Verordnung des Bundesministers für Finanzen über die technischen Einzelheiten für Sicherheitseinrichtungen in den Registrierkassen und andere, der Datensicherheit dienende Maßnahmen (Registrierkassensicherheitsverordnung, RKSV)

Aufgrund der §§ 131b Abs. 5 Z 1, 3 und 4 und § 132a Abs. 8 der Bundesabgabenordnung – BAO, BGBl. Nr. 194/1961, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 118/2015, wird verordnet:

Inhaltsverzeichnis

1. Hauptstück
Allgemeiner Teil

Anwendungsbereich

§ 1. Die Registrierkassensicherheitsverordnung regelt

1. die zur technischen Umsetzung der Manipulationssicherheit elektronischer Aufzeichnungssysteme erforderlichen technischen Merkmale
   a) der Registrierkasse,
   b) der Signaturerstellungseinheit,
   c) der Kommunikation zwischen Registrierkasse und Signaturerstellungseinheit,
2. die zusätzlichen Anforderungen an den Beleg gemäß § 132a Abs. 8 der Bundesabgabenordnung – BAO, BGBl. Nr. 164/1961,
3. Einzelheiten über die Erlassung von Feststellungsbescheiden betreffend geschlossene Gesamtsysteme und
4. den Zugriff der Behörden auf die dafür erforderlichen Daten für aufsichts- und abgabenrechtliche Zwecke.

Personenbezogene Bezeichnungen

§ 2. Alle in dieser Verordnung verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für Personen sowohl weiblichen als auch männlichen Geschlechts.

Abkürzungen und Begriffsbestimmungen

§ 3. Im Sinne dieser Verordnung ist oder sind:

1. AES-256: Verschlüsselungsverfahren nach dem Advanced Encryption Standard (AES FIPS 197 26/11/2001) mit einer Schlüssellänge von 256 Bit
2. Barcode: Standard „Code 128“, definiert in ISO/IEC 15417:2007
3. Barumsatz: Umsätze im Sinne § 131b Abs. 1 Z 3 BAO
4. Datenbank über Sicherheitseinrichtungen in Registrierkassen: Datenbank des Bundesministeriums für Finanzen, in der die in § 18 Abs. 2 genannten Daten betreffend die Sicherheitseinrichtungen in Registrierkassen und Kontrollen der Sicherheitseinrichtungen festgehalten werden
5. Datenerfassungsprotokoll (DEP): eine im Speicher der Registrierkasse oder in einem externen Speicher mitlaufende Ereignisprotokolldatei, die in Echtzeit jeweils mit Belegerstellung vollständig, fortlaufend chronologisch die Barumsätze mit Beleginhalten dokumentiert
6. Eingabestation: Einrichtung zur Erfassung von Barumsätzen, die mit einer Registrierkasse insbesondere zur Signierung und Dokumentation der Barumsätze verbunden ist
7. Elektronische Aufzeichnung: vollständige, fortlaufend chronologisch geordnete Dokumentation von Bargeschäften in elektronischer Form
8. Elektronische (kryptographische) Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung dienen im Sinne des § 2 Z 1 des Signaturgesetzes – SigG, BGBl. I Nr. 190/1999
9. FinanzOnline: elektronisches Verfahren der Abgabenbehörde nach der FinanzOnline-Verordnung 2006, BGBl. II Nr. 97/2006, in der jeweils geltenden Fassung
10. Geschlossenes Gesamtsystem: elektronisches Aufzeichnungssystem, in welchem Warenwirtschafts-, Buchhaltungs- und Kassensysteme lückenlos miteinander verbunden sind und das mit mehr als 30 Registrierkassen verbunden ist
11. Global Location Number (GLN): von der Bundesanstalt Statistik Österreich unter der Bezeichnung „Sekundär ID“ vergebener Ordnungsbegriff
12. Hardware-Sicherheitsmodul (HSM): Signaturerstellungseinheit, die zur Erstellung (qualifizierter) elektronischer Signaturen verwendet wird und vor allem bei serverbasierten Lösungen zum Einsatz kommt
13. Homepage des Bundesministeriums für Finanzen (BMF): www.bmf.gv.at
14. Kassenidentifikationsnummer: über FinanzOnline gemeldetes Kennzeichen einer Registrierkasse, das auch die Unterscheidung verschiedener Registrierkassen mit gleicher Signaturerstellungseinheit ermöglicht
15. Maschinenlesbarer Code: Eingangswert für OCR-, Barcode- oder QR-Code-Repräsentation

16. Monatszähler: Summenspeicher in der Registrierkasse, der die Zwischenstände des Umsatzzählers zum Monatsende festhält
17. Object Identifier (OID): weltweit eindeutiger Bezeichner nach ISO/IEC 9834-1 und A 2642, der benutzt wird, um ein Informationsobjekt zu benennen. In dieser Verordnung wird der OID verwendet, um die Verwendung des Signaturzertifikates nach § 5 Abs. 1 Z 8 SigG in der jeweils geltenden Fassung, auf den Zweck 'Österreichische Finanzverwaltung Registrierkasseninhaber' einzuschränken
18. Optical Character Recognition (OCR): Standard OCR-A, definiert in ISO 1073-1:1976
19. Ordnungsbegriff des Unternehmers: ein der Abgabenbehörde bekannter Schlüssel zur Identifizierung des Unternehmers (Steuernummer, UID-Nummer, GLN)
20. QR-Code: zweidimensionales Symbol nach Standard JIS X 0510/2004
21. Registrierkasse (auch elektronische Registrierkasse): verallgemeinerte Form jedes elektronischen Datenverarbeitungssystems, das elektronische Aufzeichnungen zur Losungsermittlung und Dokumentation von einzelnen Barumsätzen erstellt, insbesondere elektronische Registrierkassen jeglicher Bauart, serverbasierte Aufzeichnungssysteme (auch zur Abwicklung von Online-Geschäften), Waagen mit Kassenfunktionen und Taxameter. Eine Registrierkasse kann mit Eingabestationen verbunden sein
22. Seriennummer des Signaturzertifikates: eine durch den Zertifizierungsdiensteanbieter ausgegebene, im Zertifikat enthaltene, eindeutige Kennung des Zertifikates zum erleichterten Auffinden des Zertifikates im Verzeichnis des ZDA
23. Sichere Signaturerstellungseinheit: konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird und die den Sicherheitsanforderungen des SigG sowie den dazu erlassenen Verordnungen entspricht (§ 2 Z 5 SigG)
24. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden (§ 2 Z 6 SigG)
25. Signaturwert: im Rahmen der Signaturerstellung ermittelter elektronischer Wert der Signatur
26. Startbeleg: erster Beleg, der unter Verwendung einer Kassenidentifikationsnummer erstellt wird und die vollständige Verkettung aller unter dieser Kassenidentifikationsnummer erzeugten und gespeicherten Belege sicherstellt
27. Summenspeicher: Speicher in der Registrierkasse, die Zwischen- oder einen aktuellen Endstand aufsummierter Beträge wiedergeben
28. Trust-List (vertrauenswürdige Liste gemäß der Entscheidung der Kommission 2009/767/EG über Maßnahmen zur Erleichterung der Nutzung elektronischer Verfahren über einheitliche Ansprechpartner gemäß der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt, ABl. Nr. L 274 vom 20.10.2009 S. 36): nach den Verpflichtungen aus Artikel 2 der Entscheidung 2009/767/EG von allen Mitgliedstaaten zu führende Liste der ZDAs für qualifizierte Zertifikate
29. Umsatzzähler: Summenspeicher in der Registrierkasse, der die Barumsätze der Registrierkasse laufend aufsummiert
30. Verifikation: Überprüfung signierter Daten auf Integrität und Authentizität, dass die Daten nach der Signaturerstellung von der korrekten Signaturerstellungseinheit signiert und nicht verändert wurden
31. Zahlungsbeleg (Beleg): Bestätigung mit bestimmten formalen Inhalten, die in Papierform oder in elektronischer Form den wesentlichen Inhalt des Rechtsgeschäftes zwischen den Geschäftspartnern dokumentiert und bei Bezahlung übergeben bzw. elektronisch übermittelt wird
32. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird im Sinne des § 2 Z 8 SigG
33. Zertifizierungsdiensteanbieter (ZDA): Organisation, die Zertifikate ausstellt oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen bereitstellt im Sinne der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. Nr. L 13 vom 19.01.2000 S. 12.

