Das Kassensicherungssystem INSIKA und seine Anwendbarkeit auf Spielgeräte

Norbert Zisky
Physikalisch-Technische Bundesanstalt

Workshop „Sicherheit von Spielgeräten“

Übersicht

- Problem
- Lösungskonzept
- Systemarchitektur
- Technischer Ablauf
- Aufwand
- Konzeptanwendung für Spielgeräte

Aufzeichnung von Bargeschäften

- Aufzeichnungspflichten von Bargeschäften werden massiv verletzt (GoB, GDPdU)
- Schäden sind schwer zu beziffern
- Steuerverkürzung
- Schwarzarbeit
- Steuergerechtigkeit
- Wettbewerbsverzerrungen

Internationale Entwicklungen

- Alle Staaten sind mit gleichen Problemen bei Bargeschäften konfrontiert

  → weltweit unterschiedliche Lösungsansätze

- Europäische Bemühungen zur Suche neuer Ansätze im Rahmen des EU-Fiskalisprogramms 2013

- Weltweite Bemühungen zur Lösung der Probleme
  → Fiskalisierung von Kassensystemen
  → Verschärfung gesetzlicher Auflagen

Erosion of the Tax Base in Quebec/Canada

According to a study by RQ for 2002:

- **Percentage of restaurant operators who hide income: 48.4%**
- **Percentage of hidden income relative to declared income: 51.9%**

According to Revenu Québec's estimates for 2007–08:

- **Tax losses (Quebec laws only): $417M**
  - **$133M of QST charged by restaurant operators but not remitted to the government**
  - **Federal tax losses are as high as Quebec losses**

Quelle: Gilles,Bernard, FTA-Conf. Denver, June, 2nd, 2009

Tax fraud in US restaurant industry

We assume:

- (a) that there are restaurants in each US State, and
- (b) that people pay in cash in the US about the same as they do in
- Quebec, and
- (c) that the state taxes restaurant sales, and
- (d) the tax rate is similar to that of Quebec, and
- (e) that restaurant sales vary directly with GDP,
- … then there is fraud in the US restaurant sector of about $20 billion.

→Geschätzter Steuerbetrug:
20 Milliarden US Dollar!!! bei einem BIP von 8,3 Billionen US Dollar)

Quelle: R. Ainsworth, Unpublished Calculation May, 30th, 2009

Gleicher Ansatz für Deutschland

Unter Voraussetzung vergleichbarer Bedingungen und Verhältnisse wie Provinz Quebec/Kanada

BIP Deutschland 2007: 2,5 Billionen

→ Geschätzter Steuerschaden nur Gastronomie:

6,3 Milliarden/Jahr

Untersuchung des BRH

Bemerkungen 2003 Nr. 54

Drohende Steuerausfälle augrund moderner Kassensysteme

Feststellungen und Empfehlungen des Bundesrechnungshofes

Gefahr nicht abschätzbarer Steuerausfälle

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.

Neue Systeme ermöglichen Manipulationen

Der BRH hat darauf hingewiesen, dass die Finanzbehörden falsche Angaben über eingenommenes Bargeld zunehmend nicht mehr aufdecken können. Grund dafür sind neuere elektronische Kassensysteme und Registrierkassen. Eingegebene und im System erzeugte Daten lassen sich bei diesen Geräten ohne nachweisbare Spuren verändern.

BRH macht Verbesserungsvorschlag

Der BRH hat das BMF aufgefordert, unverzüglich dafür zu sorgen, dass die Aufzeichnung von Bargeschäften den Grundsätzen ordnungsgemäßer Buchführung entspricht. Hierbei empfehle es sich, die Kassen um ein eingriffsicheres Bauteil zu ergänzen und den Nutzern neuerer elektronischer Kassen den Nachweis über die Eingriffsicherheit aufzuerlegen.

Parlamentarische Beratung und Ergebnis

Parlament unterstützt Vorschlag des BRH

Der Rechnungsprüfungsausschuss hat die Bemerkung am 7. Mai 2004 zustimmend zur Kenntnis genommen. Er hat das BMF aufgefordert, unverzüglich Maßnahmen einzuleiten und hierüber bis zum 31. Dezember 2004 zu berichten.

BMF unterbreitet Lösungsvorschlag

Das BMF hat mitgeteilt, es sei daran gedacht, den Einbau eines zusätzlichen, vor Veränderungen geschützten, verschlüsselten Speichers zu verlangen. Damit solle der Nachweis materieller Verstöße gegen die Grundsätze ordnungsgemäßer Buchführung wieder möglich werden.

Parlament hält an BRH-Vorschlag fest

Der Rechnungsprüfungsausschuss hat das BMF am 10. März 2006 gebeten, rechtliche Vorgaben für ordnungsmäßige DV-gestützte Buchführungssysteme und die Aufzeichnung von Bargeschäften mit Hilfe elektronischer Kassen und Kassensysteme nach dem jeweils neuesten technischen Stand festzulegen. Er hat das BMF gebeten, bis zum 31. Dezember 2006 erneut zu berichten.

Untersuchung des BRH

Bemerkungen 2003 Nr. 54	Die Aufzeichnung von Bargeschäften durch elektronische Kassensysteme der neuesten Bauart genügt nicht den Grundsätzen ordnungsgemäßer Buchführung. Bei Bargeld-geschäften in mehrstelliger Milliardenhöhe drohen nicht abschätzbare Steuerausfälle.
Gefahr nicht abschätzbarer Steuerausfälle	Der BRH hat darauf hingewiesen, dass die Finanzbehörden falsche Angaben über eingenommenes Bargeld zunehmend nicht mehr aufdecken können. Grund dafür sind neuere elektro-nische Kassensysteme und Registrierkassen. Eingegebene und im System erzeugte Daten lassen sich bei diesen Geräten ohne nachweisbare Spuren verändern.
Neue Systeme ermöglichen Manipulationen	
BRH macht Verbesserungsvorschlag	Der BRH hat das BMF aufgefordert, unverzüglich dafür zu sorgen, dass die Aufzeichnung von Bargeschäften den Grund-sätzen ordnungsgemäßer Buchführung entspricht. Hierbei empfehle es sich, die Kassen um ein eingriffsicheres Bauteil zu ergänzen und den Nutzern neuerer elektronischer Kassen den Nachweis über die Eingriffsicherheit aufzuerlegen.
Parlament unterstützt Vorschlag des BRH	
BMF unterbreitet Lösungsvorschlag	Der Rechnungsprüfungsausschuss hat das BMF am 10. März 2006 gebeten, rechtliche Vorgaben für ordnungsmäßige DV-gestützte Buchführungssysteme und die Aufzeichnung von Bargeschäften mit Hilfe elektronischer Kassen und Kassensysteme nach dem jeweils neuesten technischen Stand festzulegen.
Parlament hält an BRH-Vorschlag fest	

Problem

Erfasster Datensatz

Mexico Bar

Bonn/xyz-Strasse 22

26.03.2004/18:26:01 Kellner 4

#151 A 10x1.80 18.00

#WB A 5 x8.00 40.00

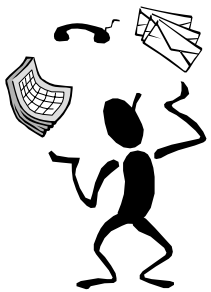
Wochenend Buffet

gesamt in Euro 58.00

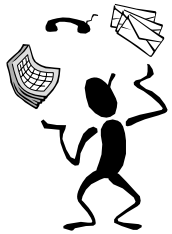
Kasse: 0007

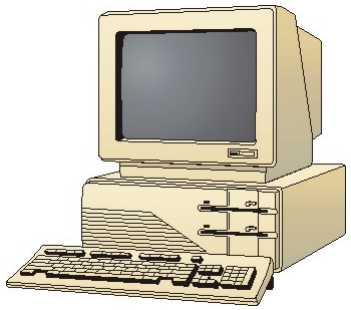
Steuer-Nr. 4555 54535535546

Ust-IdNr.: DE 6578848378



Kasse





Verbuchter Datensatz

Mexico Bar

Bonn/xyz-Strasse 22

26.03.2004/18:26:01 Kellner 4

#151 A 10x1.80 18.00

#WB A 4 x8.00 32.00

Wochenend Buffet

gesamt in Euro 50.00

Kasse: 0007

Steuer-Nr. 4555 54535535546

Ust-IdNr.: DE 6578848378

Mit geeigneter Software ist eine derartige Änderung spurenlos ausführbar!!!

