Entwurf

Erläuterungen

I. Allgemeiner Teil

Hauptgesichtspunkte des Entwurfes zu einer Registrierkassensicherheitsverordnung:

Mit der Änderung der Bundesabgabenordnung – BAO, BGBl. I Nr. XX/2015 wurde der Grundstein für die verpflichtende Erfassung jedes Barumsatzes mittels elektronischer Registrierkasse mit technischer Sicherheitseinrichtung gegen Manipulation sowie für die Belegerteilung und -entgegennahme gelegt. Durch Anforderungen an Registrierkassen und Signaturerstellungseinheiten soll die Manipulationssicherheit und deren Überprüfbarkeit sichergestellt werden.

II. Besonderer Teil

Inhalt der Verordnung

Zu §§ 4 Abs. 2, 6 Abs. 1 und 4:

Mit gesetzeskonformer Inbetriebnahme der Sicherheitseinrichtung in der Registrierkasse (einschließlich Überprüfung des Startbeleges gemäß § 6 Abs. 4) gilt die gesetzliche Vermutung des § 163 Abs. 1 BAO für die Ordnungsmäßigkeit der Losungsermittlung der Barumsätze der jeweiligen Registrierkasse.

Zu § 5:

Als Registrierkasse kommen auch Server in Frage, die mit Eingabestationen zur Erfassung der Barumsätze verbunden sind, über eine Signaturerstellungseinheit (z.B.: HSM) elektronische Signaturen bereitstellen, den Ausdruck eines Beleges auslösen und die Aufzeichnung von Barumsätzen bewerkstelligen können. Unter Vorrichtung zur elektronischen Übermittlung von Zahlungsbelegen ist eine Softwarekomponente zu verstehen, die beispielsweise bei Abschluss eines Online-Geschäftes mit einem in Österreich steuerpflichtigen Unternehmen eine Zahlungsbestätigung mit elektronischer Signatur zum Download bereitstellt.

Als geeignete Schnittstelle zwischen Registrierkasse und Signaturerstellungseinheit gelten beispielsweise ein USB-Anschluss und ein Steckplatz in der Systemplatine der Registrierkasse, über die Daten gesendet und empfangen (ausgetauscht) werden können oder ein dazu geeigneter Netzwerkanschluss.

Insofern eine Signaturerstellungseinheit von mehreren Registrierkassen direkt (z. B.: HSM) oder indirekt (z. B.: „Masterkasse“) angesteuert wird und die erforderlichen Signaturen liefern kann, kann eine Signaturerstellungseinheit für mehrere Registrierkassen verwendet werden. In diesen Fällen ist über FinanzOnline im Zuge der Registrierung der Signaturerstellungseinheit für jede Registrierkasse u.a. eine pro Unternehmer eindeutige Kassenidentifikationsnummer zu melden. Das Verbot für Vorrichtungen zur Umgehung der Ansteuerung der Sicherheitseinrichtung gilt nicht für die Erfassung von Geschäftsvorfällen, die keine Barumsätze darstellen (z.B.: Lieferscheine, Banküberweisungen und -einzug, durchlaufende Posten).

Zu § 6:

Eine erfolgreiche Inbetriebnahme der Sicherheitseinrichtung einer Registrierkasse liegt mit Vorliegen eines erfolgreich geprüften Belegs des ersten Barumsatzes der Registrierkasse (Startbeleg) vor. Davor müssen die Signaturerstellungseinheit dieser Registrierkasse über FinanzOnline gemeldet, das

Datenerfassungsprotokoll in der Registrierkasse eingerichtet und die Kassenidentifikationsnummer als Verkettungswert für die Signaturerstellung des Startbeleges im Datenerfassungsprotokoll abgelegt sein. Der Startbeleg kann durch Eingabe eines Barumsatzes mit Betrag 0 ausgelöst oder programmgesteuert angelegt werden. Der Startbeleg hat als fortlaufende Nummer „eins (1)“, als Tag der Belegausstellung das Datum der Inbetriebnahme der Sicherheitseinrichtung (§ 6), als Menge „Null (0)“, als handelsübliche Bezeichnung „Startbeleg“ und als Betrag der Barzahlung „Null (0)“ zu enthalten. Der Startbeleg ist als Grundaufzeichnung zumindest sieben Jahre aufzubewahren (§ 132 BAO). Bis zum 31. Dezember 2016 kann eine Sicherheitseinrichtung auch ohne Prüfung des Startbeleges in Betrieb genommen werden, die Prüfung des Startbeleges ist dann bis zum 31. Dezember 2016 nach Registrierung der Signaturerstellungseinheit nachzuholen. Für die Prüfung des Startbeleges wird das BMF eine Prüfsoftware (z.B.: Mobile App, Web-Sevice) zur Verfügung stellen, die den am Beleg ausgegebenen maschinenlesbaren Code auslesen und die darin enthaltenen Daten (Seriennummer des Zertifikates, Signaturwert, Verschlüsselung des Umsatzzählers, etc.) mit den in der Datenbank über Sicherheitseinrichtungen für Registrierkassen gespeicherten Daten auf Plausibilität überprüfen kann.

