Stand 12. Oktober 2016

Stellungnahme des DFKA e.V. zum Entwurf eines „Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen“

zur öffentlichen Anhörung in der 89. Sitzung des Finanzausschusses am 17. Oktober 2016 in Berlin zum Regierungsentwurf vom 13. Juli 2016, Bundestagsdrucksache 18/9535

Für die Anbieter – also die Hersteller und Vertreiber – von Registrierkassen ist der Gesetzentwurf ein **sehr wichtiger Schritt in die richtige Richtung**. Durch den Einsatz der gesetzlich vorgeschriebenen Sicherheitseinrichtung können die Anbieter damit in Zukunft eine weitgehende Rechtssicherheit erlangen. Die Beschränkung der Zertifizierungspflicht auf die Sicherheitseinrichtung (anstelle einer Zertifizierung des Gesamtsystems) ist ebenfalls sehr positiv, weil damit der technische Fortschritt und die – auch internationale – Wettbewerbsfähigkeit der Anbieter nicht behindert werden.

Nach Auffassung des DFKA ist der Gesetzentwurf in der vorliegenden Form jedoch **noch nicht praktikabel**. Die wesentlichen negativen Folgen haben die Anwender von Registrierkassen und die Finanzverwaltung zu tragen. Aber auch für die Anbieter der Systeme entstehen wirtschaftliche Risiken, z.B. durch mögliche Verzögerungen bei der Umsetzung.

Wesentliche Zielvorgaben im Gesetzentwurf sind zu unscharf, um eine erfolgreiche Umsetzung sicherstellen zu können.

Im Einzelnen ergeben sich die folgenden Feststellungen und Forderungen:

1. **Politische Kompromisse bei technischen Sicherungskonzepten oft unmöglich**: Technische Sicherheitsverfahren bestehen aus mehreren exakt ineinandergreifenden Komponenten. Bereits kleine, unsachgemäße Veränderungen können das gesamte Verfahren weitgehend wirkungslos machen.
2. **Ohne Kassenpflicht droht die „Flucht in die offene Ladenkasse“**: Der Druck zur Hinterziehung von Steuern und Sozialabgaben war und ist in vielen Branchen derart groß, dass oft mit hoher krimineller Energie vorgegangen wird. Da der vorliegende Gesetzentwurf nicht die Ursachen bekämpfen kann, werden diese bestehen bleiben und sehr wahrscheinlich ein vermehrtes Ausweichen auf die kaum prüfbare offene Ladenkasse bewirken. Zu verhindern ist das nur durch eine allgemeine Kassenpflicht (mit sinnvollen Ausnahmeregelungen).
3. **Eine Belegpflicht ist unbedingt erforderlich**: Nur eine Belegpflicht erlaubt wirkungsvolle Kontrollen der korrekten Funktion und Nutzung der Registrierkassen. Dazu müssen die Belege über ein prüfbares Sicherheitsmerkmal verfügen. Unter bestimmten Voraussetzungen sind auch elektronische Belege möglich.
4. **Ausreichende Kontrolldichte ist Voraussetzung für einen Erfolg**: Nur durch ausreichend häufige Kontrollen in Form von Kassennachschauen sind eine Verhaltensänderung und damit ein gleichmäßiger Steuervollzug zu bewirken. Das einzuführende Sicherungsverfahren muss daher – anders als das im vorliegenden Gesetzentwurf umrissene – diese Kontrollen einfach, schnell und effektiv machen.
5. **Erweiterte Aufzeichnungen sind kein Ersatz für Belegpflicht und Kassennachschau**: Eine Aufzeichnung „anderer Vorgänge“ (von der Uhrzeit eines Vorgangsbe-

ginns bis hin zu jedem Tastendruck[1]) kann die Belegpflicht nicht ersetzen, sondern führt lediglich zu einer nicht prüfbaren Datenflut.

