INSIKA®: Kryptografischer Manipulationsschutz für Registrierkassen und Taxameter

Sichere Registrierkassen und Technologieoffenheit – eine Analyse

Stand: 26. Oktober 2015

In der Diskussion über die Absicherung von Registrierkassen und ähnlichen Systemen gegen Manipulationen taucht verstärkt der Begriff „Technologieoffenheit“ auf. Hier wird dargestellt, was das im konkreten Fall bedeutet und warum INSIKA technologieoffen ist.

Technologieoffenheit zielt einerseits auf die jederzeitige mögliche Anpassung der Sicherheitskomponenten an sich ändernde Risiken oder an höhere Sicherheitsstandards und andererseits darauf, Innovationen und Wettbewerb auf dem Markt der Registrierkassen nicht zu behindern. Der wesentliche Einflussfaktor in diesem Markt ist hierbei die genaue Ausgestaltung der Anforderungen, und dabei vor allem der Grad des Eingriffs in die Produkte selbst. Dieser Eingriff muss minimal gehalten werden, um Einschränkungen von Innovationen und Wettbewerb zu vermeiden. Eindeutige Regeln für die eigentliche Sicherheitskomponente in Verbindung mit technischen Freiheiten bei der Umsetzung wirken demgegenüber vereinfachend, innovationsfördernd und kostensenkend.

„Technologieoffenheit“

Spätestens seit den Pressemitteilungen nach der Finanzministerkonferenz vom 25. Juni 2015 wird der Begriff „Technologieoffenheit“ in der Diskussion über einen Manipulationsschutz für Registrierkassen verwendet. Weitgehend unklar ist allerdings, was genau damit gemeint ist.

Dieses Dokument versucht erstmals, die Zusammenhänge zu analysieren und damit eine Diskussionsgrundlage zu liefern. Einige der Aspekte wurden bereits im *Whitepaper: Fiskalsysteme – Anforderungen und Lösungen* angeschnitten.

Der Begriff „Technologieoffenheit“ entstammt keiner Fachterminologie, sondern findet vor allem in Marketing und Politik Verwendung. Gemeint ist damit offenbar, dass …

- Politik und Gesetzgeber in Bezug auf die Umsetzung bestimmter Anforderungen möglichst wenig Vorgaben in Bezug auf die konkrete Lösung machen sollten,
- die Wirtschaft in der Folge größtmögliche Freiheit in der Umsetzung der Anforderungen erhalten sollte und
- dadurch der technische Fortschritt möglichst nicht durch Auflagen behindert wird.

Begriffe

Um Fehlinterpretationen der in diesem Dokument erläuterten Zusammenhänge zu vermeiden, werden hier die wesentlichen Begriffe definiert:

Registrierkasse: Jedes elektronische System, das Bargeschäfte verwaltet und digitale Aufzeichnungen darüber erstellt, also z.B. auch Taxameter oder Waagen mit Abrechnungsfunktionen. Mit dem eigentlichen Kassenplatz verbundene Systeme, die Aufzeichnungen speichern wie etwa eine zentrale Auswertungssoftware, sind im Sinne dieser Definition ebenfalls Teil der Registrierkasse.

Sicherungsverfahren: Grundsätzliche logische Strukturen und Prozeduren des Gesamtsystems einschließlich der Registrierkasse, die im Ergebnis die Einhaltung der in der Abgabenordnung (§§ 145 ff.) formulierten Anforderungen an Aufzeichnungen sicherstellen.

Sicherheitskomponente: Teilsystem der Registrierkasse als verbundenes oder integriertes Element, das die Integrität und Authentizität der Aufzeichnungen gewährleistet.

Kassen-Anwendung: Alle Teile der Registrierkasse (Hard- und Software), die nicht zur Sicherheitskomponente gehören, die also die gerätespezifischen Aufgaben erfüllen.

Bauartzulassung: Geräteprüfverfahren durch eine unabhängige Instanz, das die Erfüllung aller fachlichen Anforderungen bestätigt. Es wird hier bewusst nicht von „Zertifizierung“ gesprochen, um eine Verwechselung mit kryptografischen Zertifikaten zu vermeiden.

