Konzept zum Aufbau und Betrieb revisionssicherer Kassensysteme und Messeinrichtungen

Norbert Zisky
Physikalisch-Technische Bundesanstalt

246. PTB-Seminar: Revisionssicheres System zur Aufzeichnung von Kassenvorgängen und Messinformationen

Übersicht

- Einleitung
- Zeitlicher Überblick
- Sicherheitskonzept
- Sicherheitsarchitektur
- Technische Abläufe
- Aufwand
- Vor- und Nachteile
- Ausblick

Schutzziele allgemein

Sicherung sensibler Daten gegen
bewusste oder unbewusste Verfälschungen

- Vollständige, richtige, geordnete und zeitgerechte Aufzeichnung aller als „zu schützend“ definierten Daten
- Verfälschungen von Daten sollen sicher erkannt werden
- Überprüfbarkeit von Aufzeichnungen auf Vollständigkeit und Richtigkeit durch entsprechend festgelegte Stellen

Übertragbarkeit auf Messdaten und Kassendaten

Wurzeln des Konzepts

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

Wurzeln des Konzepts

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

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 elektro-nische 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 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 Kassensys-teme nach dem jeweils neuesten technischen Stand festzulegen.

Parlament hält an BRH-Vorschlag fest

Wurzeln des Konzepts

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

02/2008 Start INSIKA-Projekt

Wurzeln des Konzepts

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 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 erarbeitet
- Alle technischen, allgemeingültigen Spezifikationen werden nach Fertigstellung frei zur Verfügung stehen

Interessierte Unternehmen können bereits jetzt technische Spezifikationen erhalten

Internationale Entwicklungen

- Alle entwickelten Staaten sind mit den gleichen Problemen bei Bargeschäften konfrontiert

  → weltweit sehr unterschiedliche Lösungsansätze

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

- Weltweite Bemühungen zur Lösung der Probleme

INSIKA-Projekt

- 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: Entwicklungs 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)

Das Konzept

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

Allgemeine 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 gebuchter Daten auf Vollständigkeit und Richtigkeit durch zuständige Stellen

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

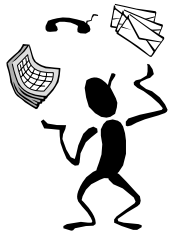
Wochenend Bueffet

gesamt in Euro 58.00

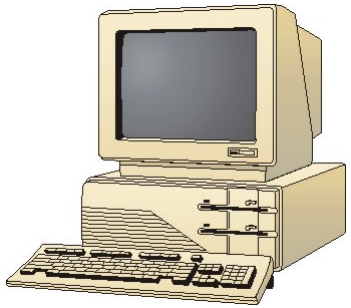
Kasse: 0007

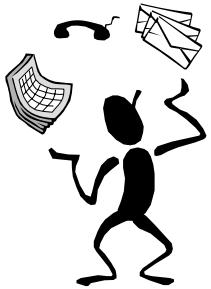
Steuer-Nr. 4555 54535535546

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 Bueffet

gesamt in Euro 40.00

Kasse: 0007

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

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 Bueffet

gesamt in Euro 58.00

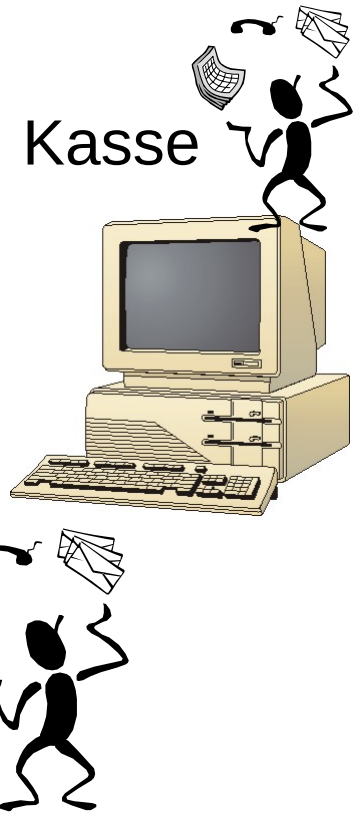
Kasse: 0007

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 Bueffet

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

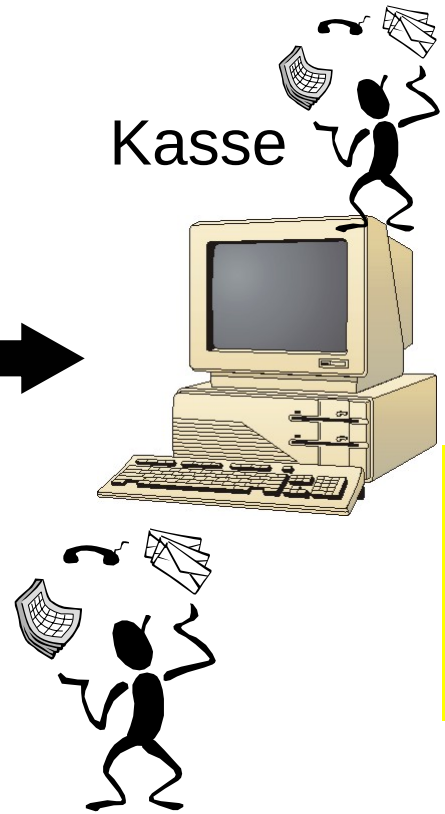
#151 A 10x1.80 18.00

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

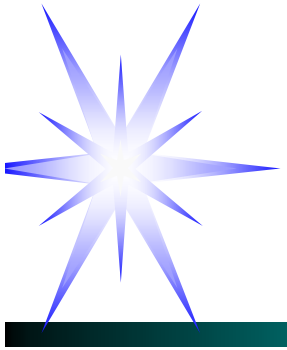
#WB A 5 x8.00 40.00

Wochenend Bueffet

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

Unterschrift der Finanzbehörde:

Finanzamt Bonn: H. Meier



Das verstehe ich nicht ????!!!!
Geht denn das ??

