Kassenführung und kryptografischer Manipulationsschutz: Freiwillig und technologieoffen?

Plädoyer für das INSIKA-Verfahren

Arno Becker*

Dem steigenden Bedarf an qualifizierter steuerlicher Beratung über Art, Umfang und Organisation der Kassenführung stellen sich vergleichsweise wenige Berater.[1] Das mag mit ein Grund dafür sein, dass sich deren Berufskammern und -verbände bisher in der derzeitigen Diskussion um Sicherungsverfahren für Kassen und kassenähnliche Systeme nicht zu Wort gemeldet haben. Und das, obwohl hier in einem nicht unwesentlichen wirtschaftlichen Feld – den Bargeldbranchen – erhebliches Potenzial für eine nachhaltige „Modernisierung des Besteuerungsverfahrens" schlummert. Die jüngste Rechtsprechung[2] und eine Anfang des Jahres erfolgte Buchveröffentlichung zum Thema Kassenführung von über zweihundert Seiten[3] machen mehr als deutlich, wie komplex angesichts des sich beschleunigenden technischen Fortschritts eine rechtssichere Umsetzung der Grundsätze ordnungsgemäßer Kassenführung geworden ist.
Eine vertrauenswürdige – weil hohen Sicherheitsansprüchen genügende – Lösung vermag hier aufgrund eindeutiger Nachweisbarkeit Rechtssicherheit für ehrliche Steuerpflichtige und ihre Berater sowie – vice versa – aufwandsarme Prüfbarkeit auf Seiten der Finanzverwaltung gewährleisten.

L Teutemacher, Handbuch zur Kassenführung, Herne 2015

Inhaltsübersicht

I. Gesetzliche Grundlage als zwingende Voraussetzung für den Einsatz von Sicherheitsverfahren

Rechtssicherheit bedingt gesetzliche Regelung

Wenn insoweit eingewandt wird, dass „ein konkreter exklusiv vorgeschriebener kryptografischer Manipulationsschutz (z. B. INSIKA) auf der Basis der derzeitigen Gesetzeslage

* Leitender Regierungsdirektor Arno Becker ist Leiter des Referats St 4 für Außenprüfungsdienste, Steuerstrafrecht und Umsatzsteuer bei der Oberfinanzdirektion Nordrhein-Westfalen. Der Beitrag wurde nicht in dienstlicher Eigenschaft verfasst.

1 Pump/Heidl, Hilfestellung bei der Kassenführung durch den steuerlichen Berater – Ärger wegen § 162 AO durch unzulängliche Kassenbuchführung, StBp 6/2014 S. 162 und StBp 7/2014 S. 204; Pump, Die ungenutzten Möglichkeiten zur Sicherung der Einzeltransaktionen gemäß § 146 Abs. 4 AO bei Registrierkassen und Taxametern – INSIKA als technische Lösung, um Vollzugsdefizite bei bargeldintensiven Betrieben zu vermeiden, DStZ 7/2014 S. 251; so auch Becker, DStR 42/2015 S. 14.

2 BFH, Urteile vom 16. 12. 2014 - X R 29/13 [→RAAAE-88364] und X R 47/13 [→VAAAE-88380], sowie BFH, Urteil vom 25. 3. 2015 - X R 20/13, BStBl 2015 II S. 743 [→GAAAE-96112].

3 Teutemacher, Handbuch zur Kassenführung – Praxishandbuch für die rechtssichere Umsetzung, Herne 2015.

nicht vorgeschrieben werden“[4] kann, ist das zwar zutreffend, trifft aber nicht den Kern der Sache. Entscheidend ist: Ohne eine gesetzliche Regelung ist die mit der Verpflichtung zum Einsatz korrespondierende gerichtsfeste Rechtssicherheit des Steuerpflichtigen für eine Unveränderbarkeit bzw. unveränderbar dokumentierte Veränderung seiner Daten im Sinne des § 146 Abs. 4 AO derzeit nicht herzustellen.

Weder das Gesetz selbst noch die dazu ergangenen Verwaltungsanweisungen geben einen Sicherheitsstandard im Sinne eines technischen Sicherheitsniveaus vor. Ohne Bindung der Verwaltung ist Rechtssicherheit für den Steuerpflichtigen unter den heutigen technischen Voraussetzungen und Möglichkeiten nicht zu gewährleisten.