Marktüberwachung: Laufende Kontrollen der im Einsatz befindlichen Geräte auf Übereinstimmung mit den Anforderungen, korrekte Nutzung und Funktion.

Angenommene Anforderungen an das Sicherungsverfahren

Für die weitere Analyse werden folgende Anforderungen an das Sicherungsverfahren vorausgesetzt:

- Jede Registrierkasse bedarf einer eindeutig abgrenzbaren Sicherheitskomponente; ohne diese Abgrenzung wäre die ordnungsgemäße Funktion des Sicherungsverfahrens aufgrund der Komplexität des Gesamtsystems praktisch nicht prüfbar.
- Die Sicherheitsfunktionen dieser Komponente müssen durch neutrale Dritte zuverlässig prüfbar sein.
- Das Sicherungsverfahren muss (technisch und rechtlich) derart gestaltet sein, dass es Beweiskraft für Steuerpflichtige und Prüfbehörde gewährleistet. Das bedingt auch einen sehr hohen Grad an Manipulationssicherheit der Sicherheitskomponente.

Warum Technologieoffenheit?

Wie jede Forderung darf auch die Forderung nach Technologieoffenheit kein Selbstzweck sein, sondern muss zur Erreichung bestimmter Ziele dienen.

Folgende Faktoren können in der hier analysierten Situation durch die unterschiedliche Ausgestaltung der Vorgaben positiv oder negativ beeinflusst werden:

- Entwicklung von Funktionalitäten und Innovationen bei Registrierkassen
- Fairness des Wettbewerbs – auf Ebene der Kassenhersteller und auf Ebene der Anwender
- Kosten – das betrifft Anschaffungs- und laufende Kosten des Anwenders
- Aufwand des Gesetzgebers bei der Einführung, beispielsweise unter Berücksichtigung vergaberechtlicher Aspekte
- Aufwand für Prüfbehörden im Vollzug

Grundlegende Typen von Sicherungsverfahren

Um den Grad der Technologieoffenheit eines Verfahrens konkreter bestimmen zu können, werden diese im Folgenden in vier Typen unterteilt (Übersicht in Abbildung 1):

A: Das Sicherungsverfahren sowie dessen Implementierung sind freigestellt, es gibt lediglich eine Festlegung der zu erreichenden Sicherheitsziele.

B: Das Sicherungsverfahren selbst ist zwar definiert, die Implementierung des Verfahrens, also die konkrete Ausgestaltung der Sicherheitskomponente ist hingegen nicht reglementiert.

<table>
<tr><th>Typ</th><th>Verfahren</th><th>Implementierung</th><th>Anbieter</th></tr>
<tr><td>A</td><td>Offen</td><td rowspan="2">Offen</td><td rowspan="3">Mehrere</td></tr>
<tr><td>B</td><td rowspan="3">Vorgegeben</td></tr>
<tr><td>C</td><td rowspan="2">Vorgegeben</td></tr>
<tr><td>D</td><td>Einer</td></tr>
</table>

Abbildung 1: Typen von Sicherungsverfahren

C: Sicherungsverfahren und Implementierung sind vorgegeben, für die Sicherheitskomponente gibt es mehrere Anbieter

D: wie C, jedoch mit nur einem Anbieter der Sicherheitskomponente

Im Abschnitt „Beispiele für Sicherungsverfahren“ werden konkrete Beispiele für die hier aufgeführten Typen genannt.

Technologieoffenheit der Sicherheitskomponente

Innovationen und Wettbewerb im Bereich der Sicherheitskomponente haben keinen großen Einfluss auf den Kundennutzen. Die Hauptaufgabe der Komponente ist es, auf Grundlage des fachlichen Anforderungsprofils den größtmöglichen Grad an technischem Schutzniveau und damit an Rechtssicherheit zu gewährleisten. Dieses Sicherheitsniveau muss von Anfang an erreicht werden, also auch ohne dass erst eine eventuelle, zukünftige technische Weiterentwicklung stattfinden müsste. Eine Anpassung an den Stand der Technik (z.B. die Verwendung längerer Signaturschlüssel) oder an sich verändernde Risiken muss gleichwohl möglich sein.