2. Hauptstück
Technische Vorschriften

1. Abschnitt
Allgemeines

Beschreibung der Sicherheitseinrichtung

§ 4. (1) Die Sicherheitseinrichtung gemäß § 131b Abs. 2 BAO besteht aus einer Verkettung der Barumsätze mit Hilfe der elektronischen Signatur der Signaturerstellungseinheit.

(2) Die Verkettung wird durch die Einbeziehung von Elementen der zuletzt vergebenen, im Datenerfassungsprotokoll gespeicherten Signatur in die aktuell zu erstellende Signatur gebildet. Bei der Erfassung des ersten Barumsatzes tritt an die Stelle der zuletzt vergebenen Signatur die Kassenidentifikationsnummer.

2. Abschnitt
Anforderungen an die Registrierkasse

Allgemeine Anforderungen

§ 5. (1) Jede Registrierkasse muss über ein Datenerfassungsprotokoll und einen Drucker zur Erstellung oder eine Vorrichtung zur elektronischen Übermittlung von Zahlungsbelegen verfügen.

(2) Jede Registrierkasse muss über eine geeignete Schnittstelle zu einer Sicherheitseinrichtung mit einer Signaturerstellungseinheit verfügen. Mit einer Signaturerstellungseinheit können auch mehrere Registrierkassen verbunden sein.

(3) Jede Registrierkasse muss mit dem frei verfügbaren Verschlüsselungsalgorithmus AES 256 ausgestattet sein, um die für den maschinenlesbaren Code erforderlichen Verschlüsselungen durchführen zu können.

(4) Jeder Registrierkasse muss eine eindeutige Kassenidentifikationsnummer im Unternehmen zugeordnet werden.

(5) Die Registrierkasse darf keine Vorrichtungen enthalten, über die das Ansteuern der Sicherheitseinrichtung umgangen werden kann.

(6) Die Nutzung einer Registrierkasse durch mehrere Unternehmer ist nur unter der Voraussetzung zulässig, dass jeder Unternehmer ein ihm zugeordnetes Zertifikat verwenden und die Registrierkasse für jeden Unternehmer ein gesondertes Datenerfassungsprotokoll führen kann.

Inbetriebnahme der Sicherheitseinrichtung für die Registrierkasse

§ 6. (1) Die Inbetriebnahme der Sicherheitseinrichtung für die Registrierkasse besteht aus der Einrichtung des Datenerfassungsprotokolls (§ 7) und der Ablage der Kassenidentifikationsnummer als Bestandteil der zu signierenden Daten des ersten Barumsatzes mit Betrag Null (0) (Startbeleg) im Datenerfassungsprotokoll.

(2) Vor dem 1. Jänner 2017 kann die Inbetriebnahme der Sicherheitseinrichtung im Sinne Abs. 1 bereits vor der Registrierung (§ 16) vorgenommen werden. Die Registrierung muss bis zum 1. Jänner 2017 erfolgt sein.

(3) Wird eine Registrierung nach dem 31. Dezember 2016 vorgenommen, so hat die Inbetriebnahme binnen einer Woche nach Registrierung der Signaturerstellungseinheit (§ 16) zu erfolgen.

(4) Der Unternehmer hat vor Inbetriebnahme die Erstellung der Signatur (§ 9 Abs. 3) und die Verschlüsselung des Umsatzzählers (§ 9 Abs. 2 Z 5) unter Zuhilfenahme des Startbeleges zu überprüfen. Entspricht die Erstellung der Signatur bzw. die Verschlüsselung des Umsatzzählers nicht den Erfordernissen des § 9, so ist die Registrierkasse unmittelbar als Registrierkasse mit ausgefallener Signaturerstellungseinheit im Sinne des § 17 Abs. 4 zu behandeln. Das Prüfergebnis ist zu protokollieren und mit dem ausgedruckten Startbeleg gemäß § 132 BAO aufzubewahren.

Datenerfassungsprotokoll

§ 7. (1) Jede Registrierkasse hat ein Datenerfassungsprotokoll zu führen, in dem jeder einzelne Barumsatz zu erfassen und abzuspeichern ist. Für jeden Barumsatz sind zumindest die Belegdaten gemäß § 132a Abs. 3 BAO festzuhalten.

(2) Trainings- und Stornobuchungen sind wie Barumsätze zu erfassen und im Datenerfassungsprotokoll abzuspeichern.

(3) Die Daten des Datenerfassungsprotokolls sind zumindest vierteljährlich auf einem elektronischen externen Medium unveränderbar zu sichern. Diese Sicherung ist gemäß § 132 BAO aufzubewahren.

(4) Die Inhalte des maschinenlesbaren Codes (§ 10 Abs. 2) der Barumsätze sind im Datenerfassungsprotokoll der Registrierkasse gemeinsam mit den zugehörigen Barumsätzen festzuhalten.

(5) Das Datenerfassungsprotokoll einer Registrierkasse muss ab 1. Jänner 2017 jederzeit auf einen externen Datenträger im Exportformat Datenerfassungsprotokoll laut Z 3 der **Anlage** exportiert werden können.

Summenspeicher

§ 8. (1) Die in der Registrierkasse erfassten Barumsätze sind laufend aufzusummieren (Umsatzzähler). Trainingsbuchungen dürfen sich nicht auf den Umsatzzähler auswirken.

(2) Zu jedem Monatsende sind die Zwischenstände des Umsatzzählers zu ermitteln (Monatszähler) und als Barumsatz mit Betrag Null (0) und elektronischer Signatur der Signaturerstellungseinheit (Monatsbeleg) im Datenerfassungsprotokoll der Registrierkasse zu speichern.

(3) Mit Ablauf jedes Kalenderjahres ist der Monatsbeleg, der den Zählerstand zum Jahresende enthält (Jahresbeleg), auszudrucken, zu prüfen und gemäß § 132 BAO aufzubewahren. Bei der Prüfung des Jahresbeleges ist § 6 Abs. 4 sinngemäß anzuwenden.

Signaturerstellung durch die Signaturerstellungseinheit

§ 9. (1) Zur Gewährleistung des Manipulationsschutzes im Sinne des § 131b Abs. 2 BAO müssen von der Registrierkasse über eine geeignete Schnittstelle zur Signaturerstellungseinheit elektronische Signaturen angefordert und übernommen werden können. Jeder einzelne Barumsatz und Monats-, Jahres- und Schlussbeleg sowie jede Trainings- und Stornobuchung sind elektronisch zu signieren.

(2) In die Signaturerstellung sind folgende Daten einzubeziehen:

1. Kassenidentifikationsnummer
2. fortlaufende Nummer des Barumsatzes
3. Datum und Uhrzeit der Belegausstellung
4. Betrag der Barzahlung getrennt nach Steuersätzen gemäß § 10 des Umsatzsteuergesetzes 1994 – UStG 1994, BGBl. Nr. 663/1994, in der jeweils geltenden Fassung
5. mit dem Verschlüsselungsalgorithmus AES 256 laut Z 8 und Z 9 der **Anlage** verschlüsselter Stand des Umsatzzählers
6. Seriennummer des Signaturzertifikates
7. Signaturwert des vorhergehenden Barumsatzes des Datenerfassungsprotokolls (Verkettungswert laut Z 4 der **Anlage**)

(3) Die aufbereiteten Daten (Abs. 2) müssen nach dem Signaturformat laut Z 4 und Z 5 der **Anlage** durch die Signaturerstellungseinheit automatisiert elektronisch signiert werden.

(4) Die von der Signaturerstellungseinheit im Ergebnisformat der Signaturerstellung laut Z 6 der **Anlage** rückgemeldete Signatur ist auf dem zugehörigen Beleg nach den Vorgaben des § 10 als Teil des maschinenlesbaren Codes abzudrucken und im Datenerfassungsprotokoll mit den Belegdaten laut Z 11 der **Anlage** dauerhaft zu speichern (§ 7 Abs. 4).

