Umsetzung der Kassensicherungsverordnung Eine kritische Analyse

Stand: 10. Dezember 2018[1]

1 Zusammenfassung

Zur praktischen Umsetzung der Kassensicherungsverordnung (KassenSichV), die ab 2020 eine „technische Sicherheitseinrichtung" (TSE) in Registrierkassen fordert, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Juni 2018 Technische Richtlinien (TR) veröffentlicht.

Diese beschreiben sehr abstrakt ein vergleichsweise komplexes Verfahren zur sicheren Speicherung beliebiger Daten. Die speziellen Anforderungen an eine Absicherung von Kassendaten sind dabei nicht berücksichtigt worden.

Ein derartiges Verfahren könnte auch weitgehend als Kombination bereits vorhandener Komponenten umgesetzt werden, jedoch erzwingen einige spezielle Anforderungen eine vollständige Neuentwicklung. Eine nachvollziehbare Begründung für diese speziellen Anforderungen gibt es nicht.

Der gesetzlich vorgegebene Termin 1. Januar 2020 soll offenbar unbedingt eingehalten werden, beispielsweise dadurch, dass das ursprünglich vom BSI geforderte Sicherheitsniveau anfänglich reduziert wird.

Ein weitaus größeres Problem ist allerdings die Tatsache, dass die TR nur einen kleinen Teil der zu lösenden Aufgaben abdecken. Es müssen weitere Prozesse und Komponenten entwickelt werden. Nach unserer Kenntnis sind diese weder klar definiert, noch wird daran gearbeitet.

Nach Ansicht des DFKA wird diese Herangehensweise zu unnötig hohen Kosten und einer Vielzahl von weiteren Schwierigkeiten bei der Umsetzung führen. Auch das Ziel der „Technologieoffenheit" dürfte verfehlt werden.

Um massive und langwierige Einführungsprobleme zu verhindern und mit Kosten von unter 50 Euro für eine TSE zumindest in die Nähe des in der Gesetzesbegründung genannten Kostenziels von 10 Euro zu kommen, halten wir es für unausweichlich, eine Kombination aus der Taxonomie für Kassendaten und dem INSIKA-Verfahren zumindest als Übergangslösung zuzulassen.

2 Grundsätzliches

Ende 2016 trat das Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen[2] in Kraft. Es fordert ab dem 1. Januar 2020 den Einsatz einer TSE in „elektronischen Auf-

[1] Diese Analyse wurde erstmals im September 2018 veröffentlicht. Die vorliegende, aktualisierte Version wurde wie folgt ergänzt: Kurze Beschreibung der Testspezifikation für TR-03153 im neuen Abschnitt 4.1.6; Ergänzte Liste der Prozesse im Abschnitt 5.1; Erläuterung des Bedarfs einer Meldung der Seriennummer der TSE an das Finanzamt im Abschnitt 6.3 per Fußnote

zeichnungssystemen", womit gemäß Konkretisierung in § 1 der KassenSichV[3] momentan allein „elektronische oder computergestützte Kassensysteme oder Registrierkassen" gemeint sind – das schließt Waagen mit Kassenfunktion[4] ein. Im Folgenden werden diese Geräte der Einfachheit halber durchgängig als „Registrierkasse" oder „Kasse" bezeichnet.

Zur praktischen Umsetzung bedarf es einer Reihe weiterer Schritte von der Formulierung der konkreten Anforderungen über die Definition von Prozessen, Produktentwicklungen und Zertifizierungen bis hin zur Installation der fertigen Systeme.

Während das Gesetzgebungsverfahren relativ transparent und auch für Nicht-Experten recht gut nachvollziehbar ablief, ist die praktische Umsetzung deutlich schwerer zu verfolgen und zu verstehen. Daher soll im Folgenden der aktuelle Stand dargestellt, analysiert und aus Sicht des DFKA bewertet werden. Im DFKA sind vor allem Anbieter von Kassenlösungen, also Hersteller und Wiederverkäufer organisiert.

Aufgrund der vielen Unklarheiten und des sich laufend ändernden Informationsstandes kann diese Analyse selbstverständlich nur eine Momentaufnahme darstellen. Sie gibt den Kenntnisstand und die Perspektive der an der Erstellung beteiligten Unternehmen und Personen wieder. Daher ist der DFKA jederzeit an einer weiterführenden Diskussion mit allen Beteiligten interessiert.[5]

In der nachstehenden Übersicht sind die wesentlichen zeitlichen Eckpunkte des Verfahrens dargestellt:

Datum	**Ereignis**
18.03.2016	Referentenentwurf des Gesetzes
13.07.2016	Regierungsentwurf des Gesetzes
22.12.2016	Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen
03.04.2017	Referentenentwurf Kassensicherungsverordnung
03.05.2017	Regierungsentwurf Kassensicherungsverordnung
26.09.2017	Kassensicherungsverordnung
Nov. 2017	Entwurf Technische Richtlinien
27.03.2018	Anhörung von Verbänden und Herstellern zu den Technischen Richtlinien
12.06.2018	Veröffentlichung der Technischen Richtlinien
26.07.2018	Ausschreibung Projekt „Zersika" durch BSI
01.01.2020	Gesetzlicher Einführungstermin

3 Aufgabenstellung

Die Absicherung von Registrierkassen gegen Manipulationen erscheint auf den ersten Blick relativ einfach und geradlinig. Tatsächlich handelt es sich aber um einen Eingriff in eine komplexe, heterogene Systemlandschaft. Daher ist es sinnvoll, zunächst die Aufgabenstellung in einer Übersicht darzustellen.

3.1 Anwendungsbereich / Relevante Daten

In vielen Unternehmen werden große Anteile des Umsatzes in Form von Bargeschäften getätigt. Die Kassenführung ist dort ein wichtiger Prüfungsschwerpunkt der Finanzverwaltung. An

---

[2] BGBl I Nr. 65 v. 28.12.2016, S. 3152-3154 <https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl116s3152.pdf>

[3] BGBl I Nr. 66 v. 06.10.2017, S. 3515-3516 <https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s3515.pdf>

[4] Aus der KassenSichV ist das nicht unmittelbar zu entnehmen, sondern nur im Begründungsteil des Entwurf ausgeführt <http://dip21.bundestag.de/dip21/btd/18/122/1812221.pdf#page=10>

[5] Kontakt: info@dfka.net

elektronische Registrierkassen als „Vorsysteme" der eigentlichen Buchführung werden deswegen besondere Anforderungen gestellt.

Spätestens seitdem Ende 2016 die Übergangsfrist aus dem BMF-Schreiben „Aufbewahrung digitaler Unterlagen bei Bargeschäften" vom 26. November 2010[6] ausgelaufen ist, müssen die Verkaufsdaten aus Registrierkassen immer als „Einzelaufzeichnungen" vorliegen. Damit ist gemeint, dass jeder einzelne Verkaufsvorgang im Detail (also mit Nennung der einzelnen Waren bzw. Dienstleistungen mit Menge und Preis) aufzuzeichnen ist.

Die Einzelaufzeichnungen sollen die Prüfmöglichkeiten der Finanzverwaltung gegenüber den vorher in vielen Fällen akzeptieren „Tagesendsummenbons"[7] verbessern und damit Umsatzverkürzungen erschweren. Dieses Ziel konnte nicht in ausreichender Form erreicht werden, da auch Einzelaufzeichnungen manipuliert werden können. Die Anzahl der aufgedeckten Fälle war offenbar groß genug, um einen politischen Handlungsbedarf entstehen zu lassen.

