Sachverständige Begutachtung geschlossener Gesamtsysteme lt. § 21 RKSV

Muster für Befund und Gutachten

Das vorliegende Dokument enthält, **Ergebnisse aus Arbeitsgesprächen** zwischen Vertretern des Landesverbandes der Gerichtssachverständigen, des BMF und von A-SIT.

Es handelt sich um eine **unverbindliche Arbeitsunterlage**, die den aktuellen Kenntnisstand der Autoren wiedergibt.

Die Interpretation der Kriterien, die sich für die Gutachten der SV aus den gesetzlichen Vorgaben ergeben liegt ausschließlich im Verantwortungsbereich des erstellenden SV der auch die Gliederung und den Aufbau der Gutachten bestimmt. Die dem Befund und Gutachten zu Grunde liegende Prüftiefe und damit der Aufwand zur Erstellung sind weiters auch durch den Auftrag an den SV bestimmt und vom erstellenden SV festzulegen.

Wien, 26.1.2016

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. JUDMANN Dipl.-Ing. Dr. Georg REINISCH

Hauptverband der allgemein beeideten und gerichtlich zertifizierten Sachverständigen Österreichs
Landesverband Wien, Niederösterreich und Burgenland
Doblhoffgasse 3/5, A-1010 Wien, Telefon: 01/ 405 45 46, 01/ 406 32 67, Fax: 01/ 406 11 56
E-Mail: office@gerichts-sv.at, Web: wien.gerichts-sv.at

Muster für Befund und Gutachten

1 Auftraggeber und Auftrag

2 Beurteilungsgegenstand

- Beschreibung und Abgrenzung des beurteilten Systems
- Definition der inhaltliche Beurteilung:
  Gesamtsystem
  Allgemeine Sicherheit
  Signaturerstellungseinheit

3 Befund

3.1 Geschlossenes Gesamtsystem

Befund zur Dokumentation von (Funktion und Schnittstellen):

- Warenwirtschaftssystem
- Finanzbuchhaltung
- Kassensysteme

Grundlagen:
Systemeigenschaften lt. § 3 Abs. 10:

Elektronisches Aufzeichnungssystem, in welchem Warenwirtschafts-, Buchhaltungs- und Kassensysteme lückenlos miteinander verbunden sind und das mit mehr als 30 Registrierkassen verbunden ist.

Siehe Erläuterungen lt. Punkt 1 und 4 der Beilage.

3.2 Registrierkasse

Befund zur Dokumentation der Erfüllung der Anforderungen an die Registrierkasse(n) wie nachstehend dargestellt:

Zu erhebende Inhalte (Dokumentation) ergeben sich aus den Anforderungen lt. § 20 Abs. 2, soweit sie auch für geschlossene Gesamtsysteme relevant sind

Dokumentation zu:

- Allgemeine Anforderungen (§ 5 – ohne Abs. 2)
- Inbetriebnahme der Sicherheitseinrichtung (§ 6)
- Datenerfassungsprotokoll (§ 7)
- Summenspeicher (§ 8)
- Signaturerstellung (§ 9 Abs. 2)

Grundlagen:
Definition laut § 3 Abs. 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.

3.3 Organisatorische Voraussetzungen: geschlossene Gesamtsysteme

Befund zur Dokumentation der Maßnahmen zur Erfüllung der Anforderungen an geschlossene Gesamtsysteme laut § 21 Abs. 3 wie nachstehend dargestellt:

Zur Beurteilung erforderliche Dokumentationen:

- Vorlage von betrieblichen Sicherheitskonzepten
- Prozessgliederung und Verantwortungszuordnung
- Logging von Systemänderungen (weitere Abfragen)
- Incident-Management
- Ausfallsplan
- Reviewzyklen des Sicherheitskonzeptes

3.4 Technische Voraussetzungen: geschlossene Gesamtsysteme

Befund zur Dokumentation und Implementierung der technischen Umsetzung der Anforderungen an geschlossene Gesamtsysteme laut § 21 Abs. 2 (Signaturerstellung), wie nachstehend dargestellt:

