron-Kassensysteme wurden zwei verschiedene Kartenleser eingesetzt.

Abbildung 3 zeigt eine Erweiterungsplatine für die proprietären Vectron-Kassensysteme, die neben dem eigentlich Kartenleser (bestehend aus Controller, Quarz, Kartenhalter und einigen wenigen passiven Bauteilen – im Bild eingerahmt), einen Schnittstellenbaustein sowie eine Speichererweiterung beinhaltet. Die Komponenten des Kartenlesers wurden zudem auch problemlos in mobile Kassensysteme integriert.

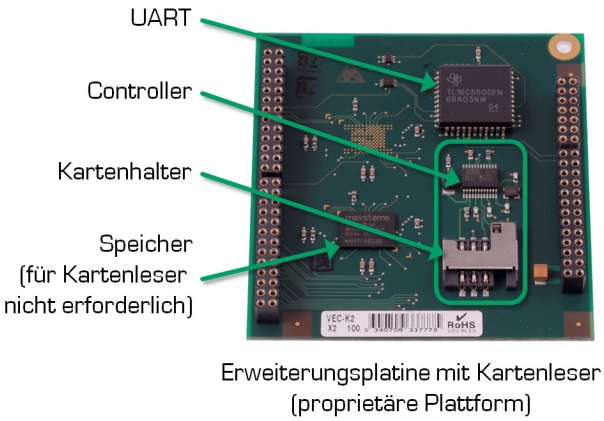


Abbildung 3: Kartenleser für proprietäre Systeme

Abbildung 4 zeigt einen handelsüblichen Kartenleser mit USB-Schnittstelle, wie er für die Integration des TIM in ein PC-basiertes Kassensystem genutzt wurde.

2.4 Transportprotokoll

Die Kommunikation zwischen dem Host (also dem Kassensystem) und der Smartcard folgt einem klaren Master-Slave-Prinzip. Die Karte antwortet also grundsätzlich nur auf Befehle des Hosts.

Es wird ein Transportprotokoll verwendet, das Übertragungsfehler erkennt und wenn möglich (durch Wiederholung der Übertragung) korrigiert. Bei Verwendung fertiger Komponenten (Kartenleser bzw. Controller) ist dieses Protokoll bereits implementiert.

Zwischen Host und Karte werden sog. APDUs („Application Protocol Data Units“) übertragen. Sowohl Befehle für die Karte als auch Antworten von der Karte sind immer APDUs. Bei APDUs handelt es sich um präzise definierte Datensatzstrukturen mit teilweise vordefinierten und teilweise anwendungsspe-

Abbildung 4: Kartenleser für PC-Systeme

zifischen Datenfeldern. Inhalte werden größtenteils als TLV-Strukturen („Tag, Length, Value“) codiert. Für eine Einführung in die Materie siehe z. B. [2].

2.5 Signaturerstellung

Zur korrekten Erstellung der Signatur muss der Registrierablauf entsprechend erweitert werden. Im Wesentlichen erfordert dies folgende Schritte:

- Aufbereitung der Daten des Belegs
- Errechnen eines Hashwertes (zum SHA-1-Algorithmus siehe [3]) aus den entsprechend der INSIKA-Spezifikation aufbereiteten Positionsdaten
- Berechnung von Summen für Steuern, Agenturumsatz, Lieferscheine
- Generierung der APDU
- Kommunikation mit dem TIM
- Auswerten der Antwort-APDU
- Speichern der Rückmeldungen
- Ausdrucken der relevanten Daten
- Bei Bedarf Fehlerbehandlung

Die Signaturerstellung im TIM dauert ca. 300 Millisekunden. Diese Zeit ist nach bisherigen praktischen Erfahrungen unkritisch, da sie vom Anwender nur als geringe, nicht störende Verzögerung wahrgenommen wird. Trotzdem sollte bei der Implementierung darauf geachtet werden, dass die Kommunikation so weit wie möglich optimiert wird. Dazu bieten sich folgende Punkte an (je nach Struktur der Software und Leistungsfähigkeit der Hardware):

- Nutzung der maximal möglichen Übertragungsgeschwindigkeiten zum TIM
- Minimierung der Größe der APDUs, die zum TIM übertragen werden – dazu sind entsprechende Nullunterdrückungen definiert worden
- Berechnung signaturrelevanter Daten während des Registriervorgangs
- Kommunikation mit dem TIM parallel zum Druckvorgang

2.6 Einschränkungen für gedruckte Belege

Ein wichtiges Element des INSIKA-Systems ist die Tatsache, dass die Signatur auf Ausdrucken verifizierbar sein muss, und zwar ohne Rückgriff auf die elektronisch aufgezeichnete Transaktion.

Dazu müssen alle relevanten Daten auf dem Ausdruck enthalten sein und genau der signierten Form entsprechen. Einige konkrete Beispiele:

- Der Artikeltext darf im Ausdruck nicht gegenüber dem Text, der für die Ermittlung des Hashwertes der Buchungspositionen genutzt wird, gekürzt werden.
- Agenturumsätze müssen pro Position einzeln erkennbar sein.
- Wenn in einer Buchungsposition gemischte Steuersätze auftreten, müssen diese betragsmäßig eindeutig aus dem gedruckten Beleg heraus ermittelbar sein.

2.7 Speicherung der Journaldaten

Das INSIKA-Konzept erfordert zwingend die Aufzeichnung aller Buchungen im Detail. Für jeden Kassenbeleg werden also alle Positionen sowie die wesentlichen Summenwerte erfasst. Nach aktueller Rechtslage (BMF-Schreiben vom 26.11.2010 [4]) ist das bereits jetzt erforderlich, wird aber in der Praxis trotzdem oft noch nicht umgesetzt.

Alle Transaktionen und Tagesabschlüsse müssen als „elektronisches Journal“ gespeichert werden. Bei einigen Systemen ist dieses evtl. noch gar nicht vorhanden oder technisch nicht geeignet. Gründe dafür können sein, dass es nicht flexibel genug ist, um zusätzliche Datensätze wie Signaturen abzuspeichern oder weil Daten wie Artikelbezeichnungen nur als Referenz auf einen Stammdatensatz gespeichert werden.

Je nachdem über welche Speicherkapazität ein bestehendes System verfügt und über welchen Zeitraum

Daten in der Kasse gespeichert werden sollen, muss hier evtl. eine Erweiterung vorgenommen werden.

Da sich die Bedeutung des Journals erheblich erhöht, müssen Datenverluste aufgrund von technischen oder Bedienfehlern so weit wie möglich vermieden werden. Speziell die Abläufe beim Abruf der Daten (z. B. beim Schreiben auf Datenträger oder Übertragen per DFÜ) müssen so fehlertolerant wie möglich sein. So sollte z. B. nach dem Übertragen der Journaldaten auf einen USB-Speicher eine Sicherheitskopie in der Kasse verbleiben, da der USB-Speicher verloren gehen oder beschädigt werden kann, bevor die Daten im zentralen PC eingelesen werden konnten.

2.8 Speicherbedarf

Das „elektronische Journal“ inkl. der Signaturen kann aufgrund des Sicherheitskonzepts an einer beliebigen Stelle gespeichert werden und muss nicht wie bei klassischen Fiskalspeicherlösungen (sofern diese überhaupt mit einem Journal arbeiten) im Fiskalspeicher der Kasse abgelegt werden. In einer PC-Umgebung wird i. d. R. immer genug Speicher zur Verfügung stehen, so dass der problematischste Fall die Speicherung in einer proprietären Kasse über einen längen Zeitraum sein dürfte.

Um einen Eindruck über den Speicherbedarf für ein signiertes elektronisches Journal zu geben, ist in der Tabelle 1 der Speicherbedarf der Vectron-Implementierung aufgeführt.

Tabelle 1: Speicherbedarf

Transaktionen	Positionen pro Transaktion	Speicher pro Tag (kB)	Speicher pro Jahr (MB)
200	3	38	11
200	4	43	13
400	5	95	29
600	5	143	43

Es liegt die Annahme zugrunde, dass der Kassenplatz an 300 Tagen im Jahr genutzt wird. Die Zahl der Transaktionen ist relativ hoch angesetzt, die der Positionen pro Transaktionen eher gering. Bei einer Verschiebung zu weniger Transaktionen bei gleichbleibender Gesamtzahl der Positionen (also mehr Positionen pro Transaktion) reduziert sich der Speicherbedarf.

Da die Datenspeicherung relativ stark optimiert ist, kann der Speicherbedarf bei anderen Implementierungen nach oben abweichen – eine noch kompaktere Datenspeicherung ist aber auch ohne besonders hohen technischen Aufwand möglich (z. B. durch Anwendung gängiger Kompressionsalgorithmen z. B. auf alle Daten eines Tages).

2.9 Tagesabschlüsse

Beim Tagesabschluss werden durch ein spezielles Kommando signierte Summenzähler vom TIM gelesen. Diese Daten müssen ebenfalls im elektronischen Journal gespeichert werden.

Um die Bedienung zu erleichtern und Anwenderfehler zu verhindern, ist eine Automatisierung durch Verknüpfung mit einer entsprechenden Kassenabrechnungsfunktion (Tagesabschluss, Kassenschnitt o. ä.) sinnvoll.

2.10 Übertragung und Weiterverarbeitung

Es ist eine dauerhafte Speicherung der Journaldaten erforderlich. Außerdem muss eine regelmäßige Datensicherung gewährleistet werden.

Speziell bei Filialbetrieben ist eine regelmäßige Übertragung der Daten in ein Backoffice-System sinnvoll, da dort eine zweckmäßige Verwaltung und Datensicherung wesentlich einfacher ist. Dieses Vorgehen ist aber keineswegs verpflichtend – eine Langzeitspeicherung und Datensicherung kann auch am Kassensystem selbst erfolgen.

Für die Anbindung der Kassenplätze an ein zentrales System ist die Nutzung bereits vorhandener Kommunikationswege (z. B. ISDN-Übertragung oder Internet für die Kassenabrechnung) naheliegend.

Damit ein gezielter Zugriff auf die aufgezeichneten Daten möglich ist, muss es ein System für den einfachen und schnellen Zugriff auch auf verhältnismäßig große Datenmengen geben. Bei einem großen Filialbetrieb mit Tausenden von Kassenplätzen können bei der notwendigen Speicherung über mehrere Jahre mehrere Milliarden Datensätze anfallen. Dies stellt technisch heute kein Problem mehr dar, muss allerdings konzeptionell ausreichend früh berücksichtigt werden.

2.11 Export

Zur Prüfung der Daten müssen diese in einem vorgegebenen XML-Format exportiert werden können. Damit eine Verifikation der Daten überhaupt möglich ist, müssen die Daten nach dem Auswerten der XML-Exportdatei exakt in das beim Verkaufsvorgang signierte Format umgewandelt werden können. Aus diesem Grund müssen Struktur und Inhalt des Exportformates sehr detailliert vorgegeben werden

Tabelle 2: Entwicklungsaufwand

Aufgabe	Initialkosten in €	Personalaufwand Ist (Manntage)	Schätzung Aufwand bei fertiger Spezifikation
Eigener Kartenleser (anteilig)	1.500	10	10
Ansteuerung Smartcard		10	10
Signaturerstellung		12	3
Fiskaljournal in der Kasse		50	50
Fiskaljournal in Backoffice-Software		45	45
XML-Export		5	4
Verifikationssoftware		10	6
Summe gesamt	1.500	142	128
Summe ohne Fiskaljournal	1.500	47	33

Durch die genaue Definition des Exportformats dürfte es kaum Unklarheiten bei der Implementierung geben. Daher ist eine Umsetzung wesentlich einfach als z. B. die Implementierung einer GDPdU-konformen Schnittstelle, deren Inhalte und Formate nur rudimentär spezifiziert sind

2.12 Verwalten von TIMs und Zertifikaten

Für Anwender mit vielen TIMs (also vor allem Filialbetriebe) sind Hilfsfunktionen zur Verwaltung der Karten sinnvoll, um den Verbleib und den Zustand der Karten (in Betrieb, außer Betrieb, noch ungenutzte Reservekarte) zentral erfassen zu können.

Es bietet sich an, alle Karten in einer PC-Anwendung zu erfassen. Dabei sollten auch die Zertifikate (diese enthalten die Schlüssel zu Verifikation der Daten und können aus der Karte ausgelesen werden) für einen einfachen Zugriff dort gespeichert werden.

2.13 Plausibilisierung / eigene Verifikation

Es ist davon auszugehen, dass Anwender eine Lösung nachfragen werden, mit der sie Ihre Daten selbst verifizieren und eigene Plausibilitätskontrollen vornehmen können. Damit kann z. B. sichergestellt werden, dass die Daten vollständig sind und die sich daraus ergebenden Summen mit den entsprechenden Umsätzen im Buchhaltungssystem übereinstimmen. Durch diese Prüfung können z. B. Fehler bei der Übernahme von Datenbeständen erkannt werden.

Da alle zu verifizierenden Daten genau spezifiziert sind, ist so eine Software zur Verifikation und Plausibilisierung für alle Kassensysteme einsetzbar. Damit ist es sehr wahrscheinlich, dass kurzfristig Standardsoftware für diese Aufgabe verfügbar sein wird. In diesem Fall war jedoch noch eine Eigenentwicklung erforderlich.

3 Bewertung

3.1 Entwicklungsaufwand (ohne Tests und Dokumentation)

In der Tabelle 2 ist der bei Vectron angefallene Entwicklungsaufwand dargestellt. Dabei sind Tests und Dokumentation nicht berücksichtigt, da diese Aufgaben zum Zeitpunkt der Auswertung noch nicht abgeschlossen waren. Zusätzlich zu dem genannten Aufwand sind noch kleinere Nachbesserungen angefallen – diese haben einen Aufwand von einigen Manntagen erfordert. Der Aufwand für die Mitarbeit am eigentlichen INSIKA-Projekt ist hier ebenfalls nicht berücksichtigt.

Im Rahmen der Entwicklung wurde beschlossen, nicht das vorhandene elektronische Journal zu verwenden, sondern ein neues „Fiskaljournal“ genanntes System einzuführen. Dieser Teil der Entwicklung hat dabei insgesamt den größten Aufwand verursacht. Da eine derartige Neuentwicklung bei anderen Implementierungen in vielen Fällen nicht erforderlich sein dürfte, ist der Aufwand in der Zeile „Summe ohne Fiskaljournal“ entsprechend bereinigt.

Die Entwicklung des Fiskaljournals ist aufgrund anderer Anforderungen (z. B. in Österreich) allerdings auch unabhängig vom INSIKA-Projekt in fast unveränderter Form erforderlich gewesen. Es wurde inzwischen mit Anpassungen für weitere Einsatzzwecke (u. a. zur Erfüllung der Anforderungen des BMF-Schreibens vom 26.11.2010) verwendet.

Die Entwicklung des Kartenlesers für die proprietä-

ren Systeme stellte nur einen Teil der Entwicklung der beschriebenen Erweiterungsplatine dar. Daher sind in der Tabelle nur die auf den Kartenleser entfallenen externen Kosten (vor allem Prototypfertigung) und internen Aufwendungen dieses Projekts ausgewiesen.

Ferner war ein Teil des Entwicklungsaufwandes dadurch bedingt, dass parallel noch Änderungen an Spezifikation und TIM-Prototypen erfolgten sowie kleinere Probleme aufgrund der noch unvollständigen Dokumentation auftraten. Daher wurde von den Entwicklern noch eine Schätzung abgegeben, wie groß der Aufwand beim Vorliegen einer stabilen und vollständig dokumentierten Spezifikation gewesen wäre.

Zusammenfassend lässt sich sagen, dass Aufwand und technische Probleme recht begrenzt waren – vor allem beim Vergleich mit einen klassischen Fiskalspeichersystem. In einer optimalen Konstellation wäre die Entwicklung mit einem Aufwand von ca. 1,5 Mannmonaten möglich gewesen.

3.2 Wesentliche Erkenntnisse

Das wichtigste Resultat der Implementierung ist die Bestätigung, dass das INSIKA-System auch bei der Integration in handelsübliche Kassensysteme entsprechend der Spezifikation funktioniert. Hier hat sich sicher die frühe Einbindung von „Praktikern“, also von Kassenherstellern, ausgezahlt. Die Voraussetzungen für eine erfolgreiche Implementierung lassen sich folgendermaßen zusammenfassen:

- Es muss ein ausreichend leistungsfähiges, flexibles und großes „elektronisches Journal“ vorhanden sein bzw. entwickelt werden.
- Die Grundlagen der Kryptografie sollten bekannt sein, um das System vollständig verstehen zu können.
- Es ist eine Einarbeitung in das Thema „Smartcards“ erforderlich.

Es gab einige kleinere Probleme zu lösen:

- Es musste eine Differenzierung des Umsatzes in reguläre Umsätze, Lieferscheinumsatz und Agenturumsatz erfolgen.
- Da die Bedeutung der Umsatzsteuersätze im TIM vorgegeben ist, war eine frei definierbare Zuordnung der in der Kassen vorgegebenen Steuersätze zu denen des TIM umzusetzen.

Eine Gesamtbewertung stellt sich für Vectron folgendermaßen dar:

- Die Integration war grundsätzlich recht einfach, da es sich nur um Erweiterungen vorhandener Strukturen handelt.
- Es ergaben sich nur wenige Einschränkungen für das Gesamtprodukt (vor allem im Vergleich zu „klassischen“ Fiskallösungen).
- Die Einschränkungen bzw. Veränderungen waren klar definiert sowie leicht nachvollziehbar und damit schnell und einfach umsetzbar. Bei „klassischen“ Fiskallösungen sind die Restriktionen oft hochkomplex, unsystematisch und auslegungsbedürftig, was die Implementierung sehr aufwendig macht.
- Die Performance erwies sich als gut.
- Eine Nachrüstung vorhandener Systeme ist recht einfach.
- Die für die Einbindung erforderlichen Grundstrukturen sind auch geeignet, Einzelaufzeichnungspflichten ohne Sicherheitsmechanismen zu erfüllen.

3.3 Weitere Praxiserfahrungen

In der Folge wurde das INSIKA-System weiteren Labor- und Praxistests unterzogen, u. a. auch im Echtbetrieb in Bäckereifilialen getestet. Dabei haben sich folgende weitere Erkenntnisse ergeben:

- Die TIM-Prototypen arbeiteten zuverlässig.
- Erzeugte Daten waren einwandfrei zu verifizieren.
- Es sind noch kleine Fehler in der Implementierung (sowohl im TIM-Prototypen als auch der Kassensoftware) aufgefallen.
- Die Beschaffung, Aktivierung und Verwaltung der TIMs sowie deren Einbau müssen bei der Installation von Kassen berücksichtigt werden.
- Es ist von allem Beteiligten zu berücksichtigen, dass Testbuchungen an Kassen nicht normal signiert und dann einfach gelöscht werden dürfen.

3.4 Übertragbarkeit der Erkenntnisse auf andere Hersteller

Der Aufwand für die Implementierung war bei Vectron sicher deutlich höher als er es bei den meisten anderen Herstellern sein wird. Die Gründe dafür sind naheliegend:

- Es waren keine Erfahrungswerte vorhanden.
- Die TIM-Spezifikation wurde während der Entwicklung noch geändert.
- Die noch unfertige Dokumentation führte zu einigem Klärungsbedarf.
- Der Hauptaufwand war Überarbeitung des Journalsystems – dies wird bei anderen Herstellern aber entweder nicht erforderlich sein oder unabhängig von einer INSIKA-Implementierung erfolgen müssen, um die Anforderungen des BMF-Schreibens vom 26.11.2010 zu erfüllen.

Ganz analog zu den meisten Softwareentwicklungen werden PC-basierte Systeme i.d.R. recht einfach anzupassen sein. Bei den proprietären Systemen ist der Aufwand durchweg höher – wobei hier eine große Bandbreite zu erwarten ist.

4 Ausblick

Die INSIKA-Implementierung in den Vectron-Kassensystemen ist serienreif und hat den Praxistest bestanden. Lediglich aufgrund des Aufwandes wurde noch auf einige Bestandteile verzichtet. Dabei ist vor allem die kryptografische Absicherung der Messwerte von angeschlossenen Waagen zu nennen, die einen Eingriff in eichpflichtige Teile des Systems und damit eine Erweiterung des entsprechenden Prüfscheins erfordert.

Ein wesentlicher Teil der entwickelten Mechanismen wird momentan in Deutschland und verschiedenen anderen Ländern genutzt, um die verschärften Aufzeichnungspflichten für Bargeschäfte zu erfüllen. Aufgrund der fehlenden rechtlichen und organisatorischen Rahmenbedingungen schafft ein Einsatz von INSIKA momentan keinen Zusatznutzen für die meisten Anwender und wird daher vom Markt nicht nachgefragt. Bei einer gesetzlichen Einführung des Systems wäre eine kurzfristige Umstellung problemlos möglich.

Literatur

[1] *Vectron Systems AG - Kasse, Registrierkasse und Kassensystem*. Vectron Systems AG. März 2012. URL: http://www.vectron.de/ (besucht am 20. 12. 2012).

[2] Wolfgang Rankl und Wolfgang Effing. *Handbuch der Chipkarten*. 5. Auflage. Carl Hanser Verlag München Wien, 2008. ISBN: 978-3-446-40402-1.

[3] NIST. *FIPS Publication 180-4: Secure Hash Standard (SHS)*. National Institute of Standards und Technology, März 2012. URL: http://csrc.nist.gov/publications/PubsFIPS.html.

[4] BMF. *BMF-Schreiben vom 26.11.2010 - IV A 4 - S 0316/08/10004-07 - (2010/0946087) - Aufbewahrung digitaler Unterlagen bei Bargeschäften*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Nov. 2010. URL: http://bundesfinanzministerium.de/.

Ergebnisse und Erfahrungen eines INSIKA Feldversuches

Andreas Osswald
Ratio Elektronik GmbH
Im Kammerbrühl 34, 88212 Ravensburg
a.osswald@ratio-elektronik.de

Als INSIKA Projektpartner hat die Fa. Ratio Elektronik GmbH einen Feldversuch an zwei Tankstellen durchgeführt. Der Feldtest begleitet das INSIKA Projekt um den praxisnahen Einsatz von INSIKA und den damit verbundenen Komponenten anzuwenden und zu überprüfen.

Dabei steht die reibungslose und einfache Integration von INSIKA in bestehende Kassensysteme beim Anwender im Vordergrund. Zudem besteht die Möglichkeit, reale Umsatzdaten zu verarbeiten und praxisnahe Geschäftsfälle abzuwickeln. Darauf basierend können wichtige Informationen über Datenmengen, Zeitverhalten sowie die Handhabung erhoben werden.

Im Feldtest können sämtlich Ausprägungen und Vorgaben, die INSIKA definiert, hinsichtlich der Praxistauglichkeit geprüft und untersucht werden. Der Feldtest erstreckt sich über 18 Monate.

1 Ziel des Feldversuches

Die Fa. Ratio Elektronik GmbH mit Sitz in Ravensburg, ist spezialisiert auf die Entwicklung von Systemen für Tankstellen. Das umfangreiche Produktsortiment bietet von der Steuerung sämtlicher Komponenten (wie Zapfsäulen, Tankautomaten, Tankinhaltsmessung, Preisanzeige,...) über die Erfassung durch Kassensysteme bis hin zur Abrechnung und Verwaltung kompletter Tankstellennetze ein zuverlässiges und bewährtes Komplettsystem.

Der Antrieb für eine Beteiligung am INSIKA Projekt war, dem Kunden bzw. dem Betreiber von Kassensystemen eine einfache und preiswerte technische Lösung für den Manipulationsschutz zu bieten. Zudem sollte die Problematik von bestehenden Fiskallösungen hinsichtlich der Einschränkungen wesentlicher Funktionen verhindert werden.

Es wurde gezielt darauf geachtet, dass eine saubere Trennung zwischen abnahmerelevanten Modulen (Smart Card) und der freien Gestaltung und Erweiterung von Kassensystemen Berücksichtigung finden. Eine behördliche Abnahme der Kasse für die Umsetzung von INSIKA ist nicht erforderlich.

Ein weiterer wesentlicher Aspekt war die Berücksichtigung bestehender Kassensysteme und die damit verbundene Nachrüstung im Betrieb. Die Investitionssicherheit stand stets im Vordergrund. Aufgrund der Struktur der Projektpartner konnten vom Microcontroller-basierten proprietären Kassensystem bis hin zum PC-basierten System der funktionale Nachweis anhand von Referenzimplementierungen erbracht werden.

Mit dem Feldversuch sollte sowohl die fehlerfreie Funktionsweise von INSIKA, als auch die einfache und unauffällige Nachrüstung untersucht und nachgewiesen werden. Es sollten zudem branchenspezifische Geschäftsfälle abgewickelt und betrachtet werden. Die breite und aufwendige Betrachtung bei der konzeptionellen Entwicklung von INSIKA sollte im Feldversuch überprüft und analysiert werden.

2 Beschreibung der Pilotstation

Bei der hier analysierten Pilotstation handelt es sich um eine Tankstelle mit fünf Tankplätzen, einem Tankautomaten sowie einem Shop mit ca. 50 m² Verkaufsfläche. Die Tankstelle und der Shop werden von 06:00 Uhr bis 22:00 Uhr bewirtschaftet. Zwischen 22:00 Uhr bis 06:00 Uhr ist ein Tanken über den Tankautomaten in unbedienter Form möglich.

PTB-Bericht IT-18
doi:10.7795/210.20130206a

Abbildung 1: RPOS NT Kassensystem

Somit stellt diese Tankstelle von der Ausprägung sowie dem Umsatz -und Transaktionsaufkommen eine mittlere Tankstelle dar. Die Tankstelle ist Teil eines Verbundnetzes mit zwei weiteren Tankstellen. Ein Anschluss an ein zentrales Managementsystem der Fa. Ratio Elektronik ist gegeben. Von dort aus wird die Bepreisung der Spritartikel sowie die Abrechnung der Tankstellen vorgenommen.

2.1 Systemübersicht

Es wird ein PC-basiertes Kassensystem (Windows-XP) der Fa. Ratio Elektronik GmbH vom Typ RPOS-NT (V2.02R61) mit integrierter Tankstellensteuerung eingesetzt. Dieser entspricht dem in Abbildung 1 dargestellten Prototyp.

Die Anbindung der Zapfsäulen sowie des Tankautomaten erfolgt über den standardisierten EPSI Bus (European Petrol Station Interface). Über den Tankautomat der Fa. Ratio Elektronik kann während der Shop geschlossen ist bargeldlos mittels Stationskarte oder Debitkarte (girocard) getankt werden. Somit ist der Verkauf von Treibstoffen rund um die Uhr an sieben Tagen der Woche möglich.

Dieses Standardsystem wurde mit einem zusätzlichen Chipkartenleser vom Typ SCR335 ausgestattet und mit einem INSIKA TIM (Tax Identification Module) mit der Version 1.0.6 bestückt. Das Kassensystem wurde mit einem Softwareupdate versehen. Die Anbindung der INSIKA Chipkartenapplikation an das Kassensystem erfolgt über die standardisierte PC/SC2-Schnittstelle (siehe Bild 2).

Ratio Elektronik hat per TeamViewer-Software die Möglichkeit, die Station per Fernwartung zu kontrollieren sowie ggf. Einfluss bei Problemen zu nehmen. Es besteht ein Vollzugriff auf die Station.

3 Anbindung an das Kassensystem

3.1 Chronologischer Ablauf und Meilensteine

Anfang Mai 2010 wurde an der Pilottankstelle der Chipkartenleser angeschlossen, ein Softwareupdate aufgespielt und die INSIKA TIM Smart Card durch eine Aktivierung in Betrieb genommen. Zu Beginn des Piloten wurden keine INSIKA spezifischen Informationen auf den Kundenbeleg gedruckt. Es sollte in einem ersten Pilotversuch geprüft werden, ob die Integration des TIM in ein Produktivsystem keinerlei negativen Einfluss nimmt.

Im Vorfeld wurde dem zeitlichen Verhalten und der Verarbeitungsgeschwindigkeit von INSIKA sehr große Aufmerksamkeit geschenkt. Ein besonderer Moment stellt der Belegabschluss dar. Hier werden die Belegdaten zum TIM übergeben, signiert und die Summenspeicher aktualisiert. Der Kunde sowie der Kassier fokussieren sich in der Regel auf diesen Moment, da der Verkaufsvorgang vor dem Abschluss steht und weitere wahrnehmbare Aktionen wie das Öffnen der Kassenschublade und/oder der Druck des Kundenbeleges anstehen. Kommt es hier zu einer Verzögerung in der Verarbeitungsgeschwindigkeit des Kassensystems wird dies unmittelbar wahrgenommen.

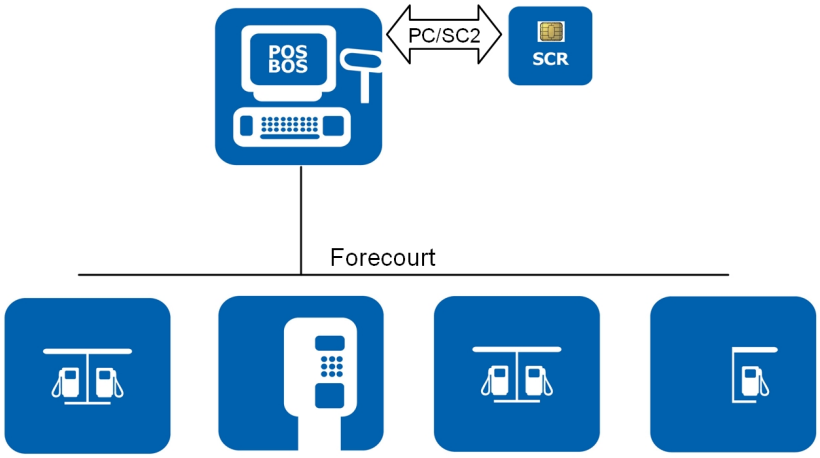


Abbildung 2: Systemübersicht

Aus diesem Grunde wurden die Kassierer bewusst nicht auf die Erweiterung hingewiesen. Es wurde lediglich ein Update des Kassensystems mitgeteilt, um die Benutzer ein wenig zu sensibilisieren. Positiv hervorzuheben ist hier, dass von keinem Beteiligten die minimale zusätzlich Verarbeitungszeit durch das TIM wahrgenommen wurde. Weiter noch hatte keiner überhaupt die Erweiterung zur Kenntnis genommen, alles funktionierte wie zuvor.

An den nachfolgenden Tagen wurde die Station mehrfach per Fernwartung kontrolliert. Es wurden Daten im INSIKA-XML Exportformat (Base64) exportiert und mit dem IVM (Verifikationstool der PTB) überprüft. Dabei kam ein Problem mit der Hashwertbildung der Buchungspositionen zum Vorschein. Die Zeichenersetzung bei den Bezeichnungen der Buchungsposition funktionierte teilweise nicht vollständig.

Der Fehler an der Kassensoftware wurde behoben. Mitte Mai 2010 wurde die korrigierte Kassenversion per Fernwartung auf das System aufgebracht. Alle weiteren Kontrollen waren positiv. Sowohl der Hashwert als auch die Signaturen waren allesamt korrekt.

Daraufhin wurde die Ausgabe der INSIKA relevanten Belegdaten an der Teststation aktiviert. Von Beginn an wurden die zusätzlichen Beleginformationen in einem QR-Code ausgegeben. Sporadisch wurden die Belegdaten an der Tankstelle durch Ratio Mitarbeiter kontrolliert. Sämtliche Belege konnten positiv verifiziert werden. Eine Belegverifikation über den QR-Code stellt sich in der Praxis als sehr einfach und zuverlässig dar.

Ab Mitte Juni 2010 wurde verstärkt mit den bis dahin erzeugten Daten gearbeitet. Es wurden Daten sowohl exportiert als auch verifiziert. Zum ersten Mal war es möglich, das zeitliche Verhalten bei der Verarbeitung größerer Datenmengen zu betrachten. Auch hierbei konnten keine Probleme festgestellt werden. Es wurden zwar Anpassungen der Software im Bezug auf die Exportgeschwindigkeit der INSIKA Daten vorgenommen, jedoch konnte hier keine erhebliche Reduzierung der Verarbeitungszeit erreicht werden.

3.2 Erkenntnisse

Die An- und Einbindung des TIM in ein PC-basiertes Kassensystem ist durch die Grundlage einer normierten Infrastruktur relativ einfach und mit einem überschaubaren Aufwand möglich.

Es zeigt sich, dass im Besonderen die Zusammenstellung der Buchungspositionen von Bedeutung ist. Es besteht ansonsten keine Möglichkeit mehr, den Hashwert der Buchungspositionen zu reproduzieren. Es muss dabei teilweise eine Denormalisierung des Datenbankmodells vorgenommen werden, um die Daten zum Buchungszeitpunkt festzuhalten (Daten müssen teilweise redundant abgespeichert werden).

Entgegen unserer Erwartungen, wurde der QR-Code mit den INSIKA-Daten auf dem Beleg kaum negativ wahrgenommen. Das Beleglayout wird durch den QR-Code kaum beeinträchtigt. Alle wichtigen Informationen für den Kunden sind nach wie vor sofort ersichtlich. Der Kunde wird nicht mit zusätzlichen Informationen abgelenkt. Aufgrund des kompakten Formates des QR-Codes ist der zusätzlich Papierbedarf marginal.

Mithilfe der Tagesschnitte (Tagesende) am TIM ist eine Plausibilisierung der Daten im Bezug auf das Kassensystem möglich. Zudem lassen sich die Summenspeicher des TIM sehr einfach mit den Umsatzdaten des Kassensystems vergleichen.

Besonders hervorzuheben ist die Tatsache, dass sowohl der Kassier als auch der Verbraucher keine Veränderung wahrgenommen hat.

3.3 Buchungsdetails der Teststation

Aus den Untersuchungen der Pilotstation konnten eine Reihe von subjektiven Erfahrungen gesammelt werden, die allesamt positiv waren. Zudem konnten eine Reihe von objektiven Fakten erfasst werden. Die nachfolgende Tabelle 1 gibt Aufschluss über die Anzahl der Transaktionen. Es kann hierbei von einem mittleren Transaktionsaufkommen ausgegangen werden.

Tabelle 1: Buchungen

ø-Anzahl der Buchungen je Tag	411
ø-Anzahl der Buchungen je Monat	12330
ø-Anzahl der Buchungen je Jahr	147960
Buchungen Pilotzeitraum (18 Mon.)	221940

3.4 Datenvolumen

Sämtliche Telegrammanfragen (Buchungen und Tagesende), die eine Signatur durch das TIM erzeugen, werden in einer Datenbank gespeichert. Zusätzlich werden sämtliche Antworttelegramme des TIM zum Kassensystem ebenfalls in einer Datenbank abgespeichert. Aus diesen Daten lassen sich dann jederzeit über beliebige Zeiträume sowohl sämtliche Auswertungen, als auch alle fiskalrelevanten Daten erzeugen. Diese Daten bilden die Grundlage der INSIKA Exportdatei.

Tabelle 2: Telegrammlänge Kasse $\leftrightarrow$ TIM

ø-Telegrammlänge aller Anfragen (Kasse $\rightarrow$ TIM)	57 Byte
ø-Telegrammlänge aller Antworten (TIM $\rightarrow$ Kasse)	74 Byte

In dem von Ratio Elektronik verwendeten Datenbanksystem wird somit für jede Buchung ein zusätzliches Datenvolumen von 586 Byte benötigt. Dieses Volumen ist natürlich sehr stark von den zusätzlichen Daten, den Indizies und letztlich vom Datenbanksystem selbst abhängig.

Über den kompletten Pilotzeitraum ergibt sich somit ein zusätzliches Datenvolumen von 124,03 MByte auf dem Kassensystem. Dieses zusätzliche Datenvolumen stellt für das verwendete Kassensystem und die vorhandenen Ressourcen absolut kein Problem dar.

3.5 Timing

Für die Betrachtung der Schnittstelle hinsichtlich des Timings wird der Zeitpunkt herangezogen, zu dem ein Telegramm an den PC/SC2- Treiber übergeben bzw. vom PC/SC2- Treiber zurück kommt. Die Zeiten sind dabei sehr konstant und reproduzierbar.

Die Vorteile der TLV-kodierten Kommunikation zum Smart Card Reader bezüglich kompakter Daten sowie der Möglichkeit Datenfelder anzupassen (Datenlänge) sind durchweg erkennbar. Auch die Umsetzung eines entsprechenden Parser ist sehr einfach möglich und kaum rechenintensiv. Das TLV Format begünstigt das Zeitverhalten in positiver Form.

Tabelle 3: Zeitverhalten der Schnittstelle

Befehl / Sequenz	ms
Initialisierungssequenz bestehend aus:	**808**
<Verbindungsaufbau SCR>	230
<Status lesen SCR>	<1
<TIM Anwendung auswählen>	47
<TIM langer Status>	16
<Liste der gebuchten Umsatzmonate>	390
<Lesen des Zertifikates>	125
Buchung	**250**
Tagesende	**720**

Es wird sofort ersichtlich, dass der Verbindungsaufbau zum Chipkartenleser, ein zeitkritischer Punkt darstellt. Somit erscheint es sinnvoll, die Verbindung einmalig aufzubauen und offen zu halten. Sollte es zu einem Verbindungsabbruch zwischen der Kasse und des Chipkartenlesers kommen, wird dies durch einen Fehler bei der nächsten Anfrage ersichtlich. Daraufhin ist ein erneuter Verbindungsaufbau erforderlich.

Durch die Komprimierung bzw. das Zusammenfassen der Buchungspositionen zu einem Hashwert ist die Buchungszeit relativ konstant. Dadurch ist es unerheblich, ob eine Buchung aus einer oder mehreren Buchungspositionen besteht.

Aufgrund der gegebenen Buchungszeit durch das TIM ist eine synchrone Buchung beim Belegabschluss möglich. Eine kalkulierbare Reaktionszeit durch das TIM ist durch die zahlreichen Maßnahmen (TLV-Codierung, Hashwert der Buchungspositionen) jederzeit gegeben.

4 INSIKA Beleghandling

4.1 Allgemein

Ein wesentliches Merkmal von INSIKA ist der Kundenbeleg. Dieser kann als öffentliches Kontrollmedium gesehen werden und wird zwangsweise ausgegeben. Sämtliche INSIKA-relevanten Informationen sind auf dem Beleg enthalten. Darauf basierend haben nicht nur Finanzbehörden die Möglichkeit einer Verifikation des Beleges und des damit verbundenen Geschäftsfalles, sondern jeder einzelne Verbraucher selbst.

Um dieser wesentlichen Bedeutung Rechnung zu tragen, sollte eine Verifikation so einfach wie möglich gestaltet werden. Sämtliche Daten sollten einfach und fehlerfrei erfassbar sein.

Diese Anforderungen lassen sich am effektivsten durch einen 2D-Code (QR-Code) verwirklichen. Dadurch können sämtliche Daten kompakt und maschinell lesbar dargestellt werden. Aktuelle POS-Belegdrucker bieten die Möglichkeit die Daten über die ESC/POS Schnittstelle zu übertragen. Der Drucker ist dabei selbständig in der Lage, den QR-Code zu generieren und auszugeben (siehe Abbildung 3).

Zusätzlich ist es möglich, im QR-Code ein Verifikationsziel festzulegen, an das die Daten online übermittelt werden. Dort findet eine Dekodierung und Überprüfung der Daten statt. Ein visuell aufbereitetes Resultat informiert den Anwender.

Aktuell verbreitete Smartphones eignen sich hervorragend für diese Art der Kontrolle. Sie bieten durch die integrierte Kamera in Verbindung mit einer entsprechenden App die Möglichkeit, einen QR-Code zu erfassen und die verifizierten Daten über den integrierten Browser darzustellen (siehe Abbildung 4).

Abbildung 3: Kundenbeleg

Abbildung 4: Resultat der Belegprüfung

5 INSIKA Datenexport (XML)

5.1 Allgemein

INSIKA legt einen einheitlichen Datenexport im XML-Format fest. Dabei stehen zwei unterschiedliche Varianten zur Auswahl. In diesem Feldversuch wurde die Variante 2, „Base64“ verwendet.

Die Betrachtung des Datenexports im INSIKA-Exportformat erfolgt hinsichtlich des zu erwartenden Datenvolumens sowie der Verarbeitungsgeschwindigkeit. Das Exportformat basiert auf der Base64 Codierung.

Die Zusammenstellung der Daten kann individuell über beliebig festgelegte Zeiträume am Kassen- oder Backofficesystem direkt erfolgen (siehe Abbil-

dung 5). Sämtliche Daten werden dynamisch aus den Umsatzdaten (Datenbanken) sowie den zugehörigen TIM-Daten (request und response) zusammengestellt (siehe Abbildung 6). Im System findet keine Konsolidierung der Daten statt.

Bei den Exportversuchen auf diversen Rechnern konnten unterschiedliche Verarbeitungsgeschwindigkeiten, je nach Ausstattung des Rechners, festgestellt werden. Im Unterschied zu den Zeitmessungen in Verbindung mit dem TIM, die durchweg rechnerunabhängig waren, ist hier die Hardware maßgeblich einflussnehmend auf die Verarbeitungsgeschwindigkeit.

Als Verifikationstool stand das IVM von der PTB zur Verfügung. Sämtliche hier dargestellten Ergebnisse basieren auf der Version 0.42 vom 29.02.2012.

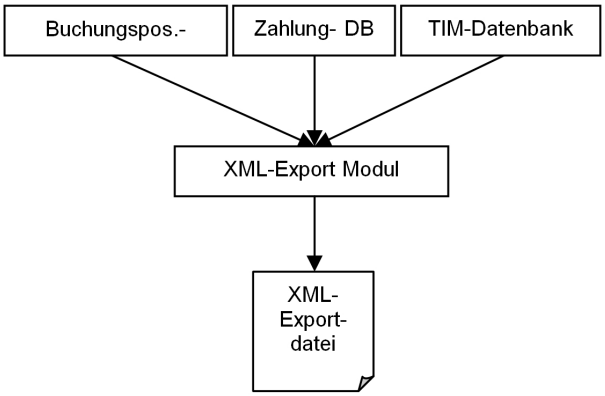


Abbildung 5: Exportübersicht

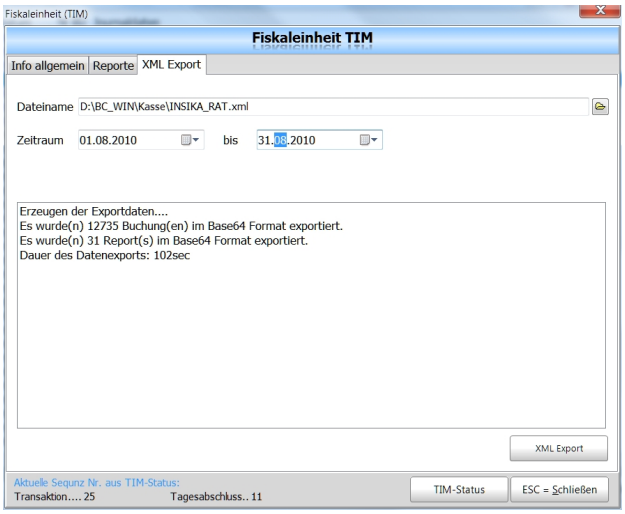


Abbildung 6: Datenexport XML

5.2 Datenvolumen und Timing

Die nachfolgenden Untersuchungen wurden auf einem Windows 7 (32 bit) Rechner mit einem Intel Core i7 Prozessor mit 2,93 GHz und 2 MByte RAM durchgeführt.

Die Zeitmessungen basieren immer auf jeweils fünf Durchläufen. Aus diesen fünf Durchläufen wurde dann der arithmetische Mittelwert gebildet. Die Abweichungen der Messwerte zwischen den einzelnen Durchläufen waren üblicherweise im Bereich $\pm$ 1 s.

5.2.1 Datenexport für einen Monat

Es wurde eine Exportdatei für den Monat August 2010 erstellt. Die Tabelle 4 stellt sämtlich Ergebnisse bezüglich Datenmenge und Verarbeitungszeit dar.

Tabelle 4: Datenexport August 2010

Anzahl der Buchungen	12735
Anzahl der Tagesschnitte	31
Größe der Exportdatei	4,93 MByte
gepackt (ZIP)	1,2 MByte
Dauer des Exports	102 s
Dauer der Verifikation durch IVM	48 s

5.2.2 Datenexport für ein Jahr

Für den Datenexport eines kompletten Jahres (Tabelle 5) wurde der Zeitraum vom 01.06.2010 bis 31.05.2011 herangezogen.

Tabelle 5: Datenexport 06/2010 – 06/2011

Anzahl der Buchungen	147960
Anzahl der Tagesschnitte	365
Größe der Exportdatei	57,11 MByte
gepackt (ZIP)	14,76 MByte
Dauer des Exports	2192 s

6 Ergebnisse

Die Umsetzung von INSIKA für ein PC-basiertes Kassensystem ist durchweg unproblematisch. Es zeigte sich bei der Implementierung, dass INSIKA komplett auf technischen Standards basiert. Sowohl die Anbindung der TIM Smart Card über die PC/SC2 Schnittstelle als auch der XML-Datenexport sind mit Standardkomponenten realisierbar.

Aus Herstellersicht ist besonders hervorzuheben, dass keinerlei Einschränkungen hinsichtlich der Kassenfunktionalität oder auch der Erweiterbarkeit von Kassensystemen zu erwarten sind. Der Innovation stehen keine Zulassungserweiterungen im Wege, da das

Kassensystem bei INSIKA keine besondere Zulassung benötigt. Der sicherheitsrelevante Teil ist sauber abgegrenzt auf das TIM. Diese Tatsache wirkt sich natürlich nicht nur auf die freie Ausbaufähigkeit der Kassensysteme aus, sondern auch unmittelbar auf den Aufwand und damit auf den Preis für die Einführung dieser Fiskallösung. Für Ratio Elektronik als mittelständisches Unternehmen ist dies von großer Bedeutung, da dadurch keine Wettbewerbsverzerrung durch unnötige Barrieren geschaffen wird.

Man erreicht mit der INSIKA Lösung eine maximale Manipulationssicherheit ohne Einschränkung der durch den Markt getriebenen Dynamic an funktionaler Beweglichkeit.

Diese positiven Merkmale, die sich bereits bei der Implementierung gezeigt haben, kommen dann auch bei der Nachrüstung von INSIKA im produktiven Umfeld voll zur Geltung. Selbst die ersten Piloten konnten ohne wahrnehmbare Probleme oder Veränderungen beim Betreiber installiert werden.

Sämtliche branchenspezifischen Besonderheiten wie Agenturgeschäfte, mannigfaltige Zahlarten und geeichte Systeme mit speziellen Beleganforderungen wurden weitsichtig im Projektverlauf erkannt und berücksichtigt. Es traten keinerlei Probleme in diesem Bereich während der kompletten Pilotphase auf.

Alle für den Betrieb eines Kassensystems bedeutenden zeitkritischen Momente konnten durch gezielte Maßnahmen wie dem Hashwert der Buchungspositionen kontrolliert und eliminiert werden. Durch INSIKA ergeben sich weitestgehend keine negativen Störgrößen für den gewohnten Ablauf. Bei der Signatur durch das TIM kann von festen Zeiten ausgegangen werden. Es spielt dabei keine Rolle, ob eine Buchung aus einer oder mehreren Buchungspositionen besteht, sämtliche Geschäftsfälle werden zum TIM einheitlich abgewickelt.

Als Hersteller von Komplettlösungen für die Mineralölbranche sehen wir keine Probleme für die Einführung von INSIKA in Verbindung mit unseren Kassensystemen. Es können sowohl sämtliche bereits betrieben System als auch alle Neuinstallationen mit INSIKA nachgerüstet oder ausgerüstet werden.

Schutz von Daten aus Registrierkassen vor unzulässigen Veränderungen: Fiskalspeicher vs. INSIKA

Rolf Pleßmann
QUORiON Data Systems GmbH
An der Klinge 6, 99095 Erfurt
rd@quorion.de

Es gibt eine weltweite Entwicklung in der zunehmend von Finanzbehörden Fiskalgesetze erlassen werden, die den Einsatz von Fiskalkassen vorsehen und in denen besondere Anforderungen zur Datenspeicherung an Kassensysteme gestellt werden, bei fortschreitender technischer Entwicklung.

Im Folgenden wird ein Vergleich des INSIKA-Projektes gegenüber anderen Fiskallösungen, wie sie in Ländern mit Fiskalgesetzen eingesetzt werden, betrachtet. Hierbei werden zum einen die Control-Unit, wie sie im Fiskalland Schweden eingesetzt wird, der INSIKA Lösung TIM (Tax Identification Module) gegenübergestellt und zum anderen herkömmliche Fiskalspeicher dem INSIKA Konzept.

1 Datenzugriff auf Registrierkassen

1.1 Gesetzliche Anforderungen an die Aufbewahrung digitaler Unterlagen bei Bargeschäften

Das Bundesministerium der Finanzen (BMF) hat seine Anforderungen an die Aufbewahrung digitaler Unterlagen bei Bargeschäften am 25. November 2010 weiter konkretisiert [1].

Die Vorgaben gelten übrigens nicht nur für sämtliche in Registrierkassen erfasste Geschäftsvorfälle wie Barverkäufe, Stornobuchungen oder Entnahmen, sondern auch für Waagen mit Registrierkassenfunktion, Taxametern und sogar Wegstreckenzählern.

Dazu kommt, dass in der Praxis neben der eigentlichen Finanzbuchhaltung auch Barverkäufe bei Außenprüfungen immer mehr automatisiert kontrolliert werden. Die Finanzbehörden verlangen dafür jetzt die sichere Aufbewahrung und den Zugriff auf alle Kassendaten.

1.2 Aufbewahrungs- und Protokollierungspflichten

Alle steuerlich relevanten Einzeldaten einschließlich etwaiger mit dem Gerät elektronisch erzeugter Rechnungen im Sinne des Umsatzsteuergesetzes (§ 14 UStG [2]) müssen vollständig, unveränderbar und unverdichtet aufbewahrt werden. Die digitalen Unterlagen und die Strukturinformationen müssen in einem (maschinell) auswertbaren Datenformat vorliegen.

2 Revisionssicheres System zur Aufzeichnung von Kassenvorgängen

Das Datenvolumen, die rechtliche Bedeutsamkeit und die Sicherheitsanforderungen an Kassendaten steigen also stetig. Daraus resultiert die Aufgabe revisionssichere Systeme zur Aufzeichnung von Kassenvorgängen zu entwickeln und einzusetzen.

2.1 INSIKA-Projekt (Integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme)

INSIKA wurde im Jahre 2008 gestartet, um eine Revisionssicherheit in Kassensystemen zu erreichen und

PTB-Bericht IT-18
doi:10.7795/210.20130206a

einer in 2008 geplanten Gesetzesvorlage zu entsprechen. Hierzu wurde ein Projektkonsortium aus PTB und mehreren Kassenherstellern gebildet, um ein technisches System zur kryptografischen Absicherung von Kassendaten zu entwerfen, zu implementieren und in der Praxis zu testen.

Das INSIKA-Projekt war ein im Rahmen des BMWi-MNPQ-Programms gefördertes Vorhaben. Im Projekt wurde unter Leitung der PTB und den Projektpartnern aus der Kassenbranche ein fertiges technisches System TIM („Tax Identification Module“) für Kassen und Kassensysteme entwickelt und für die praktische Anwendung bereitgestellt.

INSIKA setzt moderne kryptografische Signaturverfahren ein. Die sicherheitskritischen Teile des Systems laufen auf einer Smartcard, die einen sehr hohen und unabhängig prüfbaren Sicherheitsstandard bietet.

Der Manipulationsschutz basiert auf einer digitalen Signatur, die im Einsatzfall von einer durch eine autorisierte zentrale Stelle ausgegebenen Smartcard erzeugt wird. Damit können Daten nicht unerkannt verändert werden. INSIKA ist vergleichsweise einfach zu implementieren und klassischen Fiskalspeicherlösungen in jeder Hinsicht deutlich überlegen.

3 QUORiON Data Systems GmbH

DIe QUORiON Data Systems GmbH als Kassenhersteller ist einer der Projektteilnehmer des INSIKA-Projektes. QUORiON entwickelt und produziert Kassen, Kassensysteme vom Low-End-Bereich bis zum PC-basierten High-End-Touchscreen-System und eine Vielzahl von Systemkomponenten, siehe Abbildung 1.

Weltweit sind mehr als 240 000 QUORiON Kassen installiert. Eine Spezialisierungsrichtung ist dabei die Entwicklung von Hard- und Software, sowie die Produktion von Kassen für den weltweiten Einsatz in Ländern mit Fiskalgesetzen und speziellen Sicherheitsanforderungen für die Datensicherung.

In Tabelle 1 sind typische Ausprägungen von Fiskallösungen und die Länder, in denen das jeweilige Konzept eingesetzt wird, zusammengestellt.

QUORiON baut seit 15 Jahren Fiskalkassen und gegenwärtig sind 110 000 zugelassene Fiskalkassen in 23 Ländern mit Fiskalgesetzgebung im Einsatz. In vier weiteren Ländern befinden sich QUORiON-Kassen und Kassensysteme in der Zulassungsphase.

3.1 Einsatz von QUORiON Kassen in Ländern mit Fiskalgesetzen

QUORiON ist auf dem Markt der weltweiten Fiskalkassenhersteller in der Spitzengruppe positioniert und hat umfangreiche Erfahrungen in der Zulassung und dem praktischen Einsatz solcher Systeme gesammelt.

Daher hat sich QUORiON, als die Arbeitsgruppe für das Projekt INSIKA gebildet wurde, beworben, um an dem Projekt teilzunehmen.

Die Motivation war es, eine effiziente und sichere kryptografische Lösung für eine revisionssichere Datenspeicherung mit zu gestalten. QUORiON weiß aus jahrelanger praktischer Erfahrung, dass die bisherigen Fiskallösungen überwiegend mit konventionellen Speichern und zum großen Teil auch mit durchaus angreifbaren, mechanischen Hardwaresicherungen für den Datenschutz ausgestattet werden.

Besonders negativ sind die immensen materiellen Aufwände für die Entwicklung von Kassen und Kassensystemen für die bisherigen Fiskallösungen, die von Land zu Land durch zum Teil groteske Sicherheitsanforderungen bestimmt werden, aber keinen ausreichenden Nutzen für die Datensicherung haben.

Die Zulassungen von Kassen und Kassensystemen ziehen sich in manchen Ländern zum Teil über Jahre hin und sind nicht selten auch von schwer durchschaubaren Abläufen bekleidet, zum Teil betragen die Zulassungskosten bis zu 200 000 Euro.

4 Vergleich zwischen Fiskalspeicher und INSIKA Konzept-TIM („Tax Identification Module“

Tabelle 2 vergleicht anhand ausgewählter Kriterien Fiskalspeicher mit dem INSIKA-Konzept-TIM („Tax Identification Module“.

5 Vergleich Control Unit Schweden – TIM („Tax Identification Module“)

Im Vergleich mit der schwedischen Fiskallösung wird deutlich welche Vorteile die INSIKA-Lösung bietet.

Seit 01.07.2010 gilt in Schweden ein neues Fiskalgesetz. Der Gesetzgeber gibt als Zweck für das Gesetz an, es soll ehrliche Unternehmen vor unlauterem Wettbewerb schützen. Demnach müssen die Unternehmen beim Verkauf von Waren und Dienstleistungen (Dienstleister sind z.B. auch Zahnärzte mit eigener Praxis) gegen Barzahlung gewährleisten, dass ihre

QMP 50 Serie

QTouch 2

QTouch 10

POS Concerto

QMP 5000 Terminal

QMP 5000 mit eingebauter TIM Karte.

Abbildung 1: QUORiON Fiskalkassen

Tabelle 1: Typische Ausprägungen von Fiskallösungen und deren Einsatzgebiete

Protected Fiscal Memory (Vergossener Speicher EPROM PROM oder Flash)	Protected Fiscal Memory mit Datentransfer über GPRS Modem zu einem Zentralserver	Lokale Datenspeicherung durch Verschlüsselung / Signatur mit externen Geräten
Bangladesch	Albanien	Kanada (MEV)
Brasilien	Bosnien Herzegowina	Schweden Control Unit (BOXEN)
Tschechische Republik	Äthiopien	
Zypern	Serbien	
Griechenland		
Ungarn		
Italien		
Kenia		
Litauen		
Malta		
Montenegro		
Panama		
Polen		
Rumänien		
Venezuela		
Slowakei		

Tabelle 2: Fiskalspeicher versus INSIKA

Vergleichskriterien	Fiskalspeicher	INSIKA
Zulassungsprüfung und Sicherheits-maßnahmen	- Bauartzulassung nötig - keine Datensignierung - niedriger Sicherheitsstandard	- keine Bauartzulassung - kryptographisches Signaturverfahren - hohe Datensicherheit
Was passiert bei vollem Speicher?	- Kasse blockiert - Speicher muss erneuert werden (Speicher in Gehäuseteil vergossen müssen erneuert werden/ Komplettumbau)	- beliebiger neuer Speicher oder neues TIM kann angeschlossen werden werden
Datenhandling	Z Bericht Daten werden in Speicher geschrieben zum Tagesabschluss	- jede Transaktion wird gespeichert und auf den Kassenbeleg gedruckt - mit jeder Transaktion werden die Zähler im TIM aktualisiert
Nachträgliche Implementierung in einer Kasse	- verbunden mit hohem Aufwand und Kosten - umfangreiche mechanische Sicherungslösungen - oft komplettes Neudesign von Mainboard und Komponenten, - umfangreiche Zulassungs-prozeduren	- schnell, einfach und günstig - Anbindung eines handelsüblichen Kartenlesers (intern / extern) - Softwareanpassung im Vergleich zur Fiskalspeicherlösung ist wesentlich geringer - keine Zulassungen für Kassen und Kassensysteme
Prüfung der gespeicherten Daten	- Journal liegt in Papierform vor, dadurch nur manuelle, oft fehleranfällige Prüfung möglich	- Transaktionen liegen signiert als elektronisches Journal vor, dadurch schnelle automatisierte Prüfung aller Belege möglich - revisionssichere Datenspeicherung
Sicherheits-ausführung	- mechanische Sicherung (angreifbar)	- digitale Signatur bietet höchste Datensicherheit

Unternehmen mit zertifizierten Kassen und separaten Kontrolleinheiten (Control Units) ausgerüstet sind.

Die Control Unit ist mit der Kasse über eine serielle RS232-Schnittstelle verbunden.

Die Control Unit speichert Informationen über alle Transaktionen. Die Manipulationssicherung der Daten erfolgt zweistufig. In der ersten Stufe wird ein Control Code erzeugt, der aus einem Hashwert der Transaktionsdaten und den verschlüsselten, aktuellen Ständen ausgewählter Zähler besteht. Der Control Code wird sowohl in der Control Unit als auch im elektronischen Journal der Kasse gespeichert.

In der zweiten Stufe werden alle in der Control Unit gespeicherten Daten verschlüsselt. Als kryptografische Verfahren kommen HMAC-SHA1 und AES256-CBC zum Einsatz.

