

# Schutz von Daten aus Registrierkassen vor unzulässigen Veränderungen: Fiskalspeicher vs. INSIKA

Rolf Pleßmann  
QUORiON Data Systems GmbH  
An der Klinge 6, 99095 Erfurt  
rd@quorion.de

Es gibt eine weltweite Entwicklung in der zunehmend von Finanzbehörden Fiskalgesetze erlassen werden, die den Einsatz von Fiskalkassen vorsehen und in denen besondere Anforderungen zur Datenspeicherung an Kassensysteme gestellt werden, bei fortschreitender technischer Entwicklung.

Im Folgenden wird ein Vergleich des INSIKA-Projektes gegenüber anderen Fiskallösungen, wie sie in Ländern mit Fiskalgesetzen eingesetzt werden, betrachtet. Hierbei werden zum einen die Control-Unit, wie sie im Fiskalland Schweden eingesetzt wird, der INSIKA Lösung TIM (Tax Identification Module) gegenübergestellt und zum anderen herkömmliche Fiskalspeicher dem INSIKA Konzept.

## 1 Datenzugriff auf Registrierkassen

### 1.1 Gesetzliche Anforderungen an die Aufbewahrung digitaler Unterlagen bei Bargeschäften

Das Bundesministerium der Finanzen (BMF) hat seine Anforderungen an die Aufbewahrung digitaler Unterlagen bei Bargeschäften am 25. November 2010 weiter konkretisiert [1].

Die Vorgaben gelten übrigens nicht nur für sämtliche in Registrierkassen erfasste Geschäftsvorfälle wie Barverkäufe, Stornobuchungen oder Entnahmen, sondern auch für Waagen mit Registrierkassenfunktion, Taxametern und sogar Wegstreckenzählern.

Dazu kommt, dass in der Praxis neben der eigentlichen Finanzbuchhaltung auch Barverkäufe bei Au-

ßenprüfungen immer mehr automatisiert kontrolliert werden. Die Finanzbehörden verlangen dafür jetzt die sichere Aufbewahrung und den Zugriff auf alle Kassendaten.

### 1.2 Aufbewahrungs- und Protokollierungspflichten

Alle steuerlich relevanten Einzeldaten einschließlich etwaiger mit dem Gerät elektronisch erzeugter Rechnungen im Sinne des Umsatzsteuergesetzes (§ 14 UStG [2]) müssen vollständig, unveränderbar und unverdichtet aufbewahrt werden. Die digitalen Unterlagen und die Strukturinformationen müssen in einem (maschinell) auswertbaren Datenformat vorliegen.

## 2 Revisionsssicheres System zur Aufzeichnung von Kassenvorgängen

Das Datenvolumen, die rechtliche Bedeutsamkeit und die Sicherheitsanforderungen an Kassendaten steigen also stetig. Daraus resultiert die Aufgabe revisionsssichere Systeme zur Aufzeichnung von Kassenvorgängen zu entwickeln und einzusetzen.

### 2.1 INSIKA-Projekt (Integrierte Sicherheitslösung für messwertverarbeitende Kassensysteme)

INSIKA wurde im Jahre 2008 gestartet, um eine Revisionsicherheit in Kassensystemen zu erreichen und

einer in 2008 geplanten Gesetzesvorlage zu entsprechen. Hierzu wurde ein Projektkonsortium aus PTB und mehreren Kassenherstellern gebildet, um ein technisches System zur kryptografischen Absicherung von Kassendaten zu entwerfen, zu implementieren und in der Praxis zu testen.

Das INSIKA-Projekt war ein im Rahmen des BMWi-MNPQ-Programms gefördertes Vorhaben. Im Projekt wurde unter Leitung der PTB und den Projektpartnern aus der Kassenbranche ein fertiges technisches System TIM („Tax Identification Module“) für Kassen und Kassensysteme entwickelt und für die praktische Anwendung bereitgestellt.

INSIKA setzt moderne kryptografische Signaturverfahren ein. Die sicherheitskritischen Teile des Systems laufen auf einer Smartcard, die einen sehr hohen und unabhängigen prüfbareren Sicherheitsstandard bietet.

Der Manipulationsschutz basiert auf einer digitalen Signatur, die im Einsatzfall von einer durch eine autorisierte zentrale Stelle ausgegebenen Smartcard erzeugt wird. Damit können Daten nicht unerkannt verändert werden. INSIKA ist vergleichsweise einfach zu implementieren und klassischen Fiskalspeicherlösungen in jeder Hinsicht deutlich überlegen.

