Praktische Aspekte des INSIKA-Sicherheitskonzepts

Jens Reckendorf
Vectron Systems AG
Willy-Brandt-Weg 41, 48155 Münster
jreckendorf@vectron.de

Zum vollständigen Verständnis des INSIKA-Konzepts ist es erforderlich zu wissen, welche Sicherheitselemente es gibt und in welcher Form diese ineinandergreifen. Wesentliche Aspekte werden in anderen Beiträgen der vorliegenden Veröffentlichung erläutert, jedoch ohne zusammenhängende und detaillierte Darstellung. Das soll im Rahmen dieses Beitrags erfolgen.

Es werden im Vorgriff auf die Sicherheitsanalyse die in der Praxis wesentlichen Elemente dargestellt, verschiedene denkbare Angriffe vorgestellt und deren Auswirkungen erläutert. Dabei wird der Schwerpunkt auf die INSIKA-spezifischen Teile gelegt – verwendete Standardverfahren (Kryptografie, Smartcards usw.) werden nur kurz vorgestellt.

1 Überblick

1.1 Grundsätze

In diesem Beitrag werden einige Annahmen zugrunde gelegt:

- Es besteht eine Belegpflicht für jeden Kassiervorgang an einer Registrierkasse.
- Der Beleg muss bestimmte Mindestinhalte aufweisen und vor allem mit einer korrekt ermittelten, ausgedruckten Signatur versehen werden.
- Es werden Stichprobenkontrollen für die beiden o. g. Punkte durchgeführt, so dass ein realistisches Entdeckungsrisiko bei Verstößen besteht.
- Die Smartcards (TIM) werden durch die Finanzbehörden zentralisiert verwaltet und ausgegeben.

Werden diese Annahmen verändert, sind die Analysen und Schlussfolgerungen – teilweise in wesentlichen Punkten – anzupassen.

1.2 Abläufe

Die hier angenommenen Abläufe beim Erfassen von Registrierungen und bei der Weiterverarbeitung der Daten entsprechen dem aktuellen Stand der INSIKA-Spezifikation. Zur Erläuterung sei insbesondere auf die Beiträge von Zisky, Neuhaus und Wolff in diesem PTB-Bericht verwiesen.

1.3 Sicherheitsanalyse

Im Rahmen des INSIKA-Projekts wurde eine Sicherheitsanalyse erstellt. Es gibt deutliche Überschneidungen der Sicherheitsanalyse mit dem vorliegenden Beitrag. Die Sicherheitsanalyse umfasst neben den hier diskutierten Punkten jedoch noch eine Reihe von weiteren Aspekten, z. B. zufällige Gefährdungen des Systems oder sog. Koalitionsangriffe, bei der mehrere Parteien zusammenarbeiten.

1.4 Kryptografie / Smartcards

Die Elemente des INSIKA-Konzepts, die auf Standardverfahren aufbauen und damit den Stand der Technik in Bezug auf Kryptografie darstellen, werden hier nicht weiter behandelt. Auf die wichtigsten Komponenten soll jedoch ganz kurz eingegangen werden:

- Das ECDSA-Verfahren („Elliptic Curve Digital Signature Algorithm“) stellt den Stand der Technik für Signaturlösungen dar, die auch mit kurzen Schlüssel- und Signaturlängen sowie geringem Berechnungsaufwand hohe Sicherheit gewährleisten können.
- Durch die Verwendung einer Standard-Smartcard werden sämtliche Sicherheits-Funktionen der Hard- und Software genutzt. Entscheidend dabei sind die sichere Geheimhaltung des privaten

PTB-Bericht IT-18
doi:10.7795/210.20130206a

Schlüssels und der Schutz der Software vor Manipulationen.

- Durch die Verwendung von Standardverfahren für die PKI („Public-Key Infrastructure“), u.a. unter Nutzung von Zertifikaten, Identitätsprüfungen, CRLs („Certificate Revocation List“) ist sichergestellt, dass eine eindeutige Zuordnung der TIMs und der damit signierten Datensätze zu einem Steuerpflichtigen möglich ist und das verlorene bzw. gestohlene Karten bei Prüfungen erkannt werden können.

2 Prüfszenarien

In diesem Abschnitt sind die wesentlichen Prüfungen beschrieben, die das INSIKA-System vorsieht. Diese können durch Betriebsprüfer oder auch zusätzlich z. B. durch eine interne Revisionsabteilung erfolgen.

Im Folgenden werden verschiedene Begriffe für unterschiedliche Prüfungshandlungen verwendet:

Prüfung: Allgemeiner Begriff für alle Tätigkeiten, die zur Überprüfung dienen.

Kontrolle: Stichprobenartige, vergleichsweise häufige Kontrollen, die eine korrekte Nutzung des Systems sicherstellen sollen. Im Gesetzentwurf aus dem Jahr 2008 wurde dieser Vorgang „Kassennachschau“ genannt.