3.2 Ziele

Die Ziele sind vom Gesetzgeber nicht ausdrücklich formuliert worden, lassen sich aber aus Gesetzestext und -begründung relativ eindeutig ableiten:

- **Integrität**: Veränderungen der für Buchführung und Betriebsprüfung relevanten Daten soll verhindert oder eindeutig erkennbar gemacht werden
- **Authentizität**: Daten sollen sicher und eindeutig auf einen Urheber zurückgeführt werden können
- **Vollständige Erfassung**: Es soll überprüfbar sein, ob die Daten vollständig erfasst wurden
- **Zeitgerechte Erfassung**: Es soll überprüfbar sein, ob die Daten während oder kurz nach dem jeweiligen Geschäftsvorfall erfasst wurden (also nicht erst nachträglich)

3.3 Beteiligte / Rollen und deren Interessen

Die folgende Tabelle listet die beteiligten Personen bzw. Institutionen und deren wesentliche Interessen auf:[8]

Rolle	Interessen
Endkunden Personen, die an einer Registrierkasse bezahlen	- Kein zusätzlicher Aufwand - Ggf. Kontrollmöglichkeit der korrekten Registrierung des Geschäftsvorfalls[9]

[6] *BMF-Schreiben vom 26.11.2010 - IV A 4 - S 0316/08/10004-07* <https://www.bundesfinanzministerium.de/Content/DE/Downloads/BMF_Schreiben/Weitere_Steuerthemen/Betriebspruefung/2010-11-26-Aufbewahrung-digitaler-Unterlagen-bei-Bargeschaeften.html >

[7] Ein BMF-Schreiben vom 09.01.1996 erlaubte unter bestimmten Voraussetzungen, die Umsätze elektronischer Registrierkassen lediglich mit einem Ausdruck von Tagesgesamtsummen zu dokumentieren.

[8] In Ermangelung detaillierter Informationen beispielsweise aus dem Gesetzgebungsverfahren handelt es sich um eine eigene Analyse des DFKA.

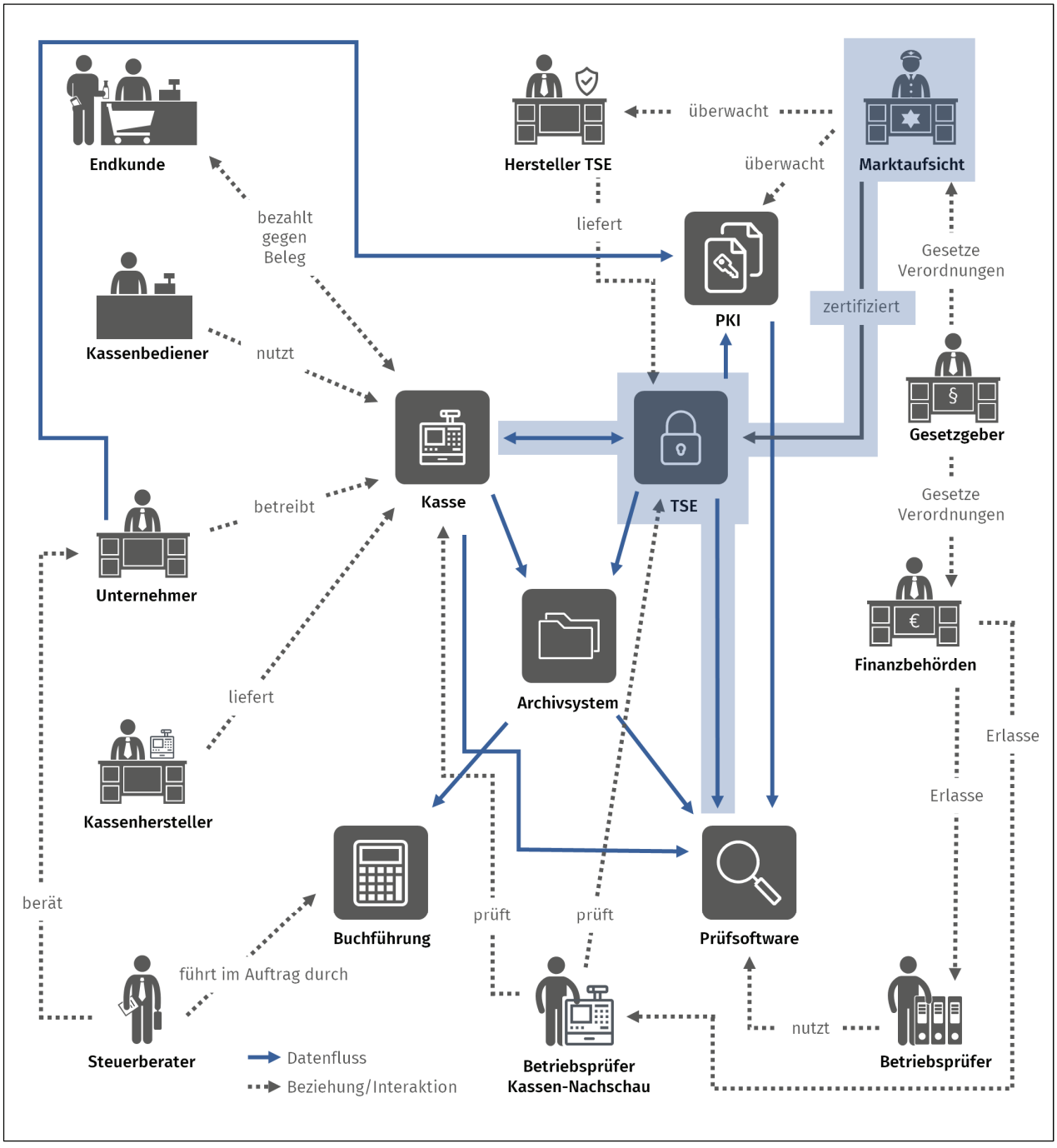
[9] Das Thema eines durch jedermann prüfbaren Sicherheitsmerkmals auf dem Beleg war politisch umstritten (bis hin zu Zweifeln an der Verfassungsmäßigkeit), jedoch dürften Bürger ein berechtigtes Interesse daran haben, dass die von Ihnen an der Registrierkasse bezahlte Umsatzsteuer auch tatsächlich angeführt wird.

Rolle	Interessen
Steuerpflichtige Einzelpersonen und Unternehmen, die Registrierkassen verwenden	- Eindeutige und einheitliche Anforderungen - Rechtssicherheit beim Einhalten der Anforderungen - Verbindliche Termine - Möglichst geringe Investitionen und laufende Kosten - Investitionssicherheit - Minimaler Bürokratieaufwand - Minimaler Dokumentationsaufwand - Keine Nachteile im Falle technischer Störungen - Kassen-Nachschau ohne Behinderung des Geschäftsablaufs
Anwender Personen, welche die Registrierkassen bedienen	- Möglichst keine Einschränkungen und Änderungen an bestehenden Abläufen - Minimaler Aufwand bei einer Kassen-Nachschau
Steuerberater Steuerliche Beratung und ausgelagerte Buchführung	- Eindeutige und einheitliche Anforderungen - Rechtssicherheit - Möglichkeit zur eigenen Verifikation und Prüfung der Kassendaten
Prüfer (Außenprüfung) Mitarbeiter/innen der Finanzverwaltung, die im Rahmen von Betriebsprüfungen Die Ordnungsmäßigkeit der Kassenführung überprüfen müssen	- Effektive Prüfabläufe - Leistungsfähige Verifikationssoftware - Standardisierung
Prüfer (Kassen-Nachschau) Mitarbeiter/innen der Finanzverwaltung, die Kassen-Nachschauen durchführen	- Schnelle und effektive Kassen-Nachschau - Einfache Erkennung von Verstößen
Anbieter von Registrierkassen Unternehmen, die Registrierkassen bzw. Softwarelösungen entwickeln, herstellen und vertreiben	- Eindeutige und einheitliche Anforderungen - Rechtssicherheit - Planungssicherheit bzgl. der Anforderungen und der Termine - Keine Behinderung der Weiterentwicklung - Minimaler Bürokratieaufwand
Anbieter von Archivsystemen Unternehmen, die Archivierungsdienstleistungen anbieten	- Eindeutige und einheitliche Anforderungen - Rechtssicherheit - Planungssicherheit bzgl. der Anforderungen und der Termine - Gleichwertigkeit von Daten im Archivsystem und in der TSE
Anbieter von TSE Unternehmen, die TSE entwickeln, herstellen und vertreiben	- Eindeutige und einheitliche Anforderungen - Rechtssicherheit - Planungssicherheit bzgl. der Anforderungen und der Termine - Kalkulierbare Kosten und Zeitaufwand für ein Entwicklungsprojekt