Zugleich sollte die Sicherheitskomponente einen möglichst geringen Einfluss auf die Performance, Funktionalität und Flexibilität der Kassen-Anwendung haben.

Größere Fortschritte, die zu einem Kundennutzen führen, sind nur im Bereich der Kosten denkbar. Vor allem technisch aufwändige Sicherheitskomponenten, wie etwa komplexe „Fiskal-Boxen“ mit einem leistungsstarken Prozessor und viel Speicher, könnten durch technische Fortentwicklungen preiswerter werden. Je preiswerter eine Komponente bereits ist, desto geringer natürlich der Effekt der Einsparung.

Technologieoffenheit bei den Registrierkassen

Auf Ebene der Registrierkassen – also vor allem bei der Kassen-Anwendung – haben technische Anforderungen wesentlich größere Auswirkungen. Aufgrund dessen sollen hier die Effekte von Technologieoffenheit auf die oben genannten Faktoren analysiert werden.

Innovationsfreundlichkeit

Innovationen, die einen Kundennutzen bieten, finden ganz überwiegend im Bereich der Kassen-Anwendung statt.

Entscheidend ist demnach, inwieweit die Nutzung der Sicherheitskomponente Innovationen der Kassen-Anwendung behindert. Bestimmt wird dies vor allem durch den Umfang der Eingriffe und Auflagen, die aus dem Sicherungsverfahren resultieren. So wären etwa Einschränkungen auf ein bestimmtes Betriebssystem (Beispiel: Sicherheitskomponente läuft nur unter Microsoft Windows) oder eine bestimmte Schnittstelle (Beispiel: Es muss zwingend eine SD-Karte eingesetzt werden) deutlich innovationshemmend.

Ein weiterer Faktor sind funktionale Einschränkungen, wie sie bei konventionellen Fiskalsystemen an der Tagesordnung sind. Beispielhaft wären hier zu nennen:

- Langzeitspeicherung der Daten ist nur innerhalb der Registrierkasse erlaubt,
- bestimmte Bedienabläufe sind vorgegeben,
- praktisch relevante Kassenfunktionen werden verboten, meist infolge von fehlender Branchenkenntnis bei der Definition der Anforderungen.

Der grundlegende Ansatz des Sicherungsverfahrens spielt hier so gut wie keine Rolle. Die Auswirkung auf die Innovationsfreundlichkeit wird allein vom Umfang der Eingriffe in die Kassen-Anwendung selbst bestimmt. Dieser Zusammenhang wird in Abbildung 2 dargestellt (die Skala von 0 bis 100 verdeutlicht die Relationen und lässt sich nicht direkt in Kosten oder Zeitaufwand umrechnen).

Wettbewerbsverzerrungen

Bei regulatorischen Eingriffen kommt es oft zu erheblichen Wettbewerbsverzerrungen. Im Markt für Registrierkassen bestehen derartige Eingriffe vor allem aus mehr oder weniger komplexen technischen Auflagen, die aus dem Steuerrecht resultieren. Diese können je nach gewähltem technischen Ansatz des Registrierkassen-Herstellers unterschiedlich leicht bzw. unterschiedlich schnell erfüllt werden. Das Ausmaß der dadurch entstehenden Wettbewerbsverzerrungen hängt ausschließlich vom Umfang der Eingriffe in die Kassen-Anwendung ab. Die Zusammenhänge sind identisch mit den im Abschnitt „Innovationfreundlichkeit“ und ebenfalls in Abbildung 2 dargestellten.

Durch konzeptionelle Mängel des Sicherungsverfahrens kann es darüber hinaus ebenfalls zu Wettbewerbsverzerrungen kommen, wenn einzelne Anbieter darauf basierende Sicherheitslücken ausnutzen. In dieser Analyse wird allerdings vorausgesetzt, dass derartige Schwachstellen nicht vorhanden sind.

