INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Analyse des Referentenentwurfs eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen vom 18. März 2016

Stand: 5. April 2016

Das Bundesministerium der Finanzen (BMF) hat am 18. März 2016 einen Referentenentwurf für ein Gesetz zur Manipulationssicherung für Registrierkassen sowie für eine dazugehörige technische Verordnung veröffentlicht. Das in den Entwürfen beschriebene Verfahren verfolgt das gleiche Ziel wie das INSIKA-Verfahren. Dieses wird jedoch in den Begründungen ausdrücklich als ungeeignet eingestuft und ausgeschlossen.

Auch wenn die Beschreibung des Verfahrens in den Entwürfen allgemein gehalten ist, erschließen sich doch die Grundzüge der technischen und praktischen Rahmenbedingungen, so dass sich die daraus resultierenden Lösungen relativ klar beschreiben lassen. Deren Grundstruktur und die Konsequenzen daraus werden hier analysiert.

Insgesamt ist der Gesetzentwurf grundsätzlich ungeeignet, die vom BMF selbst gesteckten Ziele zu erreichen. Viele Daten und Aussagen in den Entwürfen sind im Übrigen falsch oder irreführend.

Ausgangssituation

Am 18. März 2016 hat das BMF einen Referentenentwurf mit dem Titel *Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen* zusammen mit dem Entwurf einer darauf basierenden Verordnung veröffentlicht.[1]

Diese Entwürfe sollen die seit langem geforderte Manipulationssicherheit für Registrierkassen sicherstellen sowie Rechtssicherheit für alle Beteiligten schaffen.

Laut Text des Gesetzentwurfs dient das neu einzuführende Sicherungsverfahren zur „Sicherstellung der Integrität und Authentizität sowie der Vollständigkeit der elektronischen Aufzeichnung".

Eckpunkte des Verfahrens

Im Folgenden ist die im Entwurf skizzierte Lösung beschrieben. Diese wird dort als „Zertifizierungsverfahren" bezeichnet. Da dies irreführend ist,[2] wird in dieser Analyse die Bezeichnung „SE-Verfahren" (SE = Sicherheitseinrichtung) verwendet.

Die hier dargestellten Eigenschaften des Verfahrens ergeben sich entweder direkt aus den Gesetzes- und Verordnungstexten, den Erläuterungen oder aus dem Kontext.

Grundlagen

Betroffene Systeme

Im Entwurf der Verordnung werden ausdrücklich nur Registrierkassen erwähnt – Taxameter, Geldspielgeräte, Wett-Terminals usw. sind nicht genannt. Eine Abgrenzung der Registrierkassen von anderen Systemen erfolgt in den Erläuterungen zur Verordnung – unklar bleibt aber beispielsweise, ob Barverkaufs-Softwaremodule einer Warenwirtschafts- oder Unternehmenssoftware von den Regelungen betroffen sind.

Eine Kassenpflicht wird im Entwurf ausdrücklich ausgeschlossen.

Technik

Der Kern des SE-Verfahrens wird im neuen einzuführenden § 146a AO definiert: „Diese zertifizierte technische Sicherheitseinrichtung muss aus einem Sicherheitsmodul, einem Speichermedium und einer digitalen Schnittstelle bestehen."

Aus dem Kontext (z.B. „nur ein Sicherheitsmodul an der Hauptkasse") geht hervor, dass es sich dabei um eine Hardware handelt. Durch das Sicherheitsmodul soll jede digitale Aufzeichnung protokolliert werden (Form und Inhalt der Protokollierung werden jedoch offen gelassen). Dieses muss eine besonders geschützte Echtzeituhr beinhalten,

[1] Abrufbar auf der Website des BMF unter der Adresse http://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Referentenentwuerfe/2016-03-18-KassenG-und-technische-VO-Kassen.html

[2] Ein „Zertifizierungsverfahren" ist ein Prozess, der die Einhaltung vorher formulierter Anforderungen überprüft und dadurch zu einem zertifizierten System führt.

da es gemäß § 2 des Entwurfs der Verordnung Uhrzeiten von Geschäftsvorfällen „manipulationssicher festlegen“ soll.