6. **Zentrales Verzeichnis aller Sicherheitseinrichtungen unumgänglich**: Nur wenn die Finanzverwaltung jederzeit einfach ermitteln kann, welche Registrierkassen bzw. Sicherheitseinrichtungen bei einem Steuerpflichtigen im Einsatz sind, kann und muss von einer Vollständigkeit der Daten ausgegangen werden. Sonst muss – zum Nachteil der Steuerpflichtigen – immer angenommen werden, dass nicht alle Umsatzdaten vorgelegt wurden (es besteht also keine Ordnungsmäßigkeitsvermutung in Bezug auf die Vollständigkeit der Daten).
7. **Sicherungsmaßnahmen gegen technische Störungen nötig**: Die Auswirkungen von Datenverlusten aufgrund technischer Störungen muss minimiert werden, vor allem um die Interessen der Anwender zu schützen. Da Derartiges vor allem in der Verordnung und den technischen Richtlinien umzusetzen ist, sollten jedenfalls die Eckpunkte bereits im Gesetz verankert sein.
8. **Einheitliche Datenschnittstelle einführen**: Die im Gesetzentwurf ausdrücklich erwähnte „einheitliche digitale Schnittstelle“ soll vermutlich auch eine Standardisierung der aufzuzeichnenden Daten beinhalten. Dieses Konzept ist ausdrücklich zu begrüßen und sollte unbedingt umgesetzt werden, da durch klare Vorgaben in diesem Punkt Rechtssicherheit erreicht wird. Vermeintliche Freiheiten für Anbieter an dieser Stelle sind kontraproduktiv und daher abzulehnen, da sie erfahrungsgemäß in der Folge immer zu Auseinandersetzungen über die Ordnungsmäßigkeit führen.
9. **Zulassung des INSIKA-Verfahrens unbedingt sinnvoll**: Mit INSIKA existiert ein Verfahren, das technologieoffen sowie herstellerneutral ist und auf Basis der Anforderungen der Finanzbehörden teilweise mit Steuergeldern entwickelt wurde. Es ist praktisch erprobt, bewährt, preiswert und unmittelbar einsetzbar. Es ist kein Grund erkennbar, warum dieses Verfahren nicht in unveränderter Form zugelassen werden soll (ggf. mit einer kleinen Aktualisierung im Bereich der verwendeten kryptografischen Funktionen sowie einer BSI-Zertifizierung).
10. **Sinnvolle Fristen festlegen**: Bei Einführungs- und Übergangsfristen ist zum einen zu bedenken, dass erst bei der allgemeinen Pflicht zum Einsatz der Sicherheitseinrichtung das Ziel des gleichmäßigen Steuervollzugs erreicht ist, also Manipulation verhindert und ehrliche Steuerzahler geschützt werden. Zum anderen muss die Zeit für Konzeption, Entwicklung, Erprobung und flächendeckende Installation berücksichtigt werden. Je einfacher die Verfahren sind und je mehr auf Bewährtes zurückgegriffen wird, desto kürzer kann die Zeitspanne sein.
11. **Einbindung aller Stakeholder erforderlich**: Ein Großteil der Beteiligten – also Steuervollzug, Anbieter und Anwender von Registrierkassen – waren in das bisherige Verfahren nicht eingebunden. Sollte dies nicht korrigiert werden, muss mit Verzögerungen, hohen Kosten und einer beschränkten Tauglichkeit des Ergebnisses gerechnet werden. Vor allem ist das bei der Ausarbeitung der Rechtsverordnung zu beachten.

Die Forderungen unter 3, 6, 9 und 10 decken sich mit den Empfehlungen des Bundesrates vom 23. September 2016.[2] Im Übrigen betont auch der Bundesrat die Wichtigkeit der Verordnung für den Erfolg der Maßnahmen.

Anlage: Ausführliche Erläuterung der einzelnen Aussagen dieser Stellungnahme inkl. einer Analyse der Auswirkung der Aufzeichnung „anderer Vorgänge“

---

1 MdB Uwe Feiler, Rede Bundestag 22.9.2016: „Zukünftig wird ab dem ersten Tastendruck jede Eingabe in das Kassensystem protokolliert.“

2 Bundesrat Drucksache 407/16 (Beschluss)

Stand 12. Oktober 2016

Anlage zur Stellungnahme des DFKA e.V. zum Entwurf eines „Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen“

Erläuterungen und Hintergrundinformationen

Hinweis: Alle fünf Abschnitte sind jeweils für sich lesbar und verständlich. Im Abschnitt 3 sind die einzelnen Punkte der Stellungnahme jeweils erläutert.

1 Ausgangssituation für Lieferanten von Registrierkassen

Das wesentliche Ziel der Hersteller und Vertreiber von Registrierkassen ist bereits mit dem Regierungsentwurf des „Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen“ vom 13. Juli 2016 erreicht: Bei Einsatz der vorgeschriebenen Sicherheitseinrichtung besteht weitgehende Rechtssicherheit für die Lieferanten. In dieser Hinsicht ist aus Sicht des DFKA bereits ein sehr wichtiger Schritt in die richtige Richtung vollzogen worden.

Für die Anwender von Registrierkassen, also die Steuerpflichtigen sowie für die Finanzverwaltung ist das im Gesetzentwurf vorgesehene Verfahren jedoch unnötig teuer und aufwändig. Nach Ansicht des DFKA ist daher unbedingt eine Korrektur verschiedener Punkte erforderlich. Nur dann lassen sich die Ziele, über die weitgehender Konsens besteht, auch tatsächlich erreichen.

2 DFKA e.V. und INSIKA

Der Deutscher Fachverband für Kassen- und Abrechnungssystemtechnik (DFKA) e.V. wurde 2012 gegründet, um die Interessen von Herstellern, Fachhändlern, Softwarehäusern, Dienstleistern aus der Branche der Kassen und Abrechnungssysteme zu vertreten.

Das INSIKA-Verfahren (INtegrierte SIcherheitslösung für messwertverarbeitende KAssensysteme) wurde auf der Grundlage eines Konzepts der deutschen Finanzbehörden von der Physikalisch-Technischen Bundesanstalt (PTB) in den Jahren 2008 bis 2012 in einem Gemeinschaftsprojekt mit der Industrie entwickelt und erprobt. Nach erfolgreichem Projektabschluss wird das INSIKA-Verfahren vom ADM e.V. (Anwendervereinigung Dezentrale Mess-Systeme) unterstützt und weiterentwickelt. Im Taxi-Bereich wird INSIKA tausendfach erfolgreich eingesetzt. Der ADM e.V. bietet keine auf INSIKA basierenden Produkte an und erhebt keine Lizenzgebühren oder Ähnliches für die Nutzung.