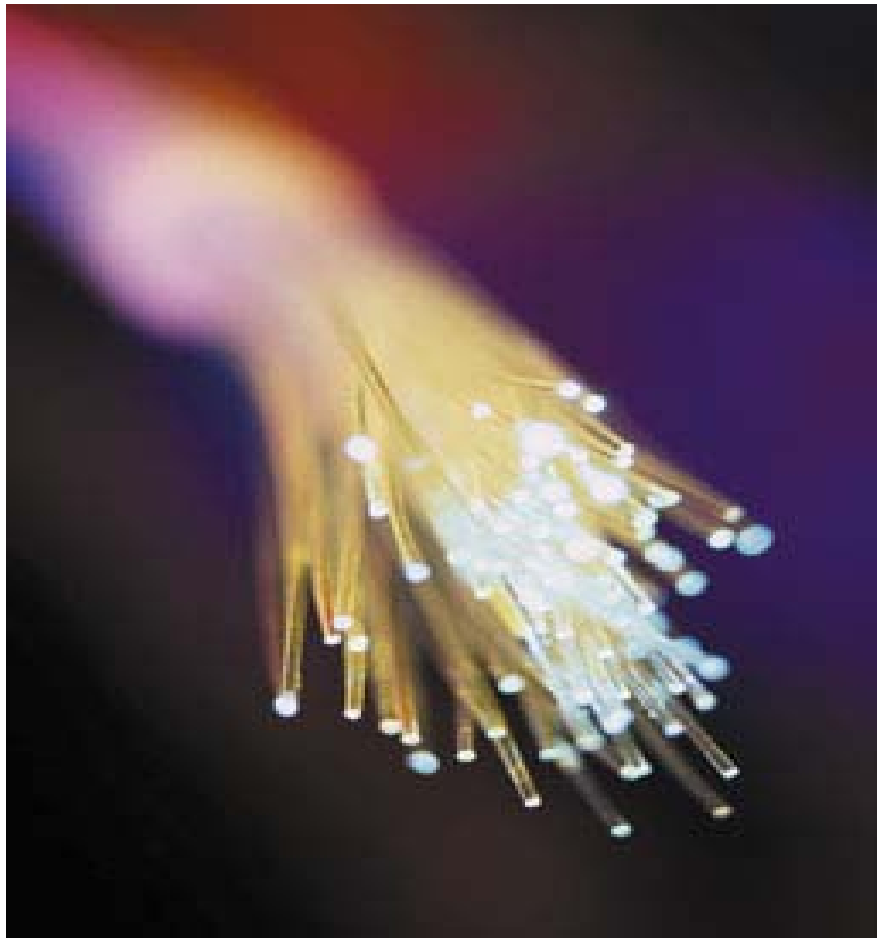
oder

etwas Kryptographie

Kryptographie – wichtige Begriffe

Wichtige Merkmale einer sicheren Datenübertragung und –speicherung

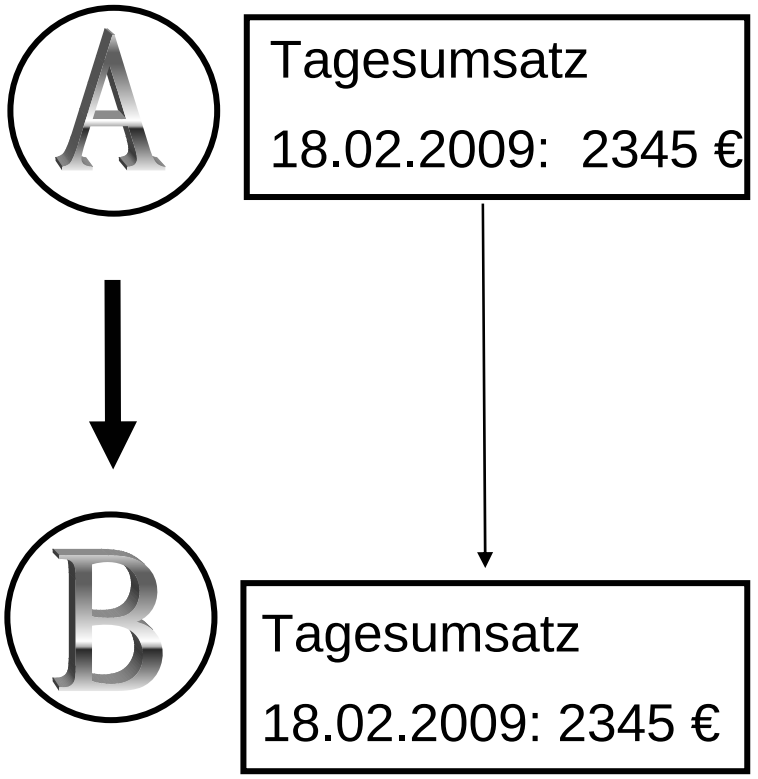
- Integrität
- Authentizität



Kryptographie (1)

Sichere Datenübermittlung oder -speicherung 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**