Rolle	Interessen
Finanzbehörden Finanzämter, Oberfinanzdirektionen o.ä., Bundeszentralamt für Steuern	- Eindeutige und einheitliche Anforderungen - Planungssicherheit bzgl. der Anforderungen und der Termine - Sauber implementierte Prozesse (z.B. zur Verwaltung gemeldeter Registrierkassen) - Vermeidung (finanz-)gerichtlicher Auseinandersetzungen
Technische Marktaufsicht Unternehmen und Behörden, die am Zertifizierungsprozess beteiligt sind	- Eindeutige und einheitliche Anforderungen - Planungssicherheit bzgl. der Anforderungen und der Termine
Gesetzgeber Bundestag, Bundesregierung und Bundesrat	- Keine Nachbesserungen an den gesetzlichen Grundlagen
Politik Initiatoren und Unterstützer der gesetzlichen Reglungen	- Erreichen der politischen Ziele, also Schaffung von Rechtssicherheit und Steuergerechtigkeit (durch gleichmäßigen Vollzug der Steuergesetze) - Minimierung Bürokratiekosten

3.4 Übersicht

In der folgenden Abbildung sind die wesentlichen Zusammenhänge schematisch dargestellt.



Die Technischen Richtlinien befassen sich lediglich mit dem markierten Teilbereich des Gesamtsystems – teilweise auch unvollständig (beispielsweise wird die Umwandlung von aus der TSE exportierten Daten in ein prüffähiges Format nicht behandelt).

3.5 Bewertung

Von der Einführung eines Manipulationsschutzes für Registrierkassen ist eine Vielzahl von Institutionen, Unternehmen und Personen betroffen. Die Strukturen und Prozesse sind zudem noch sehr verschieden, da hier die Bandbreite vom Kleinunternehmen bis zum internationalen Handelskonzern abzudecken ist.

Daher sollte eine Sicherheitslösung so wenig wie möglich in vorhandene Abläufe eingreifen. Bei der Entwicklung müssen die Interessen aller Betroffenen und sämtliche Prozesse berücksichtigt werden.

4 Entwicklung der TSE

In diesem Abschnitt wird ausschließlich die TSE betrachtet. Die weiteren Komponenten und erforderlichen Prozesse sind unter Ziffer 5 behandelt.

Die Umsetzung der Anforderungen bis zu einer zertifizierten und einsetzbaren TSE wird hier in Ermangelung eines besseren Namens als „TSE-Projekt" bezeichnet. Allerdings ist es kein Projekt im üblichen Sinne, allein schon deswegen, weil es keine Gesamtverantwortung und keine übergreifende Organisationsstruktur gibt (siehe auch 4.3.1).

4.1 Bekannte Anforderungen

Die Anforderungen für eine technische Umsetzung liegen nicht strukturiert und zusammengefasst vor, sondern müssen aus einer Vielzahl von Dokumenten zusammengetragen werden.

4.1.1 Gesetz

In der durch das Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen geänderten Abgabenordnung werden wesentliche rechtliche, organisatorische und technische Eckdaten definiert:

- Einzelaufzeichnungspflicht eindeutig gesetzlich verankert
- Verpflichtender Einsatz einer zertifizierten TSE ab dem 1. Januar 2020 (mit Übergangsfrist für nicht-nachrüstbare Systeme bis Ende 2022)
- TSE muss aus einem Sicherheitsmodul, einem Speichermedium und einer einheitlichen digitalen Schnittstelle bestehen
- Belegerteilungspflicht
- Verordnungsermächtigung (rechtliche Grundlage für die KassenSichV)
- Beauftragung des BSI
- Meldepflicht für elektronische Aufzeichnungssysteme
- Kassen-Nachschau
- Sanktionen (Bußgelder)
- Termine

4.1.2 Kassensicherungsverordnung

Die KassenSichV sollte die allgemein gehaltenen gesetzlichen Vorgaben konkretisieren. In dieser Hinsicht enttäuscht sie allerdings weitgehend. Im Wesentlichen werden die gesetzlichen Regelungen wiederholt. Auffällig ist bereits, dass der Text der Verordnung deutlich kürzer ist als derjenige des Gesetzes.

Die KassenSichV enthält gegenüber dem Gesetz lediglich folgende Konkretisierungen:

- Festlegung der betroffenen Aufzeichnungssysteme (nur „elektronische oder computergestützte Kassensysteme oder Registrierkassen")
- Vorgaben für den Inhalt einer „Transaktion" – es wird jedoch nicht ausreichend genau definiert, was eine Transaktion ist
- Anforderungen für eine Archivierung von Daten („digitale Grundaufzeichnungen") außerhalb der Registrierkasse
- Verbot einer Verdichtung der Einzelaufzeichnungen
- Definition der einheitlichen digitalen Schnittstelle als „Datensatzbeschreibung für den standardisierten Datenexport aus dem Speichermedium"
- Anforderungen an den Inhalt des Belegs

4.1.3 Technische Richtlinien

Die Technische Richtlinie *BSI TR-03153 Technische Sicherheitseinrichtung für elektronische Aufzeichnungssysteme* mit Datum 6. Juni 2018[10] behandelt folgende Aspekte:

- Genauere Darstellung der gewünschten Architektur der Sicherheitseinrichtung, also der Aufgabenverteilung zwischen Sicherheitsmodul, Speichermedium und einheitlicher digitaler Schnittstelle
- Begriffsdefinitionen – jedoch ist vor allem der zentrale Begriff der Transaktion (mit einzelnen Absicherungsschritten, die durch Log-Nachrichten dokumentiert werden) abstrakt definiert, so dass unklar bleibt, was im Kontext von Registrierkassen damit gemeint sein soll
- Beschreibung der Abläufe für die Erzeugung, die Aktualisierung und den Abschluss einer Transaktion
- Grundsätzliche Spezifikation des Sicherheitsmoduls mit der Muss-Anforderung einer internen Zeitquelle
- Grundsätzliche Spezifikation der Exportschnittstelle
- Grundsätzliche Spezifikation des Speichermediums

Die TR-03153 verweist zudem auf folgende Dokumente:

- *Technical Guideline TR-03151 – Secure Element Integration API*: Beschreibung einer allgemeinen und daher stark abstrahierten Schnittstelle zwischen der TSE und den anderen Komponenten des Gesamtsystems
- Technische Richtlinie TR-03116 – Kryptographische Vorgaben für Projekte der Bundesregierung – Teil 5 sowie Technische Richtlinie TR-02102 – Kryptographische Verfahren, Empfehlungen und Schlüssellängen: Aufstellung der momentan akzeptierten kryptografischen Verfahren
- Common Criteria Protection Profile PP-SMAERS – Security Module Application for Electronic Record-keeping Systems: siehe Ziffer 4.1.4
- Common Criteria Protection Profile PP-CSP – Protection Profile Cryptographic Service Provider: siehe Ziffer 4.1.4
- *Technical Guideline TR-03145 – Secure CA Operation*: Anforderungen an die Stellen, die kryptografische Zertifikate[11] erzeugen und verwalten

Der Gesamtumfang aller in diesem Abschnitt genannten Dokumente beträgt rund 400 Seiten.