Audit: Nachträgliche Prüfung der aufgezeichneten Daten über längere Zeiträume. I. d. R. wird das im Rahmen von Außenprüfungen erfolgen.

Verifikation: Überprüfung der Korrektheit einer Signatur.

2.1 Überprüfung gedruckter Belege

Die Prüfung eines gedruckten Belegs ist in zwei Stufen möglich:

- Die wesentlichen Daten wie Datum/Uhrzeit, Identifikation des Steuerpflichtigen, Sequenznummer, steuerpflichtige Umsätze, der Hash-Wert der Buchungspositionen und die Signatur werden erfasst. Diese Erfassung kann manuell erfolgen oder durch OCR-Verfahren weitgehend automatisiert werden. Alternativ dazu ist die Codierung der Daten als 2D-Code und damit eine einfache, automatische Auswertung möglich. Dieser Ansatz ist auch bereits praktisch erprobt. Anhand dieser Daten wird die Gültigkeit der Signatur verifiziert und damit der Nachweis erbracht, dass die Daten durch ein TIM signiert und korrekt abgedruckt wurden. Da für die Prüfung ein über die PKI verwaltetes Zertifikat verwendet wird, erfolgt gleichzeitig eine Überprüfung der Identität des Steuerpflichtigen und dass kein gefälschtes bzw. ein als gestohlen oder verloren gemeldetes TIM verwendet wurde.
- Zusätzlich können die Positionsdaten erfasst und deren Hash-Wert überprüft werden. Das belegt zusätzlich, dass hier keine Veränderungen vorgenommen wurden.

Diese Prüfungen können in folgenden Situationen durchgeführt werden:

- als Stichprobenkontrolle im laufenden Betrieb (dies kann auch ein „verdeckter Testkauf“ sein), um die Korrektheit des Registriervorgangs zu überprüfen oder
- als nachgelagerte Prüfung zu einem beliebigen Zeitpunkt, um die Echtheit eines Beleges zu bestätigen oder widerlegen.

Entsprechende Kontrollen sind bei jedem denkbaren System zur Absicherung der Aufzeichnung von Umsatzdaten erforderlich. Technische Lösungen können diese Kontrollen nur erleichtern und sicherer machen, aber nicht ersetzen.

2.2 Prüfung ohne Belege

Können Kontrolle nicht anhand gedruckter Belege erfolgen, ist nur ein zeitnaher Abgleich von erfassten Buchungen mit tatsächlich getätigten Umsätzen möglich. Diese erfordert den Zugriff auf Transaktionsdaten.

Dieses Verfahren wird beim Einsatz in INSIKA im Taxibereich angewendet, da dort aus verschiedenen Gründen keine Belegpflicht besteht. Dazu werden die signierten Transaktionsdaten per Mobilfunk an einen Server übertragen, so dass jederzeit ein Zugriff für Kontrollen möglich ist.

Alle im Folgenden beschriebenen Prüfungen werden i. d. R. im Rahmen eines Audits stattfinden.

2.3 Schnelle Prüfung der gespeicherten Buchungen

Für eine schnelle Überprüfung der gespeicherten Buchungsdaten werden alle Buchungen zwischen zwei Tagesabschlüssen summiert und mit der Differenz dieser Tagesabschlüsse verglichen. Ferner wird die Vollständigkeit und aufsteigende Folge der Sequenznummern überprüft. Eine Prüfung der Signaturen erfolgt

lediglich für die Tagesabschlüsse. Mit dieser Prüfung würde eine Verschiebung von Umsätzen zwischen Buchungen nicht erkannt werden – dafür läuft sie sehr schnell ab. Sie dürfte in der Praxis fast immer ausreichen, vor allem wenn sie mit Stichprobenprüfungen entsprechend Abschnitt 2.4 kombiniert wird.

2.4 Detailprüfung der gespeicherten Buchungen

Um zu prüfen, dass keine Buchungsdaten verändert wurden, werden die Signaturen der Buchungsdaten entweder stichprobenartig oder vollständig geprüft. Aufgrund des bereits sehr hohen Aussagewerts der unter 2.3 beschriebenen Prüfung ist eine vollständige Prüfung voraussichtlich lediglich bei einem konkreten Manipulationsverdacht und zur genauen Eingrenzung bereits entdeckter Manipulationen erforderlich.

2.5 Prüfung ungenutzter TIMs

Über die PKI ist ermittelbar, welche TIMs auf den Steuerpflichtigen personalisiert sind. Aus allen TIMs, für die bei den Prüfungen nach 2.3 und 2.4 keine Daten vorliegen oder bei denen der Verdacht besteht, dass noch weitere Daten zeitlich nach den neuesten vorliegenden signiert wurden, müssen die Summenspeicher ausgelesen werden. Damit kann verifiziert werden, dass die TIMs nicht benutzt wurden bzw. die vorgelegten Daten wirklich vollständig sind.

