

SV Gutachten laut Registrierkassensicherheitsverordnung (RKSv)

**Informationsveranstaltung
„Registrierkassensicherheitsverordnung“, 26.1.2016**



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

1

Geschlossene Gesamtsysteme

Grund für Gutachten: Feststellungsbescheid

- § 131b Abs. 4 BAO :
Das FA hat auf **Antrag des Unternehmers** mit Feststellungsbescheid die Manipulationssicherheit ... zu bestätigen, wenn eine solche auch **ohne Signaturerstellungseinheit** lt. Abs. 2 besteht.
- Mit Feststellungsbescheid bestätigte geschlossene Gesamtsysteme werden in der Datenbank über Sicherheitseinrichtungen (§ 18 RKSv) registriert.



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

2

Registrierkassensicherheitsverordnung

Geschlossenes Gesamtsystem

- § 3 Z 10 Geschlossenes Gesamtsystem: elektronisches Aufzeichnungssystem, in welchem Warenwirtschafts-, Buchhaltungs- und Kassensysteme lückenlos miteinander verbunden sind und das mit mehr als 30 Registrierkassen verbunden ist
- Annahme: Keine bescheinigte Signaturerstellungseinheit, sondern z.B. Software
- Erläuterungen BMF: Die freiwillige Verwendung einer Signaturerstellungseinheit wirkt sich nicht schädlich auf die Anerkennung eines geschlossenen Gesamtsystems aus



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

3

Registrierkassensicherheitsverordnung

Sachverständige Begutachtung geschlossener Gesamtsysteme

- § 21 Abs. 1: Im Rahmen der Begutachtung geschlossener Gesamtsysteme sind insbesondere folgende Überprüfungen vorzunehmen:
 - 1. das Vorliegen eines geschlossenen Gesamtsystems,
 - 2. das Vorliegen der **technischen** und
 - 3. der **organisatorischen**Voraussetzungen für die Manipulationssicherheit des geschlossenen Gesamtsystems.
- Bei Verwendung einer bescheinigten Signaturerstellungseinheit:
 - Pos 2: trivial
 - Gutachten nur über Pos 1. und Pos 3.



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

4

Gutachten laut RKS SV

- § 21 Abs. 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.



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

5

Befund und Gutachten:

Struktur und Inhalte

- Auftraggeber und Auftrag
- Beurteilungsgegenstand
- Befund
 - Zu: Geschlossenes Gesamtsystem
 - Zu: Registrierkassenfunktion
 - Zu: Organisatorische Voraussetzungen: Manipulationssicherheit
 - Zu: Technische Voraussetzungen: Manipulationssicherheit



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

6

Registrierkassensicherheitsverordnung

Befund und Gutachten: Struktur und Inhalte

- Gutachten
 - Geschlossenes Gesamtsystem
 - Anforderungen an die Registrierkasse §§ 5 - 11
 - Manipulationssicherheit: Vorliegen der organisatorischen
 - Manipulationssicherheit: Vorliegen der technischen Voraussetzungen
- Zusammenfassung



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

7

Vorliegen: Geschlossenes Gesamtsystem

Befund zur Dokumentation von (Funktion und Schnittstellen):

- Warenwirtschaftssystem
- Finanzbuchhaltung
- Kassensysteme

Erläuterung BMF:

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

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.

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.



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

8

Registrierkassenfunktion

Beurteilung zu den Kriterien:

- *Allgemeine Anforderungen laut § 5*
- *Inbetriebnahme Sicherheitseinrichtung laut § 6*
- *Datenerfassungsprotokoll laut § 7*
- *Summenspeicher laut § 8*
- *Signaturdatensatz laut § 9 Abs. 2*
- *Signaturerstellung und Schnittstellen für Signaturdaten*
- *Maschinenlesbarer Code laut § 10*
- *Belegerstellung laut § 11*



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

9

Registrierkassenfunktion

Erläuterungen BMF:

Verifikationen zur Registrierkassenfunktion sind stichprobenartig durchzuführen.

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

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.



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

10

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



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

11

Vorliegen der technischen Voraussetzungen

- Verwendung Signaturerstellungseinheit (bescheinigt): Nur Verweis
- Software mit „bei A-SIT bekannter und akzeptierter“ Funktion:
 - Nur Nachweis der Verwendung
- Software ohne Nachweise
 - Prüfung wie für Bescheinigung erforderlich: § 18 Abs. 5 SigG

Allgemeine Themen:

- Prüfung der Signierung der SW Komponenten
- Prüfung der Dokumentation

Erläuterung BMF:

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



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

12

Dokumentationsprüfung

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,

Erstellung von Berichten (wie z.B. Kassenjournale) usw.).

Konkreter Datenfluss an den Schnittstellen zwischen Warenwirtschaft, Kassensystem und Buchhaltung.



Technische Voraussetzungen: Detailprüfung

- Manipulationssicherheit und sicherheitstechnische Gleichwertigkeit mit einer Signaturerstellungseinheit.
- „Nachweis, dass die Signaturerstellungsdaten mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen.“
- „Nachweis, dass die Signaturerstellungsdaten mit hinreichender Sicherheit nicht ableitbar sind.“
- „Nachweis, dass die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar gemacht werden.“
- „Nachweis, dass die Geheimhaltung der Signaturerstellungsdaten sichergestellt ist.“



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 BMF:

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.



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

15

Zum Dokument: Befund und Gutachten - Informationen über Struktur und Inhalte

Das Dokument enthält, wie auch die Informationen in dieser Präsentation **Ergebnisse aus Arbeitsgesprächen** zwischen Vertretern des Landesverbandes der Gerichtssachverständigen, des BMF und von A-SIT.

Es handelt sich um eine unverbindliche Arbeitsunterlage, deren Inhalte allenfalls auch noch angepasst werden.

Die Interpretation der Kriterien die sich für die Gutachten der SV aus den gesetzlichen Vorgaben ergeben liegt ausschließlich im **Verantwortungsbereich** des erstellenden **SV**, die Gliederung und der Aufbau der Gutachten, letztlich auch die Prüftiefe und damit der Aufwand sind weiters auch durch den **Auftrag an den SV** bestimmt.

Eine entsprechend präzise Formulierung des Gutachtensauftrages wird empfohlen.



JUDMANN ZIVILTECHNIKER GMBH

Hon.-Prof. Dipl.-Ing. Dr. Kurt P. Judmann
TU Wien, Institut für Computertechnik

16