### **3 QUORION Data Systems GmbH**

Die QUORION Data Systems GmbH als Kassenhersteller ist einer der Projektteilnehmer des INSIKA-Projektes. QUORION entwickelt und produziert Kassen, Kassensysteme vom Low-End-Bereich bis zum PC-basierten High-End-Touchscreen-System und eine Vielzahl von Systemkomponenten, siehe Abbildung 1.

Weltweit sind mehr als 240 000 QUORION Kassen installiert. Eine Spezialisierungsrichtung ist dabei die Entwicklung von Hard- und Software, sowie die Produktion von Kassen für den weltweiten Einsatz in Ländern mit Fiskalgesetzen und speziellen Sicherheitsanforderungen für die Datensicherung.

In Tabelle 1 sind typische Ausprägungen von Fiskallösungen und die Länder, in denen das jeweilige Konzept eingesetzt wird, zusammengestellt.

QUORION baut seit 15 Jahren Fiskalkassen und gegenwärtig sind 110 000 zugelassene Fiskalkassen in 23 Ländern mit Fiskalgesetzgebung im Einsatz. In vier weiteren Ländern befinden sich QUORION-Kassen und Kassensysteme in der Zulassungsphase.

### **3.1 Einsatz von QUORION Kassen in Ländern mit Fiskalgesetzen**

QUORION ist auf dem Markt der weltweiten Fiskalkassenhersteller in der Spitzengruppe positioniert und hat umfangreiche Erfahrungen in der Zulassung und dem praktischen Einsatz solcher Systeme gesammelt.

Daher hat sich QUORION, als die Arbeitsgruppe für das Projekt INSIKA gebildet wurde, beworben, um an dem Projekt teilzunehmen.

Die Motivation war es, eine effiziente und sichere kryptografische Lösung für eine revisionssichere Datenspeicherung mit zu gestalten. QUORION weiß aus jahrelanger praktischer Erfahrung, dass die bisherigen Fiskallösungen überwiegend mit konventionellen Speichern und zum großen Teil auch mit durchaus angreifbaren, mechanischen Hardwaresicherungen für den Datenschutz ausgestattet werden.

Besonders negativ sind die immensen materiellen Aufwände für die Entwicklung von Kassen und Kassensystemen für die bisherigen Fiskallösungen, die von Land zu Land durch zum Teil groteske Sicherheitsanforderungen bestimmt werden, aber keinen ausreichenden Nutzen für die Datensicherung haben.

Die Zulassungen von Kassen und Kassensystemen ziehen sich in manchen Ländern zum Teil über Jahre hin und sind nicht selten auch von schwer durchschaubaren Abläufen bekleidet, zum Teil betragen die Zulassungskosten bis zu 200 000 Euro.

### **4 Vergleich zwischen Fiskalspeicher und INSIKA Konzept-TIM („Tax Identification Module“)**

Tabelle 2 vergleicht anhand ausgewählter Kriterien Fiskalspeicher mit dem INSIKA-Konzept-TIM („Tax Identification Module“).

### **5 Vergleich Control Unit Schweden – TIM („Tax Identification Module“)**

Im Vergleich mit der schwedischen Fiskallösung wird deutlich welche Vorteile die INSIKA-Lösung bietet.

Seit 01.07.2010 gilt in Schweden ein neues Fiskalgesetz. Der Gesetzgeber gibt als Zweck für das Gesetz an, es soll ehrliche Unternehmen vor unlauterem Wettbewerb schützen. Demnach müssen die Unternehmen beim Verkauf von Waren und Dienstleistungen (Dienstleister sind z.B. auch Zahnärzte mit eigener Praxis) gegen Barzahlung gewährleisten, dass ihre



**QMP 50 Serie**



**QTouch 2**



**QTouch 10**



**POS Concerto**



**QMP 5000 Terminal**



**QMP 5000 mit eingebauter TIM Karte.**

Abbildung 1: QUORiON Fiskalkassen

Tabelle 1: Typische Ausprägungen von Fiskallösungen und deren Einsatzgebiete

Protected Fiscal Memory (Vergossener Speicher EPROM PROM oder Flash)	Protected Fiscal Memory mit Datentransfer über GPRS Modem zu einem Zentralserver	Lokale Datenspeicherung durch Verschlüsselung / Signatur mit externen Geräten
Bangladesch Brasilien Tschechische Republik Zypern Griechenland Ungarn Italien Kenia Litauen Malta Montenegro Panama Polen Rumänien Venezuela Slowakei	Albanien Bosnien Herzegowina Äthiopien Serbien	Kanada (MEV) Schweden Control Unit (BOXEN)