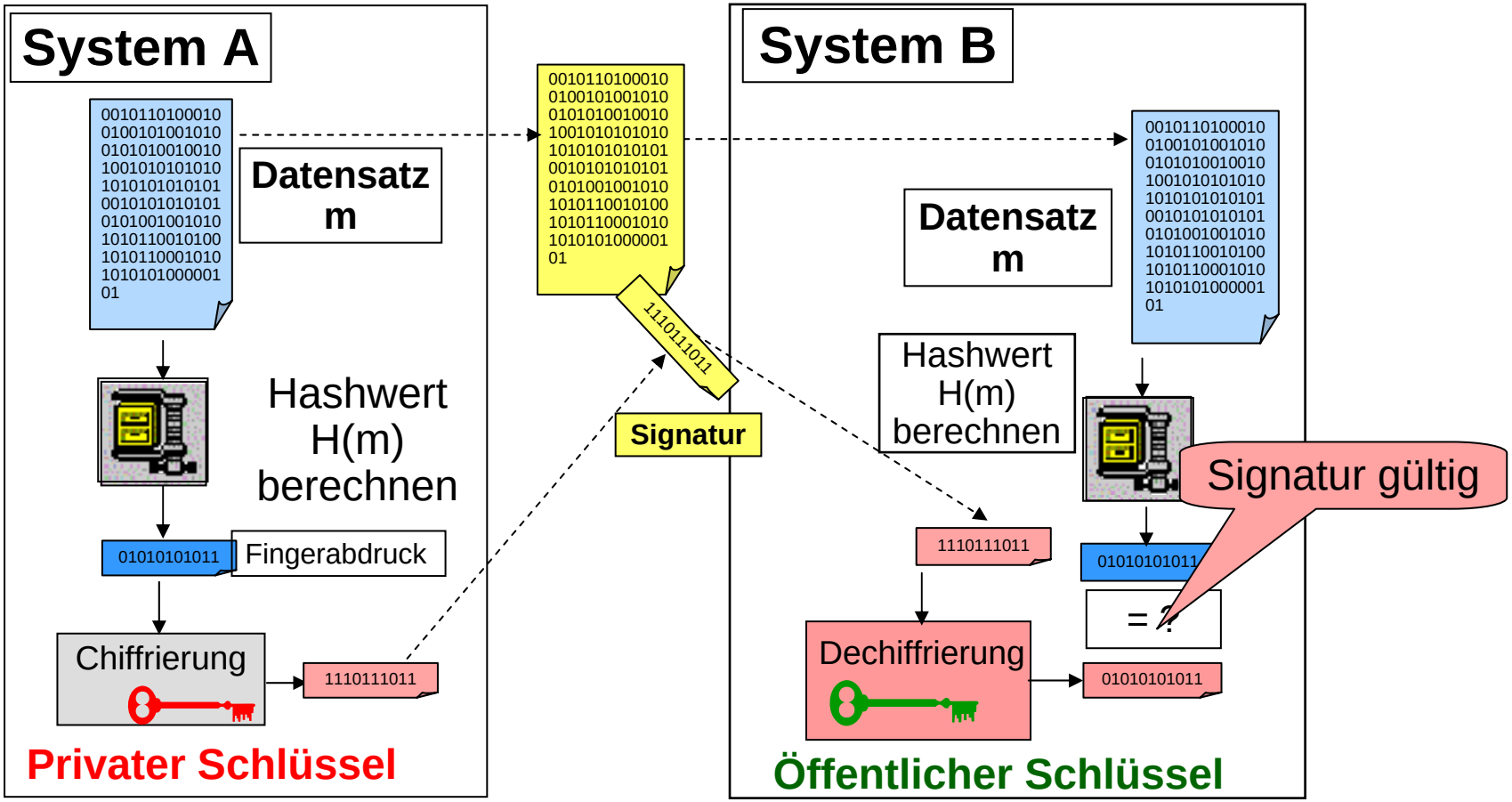
- Sicherung der Authentizität der Daten:
  Anwendung asymmetrischer Signaturverfahren
  Elliptic Curve-Technik (ECDSA)

Sicherheit durch Verwendung bekannter mathematischer Zusammenhänge und Verfahren der Kryptographie

Eingesetzte Technik

- Technik ist seit Jahren bekannt, erprobt und standardisiert
- Verfahren der kryptographischen Datensicherung wird großflächig eingesetzt
- Massenanwendungen führen zu kostengünstigen Lösungen
- Sicherheitskonzept wurde erprobt (SELMA-Projekt 2002-2005)
- SELMA erhielt IT-Sicherheitspreis NRW 2006

Hashwert und Signatur



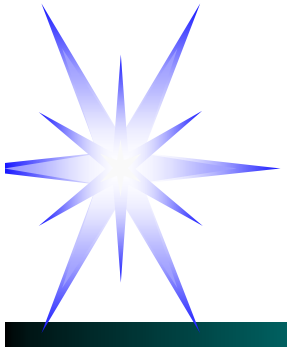
Elektronische Versiegelung

- 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 Prüfschlüssel werden benötigt

Vorteile digitaler Signaturen

Digitale Signaturen sind praktisch 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 (nur die Smartcard muss geprüft werden)
- Aktuelle Kryptografieverfahren sind praktisch nicht zu brechen