Manipulationsmöglichkeiten (1)

In nicht speziell geschützten Systemen können Datenbestände relativ leicht manipuliert werden – oft unter Nutzung regulärer Funktionen oder Sicherheitslücken:

- Nutzung von Funktionen für Servicetechniker zur Manipulation (Zugriff auf Zähler)
- Missbräuchliche Verwendung von Testfunktionen
- Direkte Änderung von Datenbeständen (in Dateien oder Datenbanken) bei PC-basierten Systemen

Manipulationsmöglichkeiten (2)

Bereitstellung spezieller Manipulationsfunktionen durch den Systemhersteller
oder
Externe Systemangriffe unter Anwendung spezieller Hardware oder Software – Zapper, Phantomware:

- Entfernung kompletter Datensätze aus elektronischen Aufzeichnungen und Neuberechnung aller Daten
- Erstellung von „Wunsch-Daten“
- Funktionen zur Modifikation von Schlüsselwerten auf einen wählbaren Wert

Lösungskonzept

Zeitliche Zusammenhänge

2001 Hinweise aus den Ländern: Unerlaubte Veränderungen

2002 Länder fordern Fiskalspeicher, BRH wird aktiv

Start Zusammenarbeit BMF-PTB

2003 Prüfbericht des BRH: Dringender Handlungsbedarf

2004 PTB/BMF-Konzept → Bildung AG Registrierkassen

2005 1. Bericht der AG an die Länder → Nachforderungen

Empfehlung: Anwendung des PTB/BMF-Konzepts

2006 BRH-Bericht 2006, AG Reg-kas. → Auftrag für ein Fachkonzept

2007 AG Reg-kassen arbeitet an Fachkonzept

2008 BMF erarbeitet Gesetzentwurf; Aktionsbündnis gg. Schwarzarbeit

02/2008 Start INSIKA-Projekt

07/2008 Fertigstellung Fachkonzept

2009 18.02.2009 Präsentation der INSIKA-Arbeitsergebnisse

Aktueller Stand Juli 2008

- Grundsicherungskonzept wurde von Bund und Ländern bereits 2006 bestätigt
- Unklarheiten/Befürchtungen zur technischen Machbarkeit
- Unklarheit bei den Kosten !!!!
- Starke Widerstände aus der Wirtschaft

BMF hat das Gesetzgebungsverfahren zur Änderung/Ergänzung der Abgabenordnung §146 vorerst gestoppt

Aber!!!

- Es liegt ein fundiertes Fachkonzept vor
- Die technische Feinspezifikation wird im BMWi-Projekt „Integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme – INSIKA“ unter Leitung der PTB seit 02/2008 erarbeitet
- Alle technischen, allgemeingültigen Spezifikationen werden nach Fertigstellung frei zur Verfügung stehen

Interessierte Unternehmen können bereits jetzt technische Spezifikationen erhalten

INSIKA-Projekt (www.insika.de)

- Projektleitung: PTB
  Huth Elektronik Systeme GmbH,
  Quorion Data Systems GmbH,
  Ratio Elektronik Systeme GmbH
  Vectron System AG
- Vertragspartner Sicherheitsfragen: cryptovison GmbH
- Laufzeit: 2008 – 2010
- **Ziel: Entwicklung einer Sicherheitslösung für Kassensysteme**

Gefördertes MNPQ-Projekt des BMWi
(Messen, Normen, Prüfen, Qualitätssicherung)

AG Registrierkassen - INSIKA-Projekt

- INSIKA hat Lösungskonzepte für alle technischen Fragen erarbeitet;
- Ergebnisse wurden von AG Registrierkassen diskutiert und validiert
- Direkte Beteiligung bei der Lösung von kritischen Aufgaben durch direkten Kontakt
- Keine Beteiligung von INSIKA an Sitzungen der AG Registrierkassen (PTB hat als Bundesoberbehörde in der AG Registrierkassen mitgearbeitet)

Konzeptursprung Messwesen

Ziel des SELMA-Projekts (2002-2005)

www.selma.eu

- Bereitstellung erprobter, rechtsverträglicher Verfahren zur Übertragung von Messdaten über offene Netze von einer Messstelle zu Nutzern dieser Messdaten
- Integrität und Authentizität der Daten muss gewährleistet sein

Ergebnisse

- ab 2005 Einsatz der SELMA-Technik möglich
- Verifiziertes und anerkanntes Verfahren für den Austausch eichrechtlich-relevanter Messdaten über offene Netze
- Anwendungen im Gasbereich und neuen Lastgangzählern

Schutzziele Baraufzeichnungen

Sicherung sensibler Daten aus Baraufzeichnungen gegen bewusste oder unbewusste Verfälschungen

- Vollständige, richtige, geordnete und zeitgerechte Aufzeichnung aller Buchungen
- Verfälschungen von Daten sollen sicher erkannt werden
- Überprüfbarkeit von einmal gebuchten Daten auf Vollständigkeit und Richtigkeit durch zuständige Stellen

Idee!!!

Mexico Bar

Bonn/xyz-Strasse 22

26.03.2004/18:26:01 Kellner 4

#151 A 10x1.80 18.00

#WB A 5 x8.00 40.00

Wochenend Buffet

gesamt in Euro 58.00

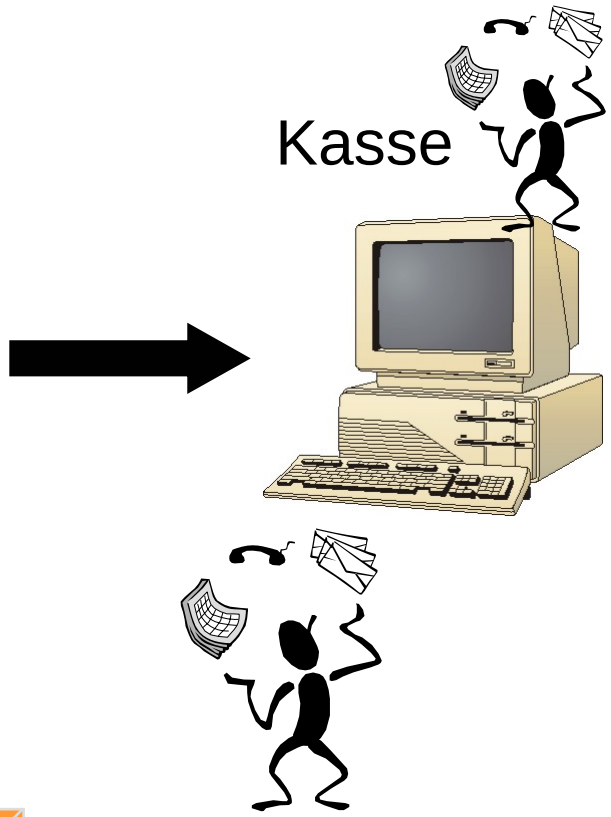
Kasse: 0007

Steuer-Nr. 4555 54535535546

Ust-IdNr.: DE 6578848378

Unterschrift der Finanzbehörde:

Finanzamt Bonn: H. Meier



Mexico Bar

Bonn/xyz-Strasse 22

26.03.2004/18:26:01 Kellner 4

#151 A 10x1.80 18.00

#WB A 5 x8.00 40.00

Wochenend Buffet

gesamt in Euro 58.00

Kasse: 0007

Steuer-Nr. 4555 54535535546

Ust-IdNr.: DE 6578848378

Unterschrift der Finanzbehörde:

Finanzamt Bonn: H. Meier

Idee!!!

Mexico Bar

Bonn/xyz-Strasse 22

26.03.2004/18:26:01 Kellner 4

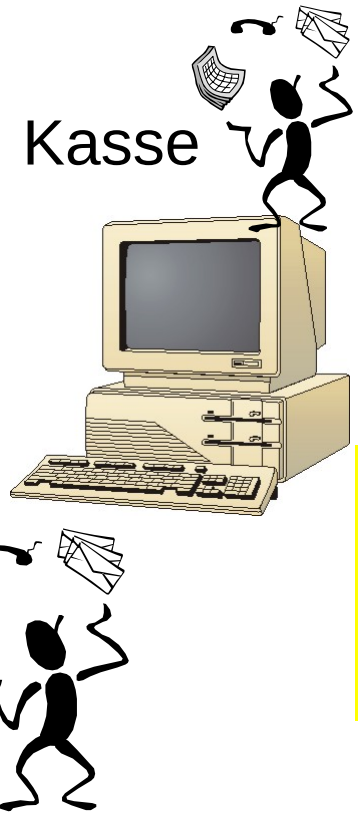
#151 A 10x1.80 18.00

Die Finanzbehörde „unterschreibt“ jeden gebuchten Datensatz bereits im Kassensystem.

Jede nachträgliche Veränderung wird erkannt.