2.6 Abgleich der Daten mit der Buchführung

Das wesentliche Ziel der Prüfung von gespeicherten Buchungsdaten im Rahmen eines Audits ist der Abgleich mit den in der Buchführung erfassten Barumsätzen. Dazu bietet sich nach der Verifikation der Buchungsdaten (welche die Vollständigkeit und Unversehrtheit der Daten sicherstellt) die Verdichtung der Daten über geeignete Zeiträume (Jahre, Monate) und der Abgleich mit der Buchführung an. Sollten dabei Abweichungen auftreten, kann die Analyse leicht auf kürzere Zeiträume bis auf die Ebene einzelner Buchungen verfeinert werden.

2.7 Abgleich mit nachgelagerten Systemen

Lieferschein- und Agenturumsätze werden zwar an der Registrierkasse erfasst und in den Signaturvorgang einbezogen. Die steuerlich relevante Verarbeitung erfolgt jedoch in einem angeschlossenen System. Durch einen Abgleich mit diesen Systemen kann die Plausibilität der betreffenden Daten sichergestellt werden. Ist dies nicht möglich, so würden die betreffenden Umsätze wie reguläre Umsätze betrachtet.

2.8 Schließen von Lücken in Buchungsdaten

Sollten Lücken in den Buchungsdaten auftreten (sehr leicht an nicht fortlaufenden Sequenznummern für Buchungen und/oder Tagesabschlüsse zu erkennen), lassen sich die wesentlichen Kennzahlen (Gesamtumsätze nach Steuersätzen, Lieferschein- und Agenturumsätze, Negativbuchungen, Anzahl der Buchungen) zwischen jeweils zwei gültigen Tagesabschlüssen ermitteln. Solche Lücken können durch Datenverluste aufgrund technischer Probleme durchaus auftreten. Mit dem beschriebenen Verfahren können die negativen Auswirkungen sowohl für Prüfer als vor allem auch für die Steuerpflichtigen minimiert werden.

2.9 Abschätzung bei fehlenden Buchungsdaten

Wenn sämtliche Buchungsdaten fehlen, ist die Auswertung der monatlichen Summenspeicher auf dem TIM möglich. Die dort verfügbaren Daten entsprechen dem unter 2.7 beschriebenen Umfang, nur dass hier grundsätzlich Monatssummen erfasst werden.

2.10 Rückgriff auf online eingereichte Daten

Im Rahmen der INSIKA-Lösung ist es technisch möglich, wesentliche Daten regelmäßig online an die Finanzbehörden zu übermitteln (z. B. könnten im Rahmen der elektronischen Umsatzsteuervoranmeldung alle Tagesabschlüsse eines Monats übertragen werden). Durch die Signaturen ist die Datenintegrität gewährleistet. Bei zentralisierter Speicherung können die Folgen eines vollständigen Datenverlustes beim Steuerpflichtigen kompensiert werden.

3 Mögliche Angriffe

In diesem Abschnitt wird eine Reihe von möglichen Angriffen auf das System beschrieben, analysiert und das Restrisiko bewertet.

3.1 Umsätze nicht erfassen

Beschreibung: Umsätze werden nicht an der Kasse erfasst sondern z. B. nur handschriftlich festgehalten.
Analyse: Gegen diese Manipulation gibt es grundsätzlich keinen rein technischen Schutz. Es kann lediglich das Entdeckungsrisiko so weit erhöht werden,

dass Anwender darauf verzichten. Das wird vor allem durch die Belegpflicht mit entsprechenden Kontrollen erreicht. Zusätzlich wird jede systematische Nichterfassung von Daten Auffälligkeiten erzeugen, die bei einem Audit z. B. über Zeitreihenvergleiche erkannt werden können. Ferner ist zu bedenken, dass die Nutzung einer Registrierkasse in vielen Betrieben eine organisatorische Notwendigkeit ist. Einen weiteren Beitrag kann eine Sensibilisierung der Verbraucher leisten. Speziell die Codierung der wesentlichen Daten eines Belegs als 2D-Code würde eine sehr einfache und schnelle Kontrolle ermöglichen. Wenn keine Belegpflicht möglich ist, stellt die unter 2.2 beschriebene Kontrolle eine – wenn auch aufwendigere und weniger effektive – Möglichkeit dar.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege)
Restrisiko: Jede Art von „Fiskal-Kassensystem“ bringt das Risiko mit sich, dass es in der beschriebenen Form umgangen wird. Das Restrisiko kann durch eine Belegpflicht (sinnvoll ist ebenfalls eine Kassenpflicht) und eine ausreichende Kontrolldichte reduziert werden.