4.1.4 Schutzprofile

Bei den Schutzprofilen (auch PP, „Protection Profile") handelt es sich um allgemein und abstrakt formulierte – und damit für Laien kaum verständliche – 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.[12] Diese Entwürfe wurden als Teil von Ausschreibungsunterlagen (siehe unter 4.1.5) veröffentlicht. Es handelt sich um bereits unter Ziffer 4.1.3 erwähnten 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 Softwareerweite-

[10] Website des BSI <https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03153/index_htm.html>
[11] Hierbei handelt es sich um Daten, die u.a. zur Prüfung digitaler Signaturen benötigt werden und nicht um die Zertifizierung von Geräten oder Software (also dem Prozess, der die Übereinstellung mit bestimmten Anforderungen bestätigt).
[12] Stand: Dezember 2018

rung des CSP, um die speziellen Anforderungen – im Wesentlichen die Abbildung von Transaktionen – an das Sicherheitsmodul zu erfüllen. Typischerweise kann das ein sog. Applet für eine Smartcard sein.

4.1.5 Ausschreibung Projekt 380 „Zersika"

Weitere Informationen lassen sich aus einer öffentlichen Ausschreibung des BSI vom 26. Juli 2018[13] ableiten. Informationen aus dem Ausschreibungstext:

- „Auftragsgegenstand ist die praktische Erprobung des neuartigen Konzeptes für die Zertifizierung eines Sicherheitsmoduls für Registrierkassen und weitere Aufzeichnungssysteme sowie die Mitwirkung bei der Optimierung des Konzeptes. Hierzu ist vom Auftragnehmer im Rahmen dieses Projektes zunächst ein Zertifizierungsverfahren für eine bestehende Implementierung eines Sicherheitsmoduls für Registrierkassenanwendungen[14] nach den vom BSI vorgegebenen Schutzprofilen […] nach CC zu durchlaufen. Anschließend ist vom Auftragnehmer zudem ein Zertifizierungsverfahren für ein Gesamtsystem einer technischen Sicherheitseinrichtung, bestehend aus Sicherheitsmodul, der zugehörigen Registrierkassenanwendung, einer digitalen Schnittstelle zur Einbindung in ein Aufzeichnungssystem sowie ein Speichermedium[…] durchzuführen."
- „[…] das BSI [hat] ein neuartiges Zertifizierungskonzept entwickelt, welches aus mehreren ‚koordiniert entwickelten' Schutzprofilen […] besteht. Dieses Konzept wurde bisher noch nicht in der Praxis erprobt."
- „In diesem Projekt werden keine Implementierungen beauftragt. Der Auftragnehmer muss daher bereits vor Projektstart sowohl über eine bestehende Implementierung eines Sicherheitsmoduls für Registrierkassenanwendungen als auch über ein funktionsfähiges Gesamtsystem verfügen, welche aus objektiver Sicht den Anforderungen der oben genannten Schutzprofile bzw. der Technischen Richtlinie genügen."
- Ein gutes Jahr (59 Wochen) nach Start des in der Ausschreibung beschriebenen Projektes soll eine komplette Sicherheitseinrichtung zertifiziert sein.
- Für den CSP wurde vom BSI bisher immer EAL4 augmented[15] (oft auch EAL4+ genannt) als Prüftiefe gefordert, also ein sehr hoher Sicherheitsstandard. In der Ausschreibung wird erstmalig ein „CSP light" mit Prüftiefe EAL2 erwähnt. In einer Antwort auf eine Bieterfrage wird das wie folgt erläutert: „Die Möglichkeit der Verwendung eines CSP light […] ist für eine angemessene Übergangszeit nach Inkrafttreten des ‚Gesetzes zum Schutz vor Manipulation an digitalen Grundaufzeichnungen' vorgesehen."

Schlussfolgerungen:

- Trotz Zeitdruck und hoher Komplexität wählt das BSI einen bisher nicht erprobten Ansatz für die Zertifizierung.
- Der gesetzliche Termin soll (weitgehend) gehalten werden.
- Das BSI geht offenbar davon aus, dass bereits jetzt oder wenigstens kurzfristig eine zertifizierungsfähige TSE vorliegt. Nach unserem Kenntnisstand ist das jedoch nicht der Fall.
- Beim „CSP light" dürfte es sich um eine Maßnahme zur Einhaltung der Termine handeln, da Zertifizierungen nach EAL4+ üblicherweise mindestens ein Jahr benötigen (die Zertifizierung des CSP ist nur eine Teilkomponente des Projektplans). Ein späterer Austausch der Hardware der TSE sowie die damit verbundenen Kosten werden also schon jetzt bewusst in Kauf genommen.

---

[13] e-Vergabe-Plattform, die Anlagen sind seit Ausschreibungsende am 27.08.2018 nicht mehr abrufbar <https://www.evergabe-online.de/tenderdetails.html?id=208108>

[14] Damit ist nicht die Software der Registrierkasse gemeint, sondern die Software im Sicherheitsmodul, die mit der Registrierkasse kommuniziert.

[15] Z.B. in der Präsentation zum Fachgespräch im Bundesministerium der Finanzen am 07.09.2017

4.1.6 Testspezifikation für TR-03153

Das BSI hat im Oktober 2018 eine Testspezifikation zur TR-03153 veröffentlicht.[16] Durch die dort beschriebenen Testfälle lassen sich einige Detailfragen etwas präziser beantworten als durch die TR allein.

Erwähnenswert sind folgende Aspekte:

- Auch die Testspezifikation nimmt keinen Bezug auf konkrete fachliche Anforderungen und behandelt die TSE rein abstrakt. Die dort definierten Tests haben damit keinen Aussagewert für die Einsetzbarkeit der TSE in einem Registrierkassen-Umfeld.
- Wesentliche Performance-Kriterien (Speicherkapazität, Verarbeitungsgeschwindigkeit bei Aufzeichnung und Datenexport) sind nicht Teil der Testspezifikation.
- Es wird erstmalig ein „fernverbundenes Speichermedium" erwähnt. Wie in diesem Fall Datenexport und Prüfung ablaufen sollen und wo genau die Abgrenzung zum Archivsystem (was ja ebenfalls ein Speichermedium außerhalb der Sicherheitseinrichtung ist) liegt, bleibt unklar.

4.2 Unbekannte Anforderungen

Mindestens genauso wichtig wie die bekannten sind die (noch) nicht bekannten Anforderungen an die TSE. Da im TSE-Projekt so gut wie alle fachlichen Anforderungen[17] bewusst ausgeblendet wurden, handelt es sich hier teilweise um sehr zentrale Fragen.