Das wars schon mit der Kryptographie

Jetzt wird’s konkret

Hauptmerkmale der Lösung

- 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

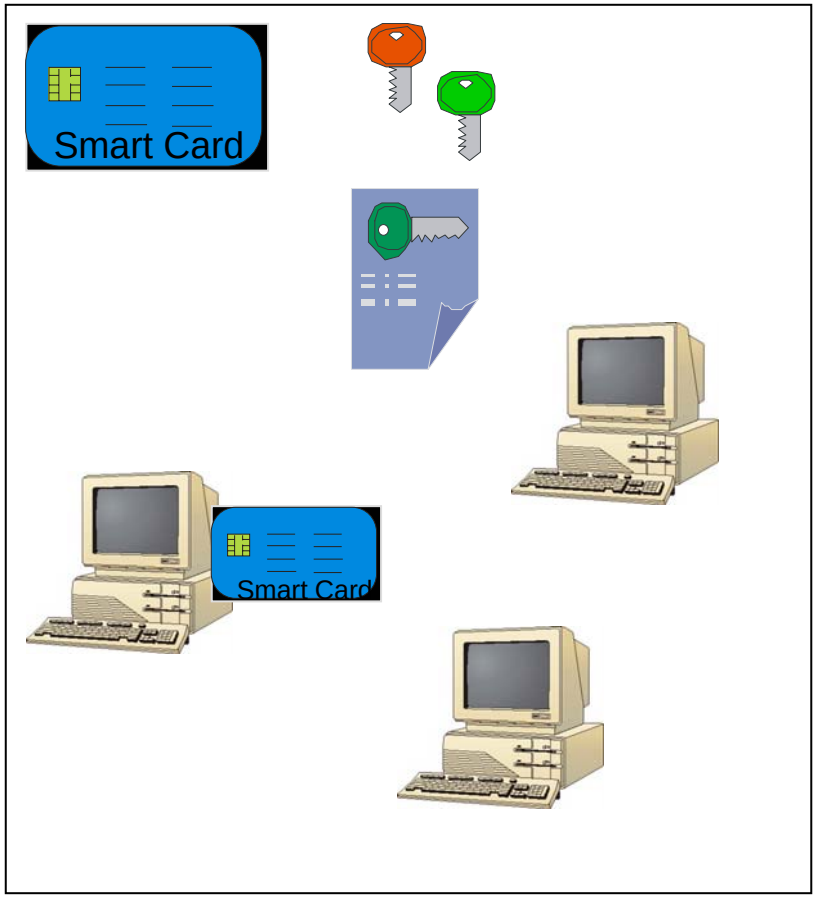
Sicherheitskomponenten

TIM

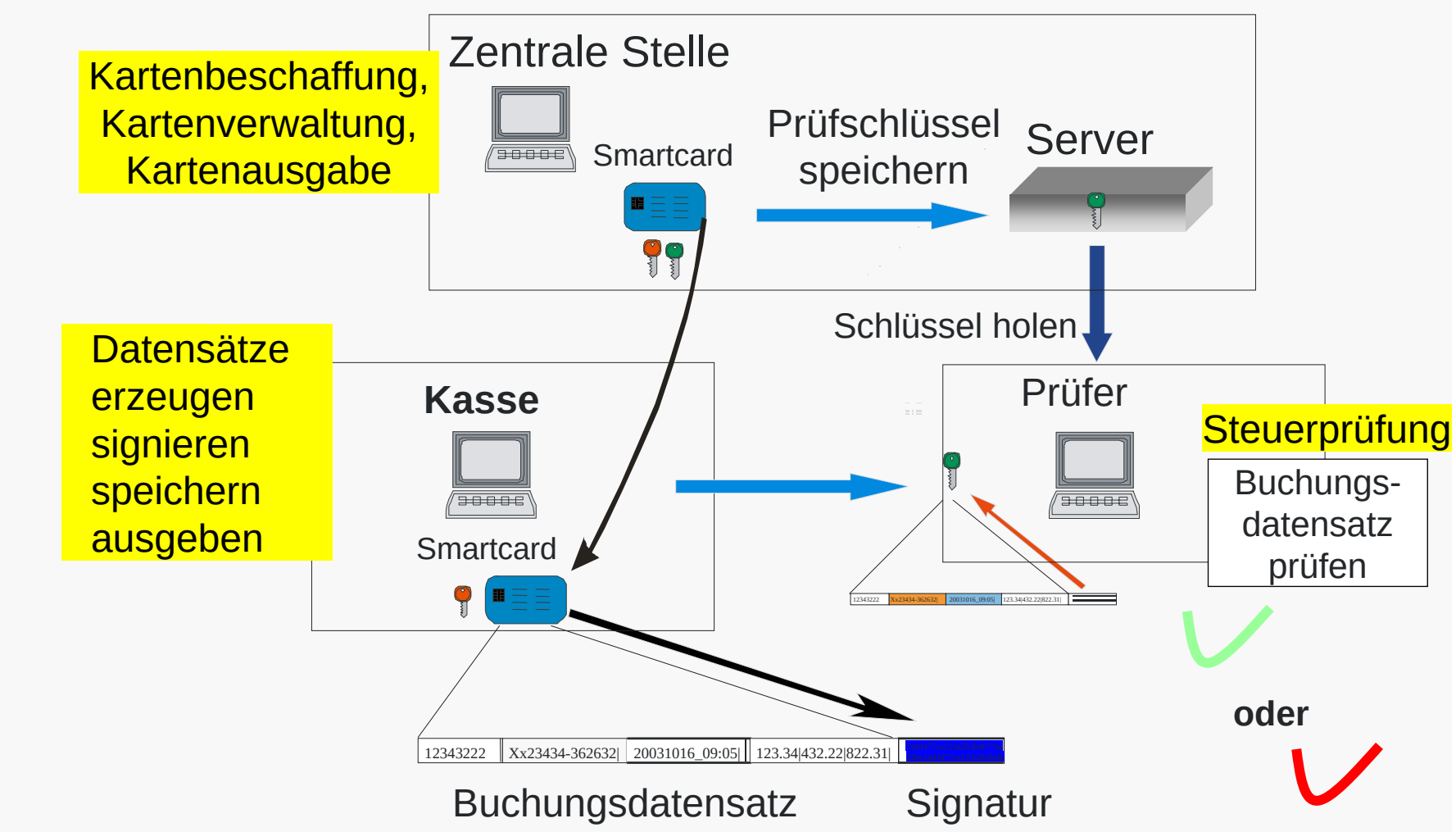
Tax Identification Module

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

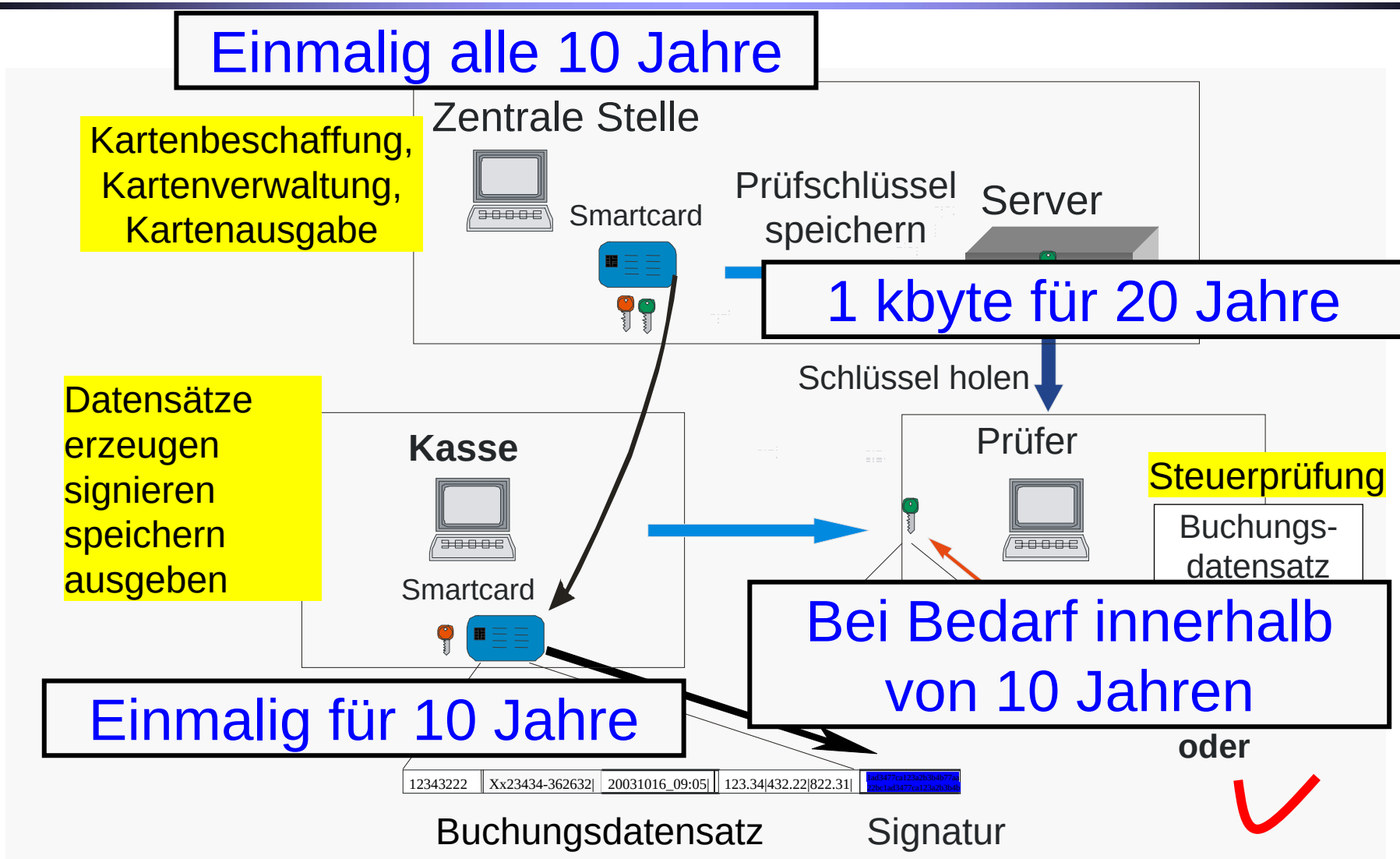
- Elektronische Kasse mit Signaturerstellungseinheit