Unterschrift der Finanzbehörde:

Finanzamt Bonn: H. Meier



Mexico Bar

Bonn/xyz-Strasse 22

26.03.2004/18:26:01 Kellner 4

#151 A 10x1.80 18.00

#WB A 5 x8.00 40.00

Wochenend Bueffet

Die Steuerprüfung beginnt mit einer Prüfung der Unversehrtheit der Daten und der Unterschrift

Unterschrift der Finanzbehörde:

Finanzamt Bonn: H. Meier

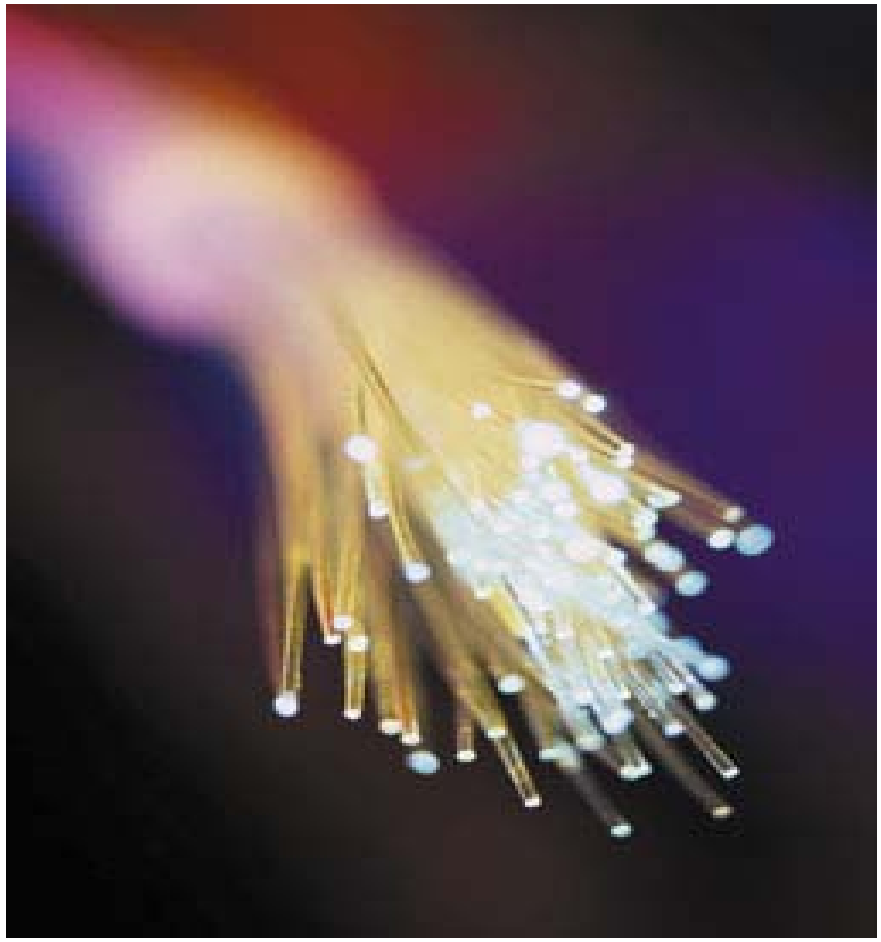
Hauptmerkmale

- Jeder Buchungsvorgang wird nach Abschluss elektronisch gesichert und gespeichert und ist nicht unerkannt veränderbar
- Mit jedem Beleg ist eine Prüfung möglich, ob die Buchung aufgezeichnet wurde
- Die Summen jeder Buchung werden fortlaufend summiert und in einem sicheren Speicher abgelegt
- Von den Summen wird täglich eine signierte Sicherungskopie angelegt
- Verwendung beliebiger Datenträger und Formate

Kryptographie – wichtige Begriffe

Wichtige Merkmale einer sicheren Datenübertragung und Datenspeicherung

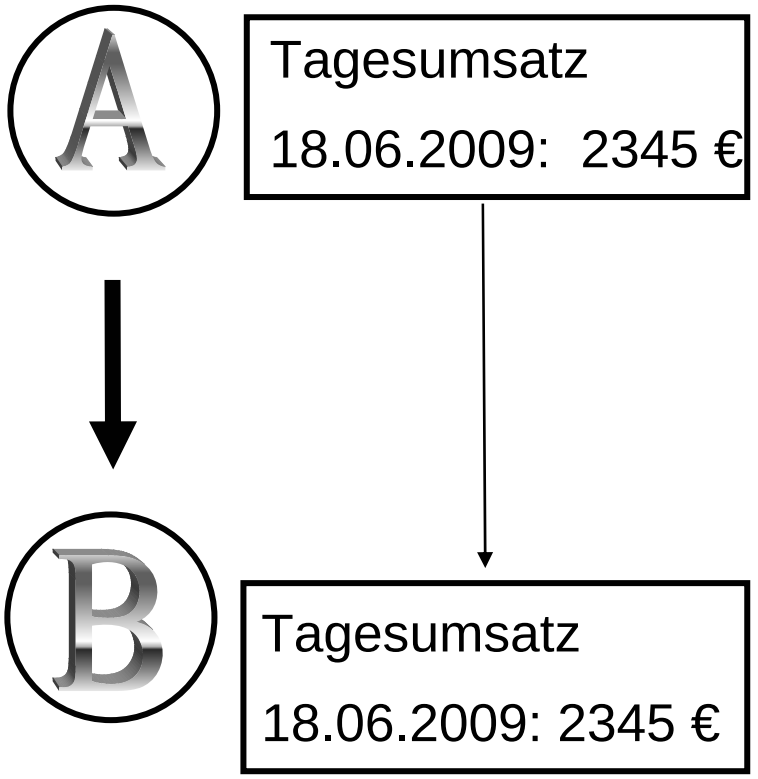
- Integrität
- Authentizität



Kryptographie (1)

Sichere Datenübermittlung
von **A** nach **B**
z.B. von der Kasse zum Prüfer

- **Integrität der Daten**
  Bei B ankommende Daten sind durch B auf ihre Korrektheit prüfbar (jede Verfälschung muss erkennbar sein)
- **Authentizität der Daten**
  Es kann durch B - und jede andere Instanz - überprüft werden, ob die bei B angekommenen Daten tatsächlich von A stammen.



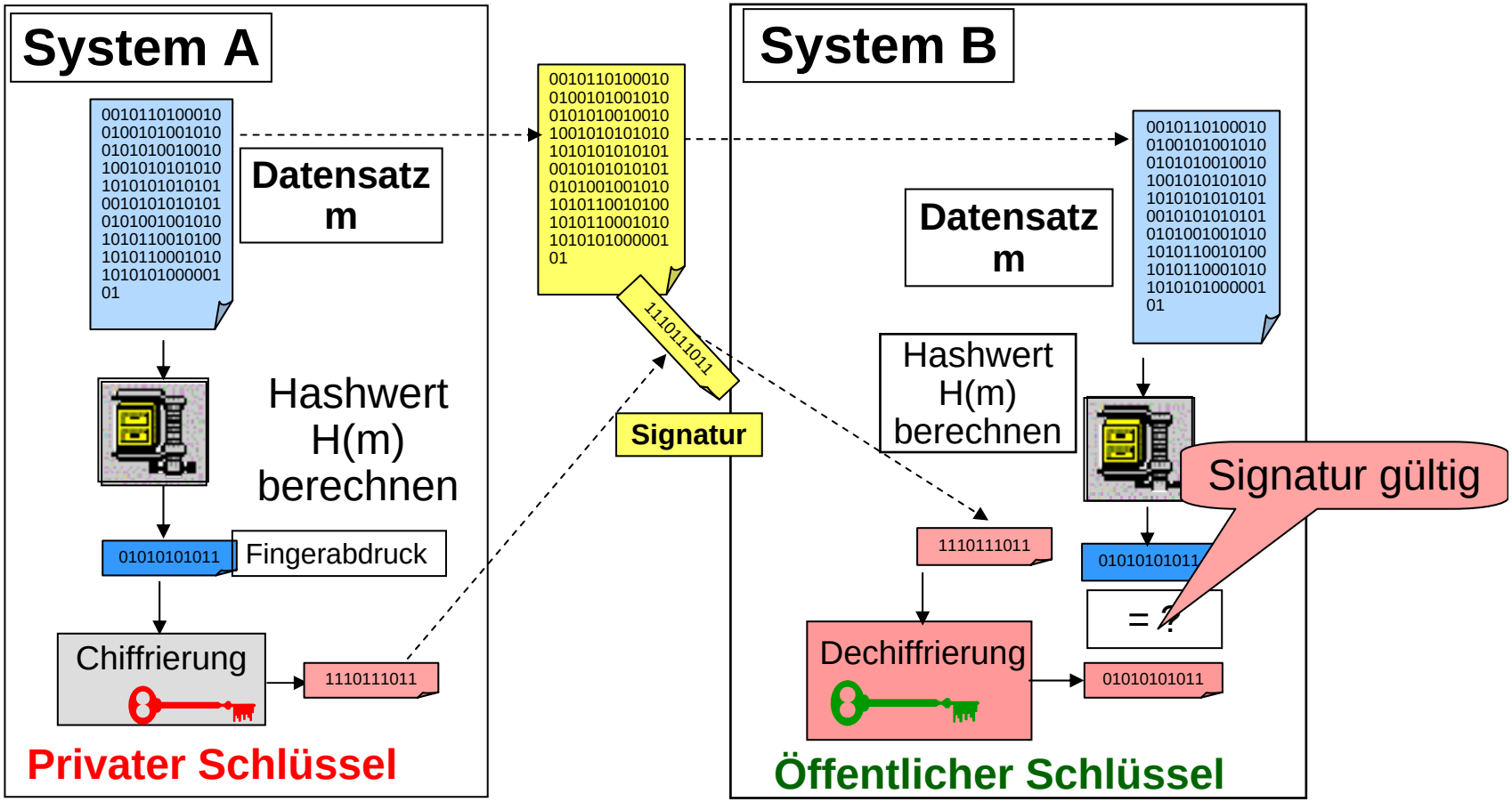
Kryptographie (2) - Verfahren des Konzepts

