Stand 22. Februar 2019

Stellungnahme des DFKA e.V. zum Entwurf des Anwendungserlasses zu § 146a AO

Am 12. Februar 2019 hat das Bundesministerium der Finanzen einen Entwurf für den Anwendungserlass zu § 146a AO per E-Mail an die obersten Finanzbehörden der Länder, eine Reihe von Verbänden sowie an verschiedene Kassenhersteller übersandt und um Stellungnahme gebeten. Dieser Bitte kommt der DFKA e.V. hiermit gerne nach.

Der Entwurf des Anwendungserlasses enthält einen **neuen, sehr positiven Ansatz**. Jedoch sind zentrale, bereits in der Vergangenheit vom DFKA angesprochene **Probleme weiterhin nicht gelöst**. In der vorliegenden Form halten wir das Sicherungsverfahren daher für nicht sachgerecht sowie nicht pünktlich und kostenoptimiert umsetzbar.

Vor allem ist die aktuelle Konzeption der technischen Sicherheitseinrichtung (TSE) für die **Buchungsvolumina von typischen Kassensystemen nicht geeignet**. Prüfungen mit angemessenem Zeitaufwand würden in vielen Fällen unmöglich sein. Es bedarf eines auf die besonderen Anforderungen von Kassensystemen abgestimmten Verfahrens, während die TSE offenbar ein generisches System zur Sicherung verschiedenster Daten sein soll. Dieser Ansatz ist aus unserer Sicht **realitäts- und praxisfern**.

Ergänzend zur nachfolgenden knappen Darstellung werden die einzelnen Punkte in der Anlage ausführlicher erläutert. Die Nummerierung in eckigen Klammern verweist auf die korrespondieren Gliederungspunkte in der Anlage.

Im Entwurf des Anwendungserlasses wird erstmalig die „Digitale Schnittstelle der Finanzverwaltung für Kassensysteme" (DSFinV-K) erwähnt. Der im Gesetz eingeführte Begriff der einheitlichen digitalen Schnittstelle wird so konkretisiert, dass es tatsächlich drei einzelne Schnittstellen geben soll:

- Einbindungsschnittstelle, in der technischen Richtlinie TR-03153 definiert
- Exportschnittstelle, in der TR-03153 definiert
- Digitale Schnittstelle der Finanzverwaltung für Kassensysteme, neu eingeführt

Planungs- und Rechtssicherheit ist nur durch eine für alle Beteiligten verbindliche Standardisierung der aufzuzeichnenden Daten erreichbar. Aus diesem Grund existieren beispielsweise auch die Taxonomie für die E-Bilanz oder die Digitale Lohnschnittstelle. In diesen sind – wie bei der DSFinV-K – Format und Inhalt der Daten standardisiert. [**2.1**]

Bei dem bisher zur Prüfung der Kassenführung genutzten Beschreibungsstandard für die Datenträgerüberlassung wird hingegen lediglich das Format standardisiert, was zu einer Vielzahl von Problemen geführt hat, von Schwierigkeiten bei der Auswertung bis hin zur Behauptung der Nichtordnungsmäßigkeit ex post. [**2.2**]

Insofern ist die **DSFinV-K** grundsätzlich ein **sehr wichtiger Schritt in Richtung Planungs- und Rechtssicherheit** und wird daher von uns ausdrücklich begrüßt.

Positiv werten wir zudem die Nutzung der DFKA-Taxonomie Kassendaten als Grundlage der DSFinV-K, da diese von einer Projektgruppe unter Einbeziehung aller wesentlichen Stakeholder (Finanzverwaltung, Steuerberatung, Kassenanbieter) entwickelt und bereits erfolgreich in der Praxis erprobt wurde. [**2.3**]

Sämtliche Ziele der **Planungs- und Rechtssicherheit werden jedoch konterkariert** durch die Aussage: „*Der nachfolgende Datenkranz beschreibt den Mindestumfang für eine standardisierte Datenaufbereitung und einen Prüfungseinstieg. Keinesfalls ist damit eine abschließende Aufzählung der für Zwecke der Außenprüfung oder der Nachschau vorzuhaltenden Daten aus elektronischen Kassensystemen verbunden.*" Damit handelt es sich eben nicht mehr um eine einheitliche Schnittstelle, was unserer Ansicht nach einen **Verstoß gegen den gesetzlichen Auftrag** darstellt. [**2.4**]

Die Daten für die DSFinV-K und die in der TSE gespeicherten Daten sollen parallel aufgezeichnet und über Verweise miteinander verbunden werden. Die Verarbeitung der Daten über zwei Wege schafft unnötige Komplexität. [**2.5**]

Außerdem werden verschiedene, zudem nicht standardisierte (sondern herstellerspezifische) Mechanismen beschrieben, die eine Vollständigkeitsprüfung erlauben sollen. Die **Gewährleistung der Vollständigkeit ist jedoch alleinige Aufgabe der TSE**. Das ist nicht nur technisch sinnvoll, sondern bereits in der Gesetzesbegründung so angelegt. [**2.6**]

Petitum

a) Die DSFinV-K muss in der spezifizierten Form eine ausreichende Basis für Prüfungen sein. Erweiterungen der DSFinV-K dürfen nur verpflichtend sein, um Geschäftsvorfälle abzubilden, die ohne diese zusätzlichen Informationen nicht nachvollziehbar wären. [**3.1**]
b) Alle Sicherheitsaspekte (einschließlich der Mechanismen zur Prüfung der Vollständigkeit) müssen von der TSE abgedeckt werden. [**3.2**]

In Bezug auf die übrigen Punkte des Anwendungserlasses erscheint es uns nicht sinnvoll und zielführend, Verbesserungsvorschläge für einzelne Details des Entwurfs zu machen. Durch solche Korrekturen sind die grundsätzlichen konzeptionellen, vom DFKA bereits mehrfach und ausführlich analysierten, Probleme nicht lösbar. [**2.7**]

Daher wird im Folgenden nur schlaglichtartig auf die wesentlichen Probleme hingewiesen:

- Es fehlt weiterhin eine abschließende Aufzählung von Geschäftsvorfällen und anderen Vorgängen, die durch die TSE aufzuzeichnen sind. [**2.8**]
- Es wird der Ausdruck des Prüfwertes auf dem Beleg verlangt. Damit soll offenbar – wie vom DFKA immer gefordert – der Beleg ohne Datenzugriff prüfbar werden, um Kassen-Nachschauen einfacher durchführen zu können. In der vorgesehenen Form erscheint das jedoch nicht durchführbar. [**2.9**]
- Es gibt weniger als ein Jahr vor dem gesetzlichen Einführungstermin weiterhin keine ausreichend stabile Grundlage für die Entwicklung einer TSE. So muss es fast zwangsläufig zu mehrfachen, teuren Nachbesserungsschleifen kommen. Die wichtigsten Aspekte:
  - Das Erfordernis einer Zeitquelle innerhalb des Sicherheitsmoduls wird bekräftigt. Diese Anforderung ist nach wie vor nicht nachvollziehbar begründet. Sie schließt die einfachste und schnellste Lösung für das Sicherheitsmodul, nämlich die Verwendung einer am Markt sofort verfügbaren, zertifizierten Smartcard-Hardware, aus. [**2.10**]
  - Der Anwendungserlass verweist auf noch laufende Überarbeitungen der Technischen Richtlinien.
  - Die erforderlichen Schutzprofile sind weiterhin nicht veröffentlicht. [**2.11**]
- Das wesentliche konzeptionelle Problem ist allerdings das für die Übermittlung der in der TSE gespeicherten Daten gewählte Verfahren. Es führt zwangsläufig zu einer derart **langsamen Verarbeitung**, dass **Prüfungen** in vielen Fällen **praktisch unmöglich werden**. [**2.12**]