- Prüfsystem für Signaturen (Prüfer)



Systemarchitektur



Systemarchitektur - Lebenszyklus

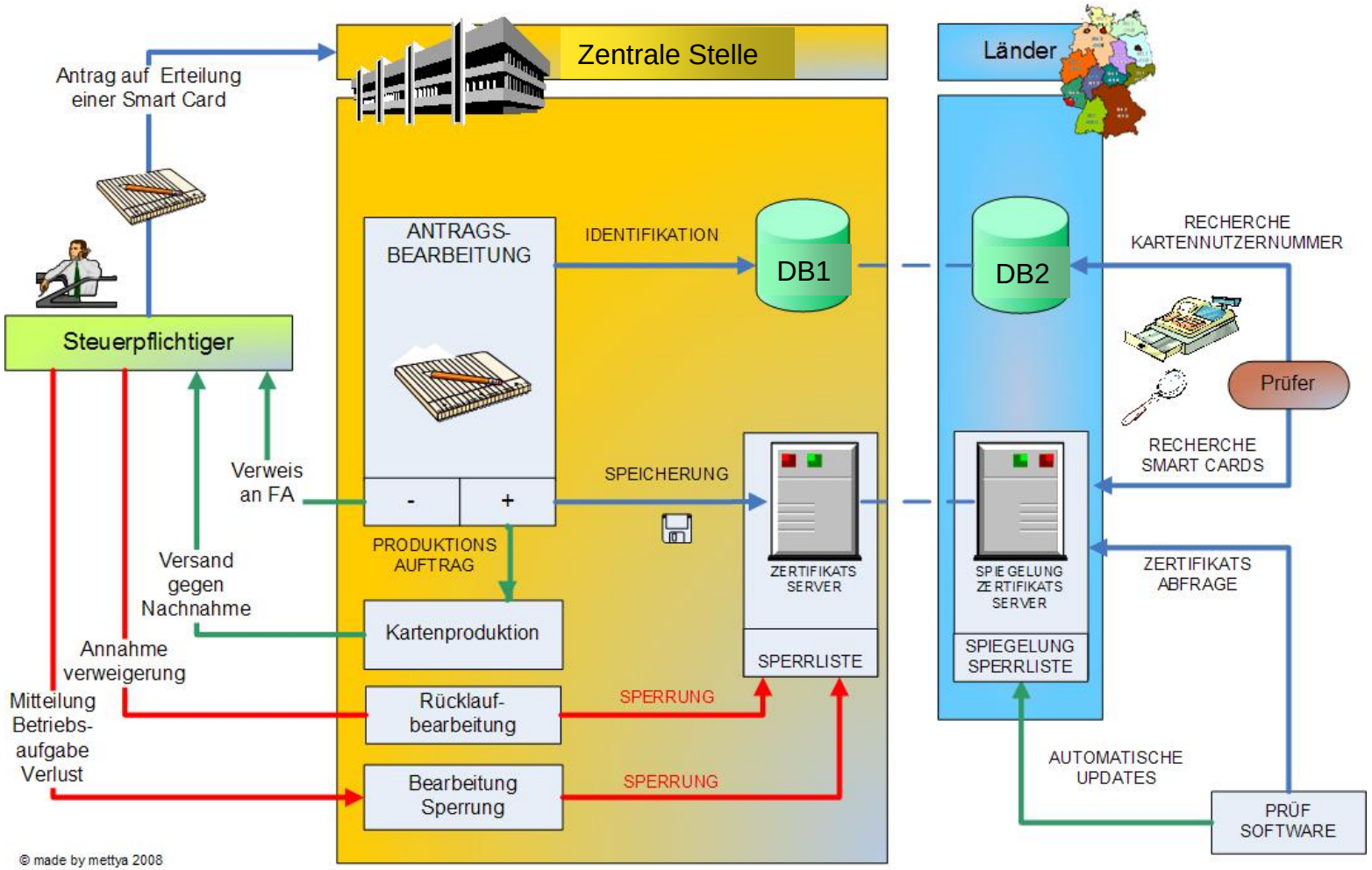


Betriebsmodell Zentrale Kartenausgabe

- 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

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
- z. B. beim bewussten Einsatz zum Eigenschutz
- 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