Aufbereitung des maschinenlesbaren Codes

§ 10. (1) Nach Ermittlung jedes Signaturwertes hat die Registrierkasse für die Belegerstellung und die Speicherung im Datenerfassungsprotokoll einen maschinenlesbaren Code laut Z 12 der **Anlage** aufzubereiten.

(2) Der maschinenlesbare Code hat folgende Daten zu enthalten:

1. Kassenidentifikationsnummer
2. fortlaufende Nummer des Barumsatzes
3. Datum und Uhrzeit der Belegausstellung
4. Betrag der Barzahlung getrennt nach Steuersätzen
5. mit dem Verschlüsselungsalgorithmus AES 256 laut Z 8 und Z 9 der **Anlage** verschlüsselten Stand des Umsatzzählers
6. Seriennummer des Signaturzertifikates
7. Signaturwert des vorhergehenden Barumsatzes des Datenerfassungsprotokolls (Verkettungswert laut Z 4 der **Anlage**)

8. Signaturwert des betreffenden Barumsatzes.

(3) Trainings- und Stornobuchungen haben im maschinenlesbaren Code zusätzlich die Bezeichnung „Trainingsbuchung“ oder „Stornobuchung“ zu enthalten.

Belegerstellung

§ 11. (1) Auf dem Beleg sind neben den Belegdaten des § 132a Abs. 3 BAO folgende Daten auszuweisen:

1. Kassenidentifikationsnummer
2. Datum und Uhrzeit der Belegausstellung
3. Betrag der Barzahlung getrennt nach Steuersätzen
4. Inhalt des maschinenlesbaren Code.

(2) Sofern ein maschinenlesbarer Code nicht als QR-Code am Beleg aufgedruckt werden kann, sind die Daten nach Abs. 1 entweder

1. als ein vom Signaturwert des betreffenden Barumsatzes abhängiger Link in maschinenlesbarer Form als Barcode oder OCR zum Abruf der Daten bereitzuhalten und am Beleg auszuweisen oder
2. entsprechend der in Z 14 der **Anlage** festgelegten Codierung am Beleg auszuweisen.

(3) Belege für Trainings- und Stornobuchungen sind ausdrücklich als solche zu bezeichnen.

3. Abschnitt
Anforderungen an die Signaturerstellungseinheiten

Allgemeine Anforderungen

§ 12. Die technischen Anforderungen an die Signaturerstellungseinheit entsprechen den Anforderungen an Signaturerstellungseinheiten für qualifizierte Signaturen nach § 18 SigG in der jeweils geltenden Fassung und nach § 6 der Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008, in der jeweils geltenden Fassung. Anstelle der in § 6 Abs. 3 letzter Satz SigV 2008 vorgesehenen Prüfung kann eine Prüfung in Bezug auf die inhaltlichen Anforderungen der Registrierkassensicherheitsverordnung erfolgen, wobei die Anforderung der alleinigen Kontrolle und deren Auswirkungen auf den Betrieb auf Grund der Verkettung nicht Gegenstand dieser Prüfung sind.

Signaturschlüsselpaar und Signaturerstellung

§ 13. Bezüglich anwendbarer Signaturalgorithmen sowie Schlüssel sind die Regelungen der SigV 2008 zu den Algorithmen und Parametern für qualifizierte Signaturen aus dem Anhang zur SigV 2008, Punkte 1 bis 7 „Algorithmen und Parameter für qualifizierte elektronische Signaturen“ anzuwenden.

Verifizierbarkeit der Signaturen

§ 14. Der Signaturwert des betreffenden Barumsatzes muss an Hand des auf dem Beleg aufgebrachten maschinenlesbaren Codes verifizierbar sein. Dazu müssen insbesondere die in § 10 Abs. 2 enthaltenen Daten auf dem Beleg enthalten sein. Die Vorbearbeitung der dazu in komprimierter Form im maschinenlesbaren Code enthaltenen Daten hat gemäß Z 13 der **Anlage** zu erfolgen.

3. Hauptstück
Beschaffung und Registrierung der Signaturerstellungseinheit; Kontrolle

Beschaffung der Signaturerstellungseinheit

§ 15. (1) Unternehmer, die der Registrierkassenpflicht nach § 131b BAO unterliegen, haben die erforderliche Anzahl von Signaturerstellungseinheiten bei einem im EU-/EWR-Raum oder in der Schweiz niedergelassenen Zertifizierungsdienstanbieter, der qualifizierte Signaturzertifikate anbietet, zu erwerben. Die Kosten für die Beschaffung der Signaturerstellungseinheit trägt der Unternehmer.

(2) Der Unternehmer hat zur Erlangung des Signaturzertifikates einen der Abgabenbehörde bekannten, dem Unternehmer zugeordneten Ordnungsbegriff und als Wert des OID „Österreichische Finanzverwaltung Registrierkasseninhaber“ (Z 16 der **Anlage**) nach Maßgabe des § 5 Abs. 1 Z 8 SigG in seinem Signaturzertifikat eintragen zu lassen.

(3) Der Zertifizierungsdiensteanbieter vergibt für jede Signaturerstellungseinheit ein Signaturzertifikat, das folgende Angaben beinhaltet:

1. Typ und Wert des der Signaturerstellungseinheit zugeordneten Ordnungsbegriffs des Unternehmers,
2. Seriennummer des Signaturzertifikates und
3. Beginn und Ende der Gültigkeit des Zertifikats.

Eine Verwendung des Zertifikates über das Ende seiner Gültigkeit hinaus ist zulässig, sofern der im Zertifikat vorhandene Signaturalgorithmus laut Z 2 der **Anlage** als sicher gilt.

Registrierung der Signaturerstellungseinheit

§ 16. (1) Der Unternehmer oder sein bevollmächtigter Parteienvertreter hat über FinanzOnline den Erwerb seiner Signaturerstellungseinheiten zu melden. Dabei sind die Seriennummer des Signaturzertifikates, die Art der Signaturerstellungseinheit und die Kassenidentifikationsnummern der mit der Signaturerstellungseinheit zu verbindenden Registrierkassen bekannt zu geben. Zusätzlich hat der Unternehmer den frei wählbaren Benutzerschlüssel für die Entschlüsselung (Z 8 der **Anlage**) der mit dem Verschlüsselungsalgorithmus AES 256 verschlüsselten Daten im maschinenlesbaren Code über FinanzOnline bekannt zu geben. Ist dem Unternehmer die Meldung über FinanzOnline mangels technischer Voraussetzungen unzumutbar, hat die Meldung unter Verwendung des amtlichen Vordrucks zu erfolgen.

(2) Erst nach Prüfung, ob für jede gemeldete Signaturerstellungseinheit unter der angegebenen Seriennummer des Signaturzertifikates und dem gültigen Ordnungsbegriff des Unternehmers der ZDA in der öffentlichen Trust-List und das Signaturzertifikat im Verzeichnis des ZDA vorhanden sind, werden diese Daten an die Datenbank über Sicherheitseinrichtungen in Registrierkassen (§ 18) übergeben.

Bekanntgabe der Außerbetriebnahme der Sicherheitseinrichtung für die Registrierkasse

§ 17. (1) Der Unternehmer oder sein bevollmächtigter Parteienvertreter hat über FinanzOnline oder dem für die Erhebung der Umsatzsteuer zuständigen Finanzamt jeden nicht nur vorübergehenden Ausfall und jede Außerbetriebnahme der Sicherheitseinrichtung in der Registrierkasse bei

1. Diebstahl oder sonstigem Verlust der Signaturerstellungseinheit oder Registrierkasse,
2. Funktionsverlust der Signaturerstellungseinheit oder Registrierkasse oder
3. Außerbetriebnahme der Signaturerstellungseinheit oder Registrierkasse

ohne unnötigen Aufschub bekannt zu geben.