- Sicherung der **Integrität** der Daten:
  Anwendung von Hash-Funktionen, **SHA-1**
  (Mathematische Einwegfunktionen)

- Sicherung der **Authentizität** der Daten:
  Anwendung asymmetrischer Signaturverfahren
  Elliptic Curve-Technik (ECDSA, 192 bit)

Sicherheit durch Verwendung bekannter mathematischer Zusammenhänge und starker Verfahren der Kryptographie

Hashwert und Signatur



Elektronische Versiegelung

- Elektronische Versiegelung der Daten zur Erkennung von Verfälschungen:
  Elektronische Signaturen machen Manipulationen an den Daten selbst erkennbar →
  Jede kleinste Veränderung von Daten ist nach deren Signierung bei Prüfungen erkennbar
- Nur Daten mit Signatur und der öffentliche Prüfschlüssel werden benötigt

Vorteile digitaler Signaturen

Digitale Signaturen sind allen anderen Verfahren zur Manipulationssicherung überlegen:

- “End-to-end”-Absicherung – Schutz der Daten zwischen den „Endpunkten“ (z.B. Belegdruck und Software des beliebigen Prüfers)
- Keine proprietäre Technologie – Sicherheit basiert nicht auf der Geheimhaltung eines Verfahrens, sondern auf sehr gut untersuchten mathematischen Verfahren
- Sicherheit kann von unabhängigen Prüfern bestätigt werden
- Aktuelle Kryptografieverfahren sind praktisch nicht zu brechen

Akzeptanz des INSIKA-Konzepts

- Starke internationale Beachtung als alternativer Lösungsansatz zu „klassischen“ Fiskalsystemen
- Großes Interesse von Herstellern an Informationen zum Konzept und Technik
  (35 registrierte Unternehmen)
- Starkes Interesse an einem Pilotversuch in bestimmten Branchen zum Nachweis ordnungsgemäßer Buchführung
- INSIKA wurde am 2. Juni 2009 anlässlich FTA-Konferenz in den USA einer breiten Öffentlichkeit vorgestellt (Steuerprüfer, Behörden und Industrie)

Systemarchitektur

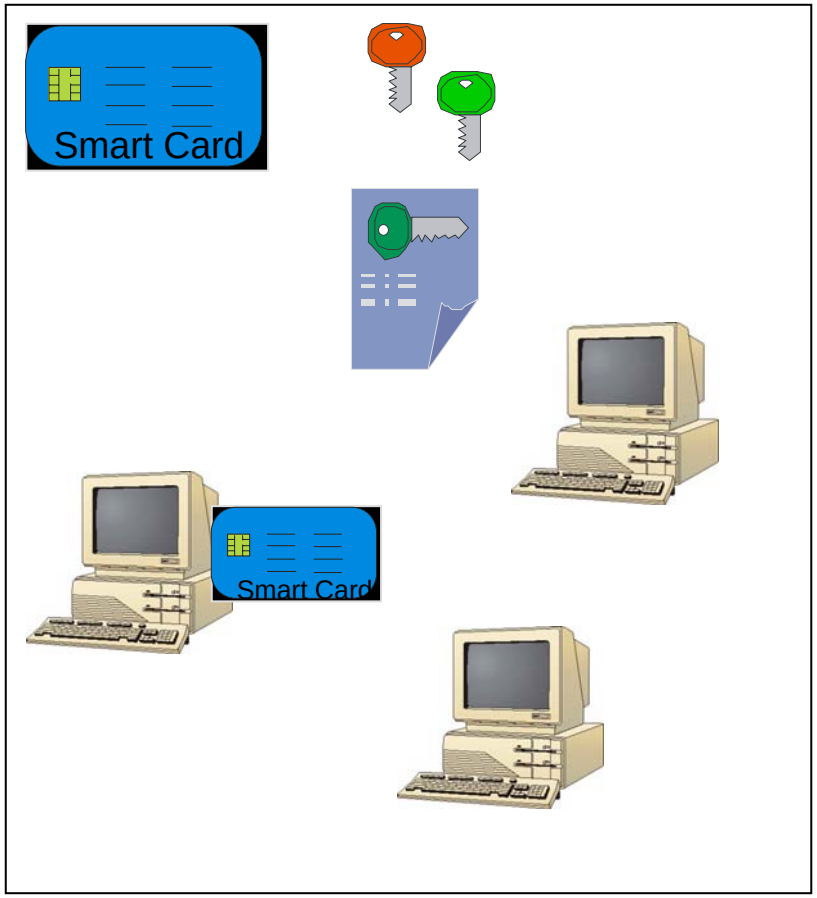
Sicherheitskomponenten

TIM

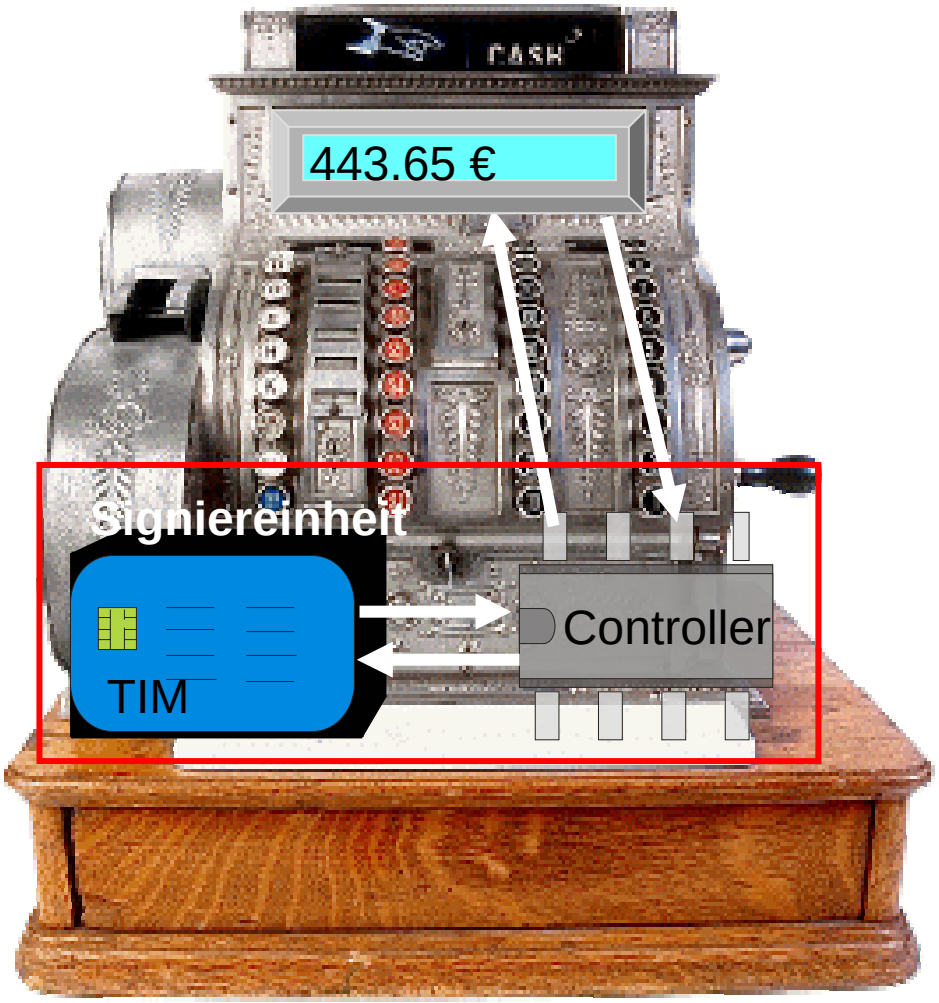
Tax Identification Module

Handelsübliche Smartcard mit einem eal 4+ - Sicherheitszertifikat mit speziellem Kryptopackage