Es bestehen keine wirtschaftlichen Beziehungen zwischen dem DFKA e.V. oder dessen Mitgliedern auf der einen und dem ADM e.V. oder potenziellen Anbietern von INSIKA-Sicherheitseinrichtungen auf der anderen Seite. Ein wirtschaftlicher Vorteil für DFKA-Mitglieder (sowie für alle anderen Anbieter) durch die Nutzung des INSIKA-Verfahrens liegt daher maximal in Kostenvorteilen gegenüber alternativen Ansätzen.

3 Erläuterung der Feststellungen und Forderungen

Im Folgenden werden die Aussagen des DFKA zum Regierungsentwurf ausführlich erklärt und begründet (die Nummerierung innerhalb dieses Abschnitts entspricht der aus der Stellungnahme).

3.1 Politische Kompromisse bei technischen Sicherungskonzepten oft unmöglich

Sicherheitsverfahren in der Informationstechnik bestehen praktisch immer aus mehreren miteinander verknüpften Elementen, die insgesamt zu einer Absicherung gegen bestimmte Bedrohungen führen. Neben Hard- und Software spielen dabei auch Verfahren und Abläufe eine große Rolle.

So erfüllt z.B. die qualifizierte elektronische Signatur (QES)[1] nur den gewünschten Zweck, weil kryptografische Signaturalgorithmen mit passender Hard- und Software (meistens Smartcards), organisatorischen Verfahren (vor allem im Rahmen der Public-Key-Infrastructure, die zur Beantragung und Verwaltung von kryptografischen Zertifikaten dient) sowie einer Zertifizierung der wesentlichen Komponenten durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) kombiniert werden. Würde man hier einzelne Elemente wegfallen lassen, z.B. die Identitätsprüfung beim Erwerb einer Signaturkarte, wäre das gesamte Verfahren weitgehend nutzlos.

Fazit: In der Diskussion über die Manipulationssicherung bei Registrierkassen können politische Kompromisse (z.B. in Bezug auf die Belegpflicht) zur weitgehenden Untauglichkeit des resultierenden Verfahrens führen.

3.2 Ohne Kassenpflicht droht die „Flucht in die offene Ladenkasse“

Die Erfahrungen aus vielen Staaten zeigen, dass es in bestimmten Branchen einen massiven Druck zur Umsatzverkürzung gibt.[2] Neben der Steuerhinterziehung ist die Finanzierung von Schwarzarbeit hier ein wesentlicher Faktor. Ein freiwilliges Ausscheren aus dem „Schwarzgeld-Kreislauf“ würde für viele Unternehmen einen existenzgefährdenden Wettbewerbsnach-

[1] Die Rahmenbedingungen für die QES werden im Signaturgesetz definiert.
[2] Siehe z.B. OECD, *Umsatzverkürzung mittels elektronischer Kassensysteme: Eine Bedrohung für die Steuereinnahmen*, 02/2013

teil bedeuten. Veränderungen erfordern „gleiche Regeln für alle“ und einen einheitlichen Stichtag.

Eine gesetzliche Manipulationssicherung für Registrierkassen ohne Kassenpflicht zeichnet den „Ausweg“ durch den Verzicht auf eine Registrierkasse vor. Es ist davon auszugehen, dass dieser Ausweg auch genutzt wird.

Fazit: Nur eine allgemeine Kassenpflicht kann die „Flucht in die offene Ladenkasse“ systematisch verhindern. Härte- und Sonderfälle müssen und können über klar definierte Ausnahmetatbestände abgefangen werden.

3.3 Eine Belegpflicht ist unbedingt erforderlich

Kein technisches System kann allein die einfachsten und am weitesten verbreiteten Manipulationen – vor allem die Nichteingabe oder die Verwendung von „Zweitkassen“[3] – verhindern. Es sind stets Kontrollen durch Vertreter der Behörden erforderlich. Die Wahl des Systems hat jedoch einen großen Einfluss auf den Aufwand für diese Kontrollen (die hier in Form von Kassen-Nachschauen stattfinden).

Ablauf einer Kontrolle ohne Belegpflicht:

- Testkauf oder Beobachtung, dabei müssen sämtliche Details – also z.B. die genaue Uhrzeit, gekaufte Waren, Preise – erfasst werden
- Datenzugriff
- Daten in Rechner des Prüfers einlesen
- Überprüfung, ob der Testkauf bzw. der beobachtete Kauf in den Daten vorhanden und korrekt abgelegt ist

Ablauf einer Kontrolle mit Belegpflicht:

- Beobachtung (bei Bedarf auch Testkauf)
- Stichprobenartige Belegkontrolle (bei maschinenlesbarem Sicherheitsmerkmal, also z.B. einem QR-Code, ohne manuellen Aufwand möglich):
    - Korrekte Signatur?
    - Übereinstimmung Beleginhalte mit Signatur (also: stimmen Datum, Zeit, Sequenznummer und Gesamtbetrag überein)?
- Datenzugriff ist nur in Verdachts- oder besonderen Einzelfällen erforderlich

Eine Kassen-Nachschau ohne Belegpflicht – die immer einen Datenzugriff und eine Auswertung der Daten bedingt – wird selbst bei einer kompletten Standardisierung der Schnittstellen einen Aufwand von jeweils mehreren Stunden für Unternehmen und Finanzverwaltung bedeuten.