Tabelle 2: Fiskalspeicher versus INSIKA

Vergleichskriterien	Fiskalspeicher	INSIKA
Zulassungsprüfung und Sicherheitsmaßnahmen	<ul style="list-style-type: none"> <li>- Bauartzulassung nötig</li> <li>- keine Datensignierung</li> <li>- niedriger Sicherheitsstandard</li> </ul>	<ul style="list-style-type: none"> <li>- keine Bauartzulassung</li> <li>- kryptographisches Signaturverfahren</li> <li>- hohe Datensicherheit</li> </ul>
Was passiert bei vollem Speicher?	<ul style="list-style-type: none"> <li>- Kasse blockiert</li> <li>- Speicher muss erneuert werden (Speicher in Gehäuseteil vergossen müssen erneuert werden/ Komplettumbau)</li> </ul>	<ul style="list-style-type: none"> <li>- beliebiger neuer Speicher oder neues TIM kann angeschlossen werden</li> </ul>
Datenhandling	<ul style="list-style-type: none"> <li>- Z Bericht Daten werden in Speicher geschrieben zum Tagesabschluss</li> </ul>	<ul style="list-style-type: none"> <li>- jede Transaktion wird gespeichert und auf den Kassenbeleg gedruckt</li> <li>- mit jeder Transaktion werden die Zähler im TIM aktualisiert</li> </ul>
Nachträgliche Implementierung in einer Kasse	<ul style="list-style-type: none"> <li>- verbunden mit hohem Aufwand und Kosten</li> <li>- umfangreiche mechanische Sicherungslösungen</li> <li>- oft komplettes Neudesign von Mainboard und Komponenten,</li> <li>- umfangreiche Zulassungsprozeduren</li> </ul>	<ul style="list-style-type: none"> <li>- schnell, einfach und günstig</li> <li>- Anbindung eines handelsüblichen Kartenlesers (intern / extern)</li> <li>- Softwareanpassung im Vergleich zur Fiskalspeicherlösung ist wesentlich geringer</li> <li>- keine Zulassungen für Kassen und Kassensysteme</li> </ul>
Prüfung der gespeicherten Daten	<ul style="list-style-type: none"> <li>- Journal liegt in Papierform vor, dadurch nur manuelle, oft fehleranfällige Prüfung möglich</li> </ul>	<ul style="list-style-type: none"> <li>- Transaktionen liegen signiert als elektronisches Journal vor, dadurch schnelle automatisierte Prüfung aller Belege möglich</li> <li>- revisionssichere Datenspeicherung</li> </ul>
Sicherheitsausführung	<ul style="list-style-type: none"> <li>- mechanische Sicherung (angreifbar)</li> </ul>	<ul style="list-style-type: none"> <li>- digitale Signatur bietet höchste Datensicherheit</li> </ul>

Unternehmen mit zertifizierten Kassen und separaten Kontrolleinheiten (Control Units) ausgerüstet sind.

Die Control Unit ist mit der Kasse über eine serielle RS232-Schnittstelle verbunden.

Die Control Unit speichert Informationen über alle Transaktionen. Die Manipulationssicherung der Daten erfolgt zweistufig. In der ersten Stufe wird ein Control Code erzeugt, der aus einem Hashwert der Transaktionsdaten und den verschlüsselten, aktuellen Ständen ausgewählter Zähler besteht. Der Control Code wird sowohl in der Control Unit als auch im elektronischen Journal der Kasse gespeichert.

In der zweiten Stufe werden alle in der Control Unit gespeicherten Daten verschlüsselt. Als kryptografische Verfahren kommen HMAC-SHA1 und AES256-CBC zum Einsatz.

Die Control Unit muss eine Speicherkapazität für sieben Millionen Transaktionen bieten. Daraus ergibt sich ein Speicherbedarf von min. 2 GB. Einmal gespeichert, können die Daten nur mit einer SD-Card über einen in der Control Unit integrierten SD-Kartenslot von den Steuerinspektoren ausgelesen werden. Der Kartenschlitz vor dem SD-Kartenslot ist mit einem fälschungssicheren Sicherheitsverschluss ausgestattet, um unbefugten Zugriff zu verhindern.

Die korrekte Funktionsweise der Control Unit muss durch eine von SWEDAC (schwedische Behörde für Akkreditierung und Konformitätsbewertung) akkreditierte Zulassungsstelle bestätigt werden.

### **5.1 Control Unit Schweden in Praxis mit hohen Aufwänden verbunden**

Diese Lösung bedingt einen großen Aufwand an Organisation und Kosten für Hersteller, Prüfinstitute, Finanzbehörden und Nutzer.