3.4.1 Dokumentationen

1. Organigramm aller Hard- und Softwarekomponenten und Datenspeicher des geschlossenen Gesamtsystems
2. Nennung der Softwareelemente für Signaturerstellung (mit Erstellungsdatum, Versionsnummer, etc.)
3. Verfahrensdokumentation (Prozessbeschreibungen) sämtlicher Funktionalitäten des Kassensystems im Zusammenhang mit den von diesem System generierten bzw. verarbeiteten Daten
4. Vorlage allfälliger Prüfberichte für Softwarekomponenten

3.4.2 Befund zur Identifikation der Softwarekomponenten für die Signaturerstellung

Verifikation durch Einsichtnahme (entsprechend § 21 Abs. 2, 2. Satz)

Vorgabe:
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.

3.4.3 Befund zur Sicherheit der Signaturerstellung

Befund zur Art der Signaturerstellung und allenfalls vorliegender Bescheinigungen.

Bestätigung der Verwendung der Komponenten für die ordnungsgemäße Signaturerstellung.

Falls keine bescheinigte Signaturerstellungseinheit verwendet wird:

Befund zu den Grundlagen der *Manipulationssicherheit und sicherheitstechnischen Gleichwertigkeit mit einer Signaturerstellungseinheit*:

- Sicherheit der Signaturerstellungsdaten (Schlüssel zur Verkettung der Barumsätze mit Hilfe der aufbereiteten Daten nach § 9 Abs. 2 im Signaturformat laut Z 4 und 5 der Anlage) bei deren Generierung, Verwahrung und Anwendung, d.h. insbesondere:
    - Nachweis, dass die Signaturerstellungsdaten mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen (detaillierte und nachvollziehbare Darstellung der Methoden und Algorithmen für die Schlüsselerzeugung und des ver-

wendeten Zufalls sowie eine genaue Darstellung des qualitätsvollen Zufalls und der Sicherung gegen alterungsbedingte Veränderungen).
Beurteilung der Verwendung der Zufallszahlen nach dem Stand der Technik.

- Nachweis, dass die Signaturerstellungsdaten mit hinreichender Sicherheit nicht ableitbar sind (detaillierte Darstellung der Schlüsselorganisation).
  Ausgeschlossene Errechenbarkeit der Signaturschlüssel aus bekannten Elementen (Signaturen, Prüfschlüssel etc.).

- Nachweis, dass die unbefugte Verwendung von Signaturerstellungsdaten verlässlich verhindert wird.
  Beurteilung des Zugangskonzepts zu den Servern und Kassen, die Schlüsselmaterial speichern (Auslesen durch Dritte).

- Nachweis, dass die Geheimhaltung der Signaturerstellungsdaten sichergestellt ist.
  Beurteilung des Konzeptes der Aufbewahrung und Verteilung der Signaturerstellungsdaten und des Ausmaßes der Aufzeichnungen und Kontrollen der Informationsbeschaffungsmöglichkeiten über Schlüsselmaterial beschaffen können.

- Unveränderbarkeit der zu signierenden Daten (§ 9 Abs. 2) im Zuge des Verarbeitungsprozesses

Bei Verwendung von Softwarekomponenten, deren Eigenschaften bei A-SIT als bekannt angesehen werden, ist die Einhaltung der vorstehenden Anforderungen nicht zu befunden.

Erläuterungen zu den Kriterien: Siehe Beilage Punkt 2.

3.4.4 Befund zur Verwendung durch mehrere Unternehmer

Zum Vorliegen der Verwendung eines geschlossenen Gesamtsystems bei der Nutzung eines Systems durch mehrere Unternehmer ist eine Beurteilung pro Unternehmen zu erstellen.