Petitum

c) Es muss eine grundlegende Überarbeitung der Gesamtkonzeption der TSE erfolgen. [**3.3**]

d) Zusätzlich muss das einzige rechtzeitig verfügbare System – die TIM Card der Bundesdruckerei (sofort lieferbar und mehr als 10.000-fach erfolgreich im Einsatz) – oder funktionsgleiche Implementierungen anderen Anbieter zumindest als Übergangslösung zugelassen werden. [**3.4**]

Fazit

Die DSFinV-K ist ein großer Schritt in die richtige Richtung. Damit die erwünschten Effekte erreicht werden, muss diese Schnittstelle jedoch einen nicht nur für Steuerpflichtige sondern auch für die Finanzverwaltung verbindlichen Charakter bekommen.

Die TSE bedarf nach wie vor einer grundlegenden konzeptionellen Überarbeitung, um in der Praxis funktionieren zu können.

Aufgrund der geringen verbleibenden Zeit ist die Einhaltung des gesetzlichen Einführungstermins nur mit Zulassung der erprobten und marktreifen TIM Card der Bundesdruckerei möglich.

Es ist für unsere Verbandsmitglieder, von denen viele an der Entwicklung und erfolgreichen Erprobung der TIM Card mitgewirkt haben, nicht nachvollziehbar, warum dieser Weg nach wie vor abgelehnt wird.

Anlage: Ausführliche Erläuterung der einzelnen Kritikpunkte und Forderungen

Stand 25. Februar 2019

Erläuterungen und Hintergrundinformationen zur

Stellungnahme des DFKA e.V. zum Entwurf des Anwendungserlasses zu § 146a AO

1 Grundsätzliches

Diese Anlage erläutert die Kritikpunkte und die sich daraus ergebenden Forderungen aus der Stellungnahme des DFKA zum Entwurf des Anwendungserlasses zu § 146a Abgabenordung (AEAO-E) im Detail.

Wie in der Stellungnahme bereits ausgeführt, verzichten wir auf eine Kommentierung jeder einzelnen Ziffer des AEAO-E, da sich durch Detailveränderungen die bereits in der Konzeption angelegten Probleme nach unserer Auffassung nicht lösen lassen. Die im Kern sinnvollen Korrekturversuche in AEAO-E und im Entwurf der DSFinV-K führen zu neuen Problemen – beispielhaft sei der Prüfwert auf dem Beleg (siehe 2.9) genannt.

Durch einen grundsätzlichen konzeptionellen Fehler ist die technische Sicherheitseinrichtung (TSE) nach unserer Auffassung für den Einsatz in Registrierkassen ungeeignet (siehe 2.12).

2 Erläuterung der Kritikpunkte zum AEAO-E

2.1 Standardisierung von Format und Inhalt

Vor der Digitalisierung des Rechnungswesens hat die Finanzverwaltung keine konkreten Vorgaben für Form und Inhalt von verpflichtenden Aufzeichnungen gemacht. Durch die Einführung elektronischer Systeme (Buchführungssoftware, elektronische Registrierkassen und andere Vorsysteme) war diese Vorgehensweise nicht mehr aufrecht zu halten, da eine Auswertung von Daten im Rahmen von Betriebsprüfungen nicht praktikabel war.

Dementsprechend wurde im Nachgang zu den zum 1. Januar 2002 in Kraft getretenen Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) Mitte 2002 der Beschreibungsstandard für die Datenträgerüberlassung bekannt gegeben. Dieser Standard erlaubt das direkte Einlesen von Daten in die Prüfsoftware IDEA. Eine Vorgabe für die Inhalte der Daten ist damit nicht verbunden.

Mit der Einführung von Verfahren, die für eine sinnvolle Funktionalität eine Standardisierung der Daten zwingend voraussetzen, hat die Finanzverwaltung entsprechende Vorgaben entwickelt, beispielsweise:

- Elster-Verfahren u.a. für elektronische Steuererklärungen
- Taxonomie für die E-Bilanz
- Digitale Lohnschnittstelle

Der Ansatz einer Standardisierung von Format und Inhalt von Daten ist in der Finanzverwaltung inzwischen also üblich geworden.

Laut § 4 der KassenSichV ist *„die einheitliche digitale Schnittstelle […] eine Datensatzbeschreibung für den standardisierten Datenexport aus dem Speichermedium […] und dem elektronischen Aufbewahrungssystem zur Übergabe an den mit der Kassen-Nachschau oder Außenprü-*

fung betrauten Amtsträger der Finanzbehörde." Dieselbe Formulierung findet im Zusammenhang mit der Digitalen Lohnschnittstelle[1] Verwendung – diese definiert verbindlich Format und Inhalte. Durch die Vorlage des Entwurfs der DSFinV-K bestätigt das BMF ausdrücklich, die Dateninhalte standardisieren zu wollen.

Sinnvoll gestaltete Vorgaben haben sich – anders als immer wieder befürchtet – auch nicht als Hindernis für den technischen Fortschritt erwiesen. So ist dem DFKA z.B. kein Fall bekannt, bei dem der Registrierkassensicherheitsverordnung (RKSV)[2] in Österreich zum Wegfall von Softwareleistungen geführt hätte (natürlich mit Ausnahme von Funktionen zur Manipulation von Aufzeichnungen).

Zusammenfassung: Die DSFinV-K standardisiert Form und Inhalt der Daten. Diese Standardisierungen sind oft sinnvoll und haben im Bereich der Finanzverwaltung bereits mehrfach erfolgreich stattgefunden.

2.2 Erfahrungen mit nicht-standardisierten Inhalten

Die Daten verschiedener Buchführungssysteme sind ähnlich aufgebaut, da diese Systeme im Kern immer die gleichen Strukturen und Abläufe abbilden. Vereinheitlichungen ergeben sich auch durch die Verwendung von Standardkontenrahmen. Fehlende inhaltliche Vorgaben haben sich für die Betriebsprüfung von daher nie als größeres Problem erwiesen.

Da es bei elektronischen Registrierkassen weitaus größere Unterschiede zwischen den verschiedenen Produkten gibt, ist die Situation nicht vergleichbar. Erfahrungsgemäß bereitet die Auswertung von Kassendaten bei Betriebsprüfungen daher häufig Probleme. Sie dauert unverhältnismäßig lange, führt vielfach zu Rückfragen und immer wieder zu Diskussionen über die Ordnungsmäßigkeit. Oft müssen spezialisierte Fachprüfer hinzugezogen werden. Die Anforderungen variieren nicht nur zwischen den Bundesländern, sondern unterscheiden sich von einer Prüfung zur anderen. Angehörigen der steuerberatenden Berufe entsteht aufgrund der Vielfalt der Lösungen bei ihren Mandaten ein sehr hoher Aufwand.