Hinweis: Belege können grundsätzlich auch in elektronischer Form erstellt werden, sofern die hier beschrieben Kontrollen damit möglich sind. Die dafür nötige Standardisierung existiert im Kassenbereich allerdings noch nicht. Mit der Übertragung der Daten per Mobilfunk beim Einsatz von INSIKA in Taxametern ist bereits heute ein prüfbares elektronisches Belegverfahren praktisch umgesetzt.

Fazit: Nur mit einer Belegpflicht sind wirksame Kontrollen (Kassen-Nachschauen) möglich, die für Finanzverwaltung sowie Steuerpflichtige mit geringem Aufwand verbunden sind.

[3] Damit sind Kassenplätze gemeint, die normal genutzt werden, deren Daten bei einer Prüfung jedoch nicht vorgelegt werden.

3.4 Ausreichende Kontrolldichte ist Voraussetzung für einen Erfolg

Die heutige durch Betriebsprüfungen und Kassen-Nachschauen erreichte Kontrolldichte hat nicht zu einem Ende der Manipulationen geführt. Nicht einmal die Nachrüstungsverpflichtungen aus dem BMF-Schreiben vom 26.11.2010[4] konnten großflächig durchgesetzt werden.

Um diesen Zustand zu verändern, ist daher eine deutliche Intensivierung der Kontrollen erforderlich. Wenn bundesweit ca. 500 Personen[5] Kassen-Nachschauen durchführen und diese im Normalfall ca. 30 Minuten dauern würden (inkl. Weg zwischen zwei Kontrollen), ließe sich jede Verkaufsstelle im Schnitt etwas mehr als einmal pro Jahr kontrollieren.[6] Hier kann dann von einer ausreichenden Wirkung ausgegangen werden.

Fazit: Eine ausreichende Kontrolldichte ist möglich. Dies erfordert schnelle und effektive Kassen-Nachschauen, die nur mit Belegkontrollen möglich sind. Kassen-Nachschauen mit Datenzugriff sind dafür zu zeitaufwändig.

3.5 Erweiterte Aufzeichnungen sind kein Ersatz für Belegpflicht und Kassen-Nachschau

Die Aufzeichnung „anderer Vorgänge“ oder sogar die „jedes Tastendrucks“[7] hätte die folgenden Auswirkungen:

- Sie produziert sehr große Datenmengen, die nur schwer zu handhaben sind.
- Eine ausreichend schnelle Verarbeitung durch marktübliche Signaturerstellungseinheiten ist sehr fraglich.
- Die Daten sind praktisch unprüfbar – nicht nur von der Menge her, sondern vor allem, weil Prüfer dazu jedes auf dem Markt befindliche System im Detail verstehen müssten.
- Die Registrierkassen selbst sollen – sinnvollerweise – nicht zertifiziert werden, sondern allein die Sicherheitseinrichtungen. Die Aufzeichnung aller Tastendrücke wäre jedoch eine Bauart-Anforderung an die Registrierkassen, die eine Zertifizierung des Gesamtsystems erfordern würde. Hier ist der Gesetzentwurf in sich widersprüchlich.
- Der Nutzen ist sehr begrenzt, siehe dazu Abschnitt 5.

Fazit: Aufzeichnungen über die eigentlichen Geschäftsvorfälle hinaus sind nicht praktikabel und kein Ersatz für eine Belegpflicht.

3.6 Zentrales Verzeichnis aller Sicherheitseinrichtungen ist unumgänglich

Nur wenn die Finanzverwaltung einfach und schnell ermitteln kann, welche Sicherheitseinrichtungen im Unternehmen eines Steuerpflichtigen in Benutzung sind, kann bei einer Prüfung festgestellt werden, ob auch alle Daten vorgelegt wurden. Andernfalls ist nur sehr schwer zu erkennen, wenn Daten einzelner Kassen fehlen.[8]

Beginnt eine Prüfung nicht mit der Gewissheit, dass die Daten aller vom Unternehmen betriebenen Registrierkassen vorliegen, gibt es in Bezug auf die Vollständigkeit der Kassen keine Verbesserung gegenüber dem Status quo. Die Rechtssicherheit für die Unternehmen wäre dann deutlich schlechter als möglich, der Aufwand für die Finanzverwaltung bei Prüfungen höher.

---

[4] Das BMF-Schreiben *Aufbewahrung digitaler Unterlagen bei Bargeschäften* vom 26.11.2010 fordert die unverzügliche Umstellung aller Systeme auf Einzelaufzeichnungen, die Übergangsregelung bis zum 31.12.2016 gilt nur für bauartbedingt nicht nachrüstbare Systeme.

[5] Angesichts von insgesamt ca. 20.000 Mitarbeitern der Außenprüfung und der Finanzkontrolle Schwarzarbeit erscheint diese Anzahl realistisch.

[6] Zur Herleitung vgl. http://www.insika.de/news/54-kostenanalyse-insika

[7] MdB Uwe Feiler, Rede Bundestag 22.9.2016: „Zukünftig wird ab dem ersten Tastendruck jede Eingabe in das Kassensystem protokolliert.“

[8] Das wäre nur möglich durch einen Datenabgleich zwischen Kassen-Nachschau und Prüfung – das würde den Aufbau eines speziellen IT-Systems in der Finanzverwaltung erfordern.