Die Control Unit muss eine Speicherkapazität für sieben Millionen Transaktionen bieten. Daraus ergibt sich ein Speicherbedarf von min. 2 GB. Einmal gespeichert, können die Daten nur mit einer SD-Card über einen in der Control Unit integrierten SD-Kartenslot von den Steuerinspektoren ausgelesen werden. Der Kartenschlitz vor dem SD-Kartenslot ist mit einem fälschungssicheren Sicherheitsverschluss ausgestattet, um unbefugten Zugriff zu verhindern.

Die korrekte Funktionsweise der Control Unit muss durch eine von SWEDAC (schwedische Behörde für Akkreditierung und Konformitätsbewertung) akkreditierte Zulassungsstelle bestätigt werden.

5.1 Control Unit Schweden in Praxis mit hohen Aufwänden verbunden

Diese Lösung bedingt einen großen Aufwand an Organisation und Kosten für Hersteller, Prüfinstitute, Finanzbehörden und Nutzer.

Die Control Unit ist ein zusätzliches, separates Gerät (Box). Die Kassen die an eine Control Unit angeschlossen werden, müssen von der Steuerbehörde zertifiziert sein und haben spezifische und funktionale Anforderungen an die Hard- und Software. Zu allen Bauelementen der Control Unit werden Herstellererklärungen und Liefernachweise für mindestens 10 Jahre hinterlegt und dienen als Garantie, dass in dieser Zeit keine technischen Änderungen erfolgen. Um eine hohe Zuverlässigkeit der Geräte zu gewährleisten, müssen Bauteile mit einer MTBF von mindestens 7 Jahren verwendet werden.

Weiterhin sind aufwendige mechanische Sicherungen der Box zu treffen. Dies bezieht sich unter anderem auf die Festigkeit und Stabilität der Box. Es ist eine umfangreiche Normenkonfomität nachzuweisen, wie EMV (EN 55022 Klasse B; EN 55024; EN 60950-1) Festigkeit und Klima. Die Produktion darf nur in besonders gesicherten Räumen erfolgen. Der Zulassungsprozess der Control Unit ist mit einem hohen Kosten- und Zeitaufwand verbunden. Es erfolgt eine gesonderte Zertifizierung des Management-Systems des Herstellers durch ein schwedisches Prüfinstitut, jährliche Audits eingeschlossen. Der Kosten liegen mehrfach höher als bei ISO 9001:2008-Zertifizierungen und Audits.

Für die Herstellung gibt das schwedische Finanzministerium Codeschlüssel aus, das gesamte Schlüsselhandling ist aufwendig. Die Schlüsselausgabe erfolgt min. 2x im Jahr nach Antragsstellung des Herstellers. Für den Transport des Schlüssels sind umfangreiche Sicherheitsvorkehrungen vorgeschrieben. Für Aufbewahrung und Handling des Schlüssels beim Hersteller gilt dasselbe; die Aufbewahrung muss in vorgeschriebenen Tresoren erfolgen, agierende Personen werden verpflichtet und müssen der Steuerbehörde bekannt gegeben werden. Außerdem gilt bei der Anwendung des Schlüssels immer das 4-Augen-Prinzip.

5.2 INSIKA TIM („Tax Identification Module“)

Das Modul ermöglicht durch ein kryptografisches Signaturverfahren eine revisionssichere Datenspeicherung. Vorteile liegen unter anderem im wesentlich geringeren Kostenaufwand gegenüber herkömmlichen Fiskalspeicherlösungen. Es ist problemlos in bereits vorhandene Kassen- und Kassensysteme implementierbar. Dadurch entstehen keine aufwendigen Zulassungen für Geräte und es ist keine Zertifizierung der Kassensoftware nötig.

Ein offen dokumentiertes Konzept stellt eine einfache Prüfbarkeit der Daten durch die Finanzbehörden sicher, mechanische Manipulationssicherungen werden nicht benötigt. Gegenüber herkömmlichen Fiskalsystemen mit Fiskalspeicher oder Lösungen wie in Schweden ist daher ein deutlich geringerer Implementierungsaufwand notwendig. Eine Wettbewerbsbeschränkung besteht nicht.

6 Fazit

Mit dem Einsatz eines im INSIKA-Projekt entwickelten TIM („Tax Identification Module“) in Kassen und Kassensystemen steht eine moderne technische Lösung zur Verfügung, die wesentliche Vorteile bei allen Aufwendungen für die Hersteller, die Finanzbehörden und Nutzer gegenüber den bisherigen Fiskallösungen hat und revisionssichere Datenspeicherung unterstützt.

Für das ständig zunehmende Datenvolumen, die rechtliche Bedeutsamkeit und die Sicherheitsanforderungen an die Datensicherheit wird die Anwendung derartiger Methoden bald alltäglich sein und unsere öffentliche, wirtschaftliche und finanzielle Infrastruktur wesentlich mittragen.

Die Datensicherheit wird deshalb zukünftig nicht nur für kommunikativ fließende Daten, sondern auch für das Handling von Daten in Geräten oder auf materiellen Trägern wesentlich mehr im Mittelpunkt aller Bemühungen in der Forschung, Entwicklung und in der praktischen Nutzung stehen.

Literatur

[1] BMF. *BMF-Schreiben vom 26.11.2010: Aufbewahrung digitaler Unterlagen bei Bargeschäften*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Nov. 2010. URL: http://bundesfinanzministerium.de/.

[2] BMJ. *Umsatzsteuergesetz (UStG)*. Version 07.12.2011. Bundesrepublik Deutschland, Bundesministerium der Justiz, Dez. 2011. URL: http://www.gesetze-im-internet.de/ustg_1980/index.html.

Implementierungsaufwendungen für bestehende Kassensysteme und Neuentwicklungen im Vergleich zu klassischen Fiskalsystemen

Benno Kerling
HUTH Elektronik Systeme GmbH
Echternacher Straße 10, 53842 Troisdorf-Spich
bkerling@huth.org

Ein Hauptziel bei der Entwicklung des INSIKA-Verfahrens war es, eine einfache und mit niedrigen Investitionen verbundene Nachrüstung der für INSIKA notwendigen Hard- und Software in bereits bestehende Kassensysteme zu ermöglichen – ebenso stand ein Betrieb mit geringen Folgekosten im Fokus.

In diesem Beitrag wird auf die diesbezüglichen Unterschiede von INSIKA zu aus anderen Ländern bekannten Fiskalisierungslösungen eingegangen. Weiterhin wird als Ausblick auf den Einsatz von INSIKA in Filial- und Agenturkassenumgebungen eingegangen, bei denen unabhängig von den rein fiskalischen Aspekten ein Mehrwert generiert werden kann.

Der Artikel schildert aus bewusst subjektiver Sicht eines etablierten Branchenkassenlösungsherstellers die Motivation zur Mitarbeit bei der Entstehung, die Umsetzung und die Möglichkeiten von INSIKA - auch unabhängig von der reinen Fiskalbetrachtung.

1 HUTH, die PTB und INSIKA

1.1 Wer ist die „HUTH Elektronik Systeme GmbH“

1.1.1 Firmenkenndaten

Die HUTH Elektronik Systeme GmbH hat Ihren Firmensitz in Troisdorf-Spich (bei Köln) und beschäftigt ca. 85 Mitarbeiter. Das inhabergeführte Unternehmen ist seit mehr als 30 Jahren spezialisiert auf den Bereich der Tankstellenmanagementsysteme und ist mit ca. 3.500 Installationen insbesondere im Tankstellenmittelstand einer der deutschen Marktführer.

1.1.2 Produktpalette

Die Produktpalette umfasst Kassen-, Tankautomaten- und Warenwirtschaftssysteme für die Tankstelle mit integrierter Steuerung von Tankstellenperipherie (Zapfsäulen, Preismaste, Tankinhaltsmessungen) und Kartenzahlungsvorgängen sowie Softwarelösungen für die zentrale Abrechnung von Tankstellennetzen.

Der Tätigkeitsbereich umfasst Entwicklung, Produktion, Vertrieb sowie den Vor-Ort-Service über 30 eigene Stützpunkte.

1.2 Motivation für HUTH zur Mitarbeit an INSIKA

1.2.1 Geeichte Kassensysteme

Im Tankstellenbereich stellt die Kasse im Sinne des Eichrechts ein „Ferndruckwerk“ für die Zapfsäulen dar und ist somit ein Teil der nachgelagerten Eichkette für das Messgerät „Zapfsäule“. Aus diesem Grunde erfolgen alle Produktentwicklungen seit jeher in enger Abstimmung mit der Physikalisch-Technischen Bundesanstalt (PTB).

1.2.2 European Petrol Station Interface (EPSI)

Unter Federführung der PTB wurde in den 90er Jahren unter aktiver Mitarbeit von HUTH ein herstellerübergreifendes Protokoll zur Steuerung von Tankstellenperipheriegeräten entwickelt. Das Protokoll basiert auf dem DIN-Messbus (DIN 66348) und ist als eigenständige DIN-Norm 26050 veröffentlicht. Die Pflege des

PTB-Bericht IT-18
doi:10.7795/210.20130206a

Standards erfolgt in der „EPSI-Task-Force“, die unter Leitung der PTB, Herrn Dr. Zisky, tagt.

1.2.3 Sichere Messdatenübertragung

Ein Themenschwerpunkt ist bei Tankstellensystemen immer die sichere Übertragung und Speicherung der Zapfsäulenmessdaten, die sowohl unverfälscht übertragen werden sollen als auch beim Empfänger auf Ihre eindeutige Herkunft zu prüfen sind. Durch diese Problemstellung kam im Rahmen der in der EPSI-Task-Force am Rande geführten Diskussionen über die Einführung einer deutschen Fiskalisierungslösung die Idee auf, den hierfür angedachten Signaturmechanismus auch für die Eichdatensicherung in Betracht zu ziehen. Weiterhin ist für HUTH als Kassenhersteller die mögliche Einführung von Fiskalsystemen ein grundsätzlich relevanter Themenbereich für zukünftige Produktentwicklungen.

1.3 Kassen-Systemplattformen bei HUTH

Zur Einordnung der in späteren Abschnitten abgegeben Einschätzungen für die Implementierungsaufwendungen seien nachfolgend die derzeit bei HUTH verwendeten Systemplattformen kurz vorgestellt.

1.3.1 Etablierte HUTH-Systeme

Der Großteil der sich aktuell im Einsatz befindenden HUTH-Kassensysteme sind vom Typ „HUTH T400/450“, der seit 1994 produziert und im Funktionsumfang ständig erweitert wird. Auch bei einer sich erst mittelfristig ergebenden Einführung eines Fiskalsystems in Deutschland wird ein Großteil dieser Systeme noch im Einsatz sein und kommt somit für eine Fiskal-Nachrüstung in Frage. Die Eckdaten des Systems HUTH T400/450 sind:

- Klassisches Mikroprozessorsystem
- Motorola 68340 32 Bit-CPU
- Komplett eigenentwickelte, proprietäre Hardware
- EPROMs zur Speicherung des geeichten Programmcodes
- Flash-Speicher zur Speicherung der Applikationssoftware
- Die Datenhaltung und die Bereitstellung des Arbeitsspeichers erfolgt in statischem, batteriegepuffertem SRAM
- Als Betriebssystem wird das echtzeit- und multitaskingtaugliche „CRTX“ verwendet, das von HUTH in weiten Bereichen weiterentwickelt wurde.
- Die Kommunikation mit sämtlichen Peripheriegeräten erfolgt ausschließlich über bis zu 26 serielle Schnittstellen. Die physikalische Anbindung (RS232, RS485, CurrentLoop etc.) kann über Steckkarten je Kanal konfiguriert werden.

1.3.2 Zukünftige HUTH-Kassensysteme

In den nächsten Jahren wird HUTH ein neues Kassensystem im Markt etablieren, das für die aktuelle und nächste Dekade als Systemplattform dient. Grundansatz ist hierbei die Migration der bestehenden Architektur in eine aktuelle Hardwareumgebung.

Die Plattform des neuen Systems lässt sich wie folgt charakterisieren:

- Die Hardware basiert auf einer dualen Architektur, bestehend aus einer embedded ARM-Linux-Plattform und einer in der Coldfire-Technologie umgesetzten Echtzeitumgebung.
- Es sind die „üblichen“ PC-Schnittstellen (u.a. V.24 seriell, USB, Ethernet) vorhanden sowie spezifisch herausgeführte RS485-Anschlüsse.
- Der Anschluss von spezieller Tankstellenperipherie (Säulen, Tankinhaltsmessungen etc.) ist über spezielle, proprietäre Schnittstellen möglich.
- Als Betriebssystem kommt ein HUTH-gehärtetes minimalisiertes Linux sowie das vorhandene CRTX zum Einsatz.
- Die Datenspeicherung erfolgt ausschließlich in Flashspeicher und statischem RAM, eine Festplatte kommt nicht zum Einsatz.
- Die Anforderungen für den geeichten Bereich werden über eine separate Druckersteuerung abgedeckt.

2 Kassen-Fiskallösungen außerhalb Deutschlands

Bevor die mögliche Einführung des INSIKA-Verfahrens in Deutschland näher betrachtet und bewertet wird, erfolgt zunächst ein Überblick über den Fiskalisierungsstand von Kassensystemen in anderen Ländern.

2.1 Fiskalisierung der Kassen im Euro-Raum

2.1.1 Länder mit eingeführter Fiskalisierung

Die nachfolgenden Länder des Euro-Raums haben aktuell bereits eine technische Fiskalisierung der Kassensysteme eingeführt:

- Griechenland
- Italien
- Malta
- Montenegro

2.1.2 Länder mit konkreten Einführungsüberlegungen

Es bestehen konkrete Einführungsüberlegungen in folgenden Ländern der Euro-Währungsunion:

- Niederlande
- Österreich
- Deutschland

2.2 Kassenfiskalisierung EU-weit

2.2.1 Aktive Lösungen

Innerhalb der EU, jedoch außerhalb der Währungsunion, existiert die Fiskalisierung bereits in den Staaten:

- Litauen
- Polen
- Rumänien
- Ungarn

2.2.2 Vorbereitet

Konkrete Überlegungen innerhalb der EU für die Einführung gibt es in den Ländern:

- Tschechien
- Slowakei

2.3 Kassenfiskalisierung in Nicht-EU-Ländern

2.3.1 Länderübersicht

Soweit recherchiert werden konnte, ist in folgenden Nicht-EU-Ländern eine Fiskalisierung der Kassensysteme Pflicht:

- Albanien
- Argentinien
- Äthiopien
- Bangladesh
- Bosnien
- Brasilien
- Cypern
- Jordanien
- Kenia
- Nepal
- Serbien
- Türkei
- Venezuela

3 Die Besonderheiten der bestehenden Fiskallösungen und der INSIKA-Ansatz

3.1 Ausprägungen der Kassenfiskalisierungen

Die Betrachtungen der länderspezifischen Fiskallösungen lassen sich wie folgt zusammenfassen:

3.1.1 Kassenpflicht

In nahezu allen Ländern ist mit der Fiskalisierungspflicht auch eine Kassenpflicht eingeführt worden. Das heißt, dass selbst „fliegende Händler“ und Marktstände zwingend ein Kassensystem für einen regulären Verkaufsvorgang verfügbar haben müssen.

3.1.2 Fiskalspeicher

Etwa 80% der Länder realisieren die Fiskalisierung im Wesentlichen durch die Speicherung der Umsatzdaten (meist tageweise kumuliert) in einem gesonderten Fiskalspeicher, der mechanisch gegen Manipulation geschützt ist.

3.1.3 Bonlayout

Bei fast allen Lösungen ist durch die meist über den Drucker realisierte Fiskalisierung das Bonlayout vorgegeben.

3.1.4 Service

In etwa 50% der aufgeführten Länder muss der Service für die Kassensysteme speziell akkreditiert sein. Entweder unterliegen die Techniker der Servicefirmen strengen Zulassungs- und Dokumentationsregularien oder sind sogar exklusiv für diese Arbeiten zugelassene Techniker von zum Teil staatlichen Institutionen.

3.1.5 Zulassung der Kassensysteme

Soweit bekannt, müssen in allen Ländern die Kassensysteme gesondert zugelassen werden. Ausnahme sind die Fiskalisierungskonzepte aus Österreich, den Niederlanden sowie Deutschland.

3.1.6 Kryptographie

Der bei INSIKA verfolge Ansatz der Absicherung einzig über einen kryptographischen Manipulationsschutz ist bisher für kein anderes etabliertes Fiskalisierungsverfahren verwendet worden.

3.2 Trend bei Fiskallösungen

Die Betrachtung der einzelnen Lösungen und der zugehörigen Länder legt einen gewissen Trend für die Einführung von Fiskallösungen nahe:

Es existiert eine niedrige Hemmschwelle zur Einführung von Fiskallösungen in Ländern, deren Wirtschaftssystem in den letzten Jahren ohnehin komplett restrukturiert wurde (z.B. EU-Beitrittsländer und -kandidaten sowie Schwellenländer).

Eine weitgehend abwartende oder zögerliche Haltung herrscht in schon lange etablierten Wirtschaftsräumen vor, insbesondere in der Euro-Währungsunion („Old-Europe“). Eventuell wird hier die Einführung der Fiskalisierung in schon lange, existierende und grundsätzlich liberal aufgestellte Wirtschaftssysteme als nicht gewollten regulatorischen Eingriff gesehen.

3.3 Nachteile klassischer Fiskallösungen

Betrachtet man die existierenden Fiskallösungen aus der Sichtweise eines Kassenherstellers, so ergibt sich eine Reihe von Kritikpunkten an den vorhandenen Konzepten:

3.3.1 Fokussierung auf den Drucker

Durch die oft vorhandene Implementierung der Fiskalisierung im Drucker wird an Kassensystemen genau das Gerät mit einem Manipulationsschutz und aufwendigen Serviceregularien versehen, das den höchsten Verschleiß hat. Während die normale Elektronik der Kassenkomponenten Standzeiten von 10 Jahren und mehr erreicht, ist bei Druckern, je nach Typ, schon nach 2-3 Jahren oft schon die durchschnittliche Standzeit erreicht.

3.3.2 Proprietäre Hardware

Viele klassische Fiskalsysteme basieren auf einer proprietären Hardwarearchitektur, die nur von Spezialisten beherrscht wird und die auf dem Bauteilemarkt unter Umständen Beschaffungsprobleme aufwirft.

3.3.3 Security by obscurity

Das Sicherheitskonzept vieler derzeit im Einsatz befindlichen Fiskallösungen fußt auf mechanisch gesicherte Elektroniken (durch vergießen, Bohrschutzfolien etc.) und Softwarearchitekturen, deren Sicherheit nur darin besteht, dass das Gesamtkonzept geheim gehalten wird. Dies steht in Widerspruch zu den mittlerweile anerkannten Regeln der Informationssicherheit, bei denen die Stärke einer Verschlüsselung nicht durch die Geheimhaltung des Rechenverfahrens, sondern einzig durch die Geheimhaltung des Schlüssels (bei gleichzeitig offen gelegten Algorithmen) erreicht wird.

3.3.4 Protektionistische Ansätze

Die länderspezifisch proprietären Ansätze bedeuten für einen international agierenden Kassenhersteller hohe Anfangsinvestitionen, um überhaupt in einem fiskalisierten Land tätig werden zu können. Zum Teil sind die Regularien für die Zulassung oft nicht präzise genug gefasst, so dass die Zertifizierungen zum Teil erheblich und scheinbar willkürlich hinausgezögert werden können. Hierdurch entstehen selbst innerhalb der EU ungleiche Wettbewerbsbedingungen für in- und ausländische Anbieter.

3.3.5 Zertifizierung der Kassensoftware

Durch die bei vielen Verfahren erforderliche Zertifizierung der kompletten Kassensoftware entsteht ein ernstzunehmendes Innovationshemmnis. Mag es bei Standardkassensystemen wenig Änderungen und Weiterentwicklungen an der Kassensoftware geben, so zeichnen sich Branchenlösungen (z.B. Gastronomie, Tankstellen etc.) oft durch regelmäßige Weiterentwicklungen aus, die zur Optimierung der Arbeitsabläufe benötigt werden. Wenn für neue Softwareversionen, die unter Umständen sogar kundenspezifisch entwickelt werden, jeweils die Kassensoftware neu zertifiziert werden muss, so führt dies zu Innovationshemmnissen.

3.3.6 Service nur durch autorisierte Firmen

Ein weiteres Hemmnis für den Wettbewerb der Kassenhersteller ist die in einigen fiskalisierten Ländern existierende Serviceregelung für die Fiskalmodule. Diese dürfen bei einem Defekt nur durch speziell akkreditierte Servicefirmen (z.T. unter staatlicher Aufsicht) repariert oder ausgetauscht werden. Die Kosten für den Anwender sind hierdurch unverhältnismäßig hoch, hinzu kommen längere Ausfallzeiten des Systems – an nicht fiskalisierten Systemen kann oft ein Komponententausch durch den Anwender selbst erfolgen!

3.3.7 Einschränkungen im Bon-Layout

Sehr viele Fiskallösungen schreiben den Aufbau des steuerrechtlichen Teils des Bons exakt vor. Hierdurch wird Innovation auf Seiten der Hersteller verhindert, ebenso sind die Kassennutzer eingeschränkt, was die Anpassung des Kundenbelegs z.B. für Marketingaktionen angeht.

3.3.8 Nachrüstung bestehender Systeme

Da Fiskalsysteme sehr oft ganze Teile der Kassenarchitektur vorgeben bzw. sogar die komplette Software in Betracht ziehen, ist eine nachträgliche Ausrüstung von bereits im Markt sich befindenden Systemen nicht oder nur mit großem Aufwand möglich.

3.4 INSIKA-Die Lösung für „Old-Europe“?

Bei der Entwicklung des INSIKA-Konzepts war es u.a. Ziel, möglichst viele der vorstehenden Nachteile und Einschränkungen zu umgehen, um eine hohe Akzeptanz bei Anwendern, Herstellern und beim Gesetzgeber zu erreichen.

3.4.1 Offenes Konzept

Bei INSIKA handelt es sich um ein völlig offengelegtes Konzept, das jeder registrierte Interessent komplett einsehen kann.

3.4.2 Kryptographie statt „Obscurity“

Die Sicherheit des Systems basiert ausschließlich auf anerkannten Regeln der Kryptograhie und nicht auf geheime Verfahren oder gekapselte Module.

3.4.3 Minimaler Hardwareaufwand

Kernstück von INSIKA ist das sogenannte TIM – eine Chip-Karte (ähnlich einer Mobiltelefon-SIM), die die kryptographischen Verfahren und den Umsatzspeicher beinhaltet. Es muss lediglich ein mit wenig Aufwand zu realisierender bzw. in einem weiten Angebotsspektrum auf dem Zuliefermarkt beschaffbarer SIM-Kartenleser an das Kassensystem angebunden werden.

3.4.4 Keine Wettbewerbsverzerrung

Durch die völlige Offenlegung des Konzeptes, keine nationalen Zulassungsbeschränkungen und einen freien Service am System existieren für keinen Kassenhersteller durch INSIKA Wettbewerbsvor- oder nachteile.

3.4.5 Minimale Änderungen in bestehenden Kassenkonzepten

Bestehende Kassensysteme (auch schon länger etablierte) können meist sehr einfach mit dem INSIKA-Verfahren nachgerüstet werden, da hardwareseitig lediglich der SIM-Kartenleser über eine serielle- oder USB-Schnittstelle eingebunden werden muss.

3.4.6 „Rule based“-Ansatz

Durch den rein regelbasierten Ansatz wird angestrebt, mit INSIKA ein einerseits für die Steuergerechtigkeit notwendiges, gleichzeitig aber auch in liberalen, etablierten Wirtschaftsordnungen akzeptiertes Verfahren umzusetzen.

4 INSIKA und die Kassenhersteller

(eine subjektive Einschätzung!...) Die Entwicklung des INSIKA-Verfahrens unter Federführung der PTB wurde von Beginn an durch einige Kassenhersteller begleitet, um als Ergebnis ein möglichst markttaugliches Verfahren zu erhalten.

Aus Sicht eines Kassenherstellers wie der HUTH Elektronik Systeme GmbH seien nachfolgend die Vorteiler des INSIKA-Systems noch einmal beleuchtet. Die Betrachtung erfolgt hierbei insbesondere unter dem Aspekt der bei HUTH eingesetzten unterschiedlichen und in ihrer Bandbreite durchaus als repräsentativ zu sehenden Systemplattformen (siehe auch Kapitel 1)

4.1 Hardwarevorteile von INSIKA

4.1.1 Plattformunabhängig

Das INSIKA-Verfahren ist völlig unabhängig von der im Kassensystem eingesetzten Hard- und Software. Sowohl Standardsysteme, die PC-basiert Linux oder Windows als Betriebssystem einsetzen, als auch proprietäre Hardware- und Betriebssystemlösungen sind voll kompatibel mit INSIKA.

4.1.2 Einfache Anbindung

Die Anbindung an alle Arten von Systemen erfolgt über einen standardisierten seriellen Dialog. Physikalisch kann der für INSIKA erforderliche Kartenleser über serielle oder USB-Schnittstellen ähnlich problemlos wie übrige Standardperipherie (z.B. Kreditkartenterminals, Kundendisplays etc.) angebunden werden.

4.1.3 Nachrüstbar

Durch die rein serielle Anbindung und die ganz klare lediglich auf die Bonsignatur beschränkte Definition der Schnittstelle ist auch in älteren Systemen eine Einbringung des INSIKA-Verfahrens möglich, ohne Systemarchitekturen, die ohne INSIKA-Hintergrund schon vor Jahren entwickelt wurden, hardwareseitig in Frage zu stellen.

4.1.4 Kaum systembelastend

Für das Kassensystem bestehen kaum Anforderungen an die Rechenkapazität für das INSIKA-Verfahren. Wünschenswert ist die Berechnung des Hash-Wertes im Kassensystem, (um die Zeit für die serielle Kommunikation mit dem TIM zu sparen), aber auch diese kann von der TIM übernommen werden, so dass für die Kasse lediglich für den INSIKA-TIM Daten zusammengestellt, übertragen und deren Ergebnisse als Ausdruck dargestellt werden müssen. Die Projektbeteiligte Firma Quorion bestätigt die problemlose Realisierung auch auf vergleichsweise eingeschränkt leistungsfähigen 8-Bit-Prozessorsystemen.

4.2 Softwarevorteile von INSIKA

4.2.1 Weitgehend rückwirkungsfrei in bestehenden Systemen implementierbar

Die Erfahrung bei den ersten Beispielimplementationen hat gezeigt, dass sich das INSIKA-Verfahren bei den unterschiedlichen Kassenherstellern unabhängig von der vorhandenen Softwarearchitektur sehr leicht und schnell implementieren lässt, ohne die bisherigen Abläufe grundlegend zu verändern.

4.2.2 Revisionssicherheit

Mit Einführung von INSIKA wird im Kassensystem ein wesentlicher Grundstein für die Revisionssicherheit des gesamten Systems gelegt. Alle auf Bonebene erzeugten Daten des Systems sind durch das INSIKA-Verfahren signiert und stellen somit eine wesentliche Grundlage für eine GDPdU-konforme Weiterverarbeitung und Dokumentation der Kassendaten dar. Würden die Daten nicht durch INSIKA signiert, müssten andere Verfahren zur Datenechtheitsbestätigung der für alle weiteren Aggregationen maßgeblichen Bondaten implementiert werden.

4.2.3 Patentfreiheit

Das INSIKA-Verfahren berührt keine Patentrechte und für INSIKA wurden keine Patente angemeldet. Es handelt sich um ein frei zugängliches, offenes und ausführlich dokumentiertes Verfahren.

4.2.4 Eigenzertifizierung

Die Kassenhersteller haben die Möglichkeit, über die vom INISKA-Projektteam bereitgestellten Tools die korrekte Implementierung selbst zu prüfen. Es ist somit bereits in den Qualitätssicherungsprozessen während der Entwicklungsphase möglich, die Korrektheit der Umsetzung der von INSIKA vorgegebenen Datenformate zu verifizieren. Ebenso kann mit den Prüfwerkzeugen (die durchaus auch in die fertige Kassenapplikation eingebunden werden können) dem Endanwender gegenüber klar dokumentiert werden, dass das System INSIKA-konform arbeitet.

5 Einsatzmöglichkeiten außerhalb der staatlichen Fiskalisierung

5.1 Warum werden Kassensysteme überhaupt eingesetzt?

Bevor im weiteren Verlauf eine Überlegung gestartet wird, warum das INSIKA-Verfahren auch außerhalb gesetzlicher Vorgaben sinnvoll sein kann, sei zunächst noch einmal in Erinnerung gerufen, warum überhaupt Kassensysteme heute bekannter Ausprägung im „B2C“-Geschäftsverkehr (also vom Handel zum Endkunden) zum Einsatz kommen:

5.1.1 Gesetzliche Dokumentationspflicht (GoB, GDPdU)

Grundsätzlich ist jeder Kaufmann verpflichtet, vollständige und lückenlose Aufzeichnungen über seine getätigten Geschäfte zu führen (Grundsätze ordnungsgemäßer Buchführung, GoB) und diese, wenn die Aufzeichnung mittels Datenverarbeitung erfolgt, auch zu Prüfungszwecken in maschinell verwertbarer Form für eine spätere Auswertung bereit zu stellen (Grundsätze zur Durchführung von Prüfungen digitaler Unterlagen, GDPdU). Diese Vorgaben sind mit modernen Kassensystemen problemlos umsetzbar.

5.1.2 Anforderungen der Kunden (UStG)

Die Kunden benötigen gegebenenfalls zur weiteren Verbuchung der Geschäfte in der eigenen Buchhaltung einen dem UStG entsprechenden Beleg, um Vorsteuer in Abzug bringen zu können. Ebenso werden an Bewirtungsbelege Anforderungen gestellt, die nur mit elektronischen Kassensystemen zu erfüllen sind. Von

daher sind Händler schon aus reinem Kundeninteresse gezwungen, aktuelle Kassensysteme einzusetzen.

5.1.3 Eigene Betriebsabläufe des Händlers

Viele Kassensysteme sind an nachgelagerte Warenwirtschafts- oder ERP-Systeme angeschlossen, um Logistik- und Buchhaltungsprozesse automatisiert mit Daten zu versorgen. Insbesondere bei Filialsystem ist das Kassensystem unverzichtbare Datenquelle für eine Vielzahl automatisierter Prozesse im Gesamtunternehmen.

5.1.4 Kontrollzwecke

Neben den finanz- und warenwirtschaftstechnischen Prozessen stellt ein Kassensystem eine unentbehrliche Kontrollinstanz zur Steuerung und Überwachung der Mitarbeiter dar. Nur mit einem Kassensystem kann das korrekte Zusammenspiel zwischen Geld- und Warenfluss sichergestellt und durch den Mitarbeiter dokumentiert werden.

5.2 Beispiel: Tankstellenmarkt

Durch die Tätigkeit der HUTH Elektronik Systeme GmbH im Tankstellenmarkt ist nachfolgend ein Ansatz beschreiben, wie INSIKA auch ohne staatlichen Zwang dem Händler helfen kann, Prozesse zu optimieren.

Der Tankstellenmarkt zeichnet sich, im Verglich zu normalen Handelsfilialisten, durch folgende Besonderheiten aus:

5.2.1 Agentur- und Eigengeschäft

Die Mineralölprodukte werden an Tankstellen meist als Agenturgeschäft im „Namen und für Rechnung“ der Mineralölgesellschaft verkauft, der Shopumsatz ist jedoch Eigengeschäft des Tankstellepartners. Erwirbt ein Kunde also an einer Tankstelle z.B. Benzin und ein Erfrischungsgetränk, so tätigt er ein Geschäft mit zwei verschiedenen Händlern – auch wenn er nur einen Kassenbon erhält und die Gesamtsumme in einem bezahlt. (Auf dem Bon finden sich bei näherer Betrachtung jedoch die Verhältnisse durch entsprechende Hinweistexte und Steuernummern klar dokumentiert)

5.2.2 Kasseneigentum

Das Kassensystem gehört meist der Mineralölgesellschaft (die in Form eines Agenturgebers auftritt) und wird einem Handelsvertreter (in Form des Tankstellenpächters) vorgeschrieben – auch für den Umsatz auf eigene Rechnung. Der Tankstellenpächter ist somit darauf angewiesen, dass das ihm vorgeschriebene Kassensystem alle Vorgänge seines Eigengeschäfts korrekt abrechnet. Andersherum muss sich die Mineralölgesellschaft darauf verlassen, dass alle Agenturvorgänge zweifelsfrei dokumentiert sind.

5.2.3 Filialsysteme im Handel

Eine ähnliche Situation ergibt sich auch im filialisierten Handel: Der Filialleiter muss mit Hilfe der Kasse das korrekte Arbeiten seiner Mitarbeiter kontrollieren und im Interesse des Unternehmens eine integre Kassenführung gewährleisten, ohne immer selber alle Kassiervorgänge überwachen zu können.

5.3 „Private“ INSIKA

Was wäre nun zu tun, wenn ein Unternehmen das INISIKA-Verfahren auch ohne staatlichen Zwang als sinnvoll erachtet, um z.B. die in den vorgenannten Branchen vorherrschenden Anforderungen auf einem sicheren Standard umzusetzen?

5.3.1 Private-INSIKA ist keine Fiskallösung!

Vorweg sei allerdings ausdrücklich vor dem Trugschluss gewarnt, dass ein freiwillig und ohne gesetzliche Grundlage eingeführtes INSIKA-Verfahren Auswirkungen auf die (möglicherweise positiv erhoffte) Beurteilung der Betriebsabläufe unter Fiskalgesichtspunkten hat.

5.3.2 TIM-Ausgabe

Herzstück von INSIKA ist das für jedes Kassensystem individuelle TIM in Form einer Chip-Karte. Um die Eindeutigkeit der Buchungssignaturen zu gewährleisten, muss jede TIM von einer zentralen Stelle mit einem abgeleiteten Zertifikat personalisiert werden. Für ein nicht-staatliches INSIKA muss hierfür ein privater Dienstleister zur Verfügung stehen. Seit dem 3. Quartal 2012 können INSIKA-TIM bei der Bundesdruckerei Berlin bezogen werden. Bei sehr großen Filialunternehmen kann es durchaus auch sinnvoll sein, die Personalisierungsinfrastruktur, ggfs. anknüpfend an schon im Hause für andere Anwendungen vorhandene Zertifikatsstellen, selbst zu stellen.

Nach der Erstausgabe an alle Standorte ist die zentrale Ausgabestelle vor allem mit der Betreuung von Systemwechseln oder der Unterstützung bei Revisionen betraut.

5.3.3 Einführung INSIKA-fähiger Kassen

Für die Einführung einer INSIKA-Infrastruktur sind an allen betroffenen Standorten die Kassensysteme mit der INSIKA-Hardware (Chipkartenleser) und einer INSIKA-kompatiblen Kassensoftware auszurüsten. Wie zuvor schon dargelegt, sollte dies auch für viele bereits vorhandene Kassensysteme mit überschaubarem Aufwand möglich sein.

5.3.4 Zentrale Archivierung der signierten Daten

Um im Revisionsfall die Vorteile von durch INSIKA signierten Daten schnell, unkompliziert und kostengünstig nutzen zu können, sollten die in den Kassensysteme erzeugten signierten Journaldaten zentral gespeichert werden. Neben den zentralen Zugriffsaspekten ist mit dieser Maßnahme auch für GDPdU ein einfacher Bereitstellungsmechanismus der niedrigsten Aggregierungssstufe geschaffen.

5.3.5 Einbindung INSIKA in die Revision

Die interne Revision sollte in den INSIKA-Prozess mit eingebunden werden, da sich durch die lückenlose, signierte Aufzeichnung eine klare Dokumentation aller Abläufe ergibt.

5.3.6 „Bon-Zwang“-Policy einführen

Das INSIKA-Verfahren basiert im Wesentlichen darauf, dass, wie es im Geschäftsverkehr ja ohnehin üblich sein sollte, bei jedem Kassiervorgang der Kunde auf jeden Fall einen Kassebon ausgehändigt bekommt. Diese Regel muss bei Einführung des INSIKA-Verfahrens innerhalb eines Unternehmens noch einmal ganz klar postuliert werden. Verstöße gegen diese in der Praxis sehr einfach zu überprüfende Regel müssen drastisch sanktioniert sein, da jede Zuwiderhandlung einen vorsätzlichen Betrugsfall nahelegt.

5.4 Vorteile des „Private-INSIKA“

5.4.1 Einfache, offene Mitarbeiterkontrolle

Durch Einführung der Bon-Pflicht und der INSIKA-Signatur wird eine klare, eindeutige Regel für den Umgang mit Kassenbuchungen herausgegeben. Die Kassierer sind so mit einfachen Mitteln kontrollierbar. Diese Kontrolle kann, im Gegensatz zu das Betriebklima gefährdenden konspirativen Maßnahmen, völlig offen erfolgen, ohne dass grundsätzliches Misstrauen geweckt wird.

5.4.2 Bessere Datenqualität aus den Kassen

Durch die Buchungspflicht und das Bewusstsein für einen sorgfältig durchgeführten Kassierprozess steigt automatisch die Qualität der an der Kasse erfassten Verkaufsdaten. Dies wirkt sich nicht nur auf die Daten für die Finanzbuchhaltung aus, sondern auch auf die Prozesse der an die Kassensysteme angeschlossenen Warenwirtschafts- und ERP-Software.

5.4.3 Dokumentierte Abläufe für interne Revision und externe Prüfung

Bereits ab einer Mitarbeiterzahl größer 50 Angestellten ist eine Kapitalgesellschaft verpflichtet, den Jahresabschluss testieren zu lassen. Die Wirtschaftsprüfer legen hierbei nicht nur bei der eigentlichen Bilanzerstellung strenge Maßstäbe an, sondern machen ihr Testat auch zunehmend von Prüfungen der internen Organisation abhängig. Durch das INSIKA-Verfahren, das automatisch eine lückenlose Verarbeitungskette der Kassendaten sicherstellt, dürfte dieser, in den meisten Handelsunternehmen sicherlich einen Großteil des Umsatz betreffenden Geschäftsbereich, für Wirtschaftsprüfer künftig sehr schnell zu auditieren sein. Neben der Vereinfachung für den Wirtschaftsprüfer ist auch vorstellbar, dass das Kreditranking des Unternehmens steigt, da die Risiken durch Betrugs- und Steuerdelikte deutlich minimiert werden. Somit stellt eine freiwillige INSIKA-Einführung zumindest für Filialunternehmen schon ab mittlerer Größe als ein echtes Investment dar, das sich bereits nach einigen Jahren amortisiert – auch wenn hierdurch keine Vorteile bei der reinen Steuerprüfung zu erwarten sind.

5.5 „Private-“ wird zu „Public-INSIKA“

Es ist nach wie vor davon auszugehen, dass auch in Deutschland ein Gesetz zur Fiskalisierung von Kassenlösungen eingeführt wird – die INSIKA-Arbeitsgruppe geht davon aus, dass die hierbei verwendete Technik auf INSIKA basiert.

5.5.1 Überführung in Fiskalgesetzlösungen

Sobald das INSIKA-Verfahren als Gesetz verpflichtend eingeführt wird, können die bereist mit dem „Private-INSIKA“ ausgerüsteten Systeme durch einfachen Wechsel der TIM offiziell fiskalisiert werden. Hierbei wird dann die bisher verwendete TIM gegen die von den Steuerbehörden ausgegeben TIM ausgetauscht.

5.6 Vereinfachung für Anwender von Private-INSIKA

Auch wenn eine Fiskallösung selbst auf mittlere Sicht in Deutschland keine politische Zustimmung findet, so wird es, wie zuvor gezeigt, für viele Unternehmen bei näherer Betrachtung durchaus sinnvoll sein, durch Signaturen nach dem INSIKA-Verfahren abgesicherte Kassensysteme auch ohne gesetzlichen Zwang einzusetzen. Sowohl der Staat als auch die Unternehmen haben hiervon langfristig Vorteile.

Um einen Anreiz für die freiwillige Einführung zu schaffen, wäre zumindest eine offizielle Anerkennung des Verfahrens durch die Finanzbehörden erstrebenswert, so dass bei lückenlosem Nachweis der INSIKA-Praxis in einem Unternehmen die Prüfungen für den Kassenbereich zumindest vereinfacht werden könnten.

6 Fazit

INSIKA stellt ein marktreifes, praxistaugliches Verfahren dar. Das Konzept ist völlig offengelegt, von jedem Kassenhersteller mit überschaubarem Aufwand implementierbar und auch in den meisten bestehenden Kassensystemen nachrüstbar. INSIKA erzeugt keinerlei Wettbewerbsverzerrungen durch aufwendige Zulassungsverfahren oder Servicerichtlinien und bietet allen Anbietern gleiche Chancen im Markt.

Selbst ohne gesetzlichen Zwang ist INSIKA bereits in Filialbetrieben mittlerer Größe eine betriebswirtschaftlich sinnvolle Maßnahme zur Optimierung und Sicherung der internen Abläufe.

Aufzeichnungspflichten bei Bargeschäften und Anforderungen an elektronische Registrierkassen und anderen Geräten aus steuerlicher Sicht

Referat IV A 4
Bundesministerium der Finanzen
Wilhelmstraße 97, 10117 Berlin
http://www.bundesfinanzministerium.de/

Seit 1. Januar 2002 ist die Finanzverwaltung berechtigt, Unterlagen im Sinne des § 147 Absatz 1 Abgabenordnung (AO), die mit Hilfe eines Datenverarbeitungssystems erstellt worden sind, durch Datenzugriff zu prüfen. Hierzu gehören auch die mittels Registrierkassen, Waagen mit Registrierkassenfunktion, Fahrpreisanzeigern (Taxameter) und Wegstreckenzählern erfassten Geschäftsvorfälle.

2003 hat der Bundesrechnungshof kritisiert, dass die aktuell gebräuchlichen Registrierkassen und Registrierkassensysteme schon deswegen nicht den Grundsätzen ordnungsmäßiger Datenverarbeitungsgestützter Buchführungssysteme (GoBS) entsprechen, weil die vom Gerät erfassten Aufzeichnungen im Nachhinein spurlos verändert oder beseitigt werden können, sei es durch technische Möglichkeiten, die die Kassenhersteller für ihre Kasse selbst anbieten oder durch den Einsatz externer Software. Die Erfahrungen in der Praxis bestätigen diese Einschätzung.

Auch bei einer Prüfung durch Datenzugriff lassen sich solche Manipulationen nicht oder zumindest nur schwer aufdecken.

Mit dem Ziel den Manipulationsschutz bei Registrierkassen, Waagen mit Registrierkassenfunktion, Fahrpreisanzeigern (Taxameter) und Wegstreckenzählern zu verbessern, hat das Bundesministerium der Finanzen (BMF) am 26. November 2010 das Schreiben zur „Aufbewahrung digitaler Unterlagen bei Bargeschäften“ erlassen (BStBl I S. 1342). Danach gilt für die mittels Registrierkassen, Waagen mit Registrierkassenfunktion, Fahrpreisanzeigern (Taxameter) und Wegstreckenzählern erfassten Geschäftsvorfälle Folgendes:

Um den Datenzugriff zu gewährleisten sind die Unterlagen für die Dauer der Aufbewahrungsfrist jederzeit verfügbar, unverzüglich lesbar und maschinell auswertbar aufzubewahren (§ 147 Abs. 2 Nr. 2 AO). Insbesondere müssen alle steuerlich relevanten Einzeldaten (Einzelaufzeichnungspflicht) einschließlich der mit dem Gerät elektronisch erzeugter Rechnungen i. S. des § 14 UStG unverändert (§ 146 Absatz 4 AO) und vollständig aufbewahrt werden. Darüber hinaus ist eine Verdichtung der Daten oder ausschließliche Speicherung der Rechnungsendsummen unzulässig. Ein ausschließliches Vorhalten aufbewahrungspflichtiger Unterlagen in ausgedruckter Form ist nicht ausreichend. Die digitalen Unterlagen und die Strukturinformationen müssen in einem auswertbaren Datenformat vorliegen.

Das bedeutet insbesondere, das System muss sicherstellen, dass von der ersten Speicherung an nachträgliche Änderungen nicht mehr möglich sind. Die Daten müssen so aufbewahrt werden, dass eine Änderung nicht mehr vorgenommen werden kann oder zumindest aber den ursprünglichen Inhalt erkennen lassen. Wurden Veränderungen vorgenommen, muss erkennbar sein, dass sie vorgenommen worden sind. Ist eine Buchung fehlerhaft, darf sie nur durch eine erkennbare Stornierung oder Umbuchung richtig gestellt werden können.

PTB-Bericht IT-18
doi:10.7795/210.20130206a

Bereitstellung einer Public-Key-Infrastruktur (PKI) für INSIKA-Systeme

Claudia Klug[1], Uta Roßberg[2]

[1]Bundesdruckerei GmbH, Oranienstraße 91, 10969 Berlin
[2]D-TRUST GmbH, Kommandantenstraße 15, 10969 Berlin
claudia.klug@bdr.de, u.rossberg@d-trust.net

Zur Absicherung von Kassen- und Taxameterdaten gegen unzulässige Veränderungen können Smartcards mit Zertifikaten aus einer vertrauenswürdigen Public-Key-Infrastruktur (PKI) eingesetzt werden (INSIKA-Smartcard).

Die D-TRUST GmbH, ein Tochterunternehmen der Bundesdruckerei GmbH, betreibt ein akkreditiertes Trustcenter und liefert seit 2001 unter Anderem sichere Signaturerstellungseinheiten für die Erzeugung von qualifizierten elektronischen Signaturen an Wirtschaftsunternehmen und Behörden. Diese werden z.B. zur Beantragung von Ursprungszeugnissen, für elektronische Ausschreibungen, das elektronische Abfallbegleitscheinverfahren, das elektronische Gerichtspostfach oder dem Emissionshandel eingesetzt.

Als akkreditierter Zertifizierungsdiensteanbieter (ZDA) verfügt D-TRUST über etablierte und geprüfte Prozesse zur Erstellung und Ausgabe von Signaturkarten sowie dem Betrieb der dazu erforderlichen PKI-Systeme und Dienstleistungen. Die INSIKA-Smartcards wurden als neues Kartenprodukt in die Standardprozesse der D-TRUST GmbH in Zusammenarbeit mit der Physikalisch-Technischen Bundesanstalt aufgenommen und können für die INSIKA-Systeme im Taxameter geliefert werden.

1 Firmendarstellung

1.1 Bundesdruckerei GmbH (BDr)

Die Bundesdruckerei GmbH in Berlin entwickelt und liefert Systemlösungen und Dienstleistungen für die sichere Identifikation in der analogen und digitalen Welt und zählt weltweit zu den führenden Unternehmen in diesem Bereich.

Neben kompletten Pass- und Ausweissystemen bietet das Unternehmen Personaldokumente, Hochsicherheitskarten, Dokumentenprüfgeräte, Sicherheitssoftware, Trustcenter-Leistungen und eID-Services für nationale und internationale Kunden im hoheitlichen sowie privatwirtschaftlichen Markt an. Darüber hinaus fertigt die Bundesdruckerei Banknoten, Postwertzeichen und Steuerzeichen sowie elektronische Publikationen.

Als ganzheitlicher Systemanbieter unterstützt die Bundesdruckerei ihre Kunden entlang der gesamten Prozesskette: von der Erfassung, Verwaltung und Weiterleitung biografischer und biometrischer Daten über die Herstellung und Personalisierung modernster ID-Dokumente bis hin zu Systemen zur Ausgabe und Verifikation dieser Dokumente. Außerdem entwickelt sie die technische Infrastruktur, damit Bürger, Behörden und Unternehmen die elektronischen Komponenten der Dokumente in der digitalen Welt nutzen können.

Mit ihren Tochtergesellschaften BIS Bundesdruckerei International Services GmbH, D-TRUST GmbH, Maurer Electronics GmbH und iNCO Sp.z o.o. beschäftigt die Bundesdruckerei-Gruppe rund 2.000 Mitarbeiter weltweit.

1.2 D-TRUST – das Trustcenter der Bundesdruckerei

Über ihr akkreditiertes Trustcenter D-TRUST bietet die Bundesdruckerei Unternehmen und Behörden umfassende Beratung rund um die elektronische Signatur sowie die kompletten Dienstleistungen eines Trust-

doi:10.7795/210.20130206a

centers an. Die Zertifizierungsstelle wurde Ende 1998 mit Sitz in Berlin gegründet. Mit hochqualifizierten Mitarbeitern und spezialisierten Partnern entwickelt D-TRUST neue Lösungen der Hochsicherheitstechnologie im Umfeld der elektronischen Signatur.

Das Trustcenter wurde in der geschützten Umgebung des hochsicheren Wertdruckgebäudes der Bundesdruckerei eingerichtet. Umfangreiche Eingangskontrollen, Überwachungsanlagen und Zutrittsprozeduren schließen den Zugang Unbefugter aus.

Auch die Verfügbarkeit und der Schutz vor Betriebsunterbrechungen werden permanent gewährleistet. Sensible Personendaten sind vor nicht autorisiertem Zugriff zuverlässig geschützt. Als eines der wenigen Trustcenter in Deutschland hat die D-TRUST GmbH das renommierte Zertifikat „Trusted Site Infrastructure – Level 3“ vom TüvIT erhalten: Dies entspricht der Note „sehr gut“ für die freiwillige Überprüfung der Gebäudesicherheit.

2 Trustcenter Leistungen

2.1 Public-Key-Infrastrukturen (PKI)

Public-Key-Infrastrukturen arbeiten immer mit dem Zusammenspiel von privatem und öffentlichem Schlüssel, die das Trustcenter einem Nutzer zuordnet. Während der private Schlüssel geheim bleibt, tritt der Nutzer mit dem öffentlichen Schlüssel nach außen in Erscheinung. Der öffentliche Schlüssel wird dazu vom Trustcenter mit einem Zertifikat versehen, das Informationen über den Nutzer enthält und ihm eindeutig zugeordnet werden kann.

Damit der Nutzer die volle Kontrolle über die Verwendung seines privaten Schlüssels hat, werden die privaten Schlüssel auf Smartcards generiert und gespeichert und können nicht ausgelesen oder kopiert werden.

Da eine Karte verloren oder gestohlen werden kann oder gegebenenfalls nicht mehr gebraucht wird, stellt das Trustcenter die Möglichkeit zur Sperrung der Karte zur Verfügung.

Die Zertifikate aller gesperrten Karten werden in Sperrlisten (Certificate Revocation Lists = CRLs) geführt und veröffentlicht. Der Empfänger einer signierten Nachricht kann so überprüfen, ob die Signatur zum Zeitpunkt der Erstellung gültig war.

2.2 Eigenschaften und Funktionsweise der Elektronischen Signatur

Die elektronische Signatur sichert elektronische Daten vor Manipulation (Datenintegrität) und ermöglicht die Zuordnung der Daten zu einer Person oder Organisation (Authentizität der Daten).

2.3 Datenintegrität

Bei der Signaturerzeugung wird von den Daten, die signiert werden sollen, mittels Signatursoftware ein so genannter Hash-Wert (eindeutiger Fingerabdruck der Daten) gebildet. Dieser Hash-Wert wird mit dem privaten Schlüssel verschlüsselt. Der verschlüsselte Hash-Wert stellt die elektronische Signatur dar. Diese passt genau zu diesen Daten. Wird in den Daten nur ein Bit geändert, so ist die Signatur nicht mehr für diese Daten gültig.

Bei der Prüfung der Signatur wird die Signatur mit dem frei verfügbaren öffentlichen Schlüssel entschlüsselt und somit der Hash-Wert der ursprünglichen Daten ermittelt. Zeitgleich wird zu den vorliegenden Daten noch einmal der Hash-Wert gebildet. Stimmen beide Hash-Werte überein, dann ist gewährleistet, dass die Daten keinerlei Veränderung erfahren haben.

2.4 Authentizität der Daten

Da die Signatur den öffentlichen Schlüssel enthält, der durch das Zertifikat dem Besitzer zugeordnet ist, kann der Empfänger einer Signatur auch die Existenz des Erzeugers und den Zertifikatsstatus beim Trustcenter überprüfen, das das Zertifikat ausgestellt hat.

Das Trustcenter stellt über geeignete Prozesse sicher, dass ein öffentlicher Schlüssel eindeutig einer Person oder Organisation zugeordnet werden kann. Diese Zuordnung wird mit einem Zertifikat, das den öffentlichen Schlüssel und Informationen zum Besitzer des Schlüsselpaares enthält, öffentlich gemacht. Verliert ein Besitzer die Kontrolle über seinen privaten Schlüssel, dann kann bzw. muss er sein Zertifikat sperren lassen. Damit wird für alle Beteiligten klar, dass sein Zertifikat ab diesem Zeitpunkt nicht mehr gültig ist und er sich für nach dem Sperrzeitpunkt erzeugte Signaturen nicht rechtfertigen muss.

3 INSIKA-Smartcards für Taxameter

Im Folgenden wird am Beispiel INSIKA-Smartcards für Taxameter beschrieben, welche Komponenten zum Einsatz kommen und wie der Antrags- und Ausgabeprozess für INSIKA-Smartcards umgesetzt wird.

Die Lieferung der INSIKA-Smartcards für den Wirkbetrieb wird durch D-TRUST, das akkreditierte Trustcenter der Bundesdruckerei GmbH, übernommen.

Dazu wurde der Standardantragsprozess für fortgeschrittene Signaturkarten um die Freigabe der Antragsdaten durch die Taxiaufsichtsbehörde erweitert und die Kartenvorpersonalisierung um das Aufbringen des INSIKA spezifischen Teils (ECC- & TIM-Package) zur sicheren Datenspeicherung auf den Smartcards ergänzt. Die Erstellung und Lieferung der INSIKA-Smartcard wird als D-TRUST Standardprozess für Signaturkarten realisiert.

3.1 Betriebsystem und Kartenprofil

Als Smartcard kommt zurzeit das Produkt der Firma Siemens mit dem Betriebssystem „CardOS V4.3B“ – und dem Infineon Chip SLE66CX642P mit 64 kB EEPROM oder SLE66CX322P mit 32 kB EEPROM zum Einsatz.

Um die Unversehrtheit der Karte vor der ersten Nutzung sicherstellen zu können, erhält der Nutzer für jede Karte einen PIN-Brief mit einer sogenannten Transport-PIN. Mit der Transport-PIN wird die Karte einmalig aktiviert.

3.2 Kartenlayout

Abbildung 1 zeigt eine INSIKA-Smartcard mit dem aktuellen Layout. Im Rahmen der optischen Personalisierung werden die Umsatzsteuer-Identifikationsnummer, die laufende Kartennummer und die Gültigkeitsdauer auf den Kartenkörper aufgedruckt.

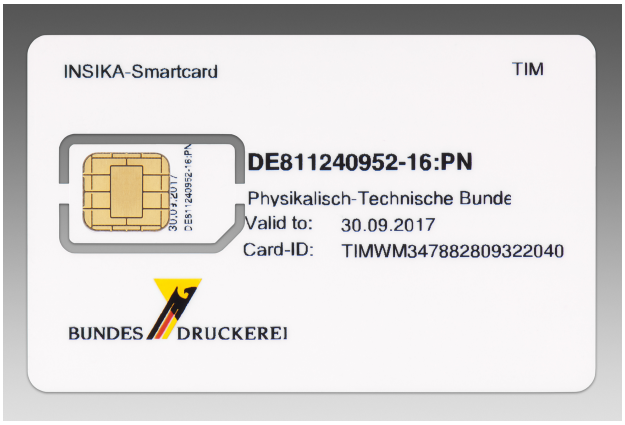


Abbildung 1: INSIKA-Smartcard

Der Kartenkörper wird im ID-1 Format ausgeliefert (Kreditkartenformat). Die Karte ist so perforiert, dass sie sich durch Herausbrechen in das ID-000 Format wandeln lässt. Dieses von SIM-Karten bekannte Format wird in den Sicherheitseinheiten für Taxameter verwendet.

4 PKI

Die D-TRUST GmbH liefert die personalisierten INSIKA-Smartcards mit einem X.509 Zertifikat aus einer bestehenden Class 2 CA Hierarchie (CA = Certification Authority).

4.1 CA-Hierarchie

Abbildung 2 zeigt die CA-Hierarchie. Die Class 2 CA unterliegt den Vorgaben der Zertifikatsrichtlinien der D-TRUST-Root PKI [1]. Class-2-Zertifikate sind hochwertig, aber nicht qualifizierte Zertifikate, die die Anforderungen von ETSI TS 102 042 erfüllen [2].

4.2 Namen

Die Zertifikate erhalten im Feld `DistinguishedName` die für die INSIKA-Anwendung erforderlichen Angaben zum Taxiunternehmen:

```
CN (CommonName) = <Umsatzsteuer-
   Identifikationsnummer> “-“ <laufende
   Nummer> “:PN“
O  (Organisation) = <Name des
   Taxiunternehmens>
C  (Country) = “DE“
```

Die Endung “`:PN`“ weißt darauf hin, dass es sich bei dem Namen um ein Pseudonym handelt. Im Trustcenter sind zu dem Pseudonym die persönlichen Daten des Karteninhabers hinterlegt und können bei einem berechtigten Anliegen offen gelegt werden.

4.3 Gültigkeit

Die Signaturzertifikate haben je nach Speicherplatz der Smartcards (32 oder 64 kB) eine Gültigkeitsdauer von zwei oder fünf Jahren. Die Prüfung der Zertifikatskette erfolgt nach dem Kettenmodell.

4.4 Veröffentlichung

Die Zertifikate werden bei der Erzeugung automatisch im LDAP-Verzeichnis unter `ldap://directory.d-trust.net` veröffentlicht. Dort werden auch die Sperrlisten (CRLs) veröffentlicht.

4.5 Sperrung

Die Zertifikate können vom Antragsteller telefonisch oder schriftlich gesperrt werden.

Bei der telefonischen Sperrung muss sich der Antragsteller mittels Sperrkennwort, das bei der Antragstellung vergeben wird, authentifizieren. Die Zertifikatssperrung erfolgt unmittelbar nach dem Anruf.