Huber, Praktische Erfahrungen mit der Kassenführung in Österreich, BBK 6/2014 S. 286 [→WAAAE-57649]

Hinweis: Der technische Sicherheitsstandard des INSIKA-Konzepts ist ausgereift und wurde bereits mehrere Jahre erfolgreich im Praxiseinsatz getestet[5] – nicht nur bei Taxametern von den Gewerbe- und Finanzbehörden in Hamburg, sondern auch von der Finanzverwaltung Nordrhein-Westfalen bei Kassen(-systemen) mehrerer Unternehmen[6]. Deshalb ist dieser Standard geeignet, die notwendige Rechtssicherheit nicht nur für die Länderfinanzverwaltungen als vollziehende Behörden, sondern vor allem auch zugunsten der Steuerpflichtigen und ihrer Berater auf dieses hohe und erprobte sowie vor allem vergleichsweise kostengünstige technische Niveau[7] zu stützen.

II. Keine Festschreibung einer „Technik von heute“ im Gesetz

Gesetzesänderung wegen technischen Fortschritts nicht zwingend

Der weitergehende Einwand, dass eine gesetzliche Verankerung eines bestimmten kryptografischen Manipulationsschutzes „wie etwa mit der INSIKA-Smartcard“ allerdings den gravierenden Nachteil hätte, „dass damit eine bestimmte Technik mit dem Stand von heute im Gesetz festgeschrieben wird und damit für Weiterentwicklung der Technik eine Gesetzesänderung erforderlich wäre“[8] ist – jedenfalls im Hinblick auf das INSIKA-Konzept – unzutreffend.

Huber/Reckendorf/Zisky, Die Unveränderbarkeit der (Kassen-)Buchführung nach § 146 Abs. 4 AO im EDV-Zeitalter und INSIKA, BBK 12/2013 S. 567 [→MAAAE-37806] + BBK 13/2013 S. 610 [→NAAAE-39375] + BBK 14/2013 S. 663 [→SAAAE-40175]

Zunächst einmal ist INSIKA keine bestimmte „Technologie“ und bezeichnet erst Recht kein „konkretes Produkt“: INSIKA ist die Kurzbezeichnung (**IN**tegrierte **SI**cherheitslösung für messwertverarbeitende **KA**ssensysteme) eines vom BMWi in den Jahren 2008 bis 2012 geförderten MNPQ[9]-Projekts, das die Physikalisch-Technische Bundesanstalt (PTB) mit einem Konsortium von Kassenherstellern durchgeführt hat und das fachlich von einer „Arbeitsgruppe Registrierkassen“ der Länderfinanzverwaltungen unter Leitung des BMF namentlich durch Formulierung der fachlichen Anforderungen unterstützt wurde.

Hinweis: Heute steht INSIKA für die Ergebnisse dieses vom BMWi nun unter dem Titel „Hightechlights“[10] beworbenen Projekts und bezeichnet einen innovativen generischen Ansatz zum sicheren und zugleich einfachen Nachweis manipulierter bzw. nicht manipulierter Daten.

---

4 Lüngen/Resing, Ordnungsmäßige Kassenführung beim Betrieb von Warenautomaten, StBp 10/2015 S. 300, 302.

5 Die Bedeutung von Praxistests ist nicht zu unterschätzen. Wie schnelle Änderungen einzelner Komponenten allein „vom grünen Tisch aus“ die Sicherheit des Gesamtsystems deutlich herabzusetzen vermögen, belegen die kurzfristig beschlossenen Abweichungen vom INSIKA-Konzept bei Implementierung der österreichischen Registrierkassen-Sicherheitsverordnung vom 1. 9. 2015; dazu i. E.: INSIKA: Technologieoffener kryptografischer Manipulationsschutz für Registrierkassen und Taxameter – Analyse der österreichischen Registrierkassen-Sicherheitsverordnung vom 1. 9. 2015, http://www.insika.de.

6 Hierbei handelt es sich um Feldtests bei einzelnen Unternehmen durch einen freiwilligen anonymisierten Versuch.

7 Namentlich gegenüber konventionellen Fiskalsystemen oder sog. Fiskalbox-Systemen.

8 Lüngen/Resing, Ordnungsmäßige Kassenführung beim Betrieb von Warenautomaten, StBp 10/2015 S. 300, 302.

9 Messen, Normen, Prüfen und Qualitätssicherung: Fördernummer Nr. 11/07.

10 http://go.nwb.de/lrrus.