Dabei kann für jene Teile, für die bereits Befund und Gutachten vorliegen, von diesem ausgegangen werden. Es sind nur Dokumentationen der Abweichungen zu befunden. Pro verbundenem Unternehmer sind die organisatorischen Voraussetzungen sinngemäß zu dokumentieren und zu beurteilen.

4. Gutachten

4.1 Geschlossenes Gesamtsystem

Die Beurteilung der Erfüllung der Kriterien basiert auf der Unternehmensdokumentation. Erläuterungen zu den Kriterien: Siehe Beilage Punkt 1 und 4.

Ergebnis: Liegt vor / nicht vor

4.2 Anforderungen an die Registrierkassen

Korrekte und vollständige Funktion der Registrierkasse, des Datenerfassungsprotokolls und des Belegdrucks. Die Erfüllung der Anforderungen an die Registrierkassenfunktion wird ebenfalls auf Basis der Dokumentation des Unternehmens beurteilt. Einzelne Funktionen wie z.B. die Bon-Erstellung und die Richtigkeit des Datenerfassungsprotokolls sind durch Tests zu verifizieren.

Beurteilung zu den Kriterien:

1. *Allgemeine Anforderungen laut § 5*
   - *(1) DEP, Drucker oder elektr. Übermittlung von Zahlungsbelegen*
   - *~~(2) Schnittstelle zu Sicherheitseinrichtung~~[1]*
   - *(3) Ausstattung mit AES 256*
   - *(4) Kassenidentifikationsnummer*
   - *(5) Keine Umgehungsvorrichtung*
   - *(6) Mehrere Unternehmer: jeweils zugeordnetes Zertifikat und DEP*

2. *Inbetriebnahme Sicherheitseinrichtung laut § 6*
   - *(1) Einrichtung DEP + Ablage Kassenidentifikationsnummer als Bestandteil Startbeleg (1. Barumsatz Null) im DEP*
   - *(2) Vor Inbetriebnahme: Prüfung der Erstellung der Signatur und der Verschlüsselung des Umsatzzählers unter Zuhilfenahme des Startbeleges.*

3. *Datenerfassungsprotokoll laut § 7*
   - *(1) Jeder einzelne Barumsatz zu erfassen u abzuspeichern*
   - *(2) Trainings- und Stornobuchungen*
   - *(3) DEP vierteljährlich auf externen Medium sichern*
   - *(4) Inhalte des maschinenlesbaren Codes mit Barumsätzen im DEP festhalten*
   - *(5) DEP jederzeit exportierbar*

[1] Laut § 20 Abs. 2 ist für geschlossene Gesamtsysteme der § 5 Abs. 2 nicht anzuwenden. Der Vollständigkeit halber sind in dieser Auflistung allerdings die Stichworte zu allen Absätzen des Paragraphen 5 aufgelistet. Der nicht anzuwendende Absatz 2 ist zur Kenntlichmachung durchgestrichen.

4. *Summenspeicher laut § 8*
   - *(1) Umsatzzähler: laufende Aufsummierung der Barumsätze*
   - *(2) Monatszähler: Zu Monatsende Zwischenstand des Umsatzzählers mit Betrag Null*
   - *(3) Jahresende: Monatsbeleg zum Jahresende ausdrucken und Prüfung nach § 6 Abs. 4 (Prüfung der Erstellung der Signatur und Verschlüsselung unter Zuhilfenahme des Startbeleges)*

5. *Signaturdatensatz laut § 9 Abs. 2*
   - *(1) Kassenidentifikationsnummer*
   - *(2) fortlaufende Nummer des Barumsatzes*
   - *(3) Datum und Uhrzeit der Belegausstellung*
   - *(4) Betrag der Barzahlung getrennt nach Steuersätzen*
   - *(5) AES 256 verschlüsselter Stand des Umsatzzählers*
   - *(6) Geändert lt. § 20 Abs. 2: Ordnungsbegriff des Unternehmers*
   - *(7) Signaturwert des vorhergehenden Barumsatzes des Datenerfassungsprotokolls (Verkettungswert)*