Aufwand für den Anwender

Die Kosten für den Anwender werden zu einem – oft erheblichen – Teil von der Sicherheitskomponente bestimmt. So sind etwa die Kosten für Online-Lösungen (die laufende Betriebskosten bedingen) oder für komplexe Fiskal-Boxen (wie sie bei-

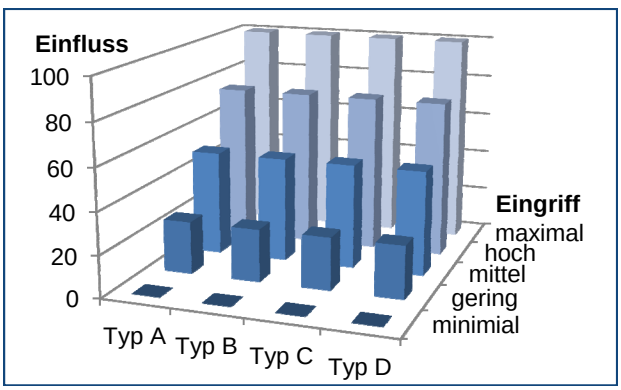

Abbildung 2: Einfluss auf Innovation und Wettbewerb

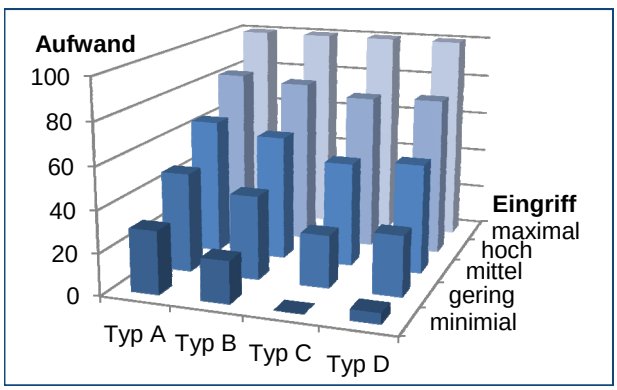

Abbildung 3: Aufwand für Anwender

spielsweise in Schweden und Belgien Verwendung finden) erheblich. Diese Kosten hängen weniger vom grundsätzlichen Ansatz des Sicherungsverfahrens, sondern vielmehr von der konkreten Ausgestaltung der Vorschriften ab.

Ein wesentlicher Teil der Kosten wird aber meist durch den Aufwand im Bereich der Kassen-Anwendung selbst bestimmt. So bedingen komplexe technische Anforderungen einen erheblichen Aufwand bei Entwicklung, Wartung und Support. Diese Kosten werden an die Kunden weitergegeben. Da alle Anbieter gleichermaßen von diesen Auflagen betroffen sind, kann auch keine Kostenreduktion durch Wettbewerb erzielt werden.

Je komplexer die Auflagen für die Kassen-Anwendung selbst sind, desto notwendiger ist aus Sicherheitsgründen die Überprüfung ihrer Einhaltung durch Bauartzulassungsverfahren. Weitgehende Eingriffe in die Kassen-Anwendung bedingen derartige Prozeduren, da nur so die Einhaltung aller Auflagen nachweisbar ist. In diesem Fall ist erfahrungsgemäß mit einer ganz erheblichen Kostenzunahme zu rechnen. Da weiterentwickelte Produktversionen jeweils neu zugelassen werden müssen, werden Innovationen massiv behindert. Das ideale Sicherungsverfahren stellt daher nur Anforderungen an die Sicherheitskomponente, beinhaltet aber keine weiteren Bauartanforderungen an die Registrierkassen und erfordert somit auch keine Bauartzulassung.