3.2 Umsätze nicht signieren und Beleg ohne Signatur drucken

Beschreibung: Eine Registrierkasse signiert grundsätzlich oder auf Anforderung des Benutzers die Umsätze nicht und druckt auch keine Signatur. Das kann z. B. auch dadurch passieren, dass nur unsignierte, „vorläufige“ Belege ausgegeben werden und die Daten anschließend ohne den Ausdruck eines signierten endgültigen Beleges verworfen werden.
Analyse: Diese Manipulation ist sehr leicht und auch rückwirkend erkennbar, da der betreffende Beleg in diesem Fall keine Signatur enthält. Dabei ist zu beachten, dass ein einziger unsignierter Beleg einen Verstoß gegen die Vorschriften beweist. Der Kontrollaufwand ist damit soweit wie möglich minimiert, da bei alternativen Lösungen ohne kryptografische Absicherung eine Kontrolle des Druckvorgangs selbst erforderlich ist. Anders ist in diesem Fall nicht nachweisbar, dass gegen die Belegpflicht verstoßen wurde, da nichtkryptografische Kennzeichnungen von Belegen (z. B. ausgedruckte Symbole) sehr leicht zu fälschen sind.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege)
Restrisiko: Das Risiko wird praktisch nur durch die Kontrolldichte bestimmt.

3.3 Umsätze nicht signieren und falsche Signatur drucken

Beschreibung: Eine Registrierkasse signiert grundsätzlich oder auf Anforderung des Benutzers die Umsätze nicht und druckt eine ungültige Signatur (z. B. Zufallswerte).
Analyse: Diese Manipulation ist durch Überprüfung der Signatur anhand des gedruckten Belegs und damit auch noch rückwirkend erkennbar. Der Kontrollaufwand ist soweit wie möglich minimiert, da bei alternativen Lösungen (ohne kryptografische Absicherung) eine Kontrolle des Druckvorgangs selbst erforderlich ist.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege), Vergleich mit der vermeintlich zugehörigen Buchung, die über die Sequenznummer gefunden werden kann.
Restrisiko: Das Risiko wird praktisch nur durch die Kontrolldichte bestimmt. Dabei ist zu beachten, dass bereits ein einziger unsignierter Beleg einen Verstoß gegen die Vorschriften beweist.

3.4 Umsätze signieren, korrekt drucken und nicht oder verändert im Journal speichern

Beschreibung: Die Registrierkasse signiert und druckt die Daten in korrekter Form, speichert sie dann aber verändert ab.
Analyse: Durch die Signatur lässt sich jede Veränderung an den Daten automatisiert feststellen. Dies umfasst die Veränderung von Inhalten und das Entfernen von Buchungen. Dabei ist auch eine Rückführung auf einzelne Belege möglich. Das Ausmaß der Veränderungen kann tagesgenau aus den Tagesabschlüssen oder bei Verlust aller Daten monatsgenau aus den Summenspeichern des TIM ermittelt werden.
Relevante Prüfung(en): 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.5 Umsätze signieren, verändert drucken und verändert im Journal speichern

Beschreibung: Die Registrierkasse signiert die korrekten Daten, druckt und speichert jedoch eine veränderte Version der Daten.
Analyse: Die Analyse entspricht der unter 3.4, nur das die Manipulation zusätzlich auch an einem gedruckten Beleg erkannt werden kann (da die Signatur nicht zu den anderen Informationen auf dem Beleg passt).

Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) sowie 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.6 Umsätze sammeln, verändern und erst später signieren

Beschreibung: Eine Registrierkasse erfasst zwar Umsätze, signiert sie jedoch nicht. Dies wird erst nach einer Manipulation der Daten „rückwirkend“ durchgeführt.
Analyse: Da das Erstellen einer Signatur im TIM fest mit der Vergabe einer neuen Sequenznummer verknüpft ist, kann jeder Umsatz nur einmal signiert werden (sonst würde er doppelt aufgezeichnet werden müssen). Damit bedingt das geschilderte Vorgehen, dass zum Zeitpunkt der Registrierung kein gültiger Beleg erstellt werden kann. Dies ist durch Kontrollen erkennbar.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege)
Restrisiko: Das Risiko wird praktisch nur durch die Kontrolldichte bestimmt.