6. *Signaturerstellung und Schnittstellen für Signaturdaten*
   - *(1) für geschlossenes Gesamtsysteme >30 DEP auf USB-Sticks exportierbar*
   - *(2) Sicherheitseinrichtungen laut Kapitel 3.4 (z.B. A-SIT Merkblatt)*

7. *Maschinenlesbarer Code laut § 10*
   - *(1) Kassenidentifikationsnummer*
   - *(2) fortlaufende Nummer des Barumsatzes*
   - *(3) Datum und Uhrzeit der Belegausstellung*
   - *(4) Betrag der Barzahlung getrennt nach Steuersätzen*
   - *(5) AES 256 verschlüsselter Stand des Umsatzzählers*
   - *(8) Geändert lt. § 20 Abs. 2: Ordnungsbegriff des Unternehmers*
   - *(6) Signaturwert des vorhergehenden Barumsatzes des Datenerfassungsprotokolls (Verkettungswert)*
   - *(7) Signaturwert des betreffenden Barumsatzes*

8. *Belegerstellung laut § 11*
   - *(1) Belegdaten gemäß § 132a Abs. 3 BAO*
   - *(2) Kassenidentifikationsnummer*
   - *(3) Datum und Uhrzeit der Belegausstellung*
   - *(4) Betrag der Barzahlung getrennt nach Steuersätzen*
   - *(5) Inhalt des maschinenlesbaren Codes*
   - *(6) oder, wenn nicht als QR-Code druckbar: Link zu Barcode oder OCR*

Erläuterungen zu den Kriterien: Siehe Beilage Punkt 5.

Ergebnis: Erfüllt / nicht erfüllt
Erstellen einer Defizitliste

4.3 Vorliegen der organisatorischen Voraussetzungen

Beurteilung, ob zu den nachfolgenden Kriterien nachvollziehbare Beschreibungen (betriebliche Dokumentation) vorhanden sind, die die Erfüllung der Anforderungen lt. § 21 Abs. 3 bestätigen:

(1) Betriebliche Funktionen mit Zugriffs- und Eingriffsrechten zur Veränderung des Gesamtsystems und für lfd. Kontrollen, Systemausfälle, Missbrauchsbekämpfung, etc.
(2) Beschreibung und Ausmaß der Verantwortlichkeiten der einzelnen betrieblichen Funktionen
(3) Protokollierung der Zugriffe und Eingriffe
(4) Frequenz der Kontrollen und Vorgehen bei Handlungsbedarf
(5) Maßnahmen zur Sicherstellung der Einzelaufzeichnung und Belegerteilung bei Ausfall des Sicherheitssystems (Ausfallplan)
(6) Weitere Maßnahmen zur laufenden Überprüfung der Manipulationssicherheit

Erläuterungen zu den Kriterien: siehe Beilage Punkt 6

Ergebnis: Erfüllt / nicht erfüllt
Erstellen einer Defizitliste

4.4 Vorliegen der technischen Voraussetzungen

Beurteilung: Die Kriterien (ersichtlich aus dem Befundteil 3.4.3) sind:

(1) *Manipulationssicherheit und sicherheitstechnische Gleichwertigkeit mit einer Signaturerstellungseinheit*

(2) *Nachweis, dass die Signaturerstellungsdaten mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen*

(3) *Nachweis, dass die Signaturerstellungsdaten mit hinreichender Sicherheit nicht ableitbar sind*

(4) *Nachweis, dass die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar gemacht werden*

(5) *Nachweis, dass die Geheimhaltung der Signaturerstellungsdaten sichergestellt ist*

Die Beurteilung ist im Falle der Verwendung einer bescheinigten Signaturerstellungseinheit und im Fall der Verwendung von Software, deren Eigenschaften bei A-SIT bekannt sind und als sicher gelten, vereinfacht und als gegeben anzusehen.

Kriterien laut § 21 Abs. 2

Erläuterungen zu den Kriterien: Siehe Beilage Punkt 7.

