# 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.

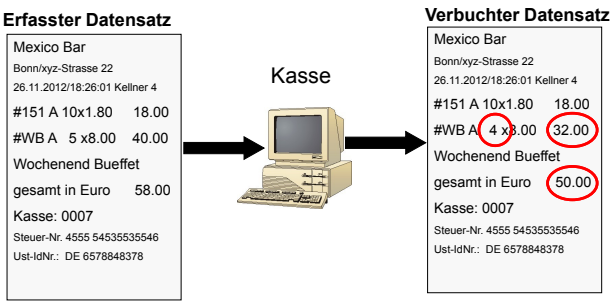


Abbildung 1: Veränderung von Datenbeständen in Registrierkassen

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.

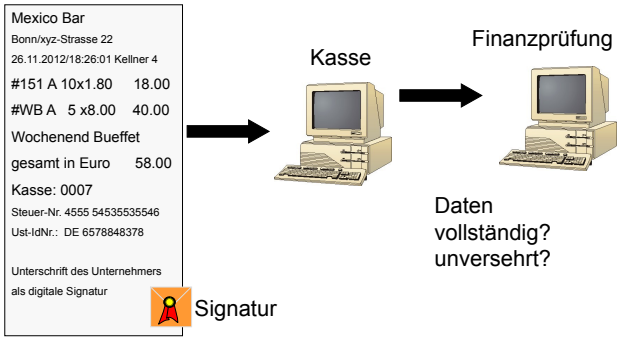


Abbildung 2: Grundsätzliches Lösungskonzept

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

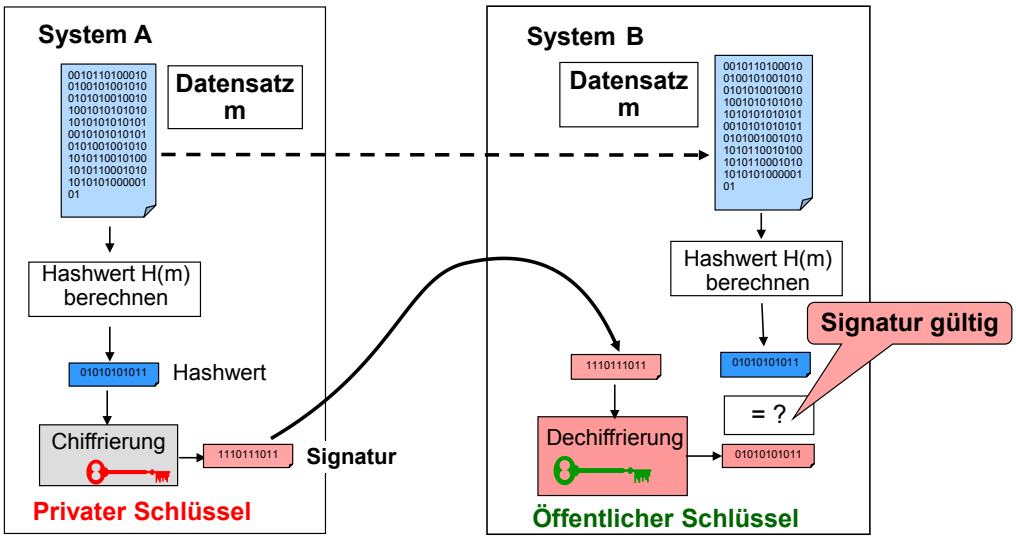


Abbildung 3: Digitale Signatur von Daten

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.

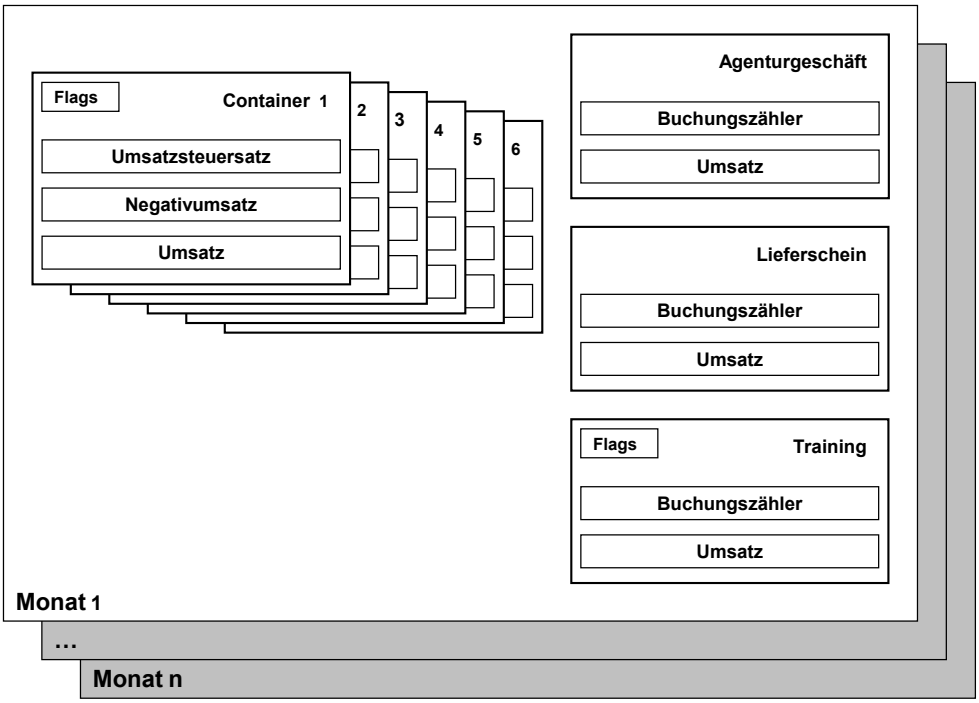


Abbildung 4: TIM-Speichermodell

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, kartenineterne 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.