Die Aussage „Ein Speichermedium ist ein Objekt in der digitalen Datenverarbeitung zum Speichern von Daten“ schafft im Detail wenig Klarheit, allerdings kann es sich hier ebenfalls nur um Hardware handeln. Das Speichermedium soll alle „elektronischen Grundaufzeichnungen“ aufnehmen.

Die digitale Schnittstelle soll die zu prüfenden Daten liefern. Ob es sich hier um eine reine Definition von Datenformaten oder auch um die Festlegung von Inhalten, Protokollen bzw. physischen Schnittstellen handelt, bleibt unklar.[3]

Alle drei Komponenten zusammen bilden die technische Sicherheitseinrichtung.

Einige Aussagen bleiben völlig unverständlich, wie z. B. „Eine Transaktionsnummer […] ist ein Einmalpasswort. Ein Einmalpasswort ist ein Kennwort zur Authentifizierung.“

Bei aller Unschärfe der Beschreibung läuft die Lösung jedoch am ehesten auf ein „Fiskalbox-System“ ähnlich denjenigen in Belgien oder Schweden hinaus.[4]

Werden Daten außerhalb des Aufzeichnungssystems in einem „externen elektronischen Archiv“ abgelegt, soll dieses Archiv „manipulationssicher“ sein, müsste also auch zertifiziert werden. Daraus lässt sich folgern, dass die Daten selbst nicht abgesichert werden[5] – sonst wäre ein „manipulationssicheres Archiv“ nicht erforderlich. Wie die Daten während der Übertragung in das Archiv gegen Manipulationen gesichert werden sollen, bleibt offen.

Zulassungsverfahren

Die technische Sicherheitseinrichtung soll durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert werden. Dieses soll hierzu die „technischen Richtlinien und Sicherheitsprofile für die technische Sicherheitseinrichtung“ erstellen und es „übernimmt die Zertifizierung und die Fortschreibung der Sicherheitsprofile.“ Im Verordnungsentwurf wird demgegenüber von „Schutzprofilen“ gesprochen. Damit ist unklar, ob eine Zertifizierung nach Common Criteria oder auf Basis einer technischen Richtlinie erfolgen soll.[6]

Die für eine BSI-Zertifizierung erforderliche Evaluierung bzw. Prüfung aller sicherheitsrelevanten Elemente[7] findet keine Erwähnung, obwohl Aufwand und Kosten der Evaluierungen die Zertifizierungskosten um ein Vielfaches übersteigen.

Aus dem Entwurf geht an vielen Stellen hervor, dass keine Bauartanforderungen an die Registrierkassen vorgesehen sind. Mithin existiert lediglich die Anforderung, die beschriebene Sicherheitseinrichtung zu verwenden. Zwar ist das BMF nach § 146a Abs. 2 AO „ermächtigt […] die Anforderungen nach Absatz 1 an […] die elektronischen Aufzeichnungssysteme […] zu bestimmen“ wobei „die Einhaltung dieser Anforderungen […] durch Zertifizierung vom Bundesamt für Sicherheit in der Informationstechnik festzustellen“ ist. Im Entwurf der Technischen Verordnung wird das Konzept einer Zertifizierung der Aufzeichnungssysteme jedoch nicht aufgegriffen. Daher wird in dieser Analyse von einer Zertifizierung nur der Sicherheitseinrichtung ausgegangen – sollte diese Annahme nicht zutreffend sein, wären die Aufwandsschätzungen sehr deutlich zu erhöhen.

Beschaffung der Sicherheitseinrichtungen

Eine zentrale Ausgabe oder Registrierung der Sicherheitseinrichtungen (bzw. Sicherheitsmodule) ist nicht vorgesehen. So können diese von den Herstellern der Sicherheitseinrichtungen bzw. der Registrierkassen ohne weitere Erfassung oder Überprüfung direkt geliefert werden.

Da ausdrücklich festgestellt wird, dass keine zentrale autorisierte Stelle eingerichtet werden soll, muss die Verwaltung der kryptografischen Schlüssel bzw. Zertifikate (sofern solche zum Einsatz kommen sollten) in der Verantwortung der Hersteller liegen.