3.7 Doppelte Verwendung eines signierten Datensatzes

Beschreibung: In einem Unternehmen mit einem kleinen Sortiment und vielen Transaktionen (z. B. Fast-Food-Restaurant) werden innerhalb einer kurzen zeitlichen Abfolge identische Belege ausgegeben. Es wird nur einmal signiert. Dieser Beleg wird mehrfach verwendet. Ab dem zweiten Beleg werden die Umsätze nicht erfasst.
Analyse: Diese Manipulation ist prinzipiell nicht auszuschließen. Kein Verfahren kann beim Einsatz branchenüblicher Druckverfahren einen "Kopierschutz"für gedruckte Belege bewirken. Selbst bei weitgehenden Einschränkungen für die Registrierkassen könnten Kopien über getrennte Systeme gedruckt werden (z. B. PC mit handelsüblichem Kassendrucker). Die Manipulation ist im Rahmen von Kontrollen leicht erkennbar, da mehrere Belege mit gleichem Datum, gleicher Zeit und Sequenznummer ausgegeben werden. Diese Daten können auf den Kopie-Belegen auch nicht geändert werden, ohne dass die Signatur ungültig würde.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege)
Restrisiko: Bei bestimmten Betriebstypen könnte eine höhere Kontrolldichte erforderlich sein, um das Restrisiko zu minimieren. Der mögliche Schaden durch den beschrieben Angriff ist jedoch in allen praktisch relevanten Fällen sehr gering.

3.8 Journal nachträglich manipulieren

Beschreibung: In einem System werden die korrekt signierten, aufgezeichneten Daten nachträglich verändert. Dies kann in der Kasse oder auch in nachgelagerten Systemen, wie z. B. einer PC-Software zur Speicherung und Verwaltung der Daten, erfolgen. Für eine entsprechende Manipulationssoftware wird oft der der Begriff „Zapper“ verwendet.
Analyse: Die Analyse entspricht der aus Punkt 3.4.
Relevante Prüfung(en): 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.9 Veränderung von Kassenberichten, Buchhaltungsdaten usw.

Beschreibung: Neben der Speicherung der signierten Buchungsdaten werden in jedem System weitere Berichte („Tagesendsummenbons“, Kassenumsätze in der Buchhaltung) erstellt und weiterverarbeitet. Die Inhalte dieser Berichte werden verändert, z. B. durch Stornieren von Umsätzen, ohne dass dies anhand von signierten Buchungen erfolgt.
Analyse: Die genannten Berichte bilden in den meisten Fällen die Grundlage der Buchführung, da die einzelnen Buchungen der Registrierkasse(n) nicht in das Buchführungssystem übernommen werden. Daher ist ein wesentliches Element eines Audits der Abgleich der an der Kasse aufgezeichneten, signierten Buchungsdaten mit den Daten im Buchführungssystem. Da diese Prüfung praktisch vollautomatisiert mit einer Summenbildung über beliebige Zeiträume erfolgen kann, ist sie mit geringem Aufwand (für Steuerpflichtige und Betriebsprüfer) möglich. Jeglicher Fehler wird sicher aufgedeckt. Bei Abweichungen ist eine Nachverfolgung bis hinunter auf die Belegebene möglich.
Relevante Prüfung(en): 2.6 (Abgleich der Daten mit der Buchführung)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.10 Umprogrammierungen von Produkten

Beschreibung: Umsätze für Produkte mit einem geringen Wareneinsatz werden nachträglich als Umsätze mit hohem Wareneinsatz deklariert, um damit bei unveränderten Umsätzen den ausgewiesenen Rohertrag zu reduzieren.

Analyse: Abgesehen davon, dass dieses Vorgehen zusätzlich fingierte Eingangsrechnungen erfordert, sind solche Änderungen eindeutig erkennbar, da in den gespeicherten Buchungsdaten Artikeltexte („handelsübliche Bezeichnung“) enthalten und signiert sind. Eine Überwachung von Programmänderungen der Registrierkasse ist dadurch überflüssig. Es muss lediglich die Analysesoftware eine Summenbildung anhand der Texte beherrschen. Die so gewonnen Summen können leicht auf Plausibilität geprüft werden.
Relevante Prüfung(en): 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent. Lediglich bei einer sehr oberflächlichen Prüfung könnten entsprechende Veränderungen unentdeckt bleiben.

3.11 Trainingsbediener, Service-Modi usw.

Beschreibung: Durch Nutzung von Funktionen zum Test des Systems, zur Einarbeitung von Bedienern etc. werden Umsätze an der Kasse zwar erfasst, aber nicht regulär gespeichert.
Analyse: Durch die Pflicht zur Ausgabe eine signierten Belegs sind solche Manipulationen eindeutig erkennbar – die Analyse entspricht praktisch der aus 3.4. Das TIM verfügt über einen Modus zur Erfassung von Trainingsbuchungen mit separatem Summenspeicher, so dass selbst beim Verlust aller Daten anhand der im TIM gespeicherten Werte das Volumen dieser Buchungen erkennbar ist.
Relevante Prüfung(en): 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege) und evtl. 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.12 Fälschliche Ausweisung von Umsätzen als Lieferschein

Beschreibung: Umsätze werden fälschlicherweise als Lieferschein-Umsatz ausgewiesen (diese Umsätze werden gemäß der Spezifikation signiert, die zugehörigen Bareinnahmen erfolgen aber nicht an der Kasse, sondern in einem nachgelagerten System).
Analyse: Im Rahmen eines Audits ist nachzuweisen, wie die Lieferschein-Umsätze weiterverarbeitet wurden. Ist das nicht möglich, werden sie wie normale Umsätze gewertet. Das gilt auch im Fall des Verlusts der gespeicherten Buchungsdaten und Rückgriff auf die Summenspeicher im TIM.
Relevante Prüfung(en): 2.7 (Abgleich mit nachgelagerten Systemen) und evtl. 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Es besteht kein Risiko, dass durch dieses Vorgehen Umsätze verschleiert werden können.