- Elektronische Kasse mit Signaturerstellungseinheit
- Prüfsystem für Prüfer



Elektronische Registrierkasse mit TIM



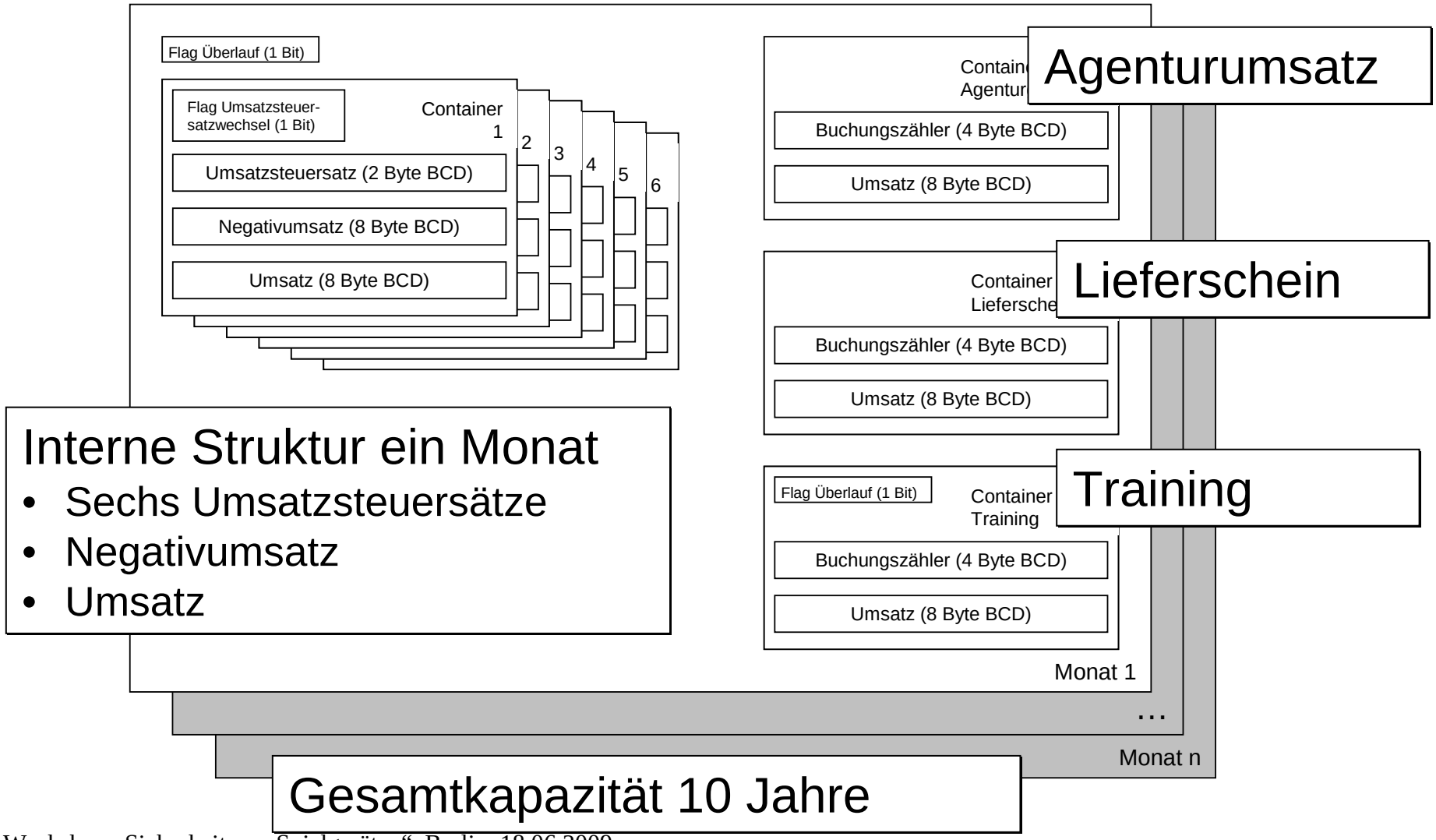
Signaturerstellungeinheit -TIM

- berechnet digitale Signaturen
- sicheren Speicher für privaten Schlüssel
- verwaltet Signatursequenznummer
- Summenspeicher

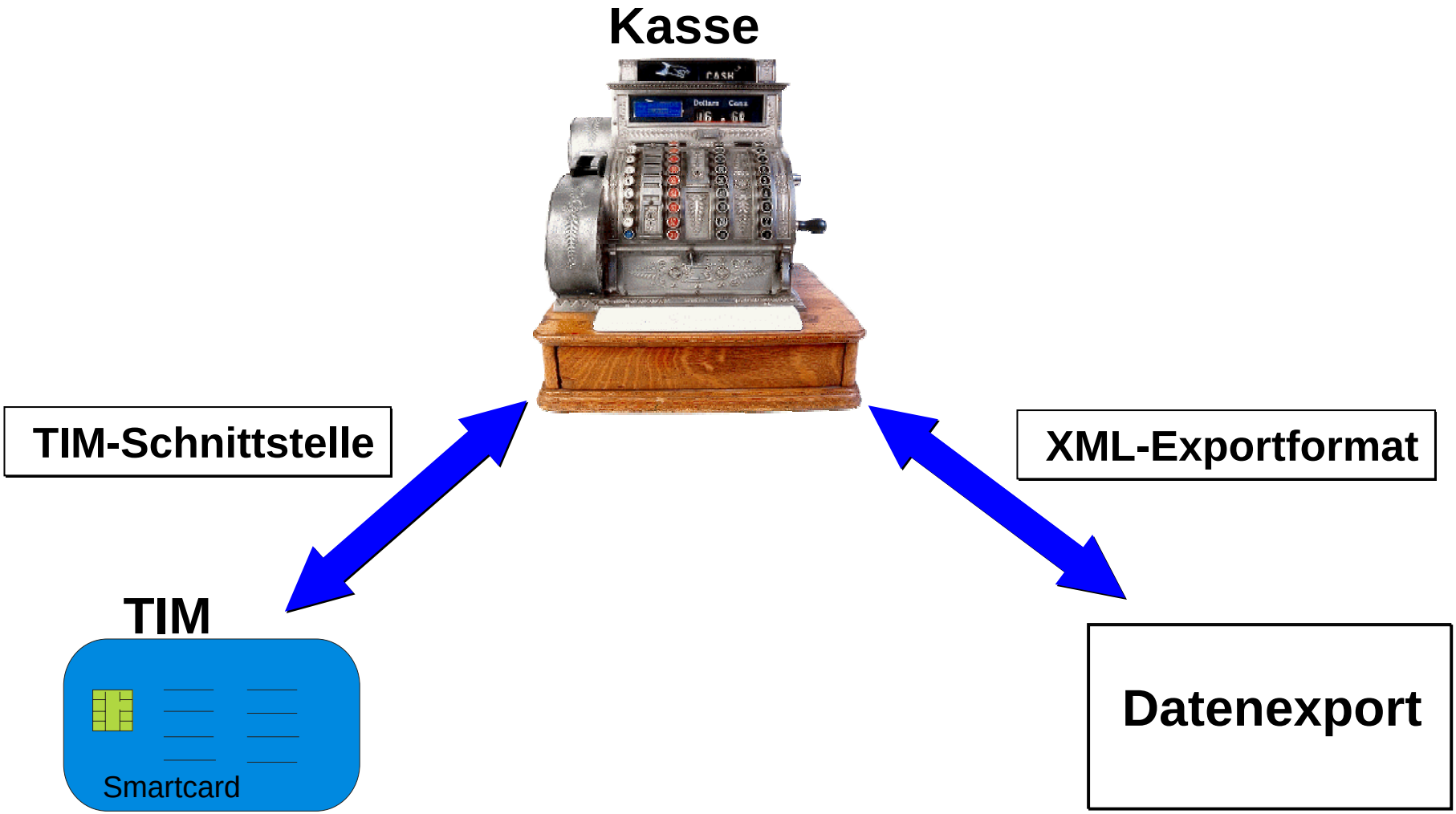
Registrierkasse

- Registrierfunktionen
- Berechnung von Hash-Werten
- Steuerung des Signiervorgangs
- Datenspeicherung