Ergebnis: Erfüllt / nicht erfüllt
Erstellen einer Defizitliste

4.5 Vorliegen der Nutzung durch mehrere Unternehmer

Beurteilung zu den Kriterien pro angeschlossenem Unternehmen soweit die Anlage von einem allenfalls vorhandenen Gutachten für das zentrale System und die Ausprägung der Nutzung abweicht:

- Verbund in einem (übergeordneten) geschlossenen Gesamtsystem
- Vorhandensein eines Feststellungsbescheides des (übergeordneten) geschlossenen Gesamtsystems
- Vorliegen der organisatorischen Voraussetzungen (siehe Kapitel 4.3)

Erläuterungen zu den Kriterien: Siehe Beilage Punkt 8.

Ergebnis: Erfüllt / nicht erfüllt
Erstellen einer Defizitliste

Beilage

Erläuterungen zu den Kriterien

1. Allgemeines

Ein Feststellungsbescheid ist auf Antrag des Unternehmens vom zuständigen Finanzamt zu erlassen. Lt. § 131b Abs 4 BAO:

… (4) Das für die Erhebung der Umsatzsteuer zuständige Finanzamt hat auf Antrag des Unternehmers mit Feststellungsbescheid die Manipulationssicherheit eines geschlossenen Gesamtsystems, das im Unternehmen als elektronisches Aufzeichnungssystem verwendet wird, zu bestätigen, wenn eine solche Sicherheit auch ohne Verwendung einer in Abs. 2 geforderten Signaturerstellungseinheit besteht.
Antragsbefugt sind nur Unternehmer, die ein solches geschlossenes Gesamtsystem verwenden und eine hohe Anzahl von Registrierkassen im Inland in Verwendung haben. Dem Antrag ist ein Gutachten eines gerichtlich beeideten Sachverständigen, in dem das Vorliegen der technischen und organisatorischen Voraussetzungen für die Manipulationssicherheit des geschlossenen Gesamtsystems bescheinigt wird, anzuschließen…

Aus dem Gutachten zum geschlossenen Gesamtsystem sind nur die Aspekte der Sicherheitseinrichtung zu bescheinigen. Diese sind jedoch mit den übrigen Elementen der Umsetzung der RKSV inhaltlich zusammenhängend. Damit wird es in aller Regel sinnvoll und notwendig sein, die übrigen Aspekte, die nicht bescheinigungswürdig sind bei der Bescheinigung vorliegend zu haben, um den Einfluss dieser Elemente auf die Sicherheit des Gesamtsystems in Bezug auf die Vollständigkeit bescheinigen zu können.

Die Lückenlosigkeit des geschlossenen Gesamtsystems, die Anforderungen an die Registrierkassenfunktion und die organisatorischen Voraussetzungen sind auf Basis einer Dokumentenprüfung zu beurteilen. Stichprobenartig sind Verifikationen zur Registrierkassenfunktion durchzuführen.

Für die Beurteilung der technischen Voraussetzung für die Sicherheit hat zusätzlich zur Beurteilung an Hand der Dokumentation eine Überprüfung der Implementierung zu erfolgen.

2. Zu 3.4.1 Dokumentationen

Beschreibung, welche Daten in das Kassensystem eingegeben werden (z.B. die Daten des Geschäftsfalles über Eingabestationen), welche Daten vom System generiert werden (wie z.B. die Bonnummer oder das Belegdatum) und was mit diesen Daten im chronologischen Ablauf passiert (wie z.B. Weiterleitung an die Sicherheitseinrichtung, Speicherung in der Datenbank, oder auch

Erstellung von Berichten (wie z.B. Kassenjournale) usw.). Konkreter Datenfluss an den Schnittstellen zwischen Warenwirtschaft, Kassensystem und Buchhaltung.