- Vor allem ist völlig offen, was eine „Transaktion" genau ist, wodurch sich folgende Unklarheiten ergeben:
- Welchen Inhalt haben die Transaktionen?
- Mit wie vielen Transaktionen und wie vielen Updates jeder Transaktion vor ihrem Abschluss ist zu rechnen? Noch im Frühjahr 2018 wurde von Vertretern des BMF geäußert, dass „jeder Tastendruck" aufzuzeichnen wäre.
- Je nach Definition einer Transaktion ist es möglich, dass diese in offenem Zustand zwischen verschiedenen Geräten mit jeweils eigener TSE ausgetauscht und dort aktualisiert werden. Das würde eine erhebliche Zunahme der Komplexität durch den gesamten Prozess hindurch (bis hin zur Prüfung der Daten) bewirken. Die wahrscheinlichste Auslegung würde erfordern, dass alle Updates einer Transaktion von der gleichen TSE verarbeitet werden – das bedingt eine komplexe Kommunikation zwischen den Geräten, die in den wenigsten Registrierkassen in dieser Form vorhanden sein dürfte.
- Es ist offen, wie Transaktionen in ein herstellerübergreifend vereinheitlichtes Format überführt werden sollen.
- Es ist nicht eindeutig definiert, ob alle prüfungsrelevanten Daten in der TSE enthalten sein sollen oder ob sie teilweise in der Registrierkasse und teilweise in TSE liegen – beide Ansätze führen zu unterschiedlichen Problemen, die jeweils eigene Lösungsansätze erfordern. In beiden Fällen integrieren sich die neuen Abläufe nicht in bereits vorhandene – das Speichern von Kassendaten in einer externen Einheit bedingt einen tiefen Eingriff in vorhandene Strukturen. Der einfachste Ansatz, bei dem die TSE selbst keine detaillierten Buchungsdaten speichert (sondern nur Informationen liefert, die zusammen mit den Buchungsdaten zu speichern sind), ist in der TR nicht vorgesehen.
- Das Verhältnis zwischen Daten in der TSE, in einem Backup und einem Archivsystem ist ungeklärt (rein technisch sollten sie aufgrund der kryptografischen Absicherung gleichwertig sein, die KassenSichV impliziert aber Unterschiede).

[16] Auf der Website des BSI am gleichen Ort wie die TR abrufbar, siehe Fußnote 10

[17] Die fachlichen Anforderungen definieren vor allem der Sicht der Anwender, was ein System leisten soll. Sie stehen im Gegensatz zu technischen Anforderungen, die beschreiben, wie ein System arbeiten soll.

- Die Anforderungen an Datenhaltung in verschiedenen Backup- und Archivsystemen sind ungeklärt, also z.B. in der Cloud, auf eigenen Servern, in PC-gestützten Backoffice-Systemen oder auf einfachen Speichermedien wie z.B. SD-Cards.

Die nötigen Entscheidungen werden sich erheblich auf das Design der TSE auswirken (vor allem in Bezug auf Speicherkapazität[18] und erforderlicher Verarbeitungsgeschwindigkeit[19]), so dass sie heute bereits getroffen sein müssten.

4.3 Risikofaktoren

Anhand der öffentlich verfügbaren Informationen und des bisherigen Verlaufs lassen sich eine Reihe von Risikofaktoren identifizieren – wie alle Aussagen in diesem Abschnitt ausschließlich bezogen das TSE-Projekt.

4.3.1 Projektorganisation

- Keine übergeordnete Projektleitung
- Keine Reporting- und Kontrollstrukturen für das Gesamtprojekt
- Aufteilung der Verantwortung
- BSI: Sicherheitsanforderungen und Zertifizierung
- BMF: steuerfachliche Anforderungen
- mehrere Unternehmen: Implementierung der Sicherheitseinrichtung
- Verschieben elementarer Fragen (z.B. Art und Umfang der abzusichernden Aufzeichnungen, die sich erst aus den noch nicht vorhanden steuerfachlichen Anforderungen ergeben werden) auf einen späteren Zeitpunkt
- Intransparente Entscheidungsprozesse
- Hoher Zeitdruck
- Keine Branchenerfahrung bei fast allen Beteiligten
- Keine Einbindung wesentlicher Stakeholder:
- Anwender
- Hersteller der verschiedenen Komponenten
- Betriebsprüfer
- Keine Nutzung der Erfahrung aus vergleichbaren nationalen und internationalen Projekten
- Neuer, bisher nicht erprobter Ansatz für die Zertifizierung

4.3.2 Anforderungen

- Die funktionalen Anforderungen[20]
- basieren teilweise auf politischen Vorgaben ohne fachliche Begründung und
- sind überwiegend technisch und nicht fachlich motiviert
- Nicht-funktionalen Anforderungen[21] wurden gar nicht erst formuliert
- Hoher Abstraktionsgrad
- Versuch, eine generische Lösung zu spezifizieren
- Komplexe Struktur der Anforderungen (mehrere wechselseitig aufeinander verweisende Dokumente)
- Widersprüche wie beispielsweise bei der Rolle des „Speichermediums" im Verhältnis zu einer Archivierung („externes elektronisches Aufbewahrungssystem") bereits in der KassenSichV

[18] Hier ist in der Praxis weniger die reine Bereitstellung von Speicher das Problem (auch in einfache Systeme lassen sich viele Gigabyte Speicher integrieren) sondern vielmehr die Verarbeitung der Daten (Konvertierung, Übertragung, Archivierung, Auswertung usw.)

[19] Die TR-03116, Teil 5 verlangt starke kryptografische Verfahren. Deren Berechnungen benötigt auf typischerweise eingesetzter Hardware mehrere Hundert Millisekunden. Dadurch, dass offenbar mehrere Änderungen an einer Transaktion zusammengefasst werden können (sofern sie in einem Zeitraum von maximal 45 Sekunden erfolgen), ist dieser Aspekt etwas entschärft.

[20] Funktionale Anforderungen legen fest, was ein System tun soll.

[21] Nicht-funktionale Anforderungen beschreiben Auflagen, Qualitätskriterien und Randbedingungen wie beispielsweise Arbeitsgeschwindigkeit, geringe Komplexität, Fehlertoleranz, Kostenziele usw.

- Keine ausreichenden Mindeststandards für eine Kompatibilität verschiedenen Implementierungen[22]

4.3.3 Entwicklung der Technik

- Forderung nach „Technologieoffenheit" wurde nicht mit konkreter Bedeutung gefüllt
- Keine marktgängige Standard-Hardware nutzbar (vor allem durch die Anforderung der sicheren Zeitquelle)
- Vorhandene, bewährte Konzepte nur teilweise genutzt
- Hohe Komplexität
- Aufteilung des Systems in mehrere, getrennt zu entwickelnde und zu zertifizierende Einzelkomponenten
- Keine Abschätzungen von kritischen Größen wie Speicherbedarf oder Performance, obwohl diese relevant für die Festlegung der Anforderungen wären
- Prototypen zur Verifikation der Grundannahmen sind nicht vorgesehen
- Keinerlei Referenzimplementierungen geplant

4.3.4 Veraltetes Design-Paradigma

Die TR definieren ein Verfahren, das hochabstrakt ist, d.h. die fachlichen Anforderungen werden weitestgehend ausblendet. Dieser Ansatz steht im diametralen Gegensatz zu modernen Herangehensweisen. Beispiele:

- Bei agilen Methoden[23] ist die Anforderung des Anwenders, z.B. in Form von „User Stories" der Ausgangspunkt für jede Implementierung.
- Beim „Domain-driven Design" folgt sogar das gesamt Softwaredesign vorrangig den fachlichen Anforderungen.

4.3.5 Bewertung der Risikofaktoren

Bereits einzelne der hier genannten Risikofaktoren führen erfahrungsgemäß zu Fehlern, Verzögerungen und unnötig hohen Kosten.