Zu § 7:

Das Datenerfassungsprotokoll (Kassenjournal) ist als Grundaufzeichnung zumindest sieben Jahre aufzubewahren (§ 132 BAO). Als Datenerfassungsprotokoll gilt auch das in einem Kassensystem geführte Journal. Die laut RKSV im Datenerfassungsprotokoll zu speichernden Daten stellen keine personenbezogenen Daten dar. Die Sicherung des Datenerfassungsprotokolls soll gewährleisten, dass bei Ausfall der Registrierkasse (§ 17) die Barumsätze zumindest bis zum vorangehenden Quartal rekonstruierbar sind und unterliegt der abgabenrechtlichen Aufbewahrungspflicht. In der Sicherung hat der Monatsbeleg des letzten Monats des Quartals, der die Unveränderbarkeit des gesamten Datenerfassungsprotokolls im Wege der Signatur sichert, als letzter Beleg enthalten zu sein. Als externes Medium können beispielsweise externe Festplatten oder USB-Sticks verwendet werden.

Als Trainingsbuchung im Sinne dieser Verordnung gilt nur eine im Rahmen eines fiktiven Geschäftsvorfalles durchgeführte Buchung in einer Registrierkasse.

Zu §§ 7 Abs. 4 und 19 Abs. 2:

Die Software einer Registrierkasse muss die Eingabe von Datumsangaben für die zeitliche Eingrenzung der Barumsätze ermöglichen und die Ausgabe der entsprechenden Barumsätze auslösen können.

Zu § 8:

Monats- bzw. Jahresbeleg können durch Eingabe eines Barumsatzes mit Betrag 0 ausgelöst oder programmgesteuert angelegt werden. Der Monats- bzw. Jahresbeleg hat als Menge „Null (0)“, als handelsübliche Bezeichnung „Monatsbeleg“ bzw. „Jahresbeleg“ und als Betrag der Barzahlung „Null (0)“ zu enthalten. Der Jahresbeleg ist als Grundaufzeichnung zumindest sieben Jahre aufzubewahren (§ 132 BAO). Bei über Mitternacht hinausgehenden Betriebszeiten ist der Monats- bzw. Jahresbeleg spätestens vor dem ersten Beleg des neuen Monats bzw. Jahres zu erstellen.

Zu § 9, 10 und 11:

Die bei der Signaturerstellung, Aufbereitung des maschinenlesbaren Codes und Belegerstellung zu berücksichtigenden Format-, Komprimierungs- und Verschlüsselungsvorgaben sind in der Anlage zur Verordnung beschrieben.

Datum und Uhrzeit sind nach dem ISO 8601_Format aufzubereiten (JJJJ-MM-TTThh:mm:ss).

Beispiel: 2017-06-14T23:34:30.

Alternativ zum kompakten QR-Code sind als maschinenlesbarer Code auch ein Link zum Abruf der Daten als Barcode oder eine OCR fähige Zeichenkette möglich.

Zu § 12, 13, 14:

Als Signaturerstellungseinheiten sind grundsätzlich für qualifizierte Signaturen zulässige Geräte geeignet. Für HSMs können einige der Anforderungen an derartige Geräte auch durch technisch-organisatorische Maßnahmen erfüllt werden. Dies betrifft insbesondere auch jene Teile der sicheren Signaturerstellungseinheit (§ 3 Z 23), die in Software umgesetzt wird. Sofern im Zusammenhang mit dieser Verordnung davon Gebrauch gemacht wird, besteht die zusätzliche Erleichterung im Wegfall der alleinigen Kontrolle, da diese aufgrund der Verkettung nicht für die Sicherheit des Gesamtsystems von Bedeutung ist.