Die Control Unit ist ein zusätzliches, separates Gerät (Box). Die Kassen die an eine Control Unit angeschlossen werden, müssen von der Steuerbehörde zertifiziert sein und haben spezifische und funktionale Anforderungen an die Hard- und Software. Zu allen Bauelementen der Control Unit werden Herstellererklärungen und Liefernachweise für mindestens 10 Jahre hinterlegt und dienen als Garantie, dass in dieser Zeit keine technischen Änderungen erfolgen. Um eine hohe Zuverlässigkeit der Geräte zu gewährleisten, müssen Bauteile mit einer MTBF von mindestens 7 Jahren verwendet werden.

Weiterhin sind aufwendige mechanische Sicherungen der Box zu treffen. Dies bezieht sich unter anderem auf die Festigkeit und Stabilität der Box. Es ist eine umfangreiche Normenkonformität nachzuweisen, wie EMV (EN 55022 Klasse B; EN 55024;

EN 60950-1) Festigkeit und Klima. Die Produktion darf nur in besonders gesicherten Räumen erfolgen. Der Zulassungsprozess der Control Unit ist mit einem hohen Kosten- und Zeitaufwand verbunden. Es erfolgt eine gesonderte Zertifizierung des Management-Systems des Herstellers durch ein schwedisches Prüfinstitut, jährliche Audits eingeschlossen. Der Kosten liegen mehrfach höher als bei ISO 9001:2008-Zertifizierungen und Audits.

Für die Herstellung gibt das schwedische Finanzministerium Codeschlüssel aus, das gesamte Schlüsselhandling ist aufwendig. Die Schlüsselausgabe erfolgt min. 2x im Jahr nach Antragsstellung des Herstellers. Für den Transport des Schlüssels sind umfangreiche Sicherheitsvorkehrungen vorgeschrieben. Für Aufbewahrung und Handling des Schlüssels beim Hersteller gilt dasselbe; die Aufbewahrung muss in vorgeschriebenen Tresoren erfolgen, agierende Personen werden verpflichtet und müssen der Steuerbehörde bekannt gegeben werden. Außerdem gilt bei der Anwendung des Schlüssels immer das 4-Augen-Prinzip.

### **5.2 INSIKA TIM („Tax Identification Module“)**

Das Modul ermöglicht durch ein kryptografisches Signaturverfahren eine revisionssichere Datenspeicherung. Vorteile liegen unter anderem im wesentlich geringeren Kostenaufwand gegenüber herkömmlichen Fiskalspeicherlösungen. Es ist problemlos in bereits vorhandene Kassen- und Kassensysteme implementierbar. Dadurch entstehen keine aufwendigen Zulassungen für Geräte und es ist keine Zertifizierung der Kassensoftware nötig.

Ein offen dokumentiertes Konzept stellt eine einfache Prüfbarkeit der Daten durch die Finanzbehörden sicher, mechanische Manipulationssicherungen werden nicht benötigt. Gegenüber herkömmlichen Fiskalsystemen mit Fiskalspeicher oder Lösungen wie in Schweden ist daher ein deutlich geringerer Implementierungsaufwand notwendig. Eine Wettbewerbsbeschränkung besteht nicht.

## **6 Fazit**

Mit dem Einsatz eines im INSIKA-Projekt entwickelten TIM („Tax Identification Module“) in Kassen und Kassensystemen steht eine moderne technische Lösung zur Verfügung, die wesentliche Vorteile bei allen Aufwendungen für die Hersteller, die Finanzbehörden und Nutzer gegenüber den bisherigen Fiskallösungen hat und revisionssichere Datenspeicherung unterstützt.

Für das ständig zunehmende Datenvolumen, die rechtliche Bedeutsamkeit und die Sicherheitsanforderungen an die Datensicherheit wird die Anwendung derartiger Methoden bald alltäglich sein und unsere öffentliche, wirtschaftliche und finanzielle Infrastruktur wesentlich mittragen.

Die Datensicherheit wird deshalb zukünftig nicht nur für kommunikativ fließende Daten, sondern auch für das Handling von Daten in Geräten oder auf materiellen Trägern wesentlich mehr im Mittelpunkt aller Bemühungen in der Forschung, Entwicklung und in der praktischen Nutzung stehen.

## Literatur

- [1] BMF. *BMF-Schreiben vom 26.11.2010: Aufbewahrung digitaler Unterlagen bei Bargeschäften*. Bundesrepublik Deutschland, Bundesministerium der Finanzen, Nov. 2010. URL: <http://bundesfinanzministerium.de/>.
- [2] BMJ. *Umsatzsteuergesetz (UStG)*. Version 07.12.2011. Bundesrepublik Deutschland, Bundesministerium der Justiz, Dez. 2011. URL: [http://www.gesetze-im-internet.de/ustg\\_1980/index.html](http://www.gesetze-im-internet.de/ustg_1980/index.html).