



RECHTLICHE UND TECHNISCHE ANFORDERUNGEN AN KASSENSYSTEME

**mit Blick auf die Nachweispflicht der
Vollständigkeit und „Unveränderbarkeit“
von Kassendaten**

zu Gast bei der
3. Bundestagung des

Arno Becker

Leitender Regierungsdirektor

Referatsleiter St 4
für Außenprüfungsdienste,
Steuerstrafrecht und Umsatzsteuer

bei der **Oberfinanzdirektion**
Nordrhein-Westfalen



am 16. und 17.08.2016 in





AGENDA



A. Anforderungen & Regierungsentwurf

- I. Fachlich-/funktionale Anforderungen
- II. Nichtfunktionale Anforderungen
- III. Umsetzung der Anforderungen im Regierungsentwurf
- IV. Inkrafttreten der Regelungen

B. INSIKA

- I. Tragbarkeit der Bedenken gegen das INSIKA-Konzept
- II. Grundlagen des INSIKA-Konzepts
- III. Umsetzung der Anforderungen im INSIKA-Konzept
- IV. Rechtssichere Umsetzbarkeit einer Public Key Infrastructure

C. Zusammenfassung und Fazit

D. Fragen und Diskussion



I. Fachlich-/funktionale Anforderungen



Regierungsentwürfe

Startseite > Service > Gesetze > Regierungsentwürfe

http://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetzentwuerfe_Arbeitsfassungen/2016-07-13-KassenG-und-technische-VO-Kassen.html

Steuern

13.07.2016

Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen

Artikel 1

2. § 146 Absatz 1 wird wie folgt gefasst:

„(1) ¹Die Buchungen und die sonst erforderlichen Aufzeichnungen sind **einzeln**, vollständig, richtig, zeitgerecht und geordnet vorzunehmen. ²Kasseneinnahmen und Kassenausgaben **sind** täglich festzuhalten.“

§ 146 Abs. 4 AO - „Unveränderbarkeit“

(4) ¹Eine Buchung oder eine Aufzeichnung darf nicht in einer Weise verändert werden, dass der ursprüngliche Inhalt nicht mehr feststellbar ist. ²Auch solche Veränderungen dürfen nicht vorgenommen werden, deren Beschaffenheit es ungewiss lässt, ob sie ursprünglich oder erst später gemacht worden sind.

VERFAHRENSRECHT

§ 158 AO - Beweiskraft der Buchführung

(Nur) die(jenige) Buchführung und die(jenigen) Aufzeichnungen des Steuerpflichtigen, die den Vorschriften der §§ 140 bis 148 entsprechen, sind der Besteuerung zugrunde zu legen, soweit nach den Umständen des Einzelfalls kein Anlass ist, ihre sachliche Richtigkeit zu beanstanden.

Formalprüfung ok



es sei denn

sachlich unrichtig



Paradigmenwechsel in der Abgabenordnung

a) Das Verfahrensrecht gibt die Anforderungen vor (WAS)

bisher:

b) die Umsetzung ist allein Sache des Kaufmanns (WIE)

neu:

c) Umsetzung wird durch die AO (teilweise) vorgegeben (SO!)

Fachlich-/funktionale Anforderungen

1. Datenintegrität

- a) einzeln
- b) richtig
- c) zeitgerecht
- d) geordnet
- e) „unveränderbar“
- f) KE und KA täglich

2. Datenvollständigkeit

- vollständig bei
Eingabe & Verarbeitung

3. Datenauthentizität

- dem Stpfl. sicher zuordbar

4. Definierte „Schnittstelle“

- a) jederzeit verfügbar § 146 VI 2 AO
- b) unverzüglich lesbar § 146 VI 2 AO
- c) maschinell auswertbar § 147 VI 2 AO

Schnelle (formale) Prüfbarkeit (§ 145 AO)

(1) ¹Die Buchführung muss so beschaffen sein, dass sie einem sachverständigen Dritten innerhalb angemessener Zeit einen Überblick über die Geschäftsvorfälle und über die Lage des Unternehmens vermitteln kann. ²Die Geschäftsvorfälle müssen sich in ihrer Entstehung und Abwicklung verfolgen lassen.

(2) Aufzeichnungen sind so vorzunehmen, dass der Zweck, den sie für die Besteuerung erfüllen sollen, erreicht wird.