3.13 Fälschliche Ausweisung von Umsätzen als Agenturumsatz

Beschreibung: Umsätze werden fälschlicherweise als Agenturgeschäfts ausgewiesen. Gemäß der Spezifikation werden diese Umsätze signiert, obwohl sie im Namen Dritter erfolgt sind. Die Weiterarbeitung erfolgt in einem anderen System als der Registrierkasse.
Analyse: Einen Agenturumsatz muss der Betreiber der Registrierkasse nicht versteuern auch wenn dieser durch ihn signiert wurde. Der Nachweis dafür muss im Rahmen eines Audits anhand des weiterverarbeitenden Systems erbracht werden. Hier ist bei Bedarf eine Verprobung mit dem System des Agenturgebers möglich. Das gilt auch im Fall des Verlusts der gespeicherten Buchungsdaten und Rückgriff auf die Summenspeicher im TIM.
Relevante Prüfung(en): 2.7 (Abgleich mit nachgelagerten Systemen) und evtl. 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Es besteht kein Risiko, dass durch dieses Vorgehen Umsätze verschleiert werden können.

3.14 Massive Stornierungen und Löschung aller Daten

Beschreibung: Es werden größere Beträge storniert, um die ausgewiesenen Umsätze zu reduzieren. Um dies nicht anhand Einzelbuchungen nachweisen zu können, werden die aufgezeichneten Buchungen gelöscht, so dass nur noch die Summenspeicher des TIM vorliegen.
Analyse: Unabhängig davon, dass der Verlust der aufgezeichneten Buchungsdaten bereits ein Verstoß gegen Vorschriften darstellt, sind die Negativbuchungen in den Summenspeichern ausgewiesen. Durch den Vergleich des Anteils der Negativbuchungen am Gesamtumsatz über alle im TIM vorhandenen Monatssummenspeicher sind Abweichungen schnell erkennbar.
Relevante Prüfung(en): 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Durch die beschriebenen Nachweismöglichkeiten ist ein Manipulationsversuch leicht erkennbar und der Effekt gut abzuschätzen. Generell sind alle Manipulationsversuche, die eine Vernichtung aller Buchungsdaten erfordern, weder in einem großen Maßstab noch wiederholt möglich.

3.15 Verwendung falscher Umsatzsteuersätze

Beschreibung: Durch die Verwendung falscher Umsatzsteuersätze werden falsche Steuern errechnet und entsprechend signiert, gedruckt und gespeichert.
Analyse: Das TIM überprüft zwar die Steuerberechnungen, speichert im Monatsspeicher den Steuersatz und vermerkt dort, wenn es eine Änderung innerhalb eines Monats gegeben hat – dies sind jedoch alles reine Plausibilitätsprüfungen, da die Steuerermittlung auf Basis der erfassten Umsätze erfolgt. Selbst bei falschen Steuersätzen ist die korrekte Ermittlung der Umsatzsteuern möglich, sogar wenn keine aufgezeichneten Buchungen mehr, sondern nur noch die Summenspeicher des TIM existieren.
Relevante Prüfung(en): Das beschriebene Vorgehen wird bei allen Prüfungsschritten angewandt.
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.16 Verwendung falscher Zeitinformationen

Beschreibung: Durch Nutzung falscher Datums- und Zeitangaben wird die Plausibilisierung von Daten bei einem Audit evtl. erschwert.
Analyse: Durch die Belegdruckpflicht, die Sequenznummer und das Einbeziehen von Datum und Uhrzeit in die Signatur fallen falsche Angaben in jedem Fall auf. Im Rahmen des Audits kann automatisch kontrolliert werden, dass alle Buchungen chronologisch aufsteigend erfasst wurden – schwer erkennbare Veränderungen sind also grundsätzlich nur in diesem Rahmen denkbar.
Relevante Prüfung(en): 2.3 (Schnelle Prüfung der gespeicherten Buchungen) oder 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Veränderungen bieten kaum Chancen zur Verschleierung von Umsätzen und sind zudem nur in geringem Ausmaß möglich, ohne dass sie erkannt würden. Ein nennenswertes Risiko erwächst daraus nicht.