---

[3] Die Beschreibung aus §4 des Entwurfs der Verordnung würde auch auf den heutigen „Datenbeschreibungsstandard für die Datenträgerüberlassung“ zutreffen. Dieser hat für alle Beteiligten nicht zu einer größeren Erleichterung bei Prüfungen geführt.

[4] Siehe auch *Sichere Registrierkassen – internationale Fallbeispiele* (http://www.insika.de/images/stories/INSIKA/Sichere_Registrierkassen_international.pdf)

[5] Eine Absicherung der Daten könnte wie beim INSIKA-Verfahren durch Signaturen erfolgen, wodurch sich Veränderungen zweifelsfrei erkennen lassen. Speichermedien und Archivsysteme müssen bei diesem Ansatz nicht „manipulationssicher“ sein.

[6] Die beiden Varianten bedingen einen deutlich unterschiedlichen Aufwand.

[7] Die Zertifizierung ist ein eher formaler Akt, der auf einer durch Dienstleister durchgeführte Evaluierung aufbaut.

Praktische Nutzung

Anwendung

Für die Anwender ist das System weitgehend unsichtbar.

Belege

Eine Belegpflicht ist in den Änderungen der Abgabenordnung nicht erwähnt. Im Begründungsteil wird ausdrücklich darauf hingewiesen, dass keine Belegausgabepflicht besteht. Dies wird in dem den Entwürfen beigefügten Schaubild zudem besonders hervorgehoben.

Kassennachschau

Die Kassennachschau nach dem Entwurf für den § 146b AO ist erkennbar nicht als bloße System- bzw. Verfahrensprüfung angelegt; vielmehr wird in Absatz 2 Satz 2 dieser Norm – ebenso wie im Rahmen einer Betriebsprüfung nach § 146 Abs. 5 und § 147 Abs. 6 Satz 2 AO – vollständiger Datenzugriff (Z 3, also Datenträgerüberlassung) gewährt. Ob diese Form des Datengriffs ausreichend ist, um den Zweck der Kassennachschau erreichen zu können, wird von der konkreten Ausgestaltung des Verfahrens abhängen.[8]

Auch die Erläuterungen zum Entwurf des § 146b Abs. 2 verdeutlichen den Aufwand: „Auf Anforderung des Amtsträgers sind das Zertifikat und Systembeschreibungen zum verwendeten Kassensystem vorzulegen, d. h. es sind Bedienungsanleitungen, Programmieranleitungen und alle weiteren Anweisungen zur Programmierung vorzulegen. Darüber hinaus sind Auskünfte zu erteilen."

Der wesentliche Unterschied zur Betriebsprüfung dürfte also das fehlende Erfordernis einer vorherigen Anordnung sein.

Prüfung

Eine Prüfung basiert vor allem auf Daten, die von der Schnittstelle der Sicherheitseinrichtung geliefert werden. Inwieweit es eine Erleichterung der Prüfung durch eine Standardisierung der Daten geben wird, ist unklar.

Sicherheitsaspekte

In den folgenden Abschnitten werden die wesentlichen Sicherheitsaspekte des SE-Verfahrens beleuchtet.[9]

Kryptografie und Hardware

Bei einer Definition der Sicherheitsanforderungen durch das BSI ist davon auszugehen, dass kryptografische Algorithmen sowie die Hardware des Sicherheitsmoduls dem Stand der Technik entsprechen werden.

Für erfolgreiche Angriffe auf dieser Ebene sollte daher nur ein geringes Restrisiko bestehen.

Schlüsselverwaltung

Eine Schlüsselverwaltung, die nicht in der Hand einer vertrauenswürdigen Stelle liegt, macht jedes kryptografische Sicherheitsverfahren grundsätzlich unsicher.[10]

Die Authentizität der zu sichernden Daten kann damit nicht gewährleistet werden.

Belege

Da keine technische Lösung einen Menschen zur Eingabe von Daten in ein System zwingen kann, lässt sich eine Prüfung vollständiger Verbuchung aller Einnahmen bei elektronischen Kassen gemäß § 146 Abs. 1 AO durch die Finanzverwaltung nur bei verpflichtender Ausgabe eines Belegs mit einem Sicherheitsmerkmal leicht und zuverlässig prüfen.