Der vermeintliche Vorteil für Hersteller und Anwender von Kassenlösungen, durch fehlende Vorgaben größere Freiheiten bei der Gestaltung und Nutzung der Systeme zu haben, verkehrt sich damit nicht selten ins Gegenteil.

Zusammenfassung: Im Bereich der Kassenprüfung ist die jetzt vorgesehene Standardisierung der Inhalte für alle Beteiligten äußerst wünschenswert.

2.3 Entwicklung und Test der Taxonomie

Die DFKA-Taxonomie für Kassendaten wurde auf Initiative mehrerer Mitglieder des DFKA entwickelt. An der Projektgruppe waren beteiligt:

- Anbieter von Buchführungssystemen
- Angehörige steuerberatender Berufe
- Mitarbeiter der Finanzverwaltung
- Anbieter von Registrierkassenlösungen für verschiedene Branchen

Bei der Entwicklung der Taxonomie gab es mehrere Zielsetzungen:

- Geräte- und herstellerübergreifende Standardisierung von Kassenabschlüssen und Einzelaufzeichnungen
- Einheitliche Schnittstelle zwischen Registrierkassen und Archivierungssystemen
- Einheitliche Schnittstelle zwischen Registrierkassen und Buchführung
- Integrationsmöglichkeit für verschiedene technische Sicherheitseinrichtungen

[1] <https://www.bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Steuern/Weitere_Steuerthemen/Abgabeordnung/Datenzugriff_GDPdU/2014-11-14-GoBD-Ergaenzende-Informationen-zur-Datentraegerueberlassung.html>

[2] <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009390&FassungVom=2017-04-01>

- Grundsätzliche Eignung als einheitliche digitale Schnittstelle gem. § 146a AO

Überblick über den zeitlichen Ablauf des Projekts:

Datum	Meilenstein
März 2016	Erstes Treffen der Projektgruppe
August 2017	Veröffentlichung einer Vorversion zum öffentlichen Review
Oktober 2017	Ende Review-Phase
April 2018	Beginn Feldversuch
August 2018	Veröffentlichung der Version 1.0 der Taxonomie für erste Implementierungen außerhalb des Feldversuchs
November 2018	Abschluss Feldversuch
Februar 2019	Veröffentlichung der Version 1.1 der Taxonomie
Februar 2019	Veröffentlichung Abschlussbericht zum Feldversuch

Der Feldversuch hat ergeben, dass die Taxonomie durch einen hohen Reifegrad bereits Praxistauglichkeit erreicht hat; Details sind im Abschlussbericht[3] dargestellt. Bei einem derart komplexen System ist es unausweichlich, dass nach Vorliegen weiterer Praxiserfahrungen noch einige Anpassungen und Erweiterungen erforderlich sind. Technisch und organisatorisch sind diese Änderungen gut beherrschbar.

Zusammenfassung: Die DFKA-Taxonomie Kassendaten als Grundlage der DSFinV-K ist von Praktikern entwickelt worden und wurde bereits erfolgreich in der Praxis erprobt.

2.4 Gesetzlicher Auftrag für einheitliche Schnittstelle

§ 146a Abs. 1 AO führt den Begriff der „einheitlichen digitalen Schnittstelle" neu ein. Daraus ist der eindeutige Wille des Gesetzgebers zu erkennen, hier eine Vereinheitlichung zu schaffen, die über das bisher Erreichte hinausgeht.

Sollte es – wie im aktuellen Entwurf der DSFinV-K unter Ziffer 1.3 beschrieben – in jedem Einzelfall möglich sein, nach freiem Ermessen Erweiterungen zur fordern und das auch noch im Nachhinein, wird damit der Ansatz der Einheitlichkeit untergraben. Diese Asymmetrie, also die Verbindlichkeit für Steuerpflichtige bei gleichzeitiger Unverbindlichkeit für die Finanzverwaltung, kann nicht die Zielsetzung des Gesetzgebers sein.

Die Situation für Steuerpflichtige würde sich damit gegenüber der heutigen Situation sogar noch verschlechtern.

Vermutlich ist dieser Ansatz der Finanzverwaltung darauf zurückzuführen, dass bis heute versucht wurde und wird, Manipulationen durch Unstimmigkeiten zwischen möglichst vielen gegeneinander verprobten Daten zu entdecken. Bei der Verwendung einer technischen Manipulationssicherung ist diese Herangehensweise jedoch überholt.

Zusammenfassung: Der Gesetzgeber spricht ausdrücklich von einer einheitlichen Schnittstelle. Dieses Ziel ist nur zu erreichen, wenn die Schnittstelle für Steuerpflichtige und Finanzverwaltung verbindlich ist.

2.5 Zwei parallele Aufzeichnungen

Aus der Beschreibung unter Ziffer 8 AEAO-E folgt, dass zwei Arten von Aufzeichnungen vorzulegen sind:

- Zum einen die Aufzeichnungen aus der TSE und
- zum anderen Daten gemäß DSFinV-K-Format.

[3] *Feldversuch DFKA-Taxonomie Kassendaten – Abschlussbericht*, November 2018, <https://dfka.net/wp-content/uploads/2019/02/Feldversuch_Taxonomie_Abschlussbericht_v1.0.0.pdf>

Diese zwei getrennten Datenbestände und Prüfpfade dürften vor allem in Sondersituationen eine Vielzahl von Problemen verursachen, beispielsweise beim Ausfall von Komponenten, Software- und Bedienfehlern oder bei einem Systemwechsel. Da ein Geschäftsvorfall auf verschiedenen Kassenplätzen bearbeitet und dokumentiert werden kann, gleichzeitig aber mit einer einzigen TSE abgesichert werden muss,[4] können die zu prüfenden Daten über mehrere Geräte verteilt sein. Zur Auswertung ist eine komplexe Prüfsoftware nötig, die Daten aus mehreren Quellen zusammenführt.

Ziffer 8.2 AEAO-E erlaubt die Übertragung von Daten aus der TSE in ein Archivsystem, in dem sie zusammen mit Aufzeichnungen für die DSFinV-K abgelegt werden können. Diese nachträgliche Zusammenführung erleichtert lediglich den Abruf der Daten, verringert die beschriebene Komplexität jedoch nicht.

Dass dieser Ansatz nicht grundsätzlich erforderlich ist, belegt die Kombination aus Taxonomie und TIM Card – dort gibt es nur einen Datenbestand. Die RKSV in Österreich verlangt zwar die Vorlage zwei verschiedener Exporte (das standardisierte sog. Datenerfassungsprotokoll und die herstellereigenen Einzelaufzeichnungen), diese lassen sich jedoch aus einem Datenbestand generieren, da keine separate Speicherung von Daten in der TSE erfolgt.