Zu § 15:

Für die Sicherheitseinrichtungen in Registrierkassen wird im Rahmen des für Österreich reservierten Verwaltungsbereiches („Teilbaum Bundesministerium für Finanzen“) der OID „Österreichische Finanzverwaltung Registrierkasseninhaber“ (OID-Bezeichner 1.2.40.0.10.1.11.1) festgelegt. Damit sind Zertifikate für Registrierkassen erkennbar und durch ZDAs ausstellbar.

Signaturen und Zertifikate sowie deren Gültigkeit und Widerruf müssen eindeutig erkennbar sein. Daher sind nur solche Zertifikate zu verwenden, zu denen der ZDA in der öffentlichen Trust-List und das Signturzertifikat im Verzeichnis des ZDA vorhanden sind. Durch diese Bestimmung werden ZDAs ausgeschlossen, deren Sorgfaltspflicht nicht im Wege der jeweiligen nationalen Aufsicht sichergestellt wäre. Die Zertifizierungsdiensteanbieter können unter https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml abgerufen werden.

Eine Liste der möglichen Zertifizierungsdiensteanbieter wird als zusätzliches Service auf der Homepage des BMF zur Verfügung gestellt werden.

Zu § 16:

Anträge und Meldepflichten des Unternehmers können auch durch seinen bevollmächtigten Parteienvertreter (z.B. Rechtsanwalt, Steuerberater, Wirtschaftstreuhänder) wahrgenommen werden.

Der vom Unternehmer frei wählbare Benutzerschlüssel stellt die Geheimhaltung der betroffenen Daten gegenüber Dritten sicher und ermöglicht die Entschlüsselung der im maschinenlesbaren Code verschlüsselt dargestellten Daten.

Zu § 17:

Von einem nur vorübergehenden Ausfall der Sicherheitseinrichtung in der Registrierkasse ist jedenfalls bei Stromausfall, planmäßigen Wartungsarbeiten und anderen Ereignissen auszugehen, die zu einer Funktionsunfähigkeit der Sicherheitseinrichtung führen, die nicht länger als 48 Stunden andauert.

Eine Außerbetriebnahme liegt beispielsweise vor bei Einstellung des Betriebes oder planmäßiger Reduzierung der Anzahl der im Betrieb verwendeten Signaturerstellungseinheiten oder Registrierkassen. Als Komponenten der Sicherheitseinrichtung in der Registrierkasse im Sinne dieser Bestimmung kommen die Registrierkasse selbst (Hard- oder Software) und die Signaturerstellungseinheit in Betracht.

Für den Sammelbeleg sind die Belegdaten gemäß § 132a Abs. 3 BAO maßgeblich, wobei sämtliche Belege, die während des jeweiligen Ausfalles mit dem Hinweis „Sicherheitseinrichtung ausgefallen“ versehen wurden, in den Sammelbeleg aufzunehmen und dabei je Beleg, als Menge die fortlaufende Nummer des jeweiligen Barumsatzes, als handelsübliche Bezeichnung der maschinenlesbare Code des jeweiligen Barumsatzes und als Betrag der Barzahlung „Null (0)“ einzutragen sind. Der Sammelbeleg ist als Grundaufzeichnung zumindest sieben Jahre aufzubewahren (§ 132 BAO).

Der Schlussbeleg kann durch Eingabe eines Barumsatzes mit Betrag 0 ausgelöst oder programmgesteuert angelegt werden. Der Schlussbeleg hat als Menge „Null (0)“, als handelsübliche Bezeichnung „Schlussbeleg“ und als Betrag der Barzahlung „Null (0)“ zu enthalten. Der Schlussbeleg ist als Grundaufzeichnung zumindest sieben Jahre aufzubewahren (§ 132 BAO). Die Meldepflichten des Unternehmers können auch durch seinen bevollmächtigten Parteienvertreter (Rechtsanwalt, Steuerberater, Wirtschaftstreuhänder) wahrgenommen werden.

Zu § 18:

Die Datenbank über Sicherheitseinrichtungen in Registrierkassen dient der Information der Abgabenbehörden und enthält die zur Registrierung (§§ 16, 22), Änderung der tatsächlichen Verhältnisse (§§ 17, 23) und Kontrolle (§§ 19, 24) erfassten Daten zu Kontrollzwecken.