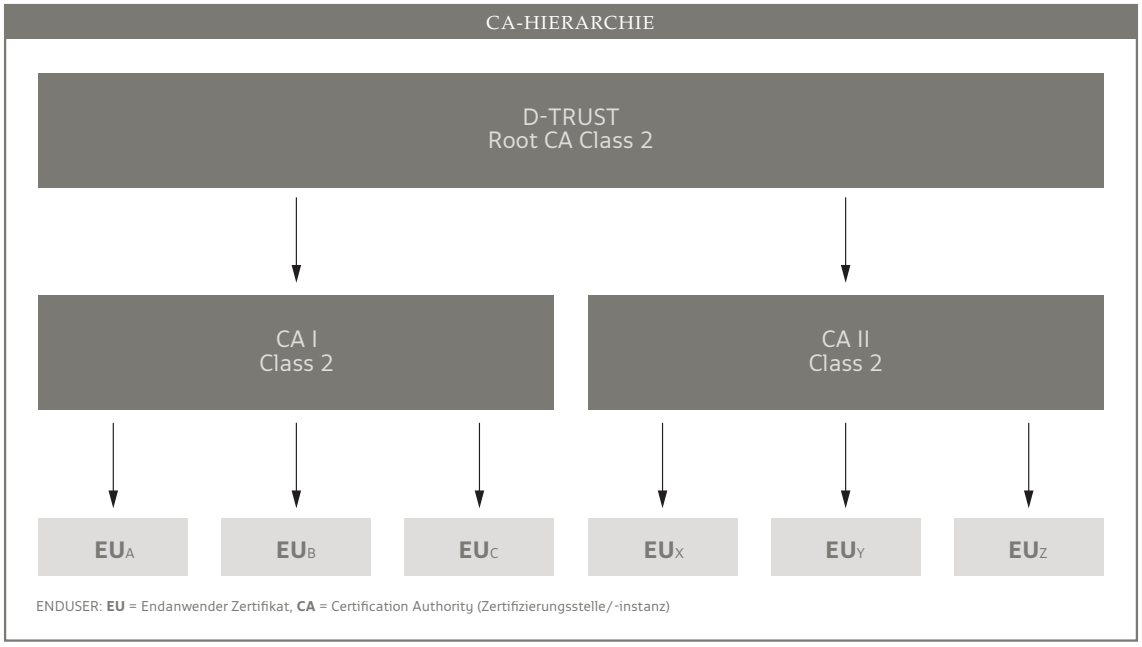


Abbildung 2: CA-Hierarchie (Quelle: Bundesdruckerei GmbH)

Bei der schriftlichen Sperrung sendet der Antragsteller einen persönlich unterschriebenen formlosen Antrag mit Namen, Umsatzsteuer-Identifikationsnummer und Antragsnummer an die D-TRUST GmbH. Die Sperrung erfolgt am ersten Werktag nach Posteingang des Sperrantrags.

5 Antragsprozess

Die Beantragung der INSIKA-Smartcard erfolgt über einen Weblink der D-TRUST GmbH. Der Taxiunternehmer füllt dazu online ein Antragsformular aus, das er am Ende ausdruckt und unterschreibt.

Im Rahmen der Beantragung werden die Personendaten, die Unternehmensdaten inklusive Umsatzsteuer-Identifikationsnummer und Rechnungsadresse abgefragt. Zudem werden die Daten der zuständigen Taxiaufsichtsbehörde zur Auswahl angezeigt.

Der Antragsteller wählt die zuständige Behörde aus und sendet den unterschriebenen Antrag an die Taxiaufsichtsbehörde.

5.1 Freigabe

Die Taxiaufsichtsbehörde prüft, ob der Antragsteller berechtigt ist und gibt den Antrag – im Fall der positiven Prüfung – frei. Anschließend sendet sie die freigegeben Antragsunterlagen an die D-TRUST GmbH.

5.2 Identifizierung

Die Identifizierung und Prüfung erfolgt auf mittlerer Stufe. Über eine Online-Abfrage wird geprüft, ob die Umsatzsteuer-Identifikationsnummer mit den Organisationsdaten übereinstimmt. Zudem wird geprüft, ob die Taxiaufsichtsbehörde den Antrag freigegeben hat.

5.3 Archivierung der Antragsunterlagen

Die Original-Antragsunterlagen werden nach der Prüfung gescannt und für die Zertifikatslaufzeit plus zehn Jahre archiviert. Die weitere Antragsbearbeitung erfolgt mit den elektronischen Daten.

5.4 Registrierung und Kartenpersonalisierung

Die Registrierung erfolgt mittels der geprüften Antragsdaten. Über die Pseudonymprüfung wird sichergestellt, dass der Name im CN eindeutig ist und nur einmal vergeben wird.

Im Rahmen der Vorpersonalisierung wurde bereits ein ECC-Schlüsselpaar auf der Karte erzeugt. Der öffentliche Schlüssel wird während der Registrierung ausgelesen und zusammen mit den Zertifikatsdaten an das zentrale Zertifikatsmanagement System der D-TRUST GmbH gesendet.

Das Zertifikat wird unmittelbar erzeugt und in die Karte eingebracht. Anschließend erfolgt die optische Personalisierung mit den antragsbezogenen Zertifikatsdaten.

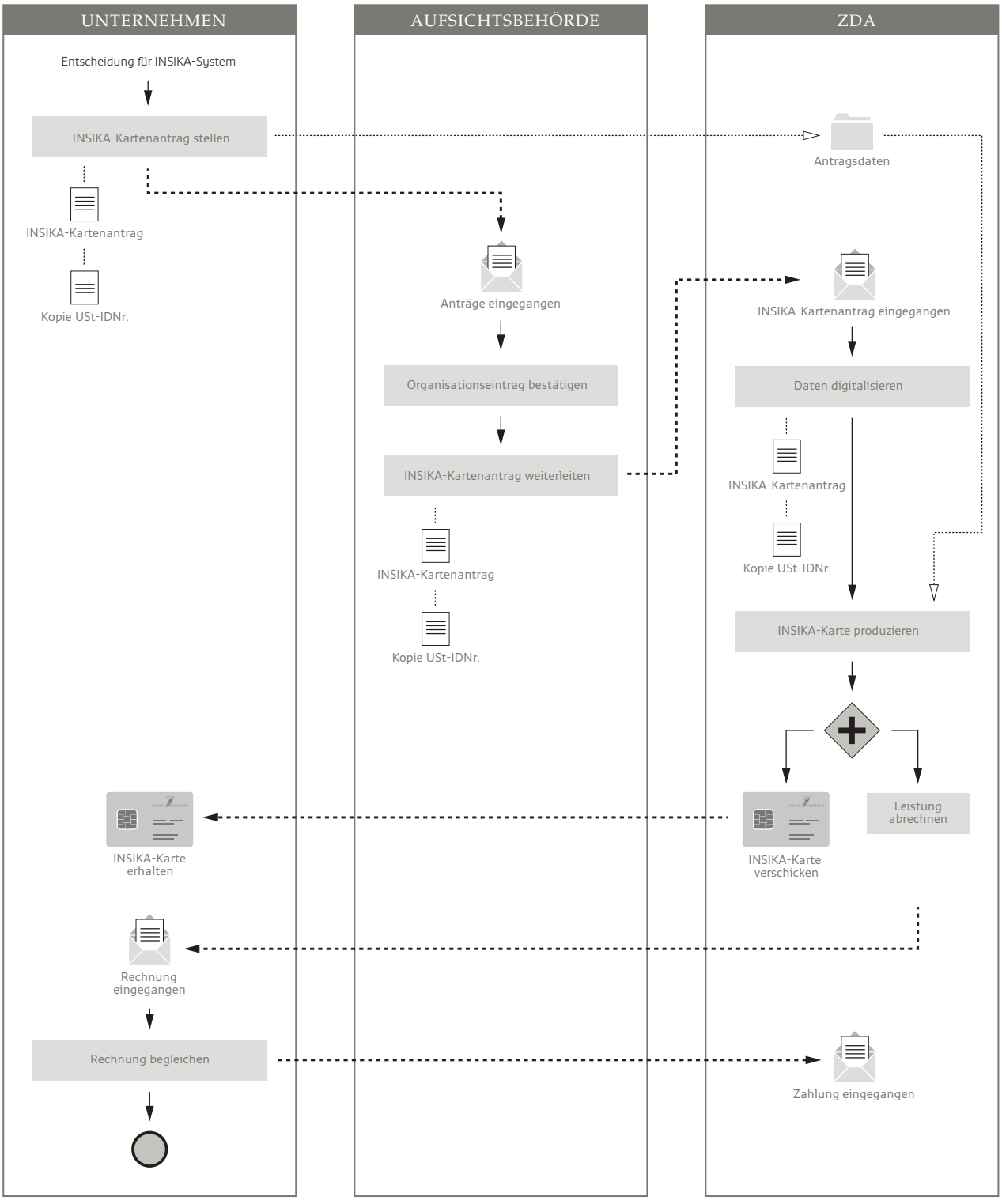


Abbildung 3: Antrags- und Ausgabeprozess INSIKA-Smartcard für Taxameter (Quelle: Bundesdruckerei GmbH)

5.5 Versand und Rechnungsstellung

Die INSIKA-Smartcards werden per Einschreiben an die Antragsteller versendet. Um Missbrauch der Karten zu vermeiden, wird der PIN-Brief zwei Tage nach Versand der Karte per Post an den Antragsteller gesendet. Die Rechnungsstellung erfolgt durch die Bundesdruckerei GmbH an den Antragsteller.

In der Abbildung 3 wird der komplette Prozess für die Ausgabe von INSIKA-Smartcard skizziert.

6 Ausblick

Die Ausgabe der INSIKA-Smartcards für Taxameter startete im 3. Quartal 2012. Eine Ausweitung der Lieferung von INSIKA-Smartcards, z. B. für Registrierkassen, kann problemlos analog umgesetzt werden.

In der ersten Phase sieht der oben beschriebene Antragsprozess und Freigabeprozess noch einen Papierantrag vor, dieser sollte mittelfristig auf einen rein elektronischen Prozess umgestellt werden.

Denkbar sind hierbei der Einsatz des neuen Personalausweises oder des elektronischen Aufenthaltstitels zur Beantragung der INSIKA-Smartcard durch den Unternehmer mittels eID-Funktion, sowie der Einsatz von qualifizierten Signaturkarten für den Freigabeprozess in der zuständigen Behörde.

Die Systeme für die elektronische Antragsprüfung, automatische Bearbeitung und elektronische Archivierung sind schon heute bei D-TRUST vorhanden.

Literatur

[1] D-TRUST GmbH. *Zertifikatsrichtlinie der D-TRUST-Root PKI*. Version 1.6. 13. Aug. 2012. URL: `https://www.d-trust.net/unternehmen/d-trust-cpcps/`.

[2] ETSI. *TS 102 042: Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*. Version V2.1.2. European Telecommunications Standards Institute, Apr. 2010. URL: `http://www.etsi.org/`.

Praktische Aspekte des INSIKA-Sicherheitskonzepts

Jens Reckendorf
Vectron Systems AG
Willy-Brandt-Weg 41, 48155 Münster
jreckendorf@vectron.de

Zum vollständigen Verständnis des INSIKA-Konzepts ist es erforderlich zu wissen, welche Sicherheitselemente es gibt und in welcher Form diese ineinandergreifen. Wesentliche Aspekte werden in anderen Beiträgen der vorliegenden Veröffentlichung erläutert, jedoch ohne zusammenhängende und detaillierte Darstellung. Das soll im Rahmen dieses Beitrags erfolgen.

Es werden im Vorgriff auf die Sicherheitsanalyse die in der Praxis wesentlichen Elemente dargestellt, verschiedene denkbare Angriffe vorgestellt und deren Auswirkungen erläutert. Dabei wird der Schwerpunkt auf die INSIKA-spezifischen Teile gelegt – verwendete Standardverfahren (Kryptografie, Smartcards usw.) werden nur kurz vorgestellt.

1 Überblick

1.1 Grundsätze

In diesem Beitrag werden einige Annahmen zugrunde gelegt:

- Es besteht eine Belegpflicht für jeden Kassiervorgang an einer Registrierkasse.
- Der Beleg muss bestimmte Mindestinhalte aufweisen und vor allem mit einer korrekt ermittelten, ausgedruckten Signatur versehen werden.
- Es werden Stichprobenkontrollen für die beiden o. g. Punkte durchgeführt, so dass ein realistisches Entdeckungsrisiko bei Verstößen besteht.
- Die Smartcards (TIM) werden durch die Finanzbehörden zentralisiert verwaltet und ausgegeben.

Werden diese Annahmen verändert, sind die Analysen und Schlussfolgerungen – teilweise in wesentlichen Punkten – anzupassen.

1.2 Abläufe

Die hier angenommenen Abläufe beim Erfassen von Registrierungen und bei der Weiterverarbeitung der Daten entsprechen dem aktuellen Stand der INSIKA-Spezifikation. Zur Erläuterung sei insbesondere auf die Beiträge von Zisky, Neuhaus und Wolff in diesem PTB-Bericht verwiesen.

1.3 Sicherheitsanalyse

Im Rahmen des INSIKA-Projekts wurde eine Sicherheitsanalyse erstellt. Es gibt deutliche Überschneidungen der Sicherheitsanalyse mit dem vorliegenden Beitrag. Die Sicherheitsanalyse umfasst neben den hier diskutierten Punkten jedoch noch eine Reihe von weiteren Aspekten, z. B. zufällige Gefährdungen des Systems oder sog. Koalitionsangriffe, bei der mehrere Parteien zusammenarbeiten.

1.4 Kryptografie / Smartcards

Die Elemente des INSIKA-Konzepts, die auf Standardverfahren aufbauen und damit den Stand der Technik in Bezug auf Kryptografie darstellen, werden hier nicht weiter behandelt. Auf die wichtigsten Komponenten soll jedoch ganz kurz eingegangen werden:

- Das ECDSA-Verfahren („Elliptic Curve Digital Signature Algorithm“) stellt den Stand der Technik für Signaturlösungen dar, die auch mit kurzen Schlüssel- und Signaturlängen sowie geringem Berechnungsaufwand hohe Sicherheit gewährleisten können.
- Durch die Verwendung einer Standard-Smartcard werden sämtliche Sicherheits-Funktionen der Hard- und Software genutzt. Entscheidend dabei sind die sichere Geheimhaltung des privaten

PTB-Bericht IT-18
doi:10.7795/210.20130206a

Schlüssels und der Schutz der Software vor Manipulationen.

- Durch die Verwendung von Standardverfahren für die PKI („Public-Key Infrastructure“), u.a. unter Nutzung von Zertifikaten, Identitätsprüfungen, CRLs („Certificate Revocation List“) ist sichergestellt, dass eine eindeutige Zuordnung der TIMs und der damit signierten Datensätze zu einem Steuerpflichtigen möglich ist und das verlorene bzw. gestohlene Karten bei Prüfungen erkannt werden können.

2 Prüfszenarien

In diesem Abschnitt sind die wesentlichen Prüfungen beschrieben, die das INSIKA-System vorsieht. Diese können durch Betriebsprüfer oder auch zusätzlich z. B. durch eine interne Revisionsabteilung erfolgen.

Im Folgenden werden verschiedene Begriffe für unterschiedliche Prüfungshandlungen verwendet:

Prüfung: Allgemeiner Begriff für alle Tätigkeiten, die zur Überprüfung dienen.

Kontrolle: Stichprobenartige, vergleichsweise häufige Kontrollen, die eine korrekte Nutzung des Systems sicherstellen sollen. Im Gesetzentwurf aus dem Jahr 2008 wurde dieser Vorgang „Kassennachschau“ genannt.

Audit: Nachträgliche Prüfung der aufgezeichneten Daten über längere Zeiträume. I. d. R. wird das im Rahmen von Außenprüfungen erfolgen.

Verifikation: Überprüfung der Korrektheit einer Signatur.

2.1 Überprüfung gedruckter Belege

Die Prüfung eines gedruckten Belegs ist in zwei Stufen möglich:

- Die wesentlichen Daten wie Datum/Uhrzeit, Identifikation des Steuerpflichtigen, Sequenznummer, steuerpflichtige Umsätze, der Hash-Wert der Buchungspositionen und die Signatur werden erfasst. Diese Erfassung kann manuell erfolgen oder durch OCR-Verfahren weitgehend automatisiert werden. Alternativ dazu ist die Codierung der Daten als 2D-Code und damit eine einfache, automatische Auswertung möglich. Dieser Ansatz ist auch bereits praktisch erprobt. Anhand dieser Daten wird die Gültigkeit der Signatur verifiziert und damit der Nachweis erbracht, dass die Daten durch ein TIM signiert und korrekt abgedruckt wurden. Da für die Prüfung ein über die PKI verwaltetes Zertifikat verwendet wird, erfolgt gleichzeitig eine Überprüfung der Identität des Steuerpflichtigen und dass kein gefälschtes bzw. ein als gestohlen oder verloren gemeldetes TIM verwendet wurde.
- Zusätzlich können die Positionsdaten erfasst und deren Hash-Wert überprüft werden. Das belegt zusätzlich, dass hier keine Veränderungen vorgenommen wurden.

Diese Prüfungen können in folgenden Situationen durchgeführt werden:

- als Stichprobenkontrolle im laufenden Betrieb (dies kann auch ein „verdeckter Testkauf“ sein), um die Korrektheit des Registriervorgangs zu überprüfen oder
- als nachgelagerte Prüfung zu einem beliebigen Zeitpunkt, um die Echtheit eines Beleges zu bestätigen oder widerlegen.

Entsprechende Kontrollen sind bei jedem denkbaren System zur Absicherung der Aufzeichnung von Umsatzdaten erforderlich. Technische Lösungen können diese Kontrollen nur erleichtern und sicherer machen, aber nicht ersetzen.

2.2 Prüfung ohne Belege

Können Kontrolle nicht anhand gedruckter Belege erfolgen, ist nur ein zeitnaher Abgleich von erfassten Buchungen mit tatsächlich getätigten Umsätzen möglich. Diese erfordert den Zugriff auf Transaktionsdaten.

Dieses Verfahren wird beim Einsatz in INSIKA im Taxibereich angewendet, da dort aus verschiedenen Gründen keine Belegpflicht besteht. Dazu werden die signierten Transaktionsdaten per Mobilfunk an einen Server übertragen, so dass jederzeit ein Zugriff für Kontrollen möglich ist.

Alle im Folgenden beschriebenen Prüfungen werden i. d. R. im Rahmen eines Audits stattfinden.

2.3 Schnelle Prüfung der gespeicherten Buchungen

Für eine schnelle Überprüfung der gespeicherten Buchungsdaten werden alle Buchungen zwischen zwei Tagesabschlüssen summiert und mit der Differenz dieser Tagesabschlüsse verglichen. Ferner wird die Vollständigkeit und aufsteigende Folge der Sequenznummern überprüft. Eine Prüfung der Signaturen erfolgt

lediglich für die Tagesabschlüsse. Mit dieser Prüfung würde eine Verschiebung von Umsätzen zwischen Buchungen nicht erkannt werden – dafür läuft sie sehr schnell ab. Sie dürfte in der Praxis fast immer ausreichen, vor allem wenn sie mit Stichprobenprüfungen entsprechend Abschnitt 2.4 kombiniert wird.

2.4 Detailprüfung der gespeicherten Buchungen

Um zu prüfen, dass keine Buchungsdaten verändert wurden, werden die Signaturen der Buchungsdaten entweder stichprobenartig oder vollständig geprüft. Aufgrund des bereits sehr hohen Aussagewerts der unter 2.3 beschriebenen Prüfung ist eine vollständige Prüfung voraussichtlich lediglich bei einem konkreten Manipulationsverdacht und zur genauen Eingrenzung bereits entdeckter Manipulationen erforderlich.

2.5 Prüfung ungenutzter TIMs

Über die PKI ist ermittelbar, welche TIMs auf den Steuerpflichtigen personalisiert sind. Aus allen TIMs, für die bei den Prüfungen nach 2.3 und 2.4 keine Daten vorliegen oder bei denen der Verdacht besteht, dass noch weitere Daten zeitlich nach den neuesten vorliegenden signiert wurden, müssen die Summenspeicher ausgelesen werden. Damit kann verifiziert werden, dass die TIMs nicht benutzt wurden bzw. die vorgelegten Daten wirklich vollständig sind.

2.6 Abgleich der Daten mit der Buchführung

Das wesentliche Ziel der Prüfung von gespeicherten Buchungsdaten im Rahmen eines Audits ist der Abgleich mit den in der Buchführung erfassten Barumsätzen. Dazu bietet sich nach der Verifikation der Buchungsdaten (welche die Vollständigkeit und Unversehrtheit der Daten sicherstellt) die Verdichtung der Daten über geeignete Zeiträume (Jahre, Monate) und der Abgleich mit der Buchführung an. Sollten dabei Abweichungen auftreten, kann die Analyse leicht auf kürzere Zeiträume bis auf die Ebene einzelner Buchungen verfeinert werden.

2.7 Abgleich mit nachgelagerten Systemen

Lieferschein- und Agenturumsätze werden zwar an der Registrierkasse erfasst und in den Signaturvorgang einbezogen. Die steuerlich relevante Verarbeitung erfolgt jedoch in einem angeschlossenen System. Durch einen Abgleich mit diesen Systemen kann die Plausibilität der betreffenden Daten sichergestellt werden. Ist dies nicht möglich, so würden die betreffenden Umsätze wie reguläre Umsätze betrachtet.

2.8 Schließen von Lücken in Buchungsdaten

Sollten Lücken in den Buchungsdaten auftreten (sehr leicht an nicht fortlaufenden Sequenznummern für Buchungen und/oder Tagesabschlüsse zu erkennen), lassen sich die wesentlichen Kennzahlen (Gesamtumsätze nach Steuersätzen, Lieferschein- und Agenturumsätze, Negativbuchungen, Anzahl der Buchungen) zwischen jeweils zwei gültigen Tagesabschlüssen ermitteln. Solche Lücken können durch Datenverluste aufgrund technischer Probleme durchaus auftreten. Mit dem beschriebenen Verfahren können die negativen Auswirkungen sowohl für Prüfer als vor allem auch für die Steuerpflichtigen minimiert werden.

2.9 Abschätzung bei fehlenden Buchungsdaten

Wenn sämtliche Buchungsdaten fehlen, ist die Auswertung der monatlichen Summenspeicher auf dem TIM möglich. Die dort verfügbaren Daten entsprechen dem unter 2.7 beschriebenen Umfang, nur dass hier grundsätzlich Monatssummen erfasst werden.

2.10 Rückgriff auf online eingereichte Daten

Im Rahmen der INSIKA-Lösung ist es technisch möglich, wesentliche Daten regelmäßig online an die Finanzbehörden zu übermitteln (z. B. könnten im Rahmen der elektronischen Umsatzsteuervoranmeldung alle Tagesabschlüsse eines Monats übertragen werden). Durch die Signaturen ist die Datenintegrität gewährleistet. Bei zentralisierter Speicherung können die Folgen eines vollständigen Datenverlustes beim Steuerpflichtigen kompensiert werden.

3 Mögliche Angriffe

In diesem Abschnitt wird eine Reihe von möglichen Angriffen auf das System beschrieben, analysiert und das Restrisiko bewertet.

3.1 Umsätze nicht erfassen

Beschreibung: Umsätze werden nicht an der Kasse erfasst sondern z. B. nur handschriftlich festgehalten.
Analyse: Gegen diese Manipulation gibt es grundsätzlich keinen rein technischen Schutz. Es kann lediglich das Entdeckungsrisiko so weit erhöht werden,

dass Anwender darauf verzichten. Das wird vor allem durch die Belegpflicht mit entsprechenden Kontrollen erreicht. Zusätzlich wird jede systematische Nichterfassung von Daten Auffälligkeiten erzeugen, die bei einem Audit z. B. über Zeitreihenvergleiche erkannt werden können. Ferner ist zu bedenken, dass die Nutzung einer Registrierkasse in vielen Betrieben eine organisatorische Notwendigkeit ist. Einen weiteren Beitrag kann eine Sensibilisierung der Verbraucher leisten. Speziell die Codierung der wesentlichen Daten eines Belegs als 2D-Code würde eine sehr einfache und schnelle Kontrolle ermöglichen. Wenn keine Belegpflicht möglich ist, stellt die unter 2.2 beschriebene Kontrolle eine – wenn auch aufwendigere und weniger effektive – Möglichkeit dar.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege)
Restrisiko: Jede Art von „Fiskal-Kassensystem“ bringt das Risiko mit sich, dass es in der beschriebenen Form umgangen wird. Das Restrisiko kann durch eine Belegpflicht (sinnvoll ist ebenfalls eine Kassenpflicht) und eine ausreichende Kontrolldichte reduziert werden.

3.2 Umsätze nicht signieren und Beleg ohne Signatur drucken

Beschreibung: Eine Registrierkasse signiert grundsätzlich oder auf Anforderung des Benutzers die Umsätze nicht und druckt auch keine Signatur. Das kann z. B. auch dadurch passieren, dass nur unsignierte, „vorläufige“ Belege ausgegeben werden und die Daten anschließend ohne den Ausdruck eines signierten endgültigen Beleges verworfen werden.
Analyse: Diese Manipulation ist sehr leicht und auch rückwirkend erkennbar, da der betreffende Beleg in diesem Fall keine Signatur enthält. Dabei ist zu beachten, dass ein einziger unsignierter Beleg einen Verstoß gegen die Vorschriften beweist. Der Kontrollaufwand ist damit soweit wie möglich minimiert, da bei alternativen Lösungen ohne kryptografische Absicherung eine Kontrolle des Druckvorgangs selbst erforderlich ist. Anders ist in diesem Fall nicht nachweisbar, dass gegen die Belegpflicht verstoßen wurde, da nichtkryptografische Kennzeichnungen von Belegen (z. B. ausgedruckte Symbole) sehr leicht zu fälschen sind.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege)
Restrisiko: Das Risiko wird praktisch nur durch die Kontrolldichte bestimmt.

3.3 Umsätze nicht signieren und falsche Signatur drucken

Beschreibung: Eine Registrierkasse signiert grundsätzlich oder auf Anforderung des Benutzers die Umsätze nicht und druckt eine ungültige Signatur (z. B. Zufallswerte).
Analyse: Diese Manipulation ist durch Überprüfung der Signatur anhand des gedruckten Belegs und damit auch noch rückwirkend erkennbar. Der Kontrollaufwand ist soweit wie möglich minimiert, da bei alternativen Lösungen (ohne kryptografische Absicherung) eine Kontrolle des Druckvorgangs selbst erforderlich ist.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege), Vergleich mit der vermeintlich zugehörigen Buchung, die über die Sequenznummer gefunden werden kann.
Restrisiko: Das Risiko wird praktisch nur durch die Kontrolldichte bestimmt. Dabei ist zu beachten, dass bereits ein einziger unsignierter Beleg einen Verstoß gegen die Vorschriften beweist.

3.4 Umsätze signieren, korrekt drucken und nicht oder verändert im Journal speichern

Beschreibung: Die Registrierkasse signiert und druckt die Daten in korrekter Form, speichert sie dann aber verändert ab.
Analyse: Durch die Signatur lässt sich jede Veränderung an den Daten automatisiert feststellen. Dies umfasst die Veränderung von Inhalten und das Entfernen von Buchungen. Dabei ist auch eine Rückführung auf einzelne Belege möglich. Das Ausmaß der Veränderungen kann tagesgenau aus den Tagesabschlüssen oder bei Verlust aller Daten monatsgenau aus den Summenspeichern des TIM ermittelt werden.
Relevante Prüfung(en): 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.5 Umsätze signieren, verändert drucken und verändert im Journal speichern

Beschreibung: Die Registrierkasse signiert die korrekten Daten, druckt und speichert jedoch eine veränderte Version der Daten.
Analyse: Die Analyse entspricht der unter 3.4, nur das die Manipulation zusätzlich auch an einem gedruckten Beleg erkannt werden kann (da die Signatur nicht zu den anderen Informationen auf dem Beleg passt).

Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) sowie 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.6 Umsätze sammeln, verändern und erst später signieren

Beschreibung: Eine Registrierkasse erfasst zwar Umsätze, signiert sie jedoch nicht. Dies wird erst nach einer Manipulation der Daten „rückwirkend“ durchgeführt.
Analyse: Da das Erstellen einer Signatur im TIM fest mit der Vergabe einer neuen Sequenznummer verknüpft ist, kann jeder Umsatz nur einmal signiert werden (sonst würde er doppelt aufgezeichnet werden müssen). Damit bedingt das geschilderte Vorgehen, dass zum Zeitpunkt der Registrierung kein gültiger Beleg erstellt werden kann. Dies ist durch Kontrollen erkennbar.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege)
Restrisiko: Das Risiko wird praktisch nur durch die Kontrolldichte bestimmt.

3.7 Doppelte Verwendung eines signierten Datensatzes

Beschreibung: In einem Unternehmen mit einem kleinen Sortiment und vielen Transaktionen (z. B. Fast-Food-Restaurant) werden innerhalb einer kurzen zeitlichen Abfolge identische Belege ausgegeben. Es wird nur einmal signiert. Dieser Beleg wird mehrfach verwendet. Ab dem zweiten Beleg werden die Umsätze nicht erfasst.
Analyse: Diese Manipulation ist prinzipiell nicht auszuschließen. Kein Verfahren kann beim Einsatz branchenüblicher Druckverfahren einen "Kopierschutz"für gedruckte Belege bewirken. Selbst bei weitgehenden Einschränkungen für die Registrierkassen könnten Kopien über getrennte Systeme gedruckt werden (z. B. PC mit handelsüblichem Kassendrucker). Die Manipulation ist im Rahmen von Kontrollen leicht erkennbar, da mehrere Belege mit gleichem Datum, gleicher Zeit und Sequenznummer ausgegeben werden. Diese Daten können auf den Kopie-Belegen auch nicht geändert werden, ohne dass die Signatur ungültig würde.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege)
Restrisiko: Bei bestimmten Betriebstypen könnte eine höhere Kontrolldichte erforderlich sein, um das Restrisiko zu minimieren. Der mögliche Schaden durch den beschrieben Angriff ist jedoch in allen praktisch relevanten Fällen sehr gering.

3.8 Journal nachträglich manipulieren

Beschreibung: In einem System werden die korrekt signierten, aufgezeichneten Daten nachträglich verändert. Dies kann in der Kasse oder auch in nachgelagerten Systemen, wie z. B. einer PC-Software zur Speicherung und Verwaltung der Daten, erfolgen. Für eine entsprechende Manipulationssoftware wird oft der der Begriff „Zapper“ verwendet.
Analyse: Die Analyse entspricht der aus Punkt 3.4.
Relevante Prüfung(en): 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.9 Veränderung von Kassenberichten, Buchhaltungsdaten usw.

Beschreibung: Neben der Speicherung der signierten Buchungsdaten werden in jedem System weitere Berichte („Tagesendsummenbons“, Kassenumsätze in der Buchhaltung) erstellt und weiterverarbeitet. Die Inhalte dieser Berichte werden verändert, z. B. durch Stornieren von Umsätzen, ohne dass dies anhand von signierten Buchungen erfolgt.
Analyse: Die genannten Berichte bilden in den meisten Fällen die Grundlage der Buchführung, da die einzelnen Buchungen der Registrierkasse(n) nicht in das Buchführungssystem übernommen werden. Daher ist ein wesentliches Element eines Audits der Abgleich der an der Kasse aufgezeichneten, signierten Buchungsdaten mit den Daten im Buchführungssystem. Da diese Prüfung praktisch vollautomatisiert mit einer Summenbildung über beliebige Zeiträume erfolgen kann, ist sie mit geringem Aufwand (für Steuerpflichtige und Betriebsprüfer) möglich. Jeglicher Fehler wird sicher aufgedeckt. Bei Abweichungen ist eine Nachverfolgung bis hinunter auf die Belegebene möglich.
Relevante Prüfung(en): 2.6 (Abgleich der Daten mit der Buchführung)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.10 Umprogrammierungen von Produkten

Beschreibung: Umsätze für Produkte mit einem geringen Wareneinsatz werden nachträglich als Umsätze mit hohem Wareneinsatz deklariert, um damit bei unveränderten Umsätzen den ausgewiesenen Rohertrag zu reduzieren.

Analyse: Abgesehen davon, dass dieses Vorgehen zusätzlich fingierte Eingangsrechnungen erfordert, sind solche Änderungen eindeutig erkennbar, da in den gespeicherten Buchungsdaten Artikeltexte („handelsübliche Bezeichnung“) enthalten und signiert sind. Eine Überwachung von Programmänderungen der Registrierkasse ist dadurch überflüssig. Es muss lediglich die Analysesoftware eine Summenbildung anhand der Texte beherrschen. Die so gewonnen Summen können leicht auf Plausibilität geprüft werden.
Relevante Prüfung(en): 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent. Lediglich bei einer sehr oberflächlichen Prüfung könnten entsprechende Veränderungen unentdeckt bleiben.

3.11 Trainingsbediener, Service-Modi usw.

Beschreibung: Durch Nutzung von Funktionen zum Test des Systems, zur Einarbeitung von Bedienern etc. werden Umsätze an der Kasse zwar erfasst, aber nicht regulär gespeichert.
Analyse: Durch die Pflicht zur Ausgabe eine signierten Belegs sind solche Manipulationen eindeutig erkennbar – die Analyse entspricht praktisch der aus 3.4. Das TIM verfügt über einen Modus zur Erfassung von Trainingsbuchungen mit separatem Summenspeicher, so dass selbst beim Verlust aller Daten anhand der im TIM gespeicherten Werte das Volumen dieser Buchungen erkennbar ist.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege) und evtl. 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.12 Fälschliche Ausweisung von Umsätzen als Lieferschein

Beschreibung: Umsätze werden fälschlicherweise als Lieferschein-Umsatz ausgewiesen (diese Umsätze werden gemäß der Spezifikation signiert, die zugehörigen Bareinnahmen erfolgen aber nicht an der Kasse, sondern in einem nachgelagerten System).
Analyse: Im Rahmen eines Audits ist nachzuweisen, wie die Lieferschein-Umsätze weiterverarbeitet wurden. Ist das nicht möglich, werden sie wie normale Umsätze gewertet. Das gilt auch im Fall des Verlusts der gespeicherten Buchungsdaten und Rückgriff auf die Summenspeicher im TIM.
Relevante Prüfung(en): 2.7 (Abgleich mit nachgelagerten Systemen) und evtl. 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Es besteht kein Risiko, dass durch dieses Vorgehen Umsätze verschleiert werden können.

3.13 Fälschliche Ausweisung von Umsätzen als Agenturumsatz

Beschreibung: Umsätze werden fälschlicherweise als Agenturgeschäfts ausgewiesen. Gemäß der Spezifikation werden diese Umsätze signiert, obwohl sie im Namen Dritter erfolgt sind. Die Weiterarbeitung erfolgt in einem anderen System als der Registrierkasse.
Analyse: Einen Agenturumsatz muss der Betreiber der Registrierkasse nicht versteuern auch wenn dieser durch ihn signiert wurde. Der Nachweis dafür muss im Rahmen eines Audits anhand des weiterverarbeitenden Systems erbracht werden. Hier ist bei Bedarf eine Verprobung mit dem System des Agenturgebers möglich. Das gilt auch im Fall des Verlusts der gespeicherten Buchungsdaten und Rückgriff auf die Summenspeicher im TIM.
Relevante Prüfung(en): 2.7 (Abgleich mit nachgelagerten Systemen) und evtl. 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Es besteht kein Risiko, dass durch dieses Vorgehen Umsätze verschleiert werden können.

3.14 Massive Stornierungen und Löschung aller Daten

Beschreibung: Es werden größere Beträge storniert, um die ausgewiesenen Umsätze zu reduzieren. Um dies nicht anhand Einzelbuchungen nachweisen zu können, werden die aufgezeichneten Buchungen gelöscht, so dass nur noch die Summenspeicher des TIM vorliegen.
Analyse: Unabhängig davon, dass der Verlust der aufgezeichneten Buchungsdaten bereits ein Verstoß gegen Vorschriften darstellt, sind die Negativbuchungen in den Summenspeichern ausgewiesen. Durch den Vergleich des Anteils der Negativbuchungen am Gesamtumsatz über alle im TIM vorhandenen Monatssummenspeicher sind Abweichungen schnell erkennbar.
Relevante Prüfung(en): 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Durch die beschriebenen Nachweismöglichkeiten ist ein Manipulationsversuch leicht erkennbar und der Effekt gut abzuschätzen. Generell sind alle Manipulationsversuche, die eine Vernichtung aller Buchungsdaten erfordern, weder in einem großen Maßstab noch wiederholt möglich.

3.15 Verwendung falscher Umsatzsteuersätze

Beschreibung: Durch die Verwendung falscher Umsatzsteuersätze werden falsche Steuern errechnet und entsprechend signiert, gedruckt und gespeichert.
Analyse: Das TIM überprüft zwar die Steuerberechnungen, speichert im Monatsspeicher den Steuersatz und vermerkt dort, wenn es eine Änderung innerhalb eines Monats gegeben hat – dies sind jedoch alles reine Plausibilitätsprüfungen, da die Steuerermittlung auf Basis der erfassten Umsätze erfolgt. Selbst bei falschen Steuersätzen ist die korrekte Ermittlung der Umsatzsteuern möglich, sogar wenn keine aufgezeichneten Buchungen mehr, sondern nur noch die Summenspeicher des TIM existieren.
Relevante Prüfung(en): Das beschriebene Vorgehen wird bei allen Prüfungsschritten angewandt.
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.16 Verwendung falscher Zeitinformationen

Beschreibung: Durch Nutzung falscher Datums- und Zeitangaben wird die Plausibilisierung von Daten bei einem Audit evtl. erschwert.
Analyse: Durch die Belegdruckpflicht, die Sequenznummer und das Einbeziehen von Datum und Uhrzeit in die Signatur fallen falsche Angaben in jedem Fall auf. Im Rahmen des Audits kann automatisch kontrolliert werden, dass alle Buchungen chronologisch aufsteigend erfasst wurden – schwer erkennbare Veränderungen sind also grundsätzlich nur in diesem Rahmen denkbar.
Relevante Prüfung(en): 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Veränderungen bieten kaum Chancen zur Verschleierung von Umsätzen und sind zudem nur in geringem Ausmaß möglich, ohne dass sie erkannt würden. Ein nennenswertes Risiko erwächst daraus nicht.

3.17 Verlust von aufgezeichneten Daten provozieren

Beschreibung: Die aufgezeichneten Buchungsdaten werden bewusst ganz oder teilweise vernichtet.
Analyse: Abgesehen von der Tatsache, dass durch einen Datenverlust gegen die gesetzlichen Aufbewahrungspflichten verstoßen wird, ist eine Abschätzung des Effekts in zwei Stufen möglich: Zum einen können die Gesamtumsätze (und einige zusätzliche Werte) zwischen zwei beliebigen Tagesabschlüssen errechnet und damit eine entsprechende Lücke in den Daten kompensiert werden. Zum anderen sind monatsgenaue Summenspeicher auf dem TIM enthalten, die auch beim Verlust von aller anderen Daten auslesbar sind.
Relevante Prüfung(en): 2.8 (Schließen von Lücken in Buchungsdaten) oder 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Durch die Möglichkeit, die Gesamtbeträge der verlorenen Buchungen zu rekonstruieren, können die Auswirkungen der Manipulation sehr weitgehend reduziert werden.

3.18 Zerstörung des TIMs

Beschreibung: Das TIM wird bewusst zerstört, um eine Signatur von neuen Buchungen unmöglich zu machen und um die darauf gespeicherten Daten zu vernichten.
Analyse: Aufgrund der konzeptionell vorgesehenen Möglichkeit, Reserve-TIMs auszugeben, sollte ein defektes TIM keinen Begründung darstellen, Umsatzdaten selbst für einen kurzen Zeitraum nicht zu signieren. Der Datenverlust ist unkritisch, solange noch die gespeicherten, signierten Buchungen vorliegen.
Relevante Prüfung(en): Keine
Restrisiko: Ein zerstörtes TIM liefert weder eine tragfähige Begründung dafür, keine Signaturen mehr zu erstellen noch dafür, keine Daten vorlegen zu können.

3.19 Vernichtung aller Daten und des TIMs

Beschreibung: Ein Steuerpflichtiger vernichtet bewusst alle aufgezeichneten Daten (inklusive der Datensicherungen) und das TIM.
Analyse: In diesem Fall ist natürlich kein Rückgriff auf die Daten oder eine Rekonstruktion möglich. Da der Verlust aller Daten einen mehrfachen Verstoß gegen Vorschriften darstellt, sollte der Nachweis von Vorsatz oder grober Fahrlässigkeit generell einfach möglich sein. Mit einer technisch möglichen, regelmäßigen Online-Übertragung wesentlicher Daten ließe sich auch in so einem Fall eine gute Abschätzung der Umsätze vornehmen.
Relevante Prüfung(en): 2.10 (Rückgriff auf online eingereichte Daten)
Restrisiko: Die Vernichtung aller Daten ist praktisch nicht zu verhindern. Es wäre noch zu bewerten, ob die Zerstörung einer Smartcard eine geringere „Hemmschwelle“ bedingt als die Zerstörung einer klassischen Fiskalkasse bzw. eines Fiskaldruckers. Per Online-

Meldung der Daten lässt sich auch dieses Restrisiko praktisch vollständig ausschließen.

3.20 Nutzung von Reserve-TIMs

Beschreibung: Überzählige (also momentan nicht genutzte) TIMs werden genutzt, um einen Teil der Umsätze gültig zu signieren – die Daten der Reserve-TIMs werden jedoch bei einem Audit nicht vorgelegt.
Analyse: Bei einem Audit werden die Daten aller für einen Steuerpflichtigen ausgegebenen TIMs geprüft. Dabei ist anhand der aktuellen Sequenznummern und der Summenspeicher der TIMs, die nicht im täglichen Einsatz sind, leicht festzustellen, ob die Daten vollständig sind oder ob einzelne TIMs bisher noch gar nicht benutzt wurden.
Relevante Prüfung(en): 2.5 (Prüfung ungenutzter TIMs)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.21 Einsatz von zwei Kassen – nur das Journal einer Kasse wird zur Prüfung vorgelegt

Beschreibung: Ein Steuerpflichtiger verwendet zwei Kassen, die beide mit einem TIM bestückt sind. Nur die Daten einer Kasse werden bei einer Prüfung vorgelegt. Rein technisch könnte dies auch mit einer Kasse, die mit zwei TIMs ausgestattet ist, versucht werden.
Analyse: Da ohne ein zweites TIM keine gültigen Signaturen erstellt werden können, entspricht die Analyse genau dem Punkt 3.20.
Relevante Prüfung(en): Siehe 3.20.
Restrisiko: Siehe 3.20.

3.22 Diebstahl eines TIMs

Beschreibung: Ein gestohlenes TIM wird zu Erstellung rechnerisch gültiger Signaturen verwendet.
Analyse: Über verschiedene Wege (signierte Identifikation des Steuerpflichtigen als Teil der gedruckten und aufgezeichneten Daten, Zertifikat, Sperrung der Zertifikate für als gestohlen gemeldete TIMs) ist eindeutig erkennbar, dass Belege nicht korrekt signiert wurden.
Relevante Prüfung(en): Alle Prüfungen, bei denen Signaturen verifiziert werden – also 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege), 2.3 (Schnelle Prüfung der gespeicherten Buchungen) und 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Wenn lediglich gedruckte Belege geprüft werden, ist das Risiko analog zu Punkt 3.3 zu bewerten, bei einer Prüfung gespeicherter Buchungsdaten ist ein Restrisiko praktisch nicht vorhanden.

3.23 TIM wird fälschlicherweise als gestohlen gemeldet

Beschreibung: Ein TIM wird fälschlicherweise als gestohlen gemeldet, jedoch weiter zur Erstellung von Signaturen benutzt.
Analyse: Bei jeder Prüfung von gespeicherten Buchungen oder gedruckten Belegen sind alle nach dem vermeintlichen Datum des gemeldeten Diebstahls signierten Vorgänge eindeutig erkennbar (das ist eine der Funktionen der PKI). Damit besteht genau das gleiche Entdeckungsrisiko wie beim Sachverhalt unter Punkt 3.3.
Relevante Prüfung(en): Analog zu 3.22.
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.24 „Abhören“ der Kommunikation mit dem TIM

Beschreibung: Durch Erfassung des Datenaustausches zwischen Registrierkasse und TIM und eventuellen Eingriff in die Kommunikation werden Erkenntnisse für einen Angriff gewonnen bzw. Daten manipuliert.
Analyse: Die Kommunikation zwischen Kassen und TIM ist nicht verschlüsselt und folgt einem offengelegten Verfahren. Dies ist möglich, da die Sicherheit ausschließlich auf dem Signaturverfahren und der festen Verknüpfung verschiedener Schritte (Signatur, Verwaltung der Sequenznummer, Plausibilitätsprüfung der Daten, Aktualisierung der Summenzähler) im TIM basiert.
Relevante Prüfung(en): keine
Restrisiko: Ein Angriff in der beschriebenen Form ist wirkungslos, solange dadurch keine Angriffe auf den Signaturalgorithmus oder die Smartcard selbst möglich sind.

3.25 Erstellung von Signaturen mit einem "TIM-Nachbau" oder einer Emulation

Beschreibung: Eine Registrierkasse erstellt kryptografisch korrekte Signaturen mit einem „nachgebauten“ TIM bzw. einer Emulation.
Analyse: Da das gesamte Verfahren offengelegt ist, kann die Funktion des TIM mit vertretbarem Aufwand nachgebildet werden. Die Sicherheit basiert jedoch auf dem geheimen Schlüssel, der im TIM (und nur dort) gespeichert ist. Dieser Schlüssel ist nicht auslesbar – auf dieser Tatsache basiert die Sicherheit aller

mit Hilfe von Smartcards umgesetzten kryptografischen Lösungen. Die Erstellung eines eigenen geheimen Schlüssels wäre wirkungslos, da der zugehörige öffentliche Schlüssel nicht als Zertifikat verfügbar ist (durch das Zertifikat bestätigt eine vertrauenswürdige Stelle, dass der dort enthaltene öffentliche Schlüssel korrekt und gültig ist sowie zum Steuerpflichten gehört).
Relevante Prüfung(en): Alle Prüfungen, bei denen Signaturen verifiziert werden – also 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege), 2.3 (Schnelle Prüfung der gespeicherten Buchungen) und 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

4 Gesamtbetrachtung

Die Sicherheit des gesamten Systems basiert vor allem auf geeigneten Kontrollen und Audits. Verfahren und Technik des INSIKA-Konzepts bergen nur minimale Restrisiken. Wesentlich sind vor allem die Kontrollen, mit denen erreicht werden muss, dass die bei jedem System mögliche Nicht-Benutzung mit ausreichender Wahrscheinlichkeit entdeckt wird. Das INSIKA-Konzept macht diese Kontrollen einfach und sicher.

5 Ausblick

Wie bereits in der Einleitung erörtert, stellen die hier beschriebenen Punkte nur einen Ausschnitt und eine Momentaufnahme der Sicherheitsanalyse dar. Im Rahmen des Abschlusses der Sicherheitsanalyse erfolgen eine Vertiefung der Analyse und die Einbeziehung weiterer Risiken und Angriffsmöglichkeiten.

Nationale Umsetzung der europäischen Messgeräterichtlinie (MID) für Taxameter

Frank Jäger, Helga Grohne
Physikalisch-Technische Bundesanstalt (PTB)
Bundesallee 100, 38116 Braunschweig
{frank.jaeger, helga.grohne}@ptb.de

Während bis 2004 für Taxameter in Deutschland ausschließlich deutsche Vorschriften galten, gibt es seit dem Inkrafttreten der europäischen Messgeräterichtlinie (MID) in ganz Europa weitgehend vereinheitlichte Regeln. Auf der Basis dieser Regeln durchläuft der Hersteller ein europaweit gültiges Zertifizierungsverfahren, üblicherweise in Form einer Baumusterprüfung, die es ihm ermöglichen muss, eine europaweit einheitliche Taxameter-Bauart zu vertreiben. Diese Regeln lassen allerdings zu, dass national der Einsatz von national spezifizierten Zusatzeinrichtungen – wie beispielsweise auch ein Kassensystem – obligatorisch wird. Voraussetzung hierfür ist allerdings, dass die Zusatzeinrichtung vom Taxameter nur die entsprechend der MID spezifizierten Daten benötigt, so dass die nationalen Anforderungen zu keinen Handelshemmnissen für die Taxameter führen.

1 Internationale Vorschriften, Normen und Gremien für Taxameter

1.1 MID Measuring Instruments Directive (2004/22/EG)

Seit einigen Jahren gilt für Taxameter (wie für einige andere Messgerätearten) die „Richtlinie des europäischen Parlaments und des Rates vom 31.3.2004 über Messgeräte“ als Grundlage für die europaweite Verwendung. Abgekürzt wird sie üblicherweise MID genannt (Measuring Instruments Directive). Diese Richtlinie umfasst einen allgemeinen Teil und spezielle Anhänge für die jeweiligen Messgerätearten. Für Taxameter ist dies der Anhang MI-007. Der wesentliche Vorteil für Hersteller von Taxametern besteht darin, dass anstelle von separaten Zulassungsverfahren in jedem Mitgliedstaat der EU – die in der Vergangenheit ein Handelshemmnis darstellen konnten – nun nur noch ein Zertifizierungsverfahren erforderlich ist. Zusätzlich sind für den Hersteller anstelle von Bauartprüfungen andere Konformitätsbewertungsverfahren möglich, wenn er über ein entsprechendes Qualitätsmanagement-System verfügt und dieses von der Benannten Stelle zertifiziert ist. Näheres zur MID ist über das Internet verfügbar [1].

Auch wenn die MID nicht unmittelbaren Gesetzescharakter hat, so waren alle Mitgliedstaaten der EU verpflichtet, die MID in nationales Recht umzusetzen. Diese Umsetzung ist in Deutschland mit dem Stichtag 30.10.2006 erfolgt (siehe Abschnitt 2), auf die Erläuterung von Übergangsvorschriften kann in diesem Beitrag verzichtet werden.

1.2 OIML

OIML (Organisation Internationale de Métrologie Légale) hat sich zum Ziel gesetzt, das gesetzliche Messwesen weltweit (d.h. deutlich über die EU hinausgehend) auf freiwilliger Basis zumindest in gewissem Umfang zu vereinheitlichen. Zu diesem Zweck erstellen Expertengruppen aus den Zulassungsbehörden Dokumente, die für die Gesetzgeber als Empfehlungen für nationale Regelungen dienen sollen. Im Jahr 2007 wurden nach mehrjähriger Arbeit entsprechende Empfehlungen für Taxameter „R 21 (2007) Taximeters“, siehe [2] veröffentlicht, sie lösen die nicht mehr zeitgemäßen Empfehlungen aus dem Jahr 1973 ab. Die Empfehlungen beinhalten zum einen etwas detailliertere Anforderungen als die MID und zum anderen

PTB-Bericht IT-18
doi:10.7795/210.20130206a

einen Prüfplan, der bei Bauartprüfungen angewendet werden kann.

1.3 WELMEC

Die europäische Organisation WELMEC (Western European Legal Metrology Cooperation) möchte für eine Harmonisierung des gesetzlichen Messwesens im Rahmen europäischer Regeln bzw. Gesetze sorgen. Zu diesem Zweck wurden verschiedene Expertengruppen eingesetzt, im Bereich der Taxameter ist insbesondere die WG8 subgroup „taximeters“ zu nennen, die von Deutschland geleitet wird. Die bisher wichtigste Arbeit dieser subgroup war die Erstellung einer detaillierten Liste mit Querverweisen (sogenannte cross-reference table) zwischen den Anforderungen der MID (einschließlich des Anhangs 007) und denen der OIML-Empfehlung R 21 [3]. Dies ermöglicht einer benannten Stelle die verlässliche Anwendung der OIML R 21 als Basis für eine MID-Zertifizierung. Die Kooperation in WELMEC und die Anwendung von WELMEC Dokumenten ist für die Vertreter der Mitgliedsstaaten grundsätzlich freiwillig. Die besondere Bedeutung der OIML R 21 und der zugehörigen cross-reference table für Taxameter besteht darin, dass die EU-Kommission sich die Anwendung der OIML R 21 und der zugehörigen cross-reference table zu eigen macht.

1.4 CENELEC

Neben der OIML-Empfehlung R 21 gibt es für Taxameter auch eine in einer CENELEC-Arbeitsgruppe (Comité Européen de Normalisation Electrotechnique) entworfene europäische Norm EN 50148 „electronic taximeters“ aus dem Jahr 1996. Diese Norm passte allerdings in vielen Details nicht zu den Anforderungen der MID und wird auch von der EU-Kommission nicht als normatives Dokument und damit nicht als verbindliche Grundlage für MID-Zertifizierungen angesehen. Aktuell gibt es Bestrebungen zur Überarbeitung dieser Norm, ein Abschluss ist aber nach unserem Kenntnisstand noch nicht abzusehen.

2 Nationale Vorschriften, Normen und Gremien für Taxameter in Deutschland

2.1 Personenbeförderungsgesetz

Das Personenbeförderungsgesetz (PBefG) regelt Grundsätzliches über die entgeltliche und geschäftsmäßige Beförderung von Personen mit Taxen und anderen Fahrzeugen. Insbesondere ist hier festgelegt, dass die Genehmigung und die Kontrolle des Betriebs von Taxen Ländersache ist, so dass es im Detail von Bundesland zu Bundesland unterschiedliche Rechtsverordnungen geben kann.

2.2 BOKraft

Die Verordnung über den Betrieb von Kraftfahrunternehmen im Personenverkehr (abgekürzt BOKraft genannt) regelt bundesweit einheitlich wichtige Details über die Ausstattung von Taxen. Insbesondere ist hier festgelegt, dass im Taxi die Verwendung von Taxametern vorgeschrieben ist.

2.3 Vorschriften des Eichwesens

Die detaillierteren Anforderungen über die Funktionsweise eines Taxameters und über die Eichpflicht ergeben sich in Deutschland aus den folgenden Vorschriften des Eichwesens:

- Gesetz über das Mess- und Eichwesen (Eichgesetz)
- Eichordnung -Allgemeine Vorschriften- (EO)
- Abschnitt 2 der Anlage 18 zur Eichordnung EO 18-2 „Taxameter in Kraftfahrzeugen“ mit
  - Teil 1 „EG-Anforderungen“
  - Teil 2 „Innerstaatliche Anforderungen“
  - PTB-A 18.21 „Quittungsdrucker für Taxameter“

Es handelt sich dabei im Wesentlichen um die Umsetzung der MID in deutsches Recht. Diese Umsetzung besteht aus deutschen Regelungen, die ggf. auch vom deutschen Gesetz- bzw. Verordnungsgeber geändert werden können. Bei Änderungen oder Ergänzungen muss aber darauf geachtet werden, dass sie nicht der europäischen Richtlinie MID widersprechen. Insbesondere zusätzliche Anforderungen an das von der MID erfasste Kerngerät (s.u.) sind nicht zulässig, da diese als Handelshemmnisse bzw. als unzulässige Bevorzugung einzelner Firmen aufgefasst werden können.

Benannte Stelle in Deutschland für Zertifizierungen von Taxametern ist die PTB als Bundesbehörde, für die Eichung der Geräte (auch der in anderen EU-Mitgliedsstaaten zertifizierten Bauarten) sind die Eichbehörden der Länder zuständig. Zur Abstimmung der Länder untereinander und ggf. auch mit der PTB dient insbesondere der Arbeitsausschuss „Fahrpreisanzeiger“ der Arbeitsgemeinschaft Mess- und Eichwesen.

3 Definition eines Taxameters

Bei den Vorschriften für Taxameter ist eine der wichtigsten Fragen, für welche Komponenten des Gesamtgerätes nationale und für welche europäische gelten. Bild 1 erläutert, welche Komponenten bzw. welche Funktionalitäten von der MID erfasst sind und für welche nationale Regelungen vorgesehen sind. Der Anhang MI-007 enthält zu diesem Zweck die folgende Definition für ein Taxameter:

> Ein Taxameter ist ein Gerät, das zusammen mit einem Signalgeber betrieben wird und mit diesem ein Messgerät bildet (der Geber fällt nicht in den Geltungsbereich der Richtlinie).
>
> Dieses Gerät misst die Fahrtdauer und errechnet die Wegstrecke auf der Grundlage eines von einem Wegstreckensignalgeber übermittelten Signals. Außerdem errechnet es den für eine Fahrt zu entrichtenden Fahrpreis auf der Grundlage der errechneten Wegstrecke und/oder der gemessenen Fahrtdauer und zeigt diesen Preis an.

Zur Unterscheidung sind in der Eichordnung die Formulierungen „Taxameter“ für das Kerngerät und „Taxameter in Fahrzeug“ für das Gerät einschließlich Wegstreckensignalgeber gewählt worden.

4 Zählwerke

Die o.a. Definition eines Taxameters erläutert seine Funktion als Messgerät (mit Anzeige) für den Fahrpreis. Diese Hauptfunktion betrifft den üblichen geschäftlichen Verkehr in einem Taxi zwischen Fahrgast und Fahrer. Neben dieser Hauptfunktion ist aber bereits in der MID (Nummer 15.1) eine weitere Funktion festgelegt, die insbesondere der Abrechnung zwischen dem Fahrer und dem Taxenunternehmer dient, die aber ggf. auch für Kassensysteme von erheblicher Bedeutung sein kann.

Ein Taxameter muss mit nicht rückstellbaren Zählwerken für alle folgenden Werte ausgestattet sein:

- gesamte vom Taxi zurückgelegte Wegstrecke,
- gesamte mit Fahrgästen zurückgelegte Wegstrecke,
- Gesamtzahl der ausgeführten Fahrgast-Übernahmen,
- Gesamtsumme der in Rechnung gestellten Zuschläge,
- Gesamtsumme der als Fahrpreis in Rechnung gestellten Beträge.

Üblicherweise beinhalten Taxameter weitere, für den Taxenunternehmer vorgesehene Zählwerke (insbesondere für die Schicht eines Fahrers), diese zusätzlichen Zählwerke dürfen aber nicht in nationalen Vorschriften für Taxameter gefordert werden.

5 Zusatzgeräte und zugehörige Schnittstelle

Taxameter werden in der Praxis mit verschiedenen Zusatzgeräten betrieben, die nationaler Gesetzgebung unterliegen (siehe Abbildung 1). Hierzu zählen beispielsweise ein Dachzeichen, ein Quittungsdrucker oder ein Bordcomputer, solche Zusatzgeräte können in den einzelnen Staaten optional oder auch obligatorisch sein.

Ein Spielraum für nationale Forderungen nach Zusatzgeräten ist in der MID ausdrücklich vorgesehen (Punkt 4):

Aufgrund nationaler Rechtsvorschriften besteht möglicherweise die Pflicht, bestimmte Geräte an die Schnittstelle(n) eines Taxameters anzuschließen.

Zur Umsetzung sind in der MID als Basis für nationale Regelungen zwei Forderungen an das Kerngerät spezifiziert:

- In diesem Fall muss es möglich sein, mittels einer Sicherheitseinstellung den Betrieb des Taxameters automatisch zu verhindern, wenn das erforderliche Gerät nicht vorhanden ist oder nicht vorschriftsmäßig funktioniert.
- Ein Taxameter muss über eine (oder mehrere) geeignete gesicherte Schnittstelle(n) folgende Daten übertragen können:
  - Betriebseinstellung, permanent
  - Zählwerksdaten gemäß Nummer 15.1 auf Abruf
  - allgemeine Daten, auf Abruf
  - Preisdaten einer Fahrt (s.u.) automatisch am Ende der Fahrt
  - Tarifdaten, auf Abruf

Die Schnittstelle des von der MID erfassten Kerngerätes für Zusatzeinrichtungen ist damit im Wesentlichen spezifiziert, darüber hinausgehende nationale Anforderungen sind nicht zulässig, um Handelshemmnisse zu vermeiden. Eine kryptografische Sicherung der Daten ist dabei bisher nicht gefordert (weder in der MID, noch in OIML R 21 oder in EN 50148) und auch noch nicht Stand der Technik bei Taxametern.

Die Zusatzgeräte können als separates Gerät oder in einem gemeinsamen Gehäuse mit dem Taxameter ausgeführt sein.