Je stärker eine Sicherheitskomponente standardisiert ist, desto einfacher und damit preiswerter ist sie in eine Registrierkasse zu integrieren. Existiert nur ein Anbieter von Sicherheitskomponenten, könnte der Preis für diese höher ausfallen als bei einem Wettbewerb mehrerer Anbieter. In Schweden und Belgien hat dieser Marktmechanismus allerdings nicht funktioniert; trotz einer Mehrzahl von Anbietern liegen die Marktpreise allein für die Fiskal-Boxen bereits bei mehreren Hundert Euro.

Das sich daraus ergebende Gesamtbild wird in Abbildung 3 veranschaulicht.

Aufwand des Gesetzgebers bei Einführung

Auf Seiten des Gesetzgebers wird der Einführungsaufwand weniger durch den Grad des Eingriffs in die Kassen-Anwendung bestimmt. Die Formulierung komplexer Anforderungen mag etwas aufwändiger sein – umsetzen müssen sie aber die Hersteller.

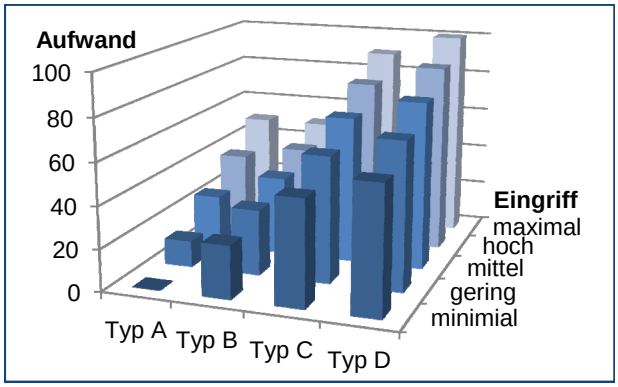

Abbildung 4: Aufwand für den Gesetzgeber

Die präzise Festlegung des Sicherungsverfahrens erzeugt demgegenüber deutlich mehr Aufwand. Es muss ein konkret ausformuliertes Anforderungsprofil und darauf basierend eine Spezifikation erstellt werden. Eine entsprechende technische Lösung ist zu entwickeln oder zu beschaffen. Detaillierte technische Regeln bedingen auch einen gewissen Aufwand zur Vermeidung eventueller vergaberechtlicher Probleme.

Dargestellt werden diese Zusammenhänge in Abbildung 4.

Aufwand der Verwaltung im Praxiseinsatz

Bei den Prüfbehörden – also vor allem im Steuervollzug – reduziert jede Standardisierung den Arbeitsaufwand und die Fehlerquote. Vorgegebene Implementierungen von Sicherungsverfahren (Typ C oder D) führen hier also zu wesentlichen Vereinfachungen gegenüber offenen Implementierungen (Typ A oder B), die zwangsweise einen erheblichen Aufwand und spezialisiertes Personal zur Marktüberwachung erfordern.

Der Aufwand zur Ermittlung aller gesicherten Registrierkassen eines Steuerpflichtigen kann minimiert werden, wenn Ausgabe und Verwaltung

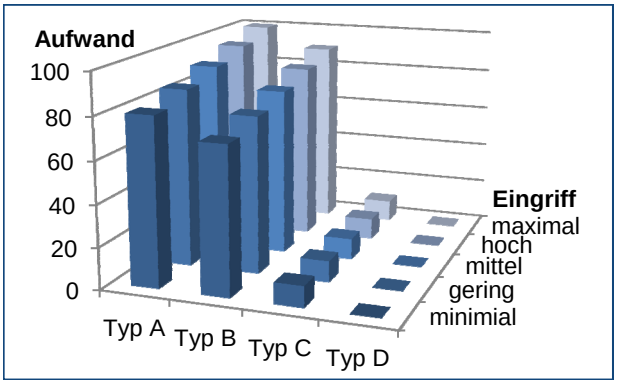

Abbildung 5: Aufwand der Verwaltung

der Sicherheitskomponenten auf eine zentrale Stelle beschränkt sind. Diese Information ist grundlegende Voraussetzung für eine flächendeckende Marktüberwachung.