3. Zu 3.4.3 Befund zur Sicherheit der Signaturerstellung

Prüfumfang und Prüftiefe:

Die RKSV sieht keine konkreten Prüfstandards für die sicherheitsrelevanten Überprüfungen vor. Es ist jedoch entsprechend § 21 Abs. 2, 4. Satz „*die Manipulationssicherheit und sicherheitstechnische Gleichwertigkeit mit einer Signaturerstellungseinheit*“ zu bestätigen, daher sind hinsichtlich des Prüfumfangs und der Prüftiefe gleichwertige Kriterien heranzuziehen, wie sie bei der Bescheinigung von sicheren Signaturerstellungseinheiten für qualifizierte Signaturen herangezogen werden.

Da jedoch keine Evaluierung bzw. Zertifizierung nach Common Criteria (ISO/IEC 15408) erforderlich ist, müssen die Dokumentation und der Prüfprozess nicht den formalen Anforderungen dieses Standards genügen, sondern es ist ausreichend, wenn aus dem Prüfgutachten hervorgeht, dass die o.g. Bereiche im Zuge der Überprüfung berücksichtigt wurden.

Die funktionalen Sicherheitsanforderungen können sowohl durch technische als auch durch organisatorische Sicherheitsmaßnahmen umgesetzt werden. Aus den o.g. Sicherheitsvorgaben (Security Target) und dem Prüfgutachten muss hervorgehen, welche Anforderungen durch technische, durch organisatorische Maßnahmen bzw. welche durch das Zusammenspiel von technischen und organisatorischen Maßnahmen umgesetzt werden. Insbesondere ist auch eine klare Definition der Vorgangsweise erforderlich, wenn durch organisatorische Maßnahmen (z.B. Protokollierung) ein Verdacht auf Kompromittierung der Manipulationssicherheit entsteht.

4. Zu 4.1 Geschlossenes Gesamtsystem

Die freiwillige Verwendung einer Signaturerstellungseinheit zur Signierung der Barumsätze wirkt sich nicht schädlich auf die Anerkennung eines geschlossenen Gesamtsystems aus.

Die „lückenlose“ Verkettung der Softwaremodule für die Aufgabenbereiche Warenwirtschaft und Buchhaltung ist nur insofern zu prüfen, als solche Module im Einsatz sind und die auszutauschenden Daten (lückenlos) für die signierten Kassendaten von Relevanz sind. Z.B. Daten, die im Kassensystem entstehen, dürfen nicht manuell in das Buchhaltungssystem eingegeben werden müssen (siehe Kapitel 3.4.1 Dokumentationen).

Bei Verwendung des geschlossenen Gesamtsystems ist hinsichtlich der Schnittstelle zur Buchhaltung auch dann von einer lückenlosen Verkettung auszugehen, wenn während der Übertragung der Daten keine unentdeckte Manipulation der Daten stattfinden kann.

Wenn der Betriebsgegenstand des Unternehmens keine Warenwirtschaft erfordert, kann auch eine lückenlose Verbindung eines Buchhaltungs- und Kassensystems für die Anerkennung eines geschlossenen Gesamtsystems ausreichen.

Im Gutachten ist bzgl. der Lückenlosigkeit beispielsweise der Buchhaltung der „technische Kanal" zu beurteilen und nicht die Richtigkeit der Zuordnung von Datensätzen zu Buchhaltungskonten u dgl. Es sind die Dokumentationen zu den Schnittstellen zum Buchhalts-, Warenwirtschafts- und Kassensystem zu betrachten und zu beurteilen, in wieweit diese manipulationssicher ausgeführt sind (z.B. durch signierte Datensätze oder Dateien).

5. Zu 4.2 Anforderungen an die Registrierkassen

§ 20 Abs. 2 besagt, „*Für **geschlossene Gesamtsysteme** gilt diese Verordnung mit Ausnahme der §§ 5 Abs. 2, 12, 15 und 17 Abs. 4*".