Summenspeichermodell TIM



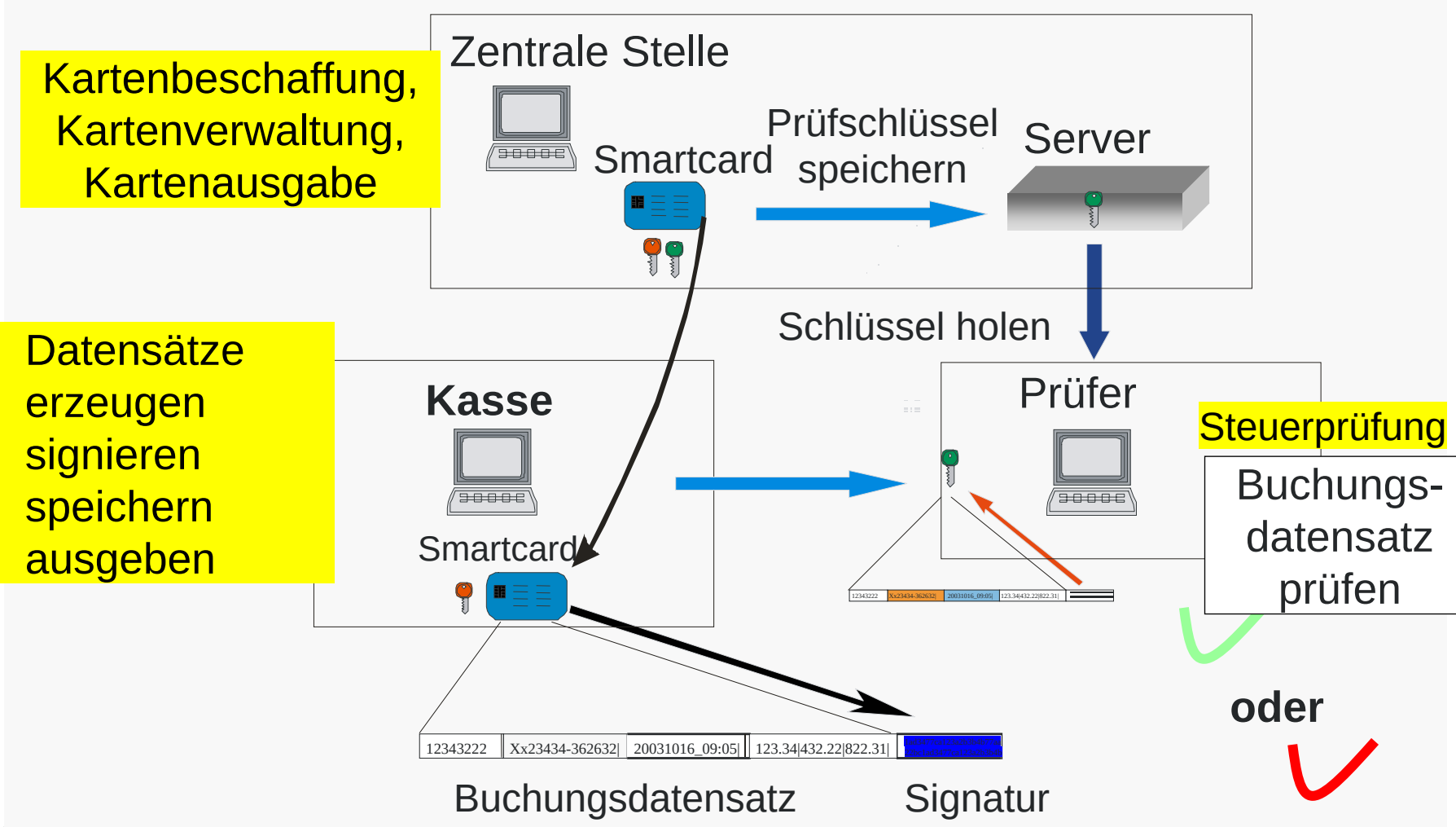
Kasse Systemschnittstellen



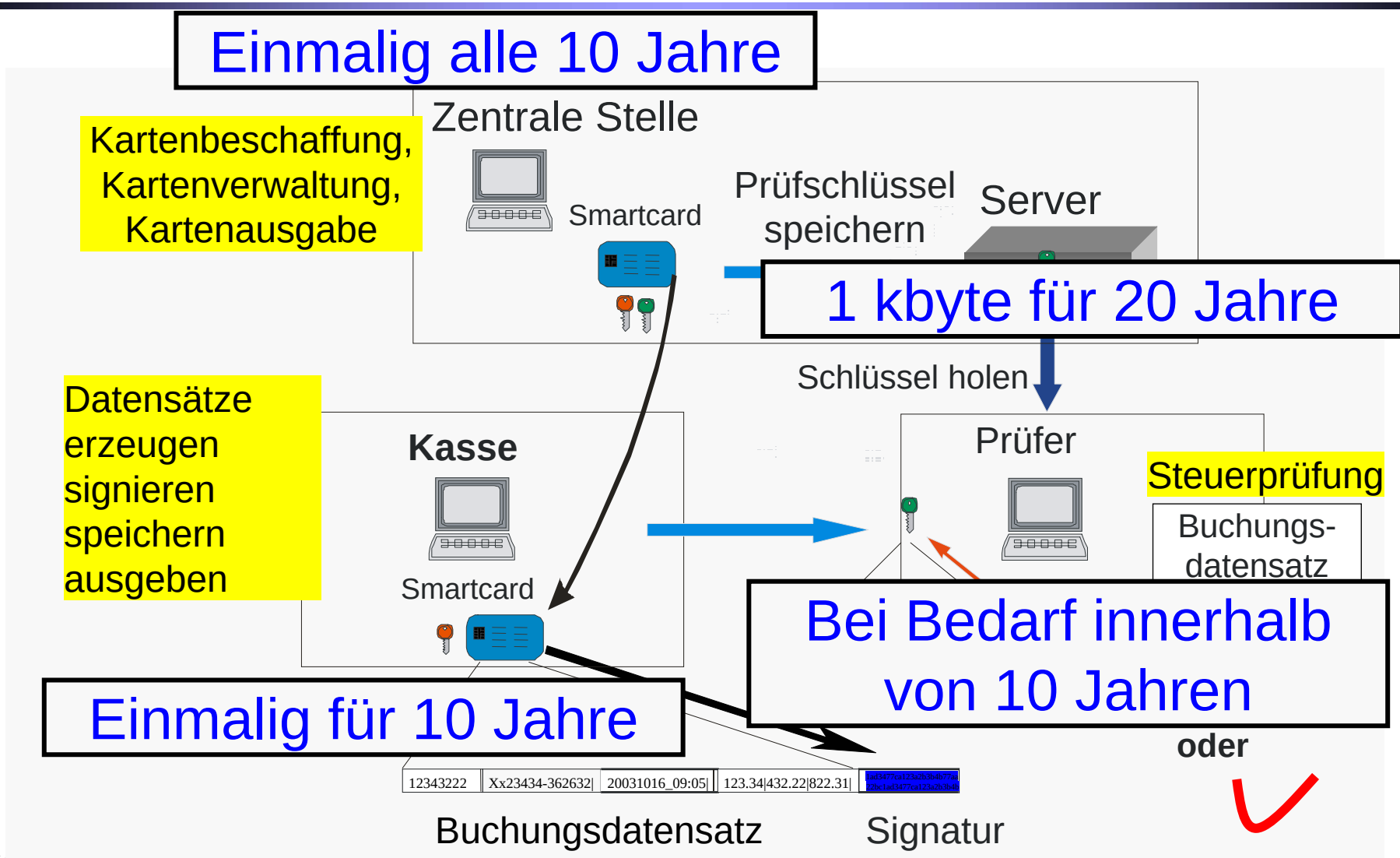
Betriebsmodell Zentrale Kartenausgabe

- Zentrale Stelle gibt Signaturkarten und Handlungsanweisungen für Kassenbetreiber aus (Sicherheitsaspekte - Datum, Sequenznummer)
- Finanzbehörden legen zu signierende Datensätze und Datenstrukturen fest
- Kassenhersteller integrieren die Signaturerstellungseinheiten in die Kassensysteme
- Steuerliche Prüfung beginnt mit Integritäts- und Plausibilitätsprüfung der Steuerdaten