Dürfen ausschließlich mit einer standardisierten Sicherheitskomponente versehene Registrierkassen genutzt werden, muss sich die Verwaltung nicht mehr auf Ebene der Kassen-Anwendung mit Registrierkassen befassen.

Dargestellt wird dieser Zusammenhang in Abbildung 5.

Beispiele für Sicherungsverfahren

Vor diesem Hintergrund lassen sich für die oben bezeichneten grundlegenden Typen von Sicherungsverfahrend folgende Beispiele anführen:

A: Ansätze dieser Art, die eine so große Sicherheit bieten, dass sie Beweiskraft hätten, sind nicht bekannt. Unabhängig von dieser nicht erfüllten Grundanforderung fallen folgende Verfahren in diese Kategorie:

- Software-Testate nach PS880 in Deutschland
- NF525 in Frankreich
- „Keurmerk Het Betrouwbare Afrekensysteem“ in den Niederlanden

B: Auf Signaturen (reine Softwarelösung mit bekannten Sicherheitslücken) basierendes System in Portugal

C: Fast alle konventionellen Fiskalsysteme, System in Schweden und Belgien, Verfahren der österreichischen Registrierkassensicherheits-Verordnung, INSIKA bei Vergabe der Smartcards durch mehrere Trustcenter

D: Online-System in Kroatien, INSIKA bei nur einem Trustcenter

In Abbildung 6 ist dargestellt, wie sich diese Beispiele nach den hier dargestellten Kriterien einordnen lassen.

Parallelen

An den folgenden Beispielen (nicht nur aus dem Bereich sicherer IT-Lösungen) wird deutlich, wo Technologieoffenheit sinnvoll ist und wo sie ihre Grenzen findet.

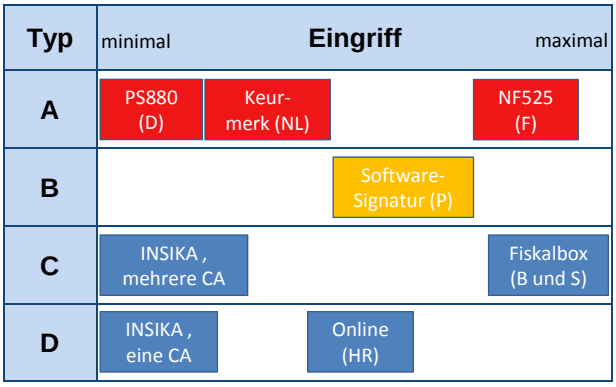

Abbildung 6: Beispiele (rot: unsicher, gelb: Sicherheitslücken bekannt)

Digitale Tachografen (Fahrtenschreiber)

In den meisten Lkw und Bussen in der EU müssen Fahrtenschreiber zur Erfassung der Lenk- und Ruhezeiten verwendet werden. In Fahrzeugen, die nach dem 1. Mai 2006 neu zugelassen wurden, müssen digitale Fahrtenschreiber verwendet werden.

Ein wesentlicher Teil der Sicherheit beruht auf Smartcards für Fahrer, Unternehmer etc. Die Funktion der Karten ist exakt vorgegeben. Die Karten werden von verschiedenen Stellen im Auftrag des Kraftfahrt-Bundesamtes ausgegeben. Fahrtenschreiber werden von verschiedenen Herstellern angeboten. Die digitalen Tachografen entsprechen damit dem oben definierten Typ D, wobei die Anbieterauswahl für die Smartcards durch Ausschreibung erfolgt. Bei den Smartcards gibt es nur eine teilweise Technologieoffenheit – die Implementierung wird offen gelassen, Funktionen und Schnittstellen sind vorgegeben.

Politisch, rechtlich, technisch und praktisch funktioniert dieser Ansatz. Obwohl es im Teilbereich der Smartcards keine vollständige Technologieoffenheit gibt, werden die Hersteller der Fahrtenschreiber durch klare Schnittstellen und minimale Eingriffe in Bezug auf Innovationen, Wettbewerb und Technologie nicht behindert.