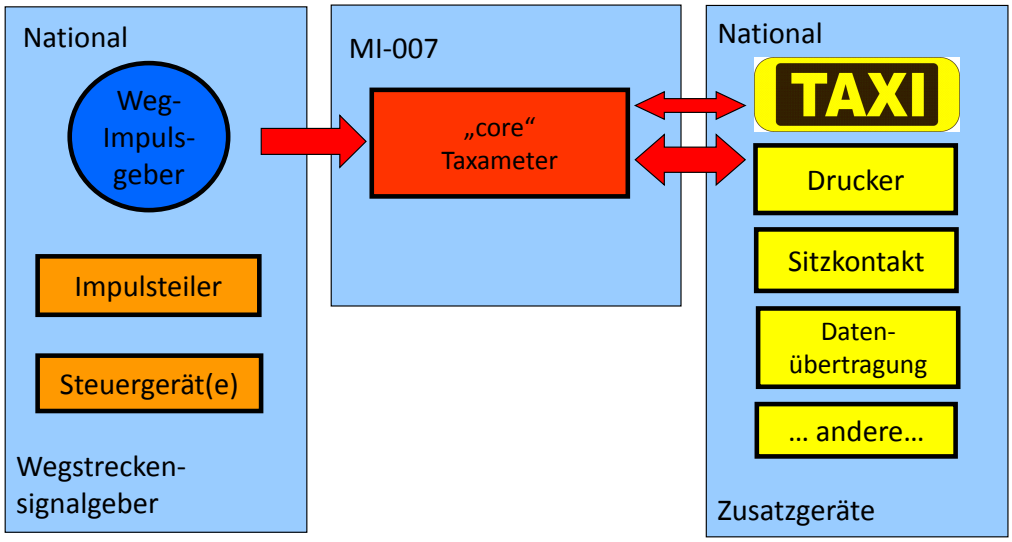


Abbildung 1: Blockschaltbild eines Taxameters und Gültigkeitsbereich der MID

Sind die Geräte in einem gemeinsamen Gehäuse untergebracht, ist eine klare Trennung der Hard- und auch der Softwareteile wichtig, um eine effektive Prüfung des Kerngerätes im Rahmen einer MID-Zertifizierung zu ermöglichen. Näheres zu einer geeigneten Software-Trennung ist dem WELMEC softwareguide 7.2 zu entnehmen [4].

Für die Gesetzgeber in den verschiedenen Ländern wäre ein Überblick über alle in der EU geforderten Zusatzgeräte und über die zugehörigen detaillierten Anforderungen an diese Zusatzgeräte hilfreich. Zu diesem Zweck hat die WELMEC WG 8 subgroup „taximeters“ eine Abfrage an die Mitgliedsstaaten gestartet. Die wichtigste Zusatzeinrichtung ist ein Drucker; Der Einsatz eines Druckers ist inzwischen in mehr als 10 Ländern vorgeschrieben und in den meisten Ländern zulässig.

6 Vom Taxameter gelieferte Daten

6.1 Zählwerksdaten

Ein Taxameter muss entsprechend der MID die o.a. (Abschnitt 4) erläuterten Zählwerke nicht nur anzeigen, sondern auch als Daten über eine Schnittstelle zur Verfügung stellen. Auf diese Weise kann ein angeschlossenes Kassensystem die für die Ermittlung der Steuern wichtigsten Daten erhalten.

6.2 Daten einer Fahrt

Für eine detailliertere Kontrolle muss das Taxameter entsprechend der MID neben den Zählwerksdaten über eine Schnittstelle am Ende jeder Fahrt die folgenden Daten über die jeweilige Fahrt liefern:

- in Rechnung gestellte Gesamtsumme (einschließlich Zuschlägen)
- Fahrpreis
- Berechnung des Fahrpreises
- Zuschlag
- Datum
- Uhrzeit des Fahrtbeginns
- Uhrzeit des Fahrtendes
- zurückgelegte Strecke

6.3 Allgemeine Daten

Zusätzlich muss ein Taxameter entsprechend der MID über die Schnittstelle folgende allgemeine Daten auf Abruf zur Verfügung stellen:

- Konstante des Wegstreckensignalgebers (Parameter zur Angleichung des Taxameters an den Radumfang)
- Datum der eichtechnischen Sicherung
- Taxikennung
- Echtzeit
- Tarifkennung

7 Quittungsdrucker für Taxameter in Deutschland

Aktuell sind in Deutschland Quittungsdrucker eine optionale Zusatzeinrichtung. Wenn ein Quittungsdrucker eingesetzt wird, so ist er eichpflichtig; auf diese Weise sollen Betrugsmöglichkeiten für den Fahrer minimiert werden. Die PTB-Anforderungen 18.21 enthalten detailliertere Spezifikationen für den Drucker. Neben

der Störfestigkeit gegenüber den in der Praxis im Taxi relevanten Umwelteinflüssen sind dies vor allem Anforderungen an den Umfang und das Layout von Ausdrucken, insbesondere der ausgedruckten Quittungen, Näheres siehe [5].

8 Konsequenzen für Kassensysteme und Ausblick

Für ein Kassensystem stellt ein auf Basis der MID zugelassenes Taxameter eine Reihe von wichtigen Daten zur Verfügung. Diese Daten müssen aber, darauf sei hier nochmals hingewiesen, nicht kryptografisch gesichert sein. Sollte ein Kassensystem kryptografisch gesicherte Daten benötigen, so ergäbe sich eine zusätzliche Anforderung an das MID-Taxameter. Hierfür wäre eine Ergänzung der MID erforderlich. Da Kassensysteme oder ähnliche Geräte zur amtlichen Kontrolle in anderen Mitgliedsstaaten bereits vorgeschrieben sind, wären vermutlich auch andere Mitgliedsstaaten an einer kryptografischen Sicherung interessiert, so dass eine entsprechende Initiative durchaus Aussicht auf Erfolg hätte.

Literatur

[1] Rat der Europäischen Union. *Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte*. Amtsblatt der Europäischen Union L135 vom 30.04.2004. März 2004. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0022:DE:NOT.

[2] OIML. *International Recommendation OIML R21 Taximeters. Metrological and technical requirements, test procedures and test report format*. Version Edition 2007. Organisation Internationale de Métrologie Légale, 2007. URL: http://www.oiml.org/publications/.

[3] WELMEC. *WELMEC 8.17: Guide for Measuring Instruments Directive 2004/22/EC Taximeters Corresponding Tables OIML R21 - MID-007 II*. Version Issue 1. European Cooperation in Legal Metrology WG 8, Sep. 2008. URL: http://www.welmec.org/latest/guides/817.html.

[4] WELMEC. *WELMEC 7.2: Software Guide (Measuring Instruments Directive 2004/22/EC)*. European Cooperation in Legal Metrology WG 7. URL: http://www.welmec.org/latest/guides/72.html.

[5] PTB. *PTB-Anforderungen PTB-A 18.21: Quittungsdrucker für Taxameter*. Physikalisch-Technische Bundesanstalt, Nov. 2006. URL: http://www.ptb.de/de/org/q/q3/q31/.

INSIKA im Taxi – von der Idee zum Serieneinsatz

Barbara Stering
HALE electronic GmbH
Eugen-Müller-Straße 18, 5020 Salzburg, Österreich
barbara.stering@hale.at

Zunehmend mehr Länder stellen Fiskalanforderungen an Taxameter. Dabei wird oft ein für Taxameter schlecht passendes Registrierkassensystem vorgeschrieben. INSIKA bietet erstmals eine technologisch aktuelle, durch kryptografisch gesicherte Datenaufzeichnung und -speicherung, einfach kontrollierbare Fiskallösung.

Auf Basis der in neuen Taxametern vorhandenen MID-Schnittstelle wurde ein Pilotprojekt durchgeführt und die Anwendbarkeit der Sicherheitslösung im Taxibereich getestet.

Das Projektergebnis war positiv, wird von der Hamburger Behörde für Stadtentwicklung und Umwelt (Verkehrsgewerbeaufsicht) zur Konzessionsverlängerung gefördert und ist bereits im Serieneinsatz.

1 Über HALE electronic GmbH

HALE ist europaweit führend in der Entwicklung und Herstellung elektronischer Taxametersysteme. Taxameter und -zubehör bis hin zu Abrechnungs- und Flottenmanagementsystemen werden in 40 Länder vertrieben. Entwicklung, Produktion und Vertrieb erfolgt mit 85 Personen am Standort Salzburg. HALE ist unter anderem Marktführer im Bereich Taxameter in Deutschland und Österreich.

2 Einleitung

Ausgangspunkt für das Projekt war die Idee der PTB, das unter ihrer Leitung entwickelte INSIKA-Verfahren nicht nur in Registrierkassen, sondern auch in Taxen einzusetzen, um damit auch im Taxi-Gewerbe mit dieser anerkannt sicheren Lösung den Anforderungen des deutschen Fiskus (BMF) gerecht werden zu können.

HALE hat bereits einige „Fiskaltaxameter“ für Länder wie Ungarn, Tschechien und Griechenland entwickelt. Den bisherigen Fiskallösungen im Taxibereich ist gemein, dass diese auf größtenteils geringfügig angepassten Gesetzen für Registrierkassen mit Fiskalspeicher basieren, in denen u.a. die Datenspeicherung in einem vergossenen EPROM gefordert wird. Meist ist die Marktüberwachung schlecht organisierbar oder wird teilweise gar nicht vorgenommen.

Im Gegensatz dazu ermöglicht INSIKA eine kryptografisch gesicherte Aufzeichnung, die zudem einfach kontrollierbar ist.

3 Pilotprojekt ‚INSIKA im Taxi’ – Phase 1

Ziel der ersten Phase des Pilotversuchs war es, INSIKA gemäß den Vorgaben des BMF für ‚Aufbewahrung digitaler Unterlagen bei Bargeschäften’ [1] im Taxibereich zu definieren, sowie nach Erstellung der erforderlichen Hardware, Software und Serverkomponenten einen ersten Pilotbetrieb mit 10 Fahrzeugen zu gestalten.

Ein Taxameter als eichrelevantes, ortsunabhängiges Einzelgerät stellt andere Bedingungen an INSIKA als ein Registrierkassensystem. Als erstes musste ein INSIKA-Profil [2] für die zusätzlich geforderten Daten, wie Schichtdaten oder Zählerstände für Total- und Besetztkilometer, spezifiziert werden. Auch die Einbeziehung des entsprechenden Mehrwertsteuer-Satzes stellt am Taxameter ein Problem dar, da die in der MID (europäische Taxameterrichtlinie [3]) vorgeschriebenen Schnittstelle eine Übermittlung von Mehrwertsteuer-Daten nicht vorsieht.

Das INSIKA-Modell wurde für den Einsatzbereich „Taxi“ angepasst und erweitert. Aufgrund von fehlenden Vorschriften bezüglich Drucker im Taxi, wur-

doi:10.7795/210.20130206a

de auf diesen vorerst verzichtet und statt dessen eine online-Lösung entworfen.

Auf Basis der von HALE bereits im Feld eingesetzten MID-Taxameter wurde für die vorhandene MID-Schnittstelle ein entsprechendes Zusatzgerät entworfen, mit dem die Daten vom Taxameter empfangen, mittels TIM signiert und an einen Server abgeladen werden können.

Hierzu musste u.a. der Einsatz der INSIKA-Smartcard im automotiven Umfeld untersucht und die Hard- und Software der im Fahrzeug einzusetzenden Komponenten entsprechend ausgelegt werden. Dieses Zusatzgerät, kurz SEI für Signiereinheit (siehe Abbildung 1), liest also die relevanten Daten des Taxameters bei jedem Statuswechsel an der MID-Schnittstelle aus, gibt diese zur Signierung an die INSIKA-Smartcard weiter und übermittelt die signierten Daten per GSM an ein Datencenter (Ablauf siehe Abbildung 2).

Abbildung 1: MID-Taxameter und Signiereinheit

HALE hat innerhalb eines halben Jahres die Hardware inklusive Firmware der SEI als Prototyp entwickelt, die Firma Tesymex einen ersten Prototypen des Datenservers und Client-Programmes. Somit konnten bereits nach kurzer Zeit die ersten zehn Taxifahrzeuge in Hamburg und Berlin in den Pilotbetrieb gehen.

In der ersten Pilotphase wurden Erfahrungen wie Systemverhalten bei fehlender GSM-Verbindung oder Serverausfall gesammelt, sowie weitere Verbesserungen vorgenommen. Es konnte prinzipiell die Einsatzmöglichkeit von INSIKA im Taxi erfolgreich verifiziert werden.

4 Pilotprojekt ‚INSIKA im Taxi' – Phase 2

In der zweiten Pilotphase wurde das Hauptaugenmerk auf die betrieblichen Abläufe und Prozesse gelegt: So galt es zunächst, das Betriebsmodell zu entwickeln

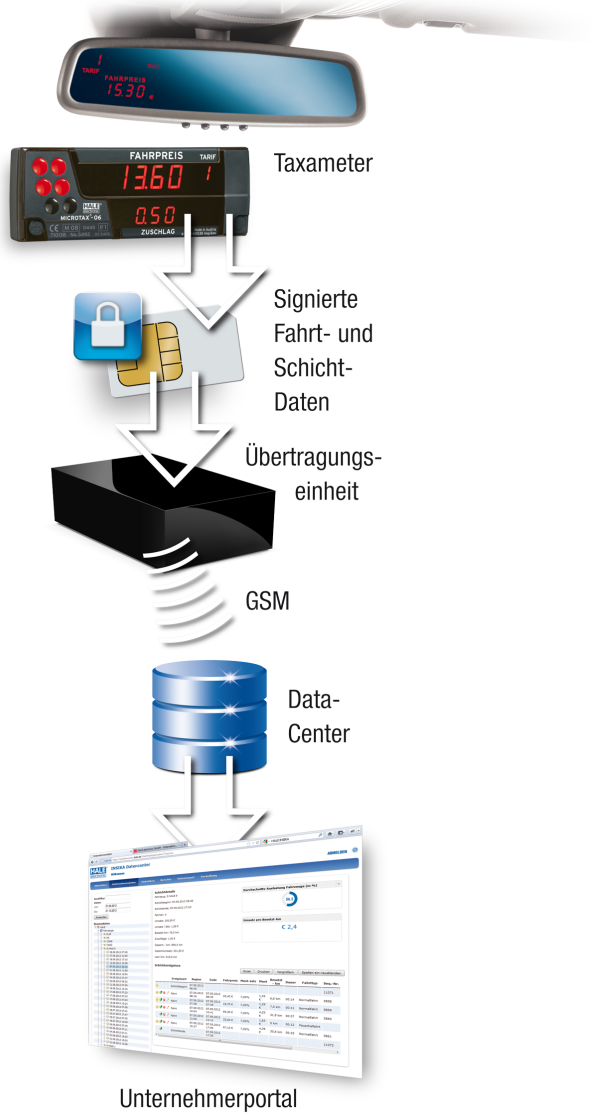


Abbildung 2: Ablauf INSIKA System im Taxi

und einem Echtbetrieb zu unterziehen, sowie Abläufe wie Bestellung der INSIKA-Smartcard, deren Aktivierung und den Verbau der Geräte im Fahrzeug zu synchronisieren.

Die Datenübertragung wurde mit HTTPS [4] abgesichert, ein einfacher Wechsel des GSM-Providers und auch Datendienstleisters musste vorgesehen werden. Die Einbauwerkstätten wurden eingeschult, sowie ein Tool zum Softwareupdate der Geräte wurde entwickelt. Die SEI wurde als Nullserie gefertigt und der Datenserver wurde weiter ausgebaut.

Während dieser Pilotphase befanden sich dauerhaft zwischen elf und zuletzt achtzehn Fahrzeuge im Einsatz. Es wurden 16.000 Datensätze empfangen. 5.000 Datensätze wurden detailliert analysiert und erfolgreich verifiziert.

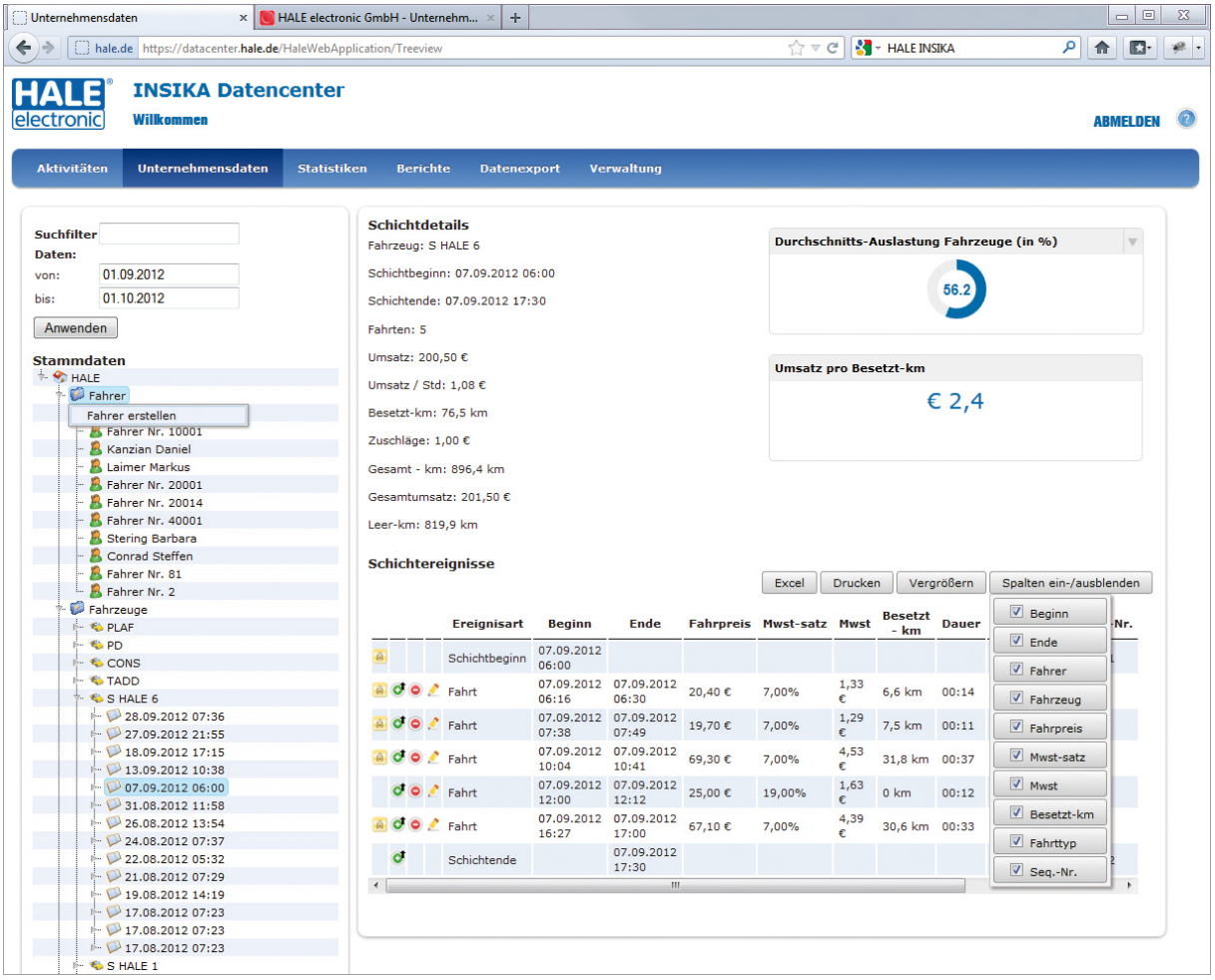


Abbildung 3: HALE Datencenter: Unternehmer-Webportal

Die notwendigen Zusatzgeräte zum Taxameter (SEI und Modem) wurden allen fahrzeugrelevanten Prüfungen unterzogen und entsprechend zugelassen.

Es existiert nunmehr eine Lösung, die die Investitionen der Taxenbetriebe der letzten Jahre wie MCT-06 und Spiegeltaxameter SPT-02 sichert und eine Nachrüstlösung ermöglicht.

5 Serieneinsatz

Die Freie Hansestadt Hamburg fördert die Anschaffung und den Einbau von Geräten, die geeignet sind, die im Taxameter erzeugten Daten unveränderbar zu sichern und auf externe Speichermedien zu übertragen.

Diese Anforderungen werden von der oben beschriebenen Implementierung von INSIKA im Taxi erfüllt und werden von der Verkehrsgewerbeaufsicht zur einfachen Überprüfung hinsichtlich der Konzessionsverlängerung genutzt.

Die SEI wird nun in zwei Ausführungen produziert, als Variante mit inkludiertem Modem, sowie als kostengünstigeres Einzelgerät, welches in Verbindung mit einem im Fahrzeug befindlichen Modem (z.B: Datenfunk-Modem) eingesetzt werden kann.

Mittlerweile gibt es außer Tesymex auch weitere Datenserveranbieter, die über die beschriebenen offenen Schnittstellen problemlos mit HALE Taxametern und den entsprechenden INSIKA-Zusatzgeräten integrieren.

Für HALE Kunden, die bisher HALE-Abrechnungssoftware oder andere HALE-Lösungen benutzt haben, bietet HALE nun nach verstärkter Anfrage ebenfalls einen Serverbetrieb für die sichere Datenverwahrung an. Der Zugriff erfolgt installations- und systemunabhängig über einen Webbrowser (siehe Abbildung 3).

6 Ausblick

INSIKA bietet im Taxenbereich eine technologisch aktuelle, kryptografisch gesicherte Datenaufzeichnung und –speicherung, die zudem einfach kontrollierbar ist.

Der Trend geht zur Integration der INSIKA-Smartcard und somit der Signierung der Daten bereits im Taxameter. Dies kann jedoch aus derzeitiger Sicht nur auf freiwilliger Basis erfolgen, da die gesetzliche Grundlage fehlt. HALE wird diese Integration in zukünftigen Taxametermodellen bereits vorsehen.

Die Vorgehensweise bei Sondertarifen, die nicht am Taxameter abgebildet werden (Vereinbarungen mit Krankenkassen etc.), sowie der Einsatz in Mietwägen ist politisch sowie eichrechtlich noch abzuklären.

INSIKA ist sicherlich gesamteuropäisch gesehen eine große Chance, fiskalischen und weiteren behördlichen Anforderungen auf bestmöglicher Weise gerecht zu werden. Hierzu sollte jedoch, wie in INSIKA für Kassen vorgesehen, auch im Taxi der Belegdruck mit INSIKA-Signatur Pflicht sein, um die Marktüberwachung noch weiter zu vereinfachen.

Literatur

[1] BMF. *BMF-Schreiben vom 26.11.2010 - IV A 4 - S 0316/08/10004-07 - (2010/0946087) - Aufbewahrung digitaler Unterlagen bei Bargeschäften*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Nov. 2010. URL: http://bundesfinanzministerium.de/.

[2] INSIKA-Projekt. *INSIKA Profil Taxameter*. Version T.1.1.0-10. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: http://insika.de/.

[3] Rat der Europäischen Union. *Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte*. Amtsblatt der Europäischen Union L135 vom 30.04.2004. März 2004. URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0022:DE:NOT.

[4] E. Rescorla. *RFC 2818: HTTP Over TLS*. The Internet Engineering Task Force (IETF), Mai 2000. URL: http://tools.ietf.org/html/rfc2818.

Manipulationssichere Taxameterdatenerfassung auf INSIKA-Basis

Thomas Krause, Michael Ströh
tesymex UG
Holzdamm 51, 20099 Hamburg
{krause, stroeh}@tesymex.de

Unter Leitung der PTB wurde in einem vom Bundesministerium für Wirtschaft und Technologie (BMWi) geförderten Forschungsvorhaben ein technisches Lösungskonzept (INSIKA-Konzept) erarbeitet. Die Anwendung des INSIKA-Konzepts stellt die lückenlose, revisionssichere Aufzeichnung von Einzelbuchungen bei Bargeschäften bei Nutzung einer elektronischen Registrierkasse sicher.

1 Zusammenfassung

Das INSIKA-Konzept wurde 2009 von den Autoren aufgegriffen und mit Gründung der tesymex UG, einem Datendienstleister für das deutsche Taxengewerbe, ein entsprechendes Dienstleistungsangebot (manipulationssichere Auftragsdatenhaltung) entwickelt. Grund: Im Taxengewerbe - wie auch in anderen Branchen - gibt es keine revisionssichere Aufzeichnung betrieblicher Umsätze. In punkto Umsatzverkürzung und Schwarzarbeit ist das immer noch stark bargeldorientierte Taxigewerbe daher eine Hochrisikobranche.

Um die manipulationssichere Übertragung von signierten Fahrt- und Schichtdaten aus einem Taxifahrzeug und deren langfristiger Speicherung entsprechend den gesetzlichen Anforderungen sicherstellen zu können, wurde im Rahmen einer Kooperation der Firmen tesymex UG, Hale electronic GmbH sowie der PTB ein entsprechendes technisches Verfahren entwickelt.

Im Taxameter erzeugte Fahrtdaten werden in der an das Taxameter angeschlossenen Sicherheitseinheit digital signiert. Genutzt wird hierzu eine Smart Card, die speziell an die Anforderungen des INSIKA-Konzepts angepasst ist. Nachdem die Daten vom TIM signiert wurden, werden diese mit Hilfe eines GPRS-Modems an den Server des Datendienstleisters übertragen.

In Kenntnis dieser Entwicklung hat die Freie und Hansestadt Hamburg als erstes Bundesland bereits Ende 2010 einen Betrag von 5 Millionen Euro zur (freiwilligen) Ausrüstung sämtlicher Hamburger Taxis bereitgestellt. Politisch wird die Einführung eines manipulationssicheren Taxameterdaten-Erfassungssystems von allen in der Bürgerschaft der Stadt Hamburg vertretenen Fraktionen unterstützt.

2 Einführung

In den letzten Jahren hat die Diskussion um die Einführung manipulationssicherer Kassensysteme - unter anderem durch die Aktivitäten der Arbeitsgruppe Bargeldgeschäfte und das Schreiben des Bundesfinanzministeriums vom 26. November 2010 - wichtige Impulse erhalten. Darüber hinaus beflügelt die zunehmende Sorge um die Zukunft der öffentlichen Haushalte die Diskussion: Wo Neuverschuldung und Steuererhöhung erkennbar an ihre Grenzen stoßen, kommt der Ausschöpfung bestehender Steuerquellen umso größere Bedeutung zu.

Allmählich verlässt der Diskurs nun die engen Grenzen der technischen und rechtlichen Fachdiskussion und entwickelt Wirkung im Alltag. Dies gilt insbesondere für das deutsche Taxigewerbe.

Ein Grundproblem im Taxengewerbe - wie auch in anderen Branchen: es gibt es keine revisionssichere Aufzeichnung betrieblicher Umsätze. In punkto Umsatzverkürzung und Schwarzarbeit gilt das immer noch stark bargeldorientierte Taxigewerbe sogar als Hochrisikobranche.

In den Großstädten steht das Gewerbe zudem unter besonderem Leidensdruck. Ein existenzvernichtender

PTB-Bericht IT-18
doi:10.7795/210.20130206a

Verdrängungswettbewerb zu Ungunsten ehrlich arbeitender Betriebe hat viele Taxiunternehmer zu Befürwortern eines nachweislich steuerehrlichen Gewerbes gemacht.

Derzeit werden die steuerlich relevanten Erlösdaten im Taxigewerbe entweder handschriftlich oder in ausgedruckter Form dokumentiert (Schichtzettel: Abschrift vom Taxameter) bzw. mittels kleinvolumiger Datenträger aus den Taxametern ausgelesen und später in die EDV der Unternehmen übertragen.

Die bislang verwendeten Verfahren entsprechen nicht den Anforderungen der §§ 146 und 147 AO und den daraus abgeleiteten Verwaltungsvorschriften. Dies gilt sowohl für die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“ als auch die „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)“.

Damit eröffnen sich erhebliche Spielräume für Umsatzverkürzung und Schwarzarbeit. Es besteht ein weites Feld für Manipulationen, die von Prüfern gar nicht oder nur schwer zu erkennen bzw. nachzuweisen sind.

Bei der von einigen Betrieben bereits heute genutzten elektronischen Erfassung der Daten mittels so genannter Daten-Keys ermöglichen es „spezielle“ Softwareprogramme, die Zahlen wunschgemäß anzupassen, d.h. Fahrt- und Umsatzdaten per Mausklick nachträglich und nicht mehr nachvollziehbar zu verändern.

Diese nachweislich in der Praxis umgesetzten Methoden der Steuerhinterziehung führten bei den Autoren zu der Erkenntnis, dass neue Wege der Datenermittlung und Datendokumentation beschritten werden mussten.

In den Jahren 2009 bis 2011 wurde von den Kooperationspartnern tesymex UG (Datendienstleistung), Hale electronic GmbH (Hardwareherstellung) und der PTB (Datensicherheit), ein Taxameterdaten-Erfassungssystem auf INSIKA-Basis entwickelt und in Hamburg erfolgreich im Rahmen eines Pilotversuchs getestet. Seit Anfang 2012 ist das System zunächst in Hamburg verfügbar. Noch im Jahr 2012 ist ein bundesweites Angebot geplant.

In Kenntnis dieser Entwicklung hat der Hamburger Senat bereits Ende 2010 als erstes Bundesland einen Betrag von 5 Millionen Euro zur (freiwilligen) Ausrüstung sämtlicher Hamburger Taxis bereitgestellt.

tesymex ist ein bundesweiter Dienstleister für Taxiunternehmen und spezialisiert auf die elektronische Erfassung, Speicherung und Bereitstellung von Taxameterdaten.

tesymex erfasst Taxameterdaten revisionssicher und stellt sie den angeschlossenen Taxenunternehmen online zur Verfügung stellt.

3 INSIKA-Taxi Konzept / Verfahrensbeschreibung

Unter Leitung der PTB wurde in einem vom BMWi geförderten Forschungsvorhaben ein technisches Lösungskonzept (INSIKA-Konzept) erarbeitet. Die Anwendung des INSIKA-Konzepts stellt die lückenlose, revisionssichere Aufzeichnung von Einzelbuchungen bei Bargeschäften bei Nutzung einer elektronischen Registrierkasse sicher. Das INSIKA-Konzept ist ein neuer Ansatz zum Nachweis der Ordnungsmäßigkeit der Buchführung.

Der Manipulationsschutz basiert auf einer digitalen Signatur, die mit einer speziellen Smart Card erzeugt wird. Die Smart Card wird von einem spezialisierten Zertifizierungsdienstanbieter bereitgestellt. So geschützte Daten können nicht unerkannt verändert werden. Selbst bei einer Manipulation oder beim Verlust der Daten ist durch technische Vorkehrungen eine Abschätzung der Umsätze möglich. Die Lösung basiert auf bewährter, moderner Sicherheitstechnik, ist vergleichsweise einfach zu implementieren und klassischen Fiskalspeicherlösungen in jeder Hinsicht deutlich überlegen.

Mit digitalen Signaturen und den damit verbundenen Prozessen lässt sich sicher feststellen, dass Daten von einer bestimmten Person, einer bestimmten Registrierkasse oder einem Taxameter stammen und dass die Daten seit Erstellung der Signatur nicht verändert wurden. In den meisten Anwendungsfällen – wie auch beim INSIKA-Konzept – werden Smart Cards zur Erzeugung der Signaturen eingesetzt.

Das Projekt wurde vom BMWi im Rahmen des Förderprogramms "Unterstützung kleiner und mittlerer Unternehmen bei der Umsetzung von Innovationen in den Bereichen Messen, Normen, Prüfen und Qualitätssicherung" ("MNPQ-Transfer") gefördert.

Um die manipulationssichere Übertragung von signierten Fahrt- und Schichtdaten aus einem Taxifahrzeug und deren langfristiger Speicherung - entsprechend den gesetzlichen Anforderungen - sicherstellen zu können, wurde in Ergänzung zu den INSIKA-Festlegungen für Registrierkassen ein speziell an das Taxiumfeld angepasstes Datenmodell entwickelt, das auf dem folgenden Funktionsprinzip beruht. Abbildung 1 zeigt die dazugehörige Systemstruktur.

Im Taxameter erzeugte Fahrtdaten werden in einer an das Taxameter angeschlossenen Sicherheitseinheit digital signiert. Genutzt wird hierzu eine spezielle Smart Card, die alle Anforderungen des INSIKA-Konzepts erfüllt. Diese Smart Card wird "TIM" (Tax Identification Module) genannt. Sie muss auf das Ta-

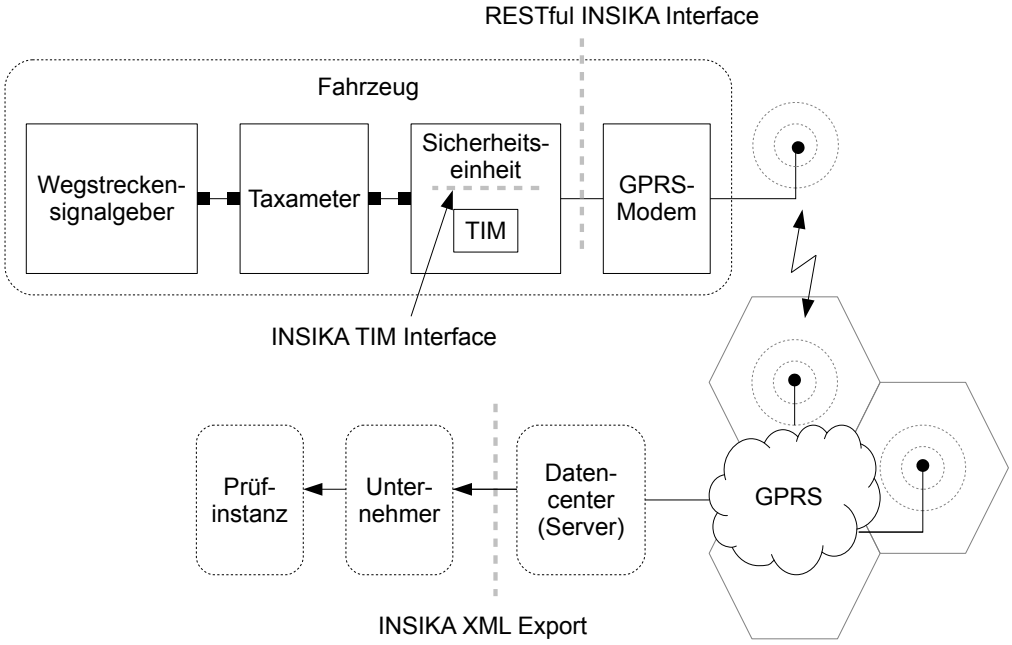


Abbildung 1: Systemstruktur [2]

xenunternehmen personalisiert sein. Wenn alle Taxen eines Mehrwagenbetriebes nach dem INSIKA-Konzept betrieben werden sollen, ist für jedes Fahrzeug eine Sicherheitseinheit und folglich auch ein TIM erforderlich.

Die Sicherheitseinheit steuert entsprechend der Spezifikation "INSIKA Profil Taxameter" [1] das TIM an. Nachdem die Daten vom TIM signiert wurden, werden diese gemäß den Festlegungen "RESTful INSIKA Interface" [2] mit Hilfe eines GPRS-Modems an einen Server übertragen. Dieser Server stellt die Daten des Taxiunternehmers gemäß INSIKA-XML-Exportformat [3] dem Unternehmer zur Verfügung.

4 Hamburg schafft Anreize

Politisch wird die Einführung eines manipulationssicheren Taxameterdaten-Erfassungssystems von allen in der Bürgerschaft der Freien uns Hansestadt Hamburg vertretenen Fraktionen einmütig unterstützt. Hamburg nimmt damit bundesweit die Rolle eines Vorreiters ein.

Das von der Stadt Hamburg bewilligte Förderprojekt "Fiskaltaxameter Hamburg" wird vom Rechtsamt der Behörde für Wirtschaft, Verkehr und Innovation geleitet, die in Hamburg gleichzeitig die Genehmigungsbehörde für das Taxigewerbe ist.

Innovation: Ein gewichtiges Argument für die Förderung bildet die hier beschriebene Entwicklung eines Taxameterdaten-Erfassungssystems, das die erstmalige flächenhafte Umsetzung von INSIKA ermöglicht. Im ersten Ansatz zielt diese Initiative zwar lediglich auf das Taxigewerbe. Interessant sind jedoch die weiterführenden Perspektiven vor allem für kleinteilige, bargeldorientierte Branchen. Damit verbinden sich Anwendungsperspektiven weit über das Taxigewerbe hinaus. Insbesondere vor diesem Hintergrund wurde 2009 die Entwicklung eines Taxameterdaten-Erfassungssystems auf INSIKA-Basis durch die Innovationsstiftung Hamburg gefördert.

Förderung: Laut BMF gelten bis 2016 Übergangsfristen, so dass Fiskaltaxameter erst 2017 verbindlich einzusetzen sind. Um allen Hamburger Taxibetrieben bereits heute den Umstieg zu erleichtern, wird die Anschaffung eines Taxameterdaten-Erfassungssystems mit bis zu 1.500 € pro Fahrzeug von der Stadt Hamburg gefördert.

Forderung: Hamburg belässt es aber nicht bei der Förderung. In einem gemeinsamen Schreiben von Genehmigungsbehörde und Finanzbehörde wurden alle Hamburger Taxibetriebe schriftlich über ihre aktuellen und zukünftigen Aufzeichnungspflichten informiert. Wer seinen Betrieb erweitert oder seine Konzession verlängert, der muss bereits heute glaubhaft nachweisen, dass er allen steuerlichen Verpflichtungen ordnungsgemäß nachkommt – auch der bereits heute gültigen Pflicht zur elektronischen Einzelaufzeichnung.

Bis heute haben bereits zahlreiche Hamburger Betriebe ihr Interesse bekundet. Derzeit liegen Anfragen für ca. 500 Taxifahrzeuge vor. Bis Ende 2013 erwarten die Autoren, dass etwa die Hälfte aller Hamburger Ta-

xis mit einem Taxameterdaten-Erfassungssystem auf INSIKA-Basis ausgerüstet sein wird.

5 INSIKA-Taxi in der betrieblichen Praxis

In der täglichen Praxis ändert sich für das Fahrpersonal wenig: Das Taxameterdaten-Erfassungssystem unterscheidet sich in der Bedienung nicht von konventionellen Taxametern. Sicherheitseinheit und Modem werden unsichtbar hinter dem Armaturenbrett verbaut.

Änderungen gibt es z. B. jedoch bei der Schichtabrechnung zwischen Fahrer und Unternehmer, die meist ein- bis zweimal wöchentlich erfolgt. Schon bevor der Fahrer zum Abrechnen fährt, weiß der Unternehmer wie viele Kilometer gefahren und welche Umsätze erzielt wurden.

Zentrales Instrument ist eine Verwaltungssoftware, die es allen angeschlossenen Taxibetrieben erlaubt, ihre Daten online aufzurufen und zu bearbeiten. Der Unternehmer kann mit einer derartigen Software von jedem beliebigen Ort aus seine Daten korrigieren und die Fahrerabrechnung vornehmen. Abbildung 2 zeigt einen Bildschirmausdruck dieser Software.

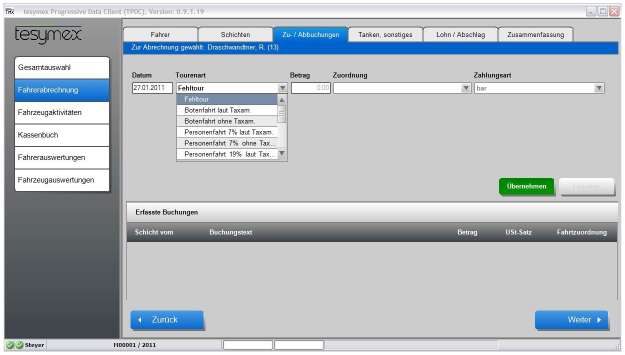


Abbildung 2: Online-Fahrerabrechnung über spezielle Verwaltungssoftware

Der entscheidende Unterschied zur heutigen Praxis: die Bearbeitung findet nicht auf dem PC des Unternehmers, sondern manipulationssicher auf dem zentralen Server des Datendienstleisters statt.

Zubuchungen: Was der Unternehmer bei der Abrechnung noch nicht kennt, sind die Erlöse, die ohne Einschalten des Taxameters gefahren wurden. Das können z.B. Fahrten für Krankenkassen, Botenfahrten oder Ferntouren gewesen sein. Solche Erlöse, für die i.d.R. auch ein schriftlicher Beleg vorliegt, müssen hinzugebucht werden.

Ausbuchungen: Ausgebucht werden müssen dagegen so genannte Fehltouren, also Touren, bei denen der Fahrgast nicht zahlen konnte oder – weit häufiger – bei denen der Fahrgast an der Bestelladresse nicht angetroffen wird, die Anfahrt aber dennoch vom Taxameter angezeigt wurde.

6 Ausblick

Kurzfristige Perspektive: Kurzfristig wird sich erweisen, ob die neue Technik Akzeptanz bei den Hamburger Unternehmern findet, auch wenn nach heutigem Stand bis 2016 noch keine Verpflichtung zum Einsatz besteht. Durch die finanzielle Förderung bei gleichzeitig konsequenter Einforderung gesetzeskonformen Handelns, haben die Hamburger Behörden einen erfolgversprechenden Weg beschritten.

Mittelfristige Perspektive: Mittelfristig sind auch Unternehmer aus anderen Städten angesprochen. Aus verschiedenen deutschen Städten liegen den Autoren bereits Interessenbekundungen vor. Ein grundsätzliches Problem zeichnet sich jedoch hinsichtlich des Mietwagengewerbes ab, das ähnliche Märkte wie das Taxigewerbe bedient – besonders in kleinen Städten und in der Fläche. Sollte es gelingen, das Taxigewerbe „steuerehrlich“ zu machen, droht eine Verlagerung der Probleme in das Mietwagengewerbe. Hier ist eine praktikable Lösung zur sicheren Erfassung von Fahrleistung und Umsatz auch für Mietwagen gefragt.

Langfristige Perspektive: Langfristig gilt es, die in der Taxibranche gesammelten praktischen Erfahrungen mit der INSIKA-Anwendung u.a. für andere transportorientierte Branchen nutzbar zu machen.

Literatur

[1] INSIKA-Projekt. *INSIKA Profil Taxameter*. Version T.1.1.0-10. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: `http://insika.de/`.

[2] INSIKA-Projekt. *RESTful INSIKA Interface. Schnittstelle zur Übertragung von signierten Fahrt- und Schichtdaten*. Version 0.13.5. Physikalisch-Technische Bundesanstalt, Feb. 2011. URL: `http://insika.de/`.

[3] INSIKA-Projekt. *INSIKA Exportformat*. Version T.1.0.6-01. Physikalisch-Technische Bundesanstalt, März 2010. URL: `http://insika.de/`.

An American Look at Zappers

Richard T. Ainsworth
Boston University School of Law
765 Commonwealth Avenue, Boston, MA 02215, USA
vatprof@bu.edu

The U.S. lags behind most other countries in the pursuit of zapper software. Sales suppression catches the attention of the Internal Revenue Service (IRS) only if the manipulation seriously impacts a taxpayer's *annual* income. This is only to be expected. The federal government secures revenue primarily through an *annual* income tax. The U.S. has no broad-based transaction tax, or federal VAT.

State and local governments on the other hand impose a retail sales tax. As a result, these jurisdictions are far more concerned with accurate sales records. On average sales taxes represent one-third of state revenue.[1]

However, the state sale tax system is not uniform. The overall system is exceedingly fragmented and localized with major variances in rates, tax base, and sourcing rules. As a result, the states very much "go it alone," and when it comes to auditing firms suspected of using zappers, none of the states have the computer forensic resources needed to properly complete a zapper audit.

It is not surprising then, that there are only three reported cases of zappers in the U.S.[2] The IRS developed each of them. State and local audits *followed* the federal audit each time. Importantly, there are no reported cases of audits sequenced in reverse (where the IRS followed a state audit) and no reported cases of a state or local government initiating a zapper audit.

The common observation in the U.S. is that enforcement against technology-facilitated sales suppression has fallen through an intra-jurisdictional crack. Neither federal nor state auditors systemically target this area. But this is changing, and the change is coming from the state side.

In recent years, revenue needs have *pushed* the states to look more closely at sales tax losses.[3] The states have also taken note of successful international enforcement efforts against sales suppression in VAT regimes, and these developments have *pulled* the states to consider enhancing enforcement measures against suppression frauds. Evidence that the state picture is changing can be gleaned from legislative developments and changes in audit priorities in roughly half the sales tax states.[4]

[1] Across the 45 states where the retail sales tax is levied more than $226 billion was collected in 2010. The retail sales tax is second to the state individual income tax as a revenue source. Mean state reliance was 34.2%. John L. Mikesell, *The Disappearing Retail Sales Tax*, 63 State Tax Notes 777 (March 5, 2012), referencing U.S. Bureau of Census, Governments Division, *State Tax Collections Summary Report* (2010).

[2] The three cases are: (1) Stew Leonard's Dairy in Danbury Connecticut. See: U.S. v. Stewart J. Leonard Sr. & Frank H. Guthman, 37 F.3d 32 (1994), aff'd. 67 F.3d 460 (2nd Cir. 1995) (although the tax case was settled, the details of the fraud are preserved in these federal sentencing appeals - $17 million sales skimmed over a 10 year period, with sales tax losses of $500,000 and a final determination of $1.4 million); (2) the LaShish restaurant chain in the Detroit, Michigan. See: Press Release, U.S. Dept of Justice, Eastern District of Michigan, *Superseding Indictment returned Against LaShish Owner* (May 30, 2007) (indicating that $20 million is cash sales were skimmed over a 5 year period); and (3) Theodore R. Kramer who installed zappers in Detroit, Michigan area strip clubs – although in this instance the tax amounts lost are not specified. See: U.S. Dept. of Justice, Eastern District of Michigan, *Michigan Software Salesman Pleads Guilty to Conspiracy to Defraud the Government* (November 17, 2010).

[3] During the heart of the Great Recession (2009-2010) budget deficits were rising in the states. In 2009 the National Conference of State Legislatures projected budget gaps of $84 billion in just 34 states. By 2010 the gap was $143 billion. These projections set off waives of tax increases and spending cuts that were exceptionally painful. Robert Buschman & David L. Sjoquist, *Recent State Legislative Tax Changes in the Face of Recession*, 63 State Tax Notes 623 (February 20, 2012).

[4] By the authors count 20 of the 45 states with a retail sales tax are engage either legislatively or through criminal investigation in the pursuit of zappers. These states have 56.8% of the U.S. population.

PTB-Bericht IT-18
doi:10.7795/210.20130206a

This paper has two main parts.[5] First, it summarizes the current state of sales suppression enforcement in the U.S. Secondly, it reviews the international solutions that are attracting the most U.S. attention. A conclusion indicates likely directions for U.S. enforcement.

1 The Great Recession – Pushing State Law Changes against Zappers

Georgia is the first state to take action. On May 3, 2011 Georgia enacted H.B. 415, which added code section 16-9-62 to Georgia statutes. This law made it illegal to willfully and knowingly sell, purchase, install, transfer, or possess any automated sales suppression device, zapper or phantom-ware in the state.[6] Prior to this date only the actual fraud was penalized; now the technology that facilitates the fraud is subject to enforcement measures. Before Georgia, no state penalized fraud-facilitating technology.

On March 1, 2012 Utah followed Georgia and passed a nearly identical bill, H.B. 96.[7] On March 10, 2012 West Virginia passed its version of the Georgia law, S.B. 411.[8] On March 13, 2012 Maine also passed its version, L.D. 1764.[9] As of March 15, 2012 the legislation in each of these states awaits a governor's signature.

This is just the beginning. Similar bills are pending in six additional states: New York,[10] Tennessee,[11] Michigan,[12] Florida,[13] Indiana,[14] and Oklahoma.[15]

The Oklahoma legislation is particularly Draconian. Where each of the other states impose a penalty of up to $100,000 and one to five years in jail, Oklahoma adds a $10,000 administrative penalty and allows the Commissioner to remove the business license from the offending establishment for up to ten years if a zapper is found. Oklahoma H.B. 2576 states:

> D. In addition to the criminal penalty provided in subsection C of this section, any person violating subsection B of this section shall be subject to an administrative fine of Ten Thousand Dollars ($10,000.00). Administrative fines collected pursuant to the provisions of this subsection shall be deposited to the General Revenue Fund.
>
> E. The Tax Commission shall immediately revoke the sales tax permit of a person who violated subsection B of this section. A person whose license is so revoked shall not be eligible to receive another sales tax permit issued pursuant to Section 1364 of Title 68 of the Oklahoma Statutes for a period of ten (10) years.

New York and Maine have amnesties provisions for merchants who step forward and voluntarily disclose a zapper. Oklahoma and the seven other states simply penalize - immediately, and without hesitation if a zapper is found.

Aside from these legislative efforts, the author is aware of nine more states where anti-zapper laws are under active consideration, or where the pursuit of zappers has become a criminal investigation priority of the department of revenue.

Finally, among the most compelling factors *pushing* the states into action is a report that New York has conducted four successful sting operations for zappers. According to the New York Post the Department of Taxation and Finances found that when they opened up false restaurants and solicited tenders for new electronic cash registers that "most"[16] of the twenty-four ECR/POS system sales representatives who showed up actively solicited orders for sales suppression software associated with their machines.[17] The ability to digitally skim sales was clearly considered a competitive selling point.

[5] Because of space constraints, this paper assumes the significance of pursuing zappers. It assumes that technology-facilitated sales suppression is as prevalent in the U.S. as it is elsewhere. It assumes both an active infection rate of approximately 50% in the restaurant industry, and an overall tax system vulnerability rate of 70% for all point of sale (POS) systems in a state. But, as a powerpoint presentation by the California Investigations Division puts it:

> Does California have a problem? We most likely haven't found it yet.

Zappers and Phantom-ware: Automated Sales Suppression (March 2012) at 6 (on file with author).

[6] Ga. Code Ann. §16-9-62(b).

[7] H.B. 96, 2012 Gen. Sess. (Utah 2012)

[8] S.B. 411, 80th Leg., Second Reg. Sess. (W. Va. 2012)

[9] L.D. 1764, 125th Me. Leg., Second Reg. Sess. (Me. 2012)

[10] S.B. 2852 & S.B. 2611 (requiring a study), 2011 Leg. Sess. (N.Y. 2011).

[11] H.B. 2226, 107th Gen. Assem., (Tenn. 2011).

[12] S.B. 768 & 769, 2011 Leg., 96th Sess. (Mich. 2011).

[13] S.B. 1304, 2012 Leg., Sess. at §6 (Fla. 2012).

[14] H.B. 1337, 117th Gen. Assem., Second Reg. Sess. (Ind. 2012).

[15] H.B. 2576, 2012 Reg. Sess. (Okla. 2012).

[16] In other venues the Department of Taxation and Finances confirmed the NY Post report and indicated that by the expression "most" the Department meant that approximately 70% to 80% of the salesmen were offering zappers.

[17] John Crudele, *Today's Special: Scam Dodges $400M in Sales Tax*, New York Post (January 24, 2011).

2 International Solutions – Pulling States to Secure POS Systems Against Zappers

State and local governments are in a position to benefit from international efforts to find a solution to zappers, and they know it. On the technology side, solutions range from very cost-effective measures, like the INSIKA-developed smart card (€50), [18] to Quebec's far more expensive *module d'enregistrement des ventes* MEV (costing between C$600 and C$800). [19] Blended applications, like BMC Inc.'s Sales Data Controller – Mobile (SDC-Mob), [20] offer the best attributes of both of these solutions, and a bit more (US$350). [21] These technology solutions encrypt data and prevent it from being "zapped away."

Non-technology (regulatory) solutions approach the same problem differently. The Netherlands and Norway establish the government's right to control POS system data, and then marshal market forces to preserve it. The assumption in these jurisdictions is that data security can be made into a competitive factor among cash register system providers. Costs in this case are indirect and more difficult to measure.

As state and local governments measure the revenue that is being lost to zappers, these promises of technological and regulatory solutions *pull* enforcement efforts forward.

Technology-based solutions. The INSIKA smart card has caught U.S. attention. It is hard to argue with a €50 solution that offers a high degree of security for ECR/POS system transactions. [22] The smart card achieves economies by taking advantage of native ECR/POS system capacities.[23] For example, sales data is stored in the electronic journal (EJ) not the smart card, but it is "signed" before storage. The smart card holds sums and counters, not large amounts of basic data.[24]

Even the data's signature is not stored on the card. Auditors find the signature in the EJ, import it into audit software, and then verify authenticity. Thus, the smart card's economy is also (in part) its chief liability. Un-encrypted data is stored on an open EJ. This is a potential security risk, because the EJ can be tampered with. If it is, then the auditor can detect it, but an audit must be performed to find the tampering.

Quebec's MEV solves the smart card's security problem by storing encrypted data in a tamper-proof external device. The MEV keeps a real-time clock independent of the ECR/POS system, and provides auditors with a scan-able bar code on each receipt to verify security.[25] The MEV makes system demands on a merchant's cash register. In some instances a new cash register is needed, and this can be a considerable expense for small businesses.[26] Although the

[18] Personal e-mail communication, Dr. Norbert Zisky, Head of INSIKA research (February 19, 2008) (on file with author).

[19] At a conference in Montreal sponsored by Revenue Quebec, *The First Conference on Tax Compliance – The Fight Against Tax Evasion* (June 2-4, 2010) the position of Revenue Quebec was that the MEV (also called in English translation a Sales Recording Module, or SRM) would cost C$600. On January 26, 2011, Allagma Technologies, an SRM dealer in Quebec posted the following FAQ:

Q: How much does an SRM (MEV) cost?

A: The cost of an SRM (MEV) unit is approximately $800 plus installation fees.

During the initial installation period prices were competitively posted on Allagma's web site in a frequently asked questions format. Now that installation is complete in Quebec this data has been taken down. Original documents on file with author. The difference in these numbers may have been that the conference announcement did not include the cost of a Microsoft software license.

[20] Sales Data Controller (SDC) is a generic term that applies to a lot of devices in the market that perform a similar function. They can be stand-alone or integrated into cash register systems. See: `http://www.salesdatacontroller.com/index.php/all-about-sales-data-controller`. SDC-Mob is a specific device made by BMC Inc. It is an SDC that includes secure mobile communications functionality.

[21] Tetsuo Yamada, CEO of BMC, indicated that US$350 was the price of a single SDC-Mob (November 16, 2011).

[22] The price of the smart card is critical to some people in the states. Thus, a further e-mail conversation with Dr. Zisky (March 15, 2012) was initiated to confirm this price point. He states:

In my opinion the costs per card in a package of 10,000 pieces is $5 to 7 including all software packages, license fees and testing/certification fees. The technical solution for handling this card (readers, drivers, software development) takes ... not more than $20. Based on that we doubled the costs and came to ($ or €) 50. This value is confirmed by our partners from industry.

[23] This, of course, imposes demands on the ECR/POS system, and there may be an upgrade to older business systems required in a jurisdiction that selects the smart card solution.

[24] A companion issue concerns the real-time clock, which originates with the ECR/POS system, not the smart card. The smart card includes output from the real-time clock in its encryption algorithm, but to the extent a fraudster would want to tamper with the clock he would have access to it in the insecure ECR/POS system. Changing the clock might be a technique used to confuse an auditor.

[25] See: Revenue Quebec, *Fight Against Tax Evasion: Sales Recording Module (SRM)* (describing the SRM system) available at: `http://www.revenuquebec.ca/en/a-propos/evasion_fiscale/restauration/mev/`.

[26] Ministry of Revenue Quebec, *Fight Against Tax Evasion: Point-of-Sale (POS) Systems*, indicates:

As a restaurateur, you are responsible for ensuring that your POS system is SRM [MEV] compatible and that it can communicate with an SRM [MEV]. To be SRM [MEV] compatible, your POS system must be adapted by its developer to meet

MEV has additional functionality,[27] it is questionable whether or not its price at fifteen times the cost of an INSIKA smart card returns fifteen times the security.

BMC's SDC-Mob provides a third-party solution that matches the capabilities of the government-involved solutions (INSIKA smart cards and the MEV) at half the price of an MEV. Transaction data is encrypted. It is signed with an INSIKA-like smart card.[28] Data is securely stored externally. SDC-Mob data can also be accessed remotely to assure compliance, and a check for tampering can be made without leaving the tax office. This kind of system appears to be acceptable under the new Belgian regulations, however if adopted, the smart card will not be INSIKA's (rather a Belgian card developed by Fedict[29] would be required), and the mobile attribute will be eliminated on political/privacy grounds.[30] This approach is similar to the Swedish solution.

From a U.S. perspective, the implementation methodologies of some of these international solutions create difficulties. The MEV is required in *all* Quebec restaurants, and the earlier version of the SDC-Mob (the eTax module)[31] is certified for use in a program that mandates it in *all* Swedish cash registers. In the U.S. a similar *technology mandate* would represent a deep government-intrusion into business privacy/ confidentiality. Proof of a compelling state reason to do so might be needed.[32]

The German use of INSIKA smart cards in taximeters is a different story. There is a considerable problem with skimming cash sales by German taxicab operators. Both the taxicab owners and the revenue authorities are loosing revenue. However, without *requiring* smart cards in *all* taximeters, the city of Hamburg established a *voluntary* program with a grant of €5 million for the adoption of taximeters that would be secure against data manipulation.[33] The Hale taximeter company has installed the INSIKA smart card and currently offers the only solution on the market.[34] The program is reportedly a success.[35]

---

our requirements and technical specifications. Developers can request that an adapted POS system be certified compliant with our technical specifications. If the adapted POS system is compliant, we issue a confirmation of certification that recognizes the compatibility of the product with an SRM [MEV]. [This page list 81 compatible systems.]

Available at: `http://www.revenuquebec.ca/en/a-propos/evasion_fiscale/restauration/produits.aspx`. That this may pose a considerable hardship for some merchants is explained in Anja Karadegllja, *Deadline Looms for Restaurant Rebates*, Actualites (February 17, 2011) (which considers how a $2,000 ECR upgrade in one business and a $6,000 upgrade in another to accommodate the MEV placed these businesses in considerable financial difficulty, even though Quebec was providing subsidies for merchants), available at `http://www.lesactualites.ca/?site=CDN&section=page&1=C110216&2=C110119_deadline`.

[27] The MEV is manufactured by AAEON, a Taiwanese company. The full commercial version with technical specifications can be seen here: `http://www.aaeonsystems.com/products/AEC-6831.php`.

[28] The SDC-Mob could use the INSIKA smart card, or as in Belgium a different smart card could be developed locally and used in the device.

[29] Fedict is a Federal Public Service of Belgium, created on May 11, 2001 as part of the plans to modernize the federal administration. It is a so-called horizontal Federal Public Service because it isn't responsible for a specific policy field, but provides services to the other Federal Public Services. Fedict is responsible for e-Government. See: `http://www.fedict.belgium.be/en/`

[30] As of March 16th, 2012, the Belgian regulations have not been finalized, however they have been reasonably well developed for some time. They were expected to have been finalized by the end of 2011. They are the topic of intergovernmental studies, and are considered for example in the Norwegian study *New Regulations for Cash Register Systems (Nytt regelverk for kassasystemer)* at 37-39 (in Norwegian, translation of file with author). They also play a significant role in a Dutch Master's thesis by M. Leurink, *Beheersmaatregelen ter Voorkoming en Bestrijding van Datamanipulatie in Afrekensystemen* (Management Measures to Prevent and Combat Data Manipulation in Cash) (March 2011) at 36-44 (in Dutch, translation on file with author) available at: `http://www.vurore.nl/images/vurore/downloads/1048_scriptie_Leurink.pdf`.