Hochsicherheitsverfahren

Das Konzept bedient sich dazu verschiedener Standardverfahren und -komponenten der IT-Hochsicherheitstechnologie. Beispielhaft seien hier angeführt:

- sichere Signaturerstellungseinheiten als kombinierte Hard-/Softwarelösung,[11] etwa in Form von Smartcards,[12]
- Funktionserweiterung der Signaturerstellungseinheit durch dort integrierte[13] Summenspeicher und Sequenzzähler für Geschäftsvorfälle und Tagesabschlüsse,
- digitale Signatur der Daten durch asymmetrisches Standardkryptosystem ECDSA (*Elliptic Curve Digital Signature Algorithm*, eingesetzt wegen kürzerer Schlüssellängen gegenüber dem RSA = *Rivest, Shamir und Adleman*-Kryptoverfahren) bei anschließend freier Datenablage sowie möglicher Weiterleitung und Weiterverarbeitung der Daten,
- kryptologische Hashfunktionen basierend auf SHA-Standard (*Secure Hash Algorithm*),
- Festlegung des Datenausgabeformats durch Signaturerstellungseinheiten, beispielsweise XML (*Extensible Markup Language*) oder CSV (*Comma-separated values* oder *Character-separated values*),
- Zertifikatserteilung für Signaturerstellungseinheiten durch bei der Bundesnetzagentur akkreditierten Zertifizierungs-[14] bzw. Vertrauensdiensteanbieter[15] (u. a. zur Authentifizierung der signierten Daten).

Damit wird sich hier also derselben Verfahren bedient, wie sie etwa auch bei Geld- und Kreditkarten zum Einsatz kommen. Wenn und soweit Anpassungen an den Stand der Technik erforderlich würden, könnten Hard- und Software der Signaturerstellungseinheit oder die kryptografischen Algorithmen folglich jederzeit ausgewechselt werden.

Papierausdrucke nicht erforderlich

Die notwendige Pflicht zur Ausgabe signierter Belege bedingt nicht zwangsläufig Belegausdrucke auf Papier. Auch die Ausgabe elektronischer Belege[16] ist konzeptionell möglich und kann rechtlich implementiert werden, sobald eine ausreichende Standardisierung des Zugriffs auf die entsprechenden Daten erfolgt ist.

Beispiel ***Das INSIKA-Konzept bei Taxametern in Hamburg etwa arbeitet mit einer Online-Datenübertragung. Die Überprüfung der korrekten Nutzung des Systems erfolgt hier derzeit nicht über gedruckte Belege, sondern durch Prüfung der zusammen mit dem signiert übertragenen Datensatz auf dem Server abgelegten Transaktionsdaten.***

W³ Checkliste zur Überprüfung der Ordnungsmäßigkeit der Kassen(buch)führung beim Einsatz elektronischer Kassensysteme [→WAAAE-32052]

Ergebnis: Vor diesem Hintergrund ist die Behauptung in der Sache unzutreffend, dass durch eine Sicherheitslösung für Kassen und kassenähnliche Systeme nach dem INSIKA-Konzept „eine bestimmte Technik mit dem Stand von heute im Gesetz festgeschrieben" würde.

Notwendige gesetzliche Regelungen

Gesetzlicher Regelung bedürfen allerdings die Gewährung von Rechtssicherheit auf Seiten des Steuerpflichtigen bei Einsatz der funktionserweiterten Signaturerstellungseinheit, das an diese zu stellende fachliche Anforderungsprofil[17] sowie das Verfahren

[11] Im Gegensatz zu einer in der IT-Hochsicherheitstechnologie keine Verwendung findenden – weil nicht sicheren – reinen Softwarelösung.
[12] Signaturerstellungseinheit nach diesem Konzept könnte allerdings auch ein Hardware-Sicherheitsmodul (HSM) sein.
[13] Und damit selbst vom Zertifizierungsdiensteanbieter nicht beeinflussbar.
[14] Vgl. §§ 15 ff. des Signaturgesetzes.
[15] Neue Terminologie eingeführt durch Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. 7. 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. vom 28. 8. 2014 L 257/73 [eIDAS-Verordnung], in Kraft getreten am 18. 9. 2014; dazu: Roßnagel, Neue Regeln für sichere elektronische Transaktionen, NJW 2014 S. 3686.
[16] Siehe etwa Müller, Elektronische Kassenzettel – Kassenbon aufs Handy, SZ vom 19. 9. 2014, http://go.nwb.de/9ywb5.
[17] Vgl. dazu: INSIKA: Technologieoffener kryptografischer Manipulationsschutz für Registrierkassen und Taxameter – Wie werden Registrierkassen und Taxameter sicher? unter: http://www.insika.de.

zur Zertifikatserteilung. Insoweit folgt das Konzept dem Vorbild des Signaturgesetzes: Auch hier werden keine konkreten Produkte vorgeschrieben, sondern lediglich grundsätzliche Verfahrensweisen normiert; die zentralen Sicherheitsanker sind aber auch hier sehr restriktiv geregelt.