(2) Dazu hat der Unternehmer folgende Angaben zu machen:

1. Bezeichnung der betroffenen Komponenten der Sicherheitseinrichtung
2. Grund des Ausfalles oder der Außerbetriebnahme
3. Beginn des Ausfalles oder der Außerbetriebnahme.

(3) Alle über FinanzOnline gemeldeten, nicht nur vorübergehenden Ausfälle und Außerbetriebnahmen werden in der Datenbank über Sicherheitseinrichtungen für die Registrierkassen vermerkt.

(4) Bei jedem Ausfall der Signaturerstellungseinheit sind die Barumsätze auf einer anderen Registrierkasse zu erfassen, die über eine aufrechte Verbindung zu einer Signaturerstellungseinheit verfügt. Sollte dies nicht möglich sein, hat der Unternehmer bei der Aufbereitung und Verwendung des maschinenlesbaren Codes (§ 10) an Stelle des Signaturwertes des betreffenden Barumsatzes (§ 10 Abs. 2 Z 8) die Zeichenkette „Sicherheitseinrichtung ausgefallen“ im Ergebnis der Signaturerstellung laut Z 6 der **Anlage** zu verwenden. Der Hinweis „Sicherheitseinrichtung ausgefallen“ ist zusätzlich gut sichtbar am Beleg (§ 11) anzubringen. Nach Wiederinbetriebnahme der Signaturerstellungseinheit ist zusätzlich über die Belege, die während des jeweiligen Ausfalles mit dem Hinweis „Sicherheitseinrichtung ausgefallen“ zu versehen waren, ein signierter Sammelbeleg mit Betrag Null (0) zu erstellen und im Datenerfassungsprotokoll zu speichern.

(5) Bei jedem Ausfall einer Registrierkasse sind die Barumsätze auf anderen Registrierkassen zu erfassen. Sollte dies nicht möglich sein, sind die Barumsätze händisch zu erfassen und Zweitschriften der Belege aufzubewahren. Nach der Fehlerbehebung sind die Einzelumsätze anhand der aufbewahrten Zweitschriften nach zu erfassen und die Zweitschriften dieser Zahlungsbelege aufzubewahren (§ 132 BAO).

(6) Wenn nach dem Ausfall einer Registrierkasse ein neues Datenerfassungsprotokoll eingerichtet werden muss, ist als Signaturwert des vorhergehenden Barumsatzes (§ 10 Abs. 2 Z 7) der Signaturwert des zuletzt verfügbaren Barumsatzes bzw. der Signaturwert des Startbeleges im Datenerfassungsprotokoll zu verwenden. Das Ende des Ausfalles oder der Außerbetriebnahme ist über FinanzOnline

bekanntzugeben. Ist dem Unternehmer die Meldung über FinanzOnline mangels technischer Voraussetzungen unzumutbar, hat die Meldung unter Verwendung des amtlichen Vordrucks zu erfolgen.

(7) Ist eine Wiederinbetriebnahme der Signaturerstellungseinheit (Abs. 4) nicht mehr möglich, hat der Unternehmer eine neue Signaturerstellungseinheit zu beschaffen (§ 15), zu registrieren (§ 16) und eine neuerliche Inbetriebnahme der Sicherheitseinrichtung im Sinne der § 6 Abs. 1 bis 4 durchzuführen. Ist der zuletzt getätigte Barumsatz aus dem Datenerfassungsprotokoll feststellbar, entfällt die Inbetriebnahme der Sicherheitseinrichtung im Sinne der § 6 Abs. 1 bis 4 und gelten die Bestimmungen zum Sammelbeleg des Abs. 4. Während des Ausfalles händisch erfasste Barumsätze sind jedenfalls nachzuerfassen.

(8) Im Fall einer planmäßigen Außerbetriebnahme der Registrierkasse (Abs. 1 Z 3) hat der Unternehmer einen Schlussbeleg mit Betrag Null (0) zu erstellen. Der Schlussbeleg ist auszudrucken und gemäß § 132 BAO aufzubewahren.

Datenbank über Sicherheitseinrichtungen für die Registrierkassen

§ 18. (1) Der Bundesminister für Finanzen führt zur internen Dokumentation über die einem Unternehmer zugeordneten Signaturerstellungseinheiten eine Datenbank über Sicherheitseinrichtungen für die Registrierkassen.

(2) Diese enthält folgende Daten:

1. Name der Unternehmer
2. Ordnungsbegriff der Unternehmer
3. Art der Sicherheitseinrichtung
4. Seriennummern der Signaturzertifikate
5. Identifikationsnummern der Registrierkassen
6. Anzahl der an die Sicherheitseinrichtungen angeschlossenen Registrierkassen
7. Benutzerschlüssel für die Entschlüsselung der mit dem Verschlüsselungsalgorithmus AES 256 verschlüsselten Daten
8. Datum der Registrierung
9. Beginn und Ende von Ausfällen oder Außerbetriebnahmen der Sicherheitseinrichtungen
10. Betroffene Komponenten von Ausfällen oder Außerbetriebnahmen der Sicherheitseinrichtungen
11. Grund des Ausfalles oder der Außerbetriebnahme der Sicherheitseinrichtungen
12. Daten aus Kontrollen.

(3) Der Bundesminister für Finanzen ist datenschutzrechtlicher Auftraggeber im Sinne des § 4 Z 4 des Datenschutzgesetzes 2000 – DSG 2000, BGBl. I Nr. 165/1999, für die Datenbank über Sicherheitseinrichtungen für die Registrierkassen. Er hat dessen Einrichtung und Betrieb zu gewährleisten. Die Bundesrechenzentrum Gesellschaft mit beschränkter Haftung (BRZ GmbH) ist für die Datenbank über Sicherheitseinrichtungen für die Registrierkassen gesetzliche Dienstleisterin im Sinne der § 4 Z 5 und § 10 Abs. 2 DSG 2000.

Kontrolle und Prüfung der Datensicherheit für die Registrierkassen

§ 19. (1) Der Unternehmer hat auf Verlangen der Organe der Abgabenbehörde einen Barumsatz mit Betrag Null (0) zu erfassen und den dafür von der Registrierkasse ausgefertigten Beleg zu Kontrollzwecken zu übergeben. Bei Registrierkassen mit einer Vorrichtung zur elektronischen Übermittlung von Zahlungsbelegen ist der Beleg elektronisch zur Verfügung zu stellen.

(2) Auf Verlangen der Organe der Abgabenbehörde hat der Unternehmer das Datenerfassungsprotokoll für einen vom Organ der Abgabenbehörde vorgegebenen Zeitraum auf einen externen Datenträger zu exportieren und zu übergeben. Der Datenträger ist vom Unternehmer bereitzustellen.

4. Hauptstück
Geschlossene Gesamtsysteme

Technische und organisatorische Anforderungen

§ 20. (1) Die Manipulationssicherheit in geschlossenen Gesamtsystemen gemäß § 131b Abs. 4 BAO ist durch eine Sicherheitseinrichtung zu gewährleisten, die aus einer Verkettung der Barumsätze mit Hilfe der aufbereiteten Daten nach § 9 Abs. 2 im Signaturformat laut Z 4 und 5 der **Anlage** besteht.

(2) Für geschlossene Gesamtsysteme gilt diese Verordnung mit Ausnahme der §§ 5 Abs. 2, 12, 15 und 17 Abs. 4. Die §§ 4 Abs. 1, 6 Abs. 4, 8 Abs. 2, 9, 16 Abs. 1 und 2, 17 Abs. 1 bis 3, 17 Abs. 7 und 18 sowie die **Anlage** sind mit der Maßgabe anzuwenden, dass weder eine Signaturerstellungseinheit noch ein Signaturzertifikat erforderlich sind und, dass einer Kassenidentifikationsnummer auch mehrere Registrierkassen mit einem gemeinsamen Datenerfassungsprotokoll zugeordnet werden dürfen. Abs. 4 bleibt hiervon unberührt.