= Rechtssicherheit für den Steuerpflichtigen durch die gesetzliche Rechtsvermutung des § 158 AO

II. Technik, Unternehmen, Kosten

II. Nicht-funktionale Anforderungen

1. hohes Sicherheitsniveau
2. geringes Ausfallrisiko
3. Sicherheit auch bei Datenverlusten
4. möglichst geringes Datenvolumen
5. keine Rechte Dritter
6. variabel ersetzbar bei Angriffen
7. keinerlei Gerätezertifizierung
8. enge Anlehnung an SigG-Verfahren
9. größenklassenunabhängig
10. Daten nutzbar durch Unternehmer
11. möglichst geringe Kosten
12. keinerlei Schulungsaufwand
13. Prüfungen müssen *sehr* schnell und möglichst unauffällig vonstatten gehen können
14. vom Prinzip her bei *allen* Kassen- und kassenähnlichen Systemen einsetzbar

Interdisziplinäres bzw. interprofessionelles Arbeiten erforderlich:

Steuerrechtler, Verwaltungsfachleute, Kassenhersteller, Kassenanwender und Sicherheitstechniker

- Lastenheft zur Beschreibung der fachlich-/funktionalen und non-funktionalen Anforderungen
- (sicherheits-)technisch saubere Umsetzung
- Evaluation
- betriebliche Tests
- Massenproduktion
- Start (gesetzlicher Anwendungszeitpunkt)



Regierungsentwurf

ge

- Geschäftsvorfälle
- und sonstige Vorgänge
- Vorgangsbeginn und -ende
- per Verkettung
- werden „gesichert“
- auf **Speichermodule** abgelegt
- keine Tagesabschlüsse

Wozu Vorgangsbeginn?

Kryptografie: Schlüsselinhaber?

doppelte Datenablage?

§ 146 Abs. 1 Satz 2 AO?

18. August 2016

III. PRÜFUNG 2



I. 2. Datenvollständigkeit



Regierungsentwurf

- Verkettung
- **aber:**
 - größtes Problem *aller* Lösungen = Nichteingabe
 - ⇒ Internet, aber Response größer 0,02 Sek.
 - ⇒ deutliche Erhöhung des Entdeckungsrisikos
 - keine Bonausgabepflicht (lediglich „auf Verlangen“)
 - keine zentrale Erfassung der Sicherheitseinrichtungen
 - Kassennachschau nicht systemisch, sondern dient vorrangig der Datenprüfung



III. PRÜFUNG 3

I. 3. Datenauthentizität

- dem Stpfl. sicher zuordbar

Regierungsentwurf

- keine (zentrale) Erfassung der Sicherheitseinrichtungen
- Erfassung ausgegebener Module durch Hersteller nicht vorgesehen

I. 4. Definierte „Schnittstelle“

- a) jederzeit verfügbar
- b) unverzüglich lesbar
- c) maschinell auswertbar

Regierungsentwurf

Dauer/Geschwindigkeit des Datenimports

- *sämtliche* Eingaben in die Kasse
- Verkettungen
- Länge kryptografischer Schlüssel nicht „vorgegeben“
- 30 Minuten für eine Kassennachschau (bei durchschnittlich zwei Kassen pro Betriebsstelle)?

Prüfbarkeit der Daten

- Konzept zur Trennung „sämtlicher Kasseneingaben“ zwecks Prüfung durch Bp nicht ersichtlich
- Wer prüft, ob sich Sicherheitsmodul zum Zeitpunkt der Prüfung noch im Zustand der Zertifizierung befindet?



III. PRÜFUNG 4



II. Non-funktionale Anforderungen

1. hohes Sicherheitsniveau
2. geringes Ausfallrisiko
3. Sicherheit auch bei Datenverlusten
4. möglichst geringes Datenvolumen
5. keine Rechte Dritter
6. variabel ersetzbar bei Angriffen
7. keinerlei Gerätezertifizierung
8. enge Anlehnung an SigG-Verfahren
9. größenklassenunabhängig
10. Daten nutzbar durch Unternehmer
11. möglichst geringe Kosten
12. keinerlei Schulungsaufwand
13. Prüfungen schnell und unauffällig
14. *alle* Kassen(ähnlichen) Systeme