III. Standard versus Technologieoffenheit

Sicherheitsstandard

Standardisierung und Technologieoffenheit schließen sich nicht per se gegeneinander aus. Allerdings steht eine Standardisierung[18] bereits definitionsgemäß vollkommener Offenheit entgegen. Nimmt man den Begriff „Technologieoffenheit" wörtlich, wird zwar die Technologie offen gelassen, nicht aber die diesen zugrunde liegenden fachlichen Anforderungen und/oder zu berücksichtigenden Rahmenbedingungen. Bei einem Sicherheitsstandard für IT-Systeme müssen demzufolge dem Rechnung tragende Eckpunkte technischer wie fachlicher Art fixiert werden. Diese müssen sowohl eindeutig definiert als auch leicht und sicher überprüfbar sein.

1. Standard

Vertrauen schaffen

Soweit es um das Verhältnis einer Standardisierung zu dem aus der Welt des Marketings stammenden Begriff „Technologieoffenheit" geht, ist anzumerken, dass allein „der Standard" die zentrale Aufgabe jedweder Sicherheitskomponente – auf Grundlage des fachlichen Anforderungsprofils den größtmöglichen Grad an Sicherheit zu gewährleisten – garantiert. Damit sichert er zugleich das öffentliche und private Vertrauen in das hohe Sicherheitsniveau und die systemgerechte Funktionsweise einer Sicherheitslösung, die sich in der Prüfbarkeit auf Seiten der Finanzverwaltung und (erstmalig) in der Beweisbarkeit auf Seiten des Steuerpflichtigen manifestiert. Aufgrund dessen muss dieses hohe Sicherheitsniveau von Anfang an erreicht werden, also auch ohne dass zunächst eine etwaig künftige technische Weiterentwicklung stattfinden müsste.

Prüfbarkeit und Beweisbarkeit

Hinweis: Prüfbarkeit und Beweisbarkeit sind also zwei Seiten derselben Medaille; denn nur durch Standardisierung wesentlicher Eigenschaften ist eine belastbare Überprüfung des Einhaltens aller gesetzlichen Anforderungen mit vertretbarem Aufwand und damit eine – technisch wie rechtlich – schnell nachweisbare Originalität elektronischer Ursprungsaufzeichnungen möglich. Das INSIKA-Konzept legt hierzu lediglich grundlegende Abläufe wie Buchung, Signatur, Belegerstellung und Bereitstellung der Daten fest.

Die darüber hinausgehenden Mindestinhalte – etwa funktionale Erweiterungen der Signaturerstellungseinheit durch Sequenz- und Summenzähler oder Exportformate – sind entweder konsequenter Ausfluss der zugrunde liegenden fachlichen Anforderungen oder aber basieren auf Notwendigkeiten der Praxis, wie etwa der Forderung nach schneller Auslesbarkeit und leichter Prüfbarkeit. Diese Anforderungen sind einer bzw. jeder IT-Sicherheitslösung für Kassen und kassenähnliche Systeme immanent und deshalb unabdingbar.

Zertifizierung der Komponenten

Vollständig offen ist demgegenüber sowohl die konkrete Implementierung des abzusichernden Aufzeichnungssystems (z. B. Registrierkasse, Warenautomat, Taxameter) als auch die Implementierung der Sicherheitskomponenten – Signaturerstellungseinheit und PKI.[19] Natürlich ist hier eine Evaluierung oder Zertifizierung der

[18] Standardisierung bedeutet im eigentlichen Wortsinn Vereinheitlichung von z. B. Maßen, Typen, Verfahrensweisen. Ziel ist die Schaffung gemeinsamer Standards respektive Parameter, etwa bei Werkzeugen, Produktions- oder Softwarekomponenten.

[19] *Public key infrastructure;* bezeichnet in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann.

Komponenten erforderlich, da allein zertifizierte Komponenten als sicher anerkannt werden.