In den allgemeinen Anforderungen an die Registrierkasse (§ 5) entfällt u.a. die Forderung, dass *jede Registrierkasse über eine geeignete Schnittstelle zu einer Sicherheitseinrichtung mit einer Signaturerstellungseinheit* verfügen muss.

Weiters entfallen die technischen Anforderungen an die Signaturerstellungseinheiten (§ 12), sowie die Vorgabe des Bezugs der Signaturerstellungseinheiten bei einem Zertifizierungsdienstanbieter (§ 15) und zum Ausfall der Signaturerstellungseinheiten (§ 17 Abs. 4).

Hintergrund für diese Einschränkungen ist die Tatsache, dass in einem geschlossenen Gesamtsystem eben die Signaturerstellungseinheiten (i.A. Chipkarte oder HSM) durch eine Software-Komponente ersetzt wird. Die Anforderung an diese Software-Komponenten sind als „*Erforderliche Nachweise gem. SigG/SigV*" von A-SIT festgehalten.

Der § 20 Abs. 2 besagt weiters, dass, wie erwähnt, für geschlossene Gesamtsysteme weder eine Signaturerstellungseinheit noch ein Signaturzertifikat erforderlich sind und damit 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, in der die Signaturerstellungseinheit und das Signaturzertifikat referenziert werden, mit der Maßnahme anzuwenden sind, dass eben die Signaturerstellungseinheit und das Signaturzertifikat durch eine Software-Komponente ersetzt werden.

Somit bleiben die Anforderungen an die Registrierkassen in den §§ 5 (ohne Abs. 2), 6, 7, 8 und §§ 9 Abs. 2, 10 und 11 auch für geschlossene Gesamtsysteme aufrecht und müssen zur Beurteilung herangezogen werden.

§ 20 Abs. 2 ermöglicht eine administrative Erleichterung bei der Registrierung der Kassen in einem geschlossenen Gesamtsystem, damit ein Unternehmer der z.B. in einer Filiale 10 Kassen betreibt nicht 10 Kassenidentifikationsnummern in FON (Finanzonline) 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.

Daraus leitet sich auch die Anforderung ab, dass für ein geschlossenes Gesamtsystem mehr als 30 Datenerfassungsprotokolle bei einer Prüfung zu übergeben sind.

Durch Stichproben ist die korrekte Verkettung der Einträge im DEP nachzuweisen für:

- den Normalbetrieb
- bei Ausfall der Sicherheitseinrichtung – sofern eine verteilte Implementierung vorliegt und dieser Aspekt damit relevant wird
- Bei Ausfall einer Registrierkasse, insbesondere bei Datenbanklösungen

Zu erheben ist weiters auch die Exportierbarkeit und Prüfbarkeit des DEP, da bei der i.d.R. sehr großen Anzahl der Registrierkassen und der komplexeren Systemarchitektur in vielen Fällen der Export des Datenerfassungsprotokolls technisch nach einer spezifischen Art gelöst sein wird. Zur Sicherstellung der praktischen Prüfbarkeit sind in diesem Aspekt, abhängig von der Umsetzung, Auflagen beim Feststellungsbescheid zu erwarten.

Bei Zusammenführung mehrerer Kassen in einem DEP sind die Dokumentationen zur Systematik der Kassenidentifikation und die Sicherstellung der lückenlosen Verkettung zu prüfen.

Die Prüfbarkeit der Signatur und der Entschlüsselbarkeit der akkumulierten Umsatzsumme ist mittels Startbeleg nachzuvollziehen.

Zur Prüfung der Korrektheit des maschinenlesbaren Code QR / OCR / Link ist insbesondere bei Verwendung eines Links die unverfälschbare Abhängigkeit von der Signatur zu beachten.

6. Zu 4.3 Vorliegen der organisatorischen Voraussetzungen

Die im Gutachten erforderlichen Angaben zu den organisatorischen Voraussetzungen der Manipulationssicherheit des geschlossenen Gesamtsystems (Maßnahmen zur laufenden Überprüfung) sind in § 21 Abs. 3 RKSV beschrieben.