Der Verzicht auf eine Beleg(ausgabe)pflicht hat deshalb zur Folge, dass eine korrekte Nutzung des Systems nur durch einen Datenzugriff überprüft werden kann.

Der Kontrollaufwand steigt damit ganz erheblich an und das Entdeckungsrisiko für eine Nicht-Nutzung bzw. Nicht-Eingabe ist entsprechend geringer.

Verzeichnis der Sicherheitsmodule

Eine zentrale Ausgabe oder Registrierung der im Einsatz befindlichen Sicherheitsmodule sieht der Referentenentwurf des BMF ebenfalls nicht vor. Folglich würde nicht bekannt sein, welche Sicherheitsmodule bei welchem Anwender im Einsatz sind.

Damit wird das Erkennen von „Zweitkassen" – also Systemen, die zwar eine Sicherheitseinrichtung benutzen, deren Daten bei einer Prüfung

---

[8] So ist eine Prüfung der korrekten Anwendung des Systems ggf. nur mit einem unmittelbaren Zugriff (Z 1) möglich.

[9] Für nicht mit dem Thema vertraute Leser wird *Wie werden Registrierkassen und Taxameter sicher?* empfohlen (http://www.insika.de/images/stories/INSIKA/Sichere_Registrierkassen_und_Taxameter.pdf).

[10] Kryptografie ist in den Entwürfen nur beispielhaft als eine mögliche Funktion des Sicherheitsmoduls erwähnt. Die Erfüllung der formulierten Anforderungen ohne Kryptografie (vor allem in Form von Signaturen) dürfte jedoch jeglichen realistischen Kostenrahmen sprengen.

jedoch nicht vorgelegt werden – unmöglich gemacht.

Bewertung des SE-Verfahrens

Sicherheit

Das SE-Verfahren hat aufgrund des Verzichts auf
- eine Belegpflicht,
- ein Sicherheitsmerkmal auf den Belegen und
- die zentrale Erfassung der Sicherheitsmodule

massive, konzeptionelle Sicherheitslücken.

Daher ist es nicht vorstellbar, dass ein Sicherheitskonzept erstellt wurde.

Betriebskonzept

Ein Betriebskonzept – also eine Konzeption aller für den Praxisbetrieb relevanten Strukturen und Prozesse – existiert offenbar ebenfalls nicht. Sonst hätte es nicht zu den konzeptionellen Lücken und Fehlern im vorliegenden Entwurf kommen können.

Technologieoffenheit

Die einzige erkennbare Technologieoffenheit des SE-Verfahrens liegt darin, dass einige Rahmenbedingungen noch nicht im vorliegenden Entwurf definiert sind, sondern erst später durch das BSI festgelegt werden sollen.

Einige konkrete Vorgaben für die Sicherheitseinrichtung (z.B. die Integration eines Speichermediums) schränken die Freiheiten bei der Umsetzung sogar über das unbedingt notwenige Maß hinaus deutlich ein.

Der ausdrückliche Ausschluss des INSIKA-Verfahrens ist nicht mit dem Ziel der Technologieoffenheit vereinbar.

Integration in Kassensysteme

Die Sicherheitseinrichtung des SE-Verfahrens greift an mindestens zwei Punkten in eine Transaktion ein – bei deren Beginn und am Ende (ergibt sich aus § 2 den Verordnungsentwurfs). Speziell bei der Nutzung einer Sicherheitseinrichtung durch mehrere Kassenplätze kann das zeitkritisch und komplex werden. Ein Eingriff am Ende würde zur Erfüllung der Anforderungen ausreichen.

Durch die parallele Speicherung der Geschäftsvorfälle im Speichermedium der Sicherheitseinrichtung und in der Kasse entsteht zusätzliche, aber unnötige Komplexität, insbesondere beim Anschluss mehrerer Kassenplätze an eine Sicherheitseinrichtung.

Kosten

Als Maßstab für preiswerte Hochsicherheitskomponenten dürften heute Smartcards gelten. Nicht plausibel ist, dass eine zertifizierte Sicherheitseinrichtung – bestehend aus einem nicht näher benannten Sicherheitsmodul mit einer Echtzeituhr plus Speichermedium plus digitaler Schnittstelle – preiswerter als eine Smartcard sein soll.