Betrieb mit zentraler Kartenausgabe

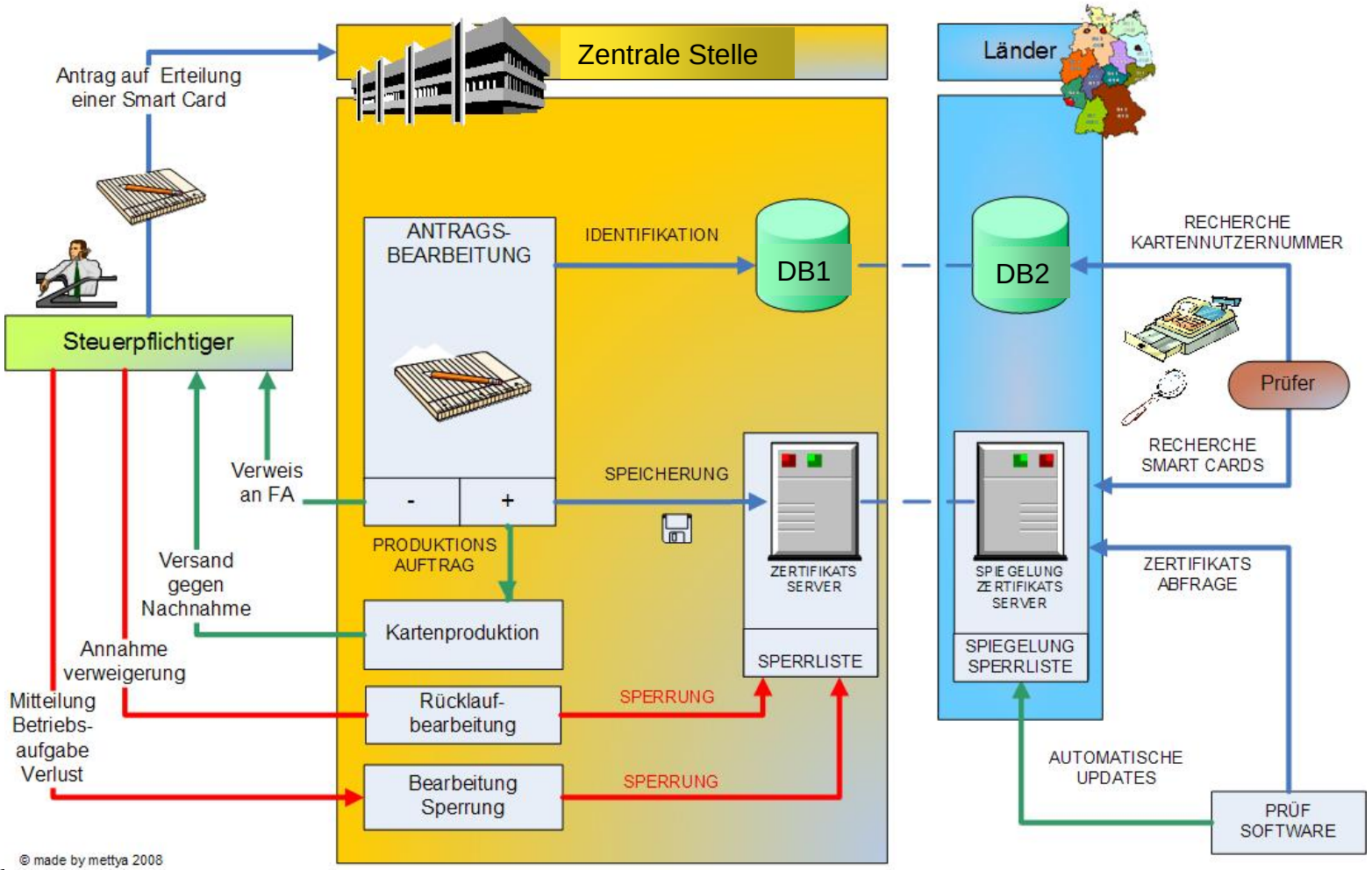


Lebenszyklus



Kartenausgabe und -verwaltung

Quelle: Fachkonzept AG Reg



Betriebsmodell dezentrale Kartenausgabe

- Dezentrale Dienstleister geben Signaturkarten für Kassenbetreiber/oder -systeme aus
- Finanzbehörden geben Handlungsempfehlungen für Kassensysteme aus: zu signierende Datensätze und Datenstrukturen, Prüfanforderungen
- Kassenhersteller integrieren die Signaturerstellungseinheiten in die Kassensysteme
- Steuerliche Prüfung beginnt mit Integritäts- und Plausibilitätsprüfung der Steuerdaten

Andere Betriebsmodelle

- Andere Betriebsmodelle vorstellbar
  - Dezentrale Kartenverwaltung
  - Personalisierung des POS
  - freiwillige Anwendung des Verfahrens
- z. B. beim bewussten Einsatz zum Eigenschutz des Unternehmens
- Nur geringe Modifikationen des Sicherheitskonzepts erforderlich

Konzept: Konkretisierung Kasse

- Aufzeichnungspflicht für alle Transaktionen (analog GoBS) zusätzlich Signaturen
- Elektronischer Datenzugriff durch Betriebsprüfer (analog GDPdU)
- Manipulationsschutz durch digitale Signaturen
- Bei Datenverlust Summenspeicher vorhanden

➡ Anwendung GoBS und GDPdU auf Kassensysteme ergänzt um sicheren Manipulationsschutz

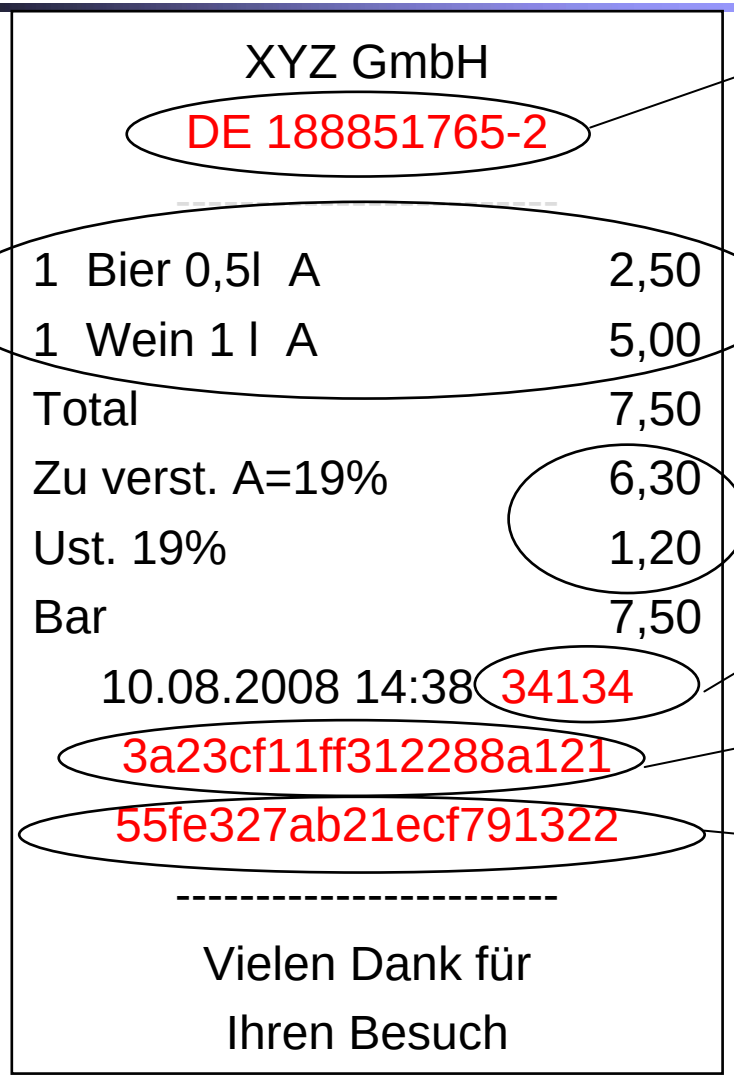
Technischer Ablauf

Buchung und Beleg

- Daten von Buchung und Beleg sind identisch
  Buchungssignatur = Belegsignatur
- Über Buchungssequenznummer ist eine eindeutige Zuordnung möglich
- Buchungsdaten sind dauerhaft elektronisch auf beliebigen Medien zu speichern – elektronisches Journal

Im Folgenden: Vorgehensweise bei der Signaturberechnung exemplarisch für Beleg

Elemente Buchung/Beleg



Steuernummer und lfd. Kartennummer

Artikelpositionen

Umsatzsteuer

Eindeutige Sequenznummer

Hashwert über Artikelpositionen

Signatur für Ausdruck

Rot = Elemente speziell für „Fiskalbelege“

Signieren: Kasse berechnet Hashwert Art.-pos.