Zusammenfassung: Die TR-03153 in Verbindung mit dem AEAO-E fordert unnötigerweise, dass zwei getrennte, miteinander verknüpfte Datenbestände verwaltet werden müssen. Dies bedingt unnötige Komplexität und Zusatzaufwand.

2.6 Vorkehrungen für Vollständigkeit der Daten sind Aufgabe der TSE

Eine IT-Systemarchitektur nach dem Stand der Technik erfordert eine klare Zuordnung von Aufgaben und Funktionen zu den einzelnen Komponenten des Systems.

Die Sicherung gegen alle Varianten von Manipulationsversuchen muss daher Aufgabe der TSE sein. Genauso sieht es auch der Gesetzgeber, so dass in der Gesetzesbegründung ausgeführt wird: *„Die zertifizierte technische Sicherheitseinrichtung dient dem Schutz der Authentizität und Integrität sowie der Vollständigkeit der aufgezeichneten Daten.*"[5] Mit „Vollständigkeit" kann hier nur die vollständige Erfassung der Aufzeichnungen gemeint sein, da die Verhinderung eines nachträglichen Löschens (was ebenfalls zu unvollständigen Daten führt) bereits durch die Forderung nach Integrität abgedeckt ist.

Kein technisches System vermag allein die Vollständigkeit der Erfassung gewährleisten. Eine Nicht-Eingabe ist technisch nicht erkennbar. Das System kann allerdings die Überprüfung der vollständigen Erfassung stark erleichtern. Folgerichtig wird auch die Formulierung „dient der Vollständigkeit" vom Gesetzgeber gewählt. Der mit weitem Abstand einfachste und effektivste Mechanismus dafür ist der prüfbare Beleg (siehe auch 2.9).

Die im Entwurf der DSFinV-K unter Ziffer 2.2 genannten Mechanismen sind kein Ersatz für einen prüffähigen Beleg und entsprechend ausgestaltete Kassen-Nachschauen. Die dort formulierten Anforderungen schaffen keinen Nutzen und verstoßen zugleich gegen das Gebot, eine einheitliche Schnittstelle zu schaffen (siehe auch 2.4).

Zusammenfassung: Es muss alleinige Aufgabe der TSE sein, die Überprüfbarkeit der Vollständigkeit der Erfassung sicherzustellen. Weitere Mechanismen – vor allem in Form herstellerspezifischer Erweiterungen der DSFinV-K – sind nicht sachgerecht.

---

[4] Vgl. *Umsetzung der Kassensicherungsverordnung – eine* kritische *Analyse*, 14. September 2018, aktualisiert 17. Dezember 2018, <https://dfka.net/aktualisiert-umsetzung-der-kassensicherungsverordnung-eine-kritische-analyse/>, Ziffer 4.2

[5] *Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen* der Bundesregierung vom 5. September 2016, Drucksache 18/9535 <http://dip21.bundestag.de/dip21/btd/18/095/1809535.pdf #page=19>

2.7 Konzeptionelle Probleme und bisherige Analysen des DFKA

Der DFKA hat seit Inkrafttreten des Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen Ende 2016 wiederholt auf die drohenden Probleme bei der Umsetzung hingewiesen – beispielhaft:

- Februar 2017 (noch vor dem ersten Entwurf der KassenSichV):[6]
    - Terminplan für Neuentwicklung sehr eng und kaum haltbar, daher Empfehlung des Einsatzes einer fertigen Lösung
    - Unzureichende Formulierung der Ziele und zu wenig Praxisorientierung können den Erfolg gefährden
- Oktober 2017:[7]
    - Zeitplan des BMF inzwischen praktisch nicht mehr haltbar
    - Fachliche Anforderungen sind Voraussetzung für Produktentwicklungen, fehlen jedoch weitgehend
- September 2018:[8]
    - Es wird lediglich an Teilaspekten gearbeitet und das mit unnötig aufwändigen Konzepten
    - Nicht angemessenes Projektmanagement
    - Unnötige hohe Kosten erwartet
    - Fachliche Anforderungen und Praxisbezug fehlen weiterhin

Neben der Veröffentlichung der Dokumente hat sich der DFKA mehrfach an verschiedene Ansprechpartner im BMF gewandt.

Ähnliche Stimmen gab es im Übrigen auch aus Kreisen der Finanzverwaltung z.B. von Herrn Leitenden Regierungsdirektor Arno Becker, seinerzeit OFD NRW.[9]

Zusammenfassung: Der DFKA hat bereits früh und wiederholt auf die drohenden Probleme hingewiesen. Die Einschätzung der zentralen Fragen hat sich dabei über zwei Jahre nicht verändert.

2.8 Aufzuzeichnende Geschäftsvorfälle und sonstige Vorgänge

Die Beschreibungen unter den Ziffern 1.4 bis 1.7 des AEAO-E enthalten einige Angaben zu Vorgängen, Transaktionen, Geschäftsvorfällen und anderen Vorgängen. Es existiert jedoch weiterhin keine abschließende Aufzählung der aufzuzeichnenden Informationen. Eine Lösung des Problems wird nicht in Aussicht gestellt.

Damit fehlt es immer noch an technischer und Rechtssicherheit für Anbieter und Nutzer von Registrierkassen. Die Auseinandersetzungen darüber, ob die Aufzeichnungen ordnungsmäßig sind, dürften sich damit fortsetzen.

Die aktuelle Situation verdeutlicht eindringlich, dass der gewählte Ansatz, die technische Entwicklung von den fachlichen Anforderungen (aus denen sich die aufzuzeichnenden Inhalte ergeben) abzukoppeln, nicht zu den gewünschten Ergebnissen führt.

Zusammenfassung: Die wesentlichen Regelungslücken der KassenSichV sind immer noch nicht geschlossen.

---

[6] *Bewertung des „Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen" und Anforderungen an die „Kassensicherheitsverordnung"*, 16. Februar 2017, <https://dfka.net/bewertung-des-gesetzes-zum-schutz-vor-manipulationen-an-digitalen-grundaufzeichnungen/>

[7] *Umsetzung der* Kassensicherungsverordnung*: Die Zeit wird knapp!*, 19. Oktober 2017, <https://dfka.net/umsetzung-der-kassensicherungsverordnung-die-zeit-wird-knapp/>

[8] Siehe Fußnote 4

[9] *Der Gesetzentwurf des BMF zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen – Konzeptioneller Fehlgriff oder politischer Affront?*, Der Betrieb, 19/2016, 1090 ff. und 20/2016, 1158 ff.; Der Gesetzentwurf zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen – Ernsthafte interdisziplinäre Auseinandersetzung auch mit der Technik tut dringend Not, BBK, 21/2016, 1039 ff.; Die Kassensicherungsverordnung (KassenSichV) – Eine vertane Chance, BBK, 17/2017, 803 ff.

2.9 Prüfbare Belege

Der DFKA hat schon immer befürwortet, dass eine Sicherheitslösung für Registrierkassen prüffähige Belege bereitstellt. Dies erlaubt, die korrekte Nutzung eines Systems bereits anhand einer reinen Belegkontrolle zu überprüfen. Ein Datenzugriff ist dafür nicht erforderlich, so dass dieser nur für vertiefende Prüfungen (z.B. in Verdachtsfällen) nötig ist. Das führt zu einer erheblichen Vereinfachung und Beschleunigung von Kassen-Nachschauen.