Regierungsentwurf

1. Sicherheitsmodul: CC EAL 4+
Speichermodule } Konformitätserklärungen
Schnittstelle } der Hersteller genügen.
2. abhängig von Herstellerlösung
3. keine Summenspeicher oder Sequenzzähler
4. sämtliche Eingaben in die Kasse, Verkettungen, keine vorgegebenen Schlüssellängen
5. doch, da „technologieoffen“ => Kosten!!
6. abhängig von Herstellerlösung
7. verbal ja, aber technisch zweifelhaft
8. „technologieoffen“
9. „technologieoffen“
10. Daten im „Speichermodule“ sicherlich nicht
11. 10 Euro/Modul: Echtzeituhr, Verarbeitung „offener Vorgänge, bei mehreren Kassen
12. „technologieoffen“
13. Kassennachschau zu üblichen Geschäftszeiten statt „Feldüberwachung“
14. sicher nicht

III. PRÜFUNG 5

Unvermutete Kassen-Nachschau nach § 146b AO-E

Betriebsprüfung, guten Tag!
Unvermutete Kassen-Nachschau.
Bitte Daten und Orga-Unterlagen.



Zentralverband des
Deutschen Bäckerhandwerks e.V.

Rundschreiben Berlin, 15. Juli 2016
Nr. 023/2016 Az.: Be/au 41-00

Regierungsentwurf zur Einführung
manipulationssicherer Kassensysteme

I. Bewertung

1. Der Regierungsentwurf greift erfreulicherweise mehrere wichtige Forderungen des ZV auf, die er zusammen mit dem ZDH und anderen Wirtschaftsverbänden an das BMF und die Politik adressiert hatte:

Betriebsprüfung, guten Tag!
Unvermutete Kassen-Nachschau.
Bitte Daten und Orga-Unterlagen.



Donnerstagmittag um 12:00 Uhr in der Frittenschmiede nebenan:

Betriebsprüfung, guten Tag!
Unvermutete Kassen-Nachschau.
Bitte Daten und Orga-Unterlagen.





IV. INKRAFTTRETEN

tritt zwar nach Verkündung inkraft,

a b e r :

Anwendungsregelung in § 30 EGAO

erstmals für Kalenderjahre anzuwenden, die nach dem 31. Dezember 2019 beginnen. (**Satz 1**)

E X K U R S :



Bundesministerium
der Finanzen

Sollte jemand im Hinblick auf das BMF-Schreiben (vom 26.11.2010) eine Kasse angeschafft haben, die zwar den Anforderungen des BMF-Schreibens genügt, jedoch nicht den neuen gesetzlichen Anforderungen (RefE v. 18.03.2016), werden wir hierfür eine angemessene Lösung finden, wenn die Kasse nicht mit einer technischen Sicherheitseinrichtung im Sinne des Referentenentwurfs aufrüstbar ist.

Ich denke, es sollte jedoch Einigkeit darüber bestehen, dass nach nunmehr sechs Jahren mindestens der Standard des o.g. BMF-Schreibens von der Finanzverwaltung vorausgesetzt werden kann.

Satz 3:

Übergangsregelung

26.11.2010

01.01.2020

31.12.2022



Kasse angeschafft, die

- Anforderungen des BMF v. 26.11.2010 entspricht
- aber: bauartbedingt *nicht* nach § 146a aufrüstbar

Weiterverwendung

B. DAS INSIKA-KONZEPT

I. Geäußerte Bedenken

- Entspricht nicht den europäischen Sicherheitsanforderungen
- Smartcard-Vergabe und -Verwaltung aufwändig
- Rechtliche Risiken bei Einbindung einer autorisierten Stelle
- Kostenintensiver durch Entwicklung der Profile durch FinVerw
- Anschaffung neuer Drucker erforderlich
- Kostenintensiver durch Smartcard und Kartenleser
- Jede Registrierkasse benötigt eine Smartcard
- Verfassungsrechtliche Bedenken

... u n d s c h l i e ß l i c h ...



VERALTET ...