[31] Swedish certification (by SWEDAC) was awarded to an earlier version of the SDC-Mob called eTax on August 24, 2009. Post-2009 development efforts by BMC included working with a smart card (like the INSIKA card) and the inclusion of remote communications (the Mobile attribute in the SDC-Mob). What is important in this regard is to notice the responsiveness of the private sector to developments in the security field. By positioning itself as a standard-setter the Belgian government is pushing the private sector to adopt and adapt to cutting-edge solutions.

[32] See: Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 Georgetown Law Journal 123 (2007) (suggesting that the American law of privacy and "inviolate personality" differ from the English concept of confidentiality which recognizes and enforces expectations of trust within relationships, and in this case the concern might be with confidentiality). Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego Law Review 745 (2007) (arguing that there is a threat to privacy in data mining and other oversight activities even when the government does not uncover illegal activities).

[33] The voluntary Hamburg program can be seen at: `http://www.hamburg.de/taxi/3030326/taxameter-foerderung.html`. The Hamburg grant is for €1,500 euro per participating taxi.

[34] The Hale taximeter system with INSIKA smart card can be seen at: `http://www.hale.at/en/solutions/fiscal-solutions/insika-solution.html`.

[35] In the 2010-2011 time frame the PTB conducted a voluntary pilot program (up to 10 taxis in Hamburg and another 10 in Berlin). Within the past six months Dr. Zisky reports that the pilot has recorded 13,000 trips without an error. (Personal

The four New York stings operations that found a high incidence of ECR/POS system salesmen also selling zappers is a start down the *mandatory* road, but these stings do not compare with the 230 litigated cases of restaurants using zappers in Quebec. Quebec was able to impose the MEV on all restaurants in the province because it had proof of widespread fraud.[36] That is not the case in the U.S., and the states may need to be looking at a program similar to the German's voluntary taximeter program.

Non-technology (regulatory) solutions. Jurisdictions that *regulate* solutions to zappers have a different focus, and a different proof-point than those that apply technology – their focus is the ECR/POS system, not the businesses that use them. The difference is subtle, but the problem is the same. Stated another way:

- A *regulatory solution* needs to prove that the *cash registers* in the commercial marketplace are inherently vulnerable to manipulation. It then regulates equipment improvements so that the systems will never manipulate transactions.
- A *technology solution* needs to prove that *businesses* are exploiting cash register vulnerabilities. It then monitors use of the equipment in a way that records manipulations whenever they occur.

Thus, the goal of regulation is to get manufacturers to produce *only* secure machines. In this regard, the Dutch and Norwegian approaches to zappers are good examples of how the regulatory approach works. There are differences in application.

The Dutch *persuade* manufacturers to improve security; the Norwegians *specify and demand* the improvements they want. The underlying premise is the same – there is a marketplace problem. The premise has a corollary: manufacturers will ultimately provide the best oversight when (*and only when*) commercial rewards align with data security.

Netherlands. Following the discovery of a zapper developer at a manufacturer of POS systems (2010) the Dutch Tax Administration (*Belastingdienst*) took the client list and asked each purchaser of this POS system to sign a statement that declared:

- The type of cash register used
- Whether they used the installed zapper
- Whether they were willing to repay lost tax revenue (if any)[37]
- Whether they were willing to take steps to prevent future fiscal damage.

Following up on the related enforcement action the public (with considerable assistance from the press where this was a big news story) became convinced that the *Belastingdienst* could find any non-compliant cash register. Based on these reports, and the signed statements, which included a promise to prevent future frauds, there very quickly was a noticeable increase in demand for complaint machines. For this purpose (and to help the industry meet this need) the *Belastingdienst* met with over 70 producers and traders of cash registers. An agreement was reached among all parties (including a signed letter of intent on April 18, 2011) that resulted in:

- A set of standards for reliable cash registers;[38]
- A Quality Mark (*Het Betrouwbare Afrekensysteem*) that would indicate that a cash register met compliance standards; and
- A commitment by the producers and traders that after July 1, 2013:
  - No POS system would be sold that could not achieve a Quality Mark;
  - All simple cash registers would have a declaration of settings by the producer.[39]

If the Dutch are successful in their cooperative-regulatory approach to zappers, there will soon be no possibility for technology-assisted sales suppression fraud in the Netherlands. After July 1, 2013 no cash register system sold in the Netherlands will be vulnerable to a zapper.

Norway. On February 15, 2012 the Norwegian Ministry of Finance released the Directorate of Taxation's report, *New Regulations for Cash Register Systems (Nytt regelverk for kassasystemer)*,[40] and placed it into public consultation until May 15, 2012.

The report essentially recommends that only qualifying cash register systems be allowed in Norway.

e-mail from Dr. Zisky on March 16, 2012, on file with author).

[36] Roy Furchgott, *With Software, Till Tampering Is Hard To Find*, NYT C6 (August 20, 2008) (indicating that Revenue Quebec had brought 230 zapper cases to court in ten years) available at: `http://www.nytimes.com/2008/08/30/technology/30zapper.html`

[37] "About 85% did not use the zapper module, 15% however did." Ben G.A.M. van der Zwet, (*Belastingdienst* computer forensic auditor) *A Pebble in the Cash-Economy* (draft, on file with author)

[38] The standards are produced by an independent Quality Mark authority, *Stichting Betrouwbare Afrekensystemen* (Reliable Cash Register Foundation) which can be found at: `http://www.keurmerkafrekensystemen.nl/`. Essentially, those standards are classified according to four management objectives: (1) register all events; (2) integrity of registrations; (3) storage of registrations; and reports are transparent and reliable.

[39] The declaration of settings is specific to each type of simple cash register, but it will describe all system attributes (no hidden capacities that are not described are allowed). It will lead to a Quality Mark.

[40] Available at: `http://www.regjeringen.no/pages/36992076/h_notat_10_4626_HS.pdf` (in Norwegian)

Suppliers of cash registers will be required to upgrade current systems, and make initial and ongoing product declarations to the tax office that the functional requirements of the regulations are met by their systems. Operators will be required to acquire new or upgrade current systems and then notify the tax administration of the change.

Secure electronic records should therefore be Norway's answer to the hardware-based security used in foreign countries through control boxes, smart cards, etc.[41] The revenue gain is projected to be substantial.[42]

The Norwegian view is that product declarations, notifications and fines "... act as a substitute for a technical solution."[43] The Cash System Act (*Kassasystemloven*) sets out the requirements of checkout systems (§3), a duty for suppliers of checkout systems to assist the tax office with software, programming, and operation of their systems (§4), requirements for product declarations by suppliers (§5), a set of seven violation fees imposed on suppliers (§6), and daily "coercive fines" also imposed on suppliers (§7). In addition, regulations are authorized (§8).[44]

The cash register system regulations (*Kassasystemforskriften*) are extensive. Most notable are the regulations at §2-5 that specify the features that a cash register must have, and those at §2-6 that specify prohibited features.[45] Cash registers that violate these rules must be "pulled from the market, unless the supplier rectifies the deficiencies."[46] Enforcing this provision is expected to be relatively easy as the supplier and user will register each cash system (by government issued ID) in an online database.[47]

Fourteen additional fines and fees are specified in the Bookkeeping Regulations (*Bokforingsforskriften*) that deal with the operator's use of the cash register system.[48]

3 The U.S. Way Forward

It is certain that the U.S. states are listening and learning from the experiences of the international community in the battle against technology-assisted sales suppression. At the moment at least nineteen states are engaged in some form of legislative or administrative enforcement actions today.

Admittedly, there is very little to show for this effort if we are using litigation as our yardstick. As of March 15, 2012 there is no public evidence that any state has initiated an audit on a firm that has used a zapper or phantom-ware to skim sales. All state cases are those where the state is following a federal income tax audit.

However, we may well be on the cusp of change in the U.S. Preparations for enforcement action are underway. Laws that penalize the sale, purchase, installation, transfer, or possession of any automated sales suppression device, zapper or phantom-ware have been enacted in one state (Georgia) and passed by the legislature in three others (Utah, West Virginia and Maine). Four highly productive stings have been conducted in New York.

Next steps in the U.S. This is the most interesting compliance question. What enforcement direction will the states move in, as suppression frauds are uncovered? Will a technology solution like the INSIKA smart card, the Quebec MEV or BMC's SDC-Mob be the route, or will a regulatory approach be used? If the later, will the states try to persuade cash register providers to comply with industry formulated rules like the Dutch, or will they mandate that providers make changes (and the users adhere to them) like the Norwegians?

Will any of these solutions work in the U.S. if they are applied universally throughout a jurisdiction (as in Sweden, or Norway), or throughout a discrete business sector, like the restaurant sector (as in Quebec and Belgium)?

A privacy push-back. The most interesting legal question deals with privacy. How will state tax administrations respond to a "business privacy" push-back?

Privacy concerns may move enforcement into more surgical responses than we have seen internationally (outside of the German use of the INSIKA smart card in taximeters). States may adopt the adage that "every dog deserves one bite," and give the Commissioner authority to mandate one of the international solutions case-by-case, and only in certain defined situations. Perhaps the rule would isolate businesses that have been shown to be regularly out of compliance with the sales tax, or with historically bad records, or with especially contentious audit positions. Maybe the rule

[41] Id., at 60.

[42] An independent IT consulting firm indicated that adoption of these rules would provide an estimate net present value gain of 14.092 billion NOK or $2.48 billion USD over ten years. Steria AS, *Skattedirektoratet: Prosjekt "Nytt regelverk for kassasystemer" – Samfunnsokonomisk analyse* (Tax Directorate: Project "New regulations for checkout systems" - Social Economic Analysis) (September 21, 2011) at 28, Table 5, available at: `http://www.regjeringen.no/pages/36992076/vedlegg_steria.pdf` (in Norwegian).

[43] *Nytt regelverk for kassasystemer*, supra note 40, at 62.

[44] Id., 97-98.

[45] Id., at 99-100.

[46] Id., at 63.

[47] Id., at 63.

[48] Id., at 67 & 104.

would be even narrower and apply only to businesses that have been found to be using a zapper or phantomware applications.

In these instances a businesses might be required by the Commissioner to install a technology solution like the SDC-Mob, which can be remotely overseen by tax authorities. Or perhaps a Norwegian approach might be authorized, and regulations could be drafted that would force problematical businesses to install cash register systems that are manufactured with security features like those required in Norway. Such an approach would be more lenient than simply revoking the sales tax permit, as Oklahoma is prepared to do.

4 Not Just Cash – Debit/Credit Transaction Too

One final point needs to be made. Technology-assisted sales suppression is no longer just about *cash* skimming; this fraud has migrated to *debit/credit card* transactions. There are two indications that this is happening, and that zappers are key instruments in facilitating it, one from Norway, and the other from the recent Fiscalis meeting in Ireland.

Norway. The recent Norwegian regulatory proposals include a discussion of "problems related to the terminal – use of an independent terminal." In short the problem involves debit/credit card terminals that are not connected to the cash register system. If the terminal is programmed to remit funds to a different (personal) account at a different bank (not the bank used by the business making the sale), then a sale can be rung up "as if" it was a cash sale and then zapped as follows:

1. The cashier scans the purchase;
2. The cash register indicates a sales total ($500, for example);
3. The credit/debit card is swiped for $500;
4. An authorization is received from the debit/credit card intermediary;
5. The cashier then presses "cash sale", (not credit/debit card sale) a receipt is issued, and the transaction completed;
6. Later that evening the false cash sale is "zapped" from the system.

Neither the debit/credit card transaction (at 3 & 4), nor the sales transaction (at 6) is recorded in the cash register system. There is no digital trace for a traditional auditor to follow to determine liability, unless the auditor knows the credit/debit card that was used, and traces the payment from the cardholder's bank to the (personal) account of the business owner.

The Norwegian regulations solve this problem by requiring debit/credit card terminals to be tied to the cash register.[49]

Irish Fiscalis meeting. How significant is this permutation of sales suppression? Significant enough so that nearly a full day of meetings at the E.U. Fiscalis held in Dublin, Ireland (October 19-21, 2011) were devoted to this problem with reports filed on the problem by the UK[50] and Portugal,[51] followed by workshops focused on combating this fraud.

The U.S. states need to take this permutation of sales suppression fraud into account as they devise their way forward. The international community is already doing so. This mutation appears to be significant.

---

[49] Checkout System Regulations (*Kassasystemforskriften*) § 2-5, second paragraph; § 2-8-3 and § 2-8-2(g); Bookkeeping Regulations (*Bokforingsforskriften*) § 5a-2, second paragraph; § 5a-14, third paragraph.

[50] Chas Coysh, HMRC Indirect Tax Team, Strategic Risk Unit, Large Business Services. His Friday, October 21, 2011 presentation focused on Merchant Acquirer Accounts – Tax Evasion in the U.K.

[51] Ana Isabel Silva Mascarenhas, the e-Audit Contact Person for the Portuguese Tax Administration, who presented on fraud with Merchant Acquirer Accounts in Portugal.

Developments towards reliable Information from Cash Registers

Ben van der Zwet[1] and Frank van Heusden[2]

[1,2]Belastingdienst
[1]Postbus 90057, 5600 PK Eindhoven, The Netherlands
[2]Postbus 10014, 8000 GA Zwolle, The Netherlands
{bgam.van.der.zwet, f_van_heusden}@belastingdienst.nl

While today's cash registers are very sophisticated and able to perform a multitude of functions that facilitate the efficient running of a business, they are also open to abuse. Tax administrations, aware of the risk of electronic sales suppression, cooperate in international expert groups to explore cost effective approaches to counter this fraud. Marketparties acknowledge their responsibility. Invited by inspiring projects like INSIKA, suppliers and software developers bring in their expertise to develop reliable and auditable cash registers.

The permanent objective of the Dutch Tax and Customs Administration (DTCA) is to increase, keep or enforce compliance. DTCA aims at cooperation with software providers and other stakeholders to increase the reliability of the chain of information from the first registration in a business process to the complete and just accounting in tax returns. Responsive supervision directs proportionate response to the fiscal conduct and behaviour of the taxpayer and his suppliers and advisors. If necessary the response is firm and might end in criminal prosecution. If possible the interaction is open and constructive.

In the Netherlands producers and suppliers of cash registers recently developed a Standard for Reliable Cash Registers. In the second half of 2012 an independent quality mark authority, "Stichting Betrouwbare Afrekensystemen" will issue a quality mark for reliable cash registers ("Keurmerk Betrouwbaar Afrekensysteem").

Like Information Technology in general, techniques to abuse information by way of electronic sales suppression tends to develop and thus asks for continuous awareness and appropriate response to this threat. Development of reliable information of cash registers benefits of cooperation of stakeholders in projects like INSIKA. Not only by sharing technical expertise, but also by developing common responsibility as a basis for an open and fair market.

1 Problem

When dealing with small to medium sized enterprises reports and totals, generated by cash registers, are frequently used as the basis for tax returns. Unless businesses have internal controls that can verify the accuracy and completeness of such records, it is difficult for tax administrations to be sure about the accuracy of tax returns. While today's cash registers are very sophisticated and able to perform a multitude of functions that facilitate the efficient running of a business, they are also open to abuse.

Examples of such abuse may include sales that are not entered on the cash register and entries that are correctly recorded but are manipulated afterwards to suppress sales. Sales suppression is supported by electronic sales suppression facilities in three ways:

- A feature of the cash register is misused, like registering sales in training mode.

PTB-Bericht IT-18
doi:10.7795/210.20130206a

- Software programs in cash registers contain features that are designed to facilitate cash skimming (Phantomware).
- External software is used to manipulate data of cash registers (ZAPPER).

Note that the way fraud is committed differs with the size of the enterprise. Skimming cash receipts is an old fashioned tax fraud. A fraud traditionally associated with small or medium sized enterprises. Large businesses with formalized internal control mechanisms, external accountants, and professional management structures do not normally engage in skimming. Skimming frauds thrive when the owner (or a close family member) is the cashier.

Then again; when auditing enterprises, big or small, the audit programme has to cover the weaknesses in internal control and monitoring.

2 Rules and Regulations for reliable Cash Registers are not the sole Answer to the Problem

Very small businesses without or with only a few employees often don't need the management information from a cash register to run the business. So if they simply do not enter sales in their cash register it is the easiest way to avoid tax. If you are not aware of this fraudulent behaviour you start to overrate the more technical answers to fight fiscal fraud.

Greece and Italy are examples of countries with strict legal obligations concerning the cash economy. Shops and Retail businesses are obliged by law to use certified cash registers. Cash receipts have to be issued and the client is obliged to take and keep the ticket. Enforcing these obligations is an intensive and thus expensive way of countering sales suppression. If tax administrations do not apply appropriate supervision fraud will continue. In December 2011 the Italian Guardia di Finanza performed an intensive supervision in Cortina d'Ampezzo. While the investigation took place, Shops and Retail businesses showed an increase of sales up to 400 % compared to normal.

3 International Awareness

Tax administrations are more and more aware of the fact that although sales transactions are registered in a cash register or Point Of Sales system, this does NOT guarantee that sales are accounted for and end up in tax returns. This awareness leads to both global and European projects to counter the problem.

In Europe there is a FISCALIS project ZAPAT, (Zappers and Phantomware Activity Team), ZAPAT develops an audit program to discover and prevent fiscal fraud misusing cash registers.

The Organization of Economic Cooperation and Development (OECD) runs a project to counter the automatic sales suppression. In this project the OECD is working out the demands that can be held to reliability of cash registers. The paper on this issue will be issued in 2012 as well.

4 A general Model for considering Risks.

The vulnerabilities in terms of electronic sales suppression can be considered as present in specific risk areas of the POS system configuration. Each of these risk areas presents opportunities for sales data to be deleted, changed or, in the case of the actual transaction, not being recorded at all. The POS system suppliers in the Netherlands in conjunction with the tax authorities have developed a model of risks for POS systems in order to stimulate compliance with tax obligations.

The OECD's electronic sales suppression expert group has adapted the Dutch model to provide a general model for considering risks within POS systems. The model has five risk areas, the integrity of transactions, the software, the transaction data, external files and reporting possibilities. The figure 1 illustrates the five risk areas:

The first risk area is the **integrity of the transaction**. To safeguard the integrity of the transactions the cash register must contain measures to ensure that input of the transaction is complete, correct and on time. If input of the transaction is not complete, correct and on time, the system produces unreliable business information with risks in terms of the ability to make the right management decisions and to file accurate tax returns.

The second risk area is the **software** itself. The software needs to be designed to ensure integrity, confidentiality and availability of the process performed by the cash register system. If the system can not ensure integrity, confidentiality and availability, the system would again produce unreliable information with the risks to management decisions and accounting for tax. It is important to ensure that the software operates so as to store all information of all actions carried out on the cash register system and creates a clear

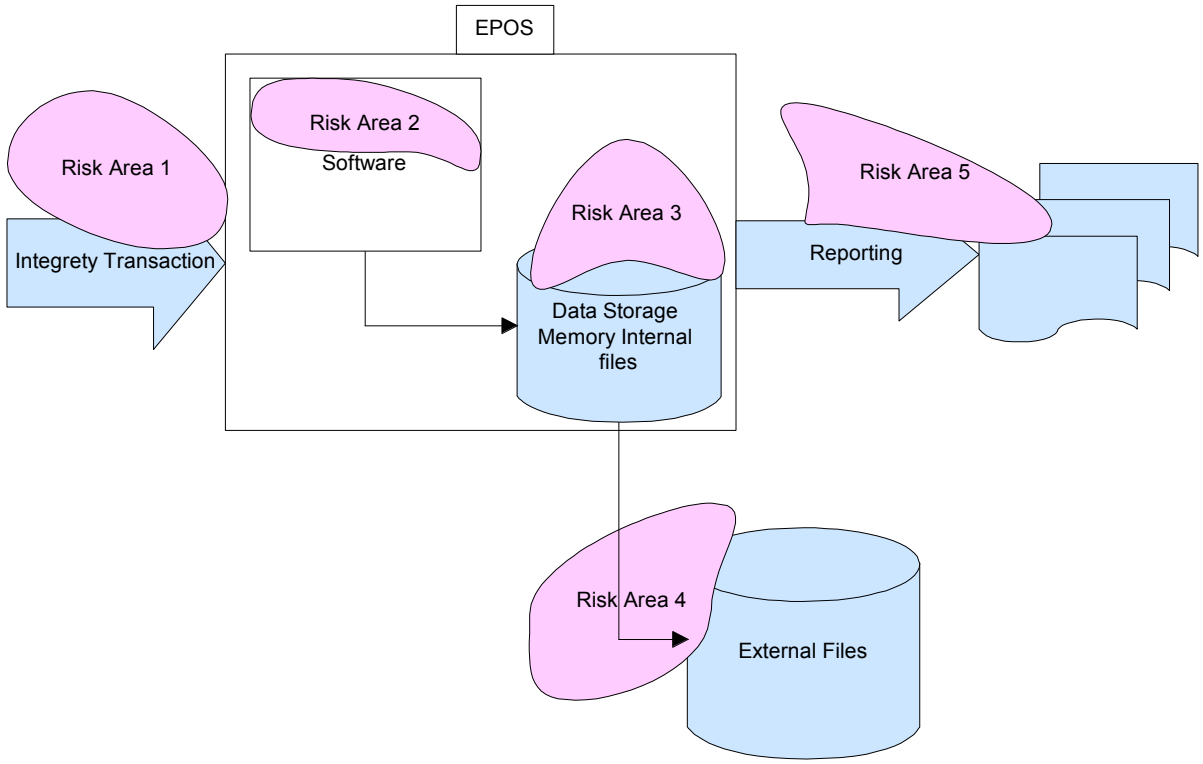


Figure 1: Risk areas

audit trail. This is necessary for effective management and control of the complete business process.

The third risk area is the **transaction data** created by the system for storage and reporting. This information, stored in memory and internal files, is the basis for all reporting and would also be within the scope of data to be examined for audits and investigations. It is in this area that the greatest risks arise of electronic sales suppression software (or other file tampering methods) being used to manipulate this information contained in transaction data.

The fourth risk area, **external files**, is the transfer to and storage of transaction data in offline files needed for example, when the electronic journal in an ECR is full. Generally, countries have laws that require persons to keep for a certain period appropriate books and accounts and this includes the data carriers on which these books and accounts are recorded. In some laws, the books and accounts should be organized in such a manner that it allows the tax auditor to audit them within a reasonable period of time. The external files could also be the files that are transferred on a daily basis from the POS system to the back office system on a separate computer (This is the case in one of the leading restaurant systems). The external files could also include the backup files for the cash register system. The backup files may be stored either on an external media or on the hard drive within the system itself but in a different folder. The backup files may contain vital information for revealing the use of electronic sales suppression in a cash register system.

The fifth risk area is the **reporting possibilities**. This risk area is strongly connected to the second risk area, the software, which controls the reporting and therefore opens possibilities for manipulation in the design and creation of reports. The reports are important for the management of the business and are used to transfer information into the accounting system, to create tax returns etc. In case of loss of the transaction data, it is very important that the business owner can rely on hard copies of reports that will show all the transaction input and stored in the cash register.

5 Market Parties start to pick up their Responsibility

Not only governments care but various stakeholders and marketparties are getting aware of the problem and are starting to realize that they have a responsibility as well.

The German working group on reliable cash registers INSIKA is a very successful example of an intensive cooperation between Government and marketpar-

ties. A firm basis to counter abuse of cash registers. With or without new legislation.

The cooperation of Developers, Scientists and the German Tax Administration in the INSIKA project offered society a thorough technical solution for reliable data of cash registers. The fiscal law also developed as part of INSIKA that would give a solid base for the introduction of this solution on the market did not pass political forces in Germany. Then again the technique is shared with governements and marketparties in other countries. INSIKA has been a leading example for the Dutch Tax and Customs Administration (DTCA) to cooperate with marketparties.

In Italy citizens can put an "app" on their smartphone to disclose suspected tax fraud. The application is to be found on `http://www.tassa.li/`. Tassa Li is Italian for "tax them". The idea is that people want the tax included in the price of their purchases being paid to the tax administration. It is remarkable that this is a private initiative of concerned civilians.

One of the public accounting firms in The Netherlands develops a management information system for the hospitality and catering businesses for the full chain of business processes. Ordering supplies, registration of sales, staff planning, banking up to accounting and filling out tax return forms. The sales registration is developed and supported by a developer and reseller of cash registers. Of course the accountant demands a reliable, complete and auditable cash register report in this chain of information.

Global developers of cash registers start to realize that there is a shared responsibility. In 2012 a big Japanese firm is developing two lines of reliable cash registers for the Dutch and the German market. The cash registers will be introduced on the market in autumn 2012. Obviously the attention that recently is paid to the problem by supervising Tax Administrations in different countries and the fact that this stakeholder has been involved in countering the problem results in the fact that this global player starts to pick up its responsibility.

6 The Dutch Tax and Customs Administration is exploring new Approaches

In the last decade the Dutch Tax and Customs Administration (DTCA) is developing new approaches to maintain fiscal law. The permanent objective of DTCA is to increase, keep or enforce compliance.

Computerized support of financial administrative processes is nowadays changing in a very fast pace. Online bookkeeping, data storage "in the cloud", and the rollout of Standard Business Reporting (SBR) all lead to new services and service providers.

The Horizontal Monitoring Program for Business- and Accounting Software aims at cooperation with software providers to increase the reliability and verifiability of software systems. This goal recently has been depicted in the document "Horizontal Monitoring + Software = Automatically Right from The Start".

The quality of tax returns in the end depends largely on the quality of information throughout the chain. An information chain from the complete and just registration of supplies, through complete and just registration of sales, through complete and just registration of (costs of) staff, through complete and just processing of primary data in accounting and payroll systems up to the complete and just processing of accountings in tax returns.

DTCA is involved in consultations with private parties (like software developers, software resellers and external auditfirms) to increase the quality of development of the financial chain from transaction to tax return or declaration.

6.1 Reliable Cash Registers Foundation (Stichting Betrouwbare Afrekensystemen)

On the subject of electronic sales suppression DTCA discussed the problem of sales suppression open and fair with developers, distributors and resellers of cash registers. In several meetings in different settings DTCA explained the difficulties they encounter when they investigate completeness of sales of enterprises using ordinary cash registers. DTCA even stated that in some cases the weaknesses are that apparent that developers risk the possibility to be subjected to criminal prosecution.

Market parties confirmed that cash registers tend to be that flexible that, by lack of a consistent audit trail and other measurements to ensure the integrity of data and reports, most of the cash registers are easily misused.

As solution against skimming developers and resellers of cash registers proposed to develop a quality mark for reliable cash registers. DTCA supports this idea. About 90 market parties subscribed the intention to develop the qualitymark and comply to rules of correct behaviour.

A standard for reliable cash registers has been set. The standard describes four risk area's or management objectives:

1. The integrity of the registration of all events.
2. The software.
3. The storage of the data.
4. The reports and export of the data.

The standard is available at the Reliable Cash Registers Foundation, `http://www.keurmerkafrekensystemen.nl/`.

At this moment marketparties, DTCA and public IT-auditors develop a self assessment program for the development of reliable cash registers.

Provided that Tax Administration supervises in a professional and consistent way, market parties aim at gaining market advantage by selling their products with a "Reliable Cash Register Qualitymark".

7 Responsive Supervision

The cooperation of the developers, distributors and suppliers to develop and install reliable cash register did not come spontaneous. The last decade DTCA is in different ways raising the awareness of the stakeholders that they have a responsibility in this.

There were several projects to arise attention for the quality of the sales administration of hospitality and catering business. Entrepreneurs and their fiscal advisors were informed in detail about the specific obligations for cash registers to store and hand over data in detail for investigation. When transactions are registered but have not been stored, the standard jurisprudence leads to change the burden of proof to the taxpayer.

This kind of projects led to increase of tax return up to 6 % for the area where DTCA ran these pilot projects.

Parallel to the Horizontal monitoring programme for software developers for cash registers DTCA is developing a supervision programme for the cash economy. The main idea in this programme is that any action of DTCA to maintain the law is a direct and in proportionate response to the fiscal conduct and behaviour of the taxpayer and his suppliers and advisors.

7.1 Responsive Supervision on the Detection of Phantomware in a Cash Register.

In 2010 an important development in the cash economy took place. The Dutch Fiscal Crime Unit, called FIOD, investigated a developer of points of sale. There were strong indications that one of the systems developed and sold by this entrepreneur contained zapper software. The entrepreneur is subjected to criminal prosecution.

The administration – including a client list – was confiscated. With this client list the Tax administration started an inquiry to the compliance of the clients on that list. Therefore an exploratory inspection was conducted by making copies of the data of the POS-systems from a representative group of clients. The results showed a normal compliance rate. About 85 % did not use the zapper module, 15 % however did. The trouble was to find them without using unnecessary force and misuse of means. Therefore a strategy was developed and a policy rule published.

The strategy was to ask all relevant clients of the developer to make a statement about the type of cash register they used, the actual usage of the zapper module and their willingness to repair fiscal damage and take measures to prevent damage in future. To make this an attractive option for non-compliant users of this POS a uniform fine rate was amended by the Ministry of Finance. This rule took the fact that such a user cooperated in consideration and maximised the penalty if one complied to an improvement accord. There are four conditions to participate in this accord:

- First the user has to be transparent about the facts concerning his fraud.
- Second the user needs to calculate the right turnovers and profits of the last five years.
- Third the user needs to take measures to prevent the possibility of this fraud in future.
- And last but not least, all tax bills and fines have to be paid without delay.

All this is written down in a contract and signed by the user, financial advisor, tax inspector and tax collector.

There were three kinds of reactions on the request to make the statement. A few admitted the fraud instantly. They were led into making the compliance agreement. Others denied. In this group there were some of which the tax administration had information about the use of zapper software. These became all subject of a tax audit. The ones of whom the tax administration did not have any indication of tax fraud were sometimes subjected to a compliance check to research the reliability of their declaration. Some of the users of the POS did not respond to our request at all. They were called by our local inspectors and even

visited when that didn't help. This way we received in fact all declarations we asked for.

At this moment we are evaluating the results of this strategy. One of the effects we hoped for is an effect on the producers and traders of cash registers. For years our contacts with producers and traders of these systems were on a “good to be in contact” level. Periodically some of the producers and traders were invited by the Tax administration to share information. This resulted in a brochure to inform the users of cash registers about their legal obligations. Real cooperation wasn't possible because of the complexity of the group, lack of knowledge and absence of interest to make POS reliable according to law. One can say that at that time the producers and traders of cash registers were caught in a prisoner's dilemma. The first one to develop or sell reliable cash registers would lose market share and therefore weaken his position compared to his competitors. Also the relation between producer and client was corrupted. It is the client who asks for the possibility to fraud and it is the producer who provides the means to do so. They are both caught in a fraudulent scheme and therefore susceptible to extortion.

Publication of our policy rule and the results of our explorative research caused quite a stir in the national media. The message was that the secretary of state would not accept unreliable cash registers anymore and that the tax administration had the means to detect these systems. For all users the possibility to repair fiscal damage in the past and to take measures to comply in future was presented. These publications were actively brought into the attention of the producers and traders of cash registers. The sense of urgency to undertake necessary steps towards reliable cash registers was felt. Feedback sessions were arranged and at the 18th of April 2011 a letter of intent was signed by 70 producers and traders of cash registers and the Director General of the tax administration. All parties declared that after the first of July 2013 no unreliable Points of Sale would be sold anymore and the simple cash registers would only be sold with a declaration of settings made by the producer. There will be a quality mark for reliable cash registers and points of sale.

Since then we see the market of producers and traders of cash registers organising itself. Knowledge about standards, methods and techniques are exchanged and an independent quality mark authority will be installed and functioning. (see `http://www.keurmerkafrekensystemen.nl/`) All this is done by market parties temporarily facilitated by the Tax administration.

The Dutch tax administration would like to go on on this path of improving the first and important stage in the chain from financial transaction to assessment or return. Therefore it develops a method to monitor compliance risks and enhance or enforce durable improvement of compliance behaviour. One of the ways this will be done is by influencing all relevant actors in the cash economy by making use of their interests. Much is yet to be learned but we are convinced it can be done. The cooperation of marketparties in the INSIKA project has been an inspiring example.

Krisen, Kassen, Konzepte, Kontrollen und die Betriebsprüfung[1]

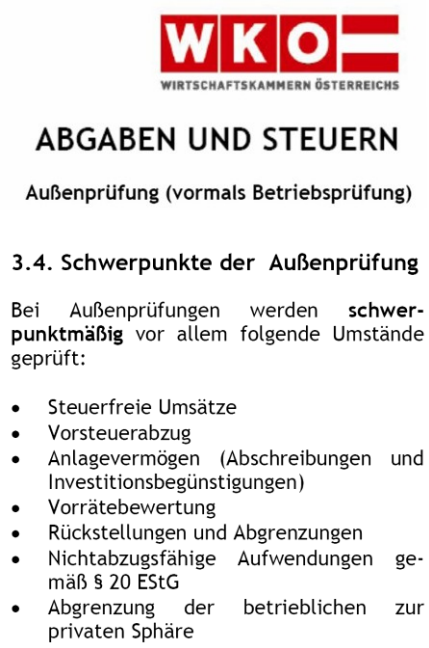
INSIKA-Inhalte als Vorbild für Österreichs steuerliches Risikomanagement im Kassenbereich

Erich Huber[2]
Bundesministerium für Finanzen, Brehmstraße 14, 1110 Wien, Österreich
erich.huber@bmf.gv.at

Zusammenfassung
Die Situation im Umfeld gesetzlicher Aufzeichnungsgrundlagen und deren Vollzug in Betrugsbekämpfung und Betriebsprüfung (BP) bei Registrierkassen (RegK) und Kassensystemen in Österreich (Ö) und Deutschland (D) ist durchaus vergleichbar. Österreich hat in der Kassenrichtlinie (KRL) 2012 die Vorgaben für eine ordnungsmäßige Kassennutzung durch die Steuerpflichtigen (StPfl) bei Erfassung der Geschäftsvorfälle (GVF) klar gestellt und überwacht deren Einhaltung über Kontrollen mittels Kassennachschauen durch die Finanzpolizei (FinPol). Als inhaltliche Grundlagen für die Kassenrichtlinie sind mehrere Punkte aus dem INSIKA-Konzept herangezogen worden, welche – wenn auch teilweise nur freiwillig erfüllbar – die Kassenmanipulation künftig erschweren sowie besser aufspürbar machen sollten, andererseits aber für jene, die die Vorgaben einhalten, Rechtssicherheit gewährleisten sollen.

1. Die Zielausrichtung der Betriebsprüfung in der Revision und die Problemebenen der Prüfansätze und der Betrugsbekämpfung im Bereich der Erlösprüfung

Modernes steuerliches Risikomanagement im Prüfungsbereich und im Umfeld der Betrugsbekämpfung bedingt die Findung von Risiken und die Ausrichtung der Ressourcen auf diese. Im Bereich der praktischen BP gibt es vielerlei Risikofelder und damit Prüfschwerpunkte – diese sind aber objektiv betrachtet ihrer Schwere und Bedeutung nach vielfach gefärbt von der Risikoorientierung und den Grundzielen der Gesamtorganisation und auch von der individuellen fachlichen Prägung des seine Prüfschwerpunkte setzenden Prüfers.
Historisch sehen viele die Aufgabe der BP in der Richtigstellung von Fehlern in Rechenwerken – meist im Bereich des materiellen Steuerrechtes oder der Buchführung an sich. Von Beginn der Geschichte der modernen BP an (30er Jahre des 20.Jhdts) begleitet den Betriebsprüfer die Aufgabe und das Image der Korrektur von Fehlbuchungen, unrichtigen Nutzungsdauern, Bewertungsfragen, Rückstellungshöhen usw. Dazu kommt auch u.a. der in der Praxis stets Stoff für Kontroversen bietende Bereich der Nichtabzugsfähigkeit von Aufwendungen, Privatanteilen oder Vorsteuern.
Als Beispiel rechts der Teil einer Veröffentlichung der ö Wirtschaftskammer, in dem als Dienst am Kunden (Steuer zahlende Wirtschaftstreibende) wohlbekannte Schwerpunkte der BP prophylaktisch angeführt werden.



WKO
WIRTSCHAFTSKAMMERN ÖSTERREICHS

ABGABEN UND STEUERN

Außenprüfung (vormals Betriebsprüfung)

3.4. Schwerpunkte der Außenprüfung

Bei Außenprüfungen werden **schwerpunktmäßig** vor allem folgende Umstände geprüft:

- Steuerfreie Umsätze
- Vorsteuerabzug
- Anlagevermögen (Abschreibungen und Investitionsbegünstigungen)
- Vorrätebewertung
- Rückstellungen und Abgrenzungen
- Nichtabzugsfähige Aufwendungen gemäß § 20 EStG
- Abgrenzung der betrieblichen zur privaten Sphäre

[1] Der Begriff „Außenprüfung“ wird im Beitrag durch „Betriebsprüfung“ (BP) ersetzt.

[2] Regierungsrat Erich Huber ist Leiter des Bereiches Prüfungs- und Analysetechnik im Risiko-, Informations- und Analysezentrum des österreichischen BMF. Er ist leitend verantwortlich für die Ausbildung der BP und Finanzpolizei im Kassenbereich über die ö. Bundesfinanzakademie und trägt als Gastdozent an der deutschen BFA in Brühl neben neuen indirekten Prüfungsmethoden auch Kassenprüfung vor. Er hat als Initiator der österreichischen Kassenrichtlinie 2012 deren Erstellung als Co-Koordinator des BMF-Arbeitskreises begleitet und ist Mitglied mehrer internationaler Kassen-Arbeitskreise. Entwicklung eines umfassenden Prüfungskonzeptes für den Risikobereich Bargeldumfeld und Publikation („neue Prüfungstechnik“). Zahlreiche Publikationen über moderne Prüfungsmethoden und steuerliches Risikomanagement im Erlösbereich. 2009 Veröffentlichung der Beitragsserie „über Registrierkassen, Phantom-ware, Zapping und Fiskallösungen aus D und Ö“ zur Kassenproblematik aus prüfungstechnischer Sicht als Erstpublikation ihrer Art im deutschen Sprachraum in stBP 09, Nr 6 bis 12. Der Autor leitet den Arbeitskreis „neue interaktive Prüfungstechnik“, in welchem führende Experten aus der Praxis der steuerlichen BP gemeinsam an der Weiterentwicklung von Theorie und Praxis in Konzepten, Methoden und Techniken der Prüfung im Erlösbereich arbeiten. Ein Großteil der Fachpublikationen des letzten Jahrzehnts zur BP im Risikofeld Barerlöse und moderne indirekte Prüfungsmethoden geht auf Mitglieder dieses Arbeitskreises zurück. Für den ständigen Erfahrungsaustausch, ohne den der Beitrag nicht in seiner Aktualität entstehen hätte können dankt der Autor einer Vielzahl von Kollegen und Kontakten, u.a. Univ-Prof. Dr. Richard Gordon *Ainsworth* (Universität Boston), Ben *van der Zwet* (Belastingsdienst NL), Walter *Wohlfahrt* (ö. Systemprüfung), Willi *Härtl* (Steuerverwaltung Bayern), Edo *Diekmann* (Steuerverwaltung Niedersachsen), Tobias *Teutemacher* (Steuerverwaltung NRW), Jens *Reckendorf* (Vectron) und nicht zuletzt Dr. Norbert *Zisky* (PTB). Erich Huber schreibt nicht in amtlicher Funktion.

doi:10.7795/210.20130206a

Bei den so zu ermittelten Feststellungen handelt es sich bis auf die nicht abzugsfähigen Aufwendungen oder Vorsteuern von den steuerlichen Auswirkungen her überwiegend um Steuerverlagerungen, also um über längere Zeiträume betrachtet aufkommensneutrale Feststellungen. Was im Jahr X zu viel abgeschrieben wurde, kann im Jahr X+1 nicht mehr abgeschrieben werden. Die Halbfertigen, welche im Jahr X aktiviert werden und dort gewinnerhöhend wirken, mindern den Gewinn des Jahres X+1, in dem die eigentliche Gewinnrealisierung stattfindet.

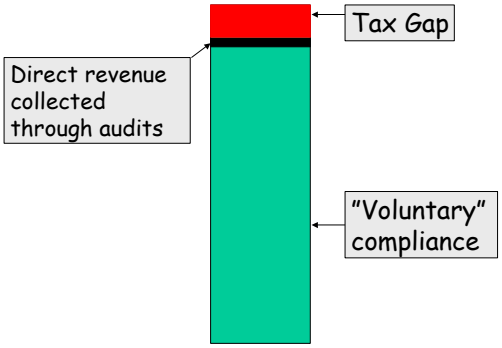
Die älteste Form[3] des Steuervergehens ist die schlichte Nichtmeldung und Nichtzahlung von Steuern aus Einnahmen – die Hinterziehung. In vielen Betriebsformen und durch mannigfache „Auslassungstaktiken" in Aufzeichnungen, Festhaltungen und Aufschreibungen entsteht hier für den Fiskus ein Großteil des Steuerlochs als einer der Ausläufer der Schattenwirtschaft.
Ein weiteres wichtiges Feld des Einsatzes der Außenprüfung liegt in der Aufdeckung von Steuerbetrug, also der ungerechtfertigten Inanspruchnahme von Steuererstattung oder -rückzahlung. Nicht, dass, wie bei der Hinterziehung, dem Fiskus zustehende Steuern nicht entrichtet werden – schlimmer - hier werden an Betrüger aus dem Staatsschatz Gelder ausbezahlt. Dieser Bereich ist erst im letzten Viertel des 20. Jahrhunderts in den Blickwinkel der Öffentlichkeit gerückt – Umsatzsteuerkarusselle, Vorsteuerschwindel, ungerechtfertigte Erstattungen von Beihilfen, Sozialbetrug kosten den Staat Geld, das er zur Erfüllung seiner Aufgaben dringend bräuchte.
Die rechts angeführte Tabelle zeigt die 3 Haupteinsatzgebiete der BP, aus welchen sich Nachforderungen ergeben können und beispielhafte Teilgebiete. Die Bereiche Mitte und rechts fallen (bis auf das Feld der nichtabzugsfähigen Aufwendungen und Vorsteuern) in den Aufgabenkreis der Betrugsbekämpfung.

Steuer-verlagerungen	endgültige Steuerausfälle	Steuerbetrug
Perioden-abgrenzungen	Steuerflucht (Oasen)	Vorsteuerschwindel
Bewertungsfragen	Steuerhinterziehung	Karusselle
Dotierung und Auflösung von Rückstellungen	nichtabzugefähige Aufwendungen, Vorsteuern	Ungerechtfertigte Beihilfen

Vom Ressourceneinsatz her gesehen geht viel in den ersten Aufgabenkreis, den der Gewährleistung der Rechtsrichtigkeit. Hier werden auch große BP-Mehrergebnisse erzielt – zB bei der Änderung von Bewertungen im Bereich der Groß-BP[4]. Nicht immer und überall gibt es hier lückenlose Anschlussprüfungen. Irgendwann in der Folge werden die Bewertungsänderungen aufgeholt – meist in ungeprüften Jahren (wäre ja sonst ein hohes Minderergebnis) und gehen dann zulasten des echten Steueraufkommens. Auch im Mittel- und Kleinbetriebsbereich verbringen manche Prüfer Tage damit, u.a. Aufwände und Erträge dem komplexen Steuerrecht gemäß zu korrigieren, periodenmäßig korrekt abzugrenzen und den Wust der gegenseitigen Auswirkungen in Bilanz, V+G-Rechnung, EA-Rechnung sowie Konten einzuarbeiten und die einzelnen Steuern wieder richtig zu stellen. Hier im Jahr X ein Plus von 200, da ein Minus von 150, dort im Jahr X+1 ein Minus von 200 und ein Plus von 220. Unterm Strich bleibt üblicherweise eine Steuernachzahlung[5]. Viele von diesen Richtigstellungen bewirken in gewisser Weise wohl eine relativ hohe Rechtsrichtigkeit im Einzelfall, aber um welchen Einsatz im Vergleich zum fiskalischen Ergebnis? Es gibt Fälle, in welchen Prüfer über Fehler, regelrecht „stolpern" müssen – weil sie so offensichtlich sind[6] – damit auch rasch an ein Mehrergebnis kommen[7] und den Rest der zur Prüfung verfügbaren Zeit mit den Folgekorrekturen verbringen. In die Aufdeckung von Steuerbetrug schließlich werden hohe Ressourcen investiert – dennoch ist die

[3] Das Problem ist so alt wie die Steuern selbst. Die Gegenmaßnahmen haben von ihrer Schwere her aber nachgelassen. Aus dem alten Ägypten wir berichtet, man hätte dort Steuerhinterziehern die Nase abgeschnitten.
[4] Siehe *Tipke*, Das Dilemma der Steuerverwaltung – zeitnahe oder gesetzmäßige Besteuerung, StWa 1994, S.- 221 ff. Je kleiner der Stpfl ist oder sich gibt, desto „maßvoller" der Gesetzesvollzug – bis hin zur maßlosen Großzügigkeit der Nichtkontrolle. Richtiger Maßstab für die gebotene Kontroll- und Prüfintensität ist nicht die Fallgröße, sondern das individuelle Kontrollbedürfnis. Große Steuerpflichtige sind im Durchschnitt sicher nicht mehr prüfungsbedürftig als kleine. Sie bringen dem Staat aber mehr Geld. Aber das ist nicht der geeignete Maßstab für das Kontrollbedürnis.
[5] Es wäre interessant festzustellen, ob bestimmte solcher Verlagerungsfeststellungen getroffen würden, wenn der selbe Betriebsprüfer den selben Fall immer wieder und weiter lückenlos prüfen müsste, weil ja die Mehrergebnisse aus Verlagerungen in den Folgejahren zu Minderergebnissen werden. Es wäre weiter auch interessant festzustellen, wie viel von hohen und statistisch als Erfolg ausgewiesenen Mehrergebnissen aus Verlagerungen in Folgejahren als Minderergebnisse das echte Steueraufkommen vermindern, ohne dass dies gesondert auffällt.
[6] *Schick* (HHSp vor §193, Tz. 64) führt bei der Besprechung der präventiven Wirkung der BP – der Tatsache, dass die Stpfl. sich von unzulässigen Steuerverkürzungen abhalten lassen zur Vervollständigung eines wirklichkeitsgetreuen Bildes auch Gegenstrategien an: Bei Bewertungen entschieden sie sich vorerst zu ihren Gunsten und warteten ab, ob der Prüfer einhake. Andererseits würden in die Buchführung leicht auffindbare Schwachstellen eingebaut, deren Aufdeckung dem Prüfer ein Erfolgserlebnis vermitteln soll, die als Tauschobjekt dienen könnten. Bewertungsänderungen bedingen eine u.U. langzeitige Steuerverlagerung. Die leicht erkennbaren Schwachstellen werden nur oberflächliche Prüfer an der tiefen Durchdringung des Sachverhaltes und der Buchführung und damit dem Auffinden der wahren Schwachstellen hindern. Die systematische Abstimmung einer Buchführung als die wahrscheinlich „effektivste Gegenstrategie" führt bei Nichtaufdeckung tatsächlich zu endgültigen Steuerausfällen.
[7] Siehe trend 12/2006: zu den Klassikern der eingebauten Sollbruchstellen in Rechenwerken würden absichtlich zu niedrig angesetzte Privatanteile bei Auto oder Telefon, oder die besonders großzügige Bemessung von Rückstellungen zählen.

frühe Entdeckungswahrscheinlichkeit gering. Bei späterer – wohl sensationell medienwirksamer - Aufdeckung ist die Vorschreibung von hohen Steuern meist aber nur mehr eine Feststellung des entstandenen Schadens ohne dessen erfolgreiche Aufholung oder Rückforderung.
Daneben bleiben großflächige Bereiche mit hohem und höchstem Risiko endgültiger Steuerausfälle durch Steuerhinterziehung ungeprüft. Es sind meist kleinere und mittlere Betriebe, die in den Bargeldhochrisikobranchen betroffen sind, doch von diesen gibt es sehr viele und die hinterzogenen Steuern sind meist kaum in voller Höher rückholbar (im Gegensatz zur Verlagerung einer durch verzögerte Gewinnrealisierung um ein Jahr verschobenen Steuern).
Diese Problemsituation hat in der letzten Zeit durch die Krise[8] zusätzliche Bedeutung erfahren. Die Kernfrage ist: Was ist die wahre Aufgabe der BP in der Krise ? Was sollte die BP bewirken? Ist es der Lösung von desaströsen Defiziten in Staatshaushalten förderlich, wenn die meisten europäischen Betriebsprüfungen weiterhin die Erzielung hoher optischer Mehrergebnisse als präsentablem Selbstzweck[9] verfolgen, von denen ein unbekannter (aber nicht unbedeutender) Teil uU gar nicht eingebracht werden kann oder diesfalls gleich gar nicht vorgeschrieben wird? Die rechts unten gezeigte OECD-Darstellung des Verhältnisses zwischen den Steuern, die durch freiwillige Mitwirkung (voluntary compliance) herein kommen mit rd. 90%, dem Steuerloch (Tax Gap) mit etwa 9% und dem Ergebnis der Nachforderungen aus BPs (audits), das etwa 1% des Aufkommens ausmacht, zeigt die Verhältnisse im Vereinigten Königreich, passt aber in etwa für die meisten Staaten Mittel- und Westeuropas. Es sollte bei eingehender Betrachtung auch die Wertung der Maßnahmen der Steuerbehörden neu ausrichten. Die fortlaufenden Bestrebungen, das Steuerloch zu verkleinern (und damit den Anteil der durch BP nachzufordernden Steuern zu maximieren) sind von ihrer Konzeption her nach den Erfahrungen langjähriger Anwendung offenbar doch nicht so ziel führend, wie erwartet oder erhofft. Moderne Steuerverwaltungen erkennen aber die Risiken, die damit verbunden sind, wenn - aufgrund welcher Ursachen auch immer – die voluntary compliance nachlässt, was zu dramatischen Ausfällen führen kann.



Die BP in Europa trägt also zu etwa 1% (wenn überhaupt) zum Gesamtbudget bei. In der Krise verringert sich der Teil des Gesamtaufkommens, welcher durch voluntary compliance hereinkommt, signifikant. Wenn dem Unternehmer wirtschaftlich das Wasser bis zum Hals steht, schrumpft „automatisch" sein fiskalischer Altruismus. Schwarzarbeit, Hinterziehung und Abgabenbetrug nehmen dramatisch zu[10]. Das Steuerrecht, welches nach dem Willen von Fachleuten seit Jahrzehnten einfacher werden soll, aber nicht werden will, hat sich für den einzelnen Bearbeiter zu einem unübersehbaren Moloch entwickelt. Die BP investiert einen Großteil ihrer schwindenden Ressourcen, die Rechtsrichtigkeit sicherzustellen. So lange umfassende Prüfwahrscheinlichkeit besteht und solange auch endgültige Steuerausfälle anderer Art (zB Hinterziehung) flächendeckend geprüft werden, sind dagegen keine Bedenken anzumelden. Nun müssen die Steuerverwaltungen bei steigender Menge der Steuersubjekte aber zunehmend unter merklichen Verwaltungseinsparungen[11] arbeiten. Die Prüfungsdichten bei Klein und Kleinstbetrieben (oder Betrieben, die sich als solche „verkleiden", solange bis eine Prüfungsmaßnahme Platz greift), nähern sich dem 100Jahre-Bereich[12]. Es ist zu hinterfragen, ob das Grundkonzept noch zeitgemäß bzw unter dem Grundsatz der Gleichmäßigkeit[13] noch rechtmäßig[14]. ist.

---

[8] *Tipke* Steuerrechtsordnung, Bd. III S. 1404 sieht im Ausgleich von Steuerhinterziehungen durch Steuererhöhungen keinen Akt der Gerechtigkeit, da die Steuerehrlichen auch von der Steuererhöhung wieder am stärksten betroffen werden.

[9] Schon *Grabower* zur steuerlichen BP, StuW 1956 S. 612 betont, dass die Betriebsprüfer falsch erzogen würden, wenn die BP in erster Linie auf fiskalischen Gesichtspunkten beruhe. *La rage du nombre* würde sie dann regieren. Ein derart fiskalisches Denken sei *Popitz* bei Wiederaufbau der BP fremd gewesen. Natürlich wusste er, dass in der BP erhebliche Reserven steckten und dass sie in vielen Fällen kein harmloser Spaziergang sei. Der Hauptgrund ihrer Einführung und ihres Aufbaus bestand aber darin, nach Möglichkeit für steuerliche Gleichmäßigkeit zu sorgen und gewissenlose Stpfl daran zu hindern, durch illegale Steuervermeidungen ihre steuerliche Konkurrenz tot zu machen. Siehe auch *Eckhoff* in HHSp, vor § 193 – 203, 159: Nicht die Summe der Mehrergebnisse, sondern vielmehr die generalpräventive Wirkung ist das eigentliche Ziel der Außenprüfung.

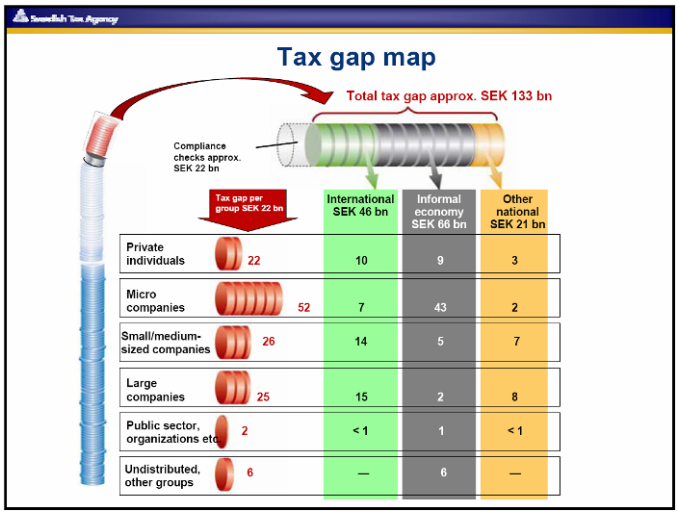
[10] Wie hoch ist die wahre Bedeutung von BP-Mehrergebnissen unter der fiskalischen Bedrohung durch eine 15%-ige Schattenwirtschaft? - siehe http://www.welt.de/wirtschaft/article4599093/In-der-Krise-boomt-die-Schwarzarbeit.html

[11] *Tipke*, in Tipke/Kruse § 88, Rz. 10, S. 1406 bemerkt, wenn sich ein StPfl unter Herabsetzung der steuermoralischen Hemmschwelle zur Hinterziehung entschließe im Wissen oder Glauben, dass alle oder viele andere es ebenso tun, Bestrafung des einzelnen nichts helfe, sondern nur die Wiederherstellung einer durchgehend effizienten Kontrolle zur Erhöhung der Entdeckungswahrscheinlichkeit

[12] *Tipke, Kruse* AO, § 193, Tz 30 stellen fest, dass Klein- und Kleinstbetriebe besonders prüfungsbedürftig seien, wenn man die Mehrergebnisse in ein Verhältnis zum Umsatz bringe. Die zunehmenden Verkürzungen erklärten sich aus zeitlich sehr langen Intervallen zwischen BPs bei solchen Betrieben (kaum neuerliche Prüfung innerhalb einer Generation)

[13] *Tipke*, Steuerrechtsordnung, Bd. III, S. 1406, 1407: Ein Stpfl kann sich zur Steuerhinterziehung auch entschließen, weil er weiß oder glaubt, dass alle oder viele andere es ebenso tun. Demgegenüber hilft u.a. nur eins: effiziente Kontrollen zur Erhöhung der Entdeckungswahrscheinlichkeit, weniger die Bestrafung einzelner, die zufällig aufgefallen sind, sondern die Wiederherstellung durchgehend effizienter

Aus der nachfolgende Folie der schwedischen Steuerverwaltung geht hervor, dass der größte Anteil des fiskalischen Risikos im Steuerloch (Tax Gap) auf kleine (u. mittlere) Betriebe zurückzuführen ist.



Die beiden Grenzansätze sollten als Alternativen unter der Sicht eben dieser begrenzten Ressourcen und der möglichen Auswirkungen von Risiken beurteilt werden:

- Umfassende Rechtsrichtigkeit der Besteuerung im isolierten Einzelfall auf Kosten weit verbreiteter Ungleichmäßigkeit der Besteuerung
- Garantie einer so hohen allgemeinen Gleichmäßigkeit der Besteuerung wie durch optimale Ressourcennutzung möglich

Im Bereich der Gleichmäßigkeit ist es vor allem die Verhinderung der Steuerhinterzeihung, welche auf breiter Flur betrieben, der Allgemeinheit essentielle fiskalische Substanz kostet. Die Schattenwirtschaft spannt sich vom kriminellen Bereich (Menschenhandel, Prostitution, Drogenhandel) über Nachbarschaftshilfe (beim privaten „Häuslebau“) und einträgliche Privatjobs (Nachhilfe, Hobbykeksebacken, private Hundezucht, …) über den professionellen Pfusch (unangemeldete Hilfskräfte am Bau) bis eben zur professionellen Verkürzung von Umsätzen in Betriebsformen mit hohem Bargeldfluss und Leistung an Endverbraucher. In diesem letztgenannten Bereich wird aber - nicht so wie beim Rest ausschließlich der Fiskus betrogen, weil keine Steuern oder Beiträge abgeführt werden – an diesen laufen die Leistungen einfach vorbei – sondern auch in entscheidendem Ausmaß der Konsument, welcher für eine Leistung oder ein Produkt Umsatzsteuer zahlt, die dann der Entgeltsempfänger einbehält“. Der Bogen spannt sich über eine Vielzahl von Betriebsformen, wie zB Einzelhandel, Kleinproduzenten (Bäcker, Metzger, ...), Gastronomie, Hotellerie, Eventbetriebe, Handwerk, Dienstleister (Friseure, Taxis,...) aber auch so genannte „seriöse Branchen, zB Gesundheitsbereich (Ärzte, Apotheken, ...). In einer überwiegenden Mehrzahl der Fälle sind hier elektronische Abrechnungssysteme oder RegK mit im Spiel.