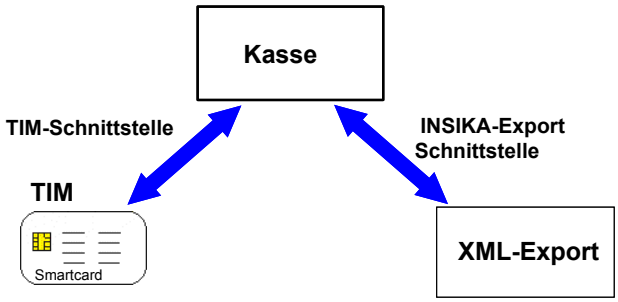


Abbildung 5: INSIKA-Schnittstellen

## 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

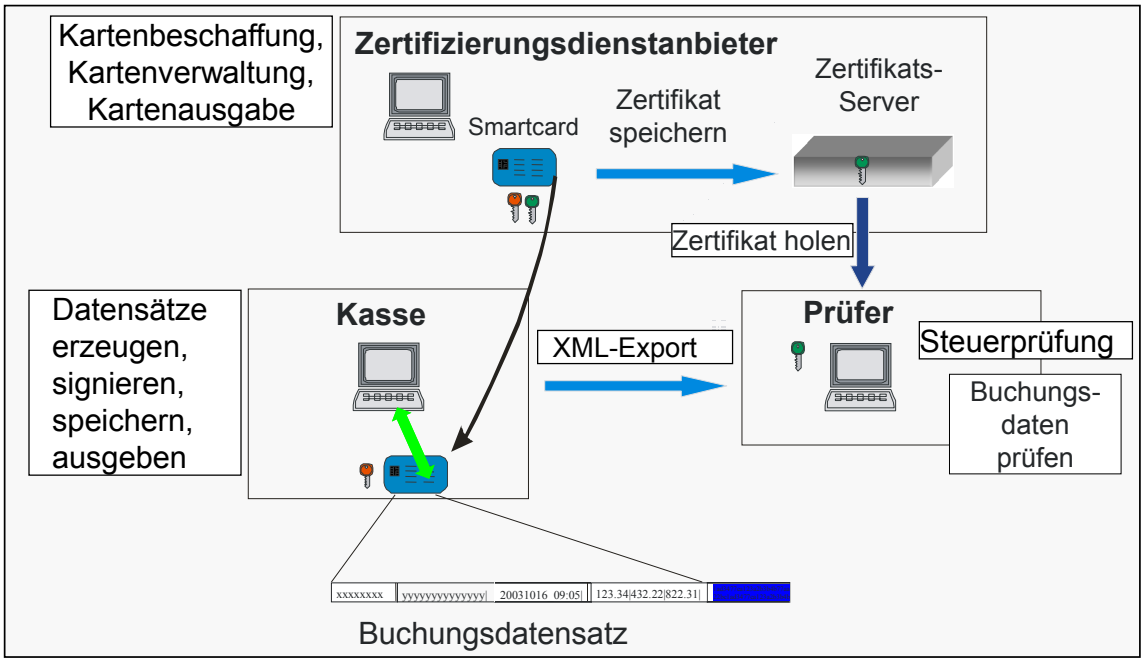


Abbildung 6: INSIKA-Systemumfeld

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=

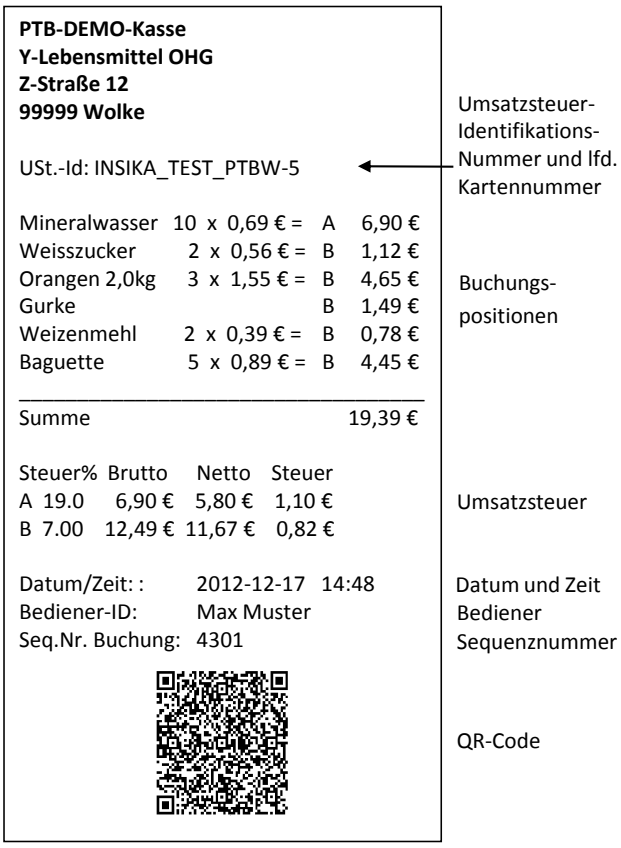


Abbildung 7: Typische Elemente eines INSIKA-Belegs

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/.