E-Bilanz

Der Sinn der E-Bilanz ist die standardisierte Übermittlung von Jahresabschlussdaten an die Finanzbehörden. Das erfordert zwangsläufig eine eindeutige Vorgabe für Datenformate, Inhalte und Übertragungsverfahren. Mit welcher Technik der Steuerpflichtige diese Daten erzeugt, ist ihm allerdings völlig freigestellt. In diesem Sinne ist das Verfahren einerseits völlig technologieoffen, andererseits jedoch sehr restriktiv. Insgesamt führt

diese Kombination – trotz aller Anlaufschwierigkeiten – zu einem funktionierenden System.

Rechnungssignatur gem. §14 UStG

Die von Anfang 2004 bis Mitte 2011 geltende gesetzliche Regelung für Rechnungssignaturen entsprach dem oben definierten Typ A. Es war also nicht nur die Implementierung unreguliert, auch für das genaue Verfahren gab es keine Vorgaben – es wurden lediglich qualifizierte elektronische Signaturen verlangt. Mithin fehlte es an einer Festlegung, was genau durch die Signatur zu schützen ist. In der Folge hat hier jeder Anbieter eine eigene Variante implementiert, was zwei wesentliche Konsequenzen hatte:

- Für die Prüfung einer Rechnung gab es keinen Standardmechanismus, sondern viele verschiedene Lösungen, so dass praktisch gar keine Prüfung möglich war. Auch eine automatisierte Prüfung mehrerer Rechnungen war nicht durchführbar.
- Die Prüfung erfolgte nicht mit einer Software der Finanzbehörden, sondern einem jeweils herstellerspezifischen Programm, dem der Prüfer vertrauen musste.

So hat das Verfahren im Ergebnis nicht funktioniert. Aus diesem Grund und bedingt durch weitere EU-Vorgaben konnte dieses offensichtlich mangelhafte Verfahren nicht weiter vorgegeben werden.

Zusammenfassung

Wie bei jeder komplexen Fragestellung muss auch beim Thema Technologieoffenheit das Gesamtbild und nicht nur eine einzelne Perspektive betrachtet werden.

Mit der Forderung nach Technologieoffenheit soll erreicht werden, dass behördliche Auflagen möglichst keine Kostensteigerung, Innovationsbehinderung und Wettbewerbsverzerrung bewirken.

Für sichere Registrierkassen ist daher einerseits wichtig, dass die Kassen-Anwendung durch die Sicherheitskomponente nur minimal behindert wird, um so Innovationsfähigkeit und Wettbewerb zu gewährleisten. Andererseits sollte die Funktion der Sicherheitskomponente so weit wie möglich vorgegeben werden, um Aufwände für Implementierung, Prüfbarkeit und Verwaltung zu minimieren.

Bei Registrierkassen mit einem Manipulationsschutz für die steuerlich relevanten Aufzeichnungen wird dies vor allem durch das Ausmaß der Eingriffe in die Kassen-Anwendung (das sog. „Host-System“) bestimmt. Die genaue Ausgestaltung der Sicherheitseinrichtung selbst hat hier kaum einen Einfluss. Freiheiten bei der Umsetzung der Anforderungen an die Sicherheitseinrichtung sind jedoch unbedingt wünschenswert, um Abhängigkeiten von bestimmten Technologien, Anbietern oder Produkten weitgehend zu vermeiden.

Die fehlende Festlegung auf ein Sicherheitskonzept erleichtert zwar ein Gesetzgebungsverfahren, schafft aber ansonsten eine Reihe zusätzlicher Probleme statt sie zu lösen.

Unter den hier analysierten Aspekten ist das INSIKA-Verfahren die beste verfügbare Lösung und stellt deshalb in der Gesamtbetrachtung die technologieoffenste Lösung dar.

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. Seit 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 den aufwändigen konventionellen „Fiskalkassensystemen“ zu bieten. Ein besonderer Schwerpunkt ist die Rechtssicherheit für die Anwender der Systeme.

Kontakt

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

www.insika.de
E-Mail: info@insika.de