XYZ GmbH
DE 188851765-2

---

1 Bier 0,5l A	2,50
1 Wein 1 l A	5,00
Total	7,50
Zu verst. A=19%	6,30
Ust. 19%	1,20
Bar	7,50

10.08.2008 14:38 34134
3a23cf11ff312288a121
55fe327ab21ecf791322

Vielen Dank für
Ihren Besuch

1	Stk	Bier 0,5l	19	2,50
1	Stk	Wein 1 l	19	5,00

Hashwert Artikelpos.

1. Schritt:
Errechnung eines Hashwert
über die Artikelpositionen

Signieren: TIM berechnet Signatur

XYZ GmbH
DE 188851765-2

---

1 Bier 0,5l A	2,50
1 Wein 1 l A	5,00
Total	7,50
Zu verst. A=19%	6,30
Ust. 19%	1,20
Bar	7,50

10.08.2008 14:38 34134
3a23cf11ff312288a121
55fe327ab21ecf791322

Vielen Dank für
Ihren Besuch

Hashcode Artikel	3a23cf11ff312288a121
Steuernummer	DE 188851765-2
Datum und Zeit	10.08.2008 14:38
Sequenznummer	34134
USt. normal	6,30 / 1,20 (19%)
USt. ermäßigt	0,0 / 0,0 (7%)

Belegsignatur

2. Schritt:
Smartcard berechnet
Belegsignatur

Signieren: TIM aktualisiert interne Speicher

Hashcode Artikel	3a23cf11ff312288a121
Steuernummer	DE 188851765-2
Datum und Zeit	10.08.2008 14:38
Sequenznummer	34134
USt. normal	6,30 / 1,20 (19%)
USt. ermäßigt	0,0 / 0,0 (7%)

Monats-Summenzähler auf Smartcard

Umsatz normal	180.422,86
Umsatz erm.	10.404,96
Negativ Umsatz normal	33.278,23
Umsatz Training	48.642,27
Umsatz Lieferschein	22.122,33
.....	.....

Signatur

3. Schritt: Smartcard aktualisiert Summenzähler

55fe327ab21ecf791322

Signieren: TIM-interne Abläufe

Folgende Vorgänge laufen in einem Schritt innerhalb der Smartcard TIM nach Datenübergabe vollautomatisch ab:

- Plausibilisierung der übergebenen Daten
- Vergabe einer neuen Sequenznummer
- Errechnen der Buchungssignatur
- Aktualisieren der Summenzähler
- Rückgabe der Signaturdaten an die Kasse

➡ Keine Manipulationen (z.B. Ändern der Daten und erneute Signaturberechnung) möglich

Signieren: Kasse speichert sign. Daten

Hashcode Artikel	3a23cf11ff312288a121
Steuernummer	DE 188851765-2
Datum und Zeit	10.08.2008 14:38
Sequenznummer	34134
USt. normal	6,30 / 1,20 (19%)
USt. ermäßigt	0,0 / 0,0 (7%)

Kasseninterne Abspeicherung der signierten Daten:
Herstellerspezifisch!! Keine Anforderungen

1,0,5,“Bier“,2.50,A
1,1,0,“Wein“,5.00,A
2,DE 188851765-2,200808101438,34134,6.30,1.20,0,0
3,55fe327ab21ecf791322

Notwendige Weiterverarbeitung

- Regelmäßige Übertragung der Daten auf ein Speichermedium (Speicherkarte, USB-Speicher, Festplatte, Abruf per DfÜ, Versand per E-Mail usw.)
- Sicherung von Tagesabschlüssen durch Auslesen der Summenspeicher der Smartcard
- Speicherung der Daten auf einem externen PC
- Konvertierung der Daten in ein „prüfungsfähiges“ Format – INSIKA-XML-Exportschnittstelle

Prüfung

Schritte zur Prüfung der Journaldaten:

- Konvertierung in das Standardformat XML-Export
- Vergleich der Summen der Buchungen mit den Tagesabschlüssen
- Kontrolle der Signaturen der Tagesabschlüsse
- Bei Bedarf:
  - Vollständige oder stichprobenartige Kontrolle der einzelnen Buchungen
  - Kontrolle gedruckter Belege, um Fälschungen erkennen zu können

Geschätzter Aufwand für Kassenhersteller

Gegenstand	Preis	Preis pro Kasse*
Hardware Leser	10 €	10 €
Hardware Speicher/Schnittstelle	5 €	5 €
Software Smartcard-Ansteuerung	30 000 €	15 €
Software Speichererweiterung	10 000 €	5 €
Software XML-Export	10 000 €	5 €
Summe		**40 €**

* Bezogen auf 2000 produzierte Einheiten

Grobe Aufwandabschätzung durch PTB auf der Grundlage der Erfahrungen aus dem SELMA-Projekt

Aufwand für Kassenbetreiber

- Beantragen der Smartcard
- Einbau der Smartcard (einmalig für 10 Jahre)
- Datensicherung (dazu ist er heute bereits verpflichtet)
- Bereithalten der Daten im Format der Exportschnittstelle

Gegenstand	Preis	Preis pro Kasse*
Antrag	0 €	0 €
Preis Smartcard	10 €	10 €
Datensicherung	0 €	0 €
Einbau Smartcard Nachrüstung	80 €	80 €
Einbau Smartcard Neubeschaffung	0 €	0 €
Summe		**10 bis 90 €**

Vorteile

- Sicherheit durch Anwendung bekannter und erprobter Verfahren mit hohem Sicherheitsstandard
- Eindeutig definierte Schnittstellen
- Daten können auf beliebigen Datenträgern in beliebigen Formaten gespeichert werden
- Keine aufwändigen Anforderungen an Systemhersteller
- Keine Bauartzulassungen von Systemen
- Effektive Prüfmöglichkeiten
- Nachweis korrekter Buchungen wird möglich

Kann das INSIKA-Konzept für Spielgeräte verwendet werden?

Anwendungsbereiche

- INSIKA wurde zunächst für den Manipulationsschutz von Buchungsdatensätzen entwickelt
- Im Focus standen jedoch immer alle Aufzeichnungen von Bargeschäften
  - Taxigewerbe
  - registrierende Waagen
- Verkaufsautomaten wurden beim Gesetzgebungsverfahren des BMF noch nicht einbezogen

Überlegungen

- These 1: Spielgeräte sind spezielle Verkaufsautomaten
- These 2: Der Schutzbedarf betrifft nicht die Daten für ein Produkt oder eine Dienstleistung
- These 3: Es können Datensätze festgelegt werden, die hohen Schutzbedarf haben
- These 4: Es können Methoden festgelegt werden, mit denen die Verwendung der Signaturerstellungseinheit einfach überprüfbar ist
- These 5: Überprüfbare signierte elektronische Journale könnten Spielgeräte „sicherer“ machen

Randbedingungen/Anforderungen

- Die Ausgabe gedruckter Belege für jede Signaturerstellung wäre optimal
- Signierte elektronische Aufzeichnungen von Einzahlungen, Auszahlungen und Ereignissen über längere Zeiträume sind heute technisch möglich
- Neben dem Schutz von Fiskaldaten hat der Spielerschutz eine sehr hohe Bedeutung
- Alle Spielautomaten sollten mit einer einheitlichen Sicherheitstechnik ausgestattet sein
- Ein Sicherheitssystem muss mit einfachen Mitteln überprüfbar sein

Einschränkungen

- INSIKA ist keine Wunderlösung
- Ohne Marktaufsicht ist das System als technische Lösung angreifbar
- Unterschiedliche Betreibermodelle erfordern mehrere Sicherheits- und Prüfkonzepte
- Hohe Gefahr von Koalitionsangriffen

Zusammenfassung

- Anwendung eines modifizierten INSIKA-Konzepts für Spielgeräte erscheint möglich
- Einheitliche Sicherheitstechnik zum Schutz genau festgelegter Datensätze minimiert das Restrisiko
- Einsatz zur Sicherung anderer Funktionsabläufe (Kommunikation, Softwareidentifikation, Zugriffsschutz)
- Anforderungen aus unterschiedlichen Bereichen nutzen die die gleiche Sicherheitstechnik und die gleiche Datenbasis
- Spielgerätebetreiber erfüllen die Anforderungen aus GoB und GDPdU

Vielen Dank!