Die zentrale Erfassung aller Registrierkassen bzw. Sicherheitseinrichtungen ist dementsprechend absoluter Standard bei bestehenden, internationalen Kassensicherheitslösungen.

Hinweis: Falls es keine einheitliche, sondern mehrere verschiedene Sicherheitslösungen gibt, ist die Führung eines zentralen Verzeichnisses organisatorisch und technisch aufwändiger, aber möglich. Es müsste von einer übergeordneten Instanz geführt werden, also z.B. vom Bundeszentralamt für Steuern. Sonst könnte der Betreiber der einheitlichen Sicherheitslösung diese Aufgabe übernehmen.

Fazit: Ein zentrales Verzeichnis aller Sicherheitseinrichtungen ist unumgänglich, um maximale Rechtssicherheit zu erreichen und den Aufwand für die Finanzbehörden zu minimieren.

3.7 Sicherungsmaßnahmen gegen technische Störungen nötig

Auch bei einer Manipulationssicherung von Einzelaufzeichnungen besteht immer das Risiko eines Datenverlustes durch technische oder Bedienfehler. Das Hauptrisiko trägt dabei der Steuerpflichtige, da ohne zuverlässige Datengrundlage bei einer Prüfung die Schätzung droht.

Eine technische Sicherheitslösung sollte daher unbedingt auch für diesen Fall vertrauenswürdige Gesamtumsatzdaten bereitstellen.

Fazit: Diese Forderung hat vor allem Auswirkungen auf die Verordnung und die technischen Richtlinien. Das Konzept sollte aber bereits im Gesetz grundsätzlich verankert sein.

3.8 Einheitliche Datenschnittstelle einführen

Bisher lehnt die Finanzverwaltung jede Festlegung konkreter Dateninhalte im Bereich der Registrierkassen ab. In der Folge sind Auseinandersetzungen über die Ordnungsmäßigkeit der vorgelegten Daten an der Tagesordnung, wobei sich die Beurteilung auch noch von Fall zu Fall unterscheidet.

In anderen Themenfeldern wie z.B. der Taxonomie für die E-Bilanz gibt es jedoch solche Vorgaben.[9] Auch der Gesetzentwurf scheint mit der „einheitlichen digitalen Schnittstelle“ diesen Ansatz zu verfolgen.

Fazit: Zur Schaffung von Rechtssicherheit für Anbieter und Nutzer sowie zur Vereinfachung von Prüfungen ist eine einheitliche Datenschnittstelle unbedingt sinnvoll. Eher kurzlebige technische Details sollten dabei nicht vorgegeben werden.[10]

3.9 Zulassung des INSIKA-Verfahrens unbedingt sinnvoll

Der Gesetzentwurf schließt im Begründungsteil immer noch die Verwendung des INSIKA-Verfahrens aus, jedenfalls in der fertig entwickelten und praktisch erprobten Version. Zugestanden wird lediglich, dass man Teile davon in modifizierter Form verwenden kann, was allerdings das Sicherheitskonzept aushebeln würde. Gleichzeitig wird jedoch der Anspruch der Technologieoffenheit formuliert.

Das INSIKA-Verfahren erforderte einen Zeitraum von vier Jahren (2004 bis 2007) für die Entwicklung des Grundkonzepts. Dies erfolgte in einer Zusammenarbeit von Bundesministerium der Finanzen (BMF), Länderfinanzverwaltungen und PTB. Die technische Feinkonzeption, Spezifikation, Entwicklung und Erprobung fand in einem Projekt der PTB zusammen mit einem Herstellerkonsortium statt. Diese Phase lief ebenfalls über einen Zeitraum von vier Jahren (2008 bis 2012). Das INSIKA-Verfahren ist kurzfristig ohne weitere Entwicklung und Erprobung einsetzbar.

---

[9] Die Taxonomie wird vom XBRL e.V. betreut und weiterentwickelt. Per Erlass wird sie vom BMF als „amtlich vorgeschriebener Datensatz“ veröffentlicht.

[10] Darunter wäre z.B. die Vorgabe bestimmter Datenträger (z.B. SD-Karten) zu verstehen. Hier könnte z.B. auf dem Erlassweg bestimmt werden, welche Verfahren momentan zulässig sind.

Auch wenn bei der Entwicklung neuer Verfahren auf die vorhandenen Konzepte zurückgegriffen würde, wäre immer noch von mehreren Jahren Entwicklungszeit auszugehen. Projekte mit höchsten Sicherheitsanforderungen unter Einbindung des BSI benötigen erfahrungsgemäß eine besonders lange Entwicklungszeit.[11]

Eine parallele Zulassung des „Zertifizierungsverfahrens“[12] und des INSIKA-Verfahrens erscheint politisch sinnvoll. Die für das INSIKA-Verfahren genutzten Signaturerstellungseinheiten sind dabei selbstverständlich ebenfalls durch das BSI zu zertifizieren. Hierfür könnte dann allerdings eine separate technische Richtlinie erforderlich sein.

Aus technischer Sicht ist der Betrieb mehrerer paralleler Sicherheitssysteme nicht optimal. So wird zum einen die zentrale Erfassung der Sicherheitseinrichtungen komplizierter und zum anderen der Prüfungsaufwand höher (die Finanzverwaltung muss mehrere verschiedene Systeme beherrschen).