Konzept: Wesentliche Elemente

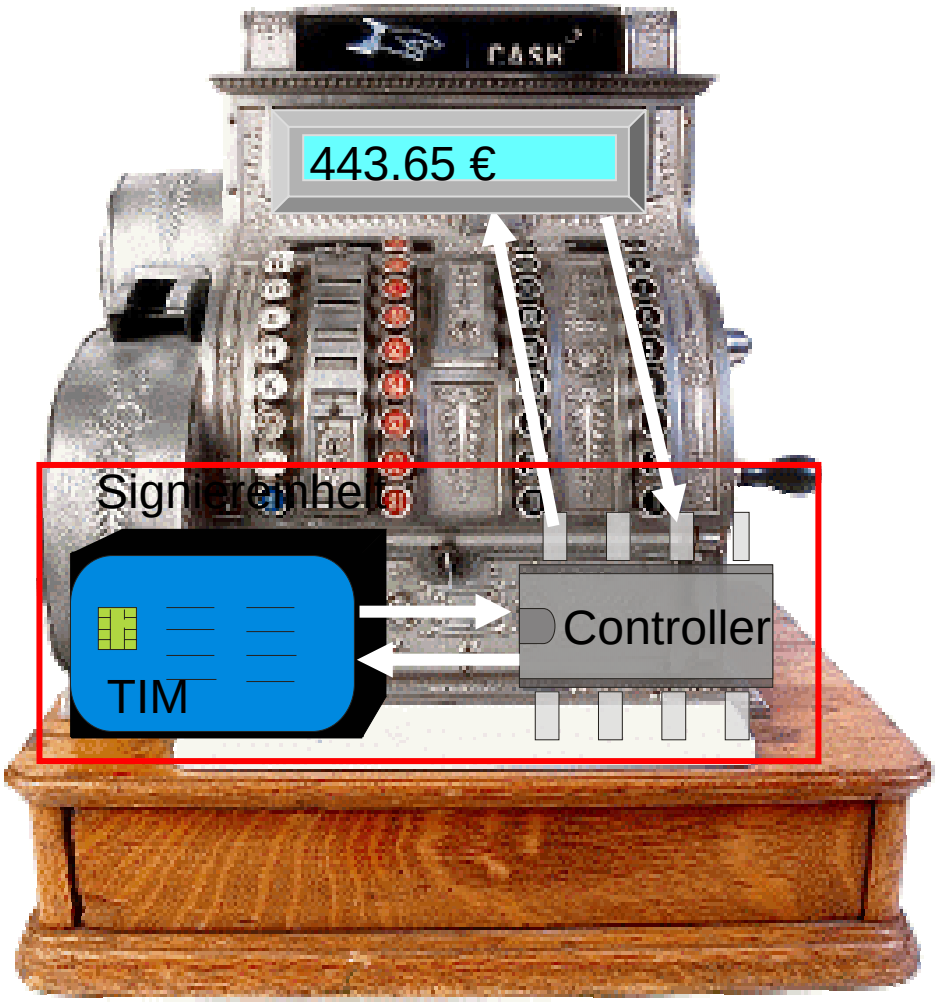
- Elektronisches Journal
- Gedruckter Beleg durch Signatur prüfbar
- Prüfung der Daten durch gängige Instrumente möglich
- Summenspeicher in Smartcard erlauben Ermittlung der wesentlichen Daten auch beim Verlust von Journaldaten
- Technisch relativ einfach – keine unnötig hohen (und teuren) Auflagen erforderlich

Anforderungen an Elektronisches Journal

Wichtige Anforderungen an das elektronische Journal:

- Festlegung eines sinnvollen Mindestumfangs (muss in allen Kassen machbar sein und ausreichende Informationen für effektive Prüfung enthalten)
- Auswertung ohne Rückgriff auf weitere Daten (z.B. Artikelstammdaten) möglich
- Kein herstellerspezifisches „Spezialwissen“ zur Auswertung des Journals erforderlich