Dieser Weg wurde beispielsweise in der RKSV gewählt und hat sich nach Auskunft von Experten der österreichischen Finanzverwaltung in der Praxis bestens bewährt.

Der AEAO-E sieht offenbar prüffähige Belege vor. Entsprechend ist unter Ziffer 5.4, Nr. 9 abweichend von § 6 KassenSichV auch der Prüfwert aufgeführt.

Es ist jedoch mehr als fraglich, ob der gewünschte Zweck auf diesem Weg erreichbar ist:

- Die TR-03153 verlangt den Einsatz von Signaturen als Prüfwert.
- Zur Prüfung von Signaturen wird der sog. öffentliche Schlüssel erforderlich.
- Dazu wird auf dem Beleg eine Information benötigt, anhand der man den öffentlichen Schlüssel ermitteln kann.
- Der öffentliche Schlüssel kann nicht aus dem „Kassenregister" der Finanzverwaltung ermittelt werden, da er nicht Teil der meldepflichtigen Daten ist.
- Stand der Technik ist die Speicherung öffentlicher Schlüssel in Zertifikaten, die dann auf einem Server bereitgestellt werden – dieser Server ist Bestandteil einer PKI[10].
- Bei einem Datenzugriff sind die Zertifikate in den Daten selbst enthalten – dieser Weg steht bei einer reinen Belegkontrolle nicht zur Verfügung.
- Hersteller einer TSE müssen lt. TR-03153, Ziffer 7.4 kein System zur Bereitstellung öffentlicher Schlüssel (also eine PKI) bereithalten: *„Betreibt ein Hersteller einer Technischen Sicherheitseinrichtung eine Public Key Infrastruktur (PKI) zur Sicherstellung der Authentizität der Prüfwerte, so ist der sichere Betrieb der PKI Bestandteil der CC-Zertifizierung des Sicherheitsmoduls*". Die PKI ist also optional.
- Eine Belegprüfung wäre also nur unter folgenden Voraussetzungen möglich:
    - Der TSE-Hersteller betreibt eine PKI,
    - auf dem Beleg ist die Seriennummer des Zertifikats (statt die der Kasse) enthalten und
    - es existiert eine Prüfsoftware, welche die entsprechenden Abläufe beherrscht (inkl. Verbindung zu mehreren PKIs für mehrere Hersteller).
- Daraus lässt sich ableiten, dass mit dem Prüfwert auf dem Beleg allein keine Prüffähigkeit hergestellt werden kann.

Zusammenfassung: Der Abdruck des in der KassenSichV eingeführten Prüfwertes führt noch nicht zu einem leicht prüfbaren Beleg und damit zur Möglichkeit einfacher und schneller Kassen-Nachschauen. Es sind weitere grundsätzliche Änderungen nötig.

2.10 Zeitquelle im Sicherheitsmodul

Unter Ziffer 3.2.6 des AEAO-E wird bekräftigt, dass das Sicherheitsmodul über eine Zeitquelle verfügen muss: *„Für die Zeitquelle ist lediglich entscheidend, dass die Zeitführung im Sicherheitsmodul erfolgen muss und damit die Transaktionszeit streng monoton wachsend ist.*"[11]

[10] PKI = „Public Key Infrastructure". Dieser Weg wurde beispielsweise beim System gemäß RKSV gegangen – hier werden die Zertifikate von der Ausgabestelle der dort verwendeten Signaturerstellungseinheiten im Rahmen einer PKI vorgehalten. Die Verknüpfung zum jeweiligen Steuerpflichtigen wird über eine Registrierung im FinanzOnline-Portal hergestellt. Ein weniger komplexer Ansatz ist die direkte Verknüpfung zwischen Schlüsseln und Steuerpflichtigen im Zertifikat.

[11] Randbemerkung: Es ist unklar, warum der zweite Teil der Aussage aus der ersten folgt, da die TR-03153 das Setzen der Uhrzeit von außen erlaubt und somit die Zeit zurückgestellt werden kann (was auch sinnvoll ist).

Momentan sind Smartcards (bzw. der dort verwendete Chip, eingebaut in einem anderen Gehäuse) der einfachste und preiswerteste Weg, ein zertifiziertes Sicherheitsmodul zu implementieren. Durch die Forderung nach einer Zeitquelle ist die Verwendung der aktuell auf dem Markt befindlichen Smartcard-Generation ausgeschlossen. Frühestens mit Smartcards nach Java Card Standard 3.1 ist eine Lösung möglich. Die Spezifikation wurde im Januar 2019 veröffentlicht,[12] ein Termin für die Verfügbarkeit zertifizierter Hardware ist nicht bekannt.

Alternativen zu Smartcards müssten auch erst neu entwickelt und zertifiziert werden. Der Zeitaufwand dafür liegt typischerweise bei Jahren.

Dieses Problem wurde offenbar auch vom BSI erkannt, so dass in der Ausschreibung für das Projekt „Zersika"[13] eine „CSP light"-Zertifizierung mit deutlich reduzierten Sicherheitsanforderungen erwähnt wird, d.h. mit einer Prüftiefe EAL 2 statt EAL 4+. Eine offizielle Erklärung dafür deutet sich lediglich in der Antwort auf eine Bieterfrage an: *„Die Möglichkeit der Verwendung eines CSP light […] ist für eine angemessene Übergangszeit nach Inkrafttreten des ‚Gesetzes zum Schutz vor Manipulation an digitalen Grundaufzeichnungen' vorgesehen."* Das verwundert umso mehr, als gerade die hohen Sicherheitsanforderungen ein zentrales Argument des BMF für den eingeschlagenen Weg einer vollständigen Neukonzeption der TSE waren.

Der konkrete Nutzen der Zeitquelle im Sicherheitsmodul – also welches Angriffsszenario damit wie verhindert werden soll und wie relevant dieses in der Praxis ist – wurde bisher nicht beschrieben.

Auch der ADM e.V., dessen Experten sich seit über 10 Jahren mit der Manipulationssicherung von Registrierkassen und Taxametern beschäftigen, hat sich detailliert mit dieser Frage befasst und kommt zu dem Schluss, dass der Nutzen einer vom Sicherheitsmodul verwalteten Zeitinformation gering ist.[14]

Zusammenfassung: Die bis heute nicht nachvollziehbar begründete Anforderung einer Zeitquelle im Sicherheitsmodul erhöht den technischen Aufwand und erfordert den Einsatz noch nicht lieferbarer Komponenten.

2.11 Noch nicht veröffentlichte Schutzprofile

Bei den Schutzprofilen (auch PP, „Protection Profile") handelt es sich um allgemein und abstrakt formulierte Sicherheitsanforderungen an eine bestimmte Kategorie informationstechnischer Produkte. Sie werden für eine Sicherheitszertifizierung von IT-Produkten nach ISO/IEC 15408 „Common Criteria" (CC) benötigt.