Bei der in vielen Aspekten ähnlichen Sicherheitstechnik für digitale Tachografen („Fahrtenschreiber“ für Lkw) hat man sich auf ein einheitliches Verfahren, das von allen Tachografen-Herstellern genutzt wird, festlegen können. Es werden einheitliche Fahrer-, Unternehmer-, Werkstatt- und Kontrollkarten genutzt. Diese werden vom Kraftfahrtbundesamt (KBA) ausgegeben und verwaltet.

Fazit: Um allen direkt Betroffenen (Anwendern und Lieferanten von Registrierkassen) schnell eine funktionierende, stabile technische Lösung bieten zu können, muss das INSIKA-Verfahren zugelassen werden. Andernfalls wären schon bei kleineren Verzögerungen in der Entwicklung der neuen Sicherungsverfahren die Zieltermine ernsthaft gefährdet.

3.10 Sinnvolle Fristen festlegen

Die Frist bis zur verpflichtenden Nutzung von Sicherheitseinrichtungen sollte so kurz wie möglich gewählt werden, um schnell einen fairen Wettbewerb und einen gleichmäßigen Steuervollzug zu erreichen. Jede Übergangsregelung schiebt diesen Zeitpunkt weiter in die Zukunft.

Die Frist muss jedoch ausreichend lang sein, damit die flächendeckende Einführung auch praktisch umsetzbar ist. Die benötige Zeit hängt stark von der Komplexität und vom Reifegrad der einzuführenden Verfahren ab. Vollständige Neuentwicklungen benötigen dabei grundsätzlich die längsten Fristen (siehe auch 3.9).

Fazit: Die Frist bis zur verpflichtenden Nutzung von Sicherheitseinrichtungen sollte so kurz wie möglich gewählt werden, um schnell einen fairen Wettbewerb und einen gleichmäßigen Steuervollzug zu erreichen. Sie muss jedoch ausreichend lang sein, damit die flächendeckende Einführung auch praktisch umsetzbar ist. Bei der Zulassung des INSIKA-Verfahrens ist der Zieltermin 1.1.2020 nach Ansicht des DFKA absolut realistisch. Der zusätzliche Bestandschutz wird in Übereinstimmung mit den Empfehlungen des Bundesrates für unnötig gehalten.

3.11 Einbindung aller Stakeholder erforderlich

Bei der ersten Initiative zur Lösung des Problems ab 2004 waren kontinuierlich Experten aus dem Steuervollzug, aus der Registrierkassenbranche und Sicherheitsfachleute eingebunden. Das daraus hervorgegangene INSIKA-Verfahren ist daher absolut praxistauglich.

Bei der Entstehung des aktuellen Gesetzentwurfs ist auf einen Erfahrungsaustausch mit den Betroffenen weitgehend verzichtet worden. In der Folge hat das zu den hier behandelten Problemen geführt. Sich daraus möglichweise ergebende Änderungen des Sicherungsverfah-

[11] Beispiele: Gesundheitskarte, Smartmeter-Gateway

[12] Der Begriff ist irreführend – ein „Zertifizierungsverfahren“ ist kein technisches Konzept, sondern ein Verfahren zur Erlangung einer Zertifizierung.

rens während der Entwicklung oder sogar im laufenden Betrieb würden einen erheblichen Aufwand bei Anbietern, Nutzern und der Verwaltung verursachen.

Die wesentlichen für die Praxistauglichkeit und Effektivität entscheidenden Festlegungen werden allerdings nicht im Gesetz, sondern in der Verordnung erfolgen.

Fazit: In den weiteren Prozess – insbesondere in die Erstellung der Verordnung – müssen unbedingt Fachleute für alle relevanten, vor allem für die praktischen Aspekte einbezogen werden.

4 Österreich als Präzedenzfall

Die Einführung der Registrierkassenpflicht und der Registrierkassensicherheitsverordnung (RKSV) in Österreich eignet sich gut als Präzedenzfall, da Österreich in Bezug auf Steuerrecht, Wirtschaftsstruktur und politische Rahmenbedingungen gut mit Deutschland vergleichbar ist.

4.1 Grundsätzliches

Im Rahmen einer großen Steuerreform (die unter anderem eine erhebliche Lohnsteuerentlastung beinhaltete) wurden in Österreich im Juli 2015 folgende Gesetzesänderungen beschlossen:

- Allgemeine Registrierkassenpflicht (mit Bagatellgrenzen) zum 1.1.2016. Durch Urteil des Verfassungsgerichtshofs bzgl. der Ermittlung der Umsatzgrenzen wurde der Termin auf den 1.5.2016 verschoben.
- Belegausgabepflicht zum 1.1.2016, analog zu Kassenpflicht verschoben auf den 1.5.2016.
- Einsatz einer kryptografischen Sicherheitslösung ab dem 1.1.2017, verschoben auf den 1.4.2017, um den Anwendern mehr Zeit für die Umstellung zu geben.