2. Entwicklung – Betriebsprüfung, Zeitebenen und Vorsysteme

2.1 historische Entwicklung

Der nachfolgende schlagwortartige Rückblick auf die Entwicklung der Prüfungstechnik, ihrer Wirkungsziele, der Risikoausrichtung der steuerlichen BP, der Aufzeichnungstechnik, der Manipulationsmorphologie und der Aufdeckungsmechanismen und ihrer Entdeckungswahrscheinlichkeit soll das Umfeld sowie seinen inneren Strukturwandel insbesondere unter Sicht der Erlösverkürzung punktuell darstellen, aber doch umfassend beleuchten.
Von besonderer Bedeutung dabei sind die Veränderung der Zielrichtung (ev. auch der „Werte“), des Risikobewußtseins und der Achtung der Bedeutung von Information über den gegenwärtigen[15] Zustand zur Risikobeurteilung, also die Diskrepanz zwischen Revision[16] der Vergangenheit (Buch-Einschau in aufgezeichnete Vergangenheit) und Steueraufsicht (tatsächliche Kontrolle der echten gegenwärtigen Verhältnisse und Aufzeichnungen in der Gegenwart), somit des Gegenwartsbezuges des steuerlichen Risikomaßnahmen. Stets ist aber im Hintergrund das Auseinanderklaffen der Realitätsnähe[17] der jeweiligen Maßnahme zu sehen. Hinzuzufügen ist noch, dass eine Zielausrichtung der BP-Ressourcen auf die Risikobereiche bei wirksamen Maßnahmen unmittelbar in der Konfrontation mit dem seine steuerlichen Pflichten nicht erfüllenden StPfl mündet, während die „Virtuosität

---

Kontrolle, die sichtbare Anwendung des Gesetzes auf alle. Geschieht das nicht, so ist die Steuerhinterziehung ein vom Staat zu verantwortender, dem Staat anzulastender Akt rechtlicher Notwehr zur Herstellung faktischer Belastungsgleichheit

[14] *Tipke*, Steuerrechtsordnung, Bd. III, S. 1407 Wenn ungleichmäßige Gesetzesanwendung, wenn der Gesetzesbruch mit staatlicher Duldung zur Regel wird, wird das Herausgreifen einzelner – mit denen ausnahmsweise nach dem Gesetz verfahren wird – zur Willkür

[15] *Seer*, Reform des Veranlagungsverfahrens, StuW 2003, S. 55, betont, dass einem kooperativen Steuerrechtsverhältnis das Prinzip zeitnaher Besteuerung entspreche, wobei die wirtschaftliche Leistungsfähigkeit abzuschöpfen sei, solange sie in Form von Liquidität noch vorhanden sei.

[16] Im Zuge der BP wird in der Regel ein Sachverhalt beurteilt, der vergangen ist. Die in der Vergangenheit liegenden Tatsachen können nicht mit absoluter Gewissheit erkannt werden, da die Wahrheit der menschlichen Erkenntnis verschlossen ist. Es geht vielmehr darum, der Wirklichkeit möglichst nahe zu kommen, somit in einem geordneten Verfahren jene Feststellungen zu treffen, von denen anzunehmen ist, dass sie dem tatsächlichen Geschehen in einem hohen Maße entsprechen und zwar in einem höheren Maße als andere ebenfalls mögliche Sachverhaltsannahmen, siehe auch *Stoll* BAO § 166,S 1754

[17] Wegen der Unmöglichkeit absoluter Gewissheit gilt im praktischen Leben der hohe Grad der Wahrscheinlichkeit, der anzunehmen ist, wenn kein vernünftiger, die Lebensverhältnisse klar überschauender Mensch noch zweifelt. Letztlich bildet der festgestellte und nicht der tatsächliche Sachverhalt die Grundlage für die behördliche Entscheidung *Siehe Kelsen* , reine Rechtslehre S 245

der Rückverschiebung von Steuerverlagerungen“ primär in einem „Klima der Partnerschaft“ abläuft, frei nach dem Motto „bei einer BP muss immer was rauskommen“ oder – schlimmer „was der Prüfer nicht sieht, sieht nach ihm auch niemand mehr – egal, Hauptsache bei der BP kommt was raus“.

„RAO- Zeit (~ 1920er bis ~ 1960er)

- Zeit der RAO-Einführung
- Schlagwort - „*wenn die BP fertig ist, ist in der Buchführung alles richtig*“
- technischer Aufzeichnungsstatus: Handschrift / Mechanik (Grundrechnungsarten) / Papierdruck
- erste BP-Interessensebene = Buchungsebene
  - Risiko Buchungsfehler
- Ziel – *richtige Buchhaltung und gerechte Besteuerung*
- Weg zum Ziel
  - Revision + Steueraufsicht
- Verprobung und Überprüfung
  - Verprobungen auf Summenebene können Verkürzungen finden (auch quantitativ)
- Voraufzeichnungen führen und aufbewahren
  - Risiko Fälschung / Nichtvorlage von Voraufzeichnungen
  - durch sachverständigen Dritten / Nachschau leicht prüfbar / kontrollierbar

„Rechentechnik-Zeit (~ 1970er bis ~ 1980er)

- Zeit der Einführung der EDV-Bestimmungen in AO
- Schlagwort - „*BP auf Ebene Maschinen- oder EDV-Buchführung durch moderne Prüfer mit Taschenrechner bis Laptop*“
- technischer Aufzeichnungsstatus: Mechanik / Elektrik / Primitiv-Programmierung
- erste BP-Interessensebene = Buchungsebene
  - Risiko Buchungsfehler
- Ziel – *rechtsrichtige Buchführung*
- Weg zum Ziel
  - Revision drängt Steueraufsicht in den Hintergrund
  - Revision argumentiert mit Formalmängeln, NOM für Schätzung
- Verprobung und Überprüfung
  - Verprobungen auf Summenebene können Verkürzungen meist finden (zunehmend weniger quantitativ)
  - aber: zunehmende Anpassung der Manipulation an Verprobungsmethoden der BP
- Voraufzeichnungen führen und aufbewahren
  - Risiko Fälschung / Nichtvorlage von Voraufzeichnungen
  - durch Nachschau leicht kontrollierbar
  - Relativ geringes Risiko Manipulation durch EDV
  - Programmierungen durch sachverständigen Dritten leicht prüfbar, Umprogrammierungen aufwendig
  - vor allem in summenspeicherbasierten Kassen Primitivschwindel mit nachträglicher Löschung von Speichern, veränderten Druckeinstellungen

„PC-Zeit (~ 1990er bis ~ 2007)

- Zeit der Nutzung komplexer Software (zB Datenbanken) im Primärbereich
- Schlagwort - „*vor der Buchhaltung existieren auch noch andere Prüfungsfelder*“
- technischer Aufzeichnungsstatus: PC-Nutzung in Buchhaltung und Vorsystemen- „weg vom Papier“
- erste BP-Interessensebene in „klassischer BP“ = Buchungsebene
  - Risiko Buchungsfehler aber zu vernachlässigen
- Steuerliche Betrugsbekämpfung und Risikobewußtsein kommt auf: dort erste Interessensebene = Primärebene
- Ziel – „*public management*“ - erfolgsorientierte Außen-Selbstdarstellung der Finanzverwaltung[18]
- Weg zum Ziel
  - Revision mit Mehrergebnissen

[18] Zur unendlichen Mehrergebnisdiskussion in der BP siehe z.B. *Muus*, Scheingewinne der BP, StBp 1983, S. 80 und die dort zitierte Literatur, sowie *Neddermeyer*, BB 1995, S. 1378, Die AP als Mittel zur vollständigen Ausschöpfung der Steuerquellen, welcher auch Vorschläge der Arthur Anderson Management Beratung anführt, wie die prüfungsbedürftigen Unternehmen anhand einer Checkliste ermitteln zu lassen, dieses Auswahlverfahren durch eine echte Zufallsauswahl zu ergänzen und die Anschlussprüfungsbedürftigkeit der Großbetriebe einer kritischen Würdigung zu unterziehen. Die Mehrergebnisse aus Großbetrieben würden zu einem erheblichen Teil auf Gewinnverlagerungen beruhen, welche für das Steueraufkommen eine nur geringe Bedeutung hätten (S. 1385).

  - Steueraufsicht bringt keine unmittelbaren Mehrergebnisse, kostet aber Ressourcen, wird zunehmend von der Wertigkeit her in den Hintergrund gedrängt
  - Revision argumentiert mit Formalmängeln und Nichtordnungsmäßigkeit für rasche Schätzung (abseits echter Größenordnungen)
- Verprobung und Überprüfung:
  - Verprobungen auf Summenebene finden nicht alle Verkürzungen
  - Weitgehende Anpassung der Manipulation an Verprobungsmethoden der BP
  - Überprüfung und Verprobung auf Primärebene (neue Prüfungstechnik) kann Verkürzungen finden (manchmal auch quantitativ)
- Voraufzeichnungen führen und aufbewahren
  - Primärsystem muß durchschaubar sein
  - erste Interessensebene = Primäraufzeichnungsebene
  - Risiko Fälschung / Nichtvorlage von Voraufzeichnungen / dann auch von Primärdaten
  - durch Nachschau leicht prüfbar, aber wenig Steueraufsicht (s.o.)
  - hohes Risiko Manipulation durch EDV
  - Programmierungen durch sachverständigen Dritten prüfbar, aber Umprogrammierungen rasch möglich
  - zapper, jumper, recaller, styler, fixer, concealer in Datenbanksystemen

„Androiden.Zeit“ (~ ab 2007)

- Zeit der Einführung von komplexen Betriebssystemen im Primärbereich
- Schlagwort - „*alles ist möglich – auch bei Kassen*“
- Technischer Aufzeichnungsstatus: Einsatz von Betriebssystemen statt Programmierung im Elektronikbereich
- erste BP-Interessensebene in „klassischer BP“ = Buchungsebene
  - Risiko Buchungsfehler tatsächlich zu vernachlässigen
- erste BP-Interessensebene in Betrugsbekämpfung = Primärebene
- Ziel – *Risikomanagement und Garantie des Steueraufkommens*
- Weg zum Ziel
- gezielte Steueraufsicht auf Datenebene mit Folgerevision
- Verprobung und Überprüfung
  - Verprobungen auf Summenebene nahezu sinnlos
  - Überprüfung, Verprobung auf Primärebene (NPT) kann manchmal Verkürzungen finden -
  - aber kaum deren Ausmaße wegen zunehmend Modell erfüllender Manipulation auf Vorebene
- Voraufzeichnungen führen und aufbewahren
  - Primärsystem muß durchschaubar sein
  - erste Interessensebene = Primäraufzeichnungsebene
  - Risiko Fälschung / Nichtvorlage von Voraufzeichnungen / Primärdaten
  - durch Nachschau (mit Datenzugriff) leicht kontrollierbar
  - Höchstes Risiko Manipulation durch EDV
  - Programmierungen durch sachverständige Dritte wegen Systemdifferenzierungen und Systemvielfalt kaum mehr flächendeckend prüfbar, Umprogrammierungen unmittelbar möglich
  - Komplexe Manipulation auch in „einfachen“ Vorsystemen

2.2 historische Grundlagen für moderne Grundsätze und effektive Maßnahmen

Rück- und überblickend kann objektiv festgestellt werden, dass all jene modernen Finanzverwaltungen, welche mit der Risikoorientierung schon die richtige Richtung eingeschlagen haben, vielleicht sogar schon auf dem richtigen Weg sind. Risikobezug und Ausrichtung der Ressourcennutzung auf die „Spitze des Eisbergs“, also jene Bereiche, welche das höchste tatsächliche fiskalische Ausfallsrisiko haben, sowie die Schaffung neuer oder die Rückbesinnung auf effektive „alte“ Maßnahmenkomplexe, welche von hohem Gegenwartsbezug sind, können am ehesten unter den schwindenden zeitlichen und personellen Vorräten der Steuerverwaltung eine Gleichmäßigkeit bzw. Rechtmäßigkeit herbeiführen. Ein Musterbeispiel dafür ist die von der Bedeutung her wörtlich zu verstehende Steueraufsicht, also das Bündel aller Maßnahmen, die die Supervision über das steuerliche Verhalten der StPfl in gegenwärtigem Zeitbezug ermöglichen, was rechtzeitige Reaktionen (also tatsächliche Verhinderung oder Rückgängigmachung von unmittelbar bevorstehenden oder gerade erst eingetreten Schäden bei Unehrlichkeit) nach sich ziehen kann.
Die Ansätze des moderne steuerlichen Risikomanagements und der Compliance, welches überwiegend aus dem außerdeutschen Umfeld (NL, nordische Länder, Kanada, Australien, UK) über D und Ö kamen, sind keineswegs so neu wie sie sich (oft gut) verkaufen. Ebenso verhält es sich mit modernen Aufzeichnungsgrundsätzen im EDV-Bereich.

Kehrt man zurück zu den Wurzeln all der steuerlichen Maßnahmen im deutschsprachigen Raum, kommt man unweigerlich an den Vater der Reichsabgabenordnung, Dr. Enno Becker (siehe Foto).
Als nahezu visionär kann seine Formulierung des § 162 der Reichabgabenordnung 1919 gelten, sie ist in Wahrheit heute noch Fundament der Formgrundsätze im Umfeld der steuerlichen Grundaufzeichnungen / Vorsystemdaten bzw der Beurteilung von deren Ordnungsmäßigkeit:

So hat Dr. Enno Becker auf damalig technisch einfache Formulierung hin die Wurzeln folgender hoch aktueller Grundsätze der Primärerfassung steuerlich relevanter GVF gepflanzt:

- **Elektronisches Radierverbot**, also die Verhinderung von Datenveränderung in quantitativer und noch wichtiger – in qualitativer Hinsicht, so hin die Gefahr, dass nicht nur hinsichtlich des Ausmaßes eines bestimmten erfassten Betrages Zweifel bestehen, sondern auch – und dies ist das höhere Risiko – Zweifel, ob ein ursprünglich erfasster Betrag „am Ende“ überhaupt noch in den Kontensummen enthalten ist
- **Sicherung der Primärdaten** wegen deren grundlegender Bedeutung im Zusammenhang mit Summenbildung (Betragsverdichtung), welche eine ureigensten Eigenschaften (aber auch der höchsten Risiken) der Buchhaltung ist
- Belegnummerierung im besonderen – im allgemeinen **Grundsatz der fortlaufenden Nummerierung**, also der Einrichtung zur Schaffung einer eineindeutigen Identifizierbarkeit des einzelnen in der Aufzeichnung zu erfassenden Objektes auf eine Weise, die einem sachverständige Dritten die echte Prüfung der Vollständigkeit in höchster Prüfqualität ermöglicht (einem Prüfer, welcher aber nicht zwingend von gleicher technischer Qualifikation wie derjenige sein muß, welcher das Aufzeichnungssystem technisch umgesetzt hat[19])

§ **162** (§ 162)

(1) Wer nach den Vorschriften der §§ 160 und 161 oder sonst nach den Steuergesetzen Bücher zu führen oder Aufzeichnungen zu machen hat, soll die folgenden Vorschriften beachten.

(2) Die Eintragungen in die Bücher sollen fortlaufend, vollständig und richtig bewirkt werden. Der Steuerpflichtige soll sich einer lebenden Sprache und der Schriftzeichen einer solchen bedienen.

(3) Geschäftsbücher sollen keine Konten enthalten, die auf einen falschen oder erdichteten Namen lauten.

(4) Die Bücher sollen, soweit es geschäftsüblich ist, gebunden und Blatt für Blatt oder Seite für Seite mit fortlaufenden Zahlen versehen sein.

(5) An Stellen, die der Regel nach zu beschreiben sind, sollen keine leeren Zwischenräume gelassen werden. Der ursprüngliche Inhalt einer Eintragung soll nicht mittels Durchstreichens oder auf andere Weise unleserlich gemacht, es soll nicht radiert, auch sollen solche Veränderungen nicht vorgenommen werden, deren Beschaffenheit es ungewiß läßt, ob sie bei der ursprünglichen Eintragung oder erst später vorgenommen sind.

(6) In Bücher soll, wo dies geschäftsüblich ist, mit Tinte eingetragen werden. Trägt der Steuerpflichtige nach vorläufigen Aufzeichnungen ein, so soll er diese aufbewahren. Belege sollen mit Nummern versehen und gleichfalls aufbewahrt werden.

(7) Kasseneinnahmen und -ausgaben sollen im geschäftlichen Verkehr mindestens täglich aufgezeichnet werden.

Doch nicht nur die Soll-Vorgaben im Aufzeichnungsumfeld, auch die Grundlagen für Maßnahmen zur Gewährleistung von deren Einhaltung finden sich in Enno Beckers Reichsabgabenordnung.

Nach einem RFH-Erkenntnis vom 2.10.1929, RFHE 25, 349 dient die Nachschau der Feststellung ob die Stpfl die ihnen im Interesse der Besteuerung auferlegten Pflichten erfüllen, sowie der Vorsorge für die Sicherung der Abgabenansprüche, wenn sich aus Feststellungen ergibt, dass gegenwärtige oder künftige Abgabenansprüche gefährdet sind oder gefährdet sein könnten.

§ **193** (§ 196)

(1) Für Zwecke der Besteuerung kann das Finanzamt auch außerhalb eines Steuerermittlungsverfahrens Nachschau halten bei den Personen, die nach § 160 Absatz 2 Aufzeichnungen zu machen haben, sowie bei solchen Unternehmern und in solchen Unternehmen, die entweder einer Steuer oder der Steueraufsicht unterliegen oder bei denen nach dem Ermessen des Finanzamts eine Steuerpflicht in Betracht kommt.

[19] Zur Frage der Qualifikation des sachverständigen Dritten siehe Punkt 6.4 Exkurs Fiskalspeicher und Ordnungsmäßigkeitsvermutung aus historischer Sicht und unter Betrachtung des § 146 (4) AO.

Hier sind für die Nachschau moderne Grundsätze im steuerlichen Risikomanagement vordefiniert worden:

- **Die Compliancefeststellung**

die Nachschau dient der Feststellung, ob die Stpfl die ihnen im Interesse der Besteuerung auferlegten Pflichten erfüllen

- **die Risikobeurteilung (Risikoskalierung) und die vorsorgliche Abgabensicherung**

die Nachschau dient der Vorsorge für die Sicherung der Abgabenansprüche, wenn sich aus Feststellungen ergibt, dass gegenwärtige oder künftige Abgabenansprüche gefährdet sind oder gefährdet sein könnten.

Zusammengefasst kann festgestellt werden:

die Nachschau ist ein überaus zeitgemäßes und modernes Instrument
- der Informationsbeschaffung
- des Risikomanagements
- der Compliance-Findung

die Nachschau dient der
- Feststellung der Erfüllung von Mitwirkungspflichten
  - Aufzeichnung
  - Aufbewahrung
  - Offenlegung
  - Mitwirkung i.e.S.
- Feststellung der Gefährdung von Abgabenansprüchen
- Vorsorge der Sicherung der Abgabenansprüche

Auf die heutige Situation im betrieblichen, technischen und steuerlichen Umfeld der Erlöserfassung bezogen kann also festgestellt werden, dass die Fundamentalgrundsätze formuliert und lange bekannt sind – es geht um deren faktische Umsetzung und dauernde Gewährleistung in flächendeckendem Umfang.
Je mehr der Steuerverwaltung die Ermittlung des Gegenwartsbezug der Steueraufsicht in Richtung auf inhaltliche, also sachlich richtige Aufzeichnungsgewähr durch einen technisch machbaren aber dann auch tatsächlich einzusetzenden „Automatismus“ mittels einer mechanistisch wirkenden Einrichtung[20] wie INSIKA abgenommen werden kann, umso mehr kann sich diese durch die zügig durchführbaren und hoch aussagekräftigen Kontrollmaßnahmen unter Nutzung der Smartcard-Prüfung bei schwindenden Ressourcen und damit schwindender Reaktionsfähigkeit[21] auch tatsächlich auf breitester Ebene der Umsetzung des Grundsatzes der Steuergerechtigkeit widmen.

3. Manipulation mit Registrierkassen und Kassensystemen

3.1 Kassenmanipulanten

Das Manipulationsproblem ist so alt wie die RegK selbst.
Der gewerbliche Steuerbetrüger des 21. Jhds hat 2 Interessensaspekte, die unmittelbar miteinander kollidieren: einerseits will er genaue Übersicht über sein betriebliches Ergebnis („Erfolg“) sowie Kontrolle über sein Personal – dies bedingt eine systematische und genaue Erfassung von Geschäftfalldaten. Andererseits würden genau diese Daten der Finanzverwaltung in die Hände kommen und gegen ihn verwendet werden - falls er überhaupt geprüft wird. Dann werden also diverse Taktiken und Scheinargumente eingesetzt, um dieser Schere erfolgreich unter Nichtvorlage von Daten oder Aufzeichnungen zu entkommen. In BP mit Kassenmängeln treten bestimmte Typen (überspitzt dargestellt) wiederkehrend auf:

[20] Im Veranlagungsverfahren bedarf das Deklarationsprinzip der Ergänzung durch das Verifikationsprinzip. BVerfG v. 27.6.1991 2 BvR 1493/89, BVerfGE 84, 239, 273 – Zinsurteil. Regelungen, die die Durchsetzung des Steueranspruches sichern und Steuerverkürzungen verhindern sollen, müssen auf die Eigenart des konkreten Lebensbereiches und des jeweiligen Steuertatbestandes ausgerichtet werden. Wird eine Steuer nicht an der Quelle erhoben, hängt ihre Festsetzung vielmehr von der Erklärung des Steuerschuldners ab, werden erhöhte Anforderungen an die Steuerehrlichkeit des StPfl gestellt. Der Gesetzgeber muss die Steuerehrlichkeit deshalb durch hinreichende, die steuerliche Belastungsgleichheit gewährleistende Kontrollmöglichkeiten abstützen.

[21] Die Steuerverwaltung ist wie alle Organisationen als nichtlineares dynamisches System in die sie umgebenden gesellschaftlichen Systeme eingebunden. Bedingt durch die Zeitschere (je komplexer Strukturen sich entwickeln, umso höher wird ihre Reaktionszeit, je dynamischer die Umwelt sich entwickelt, umso weniger Reaktionszeit steht zur Verfügung) ist auch die Steuerverwaltung gezwungen, auf diese Diskrepanz zu reagieren. Ein System überlebt nur solange, wie die Veränderungsgeschwindigkeit innerhalb des Systems ungefähr so groß ist, wie die Veränderungsgeschwindigkeit der relevanten Umwelt. siehe *Deser*, Chaos und Ordnung im Unternehmen – Chaosforschung als ein Beitrag zum besseren Verständnis von Unternehmen als nichtlineare dynamische Systeme, Physica –Verlag 1997. Siehe auch *Seer*, Vortrag, Möglichkeiten und Grenzen eines maßvollen Gesetzesvollzuges, StuW 1996, S 560 f., der zeigt, dass der Rechtsstaat verhöhnt wird, wenn der Eindruck entsteht, dass Finanzämter bei mitwirkenden Stpfl, deren Einkünfte bestimmte Grenzen überschreiten, die abgegebenen Steuererklärungen intensiv prüfen, dagegen Schwarzarbeiter und „Ohne-Rechnung“-Unternehmer in Ruhe (gewähren) lassen.

- **der vorsätzlich falsch informierte Datenvernichter**

Verließ sich voll auf seinen Berater, hat diesem auch immer pünktlich alle Buchhaltungsunterlagen geschickt, wusste aber nicht genau, dass man Daten oder Aufzeichnungen aufbewahren muss und welche. Es ist hierbei unnötig, alles zu vernichten, was unmittelbar zu einer Generalschätzung führt – es reicht aus nur „eine Kleinigkeit" nicht zu haben – welche jedoch das Kernelement für die Prüfung der Vollständigkeit ist

- **der gutmütig ahnungslos Vergessliche**

Hat vergessen oder nie genau gewußt, wie genau man das System bedient, vor allem jene Funktionen, die mit der Erstellung von ordnungsmäßigen Berichten und Abschlüssen zusammenhängen und die Auswirkungen dieses Vorgehens immer unterschätzt.

- **der wahre Unglücksrabe im Katastrophenumfeld**

Durch „höher Gewalt" oder widrige Umstände sind ihm genau jene Unterlagen und Daten verloren gegangen, die man für die Prüfung der Vollständigkeit braucht. Abstürze, Brände, Überschwemmungen Druck auf irgendwelche falschen Knöpfe zur Selbstzerstörung der Daten – eine Aufzeichnungskatastrophe folgt der nächsten.

- **der vollkommen Unschuldige im Kreise der Schuldigen**

Hat das Unglück, von skrupellosen Kassenherstellern oder Programmierern umgeben zu sein, die ihm wider besseres Wollen eine manipulationsanfällige Kasse angedreht haben, an deren bösen Einrichtungen er keine Schuld trägt, von denen er nichts wusste und die die er nie eingesetzt hat.

Endeffekt ist immer der gleiche. Steuerlich laufen die Mängel auf eine Schätzung – dem Grunde und der Höhe nach – hinaus. Je weniger brauchbare Unterlagen aber vorhanden sind und je mehr es dem Manipulanten gelingt, das Ausmaß, die Tragweite seiner Mängel herunterzuspielen umso größer ist die Wahrscheinlichkeit für ihn, „moderat" wegzukommen – in Wahrheit weit unter den Ausmaßen der wahren Verkürzung. Auf Basis dieser Taktik laufen – nicht nur im deutschen Sprachraum – eine Menge der Prüfungsverfahren in den sog Bargeldbranchen ab. Dabei hängt der Erfolg einer solchen Strategie aber auch reziprok unmittelbar vom Ausbildungsstand der Prüfenden ab. Die österreichische Finanzverwaltung hat in den Jahre 2010 und 2011 rd. 1000 Prüfer und Erhebungsorgane im Kassenbereich geschult – das Ergebnis war eine deutliche Steigerung der Aufgriffe bei Kassenfällen, sowie das Verlangen der Wirtschaftvertreter nach einer einheitlichen Richtlinie im Kassenbereich.

3.2 Entwicklung der Manipulationstechniken

Die technische Entwicklung[22] im Zusammenspiel mit Manipulationsbedarf und Verfügbarkeit von Manipulationsoptionen ging von den Phantomkassen (1. offizielle Kasse, aus der die Berichte stammen, 2. inoffizielle Kasse zur Erfassung der Schwarzerlöse oder einer 2. Kasse, auf der Wunschberichte erzeugt wurden, über nicht vom Kassenhersteller stammende Zusatzsoftware oder –einrichtungen, mittels derer das Kassenverhalten beeinflusst werden konnte, weiter über herstellerseits eingerichtete Manipulationsoptionen auf der Kasse bis zu nicht permanent im System anwesenden und daher auch nicht bei Prüfungen auffindbaren Kleinprogrammen oder Dateien, die eine „brave" Kasse rasch in eine „schlimme" verwandeln können.

Die Technik hat – ebenso wie sie in alle übrigen technischen Bereiche des Alltagslebens innovativ vordrang (Mobiltelefone, Elektronik im Auto, EDV-Optimierung usw) – vor den Kassen nicht halt gemacht. Das technische Umfeld der RegKn und Kassensysteme hat sich in den letzten 15 Jahren extrem weiterentwickelt – auch wenn es so mancher im Umfeld damit befasster Marktteilnehmer / Berater / Prüfer nicht unmittelbar realisierte.

Die dabei auftretenden prüfungstechnischen Probleme waren vor allem folgende

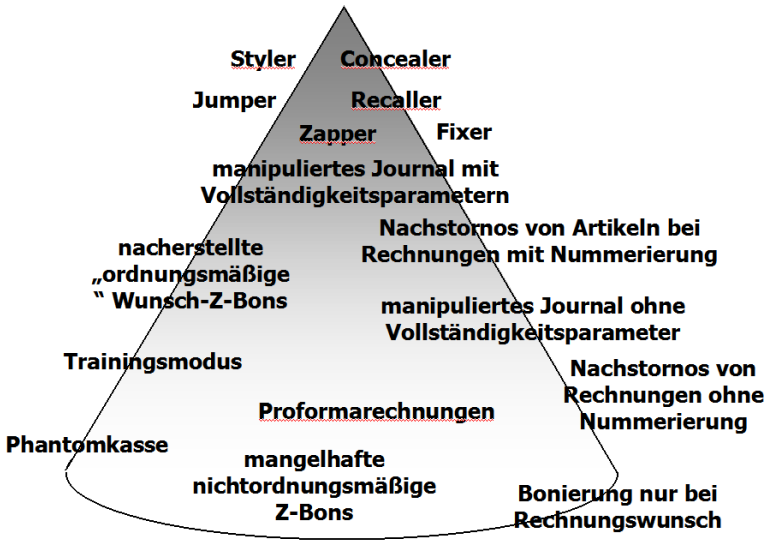
- anpassungsfähige Software ersetzt mechanistische Hardware
- fragliche Aussagekraft von früher glaubhaften Berichten, Abfragen und Protokollen
- mögliche spurlose nachträgliche Veränderungen von Daten, parallele Führung von Datensträngen
- mangelnde Prüfbarkeit

Kaum jemand wird vermeinen, dass ein Mobiltelefon von 1999 (mit dem man gerade mal telefonieren konnte) ein technisch ähnliches Gerät war, wie ein heutiges Smartphone. Im Bereich der Kassen hat aber die gleiche technische Fortentwicklung stattgefunden und so kann auch eine gut ausgestattete summenspeicherbasierte RegK aus 1996 (dem Jahr des BMF-Schreibens vom 9.1.1996) nicht mit einem proprietären Kassensystem von 2012 verglichen werden oder etwa hinsichtlich der Vorgaben für ordnungsmäßige Aufzeichnung nach denselben technischen Maßstäben gemessen werden. Eines der Vollzugsprobleme der Steuerverwaltung besteht darin, ihr Prüfungs- und Kontrollpersonal auf den aktuellen technischen Stand zu bekommen, die Kassentechnik und -optionen auch als solche zu erkennen. Das ist gar nicht einfach – gerade der Unterschied zwischen „einfachen" summenspeicherbasierten Kassen und – äußerlich aussehensmässig grob ähnlichen proprietären Kassensystemen in „herkömmlichen" Kassenchassis ist manchmal nicht sofort ersichtlich. Von der Zuordnung hängt aber die Vertrauenswürdigkeit der erzeugten Berichte und Protokolle ab.

[22] Siehe *Huber*, RegK, …, Zapper stBP 2009, FN 2

beispielhafte Darstellung von Hinterziehungsoptionen (demonstrative Aufzählung) mit Registrierkassen (Stand 1996)

- Händische Erfassung statt ECR-Bonierung
- Bonierung nur bei Rechnungswunsch
- Phantomkasse
- Nacherstellung von Tagesendsummenbons mit (zweiter) Kasse
- Tagesendsummenbons mit nicht fortlaufender Nummerierung
- Double Till
- Einsatz zweier (typgleicher) Kassen
- Abschneiden von Tagesendsummenbons
- Kellner weglassen (Bereiche)
- Artikel weglassen – Warengruppenberichte
- Datenbankabfrage
- Verschieben von Bediener (Kellner)
- Proformarechnung
- Verdeckte Storno- oder Warenrücknahmebuchungen
- Unterdrückung des Z-Zählers = Nullstellungszähler
- Trainingsmodus
- Z-Bon-Editor
- Automatischer Verkürzungslauf
- Chefstorno
- große Tische schlucken kleine Tische
- Personaltisch



Wie sehr sich die Aufzeichnungswelt verändert hat, ersieht man aus dem oben abgebildeten Risikokegel, der auch (an der Spitze) einige Hinterziehungsmodi mit Systemen nach letztem Stand der Technik zeigt (demonstrative Darstellung).

Manipulation in Form von aufzeichnungstechnischer Weglassung und Nichtmeldung von Umsätzen kann grundsätzlich auf 3 Arten geschehen

- Nichterfassung im System
- Erfassung in Subroutinen (zB Bedienerspeicher) / teilweise Nichterfassung im Journal,
  - „Trainingeinstellungen“
  - „Extrabereiche“ der Datenbank
- nachträgliche Manipulation, die oft nicht mehr aufgedeckt werden kann
  - Rechnungsstorno (Positionsverkürzung)
  - Artikelstorno (Werteverkürzung)

Die Gar-nicht-Erfassung kommt nur in Kleinstbetrieben vor, schließlich will der Unternehmer schon einen realen Überblick über seinen wahren Geschäftserfolg haben. Die parallele Erfassung bietet Überblick über wahre Zahlen und gleich auch über die inoffiziellen Zahlen. Die nachträgliche Datenveränderung schließlich ermöglicht die systematische Manipulation.

Aus der Sicht der Prüfungs- und Kontrolltechnik her sind manche Vorgangsweisen schon aus dem Handbuch erkennbar (so der Prüfer an eines kommt). Dort sind sie nicht offen als „Manipulationsoption“ beschrieben, sondern als veränderte Systemparameter oder modifizierte Druckeinstellungen. Andere Optionen können als im System integriert erkannt werden durch eine Systemkontrolle im laufenden Modus bzw. durch einen Systemprüfer. Schließlich gibt es noch die verdeckten Optionen, die nur durch unangemeldete Erhebung bzw. unmittelbaren Zugriff auf die aktuellen Kassendaten entdeckt werden können.
Nachfolgend ein Überblick.

Offene Druck-Optionen zu Manipulation in „einfachen" Kassen – Aufdeckung über Handbuch

- Z-Bon ist nicht nummeriert / hat keine Uhrzeit
- Tagesabrechnung mit X-Bon ohne Uhrzeit
- GT-Speicher wird nicht gedruckt / bei jedem Z-Bon zurückgesetzt
- Stornos werden nicht dokumentiert
- Echte Umsätze werden als nicht dokumentierte Trainingsbuchungen nicht erfasst
- Elektronisches Journal wird gelöscht und kann nicht vorgelegt werden
- Elektron Journal wird auf Papier vorgelegt

u.U. erkennbare System-Optionen zu Manipulation in „embedded" Kassensystemen - Aufdeckung durch Systemkontrolle

- Durch Managerstornos werden nachträglich Erlöse aus der Erfassung entfernt (zB Rechnungsstorno)
- „Reorganisation" von Tages- und Monatsabschlüssen
- „Datenrettung" durch Wiederherstellung der Datenbank
- „Datenerfassungsprotokoll" wird nach Manipulation aus der Datenbank erstellt
- Tagsabschlüsse werden nach Manipulation aus Tabellen erstellt

Verdeckte System-Optionen zu Manipulation in „komplexen" Kassensystemen – Aufdeckung durch Kassennachschau oder Steuerfahndung

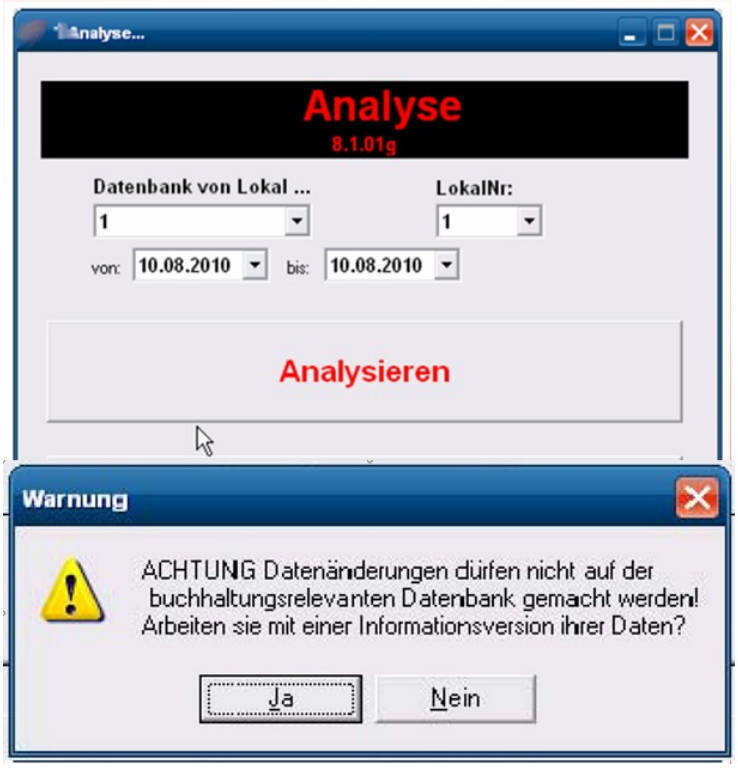
- Teilerfassungssysteme (PDAs, „Handykassen") werden ganz ausgelassen
- Über Sub-Bereiche (Bedienerspeicher, Springerschlüssel) werden Teile der Erlöse der Erfassung entzogen
- Durch nachträglichen Eingriff in die Datenbank (Tabellen) werden nachträglich Erlöse aus der Erfassung entfernt
- Tagsabschlüsse werden nach Manipulation aus der Datenbank erstellt

3.3. Beispiele „moderner" Manipulation

In der letzten Zeit haben sich international neue – klarerweise inoffizielle - Ausdrücke für Manipulationsmodi bei den Experten der BP etabliert. Sie zeigen die umfangreichen Möglichkeiten, welche die Technik bietet und sie werden planetenweit von den Kassenspezialisten der Steuerverwaltungen aufgefunden. Nachfolgend werden einige dargestellt.

Zapper („Löscher") [23]

Einzelne Datei (meist .dll oder .exe), durch welche Tabellen aus Kassensystemen oder Datenbanken eingelesen und nachbearbeitet werden. Aus den veränderten Daten werden dann Berichte erstellt. Die Zapper sind die mittlerweile bekannteste verbreitete technische Manipulation in Kassensystemen und wurden quer über den ganzen Planeten gefunden. Sie ermöglichen Manipulation trotz fortlaufender Rechnungsnummern und trotz Zwang zur „Journal"-Vorlage in Datenform. Die BP kann hier mittels Prüfsoftware kaum Auffälligkeiten finden. Die an sich mühseligen und zeitaufwendigen Stornos und Ersatzfunktionen von Teilleistungen in Rechnungen erledigen die „Hilfsprogramme" mittlerweile automatisch von sich aus intelligent (also nach vorgegebenen Parametern – zB Verhältnis zwischen Speisen / Getränken, Verhältnis der Getränkegruppen untereinander, der Steuersatzgruppen untereinander usw.



[23] Beschrieben bei *Härtl, Schieder* Ordnungsmäßigkeit digital geführter Erlösaufzeichnungen - elektronische RegK und digitale Erlöserfassungssysteme im Brennpunkt des Steuerrisikos Erlösverkürzung, stBP 2011, 68 und bei *Huber*, RegK, …, Zapper stBP 2009, FN 2

Jumper („Springer“) [24]
Bedienerschlüssel, der es ermöglicht, einen Bediener „unsichtbar“ arbeiten zu lassen. Für Resistenz gegen den ECR-Bedienerscan durch die BP sorgt der externe Bedienerschlüssel („Springerschlüssel“). Alle Berechtigungen sind nur auf dem Schlüssel gespeichert und nicht im System hinterlegt.

Concealer („Verberger“), siehe rechts
Datenbanksystem mit tragbaren Terminals, in welchen einzelne Geräte „unsichtbar“ arbeiten. Die „versteckten“ Einzelgeräte sind zwar mit Küche und Schank verbunden, sodass die Materialproduktion und –bereitstellung funktioniert, die Abrechnung läuft aber über isolierte Bereiche. Manche Geräte können überhaupt solo („Stand alone“) arbeiten und verhalten sich dann wie eine eigene Kasse.

Stand-Alone Einstiegssystem für die Drahtlose Bestellannahme.

Das [redacted] sprich [redacted], ist eine drahtlose, Einstiegslösung für die Bestellannahme in der Gastronomie. Mit diesem System steht dem Anwender eine komplette Tischverwaltung zur Verfügung, ohne das er eine Kasse verwenden muss.

Funktionen

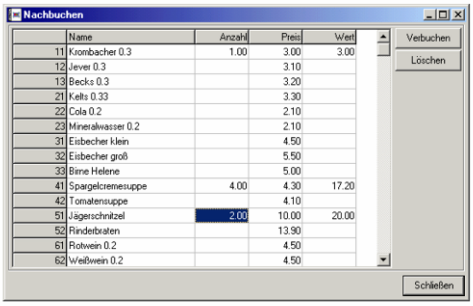
- Tische verwalten
- eine neue Bestellung eingeben
- die Gästeanzahl eingeben
- Zutaten / buchen
- Kochanweisungen buchen
- freie Textangaben eingeben
- die Bestellung / Rechnung ansehen
- die Artikel-Menge ändern
- den Artikel-Preis ändern
- die Preisebene ändern
- Rechnung Drucken und abschließen
- Zahlungsarten eingeben
- einen offenen Tisch wieder aufrufen
- eine „offene-Tische-Liste“ einsehen
- Stornos und Retouren buchen
- die Tisch-Nr. wechseln, bevor die Bestellung abgeschickt wird
- Tische transferieren und zusammenlegen
- X- und Z-Berichte erstellen
- Rechnungen splitten

Recaller[25] **(„Rückrufer“)**
Kassennetzwerk, in welchem über ein Kommandoprogramm Daten aus den Filialkassen abgerufen werden, verändert werden und dann daraus an einem Master-PC Berichte erstellt werden. Die Korrekturen über negative Nachbuchungen von Produkten liefern neue Grundlagenzahlen für die Berichte.

Umsatzdaten nachbuchen

Mit dieser Funktion können Sie nachträglich Buchungen vornehmen, zum Beispiel um Fehlbons zu stornieren oder einen Z-Bericht zu ergänzen, der aufgrund eines Übertragungsfehlers nicht aus der Kasse gelesen werden konnte. Die Berichte werden dann entsprechend angepasst.

Eingabe der Nachbuchungen



Nachdem Sie eine Kasse und einen Lesungszeitpunkt ausgewählt haben, können Sie hier für einen oder mehrere Artikel Nachbuchungen eingeben.

- **Anzahl**
  Geben Sie hier eine positive oder negative Anzahl ein, die Sie für den Artikel nachbuchen möchten.

- **Verkäufer**
  Geben Sie hier an, welchem Verkäufer die Nachbuchungen zugeordnet werden sollen.
- **Bediener**
  Geben Sie hier einen Bediener ein, dem die Nachbuchungen zugeordnet werden sollen.
- **Uhrzeit**
  Geben Sie hier die Uhrzeit ein, unter der verbucht werden soll.
- **Finanzweg**
  Geben Sie hier den Finanzweg ein (z.B. Finanzweg 1 für Bar).
- **Kunden/Gäste**
  Sofern in Ihren Berichten die Anzahl der Kunden oder Gäste berücksichtigt wird, können Sie hier eintragen, auf wie viele Gäste Ihre Nachbuchung verteilt werden soll.

Wenn Sie auch diesen Dialog mit <OK> bestätigen, werden die Umsatzdaten verbucht und in die ggf. existierenden Lesungsdaten eingeflochten.

Umsatzdaten eingeben

Hier hat der Benutzer die Möglichkeit, alle Berichtswerte frei einzugeben. Dabei liegt es voll in seiner Verantwortung „vernünftige“ Daten einzugeben, da es hier keinerlei Unterstützung durch das Programm gibt. Sinnvoll ist diese Methode vor allem bei Dateneingabefeldern der Kassen, z.B. „Bestellungen“, „Retouren“, da diese nicht mit der Nachbuchfunktion bearbeitet werden können.

Styler („Gestalter“) [26]
Embedded-Kassensysteme, die es durch komplexe Datenfesthaltung ermöglichen, Wunsch-Tagesabschlüsse zu erzeugen. Durch die teil schwere Unterscheidbarkeit von fix programmierten summenspeicherbasierten einfachen Kassen und embedded-Lösungen im „einfachen“ Kassenchassis wird hier der äußere Eindruck einer „einfachen“ Kasse vermittelt, deren Z-Berichte durchaus eine gewisse Aussagekraft haben. Wenn allerdings mittels eines Betriebssystems „Bearbeitungsfunktionen“ verfügbar werden, mittels derer Berichte „gestilt“ werden können, so fehlt diesen Berichten jede tatsächliche Aussagekraft. Aber – wie schon oben dargestellt – der Prüfer muss erst mal erkennen, dass es sich nicht um eine einfach Kasse handelt.

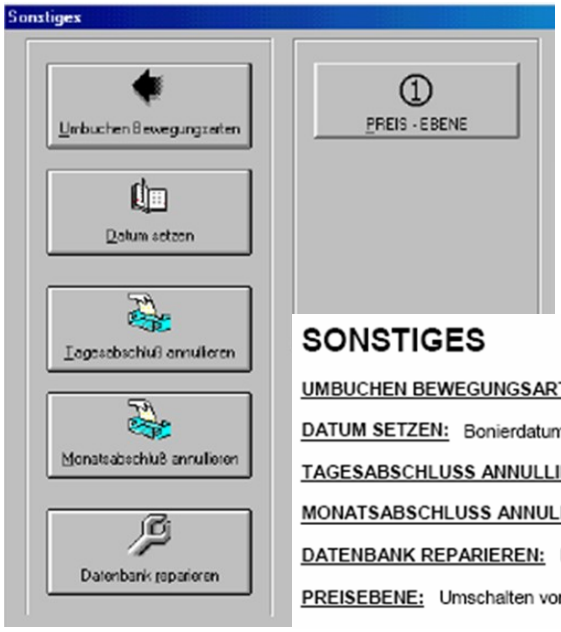
[24] Beschreiben bei *Härtl, Schieder* Ordnungsmäßigkeit, …, stBP 2011, 68
[25] Beschreiben bei *Härtl, Schieder* Ordnungsmäßigkeit …, stBP 2011, 73
[26] Beschreiben bei *Härtl, Schieder* Ordnungsmäßigkeit …, stBP 2011, 69

ZÄHLEREINSTELLUNGEN

PROGRAMMIERMODUS -> KONFIGURAT. EINSTELL. -> ZÄHLEREINSTELLUNGEN auswählen. Surfen Sie zu dem Feld, das persönlich gestaltet werden soll und geben Sie seine Daten ein (für die zu verwendenden Tasten siehe "Dateneingabemodus").

Abschließend menu ON drücken, um zum **Hauptmenü**, clerk ESC um zum vorherigen Menü zurück zu kehren.

Artikelmenü	Mögliche Werte	Beschreibung
Kassenbon-nummer	1 bis 9999	Max. 4-stellig, um anzugeben, von welcher Zahl an die Kassenbons durchnummeriert werden sollen.
Z1-Zähler	1 bis 9999	Z1 Finanzbericht-Zähler. Max. 4-stellig, um anzugeben, bei welcher Zahl der Z2-Zähler anfangen soll zu zählen. Die Registrierkassenvoreinstellung Z2 Finanzbericht-Zähler kann überschrieben werden, indem die Zahl programmiert wird, bei der der Zähler anfangen soll durchzuzählen, wenn ein Finanzbericht ausgedruckt wird.
Z2-Zähler	1 bis 9999	Z2 Finanzbericht-Zähler. Max. 4-stellig, um anzugeben, bei welcher Zahl der Z1-Zähler anfangen soll zu zählen. Die Registrierkassenvoreinstellung Z1-Finanzbericht- Zähler kann überschrieben werden, indem die Zahl programmiert wird, bei der der Zähler anfangen soll durchzuzählen, wenn ein Finanzbericht ausgedruckt wird.
GT-Wert	(Zahl)	Gesamtwert. Max.12 -stellig, um den Gesamtbetrag anzugeben. Der Transaktionsgesamtbetrag, der auf en Verwaltungsberichten ausgedruckt wird, kann programmiert werden.
Kassenbon# Rückst	**JA, NEIN**	Kassenbonnummer rückstellen. JA - Einschalten, NEIN - Ausschalten.
Z1&2 CT Rückstell	**JA, NEIN**	Z1- und Z2-Zähler rückstellen. JA - Einschalten, NEIN - Ausschalten.
GT Rückstellen	**JA, NEIN**	GT-Zähler rückstellen. JA - Einschalten, NEIN - Ausschalten.



SONSTIGES

UMBUCHEN BEWEGUNGSARTEN: Umbuchung von Bonierung auf Training, Bruch, Eigenverbrauch usw.

DATUM SETZEN: Bonierdatum setzen.

TAGESABSCHLUSS ANNULLIEREN: Tagesabschluss zum Bearbeiten zurücksetzen und entpacken.

MONATSABSCHLUSS ANNULLIEREN: Monatsabschluss zum Bearbeiten zurücksetzen und entpacken.

DATENBANK REPARIEREN: Defekte Datenbank (z.b. durch Stromschwankung, Blitzschlag usw.) reparieren.

PREISEBENE: Umschalten von Preisebene 1 auf Ebene 2.

Fixer („Reparierer“)

„Reparatur“ der Datenbank – veränderte Daten werden importiert, daraus werden Berichte erstellt. Bei einer angekündigten Kassenprüfung wird alsbald das Katastrophenszenario eingesetzt und der Totalabsturz der Datenbank („böse Viren, Wassereinbruch, PC kaputt, …“) inszeniert. Die Rettungssicherung wird nach eingespielt, deren Basisdaten sich aber von den Originaldaten wesentlich unterscheiden. „Prophylaktische“ Abstürze und deren „Gedächtnisprotokollierung“ zwischendurch sind „nützlich“.

Zusammenfassend kann festgestellt werden, dass sich die Technik der Kassen und Systeme ebenso fort entwickelt hat, wie in den anderen technisch geprägten Bereichen des täglichen Lebens. Eine permanente und zeitnahe Reaktion der Steuerverwaltung ist nicht nur personal- und zeitressoucenmäßig unmöglich. Ohne höchste technische Sicherheiten wie zB INSIKA kann heute kein System mehr für Dauer als steuerlich unbedenklich bezeichnet werden.

Die Vorschläge aus der Wirtschaft und vor allem aus der Beraterecke, doch Systeme und Kassen zu zertifizieren, scheitern in Ö gleichfalls an eben diesen Umständen. Eine Software, die heute in der Version 1.0 als grundsätzlich ordnungsmäßig bezeichnet werden kann, ist morgen in der Version 1.1. eventuell schon die „manipulative[27] Superoption“. Die ö Finanzverwaltung lehnt daher Kassenzertifizierung grundsätzlich ab.

[27] Selbst bei Compliance des Kassenherstellers oder –programmierers und der Erstellung grundsätzlich ordnungsmäßiger Systeme sind insbesondere bei PC-Kassen und Kassenandroiden auch noch nachträgliche Angriffe leicht möglich. Nach der Auskunft von Informatikern ist ein durchschnittlich begabter Informatikstudent nach dem ersten Semester imstande, einen Zapper zu programmieren.

3.4 Überblicksartige Klassifzierung von Kassentypen und deren Risiken

Die ö KRL ist den Weg gegangen, die genutzten Systeme in Kassentypen zu definieren und darauf aufbauend die Anforderungen für eine ordnungsmäßige Aufzeichnung durch diese vorzugeben. Nachfolgend ist dazu eine Übersicht dargestellt, welche die Risiken und Sicherheiten der in Ö in Nutzung befindlichen Kassen und Systeme darstellt. Die Klassifizierung folgt in erster Linie weniger exakt rein technischen Gesichtspunkten, sondern vor allem aufzeichnungs- und sicherheitsbezogenen Kriterien.

mechanische Registrierkassen
ohne Datenträger und Speicher

- **Sicherheiten**
  - laufende, chronologische Protokollierung über Journalstreifen
- **Risiken, Manipulation**
  - „Abschneiden“ des Journalstreifens
  - Nichtvorlage des Journalstreifens
- **Besonderheiten**
  - I.d.R. ablesbare mechanische Zählwerke
  - Antrieb mechanisch (Kurbel), elektrisch

Einfache elektronische Registrierkassen
I.d.R ohne Betriebssystem, welche üblicherweise die Geschäftsvorfälle mittels Datenspeicherung (i.d.R. in festen Strukturen in batteriegepuffertem RAM oder Flash-Speicher – und nur dort) festhalten und welche laufend ein elektronisches Journal speichern, welches je nach Schnittstellen exportiert werden kann.

- **Sicherheiten**
  - Komplizierte, schwer verstellbare Veränderung der Speichergrundeinstellungen zu Manipulationen auf dem EPROM - (würden bei näherer Prüfung auch auffallen)
  - Tagesabschluss aus Speichern ist i.d.R. sicher, wenn alle Angaben mit abgefragt und gedruckt werden
  - Alle Berichte sind nur Abfragen aus Summenspeichern
  - Elektronisches Journal entspricht i.d.R. dem Papierstreifen einer mechanischen RegK
  - Rechnungen mit fortlaufender Nummer, Uhrzeit
- **Risiken, Manipulation**
  - „offene“ Manipulation über Druckeinstellungen
  - GT, Stornos, Training nicht drucken
  - externe Veränderung der Daten des exportierten elektronischen Journals
- **Besonderheiten**
  - nach wie vor gibt es einfache elektronische Registrierkassen
    - die neben dem Bonstreifen einen Journalstreifen mitlaufen haben und gar kein elektronisches Journal erzeugen
    - die das elektronische Journal mangels Schnittstellen nicht exportieren können, sondern das Journal nachträglich auf den Journalstreifen drucken

Proprietäre Kassensysteme mit "embedded"-Architektur und einfachem Betriebssystem
(zB POS-Linux) - „***Kassenandroiden***“, welche üblicherweise die Geschäftsvorfälle mittels Datenspeicherung in komplexeren Strukturen (i.d.R. Tabellen) festhalten und einfach vernetzbar sind

- **Sicherheiten**
  - DEP mit Sequenznummer, Datum, Uhrzeit der einzelnen Buchungen
  - Rechnungen mit fortlaufender Nummer, Uhrzeit
- **Risiken, Manipulation**
  - Datenspeicherung in Tabellen statt Speichern ermöglicht gut nachträgliche Eingriffe
  - Betriebssystem / Verbund ermöglicht leichte Kommunikation mit PC zum Datentransfer to & back
  - verdeckte Manipulation über „Simulation“ einer speicherbasierten Registrierkasse (Styling)
    - Z-Bons, GT, Berichte werden verändert nach erstellt
  - „Analysefunktionen“, Zapping, Recalling
    - Nachträgliche Datenveränderung, Stornos, Positions- und Werteverkürzungen,
    - Erstellung eines veränderten elektronischen Journals
  - Extraverwaltung von Teilumsätzen (Jumping)

    - Bediener werden über Subbereiche kontrolliert, deren Umsätze gehen nicht in die Gesamterfassung
  - Kassenandroiden erzeugen Berichte wie speicherbasierte el. RegK
  - Berichte sind aber keine Abfragen aus Speichern, sondern werden aus Tabellen„hausgemacht“ – wahlweise mit Echtzahlen oder nach Wunsch - auch das El. Journal
  - Daher kommt diesen Berichten auch keine Aussagekraft zu, einzige sichere Kontrollgrundlage ist das DEP

- **Besonderheiten**
  - Unterscheidung zwischen einfachen speicherbasierten Kassen und proprietärem System ist nicht immer klar und einfach
  - Elektronisches Journal wird zur Manipulationsoption bewußt nicht als DEP gestaltet

PC-Kassen mit komplexem Betriebssystem
(zB Windows), welche üblicherweise mittels auf Datenbanken basierender Software die Geschäftsfälle fest halten.

- **Sicherheiten**
  - Datenerfassungsprotokoll mit Sequenznummer, Datum, Uhrzeit der einzelnen Buchungen
  - Rechnungen mit fortlaufender Nummer, Uhrzeit

- **Risiken, Manipulation**
  - Datenspeicherung in Datenbanken ermöglicht jegliche nachträglichen Eingriffe
  - Komplexes Betriebssystem / Verbund ermöglicht leichte Kommunikation mit Peripherie zum Datentransfer to & back und Einbau jeglicher individueller „Wunschlösungen“
  - Ohne echtes DEP sind alle denkbaren Datenveränderungen einfach und spurlos möglich
  - Gefälschte „fortlaufende Kontrollaufzeichnung“ durch nachträgliche Erstellung des „DEP“ aus der Datenbank
  - „Rundumerneuerung“ der Daten durch „Reparatur“ der Datenbank (Fixing)
  - Erstellung von „Wunschberichten“ (Styling)
    - Berichte werden auf Basis veränderter Daten oder vollkommen frei (erfunden) erstellt
  - „Analysefunktionen“, Zapping, Recalling
  - Ausgegliederte Verwaltung von Teilumsätzen, Kassennetzwerk, verdeckte Peripherie (Concealing)
    - Ordermen laufen als unabhängige Kassen, Rechnungen werden losgelöst von Mastersystem erstellt, deren Umsätze gehen nicht in die Gesamterfassung
  - Auch PC-Kassen erzeugen bei Bedarf Berichte wie speicherbasierte el.RegK
  - Berichte sind aber keine Abfragen aus Speichern, sondern werden aus Datenbank „hausgemacht“- auch das El. Journal
  - Daher kommt diesen Berichten auch keine echte Aussagekraft zu, einzige sichere Kontrollgrundlage ist das DEP

- **Besonderheiten**
  - Tagesabschlüsse sind nicht genormt
  - Softwaren werden permanent upgedatet und nicht auf Rechtmäßigkeit geprüft

3.5 Ergänzung: Problematik der Nutzung von Datenbanken oder Tabellen und der Erzeugung von Logs / Protokollen / Journalen

Anhand der nachfolgen schematisierten Darstellung soll gezeigt werden, worin die Hauptproblematik im Vollzug bei der Aufzeichnung mit Kassensystemen und PC-Kassen mittels Tabellen oder Datenbank liegt.

Die Datenbank erfasst die Geschäftsfälle und deren Grundlagen. Unten ist tabellenartig ein kurzer Erfassungsablauf dargestellt. Die Tagesberichte sind das summiert Erfassungsergebnis.
Die Elemente in der Datenbank sind jederzeit veränderbar oder löschbar. Wenn also ganze Rechnungen storniert werden sollen, hindert nur mehr deren Rechnungsnummer die Spurlosigkeit. Das ist auch der Grund, weshalb Systeme alle möglichen „Zettel“ ausdrucken, auf denen so wenig Information wie möglich enthalten ist.

Tischdruck

Kellner: vormittag Tisch:tische/10

Menge	Bezeichnung	Einzelpr.	Summe
2	mineral 0,33	2,60	5,20
1	apfelsaft 1/8	1,45	1,45
1	soda 1/8	0,90	0,90
1	kalbsgulasch	14,60	14,60
1	fischgulasch	11,40	11,40
1	ungar gulasch	9,60	9,60

Summe: 43,15Euro

Wenn ein Kellner auf „Training“ geschickt wird – oft auch ohne es selbst zu wissen, wird der Gesamterfolg abschließend ohne ihn ermittelt. Auch hier ist es vorteilhaft, wenn sich keine fortlaufenden Nummern bzw Buchungszeiten auf der Rechnung befinden, welche deren Inhalte nachverfolgbar machen.