Der Gesetzentwurf selbst nennt im Übrigen mehr als € 100 Mio. Erfüllungsaufwand pro Jahr für Wartung und Support.

Kontrollfähigkeit

Kontrollen in Form einer Kassennachschau bedingen einen Datenzugriff und sind damit für Steuerpflichtige und Vollzugsbehörden sehr aufwändig.

Prüfbarkeit

Eine Prüfung kann nicht mit einem „Vertrauensvorschuss“ die Vollständigkeit betreffend begonnen werden. Dadurch ist eine Vereinfachung von Prüfungen gegenüber dem Status Quo nicht zu erreichen. Erleichterung bringt allenfalls die vermutlich vorgesehene umfassende oder teilweise Standardisierung der Daten.

Rechtssicherheit

In Ermangelung eines Schlüsselmanagements durch eine vertrauenswürdige Stelle ist sehr fraglich, ob eine Rechtssicherheit bzgl. „Authentizität“ und „Unveränderbarkeit“ (§ 146 Abs. 4 AO) der Daten überhaupt möglich ist.

Aufgrund mangelnder Belegpflicht und des fehlenden Verzeichnisses aller Sicherheitsmodule ist Rechtssicherheit betreffend „Vollständigkeit“ im Sinne des § 146 Abs. 1 AO in jedem Fall ausgeschlossen. Folgerichtig fehlt der Aspekt der Vollständigkeit auch in der Begründung, wo es unter III.3 Abs. 3 lediglich heißt: „Das Zertifizierungsverfahren ist geeignet die Integrität (Unveränderbarkeit) und Authentizität (Herkunft der Daten) zu sichern.“

Bewertung der Aussagen zu INSIKA

Der Entwurf erhält eine Gegenüberstellung des SE-Verfahrens mit dem INSIKA-Verfahren sowie eine Reihe von konkreten Aussagen über INSIKA.

Die Aussagen sind ohne Kontaktaufnahme zum ADM e.V. und offenbar auch ohne Berücksichtigung der verschiedenen, öffentlich verfügbaren Dokumente zu INSIKA aufgestellt worden.

Die wesentlichen kritisierten Eigenschaften des INSIKA-Verfahrens leiten sich direkt aus dem Fachkonzept ab, das unter Federführung des BMF erstellt wurde und die Anforderungen für das Entwicklungsprojekt vorgegeben hat.[11]

Belastbarkeit der Vergleiche

Der Begründungsteil des Gesetzentwurfes stellt unter „Alternativen" nicht verschiedene Konzepte gegenüber, sondern behandelt folgende Optionen:

- Null-Option (Beibehaltung Status Quo)
- INSIKA-Verfahren
- SE-Verfahren

Es wird also ein fertig entwickeltes, erprobtes und vollständig dokumentiertes Verfahrens einer grob umrissenen Lösungsidee gegenüber gestellt. Dabei wird unterstellt, dass die am fertigen Verfahren – also INSIKA – kritisierten Nachteile tatsächlicher oder auch nur vermeintlicher Art der neuen Lösungsidee nicht anhafteten.

Die Auswahl der betrachteten Optionen erscheint angesichts der verschiedenen, real verfügbaren und theoretisch möglichen Lösungen[12] sehr eingeschränkt. Die Feststellung „Alternativen: Keine" im Vorblatt zum Verordnungsentwurf ist völlig unverständlich.

Konkrete Aussagen

Neben einigen zutreffenden Aussagen zum INSIKA-Verfahren sind die im Folgenden aufgeführten Aussagen aus der Begründung eindeutig und nachweislich falsch:[13]

Entspricht nicht den europäischen Sicherheitsanforderungen

Es existieren keine europäischen Sicherheitsanforderungen für Verfahren zur Absicherung von digitalen Grundaufzeichnungen. Es existieren lediglich europäische Anforderungen im Bereich qualifizierter elektronsicher Signaturen (QES) – für das im Gesetzentwurf behandelte Einsatzgebiet sind QES jedoch nicht nutzbar. Eine Anpassung der kryptografischen Algorithmen an den Stand der Technik ist im INSIKA-Verfahren vorgesehen und jederzeit möglich.[14]

Smartcard-Vergabe und -Verwaltung aufwändig

Jedes sinnvoll prüfbare Sicherheitssystem erfordert, dass alle Sicherheitsmodule zentral erfasst werden. Die dafür erforderlichen Prozesse zur Vergabe und Verwaltung von kryptografischen Zertifikaten und Smartcards (Zertifizierungsdienst, in Zukunft Vertrauensdienst) sind Stand der Technik und von mehreren Anbietern verfügbar.