7. Zu 4.4 Vorliegen der technischen Voraussetzungen

Der Inhalt der Begutachtung zu den technischen Voraussetzungen ist in § 21 Abs. 2 definiert.

Eine technische Begutachtung hat u.a. eine Prüfung der Dokumentation, der Signierung der Softwarekomponenten und eine Befundung der Signaturerstellung zu beinhalten.

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. Der Modul muss soweit isoliert sein, dass dieser signiert werden kann. Als Eingabewert für den Hashwert kann wahlweise der ausführbare Code oder der Source Code der Softwarekomponenten herangezogen werden.

Die Signaturerstellungskomponenten im geschlossenen Gesamtsystem sind an Hand des Anhangs „*Erforderliche Nachweise gem. SigG/SigV*“ des A-SIT Merkblattes „*Bescheinigungen der Bestätigungsstelle gemäß § 18 Abs. 5 Signaturgesetz (SigG)*“ zu prüfen. Verwiesen wird auf die Kriterien lt. Kapitel 4.4 Vorliegen der technischen Voraussetzungen.

Bestandteil ist u.a. eine Nennung der verwendeten Libraries und die Prüfung der Umsetzung der AES256 Verschlüsselung nach den Vorgaben der Anlage.

Zum Nachweis der ordnungsgemäßen Funktion ist auch die Nennung der allenfalls (üblicherweise) verwendeten Module und Libraries erforderlich. Diese müssen dem Stand der Technik entsprechen.

Für die Verwendung einschlägig bekannter und publizierter Module und Libraries kann gegebenenfalls die Richtigkeit der Signaturstellung aus bereits vorliegenden Beurteilungen abgeleitet werden. Inwieweit A-SIT für bestimmte Libraries die Richtigkeit als „bekannt“ annimmt, kann im Anlassfall dort in Erfahrung gebracht werden.

Eine taxative Liste approbierter Module und Libraries existiert allerdings nicht. Hinweise zu bereits bescheinigten Produkten erteilt die A-SIT unter „*Veröffentlichungen von Bescheinigungen nach § 18(5) (SigG)*“ bzw. auf Anfrage.

Für den Fall einer Eigenentwicklung der Module und Libraries ist eine inhaltliche Prüfung entsprechend den Vorgaben der Bescheinigung lt. § 18 Abs. 5 SigG vorzunehmen.

8. Zu 4.5 Vorliegen der Nutzung durch mehrere Unternehmer

Unternehmer, die gemeinsam ein geschlossenes Gesamtsystem verwenden, müssen jeweils einen Feststellungsbescheid beantragen.

Das Gutachten umfasst für das verbundene Unternehmen die Verbundenheit des Unternehmens zum geschlossenen Gesamtsystem sowie die Prüfung der organisatorischen Voraussetzung lt. § 21 Abs. 3, basierend auf dem vorhandenen Gutachten für das zentrale System. Zur Vorlage der technischen Voraussetzungen (lt. § 21 Abs. 2) kann auf das Gutachten des „übergeordneten“ Unternehmens verwiesen werden.

Falls ist eine „eigene“ Buchhaltung des wirtschaftlich verbundenen Unternehmens vorliegt, ist zu prüfen, ob die buchhaltungsrelevanten Daten aus dem übergeordneten geschlossenen Gesamtsystem manipulationssicher übertragen werden (z.B. Signierung von Datensätzen oder Dateien) u ggfl. manipulationssicher an die Finanzbuchhaltung des verbunden Unternehmens weitergereicht werden.

Das Vorhandensein der Vorrausetzung einer Konzernbeteiligung im Sinne des § 244 UGB ist nicht durch das Gutachten zu beurteilen.

Verfügt der antragstellende Unternehmer über ein separates, nicht verbundenes Warenwirtschaftssystem, dann ist dieser von der Wirksamkeit des Feststellungsbescheides für das „übergeordnete“ geschlossene Gesamtsystem nicht mehr umfasst.