Teile einer Gesamtlösung	INSIKA	sichere Websites (https-Protokoll) als Analogie
a) Grundkonzept	▪ digitale Signatur von Geschäftsvorfällen ▪ Sequenzzähler ▪ Summenspeicher	▪ Verschlüsselung der Transportschicht ▪ Authentifizierung
b) Standardisierungen (zur praktischen Nutzbarkeit)	▪ vorgegebene Schnittstellen ▪ vorgegebene Datenformate	das eigentliche https-Protokoll
c) kryptographische Algorithmen	Hash- und Signaturverfahren	▪ Verschlüsselungsalgorithmen ▪ Signaturalgorithmen
d) Implementierung der Sicherheitsverfahren	Smartcard, PKI, Verifikation	▪ Zertifikate ▪ Krypto-Bibliotheken
e) „Rest“ des Systems	Eigentliches System ▪ Kassensystem, ▪ Taxameter oder ▪ sonstige kassenähnlichen Geräte	▪ Rechner ▪ Betriebssystem ▪ Webbrowser ▪ ...

II. Grundlagen des INSIKA-Konzepts

Die Signaturerstellungseinheit

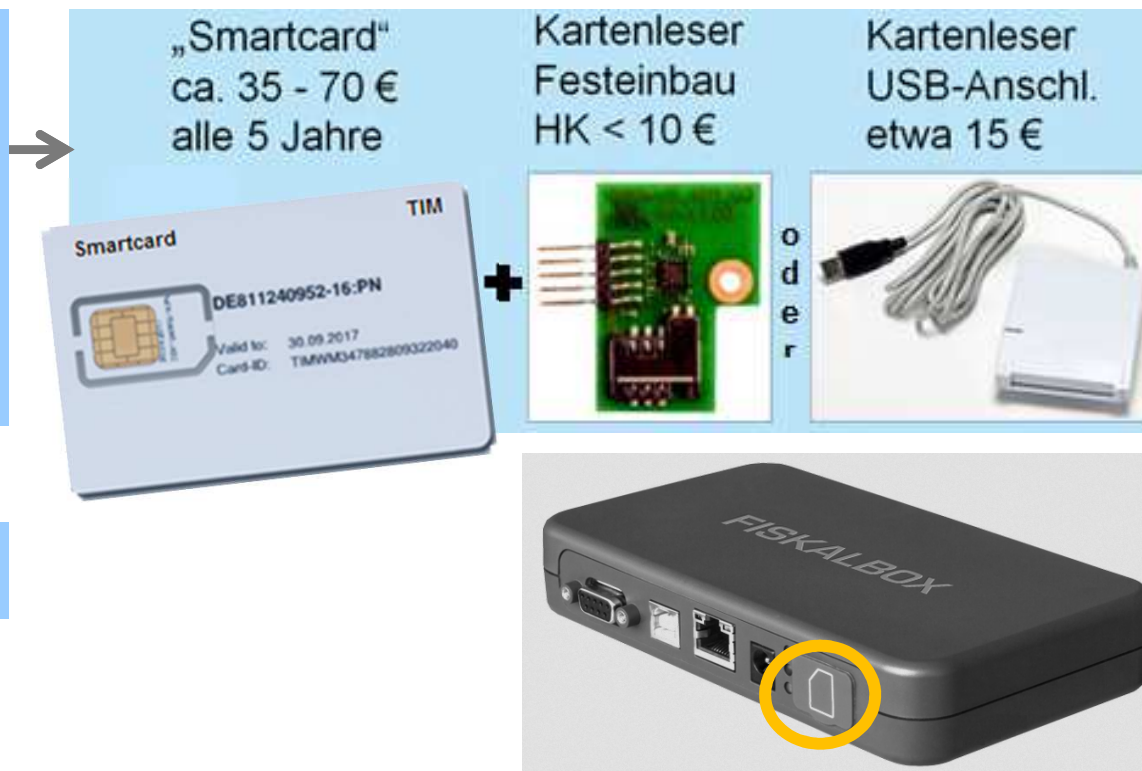
Erforderlich sind ...



mit

- Einzelaufzeichnung
- Speichermöglichkeit und
- Schnittstelle (Datenexport)

+ Zuwegung





Was wird wie signiert?