INSIKA ist kostengünstig

Bedenkt man nunmehr, dass reine Softwarelösungen grundsätzlich relativ leicht angreifbar und daher für IT-Hochsicherheitsanwendungen ungeeignet sind und alle anderen bekannten Hardware-/Software-Systeme demgegenüber höchst kostenaufwändige Zertifizierungen in Form von Gerätebauart- und Softwarezulassungsverfahren bedingen, wird die Einzigartigkeit dieses allein mit einer zertifizierten Smartcard für Kassen und kassenähnliche Systeme auskommenden Hardware-/Software-Verfahrens deutlich. Das dürfte der Grund dafür sein, dass trotz jahrelanger Auseinandersetzung bis heute nicht ein gleich sicheres Alternativkonzept zu zumindest vergleichbar niedrigen Kosten vorgelegt werden konnte.

Da Innovationen und Wettbewerb im Bereich einer Sicherheitslösung für Kassen und kassenähnliche Systeme selbst keinen großen Einfluss auf den Kundennutzen haben, kann die Forderung eines Anwenders demnach insoweit nur lauten, für einen möglichst hohen Sicherheitsstandard zu einem möglichst geringen Preis gerichtsfeste Rechtssicherheit zu erhalten.

2. Technologieoffenheit

Anpassungen an den Stand der Technik

Vor diesem Hintergrund wird der in diesem Zusammenhang oft gebrauchte Begriff „Technologieoffenheit" in der öffentlichen Diskussion – namentlich in Presseverlautbarungen des BMF[20] – wohl ein wenig überstrapaziert. Angesichts der erforderlichen – und auch politisch gewollten[21] – Standardisierung kann der Begriff „Technologieoffenheit" nämlich nur drei Forderungen an eine IT-Sicherheitslösung für Kassen und kassenähnliche Systeme beinhalten:

- möglichst kostengünstige laufende Anpassung des Sicherheitssystems an den Stand der Technik;
- möglichst geringer Eingriff ins Host-System der Geräte, damit Innovationsmöglichkeiten und Wettbewerb nicht behindert werden.
- Demgegenüber sollten die Funktionalitäten der Sicherheitskomponente möglichst umfassend vorgegeben sein, um zusätzliche Aufwände für Implementierung, Prüfbarkeit und Verwaltung zu minimieren.

2.1 Anforderungen mit Blick auf das Sicherheitssystem

Aktualisierung der kryptografischen Algorithmen

INSIKA verwendet Standard-Kryptografieverfahren und -komponenten der Hochsicherheitstechnologie, die in einer Vielzahl anderer technischer Anwendungen entsprechend eingesetzt sind und ständig fortentwickelt werden. Sobald diese bei INSIKA eingesetzten Verfahren in Form kryptografischer Algorithmen oder die verwendeten Komponenten in Form von Signaturerstellungseinheiten nicht mehr dem Stand der Technik entsprechen sollten, könnten sie jederzeit durch neuere oder aktuellere Varianten ersetzt werden, ohne dass das INSIKA-Konzept selbst geändert werden müsste. So sind derzeit etwa ein Wechsel von ECDSA-192 auf ECDSA-256 sowie eine Änderung des Datenausgabeformats von XML auf CSV konkret geplant.[22] Entsprechendes gilt für Anpassungen der abzusichernden Daten, was durch entsprechende Änderung der fachseitig initiierten Datenprofile leicht umzusetzen ist.

---

[20] So Weißgerber, zitiert bei: Klein, Insika bleibt umstritten – Finanzpolitiker suchen die Lösung gegen Steuertricks an der Ladenkasse, Lebensmittel Zeitung Nr. 41 vom 9. 10. 2015 S. 31: „Wir wollen eine technologieoffene Lösung, bei der ausgewählt werden kann."

[21] Vgl. etwa den derzeitigen Vorsitzenden der FMK und hessischen Finanzminister Dr. Thomas Schäfer: „Standards setzen um systematischen Betrug zu verhindern.", http://go.nwb.de/ct2x5.

[22] Vgl. auf www.insika.de: http://go.nwb.de/3s912 und http://go.nwb.de/t50dc.