Datum	Uhrzt	Artikel / PLU	Preis PLU	Kellner	Tisch Nr	Warengruppe	offen / abschl	Rechnung		
27.08.2011	13:01	Pizza A	10,00	Fritz	1	Hauptspeisen	a	3012		
27.08.2011	13:02	Merlot 1/8	4,00	Fritz	1	Wein	a	3012		
27.08.2011	13:24	Schnitzel mil	13,00	Margit	3	Hauptspeisen	a	3013		
27.08.2011	13:24	Salat kl	4,00	Margit	3	Beilagen	a	3013		
27.08.2011	13:24	Bier 1/2	4,00	Margit	3	Bier	a	3013		
27.08.2011	13:44	Kaffe kl	3,00	Margit	3	Kaffee	a	3013		
27.08.2011	14:12	Pizza B	12,00	Fritz	5	Hauptspeisen	a	3014		
27.08.2011	14:12	Pizza C	14,00	Fritz	5	Hauptspeisen	a	3014		
27.08.2011	14:12	Bier 1/2	4,00	Fritz	5	Bier	a	3014		
27.08.2011	14:13	Bier 1/3	3,00	Fritz	5	Bier	a	3014		
27.08.2011	15:24	Spaghetti Bolo	9,00	Paul	7	Hauptspeisen	a	3015		
27.08.2011	15:24	Fanta	2,00	Paul	7	alkfrei	a	3015		
27.08.2011	15:24	Saltimbocca	15,00	Paul	7	Hauptspeisen	a	3015		
27.08.2011	15:25	Merlot 1/2	16,00	Paul	7	Wein	a	3015		
27.08.2011	16:22	Fisch A	15,00	Margit	11	Hauptspeisen	a	3016		
27.08.2011	16:22	Pinot blanc	4,00	Margit	11	Wein	a	3016		
27.08.2011	16:22	Pizza A	10,00	Margit	11	Hauptspeisen	a	3016		
27.08.2011	16:22	Merlot 1/8	4,00	Margit	11	Wein	a	3016		

Datum	Uhrzt			Kellner	Tisch Nr			Rechnung	Rechnung Betrag	KK
27.08.2011	**14:08**			**Fritz**	**1**			**3012**	**14,00**	**x**
27.08.2011	**15:00**			**Margit**	**3**			**3013**	**24,00**	
27.08.2011	**15:20**			**Fritz**	**5**			**3014**	**33,00**	**x**
27.08.2011	**16:49**			**Paul**	**7**			**3015**	**42,00**	
27.08.2011	**17:55**			**Margit**	**11**			**3016**	**33,00**	

Eines der einfachen, aber effektiven Sicherheitseinrichtungen ist eine fortlaufende Nummerierung – nicht nur der Geschäftsfälle / Rechnungen, sondern der Einzelbuchungen. In Ö wird diese „Log-Datei“ als Datenerfassungsprotokoll (DEP) bezeichnet. Durch die eineindeutige Identifizierbarkeit der Einzelbuchung soll deren Veränderung oder Löschung erschwert werden. Dieses DEP – wenn es tatsächlich als unabhängig von der Tabelle oder Datenbank geführtes Log mitläuft – bietet hohen Sicherheitstandard. Beim Zapping wird – zur Erhaltung der Rechnungsnummer die Manipulation mittels Storno eine Ebene tiefer angesetzt. Hier werden nicht ganze Rechnungen gelöscht, sondern Einzelprodukte aus Geschäftsfällen entfernt. Bei Abschluss wird dann ein „elektronisches Journal“ mit verminderten Geschäftsfällen erzeugt. So ist nicht alles, was ein Prüfer bei einer Revision der Vergangenheit als DEP erhält ein Log.

Unten ein DEP. Man erkennt die Angabe des Datums, der Systemzeit der Buchung, einer Sequenznummer für jede Einzelbuchung und die Buchungsinhalte – Einzelleistungen und Rechnungen. In Wahrheit unterscheidet sich das DEP letztlich inhaltlich von einem Datenbankauszug nur durch die Sequenznummer der Einzelbuchungen.

Datum	Uhrzt	Seq Nr	Artikel / PLU	Preis PLU	Kellner	Tisch Nr	Rechnung	Rechnung Betrag	KK
27.08.2011	13:01	2389	Pizza A	10,00	Fritz	1			
27.08.2011	13:02	2390	Merlot 1/8	4,00	Fritz	1			
27.08.2011	13:24	2391	Schnitzel mil	13,00	Margit	3			
27.08.2011	13:24	2392	Salat kl	4,00	Margit	3			
27.08.2011	13:24	2393	Bier 1/2	4,00	Margit	3			
27.08.2011	13:44	2394	Kaffe kl	3,00	Margit	3			
27.08.2011	**14:08**	**2395**			**Fritz**	**1**	**3012**	**14,00**	**x**
27.08.2011	14:12	2396	Pizza B	12,00	Fritz	5			
27.08.2011	14:12	2397	Pizza C	14,00	Fritz	5			
27.08.2011	14:12	2398	Bier 1/2	4,00	Fritz	5			
27.08.2011	14:13	2399	Bier 1/3	3,00	Fritz	5			
27.08.2011	**15:00**	**2400**			**Margit**	**3**	**3013**	**24,00**	
27.08.2011	**15:20**	**2401**			**Fritz**	**5**	**3014**	**33,00**	**x**
27.08.2011	15:24	2402	Spaghetti Bolo	9,00	Paul	7			
27.08.2011	15:24	2403	Fanta	2,00	Paul	7			
27.08.2011	15:24	2404	Saltimbocca	15,00	Paul	7			
27.08.2011	15:25	2405	Merlot 1/2	16,00	Paul	7			
27.08.2011	16:22	2406	Fisch A	15,00	Margit	11			
27.08.2011	16:22	2407	Pinot blanc	4,00	Margit	11			
27.08.2011	16:22	2408	Pizza A	10,00	Margit	11			
27.08.2011	16:22	2409	Merlot 1/8	4,00	Margit	11			
27.08.2011	**16:49**	**2410**			**Paul**	**7**	**3015**	**42,00**	
27.08.2011	**17:55**	**2411**			**Margit**	**11**	**3016**	**33,00**	

Kassenjournale (in Prinzip die elektronischen Spiegelbilder der ausgestellten Rechnungsbons) erfüllen diese Auflagen nicht und es gibt jede Menge Systeme, die nach Manipulation aus der Datenbank ein gefälschtes „DEP“ erzeugen[28] - wobei bis zur Nachnummerierung hier alle Optionen offen sind und die vorgebliche Ordnungsmäßigkeit zu untermauern.
Ö ist der steten Diskussion in der Vergangenheit um die Natur der Herkunft des DEP bei der Umsetzung der KRL dadurch ausgewichen, dass Lösungen mit mitlaufenden Log-Dateien jedenfalls vorweg als positiv für die Ordnungsmäßigkeitsvermutung zu betrachten sind. In Systemen, welche DEP aus der Datenbankstruktur heraus erzeugen, muss durch die E 131 bzw. eine entsprechende logische und faktische Maßnahme auf technischer Ebene sichergestellt sein, dass hier spurlose Veränderungen verhindert werden. Diese Maßnahmen bzw Einrichtungen sind in der Beschreibung der E 131 anzuführen und zu erklären.

4. Theorie der Möglichen Gegenmaßnhamen der Finanzverwaltung im allgemeinen und im Besonderen aus der BP heraus

4.5.1 Prüfungstechnische Maßnahmen der BP

In der in diesem Beitrag im Absatz über Manipulation beschriebenen Situation hat sich die BP als Garant der Gleichmäßigkeit, der Rechtmäßigkeit und der Sicherstellung des Steueraufkommens zu fragen, durch welche Eigenmaßnahmen sie ihren gesetzlichen Auftrag bestmöglich erfüllen kann. Dabei sind nicht nur organisatorische, sondern auch prüfungstechnische[29] Aspekte zu beachten
Die BP sollte in der Krise als Institution vor allem zur Sicherung des essentiellen Steueraufkommens in der Gegenwart auftreten, weniger als „Nachholer“ von Ausfällen in der Vergangenheit. Betrugsbekämpfung und Steueraufsicht sollte risikobezogen zeitnah jene Bereiche überspannen, wo endgültige Ausfälle am wahrscheinlichsten sind. Nicht die Frage, ob die Rückstellung Y im seit Jahren steuerlich unauffälligen Betrieb A zu hoch gebildet wurde, berührt auf längere Zeit gesehen das Aufkommen, sondern der Umstand, ob der Betrieb B, über welchen außer Elementarinformationen aus der steuerlichen Anmeldung zur Erfassung sowie automatisch einlangenden Vorschreibungs- und Zahlungsdaten keinerlei Aussagen hinsichtlich Redlichkeit möglich sind und dessen Inhaber bei zeitlicher Annäherung an die kritische 3-Jahresfrist uU das Weite sucht.

Zur Herbeiführung einer krisenbezogenen Prävention im Bereich der Erlöshinterziehung – insbesondere im Umfeld der weit verbreiteten elektronisch unterstützten Steuerverkürzung - sind über ein kompetentes Risikomanagement hinaus prüfungstechnisch in der BP bewußtseinsbildende Maßnahmen nötig, die derzeit vom Selbstverständnis der BP her gesehen nicht unbedingt selbstverständliches Allgemeingut sind.

- **Erlösrevision Stufe 1 –**

Setzung des Prüfungsschwerpunktes Erlöse
Es sollte sichergestellt sein, dass alle Prüfer im Falle eines erhöhten Erlösrisikos diesen Bereich als wichtigen Prüfungsschwerpunkt setzen. Ein Grund für mögliche Berührungsängste mit diesem Prüfungsfeld können in der meist unausweichlichen Situation der unmittelbaren Konfrontation liegen, wenn es an die Fragen der formellen Ordnungsmäßigkeit und der sachlichen Richtigkeit geht, die in unmittelbarer Näher zur Schätzung liegen.

- **Erlösrevision Stufe 2 –**

Verlangen von Prüfgrundlagen Primäraufzeichnungen in Papier (Z-Bons), sowie elektronischen Aufzeichnungen in Datenform (DEP)
Der Großteil der EDV-unterstützten Prüfer sollte das vorderste Einsatzfeld in der Durchleuchtung von Massendaten mittels Prüfsoftwaren und digitalen, mathematisch gestützten Methoden sehen, vor allem, wenn solche bereits entwickelt und in der Praxis gut anwendbar sind, um einen Überblick über die Konsistenz der zu prüfenden Massendaten zu erhalten, bzw einen raschen Einstieg in deren Risikobereiche. Das Verlangen von Daten aus vor gelagerten Erlöserfassungssystemen, welche dann mittels der EDV-gestützten Optionen tatsächlich auf Vollständigkeit und Richtigkeit untersucht werden, sollte selbstverständlich sein.

- **Erlösrevision Stufe 3 –**

Systemkontrolle - Prüfung der Rechtmäßigkeit des Systems, korrekte Z-Bons, GT-Stände und Berichte, technisch-logistische Herkunft des Datenerfassungsprotokoll, Offene Optionen zur Manipulation
Falls Daten aus vor gelagerten Systemen verlangt und übergeben werden, bedingt der Gedankengang über eine Analyse derselben vorher die Auseinandersetzung mit der Rechtmäßigkeit des eingesetzten Systems (Unveränderbarkeit, DEP, Grundlagen für Vollständigkeitsprüfung). Daten können auch im Zuge des Erfassungsvorgangs oder unmittelbar nachher (Archivierung) manipuliert worden sein, Solange nicht die Erfassungslogistik und die zugrunde liegenden Routinen durchleuchtet worden sind, ist jede prüfungstechnische Auseinandersetzung mit den Daten unsinnig. In dieser Ebene der Erlösprüfung gilt es auch, offene Optionen zur Manipulation (zB

[28] Siehe die Darstellung eines Zappers bei *Huber* FN 2
[29] Der Erarbeitung von diesbezüglichen Grundlagen für Überlegungen und Schulungen hat sich der deutsch – österreichsiche Arbeitskreis „neue interaktive Prüfungstechnik“ verschrieben. Siehe stBP 2009, S 207, *Huber und Wähnert* das Kölner Zeitreihenurteil und das Projekt „neue interaktive Prüfungstechnik“.

unnachvollziehbare Verdichtungen, Trainingsmodus, Betrugseinstellungen für Z-Bons) aufzudecken, durch welche auf einfachste Weise Einnahmen gekürzt werden können.

- **Erlösrevision Stufe 4 -**

Überlegungen über die Originalität der Daten - Möglichkeit nachträglicher Änderungen – Datenexport, Wiedereinspielen

Die vorgelegten Daten können „alternativ erzeugt worden sein. Hier einfach und gutgläubig die Daten entgegenzunehmen, einzuspielen und für jedenfalls originär zu halten, widerspricht dem Auftrag der BP zur Feststellung der Wahrheit.

- **Erlösrevision Stufe 5 –**

verdeckte fraudante Optionen

Die letzte (und prüfungstechnisch schwierigste Stufe der Ermittlung) ist die Erkundung, ob es im präsentierten System mögliche verdeckte Optionen zur Manipulation gibt. Diese Phase ist enorm kritisch, weil hierüber kaum auf einfach zugängliche Weise zu erhaltende Informationen erlangt werden können. Umso mehr tut hier der Erfahrungsaustausch zwischen den Prüfern, Dienstellen und Ländern not.

4.2 Nötige Risikoausrichtung der Maßnahmen

Auch auf die Steuerverwaltung an sich, als Organisation, welche im Bereich der Erlösprüfung echte Betrugsbekämpfung implementieren will, kommen künftig unausweichlich mehrere nötige Maßnahmen zu:
Die Grundausrichtung der Steuerverwaltung muss risikobezogen[30] werden, präventionsgerichtet und ressourceneffizient. Nicht die Präsentation von ständig steigenden Mehrergebnissen[31], die auf irgendeine Art und Weise „erzeugt“ werden, sondern nur der durchdachte Einsatz von Risikomanagement kann dies erreichen. Innovation ist ebenso essentiell wie die Überzeugung, niemals alle Risiken kennen zu können und daher offen zu sein für alle Arten der Risikofindung. Keinesfalls darf es so weit kommen, dass ein Prüfer, eine Einheit oder die BP als ganzes glaubt, sich mit den wahren prüfungstechnischen Problembereichen „auszukennen“ , weil der einzelne auf langjährige berufliche Erfahrung zurückblickt oder die Gesamtorganisation auf methodologische Traditionen oder in der Vergangenheit wohl erworbenes organisationales Wissen (quasi auf eine Art „emergente Schwarmintelligenz“) und letztlich auch nicht, dass die BP als ganzes allein durch jährlich steigende Mehrergebnisse[32] schon ihren Gesetzauftrag zur Sicherstellung der Gleichmäßigkeit und Gesetzmäßigkeit der Besteuerung voll erfüllt hätte. Das Umfeld Erlöse muss als Hochrisikobereich und damit vordringlicher Prüfschwerpunkt erkannt werden. Das Vorhandensein und die Vorlagepflicht von Daten muss als prüfungstechnische Option in Zielrichtung der Sicherstellung der Gleichmäßigkeit der Besteuerung durchgesetzt werden. Gleichzeitig muss die Ausnutzug der sich daraus ergebenden Möglichkeiten durch verpflichtende Auseinandersetzung mit der Konsistenz der Grundlagendaten sicher gestellt werden. Dies ist großflächig noch nicht im erforderlichen Ausmaß erfolgt, sowohl nicht in der BP von Klein- und Mittelbetrieben, wo das Abverlangen von Kassendaten noch nicht im umfassenden Ausmaß verbreitet ist, als auch in der Großbetriebsprüfung, wo die schwerpunktmäßige Klärung von Umgründungs, Bewertungs- Bilanzierungs- und anderen Rechtsproblemen kaum Raum lässt für weit reichende Ansätze zur Durchdringung von essentiellen Basisdatenkomplexen mittels Prüfsoftware (Inventuren, Fakturierungssysteme, Kostenrechnungen ua), obwohl dort gleichfalls vermehrte Prüfungsfelder hohen Ausfallsrisikos bestehen. Das knowhow über die Prüfungsgrundlagen in Systemen (Erfassungslogistik, Manipulationsmorphologie, Systemkunde, Formalprüfung) muss noch einem wesentlich größeren Kreis von Prüfern vermittelt werden. Wenn Prüfungsmethoden vorhanden sind, die EDV-gestützt auf einfache oder auch komplexe Art und Weise Massendaten durchdringen und analysieren können, muss es möglich werden, dass ein großer Teil der Prüfer diese fähigkeitshalber einsetzen kann und auch tatsächlich einsetzt. Dies kann durch Eigenverständnis oder durch Standardroutinen umgesetzt werden – jedenfalls bedingen beide Ansätze einer umfassenden Schulung.

---

[30] Präsentation von hohen Mehrergebnissen oder Sicherstellung der Gleichmäßigkeit der Besteuerung und der risikobezogenen Prüfauswahl. Siehe *Seer*, Möglichkeiten und Grenzen eines maßvollen Gesetzesvollzuges, StuW 1996, S 560 f. Mit dem vorhandenen Personal sollen die geschuldeten Steuern größtmöglich (– im wesentlichen) hereingeholt werden. Demgegenüber verlange gleichmäßiger Gesetzesvollzug nicht Kontrolle entsprechend dem quantitativen Ergebnis, sondern entsprechend dem Kontrollbedürfnis.

[31] Siehe *Thiel*, Steuerliche BP im Rechtsstaat, Tipkes Engagement für die Außenprüfung, StuW 1986, S 1: Die BP ist kein Geschäftsbetrieb, der auf die Erzielung maximaler Mehrsteuern und die Erwirtschaftung eines größtmöglichen Überschusses gerichtet ist. Sie hat vielmehr – ohne Ansehen ihrer steuerlichen Ergebnisse – allein den Zweck, für eine zutreffende Erfassung der steuerlich bedeutsamen Sachverhalte zu sorgen und damit eine gleichmäßige und gerechte Besteuerung zu sichern.

[32] Dazu *Tipke*, Das Dilemma der Steuerverwaltung – zeitnahe oder gesetzmäßige Besteuerung, StWa 1994, S.- 221 Die Stpfl seien keine Kollektivschuldner, die als Gesamtheit quantitativ zufrieden stellend zu veranlagen wären. Durch Verteilungen der Kontrollressourcen zwischen den Fällen im Ausmaß ihrer Aufkommensbedeutsamkeit würden Steuern bei verschiedenen Stpfl in unterschiedlichen Relationen festgesetzt. Dabei verzichte der Fiskus aber nicht bei jedem Stpfl auf Steuern in der selben Relation, sondern je nach Fallgröße beim einen auf mehr, bei anderen auf weniger, wobei er sich dort auch noch weitgehend auf die schlüssigen Angaben des Stpfl verlasse. Auf diese Weise würde im Ergebnis das Belastungsgefüge des materiellen Rechts umgestaltet. Siehe Tipke, ff. Je kleiner der Stpfl ist oder sich gibt, desto „maßvoller“ der Gesetzesvollzug – bis hin zur maßlosen Großzügigkeit der Nichtkontrolle. Richtiger Maßstab für die gebotene Kontroll- und Prüfintensität ist nicht die Fallgröße, sondern das individuelle Kontrollbedürfnis. Große Steuerpflichtige sind im Durchschnitt sicher nicht mehr prüfungsbedürftig als kleine. Sie bringen dem Staat aber mehr Geld. Aber das ist nicht der geeignete Maßstab für das Kontrollbedürnis.

Aus der Sicht des zielgerichteten Risikomanagements besteht das derzeitige Hauptproblem im Bereich der Betrugsbekämpfung in D und Ö nicht in der Aufdeckung einzelner spektakulärer Fälle, die dann „nach Verarztung" medienwirksam als Erfolge (Ermittlung hoher Nachforderungen – ungeachtet von deren Einbringlichkeit), sowie als Nachweis der schrecklichen Eigenschaften manipulationsfähiger Kassen und Systeme präsentiert werden, aber nichts helfen zur Erreichung einer wirksamen Prävention in der Breite, sondern in der Schaffung der umfassenden Gleichmäßigkeit der Besteuerung in einer Aufzeichnungsumwelt, in der die Anbieter und Hersteller von RegK davon sprechen, dass die Nichtverfügbarkeit einer „USB-Lösung"[33] beim Verkauf eines Kassensystems ein Wettbewerbsnachteil wäre. Effektive und weit reichende Steueraufsicht hat dem Manipulanten gegenüber eine hohe Entdeckungswahrscheinlichkeit sicherzustellen – nicht nur im Sinne der Tatsache, dass Manipulation als solche aufgedeckt werden kann, sonder auch und ganz besonders in der Ermittlung des Ausmaßes der nicht bezahlten Steuern und das in jedem einzelnen Fall (quantitative Entdeckungswahrscheinlichkeit[34]). Dieses elementare Problem verlangt nach neuen Lösungsansätzen, welche aber nur mehr zu einem Teil durch die BP als solche erfüllt werden können.

4.3 Lösungsansätze zur Betrugsbekämpfung im Kassenbereich in der Praxis der Steuerverwaltungen

Weltweit überlegen die Steuerverwaltungen, wie sie dem Problem der Steuerhinterziehung und insbesondere der digitalen Manipulation im Erlösbereich begegnen können. Nachfolgend sind beispielhaft Lösungsansätze punktuell dargestellt.

- **Maßnahmen gegen das Risiko der fehlenden Ersterfassung**

Diesem kann weder durch eine prüfungstechnische noch durch eine aufzeichnungstechnische Lösung entgegen getreten werden. Dies kann nur durch vermehrte Aufsicht – unmittelbar vor Ort - erreicht werden. Einerseits kann die wahre Aufzeichnungsform ermittelt werden, andererseits kann auch für einzelne GVF festgestellt werden, ob diese Eingang in die Grunderlösaufzeichnungen gefunden haben (zB bei Belegausstellungsverpflichtung durch eine spezielle Erhebungs- und Kontrolleinheit der Steuerverwaltung, wie in Italien die Guardia de Finanza.

- **Tax Compliance-Concept**

Das Compliance-Konzept kann im Umfeld der professionellen Steuerverkürzung mit seinen Grundsätzen[35] nur wenig helfen. Die Abschreckung für den Maipulanten (Nachzahlung, u.U. Strafe) wird ihn bei der derzeit bestehenden niedrigen Prüfwahrscheinlichkeit nur wendig aufhalten. Der positive Einfluss der Idee der Partnerschaft zwischen der Steuerverwaltung und dem StPfl beeinflußt eventuell solche Steuerbürger positiv, die versuchen, erhöhe Werbungskosten in ihrer Steuerklärung zu verstecken, aber kaum jemanden, der systematische Steuerhinterziehung unter Nutzung professioneller Betrugssoftware vollendet. Dennoch ist es möglich, unter dem Compliance-Gedanken freiwillige Maßnahmen vorzuschlagen , deren Einhaltung die sachliche Fallbeurteilung positiv beeinflusst. Zu deutsch: wer sich an zusätzliche freiwillige Auflagen hält, ist gut beraten, wer nicht verbleibt in der sachlichen Unrichtigkeit.

- **Neue mathematische Ansätze zur Verprobung**

Die Entdeckung von fehlenden Umsätzen über kalkulierende, analytische oder mathematische Prüfungslösungen ist in der gesamten Breite der Prüferschaft kaum leicht umzusetzen. Die Gerichte bürden den präzisen Nachweis der Richtigkeit von Methoden in jedem Fall unmittelbar dem Prüfer auf. Wenn er hier nicht absolut sattelfest ist, kann das Verfahren leicht kippen[36]. Die andere Seite wird oft von Superexperten unterstützt – bis zu hohem akademischem Niveau. Wenn Prüfungsabläufe und Feststellungen aus der Bahn laufen und um Nachzahlungen im wahren Ausmaß zu verhindern, wird viel Geld in Experten und Expertisen investiert, um Prüfungstechniken in Zweifel ziehen zu können. Die neuen Methoden (Chi²-Test, digitale Ziffernanalyse, Strukturanalyse, Schichtprofil, Zeitreihenvergleich) können gut Risikofelder isolieren und Unplausibilitäten aufzeigen, aber nur selten den erklärten Umsatz in seinen wahren Ausmaßen exakt ermitteln – zu einfach und minder sanktionierbar ist es von den Auswirkungen für ein Prüfungsverfahren her gesehen für Manipulanten in diesem Zusammenhang, Grundlagen, Daten und Unterlagen zu unterdrücken, damit Ansatzpunkte für genauere Berechnungen zu verhindern und so einer echten quantitativen Entdeckungswahrscheinlichkeit gekonnt entgegenzuwirken. Trotz alledem sind aus einer Verbindung von unangemeldeten Aufsichtsmaßnehmen und der Anwendung neuer Prüfungsmethoden – vor allem über Verteilungsstrukturen hohe quantitative Effekte ableitbar, wenn nämlich im Zuge der Steueraufsicht echte Strukturen in Teildatenbeständen festgestellt werden können und dann damit die erklärten Strukturen aus bereits veranlagten oder erklärten Zeiträumen auf Plausibilität nachgeprüft werden können.

---

[33] Gemeint ist ein „Zapper", siehe *Huber*, FN 2.

[34] Siehe *Huber*, zum Problem der quantitativen Entdeckungswahrscheinlichkeit bei der Erlösrevision im Spannungsfeld von Aufzeichnungen, Schätzungsmethoden und mangelnder Compliance, StBP 2007, S 165f

[35] Die Grundsätze des Compliance-Konzepts – in einfachen Worten erklärt sind: „streichle die Braven und vergräme sie nicht; überrede die weniger Braven, anständig zu werden; finde die Schlimmen und steig ihnen fest auf die Zehen".

[36] Siehe FN 29 Kölner ZRV

- **Kontrolle über Rechnungsnummern**

Voraussetzung ist Belegerteilungsverpflichtung gegenüber dem Endverbraucher. Bei Nutzung von RegK ist verpflichtend ein elektronisches Journal zu erstellen, in welchem jeder einzelne GVF eine serielle Nummer erhält, welche mit der Nummer auf der dem Endverbraucher übergebenen Rechnung übereinstimmt. Ergänzend kann (wie neuerdings in Kanada) verpflichtend die Zurückhaltung und Aufbewahrung einer Durchschrift der ausgestellten Rechnung eingeführt werden. Die Steuerverwaltung kann Rechnungen als Kontrollmaterial sammeln und dadurch stichprobenartig die Vollständigkeit der Erfassung kontrollieren. Risiken bei dieser Lösung bestehen in der Veränderung von Rechnungsinhalten, dem Löschen von Artikeln, ohne dass die Rechnungsnummer storniert wird. Das Sammeln von Rechnungen für die spätere Verwertung als Kontrollgrundlage ist noch nicht verbreitet[37].

- **Hochentwickelte Fiskalspeicherlösung**

Die Betrugsverhinderungswirkung ist hier am größten. Der Speicher sollte auf Artikelniveau oder zumindest auf Rechnungsniveau einhaken (nicht lediglich auf Basis der täglichen Gesamtumsätze wie zB in Griechenland, wo dann vorher Rechnungen heraus storniert werden). Die deutsche INSIKA-Lösung ist wohl planetenweit die derzeit am wenigsten angreifbare Option auf diesem Sektor.[38]

5. Die österreichische Kassenrichtlinie und die Steueraufsicht durch die neue Finanzpolizei

5.1 Das Revisionsproblem, der Zeitvorsprung des Maipulanten und mögliche Gegenmaßnahmen

Zu Beginn des 21. Jahrhunderts prägten die Niederländer die moderne digitale BP mit dem Slogan

„Digital audit means
- *understanding the business*
- *understanding the system*
- *understanding the data"*

kurz erklärt als

- *durchblicke das Geschäft* – wahre betrieblichen Verhältnisse in Bezug auf Betriebsart, Betriebsgröße, Beschäftigungsumfeld, Warenflüsse, innerbetrieblicher Wertestrom etc
- *durchblicke das System* – Systemidentifikation, Systemkontrolle, Systemprüfung (vor allem auf Ordnungsmäßigkeit), Systemoptionen (offene und verdeckte), Durchschaubarkeit des Systems – dazu Handbuch, Verfahrendokumentation, innere und äußere Abläufe, Veränderungen der Systempapameter
- *durchblicke die Daten (und Aufzeichnungen)* – Datenstruktur, Datenherkunft, Originalität und Unversehrtheit der Daten und Aufzeichnungen, Formalkontrolle, passive Prüfbarkeit, Kontrollierbarkeit

Im Zuge der im Laufe der späten 90er Jahre sich permanent qualitativ theoretisch und praktisch verbessernden knowhows im Bereich der revisionären Prüfung erschien die Perfektion der Analysemethoden als ultima ratio. Durch die vermeintliche Gewissheit, dass mittels der technischen Unterstützung durch EDV, durch Prüfsoftware, durch ständig leistungsfähigere hardware und eine Handvoll Entwickler, die alle paar Monate neue (und wirklich brauchbare) Modelle für analytische Prüfhandlungen daher brachten, ein Datenbestand tatsächlich horizontal, vertikal und strukturell vollständig durchdringbar würde, liefen manche Bestrebungen der modernen Finanzverwaltungen ganz in Richtung automatistische Anwendung der digitalen BP. Die Überzeugung – überspitzt dargestellt: hatte man erst einmal die Daten, dann schüttete man diese einfach in den „EDV-Analysetrichter" und „unten" kam das Prüfurteil (und das Mehrergebnis) raus. Gleich war auch die umfassende „Standardisierung von Prüfschritten" ohne nachfolgende tiefe Detailprüfung bei Auffindung von Ungereimtheiten geboren – samt dem idealen Endergebnis durch eine ebenso „standardisierte Schätzung auf Knopfdruck". Die Verwaltungen träumten von einer wundersamen Vermehrung der Ressourcen durch Zeiteinsparung von Prüfkapazitäten mittels „intelligentem, quasi selbst regelndem" EDV-Support[39], von einer Maximalbeschleunigung im Output und natürlich von einem sich dadurch permanent „von selber" vergrößerndem Mehrergebnis.

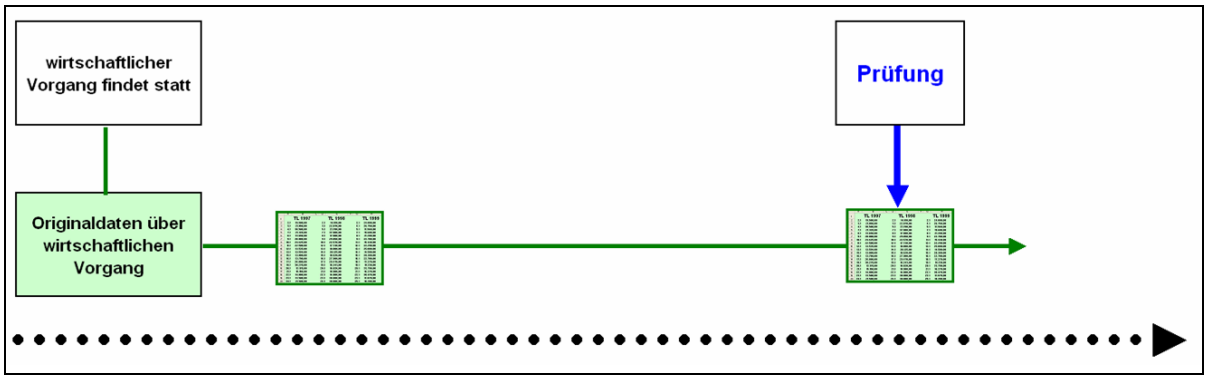
Voraussetzung dafür war die Datenvorlage. Im Bereich der Kassensysteme war der Ablauf vorgegeben:

- RegK erzeugt Daten - Prüfer bekommt Daten - Prüfer liest Daten ein - Prüfer prüft Daten mithilfe Prüfsoftware (direkt) und logischen Methoden und Modellen (indirekt) - Prüfer gibt Prüfurteil ab

[37] Als bessere Alternative zum Sammeln der Informationen der Aufzeichnungsdichte bei Rechnungen bietet sich das Verlangen einer Rechnung an, welche dann verdeckt festgehalten (fotografiert) wird und anschließend am Betriebsort zurückgelassen wird. Die Aufgriffswahrscheinlichkeit bei stornierten Rechnungen ist dann üblicherweise wesentlich höher.
[38] INSIKA umfassend dargestellt in der Beitragsserie in der stBP von *Huber* (FN2), Pkt IX.4.
[39] Fachleute warnten immer vor der „Prüfung auf Kopfdruck", zB *Odenthal*, Prüfsoftware im Einsatz, Verlag Datev, Handbuch für die praktische Analyse von Unternehmensdaten, S 174

- **„normaler“ Ablauf**

Daten entstehen, werden später (original) vorgelegt und geprüft



In der Theorie ist Voraussetzung für die Prüfung, dass Prüfungsgegenstand die Originaldaten sind. Faktum in der Praxis ist aber die Tatsache, dass Prüfungsgegenstand oft keine Originaldaten sind. Das bereitete den Revisionsbegeisterten aber keine großen Sorgen: im Vertrauen auf die hohe Qualität der automatistischen Prüfmethoden dachte man, dass man durch komplexe indirekte Methoden jede Datenveränderung nachträglich feststellen könnte. Insbesondere das „Benford-Gespenst“, welches vor allem von den Erzeuger von Prüfprogrammen ständig herbei beschwört wurde und wohl bis heute alle, die noch nicht mit ihm in Kontakt kamen, verblüfft, geisterte im Kreis der digitalen BP umher und wurde als DAS Tool zum Finden von Manipulation gehandelt – ebenso wie der Chi²-Test, quasi ein „Ableger“ von Benford.[40]

Nach und nach kamen aber - vor allem im Bereich der BP im Bargeldbereich - ein böses Problem auf:
die **modell erfüllende Datenveränderung zur Schaffung verkürzter, aber plausibler Verhältnisse mithilfe von „logisch“ manipulierenden Kassensystemen unter mittelschweren Formalmängeln**.

Die „Dummen“, welche früher runde Stückzahlen aus Warengruppenberichten entfernt hatten, bevor sie den Z-Bon erstellten, die „Gierigen“, die die großen und größten Rechnungen stornierten, weil da „am meisten raus kam“, die „Tüftler“, die manche Produkte im Artikelstamm ausließen, sodass diese gar nicht im Warengruppenbericht und im Abschluss aufschienen – sie alle konnte man mit modernen, mathematisch „angehauchten“ Prüfmethoden entlarven. Mit dem in der Folge als Reaktion aufkommenden „fortentwickelten“ Kassenschwindel lagen die Verhältnisse ganz anders.

Das Auslassen eines Bedieners (Kassierers) oder dessen Verbergen (siehe Pkt. 3.3 - Concealer) nimmt eine Substruktur, die sich bei durchgehend ähnlicher Gesamtgeschäftsfallstruktur inhaltlich, verteilungs- und betragsmäßig kongruent aufbaut, nahezu spurlos heraus. Manche kamen auf die Idee, dass man nicht unbedingt die größten Rechnungen auslassen musste, wenn man Pauschalleistungen anbot (welche in der digitalen Ziffernanalyse immer als Störfaktoren auftreten), war dies nahezu gefahrlos möglich. Oder am einfachsten – wenn man jeden z.B. 4. Geschäftsfall (oder ¼ der Tische) ganz aus ließ (oder nach stornierte), erreichte man dadurch über eine längere Zeitspanne nicht nur eine Verkürzung um 25%, sondern auch eine Beibehaltung aller Strukturen (Verteilung, Ziffernstruktur, Bedienerstruktur, Warengruppen, Artikel, usw).

---

[40] Bei aller Begeisterung der Weiterentwicklung indirekter Methoden darf nicht vergessen werden, dass die Einschätzung der sachlichen Richtigkeit sich aus einem Gesamtbild ergibt, das sich aus dem Formalzustand und der Plausibilitätsbeurteilung des Rechenwerks zusammensetzt. So sehr aussagekräftig indirekte Überprüfungs- und Verprobungsmethoden qualitativ sein können und so notwendig ihr Einsatz auch im Massendatenbereich ist – wahre Verhältnisse zu erkunden ist ihnen kaum möglich, dazu bedürfte es der absoluten Akzeptanz von Soll-Modellen v.a. im Bereich Verteilung, innerer Zahlenstruktur und von Vergleichsmaßstäben auf tief reichenden Ebenen, welche weit über steuerliche Richtsätze hinausgehen. Wichtigstes Element der digitalen BP ist es aber, alle Methoden als „Prüfungsnetz“ zu vereinen, welche eine Indizienkette aufbauen können, welche dann aber auch argumentiert werden muss. Dazu bedarf es hoch qualifizierter Ausbildung der Betriebsprüfer, um zu verhindern, dass automatistisch nach Einlesen des Datenbestandes und dem Drücken einiger Menü-buttons Ergebnisse erwartet werden, die von der Gegenseite unwidersprochen hingenommen werden. Siehe dazu diverse Judikate der letzten Zeit zum Chi²-Test über Endziffern. Benford (NBL - Newcomb / Benford Law) ist ein brauchbarer Ansatz der digitalen Ziffernanalyse für eine erste (durch Analysesoftware rasche) Knopfdruckkonsistenzprüfung. Wenn sich ein Datenbestand aber nicht Benford annähert, ist dies zwar aufklärungsbedürftig – und nahezu immer auch aufklärbar – allein – der Beweis für manipulative Datenveränderungen ist dadurch (noch) nicht erbracht.
Veröffentlichungen zu Benford (beispielhaft): *Posch*, Ziffernanalyse in Theorie und Praxis; *Odenthal*, Digitale Ziffernanalyse: Ein wirkungsvoller Beitrag zur computergestützten Deliktrevision, WP 1999, S 633; *Sosna*, Einsatz statistischer Methoden zur Risikoanalyse, Recherche und Lokalisation von Steuerausfällen, stBP 2000, S 41 (Teil 1) und S 68 (Teil 2); *Mochty*, Die Aufdeckung von Manipulationen im Rechnungswesen – Was leistet Benford’s Law? WP, 2002, S 725; *Huber*, die neue Prüfungstechnik in der BP, ARD ORAC 2004; *Odenthal* – Revidata, digitale Ziffern- und Zahlenanalysen – Strategien zur Ermittlung unterschlagungsrelevanter Faktoren in Datenbeständen – Internetveröffentlichung; *Huber und Huber* Einsatz von Supporting Audit Software als Prüfungstool für erweiterte Ziffernanalysen, stBP 2006 S. 280, 305; *Huber*, digitale Ziffernanalyse versus Strukturanalyse und die logische Herleitung von NBL, stBP 2008, S 241, 273; *Huber und Huber* Nochmals zur digitalen Ziffernanalyse und zur Herleitung von Benford (NBL), sowie zum Chi2-Test über die „Endziffern“ stBP 2009, S 65, 93, 121

Das wahre Grundproblem der Revision liegt aber im **Zeitvorsprung des Manipulanten**, der einer Prüfungsmaßnahme stets so lange gelassen entgegen sehen kann, als diese angemeldet wird und primär die aufgezeichneten Verhältnisse der Vergangenheit erkundet. Diese Verhältnisse können nachträglich unter Angleichung des nötigen Ist-Zustandes an den gewünschten Soll-Zustand „erschaffen" werden. Jegliche Revision hinkt inhaltlich stets am dem tief greifenden Problem, ob die untersuchten Daten und Aufzeichnungen originär sind oder nicht, sowie an der Taktik des Manipulanten, über seine „kleinen" Versäumnisse zwar zerknirscht zu sein, damit aber wesentliche Grundlagen für die Revision zunichte zu machen. „Logische" Manipulation kann nachträglich nicht mehr in annähernd den wahren Verhältnissen entsprechendem Ausmaß aufgedeckt werden – durch keine – noch so hoch entwickelte und komplexe Verprobungsmethode, die stets auf dem Vergleich von Ist-Strukturen mit Soll-Strukturen beruht, wobei diese Soll-Strukturen hinlänglich verbindlich sein müssen.

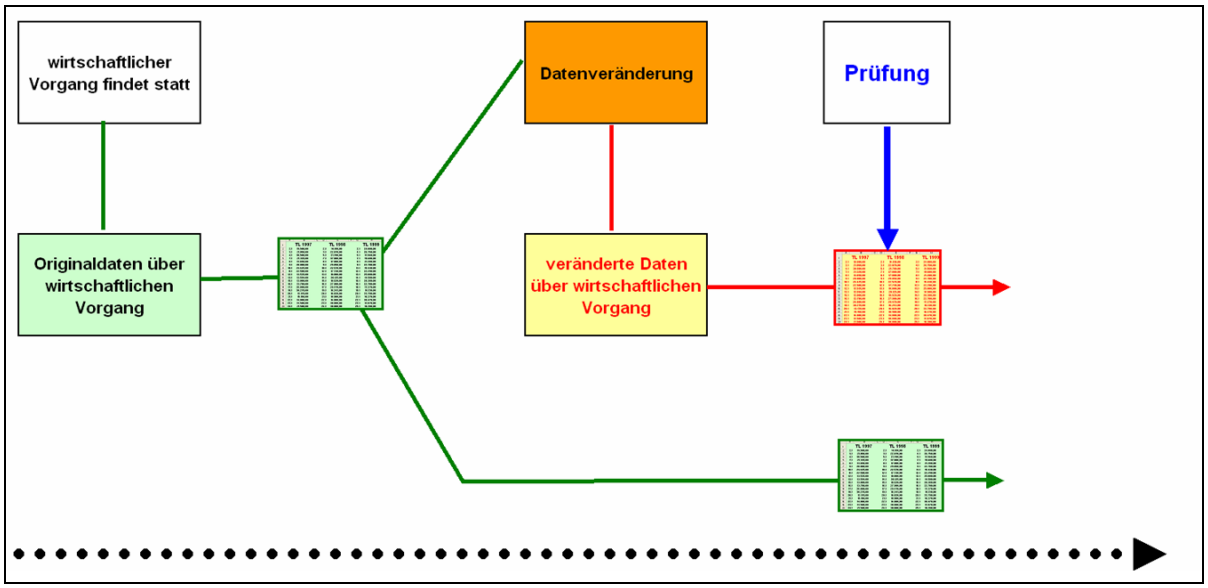
Dieser Zustand und die sich ergebenden Folgen werden nachfolgend punktuell angeführt.

Vorsprung bei Manipulation

- Qualitativ
  - Durch „späte" Revision der Vergangenheit entsteht ein erheblicher Zeitvorsprung zur Nacherstellung von Unterlagen / Daten
  - Bagatellisierung der Auswirkung von Mängeln als Beurteilungsgrundlagen für das Ausmaß der Zweifel an der sachlichen Richtigkeit
  - Wenn das Rechenwerk ist nur „ein bißchen" nicht ordnungsmäßig ist – Frage des Kippens der Ordnungsmäßigkeit (sachlichen Richtigkeit)
  - Das allgemeine Bewußtsein und Verständnis der Bedeutung von § 146 (4) AO für den Vertrauensvorschuss des § 158 AO ist weitflächig teils realitäts- und zeitfremd
- Quantitativ
  - Bei zu vielen „kleinen" Mängeln und Kippen der Ordnungsmäßigkeit Verhandlung über Höhe der Zuschätzung ohne wahre Ansatzpunkte im Rechenwerk kollidiert unmittelbar mit dem Grundsatz der Gleichmäßigkeit
  - Bei Beurteilung der „aufgezeichneten Vergangenheit" existieren keine Ansätze für reale wirtschaftliche Verhältnisse zur Schätzung

- **Problem Datenmanipulation**

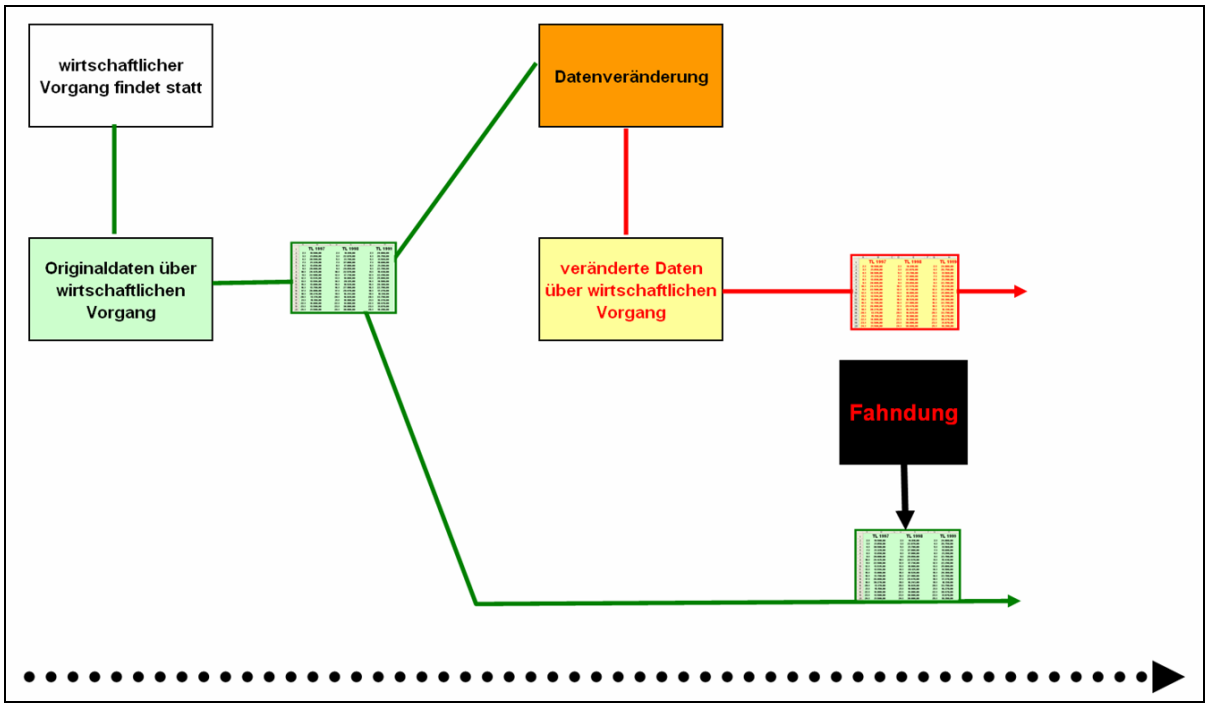
Daten entstehen, werden relativ bald verändert, die veränderten Daten werden später vorgelegt und geprüft. Die Originaldaten werden zurückbehalten



Als einzige Lösung dagegen erschien dann doch wieder nur der Einsatz der Steuerfahndung. Nur diese Verfolgung konnte - in einer „Radikaloperation" – für die Klärung wirklicher Verhältnisse sorgen. Die Fälle, welche die Steuerfahndung im Zuge ihrer Tätigkeit im Kassenumfeld aufdeckte, waren auch meist spektakulär und haben auch entscheidend zum Aufbau von Wissen im Rahmen der steuerlichen Manipulationsmorphologie bei Kassen geführt. Das Problem lag nur - erst mal abgesehen von den nötigen Rechtsgrundlagen für einen Steuerfahndungseinsatz – darin, dass man nicht in jeden Betrieb, in dem eine - eventuell manipulierbare - Kasse stand – allein deshalb die Steuerfahndung hinschicken konnte, weil es einfach zu wenig Fahnder gibt.

- **Mögliche Maßnahme 1 - Steuerfahndung**

Die veränderten Daten werden im Zuge einer späten Verfolgungshandlung gesucht und ev. gefunden



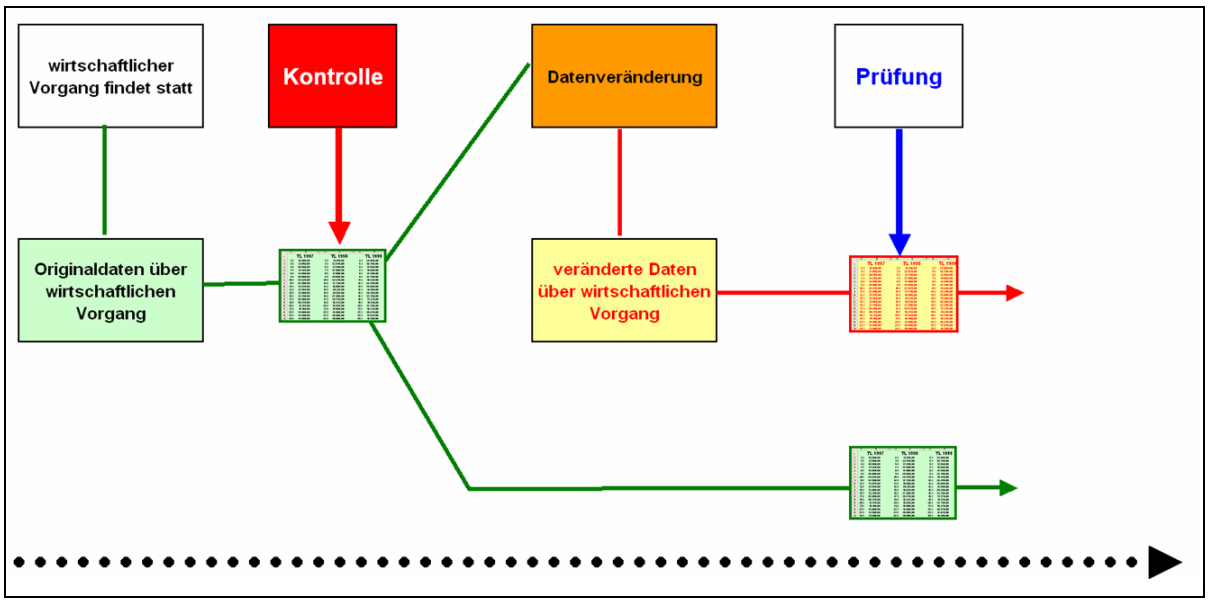
In Ö ließ eine späte Rückbesinnung auf grundlegende Maßnahmen des Verfahrensrechts eine Alternative entstehen, die sich gut und voll ins Umfeld der modernen Betrugsbekämpfung einfügte. Der Ablauf zu deren Einführung war wie folgt:

- Schritt 1 – Diskussion, Klärung und Festlegung von inhaltlichen Vorgaben bei Kassen zur Ordnungsmäßigkeit
- Schritt 2 – Verkündung der Vorgaben
- Schritt 3 – effektive Kontrolle der Einhaltung der Vorgaben

Vorderster Effekt dabei sollte die weitgehende Ausschaltung des **Zeitvorsprungs** sein, den ein Kassenmanipulant aufbauen und darin bequem die Wunsch-Angleichung seines Aufzeichnungsumfeldes vornehmen kann.

- **Mögliche Maßnahme 2 - Steueraufsicht**

Die noch nicht veränderten Daten werden im Zuge einer zeitnahen Aufsichtshandlung eingesehen und gesichert.



Dazu bedurfte es der Schaffung eines Kataloges der Klarstellung der Ordnungsmäßigkeitskriterien im Rahmen eines Diskussionsprozesses, der von der (Kassen-)Umwelt wahrgenommen wurde und so einen Publizitätseffekt auslöste, sowie einer Vollzugseinheit, die - anders als die BP, welche an der aufzeichneten Vergangenheit herumprüft – unmittelbar und unangemeldet vor Ort, gegenwärtig und in Echtzeit die wahren Verhältnisse im Aufzeichnungs- bzw Kassenbereich eines Betriebes durch Kontrolle[41] ermitteln kann.

5.2 Rechtliche Grundlagen für Gegenmaßnahmen in Ö

5.2.1 Aufzeichnungsregeln

In der ö BAO sind - spätestens seit dem Betrugsbekämpfungsgesetz 2006 – elementare und zeitgemäße, an die aktuellen EDV-Verhältnisse im Aufzeichnungsbereich angepasste Aufzeichnungsregeln enthalten, unter anderem folgende

- *Aufzeichnungen, die nach Maßgabe der einzelnen Abgabenvorschriften der Erfassung abgabepflichtiger Tatbestände dienen, sind zu führen, aufzubewahren und über Verlangen vorzulegen.*
- *Führung der Aufzeichnungen derart, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle vermitteln können*
- *Eintragungen der Zeitfolge nach geordnet, vollständig, richtig und zeitgerecht*
- *Verfolgbarkeit der einzelnen Geschäftsvorfälle in ihrer Entstehung und Abwicklung*
- *Elektronisches Radierverbot*
- *Möglichkeit der Überprüfung der vollständigen, richtigen und lückenlosen Erfassung aller Geschäftsvorfälle beispielsweise durch entsprechende Protokollierung der Datenerfassung und nachträglicher Änderungen (Mindeststandard)*
- *Sicherung der vollständigen und richtigen Erfassung und Wiedergabe aller Geschäftsvorfälle durch entsprechende Einrichtungen gesichert und*
- *leichte und sichere Führung des Nachweises der vollständigen und richtigen Erfassung aller Geschäftsvorfälle durch entsprechende Einrichtungen (Überprüfungsmöglichkeit) – die in den beiden letzten Punkten genannten Einrichtungen gem. §§ 131, 132 BAO werden kurz als Einrichtung 131 bezeichnet)*
- *Nachvollziehbarkeit von Summenbildungen*[42]

5.2.2 Kontrolle

Unabhängig von den Bestrebungen zur Regelung des Aufzeichnungsumfeldes entstand bereits im Zuge einer Regierungsinitiative 2009 gegen Steuer- und Sozialbetrug das Konzept für eine eigene Vollzugsabteilung der Finanzverwaltung, welche vor allem im Bereich der Betrugsbekämpfung die Organisation durch zeitnahe Kontrolltätigkeiten unterstützen sollte – die Finanzpolizei.

Mit dem Betrugsbekämpfungsgesetz 2010[43] wurde mit Wirkung ab 1.1.2011 die vormalige Sondereinheit KIAB (Kontrolle illegaler Ausländerbeschäftigung) in Finanzpolizei umgetauft und deren Rechte erweitert. Die KIAB war in etwa vergleichbar mit der Finanzkontrolle Schwarzarbeit (FKS), einer Arbeitseinheit des deutschen Zolls. Die nunmehrige FinPol stellt eine Sondereinheit der Finanzämter dar, welche die Einhaltung abgabenrechtlicher, sozialversicherungsrechtlicher, gewerberechtlicher und glücksspielrechtlicher Bestimmungen sowie der Bestimmungen des Ausländerbeschäftigungsgesetzes (AuslBG) überwachen soll. Zur Erfüllung dieser Aufgaben ist die Finanzpolizei nunmehr aufgrund von § 12 Abgabenverwaltungsorganisationsgesetz (AVOG) zur Betretung von Grundstücken und Baulichkeiten sowie Betriebsstätten, Betriebsräumen und Arbeitsstätten sowie zur Feststellung der Identität von Personen und zur Anhaltung und Überprüfung von Fahrzeugen und sonstigen Beförderungsmitteln einschließlich der mitgeführten Güter berechtigt, sofern Grund zur Annahme besteht, dass in diesen Räumen, Fahrzeugen oder von diesen Personen Zuwiderhandlungen gegen die von den Abgabenbehörden zu vollziehenden Rechtsvorschriften begangen werden. Gleichartige Befugnisse kommen der Finanzpolizei schon aufgrund § 26 Abs 3 und 4 AuslBG zu. Nach dem AuslBG ist die Finanzpolizei darüber hinaus berechtigt, bei Gefahr im Verzug Ausländer für die Fremdenpolizei festzunehmen, wenn Grund zur Annahme besteht, dass diese Ausländer einer illegalen Erwerbstätigkeit in Ö nachgehen.

Im Betrugsbekämpfungsgesetz 2010 heißt es im Absatz 4 des § 12 AVOG:
Zur Gewinnung von für die Erhebung von Abgaben maßgebenden Daten können allgemeine Aufsichtsmaßnahmen (§§ 143 und 144 BAO), Ersuchen um Beistand (§§ 158 f BAO) sowie die notwendigen Aufsichts-, Kontroll- und Beweissicherungsmaßnahmen gemäß Abs. 1 bis 3 von allen Abgabenbehörden vorgenommen werden. Dabei können bei Gefahr im Verzug auch 1. Sicherstellungsaufträge (§ 232 BAO) erlassen sowie 2. Vollstreckungs-

[41] *Tipke*, Steuerrechtsordnung, 1993, Bd. III, S 1208: Ohne Kontrolle gibt es in einem Rechtsstaat gewiss keine gleichmäßige Besteuerung !
[42] Zum Verdichtungsproblem siehe *Huber*, Aufzeichnungssysteme und Prüfungsebenen, stBP 2005, S 136
[43] BBG 2010 http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_00875/index.shtml

handlungen (§§ 31, 65 ff und 75 AbgEO) und 3. Sicherungsmaßnahmen (§ 78 AbgEO) vorgenommen werden. Bei der Durchführung dieser Amtshandlungen sind die Organe als Organe des jeweils zuständigen Finanzamtes tätig.

In den Erläuterungen der Hauptgesichtspunkte des Entwurfes für die Änderungen im AVOG wird ausgeführt:
Kernaufgabe der Finanzverwaltung ist die Sicherung des Abgabenaufkommens zur Finanzierung des Staatshaushaltes. Ein wesentlicher Schwerpunkt ist dabei eine effektivere Bekämpfung der Steuerverkürzung und insbesondere der Schattenwirtschaft, die bekanntermaßen außerhalb der Grundsätze ordnungsgemäßer Buchführung und Aufzeichnungen agiert. Mit den nunmehr eingeräumten Befugnissen ... werden auch die Möglichkeiten der Steueraufsicht in der Finanzverwaltung wesentlich verbessert, indem ***zeitnahe und vor Ort durchgeführte Informationsgewinnung über abgabenrechtlich relevante Sachverhalte*** *zur Aufdeckung steuerlich nicht erfasster Unternehmen, zur Ermittlung erster Besteuerungsgrundlagen aber* ***auch zur Sicherstellung der vollständigen Besteuerungsgrundlagen*** *gesetzlich normiert werden.*
Damit sind die Grundlagen für eine effektive Steueraufsicht im Kassenbereich gegeben.

5.3 Grundgedanken der ö Kassenrichtlinie

Die ö. KRL[44] entstand nach Vorschlägen des BMF im Rahmen eines Diskussionsprozesses im Arbeitskreis der davon betroffenen Gruppen (BMF, Wirtschaftskammer, Kammer der Wirtschaftstreuhänder, Kassenhersteller), welcher über nahezu ein Jahr eine weitgehend einvernehmliche Lösung in Form einer best-practise-Vorgabe im FairPlay-Umfeld (also der partnerschaftlich gesehenen Kooperation zwischen StPfl und Finanzverwaltung) entwickelte. Das bedeutete die technische und inhaltliche Auseinandersetzung mit den (vorgegebenen) gesetzlichen Rahmenbedingungen, deren technischem Umfeld, möglichen Sicherheitslösungen und den Grundlagen für machbare Kontrollmaßnahmen zum Schutze der Anwender ordnungsmäßiger Kassen bzw Systeme und deren Herstellern bzw - programmierern. Das bedeutet, dass das Verfahrensrecht nicht geändert werden musste, es wurde nur klarstellend ausgelegt. Die Auslegungen und Klarstellungen erschienen auch wegen der fortlaufenden technischen Neuerungen im Aufzeichnungsumfeld als nötig.

Wie in D basiert die Lösung der Frage, ob das Rechenwerk der Besteuerung zugrunde zulegen ist, auf der Vermutung der Ordnungsmäßigkeit (in Ö § 163 BAO). Im Zuge der Beurteilung der Ordnungsmäßigkeit ist eine Gesamtsicht anzuwenden, die für und wider abwägt. Wie oft besprochen, gibt es nahezu kein 100% ordnungsmäßiges Rechenwerk. Die auftretenden formellen Mängel sind vielmehr dahin zu würdigen, ob sich daraus Gründe für Beanstandungen bzw. Zweifel an der sachlichen Richtigkeit des Rechenwerkes ergeben, also der Wahrscheinlichkeit, dass das wirtschaftliche Geschehen, so wie es sich tatsächlich ereignet hat, auch genauso inhaltlich und betraglich seinen Eingang ins Rechenwerk gefunden hat. Daran misst sich auch die Notwenigkeit einer Korrektur der Besteuerungsgrundlagen im Zuge einer Schätzung.