Rechtliche Risiken durch Einbindung einer autorisierten Stelle

In anderen europäischen Ländern bestehen diese Risiken offenbar nicht, da bei fast jeder Sicherheitslösung für Registrierkassen ein zentrales Verzeichnis aller Systeme bzw. Sicherheitsmodule existiert.

Kostenintensiver durch Belegausgabe

Wie bereits dargestellt ist eine Belegausgabe für jedes sichere System zwingende Voraussetzung. Für einen Großteil der Geschäftsvorfälle werden bereits heute Belege ausgegeben.

Neuanschaffung Drucker erforderlich

Signaturen können auch im Klartext gedruckt werden, was den Arbeitsaufwand für Kontrollen allerdings ein wenig erhöht. Bei Bedarf könnte dies durch eine Übergangsfrist für die Weiternutzung älterer Drucker pragmatisch gelöst werden.

Kostenintensiver durch Smartcard

Es ist nicht plausibel, warum eine zertifizierte Sicherheitseinrichtung bestehend aus einem Sicherheitsmodul mit Echtzeituhr, einem Speichermedium und einer digitalen Schnittstelle preiswerter als eine Smartcard sein soll.

Jede Registrierkasse benötigt eine Smartcard

Diese Aussage ist falsch, da eine Smartcard problemlos von mehreren Kassenplätzen genutzt werden kann. Bei Bedarf können statt Smartcards auch andere Arten von Signaturerstellungseinheiten[15] genutzt werden, die einen ausreichenden Durchsatz bieten, um auch größere Anzahlen von Kassenplätzen zu versorgen.

---

[11] *Fachkonzept zur Einführung eines neuen Verfahrens zum Manipulationsschutz elektronischer bzw. PC-gestützter Registrierkassen und -systeme* aus dem Jahr 2008, erstellt von einer Bund/Länder-Arbeitsgruppe der Finanzbehörden, nicht veröffentlicht

[12] Beispiele in *Sichere Registrierkassen – internationale Fallbeispiele*, siehe Fußnote 4

[13] Zur Ergänzung siehe auch *14 Irrtümer über INSIKA* (http://www.insika.de/images/stories/INSIKA/14_INSIKA-Irrtuemer.pdf)

[14] Siehe http://www.insika.de/de/letzte-neuigkeiten/46-insika-karte-die-naechste-generation-kommt

[15] Signaturen können auch durch Hardware-Sicherheitsmodule (HSM) erzeugt werden. Für INSIKA müssen diese (analog zur Smartcard) durch einige Zusatzfunktionen erweitert werden.

Jede Smartcard muss zertifiziert werden

Die Aussage „Das Zertifizierungsverfahren ist aus folgenden Gründen kostengünstiger als das INSIKA-Konzept: Ein Sicherheitsmodul muss nur einmal zertifiziert werden und kann in einer Vielzahl von Kassen eingesetzt werden.“ impliziert, dass beim INSIKA-Verfahren jede Smartcard einzeln zertifiziert werden müsse. Auch beim INSIKA-Verfahren wird eine Signaturerstellungseinheit (also z.B. eine Smartcard) einmal zertifiziert[16] – zu jedem Exemplar wird dann ein kryptografisches Zertifikat[17] ausgestellt. Im Entwurf wurde also eine Zertifizierung nach Common Criteria bzw. technischer Richtlinie[18] auf der einen Seite und eine kryptografisches Zertifikat auf der anderen Seite verwechselt. Bis auf den Begriff „Zertifikat“ haben diese Sachverhalte jedoch rein gar nichts miteinander zu tun.