Daten-Integrität

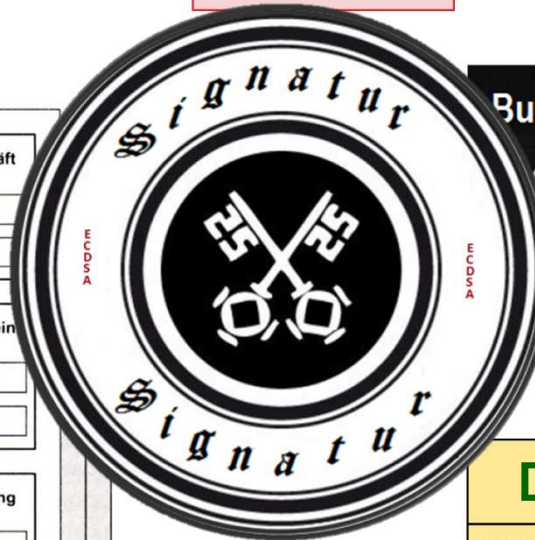
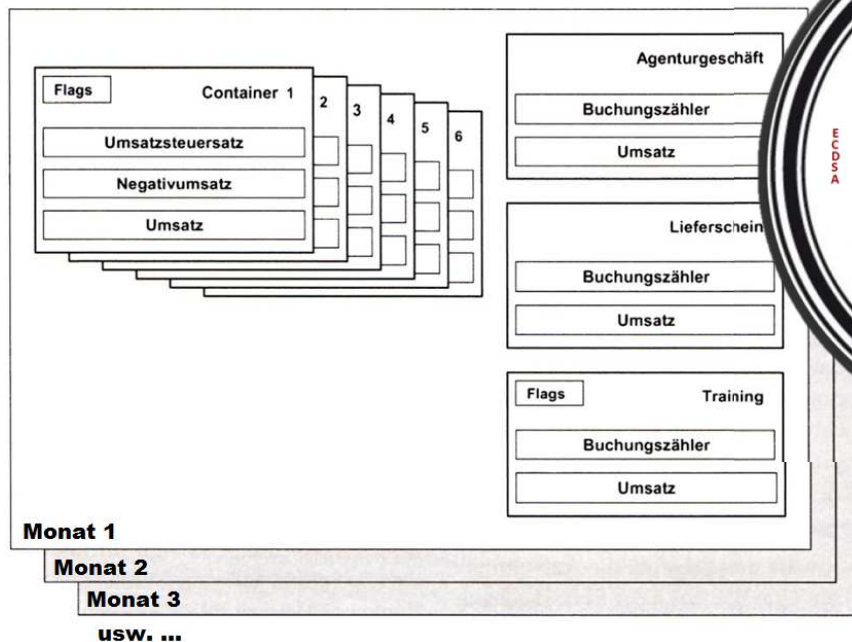
„Profildaten“ des „Geschäftsvorfalles“

Baguette		
2 x 0,89 € =	B	1,78 €
Japan Sencha		
0,12 kg x 49,90 €/kg =	B	5,99 €
Mineralwasser		
2 x 0,69 € =	A	1,38 €
Pfandartik.Einweg		
2 x 0,25 € =	A	0,50 €
Leergut		
	A	-0,25 €
Summe		9,40 €

Hashwert

Sequenzzähler

Summenspeicher
(„Unverlierbarkeit“)