2.2 Anforderungen mit Blick auf das Aufzeichnungsgerät

Signaturerstellungseinheit = Smartcard oder HSM

Betrachtet man nunmehr die Eingriffe einer Sicherheitskomponente in das Aufzeichnungssystem selbst, ist nach Vorgesagtem eindeutig, dass es beim Einsatz von Signaturerstellungseinheiten nach dem INSIKA-Konzept keine vollständige, sondern lediglich eine möglichst weitgehende Technologieoffenheit geben kann. Jedoch auch hier ist eine Sicherheitslösung nach dem INSIKA-Konzept im Vergleich zu allen anderen weltweit bekannten Fiskallösungen „minimalinvasiv", da insoweit lediglich gefordert werden:

- die Übergabe der im jeweiligen Profil festgelegten Daten des Geschäftsvorfalls an die funktionserweiterte sichere Signaturerstellungseinheit und
- bei Einsatz einer Smartcard als Signaturerstellungseinheit der entsprechende Anschluss über einen internen oder externen Smartcard-Leser mittels beliebiger Schnittstelle.

Kein INSIKA-Monopol!

Die Implementierung wird also offen gelassen; allein bestimmte Funktionalitäten und Schnittstellen sind vorgegeben. Die entsprechenden Spezifikationen sind veröffentlicht und – da frei von Patenten oder anderen Rechten Dritter – kostenlos und ohne Einschränkungen nutzbar.[23] Vor diesem Hintergrund entbehrt das vom BMF gezeichnete Bild eines „INSIKA-Monopols"[24] jedweder Grundlage.

Zertifizierung und Wettbewerb

Die Signaturerstellungseinheit selbst muss natürlich so zertifiziert sein, dass sie von der Finanzverwaltung akzeptiert wird,[25] damit im Gegenzug die Rechtssicherheit auf Seiten des Anwenders gewährleistet ist. Die abzusichernden Aufzeichnungsgeräte selbst sind demgegenüber gerade nicht in höchst kostenaufwändigen Verfahren zu zertifizieren. Obwohl es also im Teilbereich der Smartcards keine vollständige Technologieoffenheit gibt, werden die Hersteller genannter Aufzeichnungsgeräte durch klare Schnittstellen und minimale Eingriffe in das Host-System in Bezug auf Innovationen, Wettbewerb und Technologie nicht behindert.

Hinweis: Wegen weiterer Einzelheiten soll an dieser Stelle auf die instruktive Analyse der Anwendervereinigung Dezentrale Mess-Systeme (ADM e. V.)[26] zu diesem Thema verwiesen werden.[27]

W³ Krüger, Kassenführung (HGB), infoCenter [→DAAAC-28623]

Nicht zuletzt wird die weitgehende Technologieoffenheit durch den großen Anwendungsbereich einer Sicherheitslösung nach dem INSIKA-Konzept deutlich, der nicht nur elektronische Registrierkassen und PC-Kassen umfasst, sondern etwa auch Waagen mit Kassenfunktion, Taxameter, Warenautomaten, Geld- und Warenspielgeräte sowie Wett-Terminals einschließt. Selbst eine Ausweitung auf Warenwirtschafts- und Fakturierungssysteme wäre ohne Weiteres möglich.

---

[23] Derzeit zu Testzwecken – im Taxibereich auch für den Echtbetrieb – abrufbar unter: http://www.insika.de/de/spezifikationen.

[24] Weißgerber, zitiert bei: Klein, Insika bleibt umstritten – Finanzpolitiker suchen die Lösung gegen Steuertricks an der Ladenkasse, Lebensmittel Zeitung Nr. 41 vom 9. 10. 2015 S. 31: „Es könne nicht dauerhaft ein Monopol für Insika geben, argumentiert der BMF-Sprecher, dagegen sprächen auch europarechtliche Gründe."

[25] Das verhindert überdies zugleich Abhängigkeiten von einem konkreten Anbieter.

[26] Der ADM e. V. hat nach Beendigung des vom BMWi geförderten Projekts „INSIKA", das mit Veröffentlichung des PTB-Berichts IT-18 (http://public.ptb.de/oa/doidocs/210_20130206a.htm) seinen Abschluss fand, wie auch schon bei anderen Projekten zuvor (etwa das sog. SELMA-Projekt), die technische Pflege und Fortentwicklung des Verfahrens übernommen. Zu diesbezüglichen Informationszwecken unterhält der ADM e. V. die Internetseite http://www.insika.de.

[27] INSIKA: Technologieoffener kryptografischer Manipulationsschutz für Registrierkassen und Taxameter – Sichere Registrierkassen und Technologieoffenheit – eine Analyse, http://www.insika.de.

IV. Europarechtliche Zulässigkeit

BMF zweifelt Europarecht-Konformität an

Das BMF hat jüngst wieder das Thema europarechtlicher Zulässigkeit einer Sicherheitslösung für Kassen und kassenähnliche Systeme nach dem INSIKA-Konzept auf den Tisch gebracht,[28] wenngleich mancher diese Frage bereits für „abgehakt" gehalten haben dürfte.