Zu § 20:

Die Sicherheitseinrichtung bei geschlossenen Gesamtsystemen besteht so wie bei den Registrierkassen ohne geschlossenen Gesamtsystem aus der Verkettung der einzelnen Barumsätze. An Stelle der Signatur der Signaturerstellungseinheit wird dazu eine auf Basis der Signaturprüfdaten, der Belegdaten und der Zeichenkette „Sicherheitseinrichtung ausgefallen“ ermittelte Signatur herangezogen.

Der Abs. 2 ermöglicht eine administrative Erleichterung bei der Registrierung der Kassen in einem geschlossenen Gesamtsystem, damit ein Unternehmer der bspw. in einer Filiale 10 Kassen betreibt nicht 10 Kassenidentifikationsnummern in FON eingeben muss, sondern nur eine.

Der letzte Satz in Abs. 2 stellt klar, dass trotz dieser administrativen Erleichterung bei der Registrierung jedenfalls mehr als 30 Registrierkassen mit eigenem Datenerfassungsprotokoll für die Beantragung der Zertifizierung eines geschlossenen Gesamtsystems erforderlich sind.

Die für ein geschlossenes Gesamtsystem u.a. erforderliche hohe Anzahl von Registrierkassen wurde mit „mehr als 30 Registrierkassen“ festgelegt, die im geschlossenen Gesamtsystem betrieben werden müssen.

Zu §§ 21, 23 und 24:

Das Gutachten muss die einzelnen, für den Betrieb der Sicherheitseinrichtung erforderlichen Softwarekomponenten so darstellen, dass sie einzeln überprüft werden können bzw. überprüft werden kann, ob nachträglich eine Veränderung der einzelnen Softwarekomponente erfolgte. Über diese Softwarekomponenten ist ein Hashwert zu bilden. Als Eingabewert für den Hashwert kann wahlweise der ausführbare Code oder der Sourcecode der Softwarekomponenten herangezogen werden.

Das Vorgehen bei der Begutachtung muss erkennbar sein (Prüfmethode). Die Einzelergebnisse der Begutachtung müssen aufgelistet werden (Bestätigungsvermerk pro gesetzlicher Anforderung).

Neben der Prüfung der technischen Voraussetzungen für die Manipulationssicherheit des geschlossenen Gesamtsystems sind auch alle organisatorischen Maßnahmen und Verantwortlichkeiten, die die Manipulationssicherheit sicher stellen, zu prüfen und im Gutachten darzulegen.

Zu § 22:

Mit positivem Feststellungsbescheid gilt die gesetzliche Vermutung des § 163 Abs. 1 BAO für die Ordnungsmäßigkeit der Losungsermittlung der Barumsätze im jeweiligen geschlossenen Gesamtsystem.

Zu § 23:

Nur Änderungen, die einen anderen, als den mit Feststellungsbescheid beurteilten Sachverhalt begründen, führen zur zwingenden Einholung eines weiteren Sachverständigengutachtens und in der Folge eines neuerlichen Feststellungsbescheides. Für bloße Software-Updates ist eine neue Begutachtung, bzw. ein neuer Feststellungsbescheid nicht erforderlich, sondern nur bei einem gänzlichen Technologiewechsel und bei jeder Änderung der Softwarekomponenten der Sicherheitseinrichtung.

Zu § 25:

Die Regelungen über die technische Sicherheitseinrichtung sind ab 1. Jänner 2017 verpflichtend einzuhalten.

Unbeschadet der bisher geltenden Bestimmungen laut Kassenrichtlinie 2012 des Bundesministers für Finanzen treten die Bestimmungen über die Anforderungen an die Registrierkasse (Abs. 2) mit 1. Jänner 2016 in Kraft.

Bereits ab 1. Juli 2016 soll es aufgrund der technischen Umsetzung durch das Bundesministerium für Finanzen möglich sein, die technische Sicherheitseinrichtung registrieren zu lassen. Durch die Vorlaufzeit von sechs Monaten für die Registrierung und die Regelung des § 6 Abs. 2 wird für die Unternehmer die Möglichkeit geschaffen, rechtzeitig vor dem 1. Jänner 2017 den Betrieb der Registrierkassen mit Sicherheitseinrichtung vorzubereiten.