3.17 Verlust von aufgezeichneten Daten provozieren

Beschreibung: Die aufgezeichneten Buchungsdaten werden bewusst ganz oder teilweise vernichtet.
Analyse: Abgesehen von der Tatsache, dass durch einen Datenverlust gegen die gesetzlichen Aufbewahrungspflichten verstoßen wird, ist eine Abschätzung des Effekts in zwei Stufen möglich: Zum einen können die Gesamtumsätze (und einige zusätzliche Werte) zwischen zwei beliebigen Tagesabschlüssen errechnet und damit eine entsprechende Lücke in den Daten kompensiert werden. Zum anderen sind monatsgenaue Summenspeicher auf dem TIM enthalten, die auch beim Verlust von aller anderen Daten auslesbar sind.
Relevante Prüfung(en): 2.8 (Schließen von Lücken in Buchungsdaten) oder 2.9 (Abschätzung bei fehlenden Buchungsdaten)
Restrisiko: Durch die Möglichkeit, die Gesamtbeträge der verlorenen Buchungen zu rekonstruieren, können die Auswirkungen der Manipulation sehr weitgehend reduziert werden.

3.18 Zerstörung des TIMs

Beschreibung: Das TIM wird bewusst zerstört, um eine Signatur von neuen Buchungen unmöglich zu machen und um die darauf gespeicherten Daten zu vernichten.
Analyse: Aufgrund der konzeptionell vorgesehenen Möglichkeit, Reserve-TIMs auszugeben, sollte ein defektes TIM keinen Begründung darstellen, Umsatzdaten selbst für einen kurzen Zeitraum nicht zu signieren. Der Datenverlust ist unkritisch, solange noch die gespeicherten, signierten Buchungen vorliegen.
Relevante Prüfung(en): Keine
Restrisiko: Ein zerstörtes TIM liefert weder eine tragfähige Begründung dafür, keine Signaturen mehr zu erstellen noch dafür, keine Daten vorlegen zu können.

3.19 Vernichtung aller Daten und des TIMs

Beschreibung: Ein Steuerpflichtiger vernichtet bewusst alle aufgezeichneten Daten (inklusive der Datensicherungen) und das TIM.
Analyse: In diesem Fall ist natürlich kein Rückgriff auf die Daten oder eine Rekonstruktion möglich. Da der Verlust aller Daten einen mehrfachen Verstoß gegen Vorschriften darstellt, sollte der Nachweis von Vorsatz oder grober Fahrlässigkeit generell einfach möglich sein. Mit einer technisch möglichen, regelmäßigen Online-Übertragung wesentlicher Daten ließe sich auch in so einem Fall eine gute Abschätzung der Umsätze vornehmen.
Relevante Prüfung(en): 2.10 (Rückgriff auf online eingereichte Daten)
Restrisiko: Die Vernichtung aller Daten ist praktisch nicht zu verhindern. Es wäre noch zu bewerten, ob die Zerstörung einer Smartcard eine geringere „Hemmschwelle“ bedingt als die Zerstörung einer klassischen Fiskalkasse bzw. eines Fiskaldruckers. Per Online-

Meldung der Daten lässt sich auch dieses Restrisiko praktisch vollständig ausschließen.

3.20 Nutzung von Reserve-TIMs

Beschreibung: Überzählige (also momentan nicht genutzte) TIMs werden genutzt, um einen Teil der Umsätze gültig zu signieren – die Daten der Reserve-TIMs werden jedoch bei einem Audit nicht vorgelegt.
Analyse: Bei einem Audit werden die Daten aller für einen Steuerpflichtigen ausgegebenen TIMs geprüft. Dabei ist anhand der aktuellen Sequenznummern und der Summenspeicher der TIMs, die nicht im täglichen Einsatz sind, leicht festzustellen, ob die Daten vollständig sind oder ob einzelne TIMs bisher noch gar nicht benutzt wurden.
Relevante Prüfung(en): 2.5 (Prüfung ungenutzter TIMs)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.21 Einsatz von zwei Kassen – nur das Journal einer Kasse wird zur Prüfung vorgelegt

Beschreibung: Ein Steuerpflichtiger verwendet zwei Kassen, die beide mit einem TIM bestückt sind. Nur die Daten einer Kasse werden bei einer Prüfung vorgelegt. Rein technisch könnte dies auch mit einer Kasse, die mit zwei TIMs ausgestattet ist, versucht werden.
Analyse: Da ohne ein zweites TIM keine gültigen Signaturen erstellt werden können, entspricht die Analyse genau dem Punkt 3.20.
Relevante Prüfung(en): Siehe 3.20.
Restrisiko: Siehe 3.20.