4.2 Einzelkomponenten der österreichischen Lösung

Die folgenden Punkte sind in Österreich umgesetzt worden:

- **Kassenpflicht**: Es wurde zum 1.1.2016 eine allgemeine Kassenpflicht mit Ausnahmen (vor allem für Kleinunternehmen) eingeführt. Trotz heftiger Debatten gab es nur kleinere Nachbesserungen bei den Ausnahmen.
- **Belegpflicht**: Es besteht eine Belegausgabeverpflichtung.
- **Sicherheitsmerkmal auf dem Beleg**: Der Beleg muss ein prüfbares Sicherheitsmerkmal haben – in den meisten Fällen ist das ein QR-Code. Das Sicherheitsmerkmal erlaubt die schnelle Kontrolle der korrekten Erfassung.
- **Konkret vorgegebenes Verfahren**: Die RKSV legt das technische Verfahren exakt fest. Durch die Verwendung von handelsüblichen Signaturerstellungseinheiten kann der Anwender zwar zwischen mehreren Anbietern wählen, aber das technische Sicherungsverfahren ist für alle identisch. Grundsätzliche Probleme der Kassenanbieter bei der Implementierung sind nicht bekannt.
- **Zentrale Erfassung der Sicherheitseinrichtungen**: Alle Sicherheitseinrichtungen müssen vor Benutzung registriert werden. Dies erfolgt über das Internet-Portal der Finanzverwaltung („FinanzOnline“).
- **Kurze Fristen**: Die Fristen sind sehr kurz gewählt: 6 Monate für die Kassenpflicht, weitere 12 Monate für die Sicherheitseinrichtung.

4.3 Verbesserungsmöglichkeiten

Auch wenn bisher noch keine abschließende Bewertung der Einführung der Manipulationssicherung für Registrierkassen möglich ist, haben sich aus Sicht der Anbieter bisher folgende Verbesserungspotenziale gezeigt:

- **Bessere technische Lösung**: Das in der RKSV spezifizierte Sicherungsverfahren erfüllt seinen Zweck, ist jedoch in vielen Details komplizierter sowie weniger robust und sicher als es möglich wäre. Das Verfahren orientiert sich stark an INSIKA, ist jedoch in diversen Punkten abgeändert – daraus resultieren einige Sicherheitslücken, eine aufwändige Inbetriebnahme und geringere Robustheit bei technischen Störungen oder Bedienfehlern.
- **Bessere Dokumentation und Entwicklungsunterstützung**: Die kurzfristige Neudefinition des Verfahrens führte dazu, dass nur eine rudimentäre Dokumentation und unfertige Prototypen vorlagen. Gleichzeitig gab es keinen klar definierten Weg für Registrierkassenanbieter, Support bei der Entwicklung zu erhalten.
- **Weitergehende Standardisierung der digitalen Aufzeichnungen**: Die bei einer Prüfung vorzulegenden Daten sind nur zum Teil standardisiert und bleiben ansonsten herstellerspezifisch – ohne dass dies für Hersteller oder Anwender einen Vorteil hätte. Stattdessen entsteht hier Unsicherheit für die Anwender und entsteht Mehraufwand für die Finanzverwaltung.
- **Fristen zu kurz für neuentwickeltes System**: Die genauen technischen Vorgaben waren erst im September 2015 bekannt und sind im Dezember 2015 rechtskräftig geworden. Die damit verbleibende Zeit von einem Jahr für Entwicklung und flächendeckende Installation ist zu kurz, was dann auch zur Verlängerung der Frist um drei Monate geführt hat.

5 Kurze Analyse der Effekte einer Aufzeichnung „anderer Vorgänge“

5.1 Ziel und Vorgehensweise

In der bisherigen Diskussion über die Verhinderung von Manipulationen an Kassensystemen steht die Aussage im Raum, dass eine Aufzeichnung „anderer Vorgänge“ bis hin zu jedem einzelnen Tastendruck und besonders abgesicherten Uhrzeitinformationen die Sicherheit erhöhen bzw. einen Ersatz für anderen Maßnahmen darstellen würde. Diese Aussage wurde bisher noch nicht systematisch untersucht. Dies soll hier nachgeholt werden.

Die Kernfragen werden als Thesen und die Rahmenbedingungen als Prämissen formuliert. Sodann werden typische Abläufe analysiert.

5.2 Zu überprüfende Thesen

Die beiden folgenden Thesen sollen im Rahmen der Analyse überprüft werden:

- „Die Aufzeichnung ‚anderer Vorgänge‘ kann Manipulationen aufdecken“
- „Die Aufzeichnung ‚anderer Vorgänge‘ ist ein Ersatz für eine Belegpflicht“

5.3 Prämissen

Die Analyse basiert auf den folgenden Annahmen:

- Anwender und Lieferanten werden als nicht vertrauenswürdig eingestuft (nur aus diesem Grund existiert schließlich der Gesetzentwurf).
- Lediglich die Sicherheitseinrichtung soll zertifiziert werden – alle anderen Systemkomponenten unterliegen keiner besonderen Prüfung (im Gesetzentwurf so verankert).
- Kontrollen (Überwachung des Einsatzes der Systeme als Kassen-Nachschau) und Prüfungen (Prüfungen der Vergangenheit, also Betriebsprüfung) werden nicht durch IT-Sachverständige, sondern durch Betriebsprüfer, Beamte der FKS oder Amtspersonen mit vergleichbarer Qualifikation durchgeführt.
- „Andere Vorgänge“ sind alle Daten, die nicht unmittelbar zur Dokumentation der Geschäftsvorfälle oder deren nachträglicher Korrekturen dienen, z.B.:
    - Uhrzeit des Beginns der Erfassung eines Geschäftsvorfalls

    - Alle oder bestimmte Tastendrücke
    - Änderungen an der Einrichtung des Systems (Stammdaten oder Parameter)
- Die Aufzeichnung der „anderen Vorgänge“ ist praktisch möglich und die Daten sind prüfbar (auch wenn daran erhebliche Zweifel bestehen, siehe 3.5).