Buchungsdaten

3217

0459

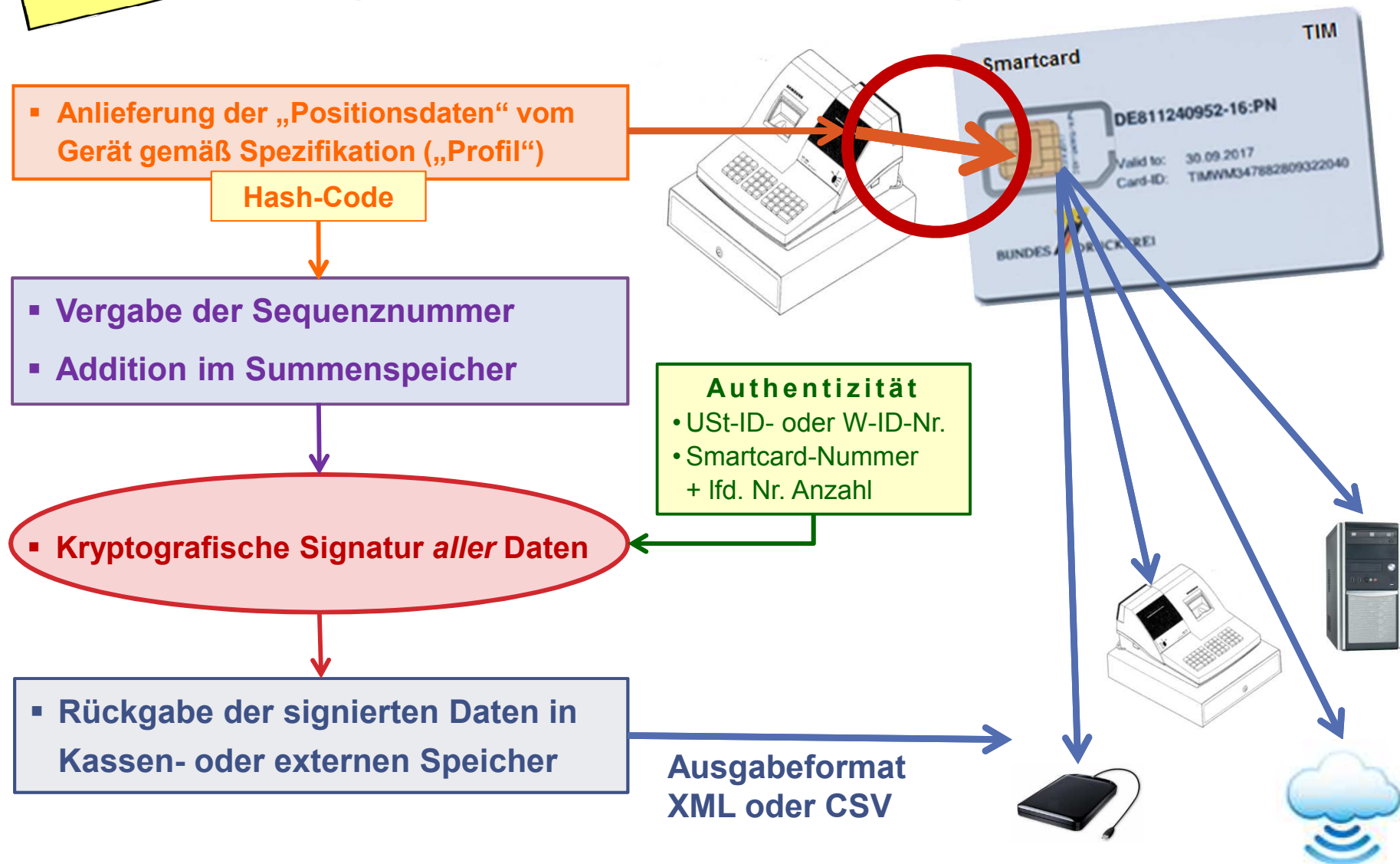
Tagesabschluss

Daten-Authentizität

USt-Identifikationsnummer
Card-Identifikationsnummer
(inkl. lfd. Nr. Anzahl von Cards)



Funktionsweise der Signaturerstellungseinheit



Welche Buchungsdaten werden i.E. signiert?



XYZ GmbH, Abbestr. 2, 10587 Berlin				Identifikationsmerkmal (USt-ID-Nr.)
DE 081508150-14				Card-Ident-Nr. + Anzahl
-----				Positionsdaten (indirekt durch deren Hashwert – SHA-1)
Frühstück Paris	A	5,98		
Kaffeebohnen Arabica				
0,253 kg x 9,99€/kg =	B	2,53		
Kaminholz Buche	A	14,98		

Summe		23,49		
USt.Satz	Brutto	Netto	USt.	Umsatz (je USt-Satz)
A 19%	20,96	17,61	3,35	
B 7%	2,53	2,36	0,17	
Hash				Hashwert der Positionsdaten
5FE5-WJ6Q-MURZ-FNUZ-UQJJ-WI				
Signatur				Signatur
U5Y4-VCBB-IGXM-SCB6-6MOF-O				
VETD-3ELO-T77N-QTA4-T6EG-T				
BXV6-4VYC-TURZ				
SEQ:	388			Sequenznummer
Bediener: Fuchs 12.02.2009 13:27:36				Bediener-ID, Datum, Uhrzeit
Vielen Dank für Ihren Einkauf!				