Verfassungsrechtliche Bedenken

Die Möglichkeit, dass jeder Bürger einen Beleg auf Echtheit überprüfen kann, soll verfassungsrechtlich bedenklich sein. Die gleiche Möglichkeit – etwa bei Prüfplaketten an Fahrzeugen oder eichpflichtigen Ladenwaagen bzw. den Sicherheitsmerkmalen von Geldscheinen – ist ganz offenbar verfassungsrechtlich unbedenklich. Durch eine kleine Modifikation des INSIKA-Verfahrens wäre diese Überprüfungsmöglichkeit sogar zu verhindern, auch wenn das nicht unbedingt sinnvoll wäre.

Bewertung der Kostenschätzungen

Der Gesetzentwurf beinhaltet in der Berechnung des Erfüllungsaufwandes eine Reihe von Zahlen, die nicht plausibel sind:

2,1 Mio. betroffene Geräte

HDE und DEHOGA gehen von zusammen 1,38 Mio. Kassenplätzen aus. Da die von den beiden Verbänden vertretenen Branchen einen sehr großen Teil der Registrierkassen betreiben, ist eine Zahl von 2,1 Mio. Geräten sehr hoch angesetzt.

Konkrete Schätzungen für Umrüstung

Ohne Vorliegen der Sicherheitsanforderungen und damit konkreter Entwürfe für die Sicherheitseinrichtung ist keine seriöse Schätzung möglich.

Sicherheitsmodul: € 10 pro Kasse

Aus den Angaben von € 17 Mio. für Sicherheitsmodule für Nachrüstungen und 1,7 Mio. davon betroffenen Geräten ergeben sich € 10 pro Kasse. Selbst bei der Nutzung eines Sicherheitsmoduls durch mehrere Kassen ist dieser Wert angesichts der Anforderungen an das Sicherheitsmodul (z. B. Echtzeituhr) völlig unrealistisch. Die weiteren Komponenten der Sicherheitseinrichtung werden offenbar mit € 22,5 Mio. für 1,7 Mio. Geräte, also € 13,23 pro Kasse beziffert.

Als Vergleichsmaßstab können die € 300 bis 400 für Fiskalboxen in Schweden und Belgien herangezogen werden.

Zertifizierung: € 75.000

Bei diesen Kosten kann es sich nur um die Gebühren für die Zertifizierung durch das BSI handeln. Der wesentliche, um ein Vielfaches höhere Aufwand entsteht jedoch bei der Evaluierung, die als Basis für den eher formellen Akt der Zertifizierung erforderlich ist.

Kassennachschauen: € 343.000

Bei einer Kassennachschau pro Verkaufsstelle[19] und Jahr liegen die Kosten jeweils bei € 0,32. Da Kassennachschauen mit dem SE-Verfahren nur mit Datenzugriff möglich sind, dürfte diese Schätzung um Zehnerpotenzen falsch sein.

[16] Die im INSIKA-Verfahren verwendete Signaturerstellungseinheit wird im Regelbetrieb selbstverständlich nach EAL 4+ evaluiert und vom BSI zertifiziert sein. Bei der aktuell im Taxibereich verwendeten Smartcard sind Hardware und Betriebssystem evaluiert und zertifiziert, für die INSIKA-spezifischen Softwareerweiterungen wurde dies aus Kostengründen auf den Start des großflächigen Echtbetriebs verschoben.

[17] Kryptografische Zertifikate sind Datensätze, die einen kryptografischen Schlüssel mit einer Identität (natürliche oder juristische Person) in einer sicheren und vertrauenswürdigen Form verknüpfen.

[18] Siehe Fußnote 2.

[19] Annahme: durchschnittlich zwei Kassenplätzen pro Verkaufsstelle

Fazit

Der Gesetzentwurf lässt vieles im Unklaren – die Grundzüge des dort skizzierten Verfahrens sind jedoch erkennbar.

Positiv zu werten ist, dass die Hard- und Software der Registrierkassen selbst keinen besonderen Anforderungen unterliegen – falls diese Auslegung korrekt ist.

Abgesehen davon weist der Entwurf viele grundsätzliche und gravierende konzeptionelle Lücken auf.

Es gibt weder eine Registrierkassenpflicht, eine Belegpflicht noch eine zentrale Registrierung der Sicherheitskomponenten. Jedes dieser Defizite für sich führt bereits zu erheblichen Sicherheitslücken. Eine Gewähr der Vollständigkeit der digitalen Aufzeichnungen ist damit ausgeschlossen.