Da jedoch alle diese Faktoren gleichzeitig vorliegen, erscheint es sehr unwahrscheinlich, dass ein zufriedenstellendes Ergebnis erreicht werden kann.

4.4 Zusammenfassung

Die Kernfunktionalität des in den TR spezifizierten Systems lässt sich relativ leicht beschreiben:

- Beliebige Datensätze können mit einer Nummerierung, einer Zeitinformation und einer elektronischen Signatur versehen,
- zu fortlaufend nummerierten Transaktionen zusammengefasst,
- abgespeichert und
- auf Anforderung in eine Datei geschrieben werden.

Für diese vergleichsweise einfachen Funktionen wird allerdings ein sehr hoher Aufwand auf allen Ebenen (Spezifikation, Technik, Zertifizierung) getrieben. Die spezifischen fachlichen Anforderungen an eine Absicherung von Registrierkassendaten sind dabei jedoch nicht berücksichtigt worden.

[22] Konkret bedeutet das in diesem Fall, dass die Daten für Betriebsprüfungen und Kassen-Nachschauen nicht soweit standardisiert sind, dass sie mit einer einheitlichen Software ohne weiteren Aufwand geprüft werden können.

[23] Wie z.B. das wohl bekannteste Vorgehensmodell „Scrum", <https://de.wikipedia.org/wiki/Scrum>

5 Weitere Entwicklungsaufgaben

Das unter Ziffer 4 beschriebene TSE-Projekt deckt nur einen Teil dessen ab, was für einen reibungslosen Betrieb der Sicherheitseinrichtungen erforderlich ist. Die weiteren Komponenten sind in diesem Abschnitt nur in Form einer groben Übersicht dargestellt.

5.1 Prozesse

Neben der technischen Lösung müssen während der Umsetzungsphase auch Prozesse definiert, getestet und optimiert werden.

Eine Übersicht ohne Anspruch auf Vollständigkeit:

- Beantragung und Personalisierung der TSE
- Verwaltung kryptografischer Zertifikate
- Anmeldung der Registrierkassen und/oder der TSE bei den Behörden (inkl. der Automatisierung des Prozesses)
- Korrektur einer versehentlich fehlerhaft durchgeführten Anmeldung der Registrierkassen und/oder der TSE
- Vergabe und Verwaltung von Seriennummern der Kassen (diese spielen eine zentrale Rolle in Gesetz und TR)
- Abläufe einer Außenprüfung mit Export der Daten aus TSE
- Abläufe einer Außenprüfung mit Export der Daten aus einem Archivsystem
- Ablauf einer Kassen-Nachschau mit reiner Belegprüfung (falls es überhaupt prüfbare Belege geben wird)
- Ablauf einer Kassen-Nachschau mit Datenzugriff (entweder als einzige Variante oder als zweite Stufe nach einer Belegprüfung)
- Außerbetriebnahme einer TSE (inkl. Diebstahl oder Verlust)
- Austausch einer defekten TSE
- Außerbetriebnahme einer Kasse bei Weiterverwendung der TSE in einer anderen Kasse
- Dauerhafter Austausch einer Kasse bei Weiterverwendung der TSE
- Temporärer Austausch einer Kasse (zur Reparatur) bei Weiterverwendung der TSE
- Nutzung einer Leihkasse (typischerweise z.B. auf Veranstaltungen wie Volksfesten)
- Zurückziehen der Zulassung einer TSE (z.B. wenn eine Sicherheitslücke erkannt wurde)
- Arbeiten bei temporärem Ausfall der TSE (z.B. bei einem defektem Kartenleser)
- Verhalten bei versehentlichem Einsatz einer falschen TSE
- Betrieb einer TSE mit einer zurückgelesenen Datensicherung einer anderen Kasse (also ggf. teilweise falschen Stammdaten)
- Plausibilitätsprüfung der aufgezeichneten Daten unternehmensintern oder durch Steuerberater
- Zugriff der Prüfer auf zentrales Register der Kassen/TSE im Rahmen von Betriebsprüfungen / Kassen-Nachschauen
- Bereitstellung von Test-TSEs z.B. für Software-Entwickler

Bei den hier genannten Prozessen gibt es im Wesentlichen zwei (grundsätzlich vermeidbare) Komplexitätstreiber:

- Berücksichtigung der Registrierkassen als einzelne Geräte (z.B. über Anmeldung der Seriennummern) – die einfachere Alternative wäre die ausschließliche Prüfung (z.B. auf Vollständigkeit der Daten) anhand der TSE
- Keine Standardisierung der Daten, die für eine Prüfung bereitzustellen sind

5.2 Weitere Komponenten

Eine wesentliche Komponente im System ist die Software zur Verifikation der Daten.[24] Sie muss u.a. folgende Anforderungen erfüllen:

- Bei mehreren TSE-Anbietern (was ja erklärtes politisches Ziel ist) muss es entweder eine einheitliche Prüfsoftware geben oder es muss eine praktikable Lösung zur parallelen Nutzung verschiedener Programme geben. Für ein praktisch funktionierendes System ist hier eine sehr weitgehende Standardisierung unausweichlich.[25] Die genaue technische Implementierung muss dabei selbstverständlich nicht vorgegeben werden.[26]
- Die Software muss im Rahmen der IT-Systeme der Finanzverwaltung funktionieren (Nutzung auf Hardware der Prüfer[27] und Schnittstelle zu bzw. Integration in die Prüfsoftware IDEA).
- Es muss eine Lösung für den Zugriff auf die Datenbank gemeldeter Registrierkassen/TSE sowie zur Zusammenführung der kryptografischen Zertifikate mehrere Anbieter implementiert werden.

Auch für die Anmeldung der Registrierkassen und/oder TSE bei den Finanzbehörden muss eine passende Software-Infrastruktur geschaffen werden.

Für jede Software-Lösung ist zu klären, wer sie liefert und wie sie finanziert wird. Die Verantwortung für Schulungen, Support und Weiterentwicklung für den gesamten erwarteten Nutzungszeitraum ist zu regeln.

5.3 Übergeordnetes Einführungsprojekt

Auch für die in diesem Abschnitt genannten Aufgaben ist eine leistungsfähige Projektorganisation erforderlich. Nach unserer Einschätzung werden mehrere qualifizierte Personen für mehrere Jahre benötigt. Die unter 4.3.1 genannten Probleme stellen sich hierbei mindestens in der gleichen Form.

6 Problemfelder

Insgesamt ergeben sich aus den Rahmenbedingungen und der Form der Umsetzung eine Vielzahl von Problemen, die im Folgenden thematisch gegliedert aufgeführt sind.

6.1 Termine

Der gesetzliche Termin soll offenbar weitgehend gehalten werden (siehe 4.1.5). Daher wird speziell in Verbindung mit den unter 4.3 geschilderten Risikofaktoren sowie der unter Ziffer 5 beschriebenen Lücken ein extremer Zeitdruck entstehen.

Typischerweise wird in solchen Situationen dann versucht, Zeit in vermeintlich weniger wichtigen Phasen, wie Reviews oder Praxistests einzusparen. Das führt fast unausweichlich zu (weiteren) konzeptionellen und Umsetzungsfehlern, die wiederum teure Nachbesserungen erfordern.

---

[24] Diese Software prüft die Daten unter den im Abschnitt 3.2 dargestellten Aspekten aber nicht deren Inhalte. Sie ist also eine Ergänzung zur heute genutzten Software zur inhaltlichen Prüfung der Daten.

[25] Bei der Rechnungssignatur gem. §14 UStG (eingeführt 2004) wurde es versäumt, einen vereinheitlichten und damit in der Praxis funktionierenden Prüfmechanismus zu schaffen. Dieser konzeptionelle Fehler dürfte ein wesentlicher Grund für das Scheitern gewesen sein (die Reglung wurde 2011 wieder abgeschafft).