(3) Bei geschlossenen Gesamtsystemen ist anstelle der Seriennummer des Signaturzertifikates (§ 9 Abs. 2 Z 6 und § 10 Abs. 2 Z 6) der Ordnungsbegriff des Unternehmers zu verwenden. Der Ordnungsbegriff des Unternehmers muss gegebenenfalls durch geeignete Zusätze (z. B. Ziffern) ergänzt werden, um eindeutige Signaturprüfdaten zu ermöglichen. In der Datenbank gemäß § 18 sind anstelle der Seriennummer des Signaturzertifikates die Signaturprüfdaten zu erfassen. Der Ordnungsbegriff des Unternehmers sowie die Signaturprüfdaten müssen aus dem Gutachten gemäß § 21 hervorgehen.

(4) Antragsbefugt im Sinne § 131b Abs. 4 BAO sind nur Unternehmer, die ein geschlossenes Gesamtsystem als elektronisches Aufzeichnungssystem verwenden, das mit mehr als 30 Registrierkassen verbunden ist.

Sachverständige Begutachtung geschlossener Gesamtsysteme

§ 21. (1) Im Rahmen der Begutachtung geschlossener Gesamtsysteme sind insbesondere folgende Überprüfungen vorzunehmen:

1. das Vorliegen eines geschlossenen Gesamtsystems,
2. das Vorliegen der technischen und organisatorischen Voraussetzungen für die Manipulationssicherheit des geschlossenen Gesamtsystems.

(2) Im Gutachten sind insbesondere alle für den Betrieb der Sicherheitseinrichtung des geschlossenen Gesamtsystems gemäß § 20 Abs. 1 erforderlichen Softwarekomponenten anzugeben und Prüfberichte für diese Komponenten anzuschließen. Die Softwarekomponenten sind mit der mathematischen Hashfunktion Secure Hash Algorithm (SHA-256) mit einem Startwert, der Null (0000 0000 0000 0000) entspricht, für eine spätere Verifikation zu signieren. Aus den Prüfberichten muss nachvollziehbar hervorgehen, wie die einzelnen Komponenten geprüft wurden. Die Manipulationssicherheit und sicherheitstechnische Gleichwertigkeit mit einer Signaturerstellungseinheit sind zu bestätigen. Dem Gutachten sind ein Organigramm mit allen Hard- und Softwarekomponenten und Datenspeicher des geschlossenen Gesamtsystems sowie ein Überblick über die automatisch ablaufenden Verarbeitungsprozesse anzuschließen.

(3) Das Gutachten hat darüber hinaus Angaben darüber zu enthalten, welche organisatorischen Maßnahmen zur laufenden Überprüfung der Manipulationssicherheit vorgesehen sind. Dabei ist insbesondere darzulegen, welche betrieblichen Funktionen in der Organisationsstruktur des Unternehmens mit welchen Zugriffs- und Eingriffsrechten, die Veränderungen am Gesamtsystem herbeiführen können, ausgestattet sind, dass die Zugriffe protokolliert werden und durch welche Maßnahmen die Manipulationssicherheit des geschlossenen Systems laufend kontrolliert wird. Zudem ist darzulegen, wie im Falle eines Ausfalles des Systems die Einzelaufzeichnungspflicht, die Sicherung der Kassenumsätze und die Belegerteilung rechtskonform gewährleistet werden (Ausfallplan).

(4) Im Gutachten ist zu beurteilen, ob das geschlossene Gesamtsystem den Anforderungen des § 20 Abs. 1 und 2 entspricht und ob die technischen und organisatorischen Sicherungsmaßnahmen des Abs. 2 und 3 erfüllt werden.

(5) Verwenden mehrere Unternehmer, die durch ein vertikales Vertriebsbindungssystem oder durch ein Waren- oder Dienstleistungsfranchising wirtschaftlich verbunden oder die Teil eines Konzerns im Sinne des § 244 UGB sind, gemeinsam ein geschlossenes Gesamtsystem mit insgesamt mehr als 30 Registrierkassen und beurteilt das Gutachten die Manipulationssicherheit dieses Systems für diese Unternehmer, so kann dieses Gutachten von mehreren Unternehmern ihrem Antrag auf Erlassung eines Feststellungsbescheides zugrunde gelegt werden. Für alle Verwender des geschlossenen Gesamtsystems ist Abs. 3 sinngemäß anzuwenden. Lieferungen und sonstige Leistungen, die außerhalb des geschlossenen Gesamtsystems im betreffenden Betrieb erfolgen, sind von der Wirksamkeit des Feststellungsbescheides nicht umfasst.

(6) Mit der Erstellung solcher Gutachten dürfen nur gerichtlich beeidete Sachverständige beauftragt werden. Die Vollständigkeit der sicherheitsrelevanten Überprüfungen im Gutachten ist durch eine Bestätigungsstelle gemäß § 19 SigG zu bescheinigen.

(7) Die Kosten für die Erstellung der Gutachten trägt der Unternehmer.

Feststellungsbescheid

§ 22. (1) Im Feststellungsbescheid der Abgabenbehörde gemäß § 131b Abs. 4 BAO sind die dem Gutachten zugrunde liegenden Softwarekomponenten der Sicherheitseinrichtung gemäß § 20 Abs. 1 mit Hilfe der Softwaresignatur (§ 21 Abs. 2) zu identifizieren.

(2) Mit Feststellungsbescheid bestätigte geschlossene Gesamtsysteme werden in der Datenbank über Sicherheitseinrichtungen (§ 18) registriert.

(3) Kann die Manipulationssicherheit des geschlossenen Gesamtsystems durch das Finanzamt nicht bestätigt werden, ist dem Unternehmer eine einmalige Nachfrist von einem Monat für die Nachholung der die Manipulationssicherheit gewährleistenden Maßnahmen unter Beibringung eines diese Maßnahmen bestätigenden Gutachtens einzuräumen. Das Finanzamt hat diesfalls unter Zugrundelegung des vorliegenden Sachverhaltes zu entscheiden.

(4) Wird die Manipulationssicherheit des geschlossenen Gesamtsystems mit rechtskräftigem Bescheid des Finanzamtes nicht bestätigt, hat der Unternehmer innerhalb von drei Monaten ab Eintritt der Rechtskraft die Manipulationssicherheit unter Verwendung einer Signaturerstellungseinheit (§ 131b Abs. 2 BAO) herbeizuführen, andernfalls mit Ablauf dieser Frist die Verpflichtungen nach § 131b Abs. 2 BAO als nicht erfüllt gelten.

Änderung der tatsächlichen Verhältnisse

§ 23. (1) Änderungen des mit Bescheid bestätigten geschlossenen Gesamtsystems sind vor ihrer Durchführung dem für die Erhebung der Umsatzsteuer zuständigen Finanzamt unter Vorlage eines neuen Gutachtens (§ 21) zu melden, wenn eine umfassende Umstellung des geschlossenen Gesamtsystems (z. B. Technologiewechsel) oder eine Änderung der Softwarekomponenten der Sicherheitseinrichtung gemäß § 20 Abs. 1 geplant ist oder die Antragsvoraussetzungen im Sinne der §§ 20 Abs. 4 oder 21 Abs. 5 nicht mehr vorliegen. Über solche Änderungen des geschlossenen Gesamtsystems ist mit Feststellungsbescheid abzusprechen.

(2) Die Meldung dieser beabsichtigten Änderungen hat über FinanzOnline zu erfolgen.

(3) Werden dem Unternehmer nach Erlassung des Feststellungsbescheides Tatsachen bekannt, die Zweifel an der Manipulationssicherheit des geschlossenen Gesamtsystems hervorrufen, hat er diese ohne unnötigen Aufschub über FinanzOnline zu melden.

Kontrolle der Identität der Softwarekomponente laut § 21 Abs. 2

§ 24. Die Organe der Abgabenbehörde sind berechtigt, die Übereinstimmung der im Gutachten ausgewiesenen Softwarekomponente laut § 21 Abs. 2 mit der im geschlossenen Gesamtsystem im Einsatz befindlichen Softwarekomponente zu überprüfen. Dazu muss das geschlossene Gesamtsystem eine Eingabemöglichkeit eines Startwertes zur lokalen Abfrage der Softwaresignaturwertes zur Verfügung stellen sowie den Softwaresignaturwert der Komponente berechnen und anzeigen.