Elektronische Registrierkasse mit TIM



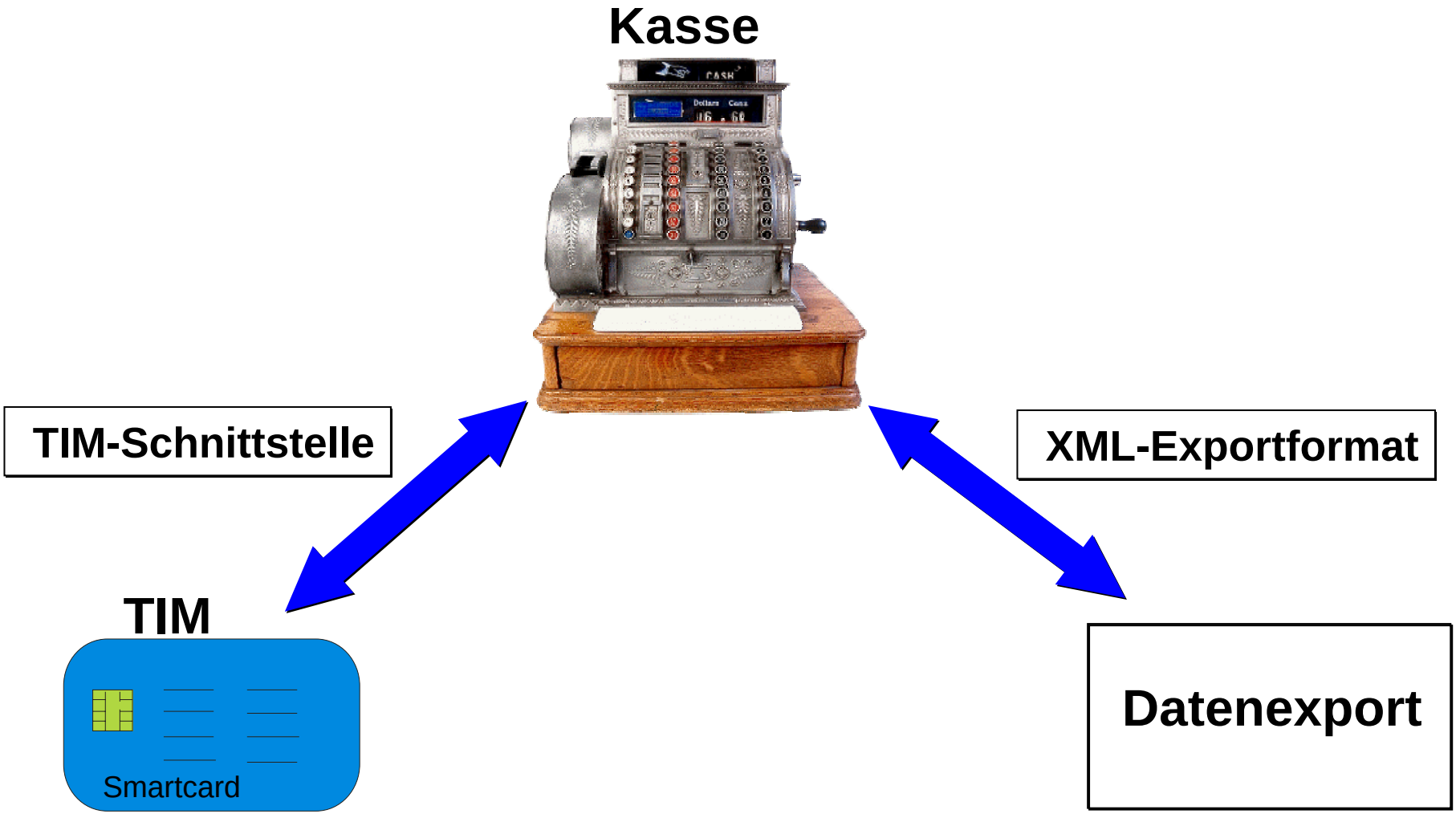
Signaturerstellungeinheit -TIM

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

Registrierkasse

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

Kasse Systemschnittstellen



Interne Abläufe in der Registrierkasse

Grundfunktionen TIM:

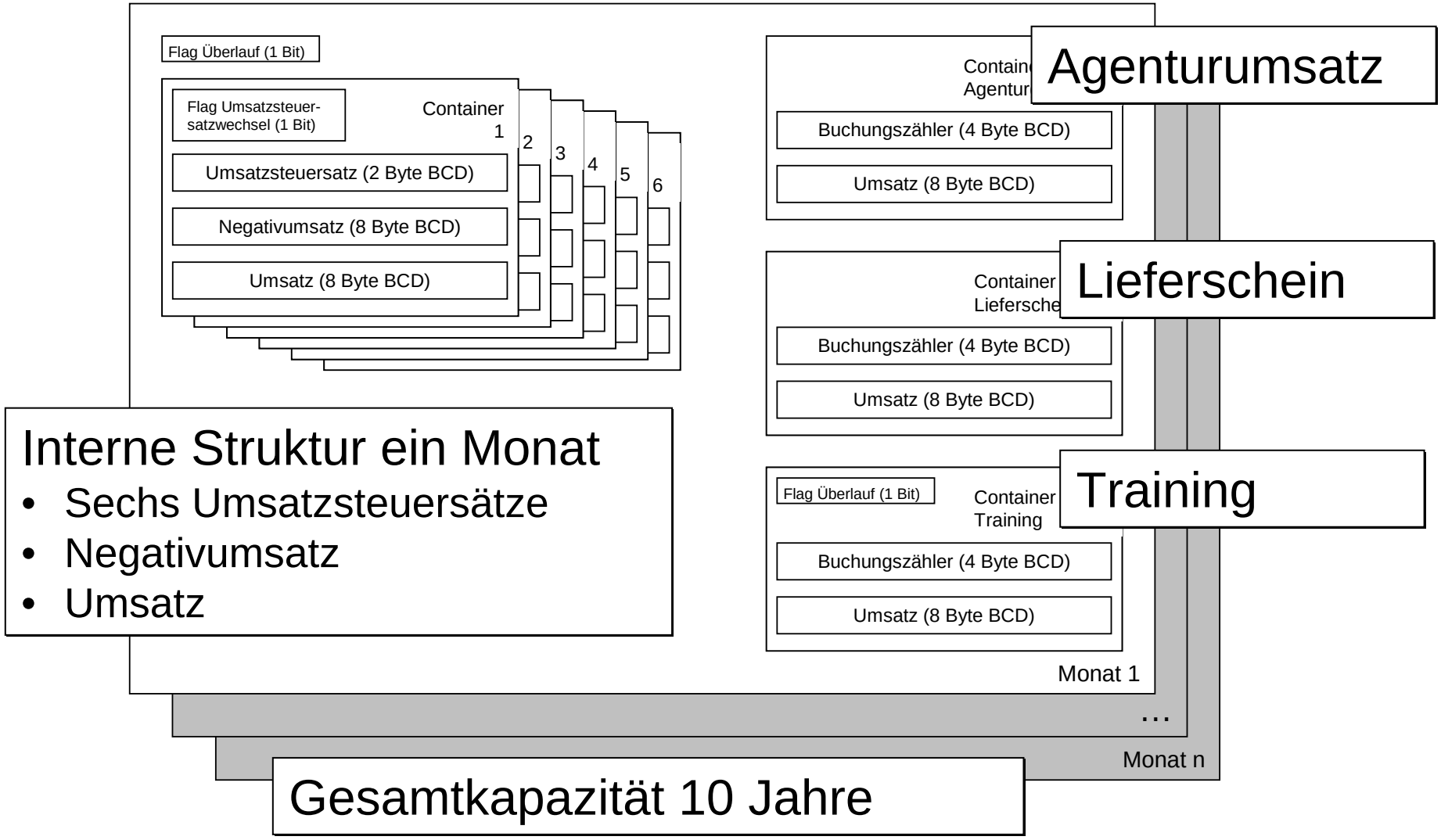
- Schlüsselspeicherung
- Datenplausibilisierung
- Sequenznummernvergabe
- Speichern von Umsatzdaten
- Signieren von Daten