Kassennachschauen sind prinzipbedingt stets mit einem hohen Aufwand für Verwaltung und Unternehmen verbunden, da sie grundsätzlich einen Datenzugriff erfordern.

Ein Sicherheits- und ein Betriebskonzept wurden ganz offenbar nicht erstellt.

Die Tatsache, dass der Gesetzentwurf nicht nur eine vollständige Neukonzeption, sondern auch Entwicklung, Erprobung und Integration eines Systems verlangt, lässt eine Einführung zum 1.1.2019 gänzlich unrealistisch erscheinen.

Zusammenfassend ist festzustellen, dass durch das im Gesetzentwurf beschriebene Sicherungsverfahren bei deutlich höheren Kosten für alle Beteiligten der Status Quo nur leicht verbessert würde. Eine wirksame Manipulationsbekämpfung und Rechtssicherheit auf Seiten der Anwender würden jedoch nicht erreicht.

Das fertig entwickelte, erprobte und frei verfügbare INSIKA-Verfahren würde alle Zielsetzungen des Gesetzentwurfs erreichen oder übertreffen. Es wäre in praktisch allen Belangen preisgünstiger – allein schon dadurch, dass es keine nennenswerten Wartungs- und Supportkosten gibt.

INSIKA wird als einzige Alternative im Entwurf behandelt und dann ausdrücklich ausgeschlossen, während der gleichzeitig „Technologieoffenheit“ eingefordert wird. In der Begründung dafür wird eine Reihe von eindeutigen Falschaussagen verwendet.

INSIKA und ADM e.V.

Das INSIKA-Verfahren („INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme“) wurde auf der Grundlage eines Konzepts der deutschen Finanzbehörden von der Physikalisch-Technischen Bundesanstalt von 2008 bis 2012 in einem Gemeinschaftsprojekt mit der Industrie entwickelt und erprobt. Nach erfolgreichem Projektabschluss werden das INSIKA-Konzept und insbesondere die daraus entstandenen technischen Verfahren vom ADM e.V. (Anwendervereinigung Dezentrale Mess-Systeme) unterstützt und weiterentwickelt.

Das INISKA-Verfahren kann ohne Patente, Lizenzkosten oder Ähnliches genutzt werden. Es bestehen daher keine wirtschaftlichen Interessen des ADM e.V. Das Hauptanliegen der Mitglieder liegt vielmehr darin, ein möglichst sicheres, preiswertes und einfach zu nutzendes Verfahren zur Absicherung elektronischer Aufzeichnungen von Bargeschäften zu etablieren – und dabei vor allem eine echte Alternative zu konventionellen, sehr aufwändigen „Fiskalkassensystemen“ zu bieten. Ein besonderer Schwerpunkt ist die Rechtssicherheit für die Anwender der Systeme.

Weitere Informationen sind auf www.insika.de frei abrufbar. Lediglich der Abruf der technischen Spezifikationen erfordert eine einfache und kostenlose Registrierung.

Kontakt

INSIKA – ADM e.V.
An der Corvinuskirche 22-26
D – 31515 Wunstorf

www.insika.de

E-Mail: info@insika.de

Änderungen am Dokument

Auf der Basis von Rückmeldungen und weiteren Prüfungsergebnissen wird dieses Dokument laufend ergänzt. In der folgenden Übersicht sind die Änderungen dargestellt.

Datum	Änderung
23.03.2016	Erstveröffentlichung
24.03.2016	Redaktionelle Änderungen
29.03.2016	Redaktionelle Änderungen
31.03.2016	Fragestellung „Zertifizierung der Aufzeichnungssysteme oder nur der Sicherheitseinrichtung“ behandelt Ergänzung unter „Praktische Nutzung, Kassennachschau“ Neuer Abschnitt „Jede Smartcard muss zertifiziert werden“ unter „Bewertung der Aussagen zu INSIKA“ Bewertung der Kostenschätzung Sicherheitsmodul aktualisiert und ergänzt Mehrere erläuternde Fußnoten ergänzt
05.04.2016	Neuer Abschnitt „Integration in Kassensysteme“ Ergänzungen zur Technologieoffenheit und zu Alternativen