Kassennachschau als Systemprüfung

- ✓ Wichtigste Belegdaten werden auf den Bon gedruckt
- ✓ Verifikation mit jedem Smartphone möglich
- ✓ Kassen-Nachschau (= Systemprüfungen) in kurzer Zeit durchführbar



online oder offline

Gut & Lecker GmbH
Abbestr. 2, 10587 Berlin
INSIKA_TEST_PTBW ③

Baguette
2 x 0,89 € = B 1,78 €
Japan Sencha
0,12 kg x 49,90 €/kg = B 5,99 €
Mineralwasser
2 x 0,69 € = A 1,38 €
Pfandartik.Einweg
2 x 0,25 € = A 0,50 €
Leergut A -0,25 €

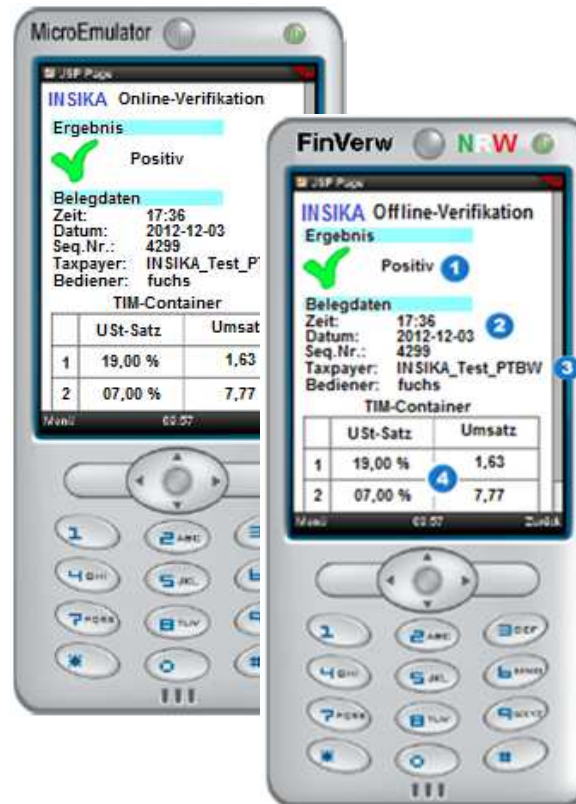
Summe 9,40 €

Steuer%	Brutto	Netto	USt.
A 19.0	1,63 € ④	1,37 €	0,26 € ④
B 7.00	7,77 €	7,26 €	0,51 €

SeqNr:4299 Bediener:Fuchs 03.12.2012 17:36
③ ②



Vielen Dank für Ihren Besuch!



- 1 Verifikation positiv
- 2 Zeit identisch
- 3 Identifikation identisch
- 4 Betrag identisch

= Beleg signiert
= jede Änderung und
Löschung sichtbar

Umsetzung der Anforderungen durch das **INSIKA-Konzept**

I. Funktionale Anforderungen

I. 1. Datenintegrität

- a) einzeln
- b) richtig
- c) zeitgerecht
- d) geordnet
- e) „unveränderbar“
- f) KE und KA täglich

I. 2. Datenvollständigkeit

I. 3. Datenauthentizität

- dem Stpfl. sicher zuordbar

I. 4. Definierte „Schnittstelle“

- a) jederzeit verfügbar
- b) unverzüglich lesbar
- c) maschinell auswertbar

II. Non-funktionale Anforderungen

1. hohes Sicherheitsniveau
2. geringes Ausfallrisiko
3. Sicherheit auch bei Datenverlusten
4. vglws. geringes Datenvolumen
5. keine Rechte Dritter
6. variabel ersetzbar bei Angriffen
7. keinerlei Gerätezertifizierung
8. enge Anlehnung an SigG-Verfahren
9. größenklassenunabhängig
10. Daten nutzbar durch Unternehmer
11. geringe Kosten
12. keinerlei Schulungsaufwand
13. Prüfungen schnell und unauffällig
14. *alle Kassen(ähnlichen) Systeme*

IV. INSIKA gibt es übrigens schon ...

Digitaler Tachograph



Kraftfahrt-Bundesamt



10.3.2004

De

Amtsblatt der europäischen Union

L 71/3

Verordnung (EG) Nr. 432/2004 DER KOMMISSION vom 5. März 2004

zur achten Anpassung der Verordnung (EWG) Nr. 3821/85
des Rates über das Kontrollgerät im Straßenverkehr an den
technischen Fortschritt