[26] Analogie: Im Internet müssen alle Geräte das standardisierte IP-Protokoll und viele weitere darauf aufbauende Protokolle verwenden. Die technische Umsetzung ist aber vollkommen freigestellt.

[27] Die Verarbeitung und Verifikation von Massendaten wie sie von Registrierkassen erzeugt werden stellt hohe Anforderungen an Hard- und Software. Werden Lösungsansätze nicht von Anfang passend ausgelegt, ist hier mit Problemen zu rechnen.

6.2 Markt und Wettbewerb

Laut Gesetzesbegründung ist eines der Ziele, den Wettbewerb zwischen mehreren Herstellern von Sicherheitseinrichtungen zu ermöglichen und zu fördern. Darüber soll offenbar unter anderem sichergestellt werden, dass Anwender den günstigsten Preis für die Sicherheitseinrichtungen bezahlen. Hier sind zumindest Zweifel angebracht.

6.2.1 Technologieoffenheit

In der politischen Diskussion wurde immer wieder die Forderung nach „Technologieoffenheit" aufgestellt – im Begründungsteil des Gesetzentwurfs wird die Regelung dementsprechend auch mehrfach als „technologieoffen" bezeichnet.

Eine objektive Bewertung wird dadurch erschwert, dass es keine Definition von „Technologieoffenheit" gibt. Da im Gesetzentwurf das Vorschreiben eines bestimmten Verfahrens als Gegenteil von „Technologieoffenheit" bezeichnet wird, lässt sich daraus zumindest eine sehr grobe Definition ableiten – es ist also „technologieoffen", kein bestimmtes Verfahren vorzugeben.

Die Forderung nach einem Sicherheitsmodul mit integrierter, sicherer Zeitquelle ist bisher niemals nachvollziehbar begründet worden. Dies schränkt die Auswahl der Hardware für das Sicherheitsmodul schon vom Grundsatz her stark ein. Aus Sicht des DFKA werden damit unnötige technische Beschränkungen auferlegt, wodurch das gesetzgeberische Ziel der Technologieoffenheit konterkariert wird. Momentan ist eine preiswerte, passende Hardware nicht lieferbar und noch nicht einmal zu einem konkreten Termin angekündigt.

6.2.2 Mögliche Effekte des Projektes „Zersika"

Die gezielte Förderung eines einzelnen Anbieters einer Sicherheitseinrichtung (vor allem durch einen Zeit- und Know-How-Vorsprung) erscheint bedenklich. Es besteht das Risiko eines faktischen Monopols. Dies müsste durch eine entsprechende Regulierung (vor allem der Preise) kompensiert werden. Entsprechende Bemühungen sind uns bisher jedoch nicht bekannt.

6.3 Praxistauglichkeit

Das Ausblenden fachlicher Anforderungen und der Anwendersicht führt dazu, dass wichtige Aspekte für einen problemlosen Einsatz in der Praxis nicht angemessen berücksichtigt wurden. Beispielhaft sind zu nennen:

- Durch die heute geltende Verpflichtung, den Finanzbehörden Einzelaufzeichnungen in digitaler Form vorzulegen, sind bei den Anwendern von Registrierkassen entsprechende Prozesse und technische Lösungen geschaffen worden.[28] Das Speichern von Daten innerhalb der TSE (unabhängig von der Frage, ob alle prüfungsrelevanten Daten oder nur in Teil dort zu speichern sind) lässt sich nicht leicht in diese vorhandenen Strukturen integrieren (siehe auch 4.2).
- Die gesetzlich geforderte Anmeldung jeder Registrierkasse beim Finanzamt könnte leicht automatisch bei der Personalisierung des Sicherheitsmoduls vorgenommen werden. Das ist offenbar nicht geplant.
- Eine zeitsparende Kassen-Nachschau in Form einer reinen Belegkontrolle (anhand eines prüfbaren Sicherheitsmerkmals auf dem Beleg) ist nicht vorgesehen. Eine Kassen-Nachschau erfordert vielmehr stets einen Datenzugriff.
- Eine Lösung für teilweise Datenverluste (wie etwa manipulationsgeschützte Summenwerte, die für Zeiträume mit Datenverlusten wenigstens Gesamtumsätze liefern) existiert nicht.

[28] Spätestens durch das BMF-Schreiben vom 26.11.2010, siehe Fußnote 6

- Bei der Meldung der Registrierkassen an das Finanzamt wird neben der Seriennummer der Kasse auch die der TSE zu übermitteln sein.[29] Diese sieht z.B. so aus: „e3d0a71a2b2d920b2cf148fdab67909e442c782f584c4ead99760f654937f540", oder etwas besser lesbar gemacht: „e3d0-a71a-2b2d-920b-2cf1-48fd-ab67-909e-442c-782f-584c-4ead-9976-0f65-4937-f540". Eine Plausibilitätsprüfung bei der Eingabe ist vermutlich nicht möglich, so dass mit einer hohen Quote von Fehleingaben zu rechnen sein dürfte.[30]

6.4 Rechtssicherheit

Es ist fraglich, ob die für alle Beteiligten vorteilhafte Rechtssicherheit erreichbar ist. Da (bisher) keine verbindlichen Vorgaben für Inhalte existieren, ist davon auszugehen, dass die Auseinandersetzungen zwischen Finanzverwaltung und Steuerpflichtigen über den Umfang der Aufzeichnungen[31] weitergehen werden.

6.5 Kosten

Während im Gesetzentwurf noch Kosten von 10 Euro[32] für eine Sicherheitseinrichtung in Aussicht gestellt wurden, erscheint ein Preis im Bereich zwischen 30 und 40 Euro realistisch. Dieser wäre erreichbar, wenn es sich bei der Sicherheitseinrichtung um eine marktgängige Smartcard mit einem speziellen Applet sowie einem weitgehend automatisierten Antrags- und Zertifikatsverwaltungsverfahren nach heutigem Stand der Technik handelt. Falls es dabei nur einen Anbieter – also keinen Wettbewerb – gäbe, müsste der Preis ggf. reguliert werden.

Das in den Technischen Richtlinien umrissene System erzwingt einige Eigenschaften der Sicherheitseinrichtung, die kostentreibend wirken:

- Das Speichermedium und die „einheitliche digitale Schnittstelle" als Teil der zertifizierten Sicherheitseinrichtung erhöhen den Hardware- und Zertifizierungsaufwand – die Sicherheitseinrichtung ähnelt damit der in Belgien eingesetzten „Fiskalbox", die mehrere Hundert Euro pro Stück kostet.
- Die Anforderung einer Zeitquelle im Sicherheitsmodul schränkt die Hardware-Auswahl erheblich ein. Die aktuelle Smartcard-Generation scheidet damit als Hardware für ein Sicherheitsmodul aus.
- Das gewählte Zulassungsverfahren, das eine Aufteilung in mehrere verschiedene Zertifizierungen bedingt, erhöht die Komplexität und damit die Kosten erheblich.

Der Preis der momentan durch die TR umrissenen Lösung dürfte daher ein Vielfaches des möglichen Optimums betragen.

7 Fazit und Handlungsempfehlung

Die aktuellen Aktivitäten von BSI und BMF befassen sich lediglich mit einer unserer Auffassung nach unnötig aufwändigen Lösung eines Teilaspekts, während wesentliche Teile des Gesamtsystems momentan nicht bearbeitet werden. Es existiert kein der Aufgabe annähernd angemessenes Projektmanagement.