5. Hauptstück
Schlussbestimmungen

Inkrafttreten

§ 25. (1) Die Verordnung tritt mit 1. Jänner 2017 in Kraft.

(2) Abweichend von Abs. 1 treten § 1 bis 3, § 5 Abs. 1, § 7 Abs. 1, § 17 Abs. 5 und § 19 Abs. 2 mit 1. Jänner 2016 in Kraft.

(3) Abweichend von Abs. 1 und 2 treten die § 6, § 15, § 16, § 18, § 21 und § 22 mit 1. Juli 2016 in Kraft.

(4) Diese Verordnung wurde gemäß der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft, ABl. Nr. L 204 vom 21.07.1998 S. 37, zuletzt geändert durch die Verordnung (EU) Nr. 1025/2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG und zur Aufhebung des Beschlusses 87/95/EWG und des Beschlusses Nr. 1673/2006/EG, ABl. Nr. L 316 vom 14.11.2012 S. 12, bei der Europäischen Kommission unter der Notifikationsnummer **XXX** notifiziert.

Anlage

Detailspezifikationen

1. Standards

Die folgenden Standards werden im Dokument unter den folgenden Abkürzungen verwendet:

- **BASE32, BASE64, BASE64-URL**: Network Working Group: Request for Comments: 4648 – The Base16, Base32, and Base64 Data Encodings
- **CRT (ICM) Mode**: NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation
- **DER**: ITU-T X.690: Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- **JSON**: Internet Engineering Task Force (IETF): Request for Comments: 7159 – The JavaScript Object Notation (JSON) Data Interchange Format
- **JSON Web Signature**: Internet Engineering Task Force (IETF): Request for Comments: 7515 – JSON Web Signature (JWS)
- **SHA-256**: FIPS PUB 180-4 – Secure Hash Standard (SHS)
- **UTF-8**: Network Working Group: Request for Comments: 3629 – UTF-8, a transformation format of ISO 10646

2. Registrierkassenalgorithmuskennzeichen

Dieses Kennzeichen definiert die verwendeten Algorithmen und den Zertifizierungsdiensteanbieter (ZDA). Sobald ein in den Registrierkassenalgorithmuskennzeichen verwendeter Algorithmus nicht mehr im Anhang der SigV 2008 genannt wird und daher als unsicher gilt, muss ein neues Registrierkassenalgorithmuskennzeichen mit sicheren Algorithmen definiert werden und darf dieses auch bei bestehenden Registrierkassen nicht mehr eingesetzt werden. Das Kennzeichen entspricht einer Zeichenkette, die wie folgt aufgebaut ist:

RN-CM:

- „R“: Fixes Präfix
- „N“: Index für die verwendete Algorithmen-Suite startend mit 1
- „-„: Fixes Trennzeichen
- „C“: Länderkennung des ZDAs
- „M“: Index für verwendeten ZDA innerhalb der gegeben Länderkennung nach ISO 3166-1 startend mit 1

Die folgenden Kennzeichen sind definiert:

R1-CM:

- **ZDA**: CM wird als Platzhalter für die zur Verfügung stehenden ZDAs gesehen. Wenn ein geschlossenes System laut § 20 zum Einsatz kommt, muss AT0 als ZDA angebenden werden.
- **Signatur/Hashalgorithmus**: Für die Erstellung der Belegsignatur laut Z 4, Z 5 dieser Anlage. Es wird der ES256 Algorithmus nach dem JWA (JSON Web Algorithmus) Standard verwendet.
- **Hashalgorithmus für die Verkettung der Belege und Berechnung des IVs, Anzahl N der extrahierten Bytes**: Es wird SHA-256 verwendet. Die Anzahl der extrahierten und damit in den nächsten Beleg übernommen Bytes entspricht 8 (N=8).
- Kompressionsalgorithmus für kompakte Darstellung des Belegs: Dieser Algorithmus entspricht den folgenden Verfahren:
  - Aufbereitung der zu signierenden Daten: Laut Z 4, Z 5 dieser Anlage.
  - Aufbereitung des maschinenlesbaren Codes: Laut Z 12, Z 13 dieser Anlage.

3. Exportformat Datenerfassungsprotokoll

Das Exportformat des Datenerfassungsprotokolls entspricht folgender JSON-Datenstruktur:

- **Belege-Gruppe**: Der Wert dieses Feldes ist ein JSON-Array. Die Anzahl der Elemente dieses JSON-Arrays entspricht der Anzahl der Signaturzertifikate die für die Signierung der zu

exportierenden Belege verwendet wurden. Ein Element dieser Liste entspricht dabei der folgenden JSON-Datenstruktur:

- **Signaturzertifikat**: Der Wert dieses Feldes ist der BASE64-kodierte Wert des im DER-Format kodierten Signaturzertifikats.
- **Zertifizierungsstellen**: Der Wert dieses Feldes ist ein JSON-Array. Die Elemente des JSON-Arrays entsprechen der Kette aller Zertifizierungsstellen, die für die Ausstellung des Signaturzertifikats verwendet wurden. Der Wert eines Elements entspricht dem BASE64-kodierten Wert des im DER-Format kodierten Zertifikats.
- **Belege-kompakt**: Der Wert dieses Feldes ist ein JSON-Array. Die Elemente entsprechen den signierten Belegen, die in der kompakten Darstellung des JSON Web Signature Formats dargestellt werden (laut Z 6 dieser Anlage). Die Reihenfolge der Belege stimmt mit der Ablagereihenfolge im DEP überein. Es muss garantiert sein, dass die Verkettung der Signatur des Beleges an Stelle x mit dem Beleg an Stelle x+1 gegeben ist (siehe Feld „Sig-Voriger-Beleg“ laut Z 4 dieser Anlage).

4. Klartextdaten für das Signaturformat für Signierung durch Signaturerstellungseinheit

Die Signaturerstellung erfolgt nach dem JSON Web Signature (JWS) Standard. Ein Beleg ist in einer JSON-Datenstruktur abgebildet die mindestens die in § 9 Abs. 2 Z 1 bis Z 7 genannten Daten enthält. Je nach Bedarf kann das Belegformat beliebig um weitere JSON-Daten erweitert werden. Für die Transformationsverfahren die für die Signaturerstellung und die Erstellung des maschinenlesbaren Codes notwendig sind, sind aber nur die in § 9 Abs. 2 Z 1 bis Z 7 genannten Belegdaten relevant, die wie folgt in einer JSON-Datenstruktur repräsentiert werden:

- **Kassen-ID**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 1 angegebenen Wert, JSON-Format *string* UTF-8 kodiert.
- **Belegnummer**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 2 angegebenen Wert, JSON-Format *string UTF-8 kodiert*.
- **Beleg-Datum-Uhrzeit:** Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 3 angegebenen Wert, JSON-Format *string* UTF-8 kodiert. Das Datum und die Uhrzeit wird im ISO 8601 Format ohne der Angabe der Zeitzone abgespeichert („JJJJ-MM-TT’T’hh:mm:ss“, z. B. 2015-07-21T14:23:34). Es wird immer von österreichischer Lokalzeit (CET/MEZ) ausgegangen.
- **Betrag-Satz-Normal**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 4 angegebenen Wert, JSON-Format *number* mit 2 Kommastellen. Ist kein Betrag mit dieser MWST vorhanden so wird 0,00 eingetragen.
- **Betrag-Satz-Ermaessigt-1**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 4 angegebenen Wert, JSON-Format *number* mit 2 Kommastellen. Ist kein Betrag mit dieser MWST vorhanden, so wird 0,00 eingetragen.
- **Betrag-Satz-Ermaessigt-2**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 4 angegebenen Wert, JSON-Format *number* mit 2 Kommastellen. Ist kein Betrag mit dieser MWST vorhanden, so wird 0,00 eingetragen.
- **Betrag-Satz-Null**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 4 angegebenen Wert, JSON-Format *number* mit 2 Kommastellen. Ist kein Betrag ohne MWST vorhanden, so wird 0,00 eingetragen.
- **Betrag-Satz-Besonders**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 4 angegebenen Wert, JSON-Format *number* mit 2 Kommastellen. Ist kein Betrag mit dieser MWST vorhanden, so wird 0,00 eingetragen.
- **Stand-Umsatz-Zaehler-AES256-ICM**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 5 angegebenen Wert, JSON-Format *string*. BASE64-kodierter Wert des verschlüsselten Gesamtumsatzes (laut Z 8, Z 9 dieser Anlage).
- **Zertifikat-Seriennummer**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 6 angegebenen Wert, JSON-Format *string*. UTF-8 kodiert.
- **Sig-Voriger-Beleg**: Der Wert dieses Feldes entspricht dem in § 9 Abs. 2 Z 7 angegebenen Wert. JSON-Format *string*. Dieser Wert wird über die im Registrierkassenalgorithmuskennzeichen definierte kryptographische Hash-Funktion berechnet. Als Input dieser Hash-Funktion wird das Ergebnis der Signaturerstellung gemäß Z 6 verwendet. Für die Erfassung des ersten Barumsatzes wird der Wert des Felds „Kassen-ID“ als Input dieser Hash-Funktion verwendet. Aus dem Ergebnis der Hash-Funktion werden startend mit Byte 0, N Bytes extrahiert und BASE-64-kodiert. Die