Sicherheitsrelevante Funktionen laufen in der Smart Card (TIM) ab

Manipulation nur mit sehr hohem Aufwand möglich,

Restrisiko gering

Summenspeichermodell TIM



Eigenschaften Summenspeicher

Summenspeicher auf der Smartcard liefern Daten auch bei verlorenem Journal

- Der Speicher der Smartcard bietet Platz für mehrere Gruppen von Summenzählern:
  - Monatscontainer für 10 Jahre ab Kartenausgabe
  - Jeder Container enthält 6 Umsatzsteuersätze
  - Kontrollelemente gegen Überlauf, ….
- Jeder Container von Summenzählern enthält Verkäufe, Stornos, Trainingsbuchungen usw.

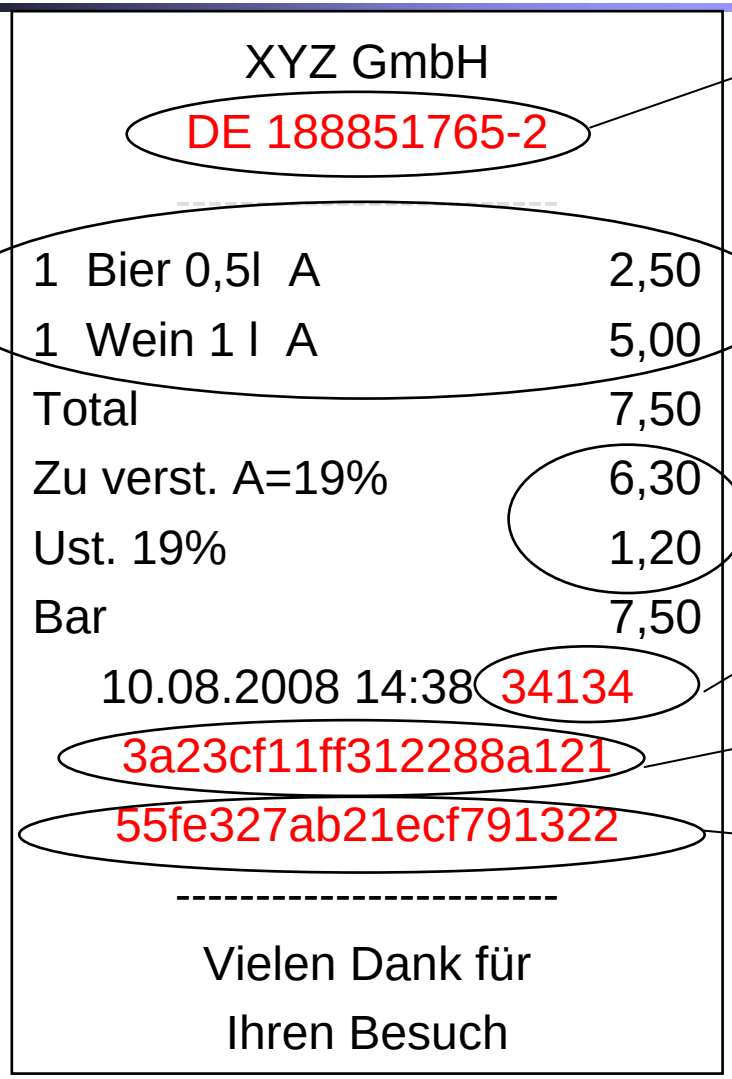
➡ „Eingebaute Datensicherung”

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

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

Erforderliche Weiterverarbeitung nach der Erfassung in der Kasse:

- 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
- Strukturierte Ablage der Daten
- Gezielter Zugriff auf die Daten
- Konvertierung der Daten in ein „prüfungsfähiges“ Format – INSIKA-XML-Exportschnittstelle

Behandlung von Tagesabschlüssen

Tagesabschlüsse beschleunigen die Daten-Verifikation

- Ein Tagesabschluss enthält die Summenspeicher aus der Smartcard in signierter Form
- I.d.R. kann auf eine Kontrolle der Buchungssignaturen verzichtet werden, wenn
  - die Summen aller Buchungen zwischen zwei Tagesabschlüssen mit der Differenz der Summenspeicher aus den Abschlüssen übereinstimmt und
  - die Anzahl der Buchungen der Differenz der Belegnummer zwischen zwei Tagesabschlüssen entspricht.

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 €**

Aufwand für Finanzbehörden

Zentrales Konzept

- Beschaffen der Smartcard (Ausschreibung)
- Ausgabe der Smartcard (Pflege der Datenbanken)
  bis zu zwei Millionen Karten
- Bereithalten der Zertifikate (LDAP-Server)
- Prüftätigkeiten (in Hoheit der Länder)

Lösungsansatz 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

Prüfaufwand/Prüfzeiten

- Vereinfachte Prüfabläufe
  Exakt festgelegte Schnittstellen und
  Datenformate ermöglichen automatisierte Prüfungen
- Prüftiefe wird erhöht
  Durch vollständige Aufzeichnung aller Buchungs- und Journaldaten steht eine sehr gute Datenbasis zur Verfügung
- Prüfzeiten werden verringert

Details im Vortrag Herr Wolff: „Prüfverfahren für Kassenbelege und aufgezeichnete Daten“

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

Nachteile/Befürchtungen/Fragen

- Sind die Kostenschätzungen der Gesamtlösung real??
- Bietet das System tatsächlich die dargestellte Sicherheit??
- Gibt es Hintertüren? Wer kann das System angreifen

Ausblick

- kommt nach 16:30 Uhr

Vielen Dank!