Vergabe und Einsatz der Signaturerstellungseinheit

Mittwoch, 16. Juli 2008

 **Bundesministerium für Arbeit und Soziales**

Bundesministerium für Arbeit und Soziales, 53107 Bonn

Schnellbrief
Bundeskanzleramt

Auswärtiges Amt

Bundesministerium des Innern

Bundesministerium der Justiz

Bundesministerium der Finanzen

Seite 2 von 56

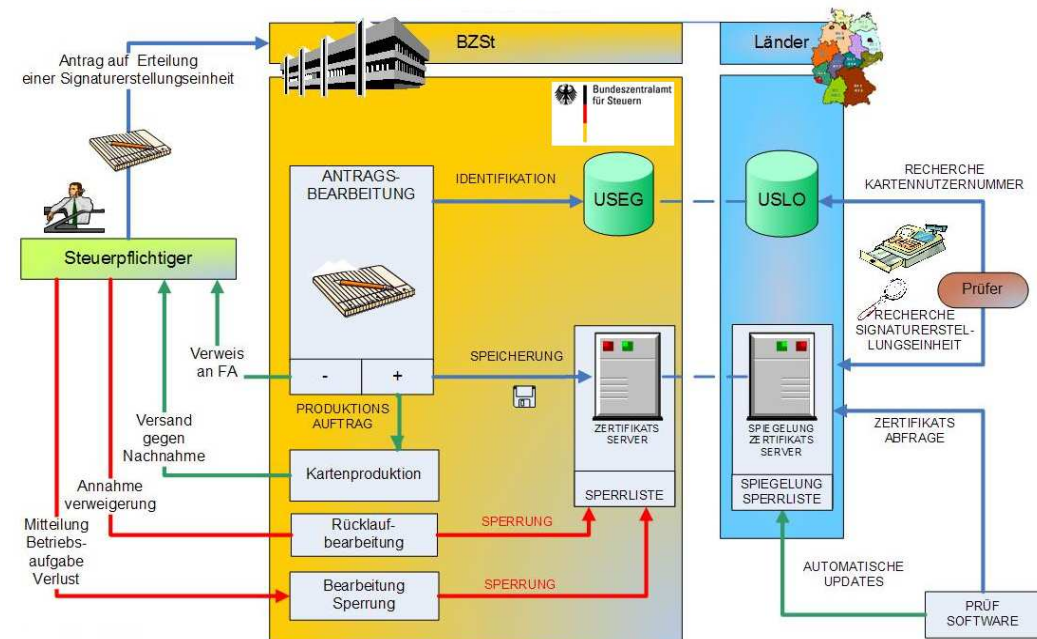
Die Übersendung erfolgt ausschließlich per Mail

Zweites Gesetz zur Änderung des Sozialgesetzbuches Viertes Buch (SGB IV) und anderer Gesetze (2. SV-ÄndG)
Anlagen: -2-

Hurnik, Ivo
ORR
Referent

HAUSANSCHRIFT Rochusstraße 1, 53123 Bonn
POSTANSCHRIFT 53107 Bonn
TEL +49 (0)228 99 527-2177
FAX +49 (0)228 99 527-1177
E-MAIL Iva2@bmas.bund.de
INTERNET www.bmas.bund.de

Bonn., 5. Juni 2008
AZ Iva 2 - 41645-13/2



ZUSAMMENFASSUNG UND FAZIT

Regierungsentwurf

- ohne „KassenSichV“
- lediglich grobes Rahmengerüst
- Datenintegrität zweifelhaft
- Datenvollständigkeit nicht gewährleistet
- keinerlei Datenauthentizität
- PKI wäre problemlos zu installieren
- Prüfbarkeit durch Bp höchst fraglich
- 10 € je Sicherheitsmodul unwahrscheinlich
- Keine Daten-, Rechts- und Kostensicherheit
- Übergangsfristen zu lang
- Keine Anwendbarkeit der Lösung auch auf kassenähnliche Systeme

INSIKA-Konzept

- in sich aufbauend und geschlossen
- langjährig erfolgreich erprobt
- Datenintegrität, -authentizität und -vollständigkeit konzeptionell gewährleistet
- Import IDEA: 1 Kasse pro 1 Jahr = 1 Minute
- Datenausgabe in festgelegtem Format
- Prüfbarkeit durch Bp garantiert
- dadurch Rechtssicherheit für Unternehmen
- Kosten überschaubar
- bei Kassen, Taxametern und Geldspielgeräten kurzfristig einsetzbar
- PKI rechtssicher umsetzbar

ICH DANKE FÜR IHRE AUFMERKSAMKEIT ...

... und wünsche uns
noch eine angeregte
Diskussion



... wir bleiben dran ...