Anzahl der zu extrahierenden Bytes (N) wird ebenfalls über das Registrierkassenalgorithmuskennzeichen definiert. Durch den Einsatz von Zugriffsteuerungsmethoden muss garantiert sein, dass auch bei der parallelen Abarbeitung der Belegerstellung die Verkettung über die Signaturwerte korrekt abgebildet wird.

5. Signaturformat für Signierung durch Signaturerstellungseinheit

Die zu signierenden Daten eines Belegs sind in § 9 Abs. 2 Z 1 bis Z 7 genannt. Um eine kompakte Darstellung der zu signierenden Daten zu ermöglichen, werden diese Daten in eine komprimierte Darstellung übergeführt. Die Transformation erfolgt nach der in § 9 Abs. 2 Z 1 bis Z 7 definierten Reihenfolge. Die einzelnen Felder werden UTF-8 kodiert und mit dem Zeichen „_“ zusammengeführt und in einer Zeichenkette gespeichert. Unter Verwendung der oben genannten Bezeichner und der Notation Wert(JSON-Feld) für das Extrahieren des Wertes aus der JSON-Datenstruktur des Belegs ergibt sich folgende Darstellung.

„Wert(Kassen-ID)_Wert(Belegnummer)_Wert(Beleg-Datum-Uhrzeit)_
Wert(Betrag-Satz-Normal)_Wert(Betrag-Satz-Ermaessigt-1)_Wert(Betrag-Satz-Ermaessigt-2)_Wert(Betrag-Satz-Null)_Wert(Betrag-Satz-Besonders)_
Wert(Stand-Umsatz-Zaehler-AES256-ICM)_Wert(Zertifikat-Seriennummer)_
Wert(Sig-Voriger-Beleg)“

Die resultierende Zeichenkette wird anschließend mit dem Präfix „_RKA_“ ergänzt. „RKA“ stellt einen Platzhalter für das Registrierkassenalgorithmuskennzeichen dar. Diese Kennzeichen werden in einer Liste (laut Z 2 dieser Anlage) zur Verfügung gestellt und identifizieren folgende Komponenten:

- Signatur/Hashalgorithmus für die Erstellung der Belegsignatur
- Zertifizierungsdienstanbieter (ZDA) der das Signaturzertifikat ausgestellt hat
- Hashalgorithmus für die Verkettung der Belege, sowie die Anzahl der Bytes N, die aus dem berechneten Hash-Wert extrahiert werden.
- Kompressionsalgorithmus der für die Erstellung des maschinenlesbaren Codes verwendet wurde.

Die resultierende Zeichenkette entspricht *dem Signaturformat für Signierung durch Signaturerstellungseinheit* und wird über den JSON Web Signature Standard mit dem angegeben Signaturzertifikat und dem gewählten Hashalgorithmus signiert. Im JWS-Format werden diese Daten als „JWS Payload“ bezeichnet.

6. Ergebnis der Signaturerstellung

Das Ergebnis der JWS-Signatur ist die nach dem JWS-Standard definierte kompakte Repräsentation. Diese Zeichenkette besteht dabei aus drei BASE64-URL-kodierten Elementen, die durch das Zeichen „.“ voneinander getrennt sind. Die drei Elemente entsprechen den Elementen in der gegebenen Reihenfolge

1. den Metainformationen über den verwendeten Hash bzw. Signaturalgorithmus
2. den signierten Daten (JWS Payload) und
3. dem berechneten Signaturwert.

Kann aufgrund des Ausfalls der Signaturerstellungseinheit keine digitale Signatur erstellt werden, wird statt dem berechneten Signaturwert (drittes Element der kompakten JWS Repräsentation) die UTF-8 kodierte Zeichenkette „Sicherheitseinrichtung ausgefallen“ BASE64-URL-kodiert eingetragen.

7. Anmerkung zum Wechsel des Signaturzertifikats

Bei einem Wechsel des Signaturzertifikats muss garantiert sein, dass weitere Belege nicht mehr mit dem vor dem Wechsel verwendeten Zertifikat signiert werden dürfen.

8. Verschlüsselungsmethode Umsatzzähler

Für die Verschlüsselung des Umsatzzählers wird AES-256 im ICM (CTR) Mode (Integer Counter Mode) ohne Padding verwendet. Der Initialisierungsvektor enthält einen laut Z 9 dieser Anlage berechneten Hash-Wert in dessen Berechnung die Belegnummer und die Kassenidentifikationsnummer eingeht. Der Umsatzzähler im Klartext wird in einer geeigneten Darstellung übergeben, die später auch ohne Padding-Informationen rekonstruiert werden kann.

Für die Bekanntgabe des AES-Schlüssels über FinanzOnline müssen die Binärdaten des AES-Schlüssel BASE64-kodiert werden.

9. Verschlüsselung

Für die Verschlüsselung des kodierten Umsatzzählers wird wie folgt vorgegangen:

- **Algorithmen**: Es wird der AES-256 im ICM (CTR) Mode verwendet. Für die Verschlüsselung wird kein „Padding“ verwendet.
- **Initialisierungsvektor**: Der Initialisierungsvektor (IV) für den Verschlüsselungsalgorithmus ist ein Byte-Array mit der Länge 16. Für die Berechnung des IVs werden die UTF-8 kodierte Kassenidentifikationsnummer (Wert des Feldes „Kassen-ID“ laut Z 4 dieser Anlage) und die UTF-8-kodierte Belegnummer (Wert des Feldes „Belegnummer“ laut Z 4 dieser Anlage) in dieser Reihenfolge zusammengefügt. Das Ergebnis ist eine UTF-8 kodierte Zeichenkette die als Eingabewert für die im Registrierkassenalgorithmuskennzeichen definierten Hash-Funktion verwendet wird. Das Ergebnis der Hash-Funktion ist der Hash-Wert abgebildet in einem Byte-Array. Die Bytes 0-15 werden daraus extrahiert und als IV verwendet.
  Anmerkung: Es muss garantiert sein, dass für jede Verschlüsselungsoperation, die mit einem gegebenen AES-Schlüssel durchgeführt wird, niemals der gleiche IV verwendet wird.
- **Kodierung des Umsatzwertes**: Die Block-Größe von AES-256 entspricht einem Byte-Array der Länge 16. Für die Kodierung des Umsatzzählers im Klartext wird dabei ein Byte-Array der Länge 16 erstellt. Jedes Element des Byte-Arrays wird mit 0 initialisiert. Der Umsatzzähler mit der Byte-Anzahl „N“ wird startend mit Byte 0 im BIG-ENDIAN Format als Zweier-Komplement Darstellung („signed“) gespeichert. „N“ entspricht der Anzahl der Bytes die für die Kodierung des Umsatzzählers notwendig sind. Es müssen mindestens 5 Byte lange Umsatzzähler verwendet werden.

Das Resultat der Verschlüsselung ist ein Byte-Array der Länge 16. Startend mit Byte 0 werden N Bytes aus dem Array extrahiert, BASE64-kodiert und im Beleg abgelegt.