---

[29] Diese Anforderung ergibt sich indirekt: § 146a AO fordert die Meldung der Seriennummer jeder Registrierkasse an das Finanzamt. Die KassenSichV erlaubt den Abdruck der Seriennummer der Kasse oder der Seriennummer der TSE auf dem Beleg. Die TR enthält diesbezüglich keine weiteren Präzisierungen. Um anhand eines Belegs eine sinnvolle Prüfung vornehmen zu können, muss über den Beleg eine Verknüpfung zum bei den Behörden gemeldeten Aufzeichnungssystem hergestellt werden können. Dazu muss das von den Finanzbehörden geführte Register beide Seriennummern enthalten.

[30] Eine Prüfsumme zur Erkennung von Eingabefehlern ist nicht enthalten. Es wäre nur ein Abgleich gegen eine Datenbank mit allen Zertifikaten möglich. Diese dürfte aber in der benötigten Form nicht existieren, da sonst ja die gesamte Meldeplicht für Kasse und TSE überflüssig wäre (denn dann wären der Finanzverwaltung bereits alle TSEs und – je nach Personalisierungsverfahren auch deren Nutzer – bekannt).

[31] Beispielsweise wird aktuell in Praxis, Rechtsprechung und Literatur über sog. Programmierprotokolle gestritten während noch nicht einmal eine Definition des Begriffs existiert.

[32] *Entwurf eines Gesetzes zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen* der Bundesregierung vom 05.09.2016, Drucksache 18/9535 <http://dip21.bundestag.de/dip21/btd/18/095/1809535.pdf#page=16>

Aus Sicht des DFKA ist es nicht vorstellbar, dass dieser Weg zu einer praktikablen und preiswerten technischen Lösung führen kann. Es gibt eine zu große Zahl von Lücken und Unklarheiten um diese in absehbarer Zeit beseitigen zu können. Da die Termine offenbar trotzdem unbedingt gehalten werden sollen, wird der daraus entstehende hohe Zeitdruck zu weiteren Schwierigkeiten führen.

Die einzig sinnvolle Alternative ist der Einsatz einer fertigen und erprobten Lösung, die sich im durch das Gesetz definierten Rahmen bewegt – ggf. auch als Übergangslösung. Hierfür kommen nach Kenntnis des DFKA momentan nur zwei Ansätze in Frage:

- INSIKA („Integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme"): Das Verfahren 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. Die Bundesdruckerei bietet mit der „TIM Card" seit mehreren Jahren eine INSIKA-Implementierung an.
- Lösung gemäß RKSV („Registrierkassensicherheitsverordnung") aus Österreich: Dieses Verfahren nutzt marktgängige Signaturkarten in Verbindung mit vorgeschriebenen Softwarefunktionen in den Registrierkassen sowie einer Cloud-Anwendung der Finanzverwaltung.

Aufgrund einer bekannten und praktisch relevanten Sicherheitslücke – der Möglichkeit, beliebig viele Buchungen vom Ende her entfernen zu können, ohne dass dies Spuren in den Daten hinterlässt – kommt das RKSV-Verfahren aber mit großer Wahrscheinlichkeit nicht in Frage.

INSIKA wurde konsequent unter Einbeziehung der Perspektive der verschiedenen Nutzer designt, implementiert und getestet. TIM Cards werden seit Jahren in mehr als 10.000 Taxametern erfolgreich eingesetzt.

Sicherheitslücken im INSIKA-Verfahren wurden immer wieder behauptet, allerdings nie belegt.[33] Ein erfolgreicher Angriff auf das Verfahren wurde bisher nicht beschrieben.

Einige weitere Ansätze haben zwar Ähnlichkeiten, entsprechen jedoch nicht den gesetzlichen Vorgaben:

- GKS („Geregistreerd kassasysteem" = „registriertes Kassensystem") in Belgien: Neben den hohen Kosten (eine Sicherheitseinrichtung kostet mehrere Hundert Euro) widerspricht die erforderliche Zertifizierung der Registrierkassen selbst (also nicht nur der Sicherheitseinrichtung) den deutschen gesetzlichen Vorgaben.
- Signierte Audit-Dateien (SAF-T) in Portugal: Dieses Verfahren bietet nicht die erforderliche Sicherheit (Management der kryptografischen Schlüssel entspricht nicht dem Stand der Technik) und erfordert ebenfalls eine Zertifizierung der Registrierkassensoftware.
- Zertifizierungsverfahren in Frankreich: Hier erfolgt ebenfalls eine Zertifizierung der Software auf Basis einer sehr allgemein gehaltenen gesetzlichen Vorgabe (durch einen von zwei Anbietern auf Basis jeweils selbst entwickelter, sehr unterschiedlicher Vorgaben)

Damit verbleiben auf dem INSIKA-Verfahren basierende Sicherheitsmodule wie die TIM Card der Bundesdruckerei als einzig realistische Lösung. Der DFKA vertritt diese Linie bereits seit 2016.[34]

Grundsätzlich ist das INSIKA-Verfahren auch um die in den TR geforderte Zeitquelle im Sicherheitsmodul erweiterbar, sobald passende Hardware verfügbar ist.[35]

---

[33] Z.B. *Ein Kasse für sich*, Spiegel Online vom 17.03.2016 <http://www.spiegel.de/wirtschaft/soziales/steuern-wolfgang-schaeuble-will-betrug-mit-kassen-bekaempfen-a-1082896.html>

[34] Siehe z.B. Stellungnahme zur Anhörung im Finanzausschuss <https://www.bundestag.de/blob/477742/2856f05a48dcdb72be73ad28c36b6fa3/protokoll-data.pdf#page=47> Seite 47 bis 60, Kommentar zum Gesetz <https://dfka.net/bewertung-des-gesetzes-zum-schutz-vor-manipulationen-an-digitalen-grundaufzeichnungen/> oder Kommentierung des Entwurfs der KassenSichV <https://dfka.net/verordnung-zur-bestimmung-der-technischen-aufzeichnungs-und-sicherungssysteme-im-geschaeftsverkehr-2/>

Idealerweise wird das INSIKA-Verfahren mit der Taxonomie für Kassendaten[36] kombiniert. In dieser Kombination sind auch die Lösungen für praktisch alle unter Ziffer 5 dargestellten Teilaspekte definiert, entwickelt und erfolgreich erprobt worden.

Die Praxistauglichkeit der Taxonomie, des INSIKA-Verfahrens und der Kombination beider Lösungen wurde im Rahmen eines Feldtests der Taxonomie für Kassendaten nachgewiesen.[37] Sieben Kassenhersteller mit verschiedenen technischen Plattformen und unterschiedlichen Branchenschwerpunkten haben das INSIKA-Verfahren im Rahmen dieses Feldtests erfolgreich implementiert sowie im Labor- und Echtbetrieb zum Einsatz gebracht. Wie erwartet, hat der Feldversuch diverse kleinere technische und konzeptionelle Probleme aufgedeckt. Entsprechende Anpassungen am INSIKA-Verfahren sind einfach möglich.

---

[35] *Whitepaper: Zeitinformationen beim Manipulationsschutz für Registrierkassen*, ADM e.V. <http://www.insika.de/news/65-whitepaper-zeitinformationen-beim-manipulationsschutz-fuer-registrierkassen>

[36] Weitere Informationen auf der Website des DFKA e.V. <https://dfka.net/taxonomie/>

[37] *Feldversuch Taxonomie Zwischenbericht Juli 2018* vom 19.07.2018, DFKA e.V. <https://dfka.net/zwischenbericht-zum-feldtest-der-taxonomie/>