Die Schutzprofile sind bisher nur als Entwurf vorhanden.[15] Diese Entwürfe wurden nur als Teil der „Zersika"-Ausschreibungsunterlagen veröffentlicht.

Es handelt sich um folgende Dokumente:

- *Common Criteria Protection Profile PP-CSP – Protection Profile Cryptographic Service Provider*: Sicherheitsanforderungen an den Cryptographic Service Provider (CSP), eine Komponente, die laut Beschreibung aus Hardware, Firmware und Software bestehen soll und die grundlegenden, sicherheitskritischen Operationen ausführt. Hierbei kann es sich beispielsweise um eine Smartcard inklusive des Betriebssystems handeln.
- *Common Criteria Protection Profile PP-SMAERS – Security Module Application for Electronic Record-keeping Systems*: Sicherheitsanforderungen an eine Softwareerweiterung des CSP, um die speziellen Anforderungen – im Wesentlichen die Abbildung von

[12] <https://docs.oracle.com/en/java/javacard/3.1/specnotes/index.html>, Ziffer 1.1.14
[13] Im August 2018 vom BSI ausgeschriebenes Projekt zur „praktische[n] Erprobung des neuartigen Konzeptes für die Zertifizierung eines Sicherheitsmoduls für Registrierkassen und weitere Aufzeichnungssysteme sowie die Mitwirkung bei der Optimierung des Konzeptes"
[14] *Whitepaper: Zeitinformationen beim* Manipulationsschutz *für Registrierkassen*, 31. Mai 2018, <http://www.insika.de/images/stories/INSIKA/Whitepaper_Zeitinformation.pdf>
[15] Stand: 19. Februar 2019

Transaktionen – an das Sicherheitsmodul zu erfüllen. Typischerweise wird das ein sog. Applet für eine Smartcard sein.

Die Schutzprofile bestimmen die Kriterien, nach denen zertifiziert wird – und damit auch die Anforderungen, die vor der Entwicklung der entsprechenden Komponente bekannt sein müssen.

Zusammenfassung: Durch noch nicht veröffentlichte Schutzprofile gibt es noch keine ausreichende Grundlage für die Entwicklung des Sicherheitsmoduls als Teil einer TSE.

2.12 Geschwindigkeitsprobleme

Das aus unserer Sicht wesentliche Problem bei der Konzeption der TSE ist jedoch die Verarbeitungsgeschwindigkeit. Eine Betrachtung für eine typische, leicht überdurchschnittlich frequentierte Bäckereifiliale illustriert das Problem:

- Es gibt etwa 300 Verkaufstransaktionen pro Tag.
- Die Filiale ist mit Ausnahme weniger Feiertage praktisch jeden Tag geöffnet.
- Daraus ergeben sich etwa 100.000 Verkaufstransaktionen pro Jahr.[16]
- Es werden mehrere sog. Log-Messages (definiert in der TR-03153) pro Verkauf erzeugt, außerdem sind „andere Vorgänge" aufzuzeichnen – daher werden fünf Log-Messages pro Verkaufstransaktion und damit 500.000 pro Jahr angenommen.
- Im Feldversuch zur Erprobung der Taxonomie lag der Spitzenwert bei 50.000 Verkaufstransaktionen in einer Verkaufsstelle, also beim 5-fachen des hier betrachteten Beispiels.
- Die momentan vorgeschriebene Einzelaufzeichnung mit Aufbereitung der Daten gemäß Beschreibungsstandard für die Datenträgerüberlassung stellt die Referenz dar, da hier bereits die Grenzen der heutigen Systeme erreicht werden.

Um die grundsätzlichen Zusammenhänge zu untersuchen, wurden Messungen mit folgenden Daten durchgeführt:

- 1.000 Verzeichnisse mit jeweils 1.000 Dateien (alle 500 Byte oder kleiner) zur Simulation von 1 Mio. Log-Messages
- Gesamte Datenmenge ca. 280 MByte
- Größe der resultierenden tar-Datei: 1 GByte

Die Messergebnisse sind der folgenden Tabelle zusammengestellt (Zeiten in Stunden, Minuten und Sekunden):

System	Vorgang	Zeit
Workstation, SSD, Windows 7, 7-zip	tar erzeugen	1:00:00
Notebook, SSD, Windows 10, mitgeliefertes tar.exe	tar erzeugen	1:45:00
ARM Dual-Core Cortex-A9, 1 GHz, 512 kB L2 Cache, eMMC-Speicher, Linux, GNU tar 1.28	tar erzeugen	0:12:00
ARM Dual-Core Cortex-A9, 1 GHz, 512 kB L2 Cache, SD-Karte, Linux, GNU tar 1.28	tar erzeugen	0:28:00
Server, schnelles SSD-Storage-System, Linux, GNU tar 1.29	tar erzeugen	0:01:30
Notebook, SSD, Windows 10, mitgeliefertes tar.exe	tar entpacken	0:10:30
Workstation, SSD, Linux, GNU tar 1.29	tar entpacken	0:01:30

[16] Plausibilitätsprüfung: Lt. Zentralverband des Deutschen Bäckerhandwerks e. V. <https://www.baeckerhandwerk.de/baeckerhandwerk/zahlen-fakten/> setzt das Bäckereihandwerk mit 46.000 Verkaufsstellen 14,5 Mrd. Euro um, also 315.000 Euro pro Verkaufsstelle und Jahr, bei einem Durchschnittsbon von ca. 3,50 Euro <https://www.baeko-magazin.de/aktuell/baeko-aktuell/31-10-2016-snacks-richtig-kalkuliert/> ergeben sich im Schnitt 90.000 Verkäufe

System	Vorgang	Zeit
Workstation, SSD, Linux, GNU tar 1.29	Alle Log-Message-Dateien einlesen	0:12:00
Notebook, SSD, Windows 7, IDEA Version 8	Einlesen CSV mit 200.000 Belegdaten	0:00:30

Schlussfolgerungen:

- Das Erzeugen und Entpacken einer sehr großen Anzahl einzelner Dateien in tar-Archiven ist ein erheblicher Zeitfaktor.
- Die Verarbeitungszeiten sind sehr stark abhängig von der Hardware und der Qualität der Implementierung der Software.
- Selbst auf vergleichsweise leistungsstarken Systemen wie der hier verwendeten Hardware mit ARM-Prozessor benötigt das Erzeugen von Daten für einen typischen Prüfungszeitraum (vier Jahre, was dem Doppelten der hier vorliegenden Datenmenge entspricht) eine halbe bis eine Stunde.
- Bei der in einer preiswerten TSE genutzten Hardware wird die Verarbeitungszeit ein Vielfaches betragen.
- Das Entpacken und Einlesen der Log-Messages wird selbst auf einem sehr leistungsfähigen System ein Vielfaches der Zeit betragen, die heute für das Einlesen der zu prüfenden Daten in die IDEA-Software benötigt wird.