In der ö. KRL sind deshalb auch freiwillige Maßnahmen angeführt, durch welche die Ordnungsmäßigkeit erhöht werden kann - auch wenn diese Maßnahmen und ihre Inhalte nicht aus der BAO als Soll- oder Mussbestimmungen herleitbar sind, ergeben sie sich doch aus den Grundsätzen der Prüfbarkeit und Kontrollierbarkeit. Ihre (freiwillige) Einhaltung schafft für diejenigen, welche ihre steuerlichen Verpflichtungen freiwillig erfüllen wollen („compliant taxpayer“) die kalkulierbare Sicherheit der Ordnungsmäßigkeit.

5.4 Exkurs: Fiskalspeicher und Ordnungsmäßigkeitsvermutung aus historischer Sicht und unter Betrachtung des § 146 (4) AO

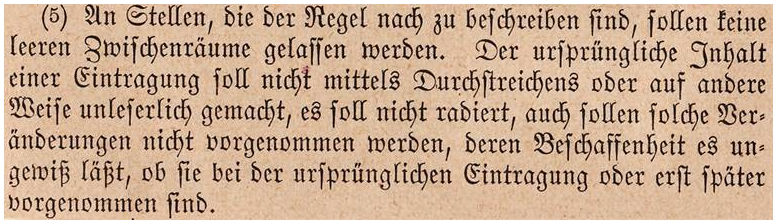
Die Möglichkeit der Einrichtung von technischen Fiskalmaßnahmen („Fiskalspeicher“) wurde im Zuge von Gesprächen zwischen der Wirtschaft, der Beraterseite und der Kassenhersteller, -bzw Programmierer diskutiert. Auch verbreitet zustimmende Meinungen scheiterten primär an mangelnden gesetzlichen und rechtlichen Grundlagen sowohl für die Speicher selbst, als auch für notwendige flankierende administrative Maßnahmen. Eine Fiskallösung ohne eine umfassende Verpflichtung zur Belegerstellung ist kaum durchführbar – eine solche ist dem ö. Verfahrensrecht aber fremd.
Daneben gab es aber auch folgende Bedenken: „Einfache“ Fiskalspeicher, also Lösungen welche nicht technisch „perfekt“ arbeiten, sind leicht angreifbar. Die Erfahrungen aus Ländern, welche solche „einfache“ Lösungen anwenden, zeigen die Problematik. Zum Beispiel: In manchen Systemen werden nur die Tagessummen (also das Ergebnis aller Geschäftsfälle) gespeichert. Für diesen Vorgang gibt es Sicherheitseinrichtungen. Für die Gebarung der Geschäftsfall-Daten selbst sind aber oft keine oder zu wenige Gewähreinrichtungen vorhanden, sodass dann Geschäftsfall-Zahlen gelöscht werden, welche die Tages-Endsummen mindern. Das Hauptproblem aus Vollzugssicht ist nicht nur, dass dann willkürlich auch manipulierte Endbeträge der Besteuerung zugrunde gelegt werden, sondern auf d und ö Verhältnisse umgelegt die Frage der Problematik des Vertrauens in die durch Fiskalspeichernutzung quasi „garantierte“ Ordnungsmäßigkeit, welche – entsprechende gesetzliche Grundlagen

[44] Kassenrichtlinie 2012 – siehe ö. BMF-Seite
https://www.bmf.gv.at/Steuern/Fachinformation/WeitereSteuern/Bundesabgabenordnung/KRL2012Kassenrichtl_12730/_start.htm

vorausgesetzt - wiederum einen „Anspruch“ auf Ordnungsmäßigkeitsvermutung – einschließlich der Akzeptanz des Rechenwerks – implementiert – sonst wäre ja „der ganze Aufwand umsonst“. Die sich in der Prüfung von Kassensystemen laufend stellende Frage der Ordnungsmäßigkeit oder Nichtordnungsmäßigkeit hat die weitere Facette der damit vom Prüfer zu akzeptierenden wirklich und wahrhaftig vollständigen Erfassung wegen der Ordnungsmäßigkeitsvermutung nach § 158 AO. Dann sind aber Plausibilitätsprüfungen und Verprobungen schon von ihrem Sinn aus nicht nötig. Wenn der bloße Einsatz eines Fiskalspeichers in der Folge die vollständige Akzeptanz der Zahlen im Rechenwerk durch die Finanz bewirkt, muss die Einrichtung so perfekt sein, dass sich dann ein sie benutzender StPfl auf diese Akzeptanz verlassen kann und nicht – wie in den Fällen, wo „durchlässige“ Einrichtungen verwendet werden – wiederum die erfassten Zahlen in Frage gestellt oder wie in allen anderen Fällen geprüft werden müssen, gleichsam als neues, zweites Umfeld von fraglichen Daten neben den ohnehin fraglichen Daten aus Nicht-Fiskalsystemen. In dieser Umgebung entsteht eine verschärfte Form der Ungleichmäßigkeit, weil dann vorweg die Ordnungsmäßigkeitskriterien als erfüllt gelten würden, ohne dass dies 100%ig sicher steht[45]. Das Verfahrenrecht – konkret Univ.Prof. Roman Seer, Uni Bochum[46] im AO-Kommentar Tipke / Kruse – hat reagiert und den umfassenden Vertrauensvorschuss des § 158 AO in Frage gestellt.

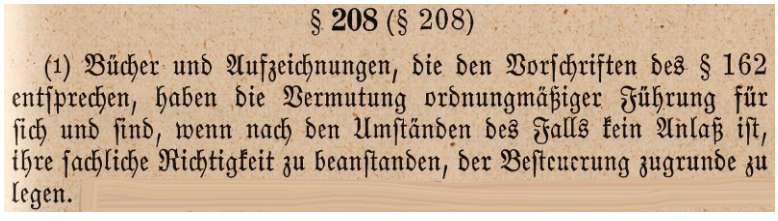
Betrachtet man den Vertrauensvorschuss[47] des § 158 AO („*Die Buchführung und die Aufzeichnungen des StPfl, **die den Vorschriften der §§ 140 bis 148 entsprechen**, sind der Besteuerung zugrunde zu legen, soweit nach den Umständen des Einzelfalls kein Anlass ist, ihre sachliche Richtigkeit zu beanstanden*“) im Zusammenhang mit der Nutzung von Kassensystemen unter der Sicht des § 146 Abs. 4 AO („*Eine Buchung oder eine Aufzeichnung darf nicht in einer Weise **verändert** werden, dass **der ursprüngliche Inhalt nicht mehr feststellbar** ist. Auch solche **Veränderungen** dürfen nicht vorgenommen werden, deren **Beschaffenheit** es **ungewiss** lässt, ob sie **ursprünglich oder erst später gemacht** worden sind*“), tut sich eine Vielzahl von Fragen und Unsicherheiten auf, welche, je länger sie hinsichtlich ihrer Auswirkungen auf die Besteuerung durchdacht werden, zu schweren rechtlichen Bedenken mutieren.

§ 146 Abs. 4 AO ist sinngemäß aus dem unten angeführten § 162 Abs. 5 RAO hervor gegangen, § 158 AO aus § 208 RAO. Der dabei artikulierte Vertrauensschutz entstand aus dem inhaltlichen sinnhaften und kausalen Zusammenwirken der beiden historischen Bestimmungen. Aus historischer Sicht beurteilt, leitet sich der Vertrauensschutz wohl aus der genialen Idee der Beweisführung Enno Beckers ab, der realistisch erkennen mußte, dass eine umfassende und vollinhaltliche Prüfung der wahren und echten Buchungsgrundlagen niemals möglich sein würde. Es hätte dazu nämlich der permanenten Kontrolle ALLER buchungs- und aufzeichnungswürdigen Vorgänge in der Wirtschaft durch sachverständige Dritte als Kontrollorgane in Echtzeit bedurft! Nur wenn bei Abwicklung eines wirtschaftlichen Vorgangs und bei dessen nachfolgender Aufzeichnung ein steuerliches Kontrollorgan mit beobachtet, kann anschließend mit Sicherheit ausgesagt werden, dass hier sachlich richtig als Basis der Besteuerung aufgezeichnet wurde.


(5) An Stellen, die der Regel nach zu beschreiben sind, sollen keine leeren Zwischenräume gelassen werden. Der ursprüngliche Inhalt einer Eintragung soll nicht mittels Durchstreichens oder auf andere Weise unleserlich gemacht, es soll nicht radiert, auch sollen solche Veränderungen nicht vorgenommen werden, deren Beschaffenheit es ungewiß läßt, ob sie bei der ursprünglichen Eintragung oder erst später vorgenommen sind.

Beckers Lösung war 2-stufig:

1. die Einsetzung eines strikten Formalismus bei Aufzeichnungen, welcher aber in sich leicht erfüllbar war mittels geordneter und ordentlicher Führung der Unterlagen.


§ 208 (§ 208)

(1) Bücher und Aufzeichnungen, die den Vorschriften des § 162 entsprechen, haben die Vermutung ordnungmäßiger Führung für sich und sind, wenn nach den Umständen des Falls kein Anlaß ist, ihre sachliche Richtigkeit zu beanstanden, der Besteuerung zugrunde zu legen.

2. Der Schluss auf die Ordnungsmäßigkeit. Becker legte zur Unnötigkeit der oben beschriebenen, real wahrhaft undurchführbaren Aufsichtstätigkeit die bekannte Vermutung zugrunde:

[45] Siehe Vortrag „Risikomanagement in der Außenprüfung“, *Huber*, Uni Bochum, Protokoll zum Bochumer Steuerseminar für Praktiker und Doktoranden vom 19. Februar 2010 http://www.fachanwalt-fuer-steuerrecht.de/pdf/Protokoll_20100002.pdf

[46] Zur Problematik der Kassenmanipulation aus verfahrensrechtlicher Sicht des § 158 AO siehe *Seer* in Tipke/Kruse AO zu 158 Tz 21b. In dem für Manipulationen besonders anfälligen Bereiche von Kassen- und Bargeschäften (s. *Huber* StBp 07, 138fff; *Huber* StBp 09, 153, 185, 217, 253, 317), *Klingelbiel* NWB 08 2293ff) sind in letzter Zeit mit erheblicher krimineller Energie und Unterstützung spezieller Kassensoftware neue Möglichkeiten entwickelt worden, um einer manipulierten Buchhaltung den Anschein der formellen Ordnungsmäßigkeit zu geben. Die Perfektionierung der Prüfsoftware und damit die einhergehende Ausbildung der Betriebsprüfer (s. *Huber* StBP 07, 161ff) ist geboten, weil sich für den Bereich der Kassen, und Bargeschäfte mit Hilfe herkömmlicher Prüfungsmethoden vielfach kaum mehr Aussagen über die Ordnungsmäßigkeit einer Buchführung machen lassen. Es besteht die Gefahr, dass dadurch im Bereich der Kassen- und Bargeschäfte die Beweiskraft des § 158 ihre Legitimation (Vertrauensvorschuss) verliert. (s. *Huber* StBp 09, 185, 188ff). Eine Lösungsmöglichkeit könnte de lege ferenda darin bestehen, die Rechtsvermutung des § 158 an die Verwendung eines zertifizierten Fiskalspeichers, der dem Standard einer „Integrierten Sicherheitslösung für messwertverarbeitende Kassensysteme – INSIKA“ (Huber, StBp 09, 286, 287 ff) entspricht, zu knüpfen.

[47] Zum Vertrauensvorschuss allgemein siehe *Huber/Seer*, Steuerverwaltung im 21. Jahrhundert: Risikomanagement und Compliance, StuW 4/2007.

Wenn Aufzeichnungen und Buchungen in „***geordneter***“ und „***ordentlicher***“ Art und Weise durchgeführt wurden, vertraute der Fiskus kraft der Vermutung des § 208 RAO auf die „***Ordnungs***“mäßigkeit (also die inhaltliche Richtigkeit) dieser Aufzeichnungen und Buchungen, somit darauf, dass die wirtschaftlichen Vorgänge in den Büchern und Aufzeichnungen ebenso betraglich abgebildet wurden, wie sie sich im echten wirtschaftlichen Leben in der Vergangenheit[48] ereignet hatten.

Diese Ermittlung der Erfüllung der Formalismen war zu RAO-Zeiten durch einen sachverständige Dritten durchaus problemlos möglich: das Erkennen von Zwischenräumen, Durchstreichungen, Unleserlichkeiten, oder zeitpunktmäßig unzuordenbaren Veränderungen war wohl jedem Betriebsprüfer, aber auch jedem mit äußerlich akkurater Buchung und Aufzeichnung in handschriftlicher Form auf Papier vertrautem Bearbeiter in vollem Umfang zuzutrauen. Also war auch das Vertrauen in diesen äußeren Formalismus durch Schluss auf Ordnungsmäßigkeit jedenfalls unzweifelhaft wahrnehmungshalber möglich und gegeben.
Der sachverständige Dritte hat sich gemessen an diesen damaligen Anforderungen bezogen auf seine nötigen technischen Fähigkeiten über die letzten 70 Jahre gewaltig weiter entwickeln müssen. Drüen[49] fügt in diese Gruppe der sachverständigen Dritten die Buchhalter, Wirtschaftsprüfer, vereidigte Buchprüfer, Steuerberater und für den BP-Dienst ausgebildete Bedienstete der Finanzverwaltung ein. Ergänzend - in Bezug auf die Angemessenheit der Frist des § 145 Abs. 1 AO - bestimmt sich diese (und die nötige Sachkenntnis des sachverständigen Dritten) entweder auf jedes, oder auf das konkret vorliegende (Buchführungs-)System.

Stoll[50] führte im BAO-Kommentar 1994, also an der Schwelle zur aufzeichnungstechnischen Neuzeit zum Erfordernis der Unabänderbarkeit und Sicherheit der Eintragungen (§ 131 Abs.1 Z4 und Z 6, Absatz 3) an: Abs.1 Z 6 verlangt die Verwendung solcher Schreibmittel, die sicherstellen, dass das Geschriebene nicht leicht entfernbar ist und zumindest solange leserlich bleibt, als die Aufbewahrungsfrist läuft. Werden zur Führung von Büchern und Aufzeichnungen Datenträger verwendet, muss sichergestellt sein, dass nachträgliche Veränderungen, ein Hinzufügen oder Löschen, erkennbar ist und bleibt. Diesem Gebot ist durch technische Einrichtungen entsprechend vorzusorgen, wie etwa durch ein Datenerfassungsprotokoll, durch Protokollierung jeder Änderung. Hierfür gäbe es bereits Softwareprodukte, die ein (leserliches) „Durchstreichen“ unter Leserlichbleiben des Vorangehenden ermöglichen und die auch gelöschte Eintragungen erfasst und erkenntlich belassen[51]. Weiter[52] – bei den an die modernen Organisationen, Techniken und Buchführungsformen zu stellenden Anforderungen handle es sich im wesentlichen nicht um neue Prinzipien aufgrund neuer Erkenntnisse, sondern um das Ergebnis einer Fortführung und um eine neue Systematik in der alten (gemeint herkömmlich und bewährten) Betrachtungswiese. Schließlich[53] – Die Anforderungen an die Ordnungsmäßigkeit der Buchführung ändern sich nicht dadurch dass die Buchhaltung (Anm. gilt wohl sinngemäß auch für die Erstellung der Grundaufzeichnungen) mit Hilfe moderner Techniken erstellt wird. Mit der Veränderung der Technik, die zur Durchführung der Buchhaltung eingesetzt wird, ändert sich lediglich die Realisierung der mit Hinblick auf die EDV-Besonderheiten spezifischen Anforderungen an die Ordnungsmäßigkeit im technischen, nicht aber im Grundsatzbereich. In ihrem Kern ändern sich die klassischen Ordnungsmäßigkeit Grundsätze somit nicht. Es sind lediglich bestimmte Aussagen der BAO in die neue Sprache der EDV-Welt“ zu übersetzen. Die alten Grundsätze sind gültig und weiterhin anzuwenden. Sie sind den neuen Herausforderungen gewachsen, erwiesen sich als flexibel, akkomodabel und transportabel.
Aus dieser Sicht kann wohl abgeleitet werden, dass die Einhaltung der „alten“ Grundsätze, wenn sie den neuen Herausforderungen tatsächlich gewachsen sein sollen, auch durch einen sachverständigen Dritten im wahren Sinn dieses Wortes (z.B. einem für den BP-Dienst ausgebildeten Bedienstete der Finanzverwaltung) möglich sein muss.

In Ansehung der latenten Zustände bei RegK und Kassensystemen ist streng genommen und gemessen an der Verantwortlichkeit der Bestimmung für die Gleichmäßigkeit, Rechtmäßigkeit der Besteuerung und auch die

---

[48] Siehe die Ausführungen *Stolls* zu § 163 BAO (korrespondierend zu § 158 AO) in BAO, 1736. Da die Wirtschaftsabläufe der Vergangenheit angehören, die buchmäßig festgehaltenen Vorgänge an Hand der gegebenen Aufzeichnungen aber in der Gegenwart zu beurteilen sind, kann - solange **andere Sicherheiten** *(Anm. - zB INSIKA)* für die Gewinnung der Gewissheit der Übereinstimmens der Aufzeichnungen mit den tatsächlichen Ereignissen nicht bestehen - mit Wahrheitsanspruch niemals die Aussage gemacht werden, die Buchhaltung sei vollständig und habe umfassend, lückenlos und sachrichtig die tatsächlichen Gegebenheiten, Vorgänge, Veränderungen und Verhältnisse festgehalten. Das Gesetz behilft sich daher mit Vermutungen. Da ein vergangenes Ereignis, die der Vergangenheit angehörige Wirklichkeit, der Erfahrung der Gegenwart nicht mit **gebotener Gewissheit** *(Anm. - zB INSIKA)* zugänglich ist, gibt das Gesetz der Vollziehung eine Vermutungsregelung zur Hand, nach der aus dem äußeren Anschein der formellen Richtigkeit der zeitnahe geführten Bücher und Aufzeichnungen auf deren materielle Ordnungsmäßigkeit zu schließen ist. Es besteht die Vermutung der Kongruenz des durch die Geschäftsaufzeichnung hergestellten förmlichen abstrakten Bildes mit dem real Gegebenen des konkreten Geschehens. § 163 BAO kann als Brücke zwischen dem mit absoluter Sicherheit niemals als wahr erkennbarem Vergangenem und der Feststellung des Sachverhaltes als Grundlage der Abgabenerhebung in der Gegenwart betrachtet werden.
[49] *Drüen* in Tipke / Kruse zu § 145, Tz 20, 21
[50] *Stoll*, BAO 1468
[51] Siehe auch Hinweise bei *Kurz*, SWK 1990, C41. Anm: wenn aber Software eingesetzt wird, welche diese Eigenschaften der Ordnungsmäßigkeitsgewähr nicht hat, ist die vollkommene Spurlosigkeit von Veränderungen möglich, jedoch keine Vermutung der Ordnungsmäßigkeit.
[52] *Stoll*, BAO 1469
[53] *Stoll*, BAO 1469, mit Hinweis auf *Kurz*, SWK 1990, C41

Sicherung des vollen Steueraufkommens sowie an den inneren historischen Zusammenhängen der Sinnausrichtung dieses Vertrauensvorschusses dessen **Aufrechterhaltung im Kassenbereich äußerst bedenklich**.
Die Aufdeckung der gängigen Kassenmanipulationen unter der bestehenden Gesetzeslage zur Aufzeichnung (damit aber auch die Ermittlung der Erfüllung der Ordnungsmäßigkeitsbestimmungen) ist, wenn überhaupt, durch nachträgliche Revision – also nicht durch Verfolgung im Rahmen einer Fahndungsmaßnahme, durch welche üblicherweise wesentlich mehr Information und aussagekräftiges Material – eventuell sogar Originaldaten vor Manipulation - erlangt werden - wenigen elitären Experten vorbehalten, welche auf Basis ihrer forensischen Spezialerfahrung mit Steuerbetrug und Datenmanipulation auf tiefsten Systemebenen eventuell vereinzelt verstümmelte Reste von oder Hinweise auf Manipulationen finden – aber in der überwiegenden Mehrzahl der Fälle keine verifizierbaren Größenordnungen, also gemäß dem Grundsatz der quantitativen Entdeckungswahrscheinlichkeit die wahren Besteuerungsgrößen. Kein Wirtschaftsprüfer, Buchhalter oder ausgebildeter „Durchschnittsbetriebsprüfer" kommt von seinen im Rahmen der Berufsausbildung vermittelten und angelernten Fähigkeiten und Erfahrungen je kompetenzhalber auf diese Ermittlungsebene hinab und kann daher auch nie mit Gewissheit, ja nicht einmal qualifizierter Wahrscheinlichkeit behaupten, dass Buchungen nicht spurlos veränderbar sind, ja nicht einmal feststellen, ob Veränderungen stattgefunden haben oder nicht, schon gar nicht in welcher Höhe. Andererseits wäre es in Anbetracht des Vertrauensvorschusses als Basis eines praktikablen Verwaltungsverfahrens, das Grundsätzen wie Zweckmäßigkeit, Verwaltungseffizienz oder Verwaltungsökonomie entsprechen soll, auch gar nicht ziel führend oder sinnvoll, jeden Betriebsprüfer in Informatik höchst aufwendig zum EDV-Superexperten auszubilden, der jegliche Form von oder jeden Hinweis auf Manipulation erkennen könnte, um ihn in einen den neuen Anforderungen des Betrugsfortschritts angemessenen „sachverständigen Dritten" zu verwandeln, wenn es einzig am StPfl liegt, ordnungsmäßig aufzuzeichnen.
Überlegt man die Auswirkungen dieses Zustandes in Richtung Rechtmäßigkeit der Besteuerung, so wäre zu hinterfragen, ob nicht einerseits der Vertrauensvorschuss hier auf Unrecht und nicht einschätzbaren „Ordnungsmäßigkeitsverhältnissen" aufsetzt, sondern ob nicht eher vielmehr ein allgemeiner und durchgehender „Misstrauensvorschuss" angebracht wäre, also die Umkehr der Beweislast bei Nutzung von ungesicherten Kassen oder hinsichtlich ihrer Wahrheitsbeweiskraft geradezu nebelhaft funktionellen Softwareprodukten zur Aufzeichnung. In diesem Fall könnte der StPl nur unter Nachweis von hochkomplexen, unangreifbaren, gesicherten, qualitativ und quantitativ exakt festhaltenden Aufzeichnungseinrichtungen[54] die Vollständigkeit und Richtigkeit seiner Primäraufzeichnungen und -daten nachweisen und dann in den Genuss des Vertrauensschutzes gelangen. Einzig die laufende, technisch perfekte Aufzeichnung und Protokollierung durch einen nach dem heutigen Sicherheitsstandard kaum angreifbaren Algorithmus und seine technische Umsetzung könnte die formellen und inhaltlichen Grundlagen für den Vertrauensvorschuss gewährleisten. **Eine solche ist in INSIKA unmittelbar gegeben**.

In einfacheren Worten: **Nur ein perfekter Fiskalspeicher ist ein guter Fiskalspeicher**.
Ein „nicht perfekter" Fiskalspeicher ist wesentlich schlechter als gar kein Fiskalspeicher, weil durch das zu Unrecht in ihn gesetzte Vertrauen (samt der Rechtsvermutung der Ordnungsmäßigkeit) in tiefgehender Weise und unvorhersehbarem Ausmaß das abgabenrechtliche Gleichheitsgebot verletzt wird.

5.5 INSIKA-Bestandteile als Vorbild für Inhalt der ö Kassenrichtlinie

Im Zuge der Erstellung der ö KRL stellte das INSIKA-Konzept – obwohl von Anfang an nicht die Einrichtung von Fiskalspeichern beabsichtigt war – mit vielen seiner Teilansätze die wichtigste Denkgrundlage dar. Die inhaltlich technisch bedeutendsten Teilansätze wurden nicht verwendet (Smartcard, Verkryptungsverfahren, Kennzeichnung auf Beleg), da mangels gesetzlicher Grundlagen wie o.a. keine Fiskalspeicherlösung angestrebt wurde.

Von den restlichen Konzeptsegmenten aber wurden viele mit einbezogen

- Notwendige Belegerteilung und Inhalte des Beleges
- Ereignisprotokollierung (Fiskaljournal / DEP) und dessen Inhalte
- Nummerierung von Geschäftsvorfällen
- Sequenznummerierung bei Buchungen
- Einrichtung eines technischer Manipulationsschutzes und dessen Beschreibung in der Verfahrensdokumentation (Einrichtung nach § 131 BAO zur vollständigen und richtigen Erfassung und Wiedergabe der GVF – auch „E131")
- Unangemeldete Kassennachschau

Zusätzlich wurden zur Klarstellung und zur Vollzugsoptimierung Themenbereiche mit eingebunden, welche bis dahin noch nicht oder nicht im nötigen Ausmaß definiert oder auf breiter Ebene publik waren

- Bedeutung der Verfahrensdokumentation und ihrer Inhalte
- Technische und aufzeichnungstechnische Klassifizierung der Kassen und Systeme
- Voraussetzungen für Ordnungsmäßigkeit nach Kassentypen

[54] Siehe *Seer* FN 46

Die Überlegungen in Ö gingen aber auch in Richtung eines umfassenden Vollzugs. Hier gab es von Anfang an wage Bedenken zur Umsetzbarkeit für eine sichere Vollziehung von weit reichenden neuen technischen Notwendigkeiten unter sehr begrenzten Verwaltungsressourcen und auch Befürchtungen der Kassenhersteller und- programmierer um ihre wirtschaftliche Existenz durch weiterhin manipulierende Kassen auf dem Markt durch Konkurrenzfirmen. Durch die künftige Kassenachschau der FinPol konnten diese Bedenken zerstreut werden.

5.6 Bestimmungen der ö Kassenrichtlinie

5.6.1 Eckpunkte der Kassenrichtlinie

inhaltliche Eckpunkte

- Feststellung der gesetzlichen Grundlagen für Ordnungsmäßigkeit
- Spezifizierung der Arten von Kassen und Systemen, Definitionen, Begriffsklärungen
- Beschreibung der durch Kassen erzeugten Grundaufzeichnungen und Daten
- rechtliche und technische Anforderungen an Systeme und Dokumentationen abgestimmt nach eingesetzten Kassenarten

technische Eckpunkte

- Verfahrensdokumentation
- „Einrichtung 131“
  - Zusätzlich deren Beschreibung durch Hersteller
- freiwillige Maßnahmen zur Erhöhung der Ordnungsmäßigkeit
  - v.a. Belegerteilung, Nummerierung
- fortlaufende und kontrollfähige Dokumentation der Erfassung

Nachfolgend wird die Kassenrichtlinie inhaltlich besprochen, wobei die auf die Einleitung (Intentionen), die Anführung der gesetzlichen Grundlagen und die Folgen der Nichtbeachtung der Ordnungsmäßigkeitskriterien hier nicht mehr näher eingegangen wird, da diese Punkte bereits in der obigen Darstellung enthalten sind. Aus Platzgründen wurde eine punktuelle Darstellung gewählt.

freiwillige Maßnahmen zur Erhöhung der Vermutung der Ordnungsmäßigkeit

- nachvollziehbare Dokumentation über die gesetzlichen Aufzeichnungspflichten hinaus
- freiwillige Belegerteilung bei allen GVF
- Ausfolgung der Belege an jeden Kunden
- die einzelnen Kassenbelege sind den einzelnen aufgezeichneten GVF aufgrund eindeutiger Merkmale konkret zuordenbar und dies ist leicht und sicher nachprüfbar
- Vergabe fortlaufender Rechnungsnummern
- Offenlegung der entsprechenden Dokumentationsgrundlagen der GVF

Schaffung zusätzlicher Kontrollmöglichkeiten

- Vergleichsoption der Rechnungsnummern der Kassenbelege mit den im System gespeicherten Rechnungsnummern
- Mindestinhalte von Kassenbelegen
- Nummerierung aller einzelnen erfassten GVF mit fortlaufender Nummer, welche grundsätzlich nur einmal je Abrechnungszeitraum auf 0 zurückgestellt werden soll

5.6.2 Dokumentationsgrundlagen und Definitionen

Dokumentationsgrundlagen

Die Dokumentation erfolgt durch Ausdrucke und Daten. Mindestangaben sollen zum Zweck der Prüfbarkeit enthalten sein. Alle üblicherweise als Ausdrucke erzeugten Unterlagen sollen als Ausdrucke im Original vorgelegt werden. Die angeführten Unterlagen (Journal, DEP) sind über Verlangen jederzeit vor Ort in Datenform vorzulegen (§§ 131, 132 BAO jeweils letzter Satz)

Kassentypen und Dokumentation

Typ 1 - mechanische RegK

- Journalstreifen

Typ 2 - einfache, konventionelle elektronische RegK

- elektronisches Journal
- Tagesendsummenbons (Z-Bons)
- GT-Speicherstände

Typ 3 - Kassensysteme bzw. PC-Kassen

- DEP
- Tagesabschlüsse (jedenfalls einschließlich Warengruppenbericht und Bedienerbericht und Finanzartenbericht)

Die Bestimmungen sind auch für sonstige Einrichtungen, die zur Aufzeichnung von Betriebseinnahmen genutzt werden und damit RegK-Funktion haben, maßgeblich und analog anzuwenden. Sonstige Einrichtungen sind je nach ihrem technischen Aufbau bzw ihrer Funktionalität den vorigen 3 Gruppen zuzurechnen (zB Taxameter, Kassenwaagen, Branchensoftware, Fakturierungsprogramme)

Ausdrucke

Tagesendsummenbons (Z-Bons) bei Typ 2-Kassen
Speicherabfrage der Tageserlöse, wobei nach der Abfrage der Speicher gelöscht (zurückgesetzt) wird bzw. die aufsummierten Tageserlöse auf 0 zurückgesetzt werden

Inhalte des Z-Bons als Dokumentationsgrundlage der Tageseinnahmen
Die äußere Gestaltung des Z-Bons liegt grundsätzlich beim StPfl

- Name des Unternehmers oder Firmenkennung
- Datum und die Uhrzeit der Erstellung
- Anzahl der Speichernullstellungen (so genannte „Z-Bon-Nummer“)
- Anzahl der insgesamt verkauften Artikel, Produkte oder der Teilleistungen, die an die Kunden ausgefolgt / verabreicht wurden
- Gesamtanzahl der Kundenabrechnungen
- Gesamttagesumsatz, Umsätze nach Steuersätzen
- nicht im Tagesumsatz enthaltene Übungsumsätze (Trainingsumsätze)
- Aufteilung der Erlöse auf die Finanzarten
- Zahlungsarten, unbare Umsätze, wie Kreditkarten-, Bankomatumsätze
- Aufteilung der Erlöse auf die Kassierer / Bediener einschließlich Bekanntgabe der nicht im Tagesumsatz enthaltenen Übungsumsätze (Trainingsumsätze)
- Minderungen des Tagesumsatzes
- durchgeführte Nach-Stornobuchungen
- Preisnachlässe, Retouren, Minusumsätze
- Nullumsätze (Bezug von Gratisware)
- gesonderter Ausweis von Gutschein- bzw. Bonverkauf

zusätzlich bei Kassen mit Bargeldlade

- rechnerischer Bargeldbestand / Kredit / andere geldwerte Bestände in Schublade
- Anzahl der Nur-Schubladenöffnungen
- Barentnahmen und Bareinlagen

GT-Speicherstände bei Typ 2-Kassen (Numerator)
Abfrage des Gesamtsummenspeichers (Numerators), welcher bei Tagesabschluss die seit der Inbetriebnahme bzw. der letzten Rücksetzung erzielten Erlöse in einer Summe anzeigt. Wenn mehrere Umsatzsummenspeicherstände geführt werden, sollen alle im Ausdruck ausgewiesen werden. Eine Rückstellung des Numerators (Gesamtsummenspeichers) soll (wenn überhaupt) nur einmal je Abrechnungszeitraum erfolgen. Die Form der Dokumentation der Stände der (des) Umsatzsummenspeicher(s) liegt grundsätzlich beim StPfl.

Journalstreifen aus mechanischen RegK
Kontrollpapierstreifen, in welchem bei einer Kasse ohne Datenträger jeweils mit Rechnungserstellung fortlaufend die GVF dokumentiert werden. In der Kontrollaufzeichnung soll die fortlaufende Nummer des GVF und das Datum mitprotokolliert werden

Daten

elektronisches Journal bei Typ 2-Registrierkassen
Protokolldatei, welche im Speicher einer el. RegK (Typ 2) mit läuft und in Echtzeit mit Rechnungserstellung fortlaufend und chronologisch die GVF bzw. Transaktionen dokumentiert. Das mitlaufende el. Journal entspricht inhaltlich dem Kassenstreifen einer mechanischen RegK. Bei Speicherbegrenzung der RegK (Typ 2) sollen die Daten rechtzeitig (vor Löschung und Überschreiben des Speichers) exportiert werden, um sie in entsprechender Form unverändert zur Verfügung stellen zu können (§ 131 Abs.3 BAO)

Mitprotokolliert werden sollen

- Rechnungsnummer des GVF
- Datum und genaue Uhrzeit des GVF
- betragliche Grundlagen des GVF (Produkte, Teilleistungen)
- Gesamtbetrag des GVF

DEP bei Typ 3-RegK

Ereignisprotokolldatei mit Protokollierung der erfassten Buchungsvorgänge

- läuft im Speicher von Kassen des Typs 3 mit
- dokumentiert jeweils fortlaufend chronologisch die GVF und deren Grundlagen (z.B. Einzelleistungen, verkaufte Produkte)

Wenn im DEP gleichzeitig mit Dokumentation der GVF auch andere Ereignisse mitprotokolliert werden, soll durch entsprechende Formatierung das Einlesen mittels Prüfsoftware und damit die Prüfbarkeit sichergestellt werden.

Das DEP protokolliert

- Geschäftsvorfall und dessen Gesamtbetrag
- dessen betragliche Grundlagen bzw. Einzelleistungen oder Einzelprodukte
- sonstige aufzeichnungspflichtige Vorgänge

Die Sicherstellung der jederzeitigen Möglichkeit der Prüfung der Vollständigkeit und Richtigkeit der chronologisch geordneten, vollständigen, richtigen und zeitgerechten Erfassung ist jedenfalls gegeben durch

- Datum, Uhrzeit und fortlaufende Nummerierung der einzelnen Buchungen

Die Überprüfungsmöglichkeit soll auch bei aktuellen Maßnahmen der Steueraufsicht gegeben sein.

Nötige Gewährleistung

- der Überprüfbarkeit der Unveränderbarkeit der Daten bei Datenübertragung bei verbundenen Systemen
- der inhaltlichen Konsistenz der Datenübertragung
- der eindeutigen Identifizierbarkeit der einzelnen Datenerfassungsgeräte (Kassen, Eingabestationen)

Berichte

Alle im Zuge des Tagesabschlusses oder zu sonstigen Zeitpunkten erzeugten Berichte und Abfragen von abgabenrechtlicher Bedeutung z.B. Bedienerberichte, Hauptgruppenberichte, Warengruppenberichte, Periodenberichte, Stundenberichte, Tischberichte, Berichte von Teilbetriebsbereichen – z.B. Bar, Gastgarten, Artikelberichte, Finanzarten-Berichte.

Geschäftsvorfälle (GVF)

Der Weg der GVF in den Büchern und Aufzeichnungen soll verfolgbar und progressiv und retrograd nachvollziehbar überprüfbar sein

- ausgehend von der Ersterfassung und Aufzeichnung
- über die Summen der erfassten Beträge im Rahmen der Losungsermittlung im Kassensystem
- durch entsprechende Buchung auf den Konten
- bis zur Bilanz/GuV bzw. Erfassung in den Aufzeichnungen

Im Regelfall handelt es sich bei GVF im Sinn der KRL um Ereignisse im Geschäftsbetrieb, die mit der Ersterfassung der Auftragsposition beginnen (z.B. Bestellungseingabe im Kassensystem, Artikelscan an der Kassa, Einschalten des Taxameters) in deren Rahmen üblicherweise ein geldwerter Leistungsaustausch zwischen StPfl und Kunden stattfindet

Auch Aufzeichnungen über Ereignisse, die letztendlich keinen GVF bewirken, der zu erfassen wäre, sollen - insoweit diese Vorgänge erfasst wurden – aufbewahrt werden, wie zB

- nicht abgeschlossene / stornierte GFV
- mit einem GFV zusammen hängende bzw. vorbereitende Vorgänge, z.B. nicht abgeschlossene oder zustande gekommene GFV – Preisabfragen, erstellte Angebote, Reservierungen
- rückgängig machende Vorgänge, z.B. nachträgliche Stornos, Rücklieferungen
- sonstige Vorgänge im Geschäftsprozess, soweit diese aus Gründen der Überprüfung der vollständigen und richtigen Erfassung aller GFV oder aus sonstigen für die Abgabenerhebung bedeutsamen Gründen aufzeichnungs- bzw. aufbewahrungspflichtig sind

Bedingt aufbewahrungspflichtige Nicht-Geschäftsvorfälle

In der Aufzeichnung erfasste - nicht aufzeichnungspflichtige - Elemente sollen erhalten bleiben, wenn ihre Löschung die Überprüfung der Vollständigkeit der erfassten aufzeichnungspflichtigen Elemente verhindern würde.

sonstige aufzeichnungspflichtige Vorgänge
sind Vorgänge im Geschäftsprozess, die zwar grundsätzlich nicht dazu geeignet sind, einen GVF anzustoßen oder zu bewirken, aber aus den o.a. Gründen der Überprüfbarkeit der vollständigen und richtigen Erfassung aller GVF aufzeichnungs- und aufbewahrungspflichtig sind. Dies sind insbesondere Vorgänge, die es im Kassensystem, in sonstigen Aufzeichnungssystemen oder in damit verbundenen vor- und nach gelagerten Systemen ermöglichen, einzelne GVF nicht nachvollziehbar außerhalb der Losungsermittlung zu erfassen bzw. als Simulation darzustellen (z.B. Übungsbuchungen, Simulationen)

Kassenbeleg - Mindestinhalte (siehe Beleg rechts)

- Bezeichnung Betrieb
- Merkmal zur Kassenidentifizierung
- Datum, Uhrzeit
- Belegnummer
- Einzelprodukte, Preise
- Gesamtsumme


Tabakfachgeschäft
Hauptstraße
Tel.:
RECHNUNG
01.02.2012 09:40:33 BonNr. 65264
Kassa: 1 Kassier Nr: 1
1 x DIE GANZE WOCHE 10 1,10 1,10
10 x PARKSCHEIN 0.5 0 0,60 6,00
6 x PARKSCHEIN 1.0 0 1,20 7,20
Gesamtsumme € 14,30
17 STK
Excl.Mwst Mwst-Betrag
Mwst 0 % 13,20
Mwst 10 % 1,00 0,10
Mwst 20 % 0,00 0,00
Parkscheinverkauf erfolgt für
MA4-DEZ. II - REF.5 - SD 2010(P)
WIR DANKEN FÜR IHREN EINKAUF!
UID: ATU

5.6.3 Weitere Unterlagen, die für die Abgabenerhebung von Bedeutung sind

Verfahrensdokumentation
Die VD ist Grundlage der Prüfbarkeit der Kasse und der von ihr erzeugten Dokumentationsgrundlagen (z.B. Handbuch, Bedienungsanleitung)

Programmabrufe
Änderungen der Systemparameter, Druckeinstellungen, Stammdatenänderungen, die für Verständnis der Aufzeichnungen und deren Grundlagen erforderlich sind, sollen entsprechend dokumentiert werden, wenn Änderungen nicht ohnehin aus sonstigen Unterlagen ersichtlich sind (zB DEP)

Korrekturbuchungen - Ausdrucke (Typ2-Kassen)
Einzelbons der Korrekturbuchungen abgeschlossener Bonierungen sollen aufbewahrt werden (z.B. für Managerstornos, Nach- und Stornobuchungen, Warenrücknahmen, Retouren).

Berichte
Alle erzeugten Berichte und Abfragen, die von abgabenrechtlicher Bedeutung sind, sollen aufbewahrt werden.

Mehrere Kassen
Dokumentationsgrundlagen, Kassenidentifikation, Kasseneinsatzprotokoll bei mehreren zeitlich / örtlich im Abrechnungszeitraum eingesetzten Kassen. Entsprechende Aufzeichnungen (Protokolle) zur Identifikation der eingesetzten Kassen sollen über deren Einsatzorte und –zeiträume geführt und aufbewahrt werden. Führung und Aufbewahrung der Dokumentationsgrundlagen der Tageseinnahmen für jede einzelne RegK getrennt. Möglichkeit der Identifikation der jeweiligen Kasse und Zuordnung ihrer Dokumentationsgrundlagen durch entsprechende Bezeichnung oder Nummerierung der Kassen.

5.6.4 Sonstiges

Kassenwaagen sind RegK gleichzuhalten.,Ihre Dokumentationsgrundlagen richten sich nach der jeweiligen technischen Vergleichbarkeit mit den Kassentypen

Taxameter dienen - auf Basis von Taxitarifen - der Berechnung von Fahrpreisen in Taxis. Wenn sie zur Losungsermittlung bzw. zur Erstellung von Kassenbelegen eingesetzt werden, richten sich ihre Dokumentationsgrundlagen nach der jeweiligen technischen Vergleichbarkeit mit den Kassentypen Grundlagenaufzeichnungen zur Überprüfung der Bareinnahmen sind für jedes Taxi getrennt zu führen

Für **sonstige Einrichtungen** gelten ebenfalls die angeführten rechtlichen Kriterien der Ordnungsmäßigkeit und die dabei erstellten Grundaufzeichnungen sind entsprechend aufzubewahren wie zB Fakturierungsprogramme, branchenspezifischen Softwareprogramme, die der Rechnungserstellung dienen / mit der Losungsermittlung verknüpft sind und damit verbundene Geschäftsprozesse darstellen, wie z.B. Bestellwesen, Reservierungen. Soweit diese Einrichtungen mit den jeweiligen Kassentypen vergleichbar sind, sind die technischen Bestimmungen analog anzuwenden.

Datensicherung
Ist ausstattungsbedingt die Gesamtspeicherung aller abgabenrechtlich relevanten Daten innerhalb einer RegK nicht möglich (nicht ausreichender Speicherplatz), soll eine unveränderbare Speicherung auf einem externen Datenträger erfolgen (z.B. Journal-, Auswertungs-, Programmier- und Stammdatenänderungsdaten) Die archivierten Daten sollen die gleichen Auswertungen wie jene im laufenden Kassensystem ermöglichen. Zur Kontrollfähigkeit im Rahmen der Steueraufsicht durch die FinPol soll die elektronische Dokumentation jedenfalls die nötigen Einzelmerkmale beinhalten, dass unmittelbar und in angemessener Zeit feststellbar ist, ob alle GVF in vollem Umfang erfasst wurden (elektronisches Journal bei RegK-Typ 2 und DEP bei RegK-Typ 3)

5.6.5 Anwendung
Die der KRL zugrunde liegenden Rechtsvorschriften sind keine Neuerungen, sondern wurden - aufgrund der fortschreitenden, laufenden technischen Entwicklung - nur näher präzisiert. Sind zusätzliche Maßnahmen zur Sicherstellung der vollständigen und richtigen Erfassung notwendig, sollen diese sobald als möglich - in zumutbarer Zeit - jedenfalls bis Ende 2012 - geschaffen werden. Dies gilt ebenfalls für die nähere Beschreibung der „E131“. Kassensysteme, welche funktionell die Ordnungsmäßigkeitskriterien nicht erfüllt haben, werden durch allfällige Übergangsregelungen nicht berührt und sind hinsichtlich der Vorzeiträume wie bisher zu beurteilen

5.7 Kassennachschau (KN) durch die FinPol

5.7.1 Inhalte
Die folgende Kurzdarstellung der Maßnahmen der FinPol soll insbesondere für den Aufzeichnungsbereich deren Inhalte darstellen. Die jederzeit möglichen Erhebungen der FinPol dienen der Sicherstellung der vollständigen Besteuerungsgrundlagen. Die Organe der FinPol sind bei Kontrolle der Losungsermittlung berechtigt, im Rahmen ihrer Möglichkeiten im Bereich der Kontrolle KN durchzuführen. Dabei ist Betracht zu nehmen auf wahre Verhältnisse bei Ermittlungen vor Ort in flächendeckendem Umfang in der Gegenwart durch Organe, die unangemeldet Wahrnehmungen treffen können.

Definition der KN
Die KN dient der Erhebung der gegenwärtigen wahren Verhältnisse bei Ermittlung der täglichen Einnahmen, bei Grundaufzeichnungen über die Ermittlung der täglichen Einnahmen, im Zusammenhang mit dem Aufzeichnungssystem bzw bei der Bargeldgebarung.

Rechtsgrundlagen der KN
Die KN gründet sich auf § 144 BAO. Ergänzend sind auch Aufsichtsmaßnahmen nach § 143 BAO möglich. Als weitere sachlich-rechtliche Grundlagen für die Inhalte der Kassennachschau sind vor allem die Regelungen über Bücher und Aufzeichnungen – insbesondere die Dokumentationsverpflichtung, welche sich aus §§ 131 und 132 BAO ergibt – maßgeblich.

Allgemeine Inhalte der KN sind
- wahres Aufzeichnungssystem
- wahre Grundaufzeichnungen
- Art und Form der wahren Grundaufzeichnungen (fortlaufend, vollständig, rechtzeitig, der Zeitfolge nach geordnet, gesichert, unveränderbar, in wahrer und klarer Form, prüfbar)
- ordnungsmäßige und zeitgerechte Führung der Bargeldgebarung

Praktische Einzelerkundungen im Rahmen der KN
Folgende Unterlagen werden vom Unternehmer eingefordert
- Tagesabschluss des vorigen Öffnungstages
- Bargeldgebarungsabschluss des vorigen Öffnungstages
- Alle Unterlagen für eine KN können auch für die vor dem letzten Öffnungstag gelegenen Tage zur Einsicht verlangt werden

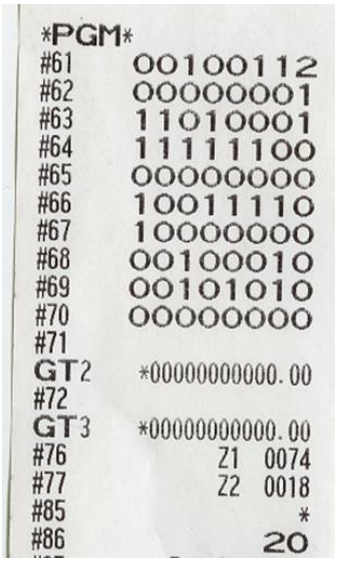
Bei RegK oder Kassensystemen werden verlangt
- Berichte über den vorigen Öffnungstag
- Tagesabschluss oder Z-Bon
- Bedienerberichte
- GT-Speicherstände

Daneben erfolgt ein Einblick in laufend zu führende elektronische und maschinelle Kontrollaufzeichnungen über Vollständigkeit (DEP, Elektronisches Journal, Papier-Journalstreifen). Bei mehreren Kassen/Eingabeterminals wird festgestellt, wie viele Kassen im Betrieb geführt werden (ev. auch durch verdeckte Ermittlung). Bei Betrieben, welche die vereinfachte Losungsermittlung (Kassensturz) in Anspruch nehmen sind kann die Vorlage aller

vorhandenen Kassen, Geldbehältnisse, betrieblichen Brieftaschen verlangt werden und ein Kassensturz durchgeführt werden (Festhaltung des gemeinsam festgestellten Kasseninhaltes durch Niederschrift). Im Rahmen des praktischen Kassenchecks wird ein Gespräch mit dem StPfl geführt, um festzustellen, ob er bereit ist, Bons oder Berichte abzufragen. wenn dies nicht der Fall ist werden die Gründe und Hindernisse in einer Niederschrift aufgenommen. Die Vorlage von Handbuch, Verfahrensdokumentation, Bedienungsanleitung der Kasse, sowie der Z-Bons, Berichte usw. wird gleichfalls in der Niederschrift protokolliert. Bei Bereitschaft zum aktiven Kassencheck ergeht das Ersuchen an StPfl, vorzuführen, wie er am Ende des Tages den Tagesabschluss vornimmt (Ausdruck von Berichten, z.B. Tagesabschlüsse, Z-Bons, X-Bons, Bedienerberichte, Feststellung der laufenden Rechnungsnummer zu einem bestimmten Zeitpunkt)

KN mit Datenzugriff
Eine solche wird in jenen Fällen durchgeführt, in welchen die Dokumentation der Vollständigkeit auf Datenträgern geführt wird (elektronische Registrierkassen mit elektronischem Journal, DEP aus proprietären Kassensystemen und PC-Kassen). Dabei fordert das Erhebungsorgan den Kassenbetreiber auf, die fortlaufende Dokumentation auf einen Datenträger zu überspielen, dessen Inhalt in der Folge die Grundlage für die Kontrolle der fortlaufenden Führung von Aufzeichnungen ist.

Einzelpunkte der KN (demonstrativ)
- Allgemeines über Betrieb, Aufzeichnung, Öffnungszeiten,
- Werden Einzelaufzeichnungen geführt / Form der Einzelaufzeichnungen über die Geschäftsfälle.
- betriebliche Besonderheiten bei der Losungsermittlung
- Kassenberichte
- Kasseneinsatzprotokoll bei mehreren Kassen
- Ermittlung der Anzahl von Kassen, bzw Eingabestationen
- Handbuch (Verfahrensdokumentation)
- Bezeichnung der Kasse , Lieferant der Kasse, Systembetreuer
- Rechnungen, Aufbewahrung der Durchschriften
- Person, die zuständig für den Tagesabschluss ist
- Vorlage des Tagesabschlusses bzw Berichte der letzten Tage
- Registrierkasse, Kassensystem - Datenerfassungsprotokoll / el. Journal - Datenübergabe im Rahmen der Kassennachschau
- Einsicht in Journalstreifen (bei mechanischen Registrierkassen)
- Durchführung eines Tagesabschlusses unter Aufsicht
- Abfrage der Druckeinstellungen (Systemscan)
- Kassensturz - Ermittlung des Bargeldbestandes gemeinsam mit dem Kassenbetreiber
- ordnungsmäßige Kassenführung / Abstimmung der Geldkasse (Bargeldgebarung)



Systemscan bei Typ 2-Kasse (siehe oben rechts)
Feststellung der derzeitigen Druckeinstellungen - Protokoll der Systemparameter. Bei Mitwirkungsbereitschaft wird der StPfl ersucht, ein Protokoll der Druckeinstellungen zu erzeugen zur Ermittlung der Einstellungen, die Einfluss auf Verhalten der RegK nehmen, zB
- fortlaufende Journal- / Rechnungsnummer wird täglich auf Null gestellt
- mögliche Unterdrückung von fortlaufender Z-Nummer, Training, Stornos, Angabe der Gesamtkundenanzahl, der verkauften Produkte

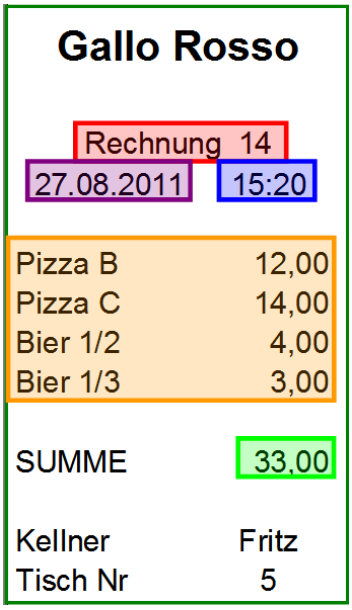
Über das Ergebnis der KN ist eine Niederschrift anzufertigen.

Die FinPol hat keine Rechte, in nicht offene Behältnisse Einsicht zu nehmen. Ihre Befugnisse beschränken sich im Prinzip auf diejenigen, welche eine reguläre Nachschau (§ 144 BAO) umfasst. Bei Verweigerung der Mitwirkung bzw der Offenlegung und Herausgabe von Unterlagen, Aufzeichnungen und Daten verhindert dieses Vorgehen eine Überprüfung der vollständigen und richtigen Aufzeichnung. Nach § 163 (2) BAO liegen Gründe, die nach dem Gesamtbild der Verhältnisse Anlass geben, die sachliche Richtigkeit in Zweifel zu ziehen, insbesondere dann vor, wenn die Bemessungsgrundlagen nicht ermittelt und berechnet werden können oder eine Überprüfung der Richtigkeit und Vollständigkeit wegen Verletzung der Mitwirkungspflicht nicht möglich ist. Wenn die sachliche Richtigkeit des Rechenwerks nicht gegeben ist, kann dies unmittelbar die Schätzung der Besteuerungsgrundlagen nach § 184(3) BAO nach sich ziehen.

5.7.2 Gegenkontrolle auf Vollständigkeit aus Rechnungen und Protokollierung

Rechts unten ist eine Rechnung abgebildet. Die eingerahmten und unterlegten Bereiche umfassen Elemente, welche im DEP (links unten) gleichfalls erfasst sein sollen. Mittels dieser Vergleichspunkte sowie der Sequenznummer sind umfassende Vollständigkeitskontrollen möglich.

Datum	Uhrzt	Seq Nr	Artikel / PLU	Preis PLU	Kellner	Tisch Nr	Rechnung	Rechnung Betrag	KK
27.08.2011	13:01	2389	Pizza A	10,00	Fritz	1			
27.08.2011	13:02	2390	Merlot 1/8	4,00	Fritz	1			
27.08.2011	13:24	2391	Schnitzel mil	13,00	Margit	3			
27.08.2011	13:24	2392	Salat kl	4,00	Margit	3			
27.08.2011	13:24	2393	Bier 1/2	4,00	Margit	3			
27.08.2011	13:44	2394	Kaffe kl	3,00	Margit	3			
27.08.2011	**14:08**	**2395**			**Fritz**	**1**	**3012**	**14,00**	**x**
27.08.2011	14:12	2396	Pizza B	12,00	Fritz	5			
27.08.2011	14:12	2397	Pizza C	14,00	Fritz	5			
27.08.2011	14:12	2398	Bier 1/2	4,00	Fritz	5			
27.08.2011	14:13	2399	Bier 1/3	3,00	Fritz	5			
27.08.2011	**15:00**	**2400**			**Margit**	**3**	**3013**	**24,00**	
27.08.2011	**15:20**	**2401**			**Fritz**	**5**	**3014**	**33,00**	**x**
27.08.2011	15:24	2402	Spaghetti Bolo	9,00	Paul	7			
27.08.2011	15:24	2403	Fanta	2,00	Paul	7			
27.08.2011	15:24	2404	Saltimbocca	15,00	Paul	7			
27.08.2011	15:25	2405	Merlot 1/2	16,00	Paul	7			
27.08.2011	16:22	2406	Fisch A	15,00	Margit	11			
27.08.2011	16:22	2407	Pinot blanc	4,00	Margit	11			
27.08.2011	16:22	2408	Pizza A	10,00	Margit	11			
27.08.2011	16:22	2409	Merlot 1/8	4,00	Margit	11			
27.08.2011	**16:49**	**2410**			**Paul**	**7**	**3015**	**42,00**	
27.08.2011	**17:55**	**2411**			**Margit**	**11**	**3016**	**33,00**	



5.7.3 Effekte der Kassennachschau

Die Auffindung und Dokumentation wahrer Verhältnisse im Aufzeichnungsbereich entscheidet uU über die Ordnungsmäßigkeit des gesamten Rechenwerkes. Einmal nachweislich festgestellte Mängel können nicht mehr saniert oder aufgeholt werden. Nicht erstellte oder formell nicht ordnungsmäßige Grundaufzeichnungen haben unmittelbare, in der Folge durch den Stpfl nicht mehr verhinderbare Konsequenzen. Die Auffindung von Originalaufzeichnungen, die uU nicht für das Rechenwerk gedacht waren, können die Gesamtbeurteilung der sachlichen Richtigkeit vollkommen verändern.

6. Ausblick

Im einem umfassenden Diskussions- und Werdungsprozess hat Ö Grundlagen für eine vollziehbare Kassenlösung geschaffen. Wie sehr diese und die neue Kassennachschau die Gleichmäßigkeit der Besteuerung gewährleisten können, kann nur die Zukunft zeigen. Dem Autor ist klar, dass sie in ihrer Wirksamkeit niemals dem INSIKA-Konzept auch nur nahe kommen können.

Zu INSIKA selbst und seiner Zukunft könnte hinterfragt werden, wie weit es sich die Allgemeinheit - bzw weiter gedacht Europa - „leisten“ kann, auf einen konzeptionell fertig entwickelten, effektiven, objektiv tatsächlich sicheren, kostengünstigen, verwaltungstechnisch machbaren Automatismus zu verzichten, der Steuerausfälle in Milliardenhöhe (auf Europa umgerechnet vermutlich in Billionenhöhe) auffangen könnte. Für einen Steuerbeamten, wie den Autor, ist es ohnehin berufsbedingt, aber auch aus der Sicht der Ethik im Umfeld der Steuererhebung unbegreiflich, weshalb genau an der Stelle und in dem staatlichen Wirkungsbereich, welcher für die Sicherung[55] der Einnahmen da ist, gespart wird. Nun, da die Staatshaushalte „brennen“ und die Bevölkerung der Staaten „zur Kasse gebeten“ wird, sollte – wenn jetzt nicht, wann dann - der Zeitpunkt da sein, die Steuern primär mal dort zu holen, wo sie monetär vorhanden sind, aber je nach Gutdünken des einzelnen nicht vollständig abgeführt werden, wo sie nur sicher einzubehalten[56] und einzuzahlen wären: beim Leistungsaustausch mit dem Endverbraucher im Barzustand.

Es wäre jetzt höchst an der Zeit, hier den großen Schritt zu tun[57], sonst bliebe es bei Tipke[58]: „Was ist das für ein Staat, in dem das Steuerzahlen den Ehrlichen[59], den Gesetzestreuen und den Dummen überlassen bleibt?“

---

[55] Siehe http://www.spiegel.de/wirtschaft/soziales/0,1518,687156,00.html Finanzbeamten-Mangel kostet Deutschland Milliarden Euro - Die deutschen Finanzämter sind unterbesetzt, vernachlässigt wird vor allem die Prüfung von Betrieben. Tausende Stellen in der Finanzverwaltung sind unbesetzt. Dadurch entgehen dem Staat laut Gewerkschaftsangaben 30 Milliarden Euro pro Jahr.

[56] Siehe auch Wähnert, Digitale Manipulation – Bedrohung für das Steueraufkommen, stBP 2010, S 56

[57] *J. Isensee* in: Festschrift für *W. Flume*, Bd II, 1978, S. 132 f. Der Steuergehorsam des Einzelnen lebt nur aus der Einsicht, dass die Abgabenpflicht allen Mitbürgern nach gleichen Kriterien auferlegt ist.

[58] *Tipke*, Steuerrechtsordnung, Bd. III, S. 1223

[59] Siehe *Tipke* Das Dilemma der Steuerverwaltung – zeitnahe oder gesetzmäßige Besteuerung, StWa 1994,StWa 1994, S. 223. Je mehr in einer Gesellschaft der individuelle Egoismus die Hauptantriebskraft ist, der materielle Erfolg der höchste Wert ist, das Prinzip „Bereichert Euch mit allen Mitteln“ weithin vorherrscht, das Auspokern von Interessen und Bedürfnissen die Regel ist, wird in dem sich ausbreitenden moralischen Vakuum auch die Steuermoral beträchtlich in Mitleidenschaft gezogen. Die Steuermoral ist Teil der allgemeinen Moral.