3.22 Diebstahl eines TIMs

Beschreibung: Ein gestohlenes TIM wird zu Erstellung rechnerisch gültiger Signaturen verwendet.
Analyse: Über verschiedene Wege (signierte Identifikation des Steuerpflichtigen als Teil der gedruckten und aufgezeichneten Daten, Zertifikat, Sperrung der Zertifikate für als gestohlen gemeldete TIMs) ist eindeutig erkennbar, dass Belege nicht korrekt signiert wurden.
Relevante Prüfung(en): Alle Prüfungen, bei denen Signaturen verifiziert werden – also 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege), 2.3 (Schnelle Prüfung der gespeicherten Buchungen) und 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Wenn lediglich gedruckte Belege geprüft werden, ist das Risiko analog zu Punkt 3.3 zu bewerten, bei einer Prüfung gespeicherter Buchungsdaten ist ein Restrisiko praktisch nicht vorhanden.

3.23 TIM wird fälschlicherweise als gestohlen gemeldet

Beschreibung: Ein TIM wird fälschlicherweise als gestohlen gemeldet, jedoch weiter zur Erstellung von Signaturen benutzt.
Analyse: Bei jeder Prüfung von gespeicherten Buchungen oder gedruckten Belegen sind alle nach dem vermeintlichen Datum des gemeldeten Diebstahls signierten Vorgänge eindeutig erkennbar (das ist eine der Funktionen der PKI). Damit besteht genau das gleiche Entdeckungsrisiko wie beim Sachverhalt unter Punkt 3.3.
Relevante Prüfung(en): Analog zu 3.22.
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

3.24 „Abhören“ der Kommunikation mit dem TIM

Beschreibung: Durch Erfassung des Datenaustausches zwischen Registrierkasse und TIM und eventuellen Eingriff in die Kommunikation werden Erkenntnisse für einen Angriff gewonnen bzw. Daten manipuliert.
Analyse: Die Kommunikation zwischen Kassen und TIM ist nicht verschlüsselt und folgt einem offengelegten Verfahren. Dies ist möglich, da die Sicherheit ausschließlich auf dem Signaturverfahren und der festen Verknüpfung verschiedener Schritte (Signatur, Verwaltung der Sequenznummer, Plausibilitätsprüfung der Daten, Aktualisierung der Summenzähler) im TIM basiert.
Relevante Prüfung(en): keine
Restrisiko: Ein Angriff in der beschriebenen Form ist wirkungslos, solange dadurch keine Angriffe auf den Signaturalgorithmus oder die Smartcard selbst möglich sind.

3.25 Erstellung von Signaturen mit einem "TIM-Nachbau" oder einer Emulation

Beschreibung: Eine Registrierkasse erstellt kryptografisch korrekte Signaturen mit einem „nachgebauten“ TIM bzw. einer Emulation.
Analyse: Da das gesamte Verfahren offengelegt ist, kann die Funktion des TIM mit vertretbarem Aufwand nachgebildet werden. Die Sicherheit basiert jedoch auf dem geheimen Schlüssel, der im TIM (und nur dort) gespeichert ist. Dieser Schlüssel ist nicht auslesbar – auf dieser Tatsache basiert die Sicherheit aller

mit Hilfe von Smartcards umgesetzten kryptografischen Lösungen. Die Erstellung eines eigenen geheimen Schlüssels wäre wirkungslos, da der zugehörige öffentliche Schlüssel nicht als Zertifikat verfügbar ist (durch das Zertifikat bestätigt eine vertrauenswürdige Stelle, dass der dort enthaltene öffentliche Schlüssel korrekt und gültig ist sowie zum Steuerpflichten gehört).
Relevante Prüfung(en): Alle Prüfungen, bei denen Signaturen verifiziert werden – also 2.1 (Überprüfung gedruckter Belege) bzw. 2.2 (Prüfung ohne Belege), 2.3 (Schnelle Prüfung der gespeicherten Buchungen) und 2.4 (Detailprüfung der gespeicherten Buchungen)
Restrisiko: Ein Restrisiko ist praktisch nicht existent.

4 Gesamtbetrachtung

Die Sicherheit des gesamten Systems basiert vor allem auf geeigneten Kontrollen und Audits. Verfahren und Technik des INSIKA-Konzepts bergen nur minimale Restrisiken. Wesentlich sind vor allem die Kontrollen, mit denen erreicht werden muss, dass die bei jedem System mögliche Nicht-Benutzung mit ausreichender Wahrscheinlichkeit entdeckt wird. Das INSIKA-Konzept macht diese Kontrollen einfach und sicher.

5 Ausblick

Wie bereits in der Einleitung erörtert, stellen die hier beschriebenen Punkte nur einen Ausschnitt und eine Momentaufnahme der Sicherheitsanalyse dar. Im Rahmen des Abschlusses der Sicherheitsanalyse erfolgen eine Vertiefung der Analyse und die Einbeziehung weiterer Risiken und Angriffsmöglichkeiten.