Steuererhebung rechtfertigt gesetzliche Regelung

Zunächst einmal würde die gesetzliche Einführung einer Verpflichtung zur Nutzung einer Signaturerstellungseinheit nach diesem Konzept beim Einsatz elektronischer Kassen und kassenähnlicher Systeme nicht gegen die Warenverkehrsfreiheit nach den Art. 28 bis 37 AEUV[29] verstoßen. Selbst wenn man eine derartige Regelung für eine produkt- oder absatzbezogene Regelung, die in den Anwendungsbereich des Art. 34 AEUV fällt, im Hinblick auf die erforderlichen, geringfügigen Softwareanpassungen zum Zweck des Zugriffs auf die vom Profil vorgegebenen Daten des Geräts bzw. Systems bejahen wollte, wäre dieser minimalinvasive Eingriff aufgrund zwingender Erfordernisse im Sinne der sog. „Cassis-de-Dijon-Formel"[30] aus Gründen einer gleichmäßigen Steuerfestsetzung und -erhebung im Bargeldbereich gerechtfertigt. Insoweit ist darauf hinzuweisen, dass die Beschaffung der für die Existenz eines Staates notwendigen Steuermittel auch von den Mitgliedern und Organen der Europäischen Union selbst als zwingendes Erfordernis anerkannt wird. So heißt es etwa in Ziffer 2 der Erwägungen zur MID:[31]

> „Diejenigen (Messgeräte), die aus Gründen des öffentlichen Interesses, des Gesundheitsschutzes, der öffentlichen Sicherheit und Ordnung, des Umweltschutzes, des Verbraucherschutzes, der Erhebung von Steuern und Abgaben und des lauteren Handels wahrgenommen werden und die sich direkt oder indirekt auf das tägliche Leben der Bürger auf vielfältige Weise auswirken, können die Verwendung gesetzlich kontrollierter Messgeräte erfordern."

Umsatzsteuer als Gemeinschaftssteuer

Dies gilt namentlich dann, wenn – wie vorliegend – insbesondere auch die Umsatzsteuer als Gemeinschaftssteuer von den Systemmanipulationen in erheblicher Weise betroffen ist. Insoweit ist hier auf den entsprechenden Bericht der OECD mit dem Titel „Umsatzverkürzung mittels elektronischer Kassensysteme, eine Bedrohung für die Steuereinnahmen" zu verweisen.[32]

Kein Verstoß gegen EU-Messgeräterichtlinie

Die gesetzliche Einführung einer Verpflichtung zur Nutzung einer Signaturerstellungseinheit nach dem INSIKA-Konzept verstieße aber auch nicht gegen die EU-Messgeräterichtlinie oder die sog. NAWID[33], da die funktionserweiterte Signaturerstellungseinheit auf den nach diesen EU-Vorschriften sicherheitsrelevanten Teil präzise abgegrenzt ist.[34]

Allenfalls könnte in Betracht kommen eine Verpflichtung zur Notifizierung der entsprechenden gesetzlichen Regelungen bei der Europäischen Kommission gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. 6. 1998 über ein

---

[28] Zuletzt Weißgerber, zitiert bei: Klein, Insika bleibt umstritten – Finanzpolitiker suchen die Lösung gegen Steuertricks an der Ladenkasse, Lebensmittel Zeitung Nr. 41 vom 9. 10. 2015 S. 31: „Es könne nicht dauerhaft ein Monopol für Insika geben, argumentiert der BMF-Sprecher, dagegen sprächen auch europarechtliche Gründe."

[29] Vertrag über die Arbeitsweise der Europäischen Union, Fassung aufgrund des am 1. 12. 2009 in Kraft getretenen Vertrags von Lissabon, konsolidierte Fassung bekannt gemacht im ABl. EG Nr. C 115 vom 9. 5. 2008 S. 47.

[30] EuGH, Urteil vom 20. 2. 1979 - Rs. C-120/78, Cassis de Dijon, Slg. 1979 S. 649.

[31] Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. 3. 2004 über Messgeräte, ABl. EU L 135/1 vom 30. 4. 2004 (Measuring Instruments Directive - MID).

[32] http://go.nwb.de/w5mro.

[33] Richtlinie 2014/31/EG des Europäischen Parlaments und des Rates vom 26. 2. 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend die Bereitstellung nichtselbsttätiger Waagen auf dem Markt.