5.4 Analyse

5.4.1 Fall „Unterdrückte Buchung bei ordnungsmäßiger Kassensoftware“

Ablauf:

- Erfassung eines Geschäftsvorfalls (also eines Verkaufs)
- Vorgang wird auf dem Display dargestellt
- Dem Kunden wird der Vorgang auf dem Display gezeigt und er bezahlt aufgrund dieser Information – das Geld wird „schwarz“ vereinnahmt
- Der Vorgang wird nicht abgeschlossen, sondern abgebrochen und damit gelöscht – ein Beleg wird nicht erstellt
- Der Abbruch des Vorgangs ist als „anderer Vorgang“ in der Datenaufzeichnung dokumentiert

Falls der Vorgang Gegenstand einer Kassen-Nachschau ist:

- Vorgang wird beobachtet
- Datenzugriff
- Vorgang wird nicht in den Daten gefunden – damit ist die Manipulation erkannt
- Die Aufzeichnung der „anderen Vorgänge“ wird dazu nicht benötigt

Falls der Vorgang Gegenstand einer Betriebsprüfung ist:

- Die Analyse der „anderen Vorgänge“ ergibt, dass Abbrüche von Verkaufsvorgängen stattgefunden haben
- Abbrüche von Verkaufsvorgängen sind weder ungewöhnlich noch automatisch der Nachweis einer Manipulation
- Es kann die Verteilung der Häufigkeit dieser Abbrüche ermittelt werden
- Wenn es hier Auffälligkeiten gibt, wird der Steuerpflichtige hierzu befragt
- Kann der Sachverhalt nicht zufriedenstellend erklärt werden, könnte daraus auf einen möglichen formellen Mangel geschlossen

5.4.2 Fall „Unterdrückte Buchung mit Manipulationsfunktionen in Kassensoftware“

Der Ablauf entspricht dem unter 5.4.1, jedoch verfügt die Kassensoftware über eine Funktion zur Unterdrückung der Aufzeichnung „anderer Vorgänge“, wenn diese in manipulativer Absicht benutzt werden.

Falls der Vorgang Gegenstand einer Kassen-Nachschau ist:

- Vorgang wird beobachtet
- Datenzugriff
- Der Abbruch des Vorgang wird nicht in der Aufzeichnung der „anderen Vorgänge“ gefunden – damit ist erkannt worden, dass die Software die „anderen Vorgänge“ nicht wie gefordert aufzeichnet
- Die Ursache für die Nichtaufzeichnung kann der Prüfer mangels IT-Fachwissen nicht ermitteln. Mögliche Ursachen: Bewusst integrierte Manipulationsfunktionen, Softwarefehler, Eingriff durch Dritte, Konfigurationsänderung durch Anwender.

Falls der Vorgang Gegenstand einer Betriebsprüfung ist:

- Die Analyse der „anderen Vorgänge“ ergibt keine Auffälligkeiten
- Die Manipulation wird nicht entdeckt

5.4.3 Betrachtung des Status quo

Die Manipulationen, die durch eine Aufzeichnung „anderer Vorgänge“ unter bestimmten Voraussetzungen erkannt werden könnten, ließen sich bereits heute erkennen, indem das Ergebnis einer Beobachtung mit den Daten aus einem Datenzugriff abgeglichen wird.

Dies ist jedoch praktisch noch nie vorgekommen. Die Aufzeichnung „anderer Vorgänge“ würde eine Manipulationserkennung nicht nennenswert vereinfachen, so dass eine Verbesserung gegenüber der heutigen Situation nicht zu erwarten ist.

5.5 Schlussfolgerungen

Aus der Analyse lassen sich die folgenden Erkenntnisse gewinnen:

- Die Aufzeichnung „anderer Vorgänge“ bis hin zu jeder einzelnen Eingabe kann eine Kassen-Nachschau nicht erleichtern.
- Bei „naiven“ Manipulationen können die Aufzeichnungen während einer Betriebsprüfung zu einem entsprechenden Verdacht führen.
- Sobald die Kassensoftware Funktionen zur Manipulationen der „anderer Aufzeichnungen“ selbst enthält, sind diese nur zufällig und mit hohem Aufwand erkennbar.
- Die Kassensoftware selbst müsste also vertrauenswürdig sein, damit die Aufzeichnung der „anderen Vorgänge“ bei Betriebsprüfungen hilft und damit einen wirklichen Nutzen hätte. Die Vertrauenswürdigkeit der Kassensoftware ließe sich jedoch nur über deren Zertifizierung herstellen, was allerdings vom Gesetzentwurf gerade nicht gewollte Bauartanforderungen an die Kasse(nsoftware) bedingen würde. In diesem Fall könnte man die entsprechenden Manipulationsmöglichkeiten aber bereits per Bauartanforderung und Zertifizierung ausschließen.

Damit sind beide unter 5.2 aufgestellte Thesen widerlegt und ein nennenswerter Nutzen der Aufzeichnung „anderer Vorgänge“ ist nicht erkennbar.