Bewertung:

- Aus der Beschreibung der Schnittstelle zur TSE ergibt sich, dass die zu exportierende tar-Datei im Moment des Exports erzeugt werden muss (da bei der Anfrage der zu exportierende Bereich spezifiziert wird).[17] Eine laufende Erzeugung z.B. durch stündliche oder tägliche Aktualisierungen der Exportdatei scheidet damit aus.
- Die Aufbereitung der Daten eines typischen Prüfungszeitraums für den Export wird innerhalb einer TSE mit leistungsschwacher Hardware Stunden erfordern.
- Der Zeitaufwand für die Datenauswertung wird sich um ein Vielfaches erhöhen (Größenordnung im betrachteten Beispiel: Minuten auf Stunden).
- Die Zeiten für das Auswerten der Log-Messages und das Prüfen der Signaturen sind noch nicht berücksichtigt.
- Damit erscheint es völlig ausgeschlossen, Daten einer TSE auch nur annähernd vollständig zu prüfen. Maximal die Prüfung einzelner kleiner Stichproben ist vorstellbar.
- Eine reine Stichprobenprüfung führt das gesamte Konzept ad absurdum.

Prototypen oder auch nur Modellrechnungen, die eine Machbarkeit der TSE gemäß TR-03153 belegen, sind uns nicht bekannt.

Die grundsätzliche Alternative ist die Ergänzung der bereits heute durchgeführten Einzelaufzeichnungen um entsprechende Sicherungsdaten und Auswertung und Prüfung aller Daten in einem Vorgang. Dieser Ansatz wird bei der TIM Card und dem Verfahren gemäß RKSV erfolgreich angewendet.

Zusammenfassung: Das aktuelle Konzept der TSE bedingt eine derart langsame Verarbeitung der Daten, dass ein **praktischer Einsatz unmöglich** ist.

[17] *BSI TR-03151 Secure Element API (SE API)*, <https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03151/index_htm.html>

3 Erläuterung der Forderungen des DFKA

3.1 DSFinV-K muss für auch für Finanzverwaltung verbindlich sein

Petitum: Die DSFinV-K muss in der spezifizierten Form eine ausreichende Basis für Prüfungen sein. Erweiterungen der DSFinV-K dürfen nur verpflichtend sein, um Geschäftsvorfälle abzubilden, die ohne diese zusätzlichen Informationen nicht nachvollziehbar wären.

Nur so kann der gesetzliche Auftrag einer einheitlichen Schnittstelle erfüllt werden. In anderen Bereichen legt die Finanzverwaltung bereits seit Jahren verbindlich die Inhalte von Datenbeständen fest. Es handelt sich also nicht um eine neue Vorgehensweise.

Eine Ausnahme stellen selbstverständlich Geschäftsvorfälle dar, die sich in der DSFinV-K nicht nachvollziehbar abbilden lassen, die aber für die Ermittlung der Besteuerungsgrundlagen relevant sind. Für diese sollte dann allerdings schnellstmöglich eine standardisierte Erweiterung der DSFinV-K vorgenommen werden.

3.2 Keine zusätzlichen Sicherheitsmechanismen in der DSFinV-K

Petitum: Alle Sicherheitsaspekte (inkl. der Mechanismen zur Prüfung der Vollständigkeit) müssen von der TSE abgedeckt werden.

Die Bereitstellung von Funktionen zur Sicherstellung der vollständigen Erfassung der Aufzeichnungen ist laut gesetzlichem Auftrag eine Aufgabe der TSE. Auch aus technischer Sicht ist das der einzig sinnvolle Ansatz. Herstellerspezifische Erweiterungen der DSFinV-K können die Aufgabe prinzipiell nicht erfüllen und wären mangels Standardisierung auch nur mit großem Aufwand prüfbar.

Derartige Erweiterungen der DSFinV-K hätten keinen Nutzen, würden demgegenüber aber Aufwand verursachen und die Rechtssicherheit für die Anwender verschlechtern.

3.3 Konzept der TSE muss grundsätzlich überarbeitet werden

Petitum: Es muss eine grundlegende Überarbeitung der Gesamtkonzeption der TSE erfolgen.

Bereits in der Grundkonzeption der KassenSichV und der TR-03153 sind diverse Probleme angelegt. Durch die bisherigen Überarbeitungen und die Korrekturversuche durch den AEAO-E und den Entwurf der DSFinV-K sind einige Probleme gelöst, jedoch gleichzeitig auch neue geschaffen worden.

Angesichts der Vielzahl der zu lösenden Aufgaben, der komplexen Projektstruktur und des Zeitdrucks ist es aus Sicht des DFKA sehr unwahrscheinlich, dass sich Detailkorrekturen ein zufriedenstellender Zustand erreichen lässt. Allein das beschriebene Geschwindigkeitsproblem erfordert erhebliche konzeptionelle Änderungen.

Nur eine Neukonzeption kann zu einem gut funktionierenden System führen.

3.4 TIM Card muss zugelassen werden

Petitum: Das einzige unmittelbar verfügbare System – die TIM Card der Bundesdruckerei oder funktionsgleiche Implementierungen anderen Anbieter – muss zumindest als Übergangslösung zugelassen werden.

Mit der TIM Card der D-Trust (Tochterunternehmen der Bundesdruckerei) ist ein sofort einsetzbarer technischer Manipulationsschutz vorhanden. Er basiert auf dem technologieoffenen – also mit unterschiedlichen technischen Ansätzen umsetzbaren – INSIKA-Verfahren, das mit Förderung des BMWi von der Physikalisch-Technischen Bundesanstalt in den Jahren 2008 bis 2012 entwickelt wurde. Das Verfahren kombiniert bewährte Standardtechnologien. Da es vollständig dokumentiert und lizenzfrei ist, können jederzeit Implementierungen durch weitere Anbieter vorgenommen werden. Es kann nicht nur mit Smartcards implementiert werden, auch andere Hardware-Sicherheitsmodule sind nutzbar.

Die TIM Cards wurden mit großem Erfolg zuerst im Hamburger Taxigewerbe eingesetzt und sind zwischenzeitlich in über 10.000 Fahrzeugen deutschlandweit im Einsatz.

Nachgewiesene Sicherheitslücken sind nicht bekannt. Die TIM Card basiert auf einer nach EAL 4+ zertifizierten Hardware. Eine Zertifizierung der darauf laufenden Zusatzsoftware ist jederzeit möglich. Dieses sog. Applet wurde bisher nicht zertifiziert, da dies für die Taxameter-Anwendungen nicht gefordert wurde. Eine routinemäßige Umstellung der TIM Card auf stärkere Kryptografieverfahren (von ECDSA-192 auf ECDSA-256) wird die D-Trust voraussichtlich Mitte 2019 vornehmen.

Eine Verringerung des Sicherheitsniveaus aus Termingründen, wie sie bei der TSE gemäß TR-03153 offenbar erfolgen soll (siehe 2.10), wäre nicht nötig.

Da die Verwaltung der ausgegebenen TIM Cards über eine standardisierte PKI erfolgt, lässt sich dadurch die gesetzliche Meldepflicht weitgehend automatisch abbilden. Auch die parallele Nutzung mehrerer PKIs bei mehreren Anbietern von Sicherheitseinrichtungen auf INSIKA-Basis ist möglich.