[34] Vgl. Osswald, Ergebnisse und Erfahrungen eines INSIKA Feldversuches, PTB-Bericht S. 51, 56 f.

„Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften“[35]. Soweit EU-Mitgliedstaaten diesen Weg vor Einsatz ihrer gegenüber dem INSIKA-Konzept erheblich restriktiveren Fiskalsysteme überhaupt beschritten haben, wurden diese durch diesen Prozess weder aufgehalten noch auch nur wesentlich verändert.

FAZIT

INSIKA = sicher, technologieoffen und preisgünstig

Das INSIKA-Konzept basiert auf einem innovativen generischen Ansatz, der durch intelligente Kombination von Standardverfahren der Hochsicherheitstechnologie eine äußerst sichere, technologieoffene und preisgünstige Lösung zur Schaffung von Datenintegrität und Datenauthentizität bietet. Diese Verfahren behindert aufgrund nur minimaler Eingriffe in die Systeme die Innovationskraft der Gerätehersteller nicht und ist zudem europarechtlich unbedenklich. INSIKA ist frei von Rechten Dritter, wodurch Abhängigkeiten ausgeschlossen sind. Vor allem aber kann eine Sicherheitslösung nach dem INSIKA-Konzept dem ehrlichen Kaufmann endlich Rechtssicherheit in Bezug auf die Unveränderbarkeit bzw. auf ausschließlich dokumentierte Veränderungen seiner Daten aus Kassen und kassenähnlichen Systemen bieten.

Wenngleich die Irrtümer über eine Sicherheitslösung für Kassen und kassenähnliche Systeme nach dem INSIKA-Konzept vielfältig sind,[36] werden die insoweit aufgestellten Behauptungen durch ständige Wiederholung nicht zutreffend. Vollständige Technologieoffenheit eines IT-Sicherheitssystems für Kassen und kassenähnliche Systeme ist eine Illusion, mithin eine derartige Lösung weltweit auch nicht existiert. Eine weitgehende Technologieoffenheit ist sehr wohl möglich und wird vom INSIKA-Verfahren geboten, was vor allem durch die minimierten Eingriffe in die Aufzeichnungssysteme selbst erreicht wird. Nicht von ungefähr fordern deshalb gerade Berufsverbände, die bereits Erfahrungen mit einer Sicherheitslösung für Kassen und kassenähnliche Systeme nach dem INSIKA-Konzept gesammelt haben, die gesetzliche Implementierung einer derartigen Lösung bei der Politik ausdrücklich ein[37] oder stehen dieser zumindest aufgeschlossen gegenüber.[38]

AUTOR

Arno Becker,
Leitender Regierungsdirektor, ist Leiter des Referats St 4 für Außenprüfungsdienste, Steuerstrafrecht und Umsatzsteuer bei der Oberfinanzdirektion Nordrhein-Westfalen.

[35] http://go.nwb.de/kweyy.

[36] Siehe: INSIKA: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter – 14 Irrtümer über INSIKA, http://www.insika.de/images/stories/INSIKA/14_INSIKA-Irrtuemer.pdf.

[37] So etwa zu lesen in *taxi times* vom 17. 6. 2015, Fiskaltaxameter: BZP bekennt sich zum INSIKA-Verfahren, unter: http://go.nwb.de/xdq3d; Fund, Bund soll fälschungssichere Kassensysteme umsetzen, taxi heute vom 23. 6. 2015, http://go.nwb.de/1vj51; Gewerkschaft Nahrung-Genuss-Gaststätten vom 25. 6. 2015: NGG fordert Umstellung der Kassensysteme auf INSIKA, http://go.nwb.de/oz10f; Deutsche Steuergewerkschaft vom 29. 7. 2015: Milliardenschwere Betrügereien bei Registrierkassen – DSTG fordert rasches Handeln der Politik, http://go.nwb.de/tvc2s.

[38] o. V., Milliardenschaden: Ladenkassen: Steuerbetrug mit Schummelsoftware, Schleswig-Holsteinische Zeitung (SHZ) vom 22. 8. 2015, http://go.nwb.de/lm1ij: „Nicht einmal der schleswig-holsteinische Hotel- und Gaststättenverband hat gegen Insika etwas einzuwenden. „Wenn wir dadurch aus dem Generalverdacht der Finanzämter herauskommen, wäre das eine Hilfe für uns“, sagt Dehoga-Präsident Axel Strehl.“