10. Entschlüsselung

Bei der Entschlüsselung wird wie folgt vorgegangen:

- **Algorithmen**: siehe Z 8, Z 9 dieser Anlage
- **Initialisierungsvektor**: siehe Z 9 dieser Anlage
- **Aufbereitung des verschlüsselten Umsatzzählers**: Es wird ein Byte-Array der Länge 16 erstellt. Jedes Element des Byte-Arrays wird mit 0 initialisiert. Startend mit Byte 0 wird das BASE64-dekodierte Byte-Array des verschlüsselten Umsatzzählers in dem erstellen 16-Byte langem Array gespeichert.

Die aufbereiteten Daten werden mit dem AES-Algorithmus und dem AES-256 Schlüssel entschlüsselt. Das Resultat der Entschlüsselung ist ein Byte-Array der Länge 16. Startend mit Byte 0 werden N Bytes aus dem Array extrahiert und entsprechen dem entschlüsselten Umsatzzähler. Das Format entspricht dem bei der Verschlüsselung genannten „Kodierung des Umsatzwertes“.

11. Übergabeformat für Datenerfassungsprotokoll

Belege, die an das Datenerfassungsprotokoll übergeben werden, entsprechen einer JSON-Datenstruktur die mindestens folgende Werte/Daten enthalten müssen. Der Hersteller kann hier optional weitere Daten hinzufügen. Pro Beleg müssen mindestens folgende in einer JSON-Datenstruktur gespeicherten Daten verwenden werden:

- **JWS-Kompakt**: Der Wert dieses Feldes entspricht der kompakten Darstellung einer Signatur nach dem JWS-Standard (laut Z 5 dieser Anlage), JSON-Format *string*.
- **Signaturzertifikat (optional)**: Der Wert dieses Feldes ist der BASE64-kodierte Wert des im DER-Format kodierten Signaturzertifikats, JSON-Format *string*.
- **Zertifizierungsstellen (optional)**: Der Wert dieses Feldes ist ein JSON-Array. Die Elemente des JSON-Arrays entsprechen der Kette aller Zertifizierungsstellen, die für die Ausstellung des Signaturzertifikats verwendet wurden. Der Wert eines Elements entspricht dem BASE64-kodierten Wert des im DER-Format kodierten Zertifikats.

Die Werte für das Signaturzertifikat und die Zertifizierungsstellen bleiben für einen längeren Zeitraum konstant. Sie müssen daher nicht für jeden Beleg übergeben werden, sondern können auch auf einem anderen Weg dem DEP zur Verfügung gestellt werden. Es muss nur garantiert sein, dass

1. das DEP für jeden Beleg die Zuordnung zum passenden Signaturzertifikat und zu den Zertifizierungsstellen des Signaturzertifikats herstellen kann und
2. alle Zertifikate im DEP zur Verfügung stehen um den Export der signierten Belegdaten zu ermöglichen.

Für die Übergabe der Belegdaten an das DEP muss durch den Einsatz von Zugriffsteuerungsmethoden garantiert sein, dass auch bei der parallelen Abarbeitung der Belegerstellung die Verkettung über die Signaturwerte korrekt abgebildet wird (laut Z 4 dieser Anlage).

12. Details der Vorbearbeitung der im maschinenlesbaren Code enthaltenen Daten für Verifizierung des Signaturwertes eines Barumsatzes

Die für den maschinenlesbaren Code aufbereiteten Daten werden durch eine Zeichenkette repräsentiert, die folgende Elemente enthält:

- **Signierte Belegdaten**: Diese Daten entsprechen der UTF-8 kodierten Zeichenkette des Signaturformats das der Signaturerstellungseinheit übergeben wurde (laut Z 5 dieser Anlage). Die Zeichenkette kann aus dem JWS-Payload-Feld der kompakten JWS-Darstellung (Ergebnis der Signaturerstellung) extrahiert werden.
- **Signaturwert**: Der Signaturwert in BASE64-Kodierung wird aus der kompakten JWS-Darstellung (Ergebnis der Signaturerstellung) extrahiert. Es muss darauf geachtet werden, dass der Signaturwert in der kompakten Darstellung des JWS-Standards BASE64-URL-kodiert ist, um die Verwendung in Web-Anwendungen zu vereinfachen. Diese Darstellung ist aber für die QR-Code Darstellung nicht geeignet, da sie auch das Zeichen „_“ enthält, das für die Trennung der Elemente der zu signierenden Daten verwendet wird. Der BASE64-URL-kodierte Signaturwert muss daher dekodiert werden und im Standard BASE64-Format kodiert werden.

Diese zwei Elemente werden in der genannten Reihenfolge mit dem Zeichen „_“ zusammengesetzt, UTF-8 kodiert und in einem maschinenlesbaren Code aufbereitet.

13. Prüfung des maschinenlesbaren Codes

Die Prüfung der Signatur, die in einem maschinenlesbaren Code aufbewahrt wird, wird wie folgt durchgeführt:

1. **Lesen des maschinenlesbaren Codes**: Die gelesene UTF8-kodierte Zeichenkette enthält die „Signierten Belegdaten“ und den „Signaturwert“.
2. **Extraktion der „Signierten Belegdaten“ und des „Signaturwerts“**: Die „Signierten Belegdaten“ und der „Signaturwert“ werden aus der UTF8-kodierten Zeichenkette über das Trennzeichen „_“ extrahiert. Der BASE64-kodierte Signaturwert wird BASE64-dekodiert.
3. **Aufbereitung der kompakten Darstellung anhand des JWS-Signatur-Standards**: Die kompakte Darstellung (laut Z 5 dieser Anlage) wird wie folgt aus dem maschinenlesbaren Code rekonstruiert. Die einzelnen Elemente werden dabei durch das Zeichen „.“ zusammengeführt.
   a) **JWS Protected Header:** Der Signatur/Hashalgorithmus des JWS Protected Headers kann über das Registrierkassenalgorithmuskennzeichen rekonstruiert werden. Der JWS Protected Header wird UTF-8-kodiert in der Zeichenkette an der 1. Stelle BASE64-URL-kodiert abgespeichert.
   b) **JWS Payload**: Die JWS Payload entspricht den zuvor extrahierten Belegdaten und wird in der Zeichenkette an der 2. Stelle BASE64-URL-kodiert abgespeichert.
   c) **JWS Signature**: Dieser Wert entspricht dem vorher extrahierten Signaturwert und wird in der Zeichenkette an der 3. Stelle BASE64-URL-kodiert abgespeichert.
4. **Prüfen der Signatur**: Die aufbereitete kompakte Darstellung anhand des JWS-Standards wird mit dem entsprechenden Signaturzertifikat geprüft.

14. Erstellung der OCR-fähigen Zeichenkette

Für die OCR-fähige Zeichenkette wird aufgrund der Schwierigkeit, alle möglichen Zeichen einer BASE64 Zeichenfolge automatisiert und bei realistischen Lichtbedingungen und Kameraeigenschaften sicher zu erkennen, statt der BASE64-Darstellung der folgenden Elemente laut Z 4, Z 12 dieser Anlage die BASE32-Darstellung der Binärdaten gewählt.

- Signaturwert
- Sig-Voriger-Beleg
- Stand-Umsatz-Zaehler-AES256-ICM

Die resultierende Zeichenkette wird im OCR-A Font auf den Beleg gedruckt.

15. Prüfung der OCR-fähigen Zeichenkette

Für die Prüfung der OCR-fähigen Zeichenkette müssen die BASE32-kodierten Elemente auf die BASE64-Kodierung umkodiert werden. Der anschließende Prüfvorgang ist äquivalent zum Prüfen des maschinenlesbaren Codes.

16. OID

Der OID-Bezeichner für die Verwendung im Signaturzertifikat entspricht 1.2.40.0.10.1.11.1 „Österreichische Finanzverwaltung Registrierkasseninhaber“.

Die OID wird aus dem Teilbaum 1.2.40.0.10.1.11 „Teilbaum Bundesministerium für Finanzen“ vergeben.