Auch wenn der Nutzen recht gering ist, ließe sich selbst die von der KassenSichV geforderte Zeitquelle integrieren, sobald eine sich derzeit in Entwicklung befindliche, neue Generation von Smartcards (bzw. vergleichbare Sicherheitsmodule) verfügbar ist.[18]

Etwa 30 Unternehmen haben gegenüber dem DFKA eine Absichtserklärung abgegeben, das Sicherungsverfahren zu implementieren, wenn es zugelassen wird.

Um die Praxistauglichkeit der Taxonomie und der TIM Card in Kombination zu bewerten, hat der DFKA von Februar bis November 2018 einen Feldversuch durchgeführt. Der Abschlussbericht ist veröffentlicht. Der Test war erfolgreich, wesentliche Probleme sind nicht aufgetreten.

Folgende Ziele wurden im Feldversuch erreicht:

- Alle Hersteller konnten die Sicherheitseinrichtung integrieren. Sechs der sieben Hersteller haben Systeme bei Kunden im Echtbetrieb eingesetzt, ein Hersteller hat sich aus Kapazitätsgründen auf Labortests beschränkt.
- Die Daten wurden kryptografisch gesichert.
- Die Herkunft der Daten konnte zweifelsfrei identifiziert werden (Ergebnis: Sicherstellung der Authentizität).
- Veränderungen und Löschungen waren eindeutig erkennbar (Ergebnis: Sicherstellung der Integrität).
- Die korrekte Nutzung der Registrierkassen (inklusive Verhinderung einer Nichteingabe) ist – wie bei jedem System – nicht allein technisch sicherzustellen, sondern erfordert die bereits gesetzlich verankerte Kassen-Nachschau. Diese ist mit der TIM Card über eine reine Belegprüfung möglich und damit ebenso schnell wie einfach durchführbar (Ergebnis: Sicherstellung der Vollständigkeit).
- Mittels Taxonomie konnten den am Versuch beteiligten Finanzbehörden prüfbare Daten in einem einheitlichen Format zur Verfügung gestellt werden.

Damit ist die Praxistauglichkeit der Taxonomie bestätigt und die Einsetzbarkeit der TIM Card nach mehrjährigem, erfolgreichen Einsatz im Taxigewerbe auch für Registrierkassen zweifelsfrei nachgewiesen.

Alternative Lösungen, die einerseits schnell verfügbar sind und sich andererseits im Rahmen der Vorgaben des § 146a AO bewegen, sind uns nicht bekannt.

[18] Siehe Fußnote 14

In der Gesetzesbegründung[19] wurde ausgeführt, warum das INSIKA-Verfahren nicht zugelassen werden sollte. Die damaligen Gründe stellen sich aus heutiger Sicht wie folgt dar (Hinweis: Mit „Zertifizierungsverfahren" ist das aktuelle TSE-Konzept gemeint):

- *„Die INSIKA-Infrastruktur ist hinsichtlich der Smartcardvergabe und der Verwaltung der Smartcards aufwändig. Weiterhin birgt sie nicht unerhebliche rechtliche und technische Risiken und verursacht Kosten hinsichtlich der Einbindung der autorisierten Stelle, der technischen Umsetzung der Schnittstelle zwischen der autorisierten Stelle und dem Bundeszentralamt für Steuern, die höher sind als beim Zertifizierungsverfahren.*": Der AEAO-E sieht einen kontrollfähigen Beleg vor. Dazu muss eine PKI (hier „INSIKA-Infrastruktur") betrieben werden. Insofern besteht kein Unterschied. Eine Schnittstelle zum Bundeszentralamt für Steuern ist in beiden Fällen nicht unbedingt erforderlich, wie es der erfolgreiche Einsatz der TIM Card im Taxiumfeld beweist.
- *„Aufgrund der verpflichtenden Belegausgabe müssten hierfür teilweise neue Drucker angeschafft werden, die den Ausdruck eines 2D-QR-Codes ermöglichen.*": Ein QR-Code ist lediglich eine – allerdings sehr sinnvolle – Prüferleichterung in beiden Verfahren (also auch beim Ausdruck des Prüfwertes gemäß AEAO-E) und damit kein Zwang.
- *„Für jedes elektronische Aufzeichnungsgerät müssten ein Kartenleser und eine Smartcard angeschafft werden.*": Bei beiden Verfahren ist eine Sicherheitseinrichtung anzuschaffen. Beim INSIKA-Verfahren kann diese aus Smartcard-Leser und Smartcard bestehen. Andere Implementierungen sind möglich. Ein Smartcard-Leser und eine Smartcard werden voraussichtlich deutlich günstiger sein als die zu erwartenden Kosten für eine TSE gemäß TR-03153.
- *„Hinsichtlich der Belegkontrollen durch Kunden durch Abgleich der Daten auf dem Beleg mit dem Verifikationsserver bestehen verfassungsrechtliche Bedenken, da diese Kontrolle grundsätzlich als hoheitliche Aufgabe der Verwaltung obliegt.*": Ob die Belegprüfung durch jede Person[20] oder nur durch autorisierte möglich ist, hängt lediglich von der genauen technischen Umsetzung des Verfahrens ab, ist also keine konzeptionelle Frage.
- *„Erst nach Abschluss des Geschäftsvorfalls kommt die Sicherung durch die elektronische Signatur zum Einsatz und verhindert ab diesem Zeitpunkt unprotokollierte Änderungen. Z. B. wird das Löschen eines Geschäftsvorfalls vor dessen Signierung nicht protokolliert.*": Es ist bis heute nicht schlüssig dargestellt worden, warum das Verfahren gemäß TR-03153 hier eine höhere Sicherheit bewirken soll.[21]
- *„Daher muss die INSIKA-Technik entsprechend ergänzt werden (wie z. B. die Erfassung des Zeitpunkts des Vorgangsbeginns über das Sicherheitsmodul), was ohne größeren Aufwand möglich ist.*": Siehe Ziffer 2.10

Abschließend ein letztes Zitat aus der Gesetzesbegründung: *„Durch die Technologieoffenheit ermöglicht das Zertifizierungsverfahren auch den Einsatz der INSIKA-Smartcard als Sicherheitsmodul in einer technischen Sicherheitseinrichtung, sofern die gesetzlichen Anforderungen erfüllt werden.*"

[19] *Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen* der Bundesregierung vom 5. September 2016, Drucksache 18/9535 <http://dip21.bundestag.de/dip21/btd/18/095/1809535.pdf #page=13>

[20] Randbemerkung: Da die Umsatzsteuer vom Empfänger der Rechnung bezahlt und vom Unternehmer lediglich treuhänderisch bis zur Zahlung an das Finanzamt verwahrt wird, stellt sich für uns als Nicht-Juristen die Frage, welche Bedenken gegen eine Kontrolle durch den Rechnungsempfänger bestehen könnten.

[21] Vgl. *Stellungnahme zum Referentenentwurf der* Kassensicherungsverordnung *(KassenSichV)*, 12. April 2017, <https://dfka.net/wp-content/uploads/2017/04/DFKA-zur-KassenSichV-E-2017-04.pdf>